Exzerpt

Datum: 18.10.2021
Dokument: Studienbrief „Basiswissen Wirtschaftsinformatik“ Seite 231-254
Kapitel: Datensicherheit und Datenschutz
Weite Quellen im Anhang
Anmerkung: IuK = Informations- und Kommunikations- Systeme

Thema: Was ist die Aufgabe des IT-Sicherheitsmanagement
Aussage:
Datensicherheit zu gewährleisten. Datensicherheit besteht wenn ein umfassender Schutz vor Verlust, Verfälschung und unberechtigter Verwendung von Daten besteht. Dazu muss der Schutz durch eine systematische Gestaltung des kompletten IuK erbracht werden und immerwährend in einem definierten Prozess weiter entwickel werden.
Die IuK-Sicherheit (also die ganzheitliche Betrachtung) kennt 3 Teile:

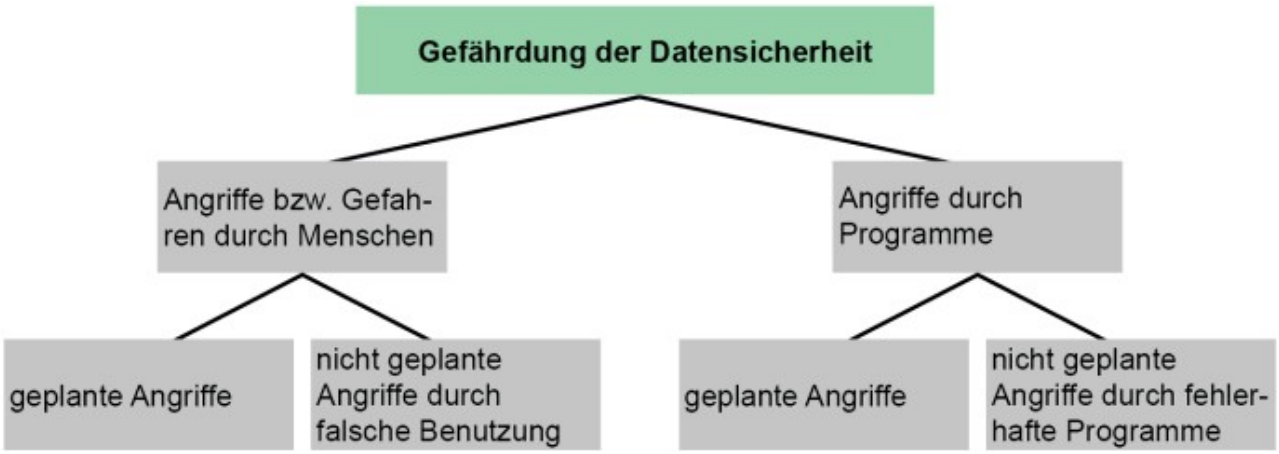
- IT-Sicherheit: Schutz der Hard- und Software (PC, Server, Netzwerk, Betriebssysteme)
- Informationssicherheit: Schutz der Anwendungen Prozesse und Daten (auch Internet, Mail und Telefon)
- Personen und Benutzersicherheit: Schutz vor unberechtigter Benutzung und Schutz vor Phisching.

Anmerkung:
Man spricht zwar von umfassender Datensicherheit, meint aber immer den aktuell möglichen Schutz, da keiner weis was zukünftig nötig sein werden wird. (Der Hacker ist immer einen Schritt voraus)

Thema Datensicherheit – Gefahren und IT-Risikomanagement
Aussage:
Da ein Businessgerechter Umgang mit Daten aus Kosten oder technischen Gründen selten perfekt sein kann, müssen Kosten, Möglichkeiten und Risiken gegeneinander abgewogen werden. Es gilt also Lösungen zu finden unter der Betrachtung der Businessanforderungen und den Complianceanforderungen
Es gibt sehr viele Möglichkeiten die Datensicherheit zu verletzen (geplante und ungeplante) wie zB

- Sabotage
- Viren, Würmer, Trojaner (allgemein: Schadsoftware)
- Technischer Ausfall von Systemen (Defekt oder äußere Einflüsse wie zB ein Unwetter)
- falsche Bedienung
- Bugs

Das IT-Risikomanagement teilt sich auf in:



Anmerkung: Compliance beschreibt das vorschriftsgemäße verhalten von Mitarbeitern sowie den korrekten Gebrauch der IuK. Dazu braucht es Regeln, Schulungen und Kontrolle

Thema: IT-Sicherheitsziele

Aussage:

Die Definