Datensicherheit und Datenschutz - Skepsis gegenüber Digitalisierung abbauen

1. Darstellung der Notwendigkeit von Datenschutz/- sicherheit

Die digitale Sicherheit ist ein entscheidender Faktor für den Wirtschaftsstandort Deutschland. Dabei stehen insbesondere kleine und mittelständische Unternehmen (KMU) und viele regionale Behörden bei der Thematik vor großen Herausforderungen. Hier gilt es einen Überblick zu möglichen Schutzmaßnahmen zu geben, um individuelle Handlungsoptionen ableiten zu können.

Allein 2022 gab es laut Bundeskriminalamt über 130.000 gemeldete Vorfälle im Bereich Cybercrime, Tendenz steigend. Als Cybercrime werden alle Straftaten bezeichnet, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden. Dazu zählen im engeren Sinne Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten. Im erweiterten Sinne Straftaten, die mittels Informationstechnik begangen werden, aber auch in der analogen Welt stattfinden könnten.

Der Digitalverband Bitkom untersucht zusammen mit dem Bundesamt für Verfassungsschutz seit 2015 jährlich, wie es um die deutsche Wirtschaft beim Thema Wirtschaftsschutz bestellt ist. Allein 2023 entstand der deutschen Wirtschaft ein Schaden von fast 206 Milliarden Euro.
Die Ergebnisse der aktuellen Studie 2023 unterstreichen, dass in Zeiten der zunehmenden Vernetzung all unserer Lebensbereiche die Resilienz der deutschen Wirtschaft gegen die steigenden Gefahren aus dem Cyberraum weiter ausgebaut werden muss. Es gilt, einen ganzheitlichen und nachhaltigen Wirtschaftsschutz zu etablieren. Dabei muss stets ein enger und vertrauensvoller Erfahrungsaustausch mit den Sicherheitsbehörden aufrechterhalten werden.

Internetkriminalität bezeichnet nach der Definition des Bundeskriminalamtes Straftaten, die im Internet oder auf Basis der Technologien des Internets begangen werden. Sie sind abzugrenzen von Straftaten im Bereich der Computerkriminalität („Cybercrime im engeren Sinne“) bei denen zwar Computer als Tatwaffe, aber nicht das Internet als solches, von Bedeutung sind.

Schwerpunkt des „Bundeslagebild Cybercrime“ des BKS sind die Delikte, die sich z. B. gegen das Internet und informationstechnische Systeme richten – die sog. Cybercrime im engeren Sinne (CCieS). Die einzelnen Delikte dieses Phänomenbereichs werden unter Punkt 8.1 des „Bundeslagebildes“ des BKA genauer seit 2020 beschrieben. Das Tatmittel Internet gewinnt im Zuge fortschreitender Digitalisierung in fast allen Deliktsbereichen zunehmend an Bedeutung.

Grundlage für den statistischen Teil des Lagebildes sind die Daten der Polizeilichen Kriminalstatistik (PKS). Hier wird das sog. Hellfeld abgebildet, also die polizeilich bekannt gewordene Kriminalität. Valide Aussagen und Einschätzungen zu Art und Umfang des komplementären Dunkelfeldes, also den Straftaten, die der Polizei nicht bekannt werden, können aus den statistischen Grunddaten der PKS nicht abgeleitet werden.

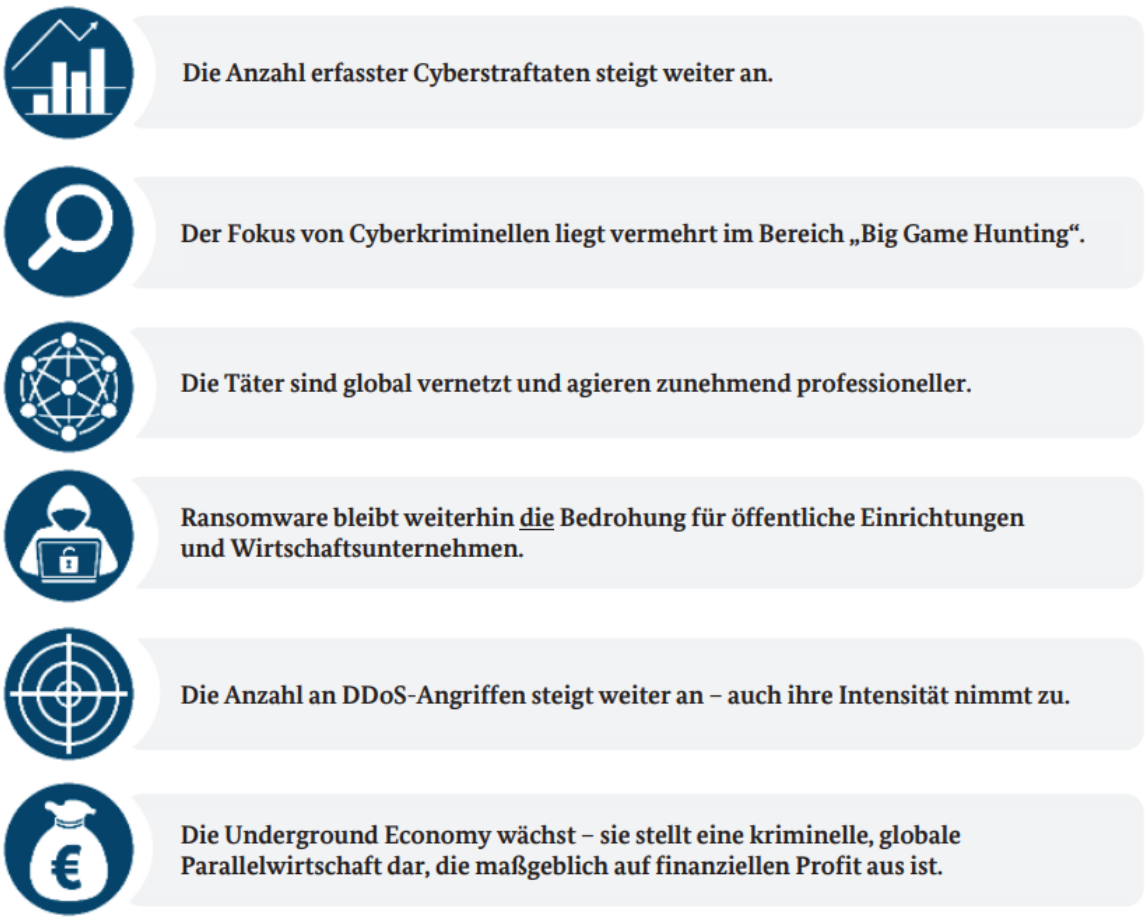


Abbildung 1 Die wesentlichen Aspekte der Cybercrime in Deutschland seit 2020, Quelle: BKA

Stichpunkte für eine Status-Aussage

2. Exemplarische Anfälligkeiten

Um an digitale Identitäten bei KMU (und anderen typischen Opferprofilen) zu gelangen, setzten Cyberkriminelle auch in 2020 auf altbekannte Methoden, allen voran Spam-Mail-Kampagnen und professionelle Phishing-Mails mit maliziösen Office-Anhängen. Der Spamversand kann über zuvor kompromittierte oder aber kommerziell angemietete Serverkapazitäten sowie über von Angreifern gestohlene legitime E-Mail-Accounts stattfinden.

Auch das aggressive Eindringen in ein System via Brute-Force-Angriff auf mangelhaft geschützte Remote-Desktop-Protokolle (RDP) ist ein beliebter Eintrittsvektor in Zielsysteme. Über diese werden wiederum Schadprogramme oder missbräuchlich eingesetzte Pentesting-Tools4 eingeschleust. In Folge dessen werden Daten ausgespäht und an die Täter weitergeleitet.

Angriffe auf KMU und Gebäudesektor

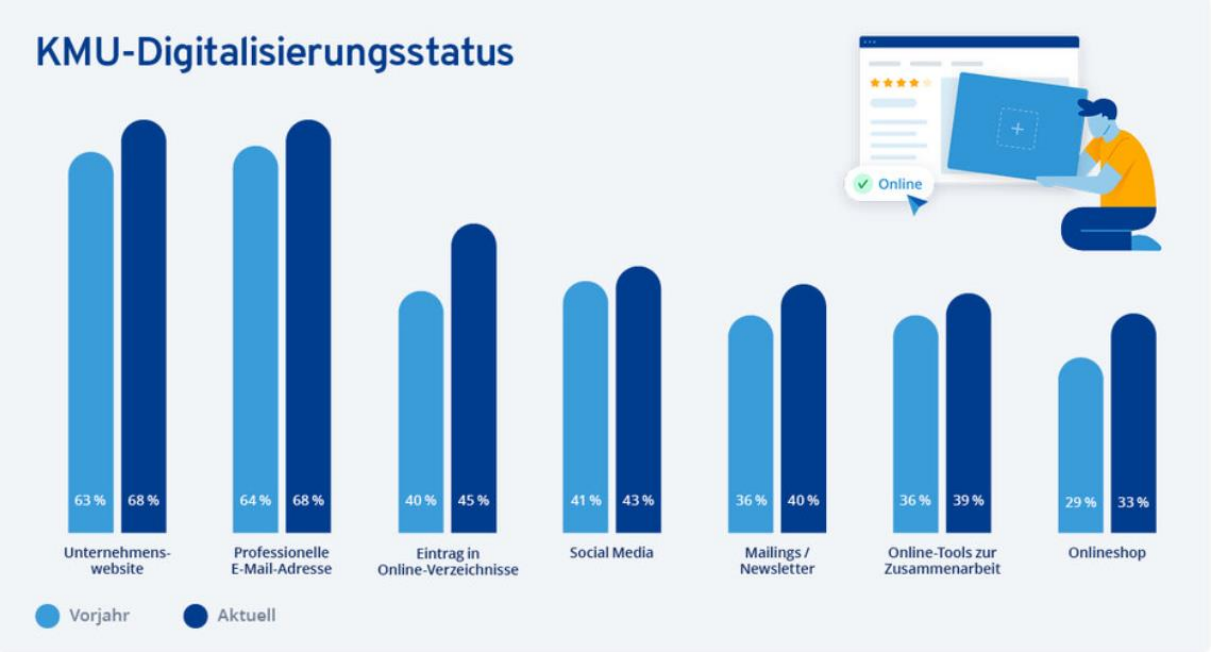
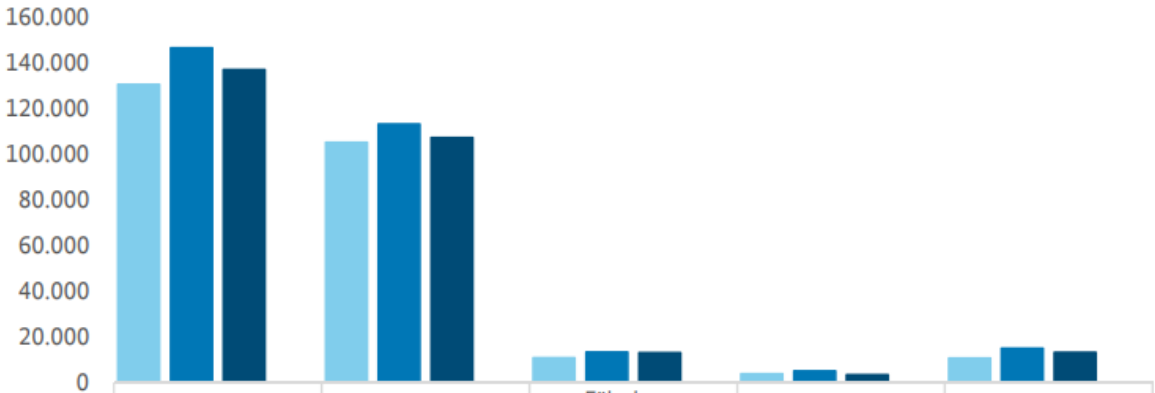


Abbildung 2 KMU-Digitalisierungsstatus 2023, Quelle: IONOS

Kleine und mittelständische Unternehmen (KMU) stehen im Fokus der Ransomware-Akteure. Die Folgen eines solchen Angriffs können für KMU teilweise existenzbedrohend sein. KMU sind größte Adressatengruppe von Cybercrime:



	CC gesamt	Computerbetrug	Fälschung beweiserheblicher Daten, Täuschungen im Rechtsverkehr bei Datenverarbeitung	Datenveränderung, Computersabotage	Ausspähen von Daten einschl. Vorbereitungs-handlungen und Datenhelerei
2020	130.477	105.049	10.895	3.770	10.763
2021	146.363	113.002	13.390	5.053	14.918
2022	136.865	107.165	13.043	3.451	13.206
Diff. zu 2021	-6,5%	-5,2%	-2,6%	-31,7%	-11,5%

Abbildung 3 Fallaufkommen Cybercrime seit 2020 nach Deliktsbereichen, Qualle: BKA

Der Faktor Mensch ist hier das größte „Einfallstor“: Cyberkriminelle analysieren genau die Schwachstellen der KMU über deren Beschäftigte. Arglosigkeit, Naivität, Gleichgültigkeit

oder gar aktive Schadensinitiativen von Saboteuren (aus welchen innerbetrieblichen Gründen auch immer) sind willkommene Umsetzungs-Helfer der Kriminellen.

Abbildung 4 Einfallstore E-mail und Phishing, Quelle: BKA

Dieser simpel erscheinende Ablauf sowie der Einsatz bereits bekannter Angriffsarten bleibt weiterhin ein elementarer Bestandteil der Cybercrime. Besonders gefährliche Malware-Familien (Schadprogramme) wie „Emotet“ und „Trickbot“ sowie einige Ransomware-Familien werden via E-Mail distribuiert. Die dadurch entstehende Sicherheitslücke kann zu einer Gefahr werden und schwerwiegende Folgen für die KMU mit sich bringen.

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) erhebt fortlaufend die sogenannten Abwehr-Indizes, die das Aufkommen und die Entwicklung von Malware-Angriffen per E-Mail auf die Netze des Bundes sowie die Menge präventiver Sperrungen von maliziösen Webseiten messen.

Der Einsatz von Malware ist und bleibt elementarer Bestandteil der CCieS – kaum eine Straftat wird ohne Malware oder missbräuchlich eingesetzte Tools begangen. Die Bandbreite an Funktionalitäten der bekannten Malware-Familien ist äußerst groß. In der folgenden Liste werden die am häufigsten eingesetzten Malware-Arten vorgestellt:

Downloader (bzw. Dropper/ Loader)

- Dient primär als "Einfallstor": Setzt sich im infizierten System fest und lädt weitere Arten von Malware nach.
- *Beispiel: Emotet*

Information-Stealer

- Stehlen alle möglichen Arten von Daten über das infizierte System z. B. digitale Identitäten, Passwörter, Online-Banking-Daten etc. Können ebenfalls die Aufzeichnung von Tastaturanschlägen und die unberechtigte Aufnahme von Screenshots umfassen.
- *Beispiel: Trickbot, Qbot, Gootkit*

Ransomware

- Verschlüsselt das System und erpresst damit das Opfer.
- Zur Entschlüsselung wird eine digitale Lösegeldsumme gefordert, die an die Täter gezahlt werden soll.
- *Beispiel: Doppelpaymer, Ryuk, Sodinokibi, Conti, Maze*

Adware

- Software, welche ungewollte Werbeinhalte anzeigt. Im Vergleich zu anderen Varianten von Schadsoftware werden im Normalfall keine Funktionen des Betriebsgerätes beeinträchtigt.
- *Beispiel: Silver Sparrow*

Abbildung 5 Darstellung typischer Malware-Arten, Quelle: BKA

Ransomware

Ransomware gehört zu den primären Bedrohungen für KMU und andere Opfergruppen. Von allen Modi Operandi im Phänomenbereich Cybercrime besitzt Ransomware das höchste Schadenspotenzial. Eine Infektion mit Ransomware und eine damit zusammenhängende Verschlüsselung des Systems kann für jede Art von Unternehmen zu massiven und kostenintensiven Geschäfts- bzw. Funktionsunterbrechungen führen.

Attacken auf KRITIS, z. B. Krankenhäuser, Stadt- und Wasserwerke, zeigen, dass erfolgreiche Ransomware Angriffe drastische Folgen für die Zivilbevölkerung nach sich ziehen und elementare Services des öffentlichen Geschehens sabotieren können.

Der Bereich der „Ransomware“ ist ein weiterer Gefahrenpunkt für KMU mit steigendem Erpressungspotenzial:

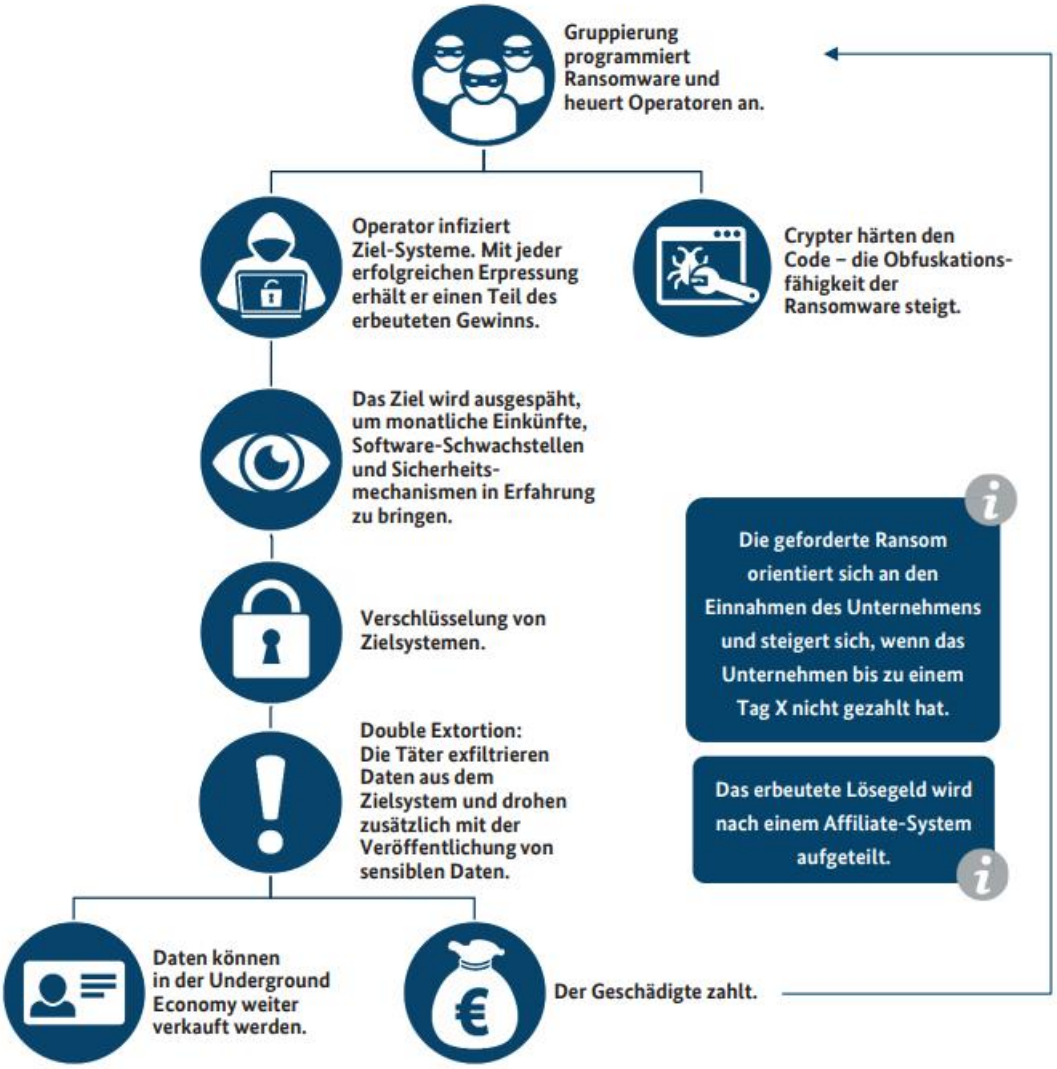


Abbildung 6 Ransomware-Wertschöpfungskette, Quelle: BKA

Ddos

DDoS-Angriffe zielen grundsätzlich darauf ab, eine Überlastung des Zielsystems herbeizuführen und verursachen so gezielt Schäden bei den angegriffenen Personen und Organisationen/Unternehmen. Sowohl in Bezug auf die Anzahl als auch die Intensität war in den letzten Jahren eine stete Steigerung bei den DDoS-Angriffen erkennbar.

DDoS-Angriffe (oder deren Androhung) erhielten während der durch die Pandemie forcierten Verlagerung von Arbeiten ins Homeoffice insgesamt ein höheres Bedrohungs- und Schädigungspotenzial. Dabei sind DDoS-Angriffe spätestens seit dem zweiten Lockdown im November 2020 ein einzukalkulierendes Risiko nicht nur für KMU, sondern auch für das Schulwesen, insb. mit Blick auf Home-Schooling.

Die zunehmende Digitalisierung in allen Lebensbereichen schafft mehr Tatgelegenheiten, während das Phänomen des „Cybercrime-as-a-Service“ die Eintrittsschranken bei der Begehung von Straftaten im Cyber-Bereich weiter absenkt. Darüber hinaus steigt mit jedem erfolgreichen Angriff das kriminelle Potenzial der Underground Economy und damit ihre Möglichkeiten, neue Malware zu entwickeln und komplexe Angriffe durchzuführen. Neben dem „Faktor Mensch“ sind vor allem unsichere IT-Systeme ein beliebtes Einfallstor. Unzureichend gesicherte oder falsch konfigurierte Datenbanken, kritische Schwachstellen in Remote-Zugängen oder fehlende Sicherheitsprogramme und Schutzmaßnahmen für gewerbliche oder private IT-Infrastrukturen ermöglichen es Angreifern, in ein Zielsystem einzudringen und es zu kompromittieren.

Der Phänomenbereich der Cybercrime im engeren Sinne (CCieS) wird durch eine hohe Arbeitsteilung zwischen Tatbeteiligten sowie der für die Begehung der Gesamttat notwendigen Tatkomponenten geprägt. Nur noch wenige Cyberkriminelle können heutzutage ihre Taten alleine und ohne wesentliche Unterstützungshandlungen Dritter begehen. Daher kommt es zu einer stetig voranschreitenden Spezialisierung einzelner Cybercrime-as-a-Service-Anbieter. Das wiederum ermöglicht auch technisch weniger versierten Tätern komplexere Straftaten zu begehen. Folglich können die entsprechenden Akteure alle technisch komplexen Tatbeiträge zunehmend outsourcen und dafür kompetente Dienstleister einkaufen. Hierbei konnten, nach aktuellem Ermittlungsstand des BKA, neun essentielle Säulen identifiziert werden:

Abbildung 7 Die 9 Säulen der Cybercrime, Quelle: BKA

2.1. Es existiert ein Problem => z.B. Anzahl an Angriffen auf KMU und Gebäudesektor

Exemplarische Anfälligkeiten im Zusammenhang mit Datenschutz und -sicherheit sind potenzielle Schwachstellen oder Schwachpunkte in einem System, die es Angreifern ermöglichen könnten, auf sensible Informationen zuzugreifen, sie zu stehlen, zu ändern oder anderweitig zu manipulieren. Diese Schwachstellen können in verschiedenen Teilen eines Systems auftreten, sei es in der Software, der Hardware, den Netzwerkverbindungen oder sogar im Verhalten der Benutzer:

1. **Unzureichende Passwortsicherheit**: Schwache Passwörter oder das Verwenden von leicht zu erratenden Passwörtern erhöhen das Risiko eines unbefugten Zugriffs.
2. **Veraltete Software und Systeme**: Wenn Software oder Betriebssysteme nicht auf dem neuesten Stand gehalten werden, können bekannte Sicherheitslücken ausgenutzt werden.
3. **Fehlende Verschlüsselung**: Daten, die während der Übertragung nicht verschlüsselt sind, könnten von Angreifern abgefangen und gelesen werden.
4. **Fehlende Zugriffskontrollen**: Wenn Systeme nicht angemessen konfiguriert sind, könnten unbefugte Benutzer oder Programme auf sensible Informationen zugreifen.
5. **Schwachstellen in Drittanbieter-Software**: Wenn eine Anwendung von einem Drittanbieter verwendet wird und dieser nicht regelmäßig Sicherheitsupdates bereitstellt, kann dies ein Einfallstor für Angreifer sein.
6. **Phishing und Social Engineering**: Durch Täuschung von Benutzern können Angreifer versuchen, an ihre Anmeldeinformationen oder andere sensible Informationen zu gelangen.
7. **Malware und Viren**: Schadhafte Software kann in ein System eindringen und dort Schaden anrichten, indem sie Daten stiehlt oder beschädigt.
8. **Mangelnde Schulung und Bewusstsein der Benutzer**: Unwissende oder unachtsame Benutzer könnten versehentlich Sicherheitsverletzungen verursachen, z.B. durch das Öffnen von gefährlichen E-Mail-Anhängen.
9. **Fehlende Datensicherung und Wiederherstellung**: Ohne geeignete Backup- und Wiederherstellungsmechanismen können Daten bei einem Vorfall verloren gehen.
10. **Physische Sicherheitslücken**: Zugang zu Serverräumen oder Geräten ohne ausreichende physische Sicherheitsmaßnahmen kann zu unbefugtem Zugriff führen.

Status Quo der häufig verwendeten Vorkehrungen und deren Wirkung (Sicherheit und Effekte

Der Status Quo der häufig verwendeten Vorkehrungen im Umgang mit Bedrohungsszenarien der Datensicherheit kann sich je nach Unternehmen und Branche deutlich unterscheiden. Hier sind einige gängige Vorkehrungen und deren Wirkung:

1. **Firewalls**: Firewalls sind eine grundlegende Sicherheitsmaßnahme, die den Datenverkehr zwischen einem Netzwerk und externen Systemen kontrollieren.

Sie können helfen, unautorisierte Zugriffe zu blockieren und schützen vor bestimmten Arten von Angriffen. Allerdings müssen sie durch permanente Pflege mittels geschulter MA gut konfiguriert und aktualisiert werdene, um effektiv zu sein.

2. **Antivirus-Software**: Antivirus-Programme erkennen und blockieren schädliche Software wie Viren, Trojaner und Malware. Sie sind eine erste Verteidigungslinie, aber sie allein können nicht alle Arten von Angriffen abwehren.
3. **Verschlüsselung**: Verschlüsselung schützt Daten vor unbefugtem Zugriff, indem sie sie in einen Code umwandelt, der nur mit dem richtigen Schlüssel entschlüsselt werden kann. Sie ist besonders wichtig für die Sicherheit von übertragenen Daten.
4. **Regelmäßige Sicherheitsupdates und Patch-Management**: Das regelmäßige Aktualisieren von Software und Betriebssystemen ist entscheidend, um bekannte Sicherheitslücken zu schließen und Angriffsvektoren zu minimieren.
5. **Zugriffskontrollen und Authentifizierung**: Durch die Implementierung von Zugriffsbeschränkungen und starken Authentifizierungsmechanismen können Unternehmen sicherstellen, dass nur autorisierte Benutzer auf bestimmte Systeme und Daten zugreifen können.
6. **Schulung und Sensibilisierung der Mitarbeiter**: Eine gut informierte Belegschaft ist ein wichtiger Bestandteil der Datensicherheit. Mitarbeiter sollten in der Lage sein, Phishing-E-Mails zu erkennen und bewusst mit sensiblen Informationen umzugehen. Alltags-Verhaltensweisen sind dabei eine bewusstseins-bildende Grundlage im Gespräch mit einzelnen MA oder auch in der Gruppe
7. **Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS)**: Diese Systeme überwachen den Netzwerkverkehr auf verdächtige Aktivitäten und können potenzielle Angriffe erkennen und blockieren.
8. **Data Loss Prevention (DLP)**: DLP-Tools helfen dabei, zu verhindern, dass sensitive Daten versehentlich oder absichtlich das Unternehmen verlassen. Sie überwachen den Datenverkehr und setzen Richtlinien zur Verhinderung von Datenlecks um.
9. **Sicherheitsrichtlinien und -verfahren**: Gut dokumentierte Sicherheitsrichtlinien und -verfahren sind entscheidend, um sicherzustellen, dass alle Mitarbeiter wissen, wie sie mit sensiblen Informationen umgehen müssen. Beispielhaft sei hier die DIN ISO 27001 genannt oder auch der BSI-Grundschutz.
10. **Notfallmaßnahmen und Incident Response-Planung**: Es ist wichtig, im Falle eines Sicherheitsvorfalls gut vorbereitet zu sein. Ein gut ausgearbeiteter Incident Response-Plan ermöglicht es, schnell zu reagieren und den Schaden zu begrenzen.

=> so viel wie nötig, nicht wie möglich) für Industrie

Der Grundsatz "so viel wie nötig, nicht wie möglich" im Umgang mit Bedrohungsszenarien der Datensicherheit für Industriebetriebe bedeutet, dass Sicherheitsmaßnahmen der Größe des Unternehmens und dessen Gefährdungsrisiko angemessen und gezielt eingesetzt werden sollen, um die

spezifischen Risiken und Anforderungen des Unternehmens zu berücksichtigen. Hier ist eine strukturierte Herangehensweise, um diesen Grundsatz umzusetzen:

1. **Risikobewertung und Klassifizierung von Daten**:
   - Identifizierung der wichtigsten Daten und Systeme im Industriebetrieb.
   - Bewertung der potenziellen Auswirkungen eines Datenverlusts oder einer Kompromittierung.
   - Einteilung der Daten in verschiedene Kategorien nach ihrer Sensibilität und Kritikalität.
2. **Bedarfsanalyse und Compliance-Anforderungen**:
   - Untersuchung der rechtlichen und regulatorischen Anforderungen, die für den Industriebetrieb gelten (z.B. DSGVO, branchenspezifische Vorschriften).
   - Festlegung der minimal erforderlichen Sicherheitsstandards, um den rechtlichen Vorgaben zu entsprechen.
   - Bewusstseinsbildung über die maximal einsetzbaren Standards, um einen Entscheidungsrahmen der Investitionen abzustimmen.
3. **Zugriffskontrolle und Authentifizierung**:
   - Implementierung von starken Zugriffskontrollen, die sicherstellen, dass nur autorisierte Personen auf bestimmte Daten und Systeme zugreifen können.
   - Verwendung von starken Authentifizierungsmethoden, wie z.B. Multi-Faktor-Authentifizierung.
   - Bei größeren Betrieben: Stellung von physisch anwesenden und geschulten MA, die den in den IT-Systemen fehlenden „Faktir Mensch“ ersetzen.
4. **Datenverschlüsselung**:
   - Identifikation von sensiblen Daten, die während der Übertragung oder Speicherung verschlüsselt werden müssen.
   - Implementierung von Verschlüsselungstechnologien, um die Vertraulichkeit der Daten zu gewährleisten.
5. **Sicherheitsbewusstsein und Schulung**:
   - Schulung der Mitarbeiter zu sicherheitsrelevanten Themen und Best Practices.
   - Sensibilisierung für die Bedeutung der richtigen Handhabung von Daten und möglichen Bedrohungen.
6. **Regelmäßige Audits und Überprüfungen**:
   - Durchführung von regelmäßigen Sicherheitsaudits und -prüfungen, um sicherzustellen, dass die implementierten Sicherheitsmaßnahmen angemessen und effektiv sind.
7. **Notfallplanung und Incident Response**:
   - Erstellung eines detaillierten Notfallplans, der klare Schritte zur Bewältigung von Sicherheitsvorfällen enthält. Ein praxisnah konstruierter Fall kann im Dialog mit Fachleuten als Vorlage für den Ernstfall dienen.
   - Schulung der Mitarbeiter zur effektiven Umsetzung des Notfallplans im Ernstfall.
8. **Datenminimierung und Berechtigungsmanagement**:

- Reduktion von Daten auf das notwendige Minimum, um das Risiko zu minimieren.
- Regelmäßige Überprüfung und Anpassung von Berechtigungen, um sicherzustellen, dass nur autorisierte Benutzer Zugriff haben.

9. **Technische Sicherheitsmaßnahmen**:
   - Implementierung von spezifischen technischen Lösungen, die den Bedürfnissen des Industriebetriebs entsprechen, wie z.B. Intrusion Detection Systems, Firewalls, etc.
10. **Kontinuierliche Verbesserung und Anpassung**:
    - Regelmäßige Überprüfung und Anpassung der Sicherheitsmaßnahmen basierend auf neuen Bedrohungsszenarien, technologischen Entwicklungen und geschäftlichen Anforderungen.

Für Gebäude

Der Grundsatz "so viel wie nötig, nicht wie möglich" im Umgang mit Bedrohungsszenarien der Datensicherheit für Gebäude und deren Verwalter unterscheidet sich teils deutlich von den vorab berichteten Maßnahmen:

1. **Risikobewertung und Klassifizierung von Daten**:
   - Identifizierung der wichtigsten Daten und Systeme im Gebäudeverwaltungsprozess.
   - Bewertung der potenziellen Auswirkungen eines Datenverlusts oder einer Kompromittierung, speziell auch auf das ERP-System.
   - Einteilung der Daten in verschiedene Kategorien nach ihrer Sensibilität und Kritikalität, Trennung von technischen von wirtschaftlichen Daten.
2. **Bedarfsanalyse und Compliance-Anforderungen**:
   - Untersuchung der rechtlichen und regulatorischen Anforderungen, die für die Gebäudeverwaltung gelten (z.B. Datenschutzbestimmungen).
   - Festlegung der minimal erforderlichen Sicherheitsstandards, um den rechtlichen Vorgaben zu entsprechen, Erkennung der optional einsetzbaren Systeme höherer Qualifikation und wirtschaftliche Abwägung durch Hinzuziehung externer Fachleute.
3. **Zugriffskontrolle und Authentifizierung**:
   - Implementierung von starken Zugriffskontrollen, die sicherstellen, dass nur autorisierte Personen auf bestimmte Daten und Systeme zugreifen können.
   - Verwendung von starken Authentifizierungsmethoden, wie z.B. Passwörter, Karten, biometrische Verfahren.
   - Ergänzung durch physische Anwesenheit von geschulten Sicherheits-MA.
4. **Datenminimierung und Berechtigungsmanagement**:
   - Hier gelten die gleichen Regeln wie bereits beschrieben
5. **Sicherheitsbewusstsein und Schulung**:
   - dto
6. **Regelmäßige Audits und Überprüfungen**:
   - dto
7. **Notfallplanung und Incident Response**:
   - dto

8. **Technische Sicherheitsmaßnahmen**:
    - Implementierung von spezifischen technischen Lösungen, die den Bedürfnissen der Gebäudeverwaltung entsprechen, wie z.B. Zutrittskontrollsysteme und eine Übersicht berechtigter Personen ggf. hochskalierte Sufen bis zum Sicherheitspoersonal), Videoüberwachung, etc.,
9. **Kontinuierliche Verbesserung und Anpassung**:
    - Regelmäßige Überprüfung und Anpassung der Sicherheitsmaßnahmen basierend auf neuen Bedrohungsszenarien, technologischen Entwicklungen und geschäftlichen Anforderungen, Durchspielen von Angriffs-Szenarien an ausgesuchten Zugängen der Gebäude

3. Anwendungsorientierte Zusammenfassung gesetzlicher Vorgaben bei Datenerfassung, -übertragung und -speicherung (Fristen, Zugriffskontrolle) in Anlehnung an die BSI-Spezifikation sind:

3.1. Nicht-personenbezogene Daten für Industrie

Bei der Erfassung, Übertragung und Speicherung von nicht-personenbezogenen Daten in der Industrie gilt es zu beachten, wie die Datensicherheit und der Datenschutz gewährleistet werden kann. In Anlehnung an die BSI-Spezifikationen könnten die Anforderungen wie folgt zusammengefasst werden:

1. **Zweckbindung und Rechtmäßigkeit**:
    - Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und verarbeitet werden.
2. **Transparenz und Informationspflicht**:
    - Betroffene müssen über die Datenerfassung informiert werden, insbesondere wenn es sich um sensible Daten handelt.
3. **Datenminimierung und Speicherbegrenzung**:
    - Es dürfen nur diejenigen Daten erfasst werden, die für den vorgesehenen Zweck notwendig sind. Daten sollten nur für den erforderlichen Zeitraum gespeichert werden.
4. **Sicherheit der Verarbeitung**:
    - Technische und organisatorische Maßnahmen sind zu implementieren, um die Datensicherheit zu gewährleisten, inklusive Zugriffskontrolle und Verschlüsselung.
5. **Integrität und Vertraulichkeit**:
    - Maßnahmen zur Gewährleistung der Datenintegrität und -vertraulichkeit müssen getroffen und ggf. über sog. „Templates“ auf bestimmte Personengruppen bzw. deren Zugang zu skalierbar sensiblen Daten projiziert werden.
6. **Verfügbarkeit und Resilienz**:
    - Es müssen Maßnahmen zur Gewährleistung der Verfügbarkeit der Daten und zur Wiederherstellung im Falle eines Vorfalls ergriffen werden, optimalerweise durch ein“Durchspielen“ eines Angriffs und dessen Bekämpfung im Vorfeld
7. **Regelmäßige Überprüfung und Aktualisierung**:

- Die Sicherheitsmaßnahmen müssen regelmäßig überprüft und an neue Bedrohungen und Anforderungen angepasst werden.

8. **Dokumentation und Nachweisbarkeit**:
   - Alle Datenerfassungs-, Übertragungs- und Speicherprozesse sollten dokumentiert werden, um die Einhaltung der Vorgaben nachweisen zu können. Die DIN ISO 27001 bietet dazu einen praktikablen Rahmen
9. **Notfallplanung und Incident Response**:
   - Ein Notfallplan sollte erstellt werden, der klare Schritte zur Bewältigung von Sicherheitsvorfällen festlegt.
10. **Schulung und Sensibilisierung**:
    - Mitarbeiter sollten regelmäßig geschult und sensibilisiert werden, um sicherheitsbewusstes Verhalten zu fördern. Wie bereits zuvor erwähnt, ist der Faktor Mensch das größte „Einfallstor“ für Cyberangriffe
11. **Auftragsverarbeitung**:
    - Wenn externe Dienstleister beauftragt werden, müssen vertragliche Regelungen zur Datenverarbeitung getroffen werden.
12. **Lösch**ung von Daten**:
    - Daten müssen nach Ablauf der festgelegten Aufbewahrungsfrist sicher und endgültig gelöscht werden.

3.2. Personenbezogene Daten für Gebäude

Bei der Erfassung, Übertragung und Speicherung von personenbezogenen Daten in Gebäuden müssen bestimmte gesetzliche Vorgaben beachtet werden, um die Datensicherheit und den Datenschutz zu gewährleisten. In Anlehnung an die BSI-Spezifikationen könnten die Anforderungen wie folgt zusammengefasst werden:

1. **Zweckbindung und Rechtmäßigkeit**:
   - Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und verarbeitet werden.
2. **Transparenz und Informationspflicht**:
   - Betroffene müssen über die Datenerfassung informiert werden, insbesondere wenn es sich um sensible Daten handelt.
3. **Einwilligung der Betroffenen**:
   - In bestimmten Fällen ist die Einwilligung der betroffenen Personen für die Verarbeitung ihrer Daten erforderlich.
4. **Datenminimierung und Speicherbegrenzung**:
   - Hier gelten die zuvor aufgelisteten Inhalte
5. **Sicherheit der Verarbeitung**:
   - Technische und organisatorische Maßnahmen sind zu implementieren, um die Datensicherheit zu gewährleisten, inklusive Zugriffskontrolle und Verschlüsselung.
6. **Integrität und Vertraulichkeit**:
   - Maßnahmen zur Gewährleistung der Datenintegrität und -vertraulichkeit müssen getroffen werden. Auch hier ist der Faktor Mensch ein großes Feld der Sensibilisierung.
7. **Verfügbarkeit und Resilienz**:

- Es müssen Maßnahmen zur Gewährleistung der Verfügbarkeit der Daten und zur Wiederherstellung im Falle eines Vorfalls ergriffen werden. So sind z.B. Vertretungspläne der MA für den „Fall der Fälle“ wichtig.

8. **Regelmäßige Überprüfung und Aktualisierung**:
   - Die Sicherheitsmaßnahmen müssen regelmäßig überprüft und MA müssen an neuen Bedrohungen und Anforderungen nachgeschult werden.
9. **Dokumentation und Nachweisbarkeit**:
   - Alle Datenerfassungs-, Übertragungs- und Speicherprozesse sollten dokumentiert werden, um die Einhaltung der Vorgaben nachweisen zu können, siehe DIN ISO 27001
10. **Notfallplanung und Incident Response**:
    - Ein Notfallplan sollte erstellt werden, der klare Schritte zur Bewältigung von Sicherheitsvorfällen festlegt.
11. **Auftragsverarbeitung**:
    - Wenn externe Dienstleister beauftragt werden, müssen vertragliche Regelungen zur Datenverarbeitung getroffen werden.
12. **Rechte der Betroffenen**:
    - Betroffene haben das Recht auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten.
13. **Löschung von Daten**:
    - Personenbezogene Daten müssen nach Ablauf der festgelegten Aufbewahrungsfrist sicher und endgültig gelöscht werden.

4. Technische Möglichkeiten zur Sicherstellung der Datensicherheit Prozessseitig (Organisation, Qualitätsmanagement, Zugriff etc.)

Es gibt eine Vielzahl von technischen Möglichkeiten, um die Datensicherheit prozessseitig zu gewährleisten. Diese hauptsächlichen Maßnahmen beziehen sich auf die Organisation, das Qualitätsmanagement und die Zugriffskontrolle. Hier sind einige technische Ansätze:

1. **Zugriffskontrollen und Berechtigungen**:
   - Es gelten die bereits vorab benannten Maßnahmen
2. **Verschlüsselung**:
   - Es gelten die bereits vorab benannten Maßnahmen
3. **Multi-Faktor-Authentifizierung (MFA)**:
   - MFA erfordert mehr als nur ein Passwort zur Authentifizierung. Es kann beispielsweise ein zusätzlicher Code über ein mobiles Gerät erforderlich sein.
4. **Intrusion Detection/Prevention Systeme (IDS/IPS)**:
   - Diese Systeme überwachen den Netzwerkverkehr auf verdächtige Aktivitäten und können potenzielle Angriffe erkennen und blockieren.
5. **Firewalls**:
   - Es gelten die bereits vorab benannten Maßnahmen
6. **Sicherheitsinformationen und Ereignismanagement (SIEM)**:

    - SIEM-Lösungen sammeln, analysieren und reagieren auf Sicherheitsereignisse in Echtzeit.
7. **Datensicherung und Wiederherstellung**:
    - Es gelten die bereits vorab benannten Maßnahmen
8. **Datenklassifikation und -kategorisierung**:
    - Durch die Klassifikation und Kategorisierung von Daten kann festgelegt werden, wie sie behandelt und gespeichert werden müssen.
9. **Vulnerability Scanning und Penetrationstests**:
    - Regelmäßige Überprüfungen (intern) der Systeme auf Schwachstellen und Sicherheitslücken helfen dabei, potenzielle Risiken zu identifizieren. Gezielte Angriffe durch externe Sicherheitsfirmen oder –institute sind gute Praxistests und erbringen manche unschöne Überraschung für diejenigen, die sich trauen.
10. **Identity and Access Management (IAM)**:
    - IAM-Systeme verwalten die Identitäten und Zugriffsrechte von Benutzern in einem Unternehmen.
11. **Patch-Management**:
    - Es gelten die bereits vorab benannten Maßnahmen
12. **Sicherheitsrichtlinien und -verfahren**:
    - Es gelten die bereits vorab benannten Maßnahmen
13. **Sicherheitsbewusstsein und Schulung**:
    - Es gelten die bereits vorab benannten Maßnahmen

Die effektivste Sicherheitsstrategie ist oft eine Kombination aus mehreren dieser Maßnahmen.

Hardware

Am Markt existiert ein breites Angebot an Hardware-Lösungen, die zur Sicherstellung der Datensicherheit prozessseitig beitragen können. Diese können in verschiedenen Bereichen der Organisation, im Qualitätsmanagement und der Zugriffskontrolle eingesetzt werden:

1. **Hardware Security Module (HSM)**:
    - Ein HSM ist ein spezielles Gerät, das kryptografische Operationen und Schlüsselmanagement für Verschlüsselung und Authentifizierung durchführt. Es bietet eine sichere Umgebung für die Verwaltung von kryptografischen Schlüsseln.
2. **Firewalls und Netzwerkgeräte**:
    - Es gelten die bereits vorab benannten Maßnahmen
3. **Intrusion Prevention Systems (IPS)**:
    - Es gelten die bereits vorab benannten Maßnahmen
4. **Sicherheitskameras und Zutrittskontrollsysteme**:
    - Diese Hardware-Lösungen ermöglichen die Überwachung von physischen Standorten und können den Zugriff auf sensible Bereiche kontrollieren.
5. **Biometrische Zugriffssysteme**:

- Biometrische Systeme nutzen individuelle biologische Merkmale wie Fingerabdrücke, Gesichtserkennung oder Iris-Scan für die Zugangskontrolle.

6. **Spezielle Verschlüsselungs-Hardware**:
   - Einige Hardware-Geräte sind darauf spezialisiert, Verschlüsselungsfunktionen durchzuführen und sensible Daten zu schützen.
7. **Hardware zur physischen Datensicherung**:
   - Dies können beispielsweise spezielle Festplatten oder USB-Sticks mit integrierter Verschlüsselung und Sicherheitsfunktionen sein.
8. **Sicherheitsmodule für IoT-Geräte**:
   - Spezielle Hardware-Module bieten zusätzliche Sicherheitsfunktionen für Internet of Things (IoT)-Geräte, um deren Schutz vor Angriffen zu gewährleisten.
9. **Kartenleser und Smartcards**:
   - Smartcards und Kartenleser können für starke Authentifizierungsmethoden verwendet werden.
10. **Racks und Server-Gehäuse mit Sicherheitsfunktionen**:
    - Speziell konzipierte Racks und Gehäuse bieten zusätzlichen Schutz für Server und Netzwerkhardware vor physischen Angriffen.
11. **Secure Tokens**:
    - Secure Tokens sind physische Geräte, die für die Authentifizierung verwendet werden und Codes generieren, die nur für kurze Zeit gültig sind.
12. **Hardware zur physischen Sicherheit von Datenzentren**:
    - Dies kann Überwachungssysteme, Zutrittskontrollen und spezielle Sicherheitsinfrastruktur für Rechenzentren umfassen.

Nicht alle, doch zahlreiche praxisnahe Angriffe unter Verwendung der o.g. Komponenten sind in unzähligen „Thrillern“ in Kino und TV abgehandelt worden und haben für ein gewisses Maß an „Wiedererkennung“ für solche Systeme gesorgt.

Software

Ebenso groß ist der Markt für Software-Lösungen, die zur Sicherstellung der Datensicherheit prozessseitig eingesetzt werden können. Diese Software-Tools decken verschiedene Aspekte der Organisation, des Qualitätsmanagements und der Zugriffskontrolle ab. Hier sind einige Beispiele:

1. **Endpoint Protection Software**:
   - Diese Software schützt Endgeräte wie PCs, Laptops und mobile Geräte vor Malware und anderen Bedrohungen.
2. **Firewall-Software**:
   - Es gelten die bereits vorab benannten Maßnahmen
3. **Antivirus- und Anti-Malware-Programme**:
   - Es gelten die bereits vorab benannten Maßnahmen
4. **Data Loss Prevention (DLP) Software**:

- DLP-Tools helfen dabei, zu verhindern, dass sensitive Daten das Unternehmen verlassen, indem sie den Datenverkehr überwachen und Richtlinien zur Verhinderung von Datenlecks umsetzen.

5. **Verschlüsselungssoftware**:
   - Es gelten die bereits vorab benannten Maßnahmen
6. **Zugriffssteuerungssoftware**:
   - Diese Software ermöglicht die Verwaltung von Benutzerzugriffen auf Systeme und Daten, einschließlich der Zuweisung von Berechtigungen und Rollen.
7. **Identity and Access Management (IAM) Tools**:
   - Es gelten die bereits vorab benannten Maßnahmen
8. **Intrusion Detection/Prevention Systems (IDS/IPS)**:
   - Es gelten die bereits vorab benannten Maßnahmen
9. **Sicherheitsinformationen und Ereignismanagement (SIEM)**:
   - SIEM-Plattformen sammeln, analysieren und reagieren auf Sicherheitsereignisse in Echtzeit.
10. **Notfall- und Incident Response-Tools**:
    - Es gelten die bereits vorab benannten Maßnahmen
11. **Vulnerability Management Software**:
    - Diese Tools helfen dabei, Schwachstellen in Systemen und Anwendungen zu identifizieren und priorisieren, um proaktiv Sicherheitslücken zu schließen.
12. **Patch-Management-Software**:
    - Diese Software verwaltet und überwacht die Aktualisierung von Software und Betriebssystemen, um bekannte Sicherheitslücken zu schließen.
13. **Compliance-Management-Software**:
    - Diese Tools unterstützen Unternehmen dabei, die Einhaltung gesetzlicher und regulatorischer Anforderungen zu überwachen und nachzuweisen.

5. Zusammenfassende Darstellung/Erläuterung von KRITIS: Wesentliche Aspekte, bspw. Meldepflichten, Maßnahmen, Audits

KRITIS steht für Kritische Infrastrukturen und umfasst lebenswichtige Einrichtungen und Systeme, deren Ausfall oder Beeinträchtigung erhebliche Auswirkungen auf das öffentliche Leben, die Gesundheit, die Sicherheit oder die wirtschaftliche Versorgung der Bevölkerung haben könnte. In vielen Ländern gibt es spezielle Regelungen und Vorschriften für den Schutz von KRITIS. Hier sind wesentliche Aspekte im Zusammenhang mit KRITIS:

1. **Bereiche der Kritischen Infrastrukturen**:
   - Zu den Sektoren, die als Kritische Infrastrukturen gelten können, gehören unter anderem Energieversorgung, Wasserversorgung, Gesundheitswesen, Informationstechnik und Telekommunikation, Transport und Verkehr, Ernährung, Finanz- und Versicherungswesen.
2. **Meldepflichten**:

- Betreiber von Kritischen Infrastrukturen müssen gesetzliche Rahmen berücksichtigen, um Sicherheitsvorfälle oder ernsthafte Bedrohungen zu melden. Dies dient dazu, schnelle Reaktionen und koordinierte Maßnahmen zu ermöglichen. Kommunikationspartner dieser Betriebe ist in Sachen Datensicherheit vorrangig das BSI, im Fall einer Attacke das BKA und nachgeschaltete Behörden.

3. **Maßnahmen zur Sicherung von KRITIS**:
   - Betreiber von Kritischen Infrastrukturen müssen detaillierte Maßnahmen zur Gewährleistung der Sicherheit und Verfügbarkeit ihrer Dienste und Systeme ergreifen, die höher sind als bei Firmen ohne KRITIS-Einordnung. Dazu gehören unter anderem DIN-Zertifikate wie etwa DIN ISO 27001, Zugangsbeschränkungen, Schutz vor Cyberangriffen, physische Sicherheitsvorkehrungen, Vorhalt eines bewaffneten Sicherheitsdienmstes und Notfallplanung zusammen mit der Polizei.
4. **Kritische Komponenten und Systeme**:
   - Innerhalb einer Kritischen Infrastruktur müssen definierte Komponenten oder Systeme identifiziert werden, deren Ausfall besonders schwerwiegende Folgen haben könnte. Diese müssen oft besonders geschützt werden.
5. **Cybersecurity-Maßnahmen**:
   - Angesichts der wachsenden Bedrohung durch Cyberangriffe sind Betreiber von Kritischen Infrastrukturen oft verpflichtet, spezifische Cybersecurity-Maßnahmen zu ergreifen. Dazu gehören regelmäßige Sicherheitsprüfungen, Verschlüsselung, Intrusion Detection und Prevention Systeme (IDS/IPS) und regelmäßige Schulungen der Mitarbeiter.
6. **Notfall- und Krisenmanagement**:
   - Betreiber von Kritischen Infrastrukturen müssen Notfallpläne entwickeln und implementieren, um im Falle eines schwerwiegenden Vorfalls schnell reagieren und die Auswirkungen minimieren zu können.
7. **Zusammenarbeit und Informationsaustausch**:
   - Betreiber von Kritischen Infrastrukturen sind verpflichtend aufgefordert, mit staatlichen Stellen, anderen Betreibern und relevanten Organisationen zusammenzuarbeiten, um ein koordiniertes Vorgehen im Falle von Bedrohungen oder Vorfällen zu ermöglichen.
8. **Compliance und Zertifizierung**:
   - Betreiber von Kritischen Infrastrukturen müssen definierte Compliance-Standards einhalten und können auch Zertifizierungen erwerben, um die Einhaltung der Vorschriften nachzuweisen.

Systeme zur Angriffserkennung

- Seit 01.05.2023 Pflicht zum Nachweis
- Pflicht für KRITIS nach BSIG §8a
  - Grenzwerte in KRITISV
- Pflicht auch für Unternehmen nach EnWG
- Ausblick: Neugestaltung der Größen und Klassen durch NIS2.0 und NIS2UmsuCG (NIS2 Umsetzungs- und Cybersicherheitsstärkungs-gesetz)

Abbildung 8 Systeme zur Angriffserkennung, Auszug aus gesetzlichen Vorgaben, Quelle: green with IT

Systeme zur Angriffserkennung

- Technische und Organisatorische Maßnahmen
- Verantwortliche Personen benennen (+ Ressourcen)
- Prozesse definieren (und leben ;-))
- Technische Lösungen als Teil des Prozesses
- Human-in-the-Loop
- Automatische Reaktion in weniger kritischen Bereichen

Abbildung 9 Innerbetriebliche Monitoring-Empfehlungen, Quelle: green with IT

Nachweispflichten

KRITIS steht für Kritische Infrastrukturen; Nachweispflichten beziehen sich auf die Anforderungen und Verpflichtungen, die Betreiber von Kritischen Infrastrukturen haben, um die Sicherheit und Verfügbarkeit ihrer Dienste und Systeme zu gewährleisten. Hier sind die wesentlichen Nachweispflichten im Zusammenhang mit KRITIS:

1. **Dokumentation und Aufzeichnungen**:
    - Betreiber von Kritischen Infrastrukturen müssen umfassende Aufzeichnungen und Dokumentationen führen, die ihre Sicherheitsmaßnahmen, Notfallpläne und Maßnahmen zur Gefahrenabwehr festhalten und auch staatlichen Stellen gegenüber dokumentieren. Dies ermöglicht die nachträgliche Überprüfung und den Nachweis der getroffenen Maßnahmen.
2. **Sicherheitskonzepte und -pläne**:
    - Es gelten die bereits vorab benannten Maßnahmen
3. **Notfallpläne und -übungen**:
    - Es gelten die bereits vorab benannten Maßnahmen
4. **Compliance-Nachweise**:
    - Es gelten die bereits vorab benannten Maßnahmen
5. **Sicherheitsaudits und Überprüfungen**:
    - Es gelten die bereits vorab benannten Maßnahmen
6. **Berichtspflichten an Behörden**:
    - In allen Bundesländern sind Betreiber von Kritischen Infrastrukturen verpflichtet, Sicherheitsvorfälle oder Bedrohungen den zuständigen Behörden zu melden.
7. **Protokollierung von Sicherheitsvorfällen**:
    - Betreiber müssen Sicherheitsvorfälle protokollieren, dokumentieren und ab einer definierten Sicherheitsstufe melden, um die Umstände, Maßnahmen und Auswirkungen nachvollziehbar zu machen.
8. **Bereitstellung von Nachweisen bei Bedarf**:
    - Betreiber müssen in der Lage sein, auf Anfrage Nachweise über die Umsetzung von Sicherheitsmaßnahmen, Notfallpläne und andere relevante Dokumente bereitzustellen.
9. **Regelmäßige Berichterstattung an Aufsichtsbehörden**:
    - Je nach den geltenden Vorschriften müssen Betreiber möglicherweise regelmäßig Berichte über ihre Sicherheitsmaßnahmen und Compliance an die zuständigen Aufsichtsbehörden senden.
10. **Durchführung von Sicherheitsprüfungen durch Dritte**:
    - In einigen Fällen können externe Prüfer oder Auditoren beauftragt werden, die Umsetzung von Sicherheitsmaßnahmen zu überprüfen und einen unabhängigen Nachweis zu erbringen.

6. Cybersicherheitsstärkungsgesetz

Das Cybersicherheitsstärkungsgesetz ist eine Initiative, die darauf abzielt, die Cybersecurity in Deutschland zu stärken. In Deutschland liegt das IT-Sicherheitsgesetz 2.0 vor, welches als Weiterentwicklung des ursprünglichen IT-Sicherheitsgesetzes betrachtet wurde. Am 18. April 2023 schlug die EU- Kommission eine gezielte Änderung des EU-Cybersicherheitsgesetzes vor. Die vorgeschlagene Änderung wird die künftige Einführung europäischer Zertifizierungssysteme für „verwaltete Sicherheitsdienste“ ermöglichen, die Bereiche wie Reaktion auf Vorfälle, Penetrationstests, Sicherheitsaudits und Beratung abdecken. Die Zertifizierung ist von entscheidender Bedeutung, um eine hohe Qualität und Zuverlässigkeit dieser hochkritischen und sensiblen Cybersicherheitsdienste zu gewährleisten, die Unternehmen und Organisationen dabei unterstützen, Vorfälle zu verhindern, zu

erkennen, darauf zu reagieren oder sich von diesen zu erholen. Hier sind einige der wichtigsten Eckpunkte des IT-Sicherheitsgesetzes 2.0, die möglicherweise relevant sind:

1. **Erweiterung des Anwendungsbereichs**:
   - Das Gesetz erweitert den Anwendungsbereich auf weitere kritische Infrastrukturen, um mehr Sektoren einzubeziehen, die von nationaler Bedeutung sind.
2. **Meldepflicht für Cybersicherheitsvorfälle**:
   - Betreiber kritischer Infrastrukturen müssen bestimmte IT-Sicherheitsvorfälle unverzüglich melden, um eine koordinierte Reaktion zu ermöglichen.
3. **Mindestanforderungen an die IT-Sicherheit**:
   - Betreiber kritischer Infrastrukturen müssen Mindeststandards für die IT-Sicherheit umsetzen, um die Schutzfähigkeit ihrer Systeme zu verbessern.
4. **Cybersicherheitsmaßnahmen und -pläne**:
   - Betreiber müssen angemessene Cybersicherheitsmaßnahmen umsetzen und über geeignete Notfallpläne verfügen, um auf Sicherheitsvorfälle reagieren zu können.
5. **Regelmäßige Sicherheitsüberprüfungen**:
   - Betreiber müssen regelmäßige Sicherheitsüberprüfungen durchführen, um sicherzustellen, dass die implementierten Maßnahmen effektiv sind.
6. **Prüfung und Zertifizierung**:
   - In einigen Fällen kann eine externe Prüfung und Zertifizierung der Sicherheitsmaßnahmen erforderlich sein.
7. **Stärkung der Zusammenarbeit**:
   - Das Gesetz fördert die Zusammenarbeit zwischen Betreibern kritischer Infrastrukturen, Behörden und anderen relevanten Stellen.
8. **Bereitstellung von Informationen und Unterstützung**:
   - Es wird vorgesehen, dass Behörden Informationen und Unterstützung für Betreiber von kritischen Infrastrukturen bereitstellen, um die Umsetzung von Sicherheitsmaßnahmen zu erleichtern.

Glossar

Definition „Cybercrime im engeren Sinne“

Straftaten, die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten

Definition „Cybercrime im weiteren Sinne“

Straftaten, die unter Nutzung von Informationstechnik begangen werden (Tatmittel Internet)

Definition „Underground Economy“

Die Gesamtheit aller täterseitig illegal genutzten Plattformen. Sie stellen eine kommerziell ausgerichtete, dynamische Landschaft dar, welche Kommunikations- und Verkaufsplattformen im Internet vereint.

Aufgrund der starken wirtschaftlichen und illegalen Ausrichtung der Plattformen werden sie unter dem Begriff „Underground Economy“ zusammengefasst.

***Clearnet** (Visible Web, Surface Web, Open Web)*

Für jedermann mit marktgängigen Browserprogrammen zugänglich, unterstützt durch einfache Handhabung mittels Suchmaschinen.

Auch im Clearnet sind vielfältige illegale Inhalte verfügbar, z. B. solche mit Bezug zu Politisch Motivierter Kriminalität oder Plattformen und Foren der sog. „Underground Economy“ (Straftaten überwiegend aus dem Bereich der Cybercrime im engeren Sinne).

***Deep Web** (Invisible Web)*

Der Teil des Internets, dessen Inhalte nicht durch Suchmaschinen auffindbar sind, weil z. B. Webseiten nicht indexiert/in Suchmaschinen verlinkt wurden oder weil sie zugriffsbeschränkt sind. Inhalte des Deep Webs können z. B. Datenbanken, Intranets oder Fachwebseiten sein und sind – sofern die URL bekannt ist und eine Zugangsberechtigung besteht – mit Browsern erreichbar.

Darknet

Darknet-Inhalte sind ausschließlich durch Nutzung spezieller Software, die der Anonymisierung dient, einsehbar.

Bestandteile des Darknets sind z. B. Foren, Blogs/Wikis mit unterschiedlichsten – legalen wie illegalen – Zielrichtungen. Einen bedeutenden Teil machen sog. Darknet-Marktplätze aus, bei denen größtenteils inkriminierte Güter gehandelt werden. Auch werden zahlreiche und bedarfsorientierte Angebote für Cybercrime-as-a-Service (Durchführung bzw. Unterstützungsleistungen krimineller Handlungen im Auftrag) oder Darknet-Seiten mit kinderpornografischen Inhalten zur Verfügung gestellt.

Was ist Malware?

Unter dem Begriff Malware versteht man alle Programme, welche schädliche Funktionen auf einem IT-System ausführen. Zu diesen maliziösen Funktionen gehören u. a.

- *Ausspähen und Weiterleiten von Account-Daten wie Usernamen und Passwörtern,*
- *Manipulation bzw. Zerstörung von Daten,*
- *illegitime Nutzung von Rechenleistung zum Kryptomining,*
- *Verschlüsseln von Daten,*
- *Einbindung in ein Bot-Netz und zum Missbrauch für DDoS-Angriffe,*
- *missbräuchliche Fernsteuerung eines fremden IT-Systems.*

Was ist „Ransomware“?

Ransomware – eine Schadsoftware, die mittels Verschlüsselung von Nutzerdaten oder Datenbanken den Zugriff auf lokale oder übers Netzwerk aufrufbare Daten und Systeme verhindert.

Wird man Opfer eines solchen Angriffs erfolgt i. d. R. eine Lösegeldforderung (Ransom) – in digitaler Währung – seitens der Täter, die erst nach Eingang der geforderten Lösegeldsumme die Verschlüsselung aufheben. Um den Druck auf die Opfer zu erhöhen, werden zudem kurze Fristen gesetzt. Zudem wird mit der Löschung oder Veröffentlichung von Daten gedroht, wenn der Aufforderung nicht rechtzeitig nachgekommen wird.

Definition „Ransomware-as-a-Service“

Ransomware, die in Form einer „Dienstleistung“ betrieben wird, stellt eine besondere Form der Ransomware dar – die sogenannte „Ransomware-as-a-Sercive“.

Distributed Denial of Service (DDoS)-Angriffe

Durch gezielt herbeigeführte Überlastung wird versucht, die Verfügbarkeit eines Internetdienstes oder eines Zielsystems zu stören.

Der DDoS-Angriff zeichnet sich dadurch aus, dass der Angriff i. d. R. von einer Vielzahl einzelner Anfragen bzw. einer großen Zahl an Rechnern – vielfach mittels großer, ferngesteuerter Botnetze – erfolgt.

Botnetze

Botnetze entstehen durch die zumeist unbemerkte Installation einer Schadsoftware auf PCs von Geschädigten. Die infizierten Geräte werden dann ohne Wissen ihrer Besitzer mittels sog. „Command & Control-Server" kontrolliert, gesteuert und zu einem Botnetz zusammengeschaltet, sodass Massenabfragen erfolgen können.

Advanced Persistant Threats (APT)

Bei einem APT handelt es sich um einen zielgerichteten Cyber-Angriff auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind i. d. R. schwierig zu detektieren.

APT sind dabei nicht ausschließlich staatliche Akteure: Die ENISA (European Union Agency for Cybersecurity) stellte fest[25], dass nur 16 % der dort identifizierten Akteure staatlich motiviert sind – 60 % lassen sich der organisierten Kriminalität zuordnen.[26]

Abbildung 10 Begriffsdefinitionen Cybercrime, Quelle: BKA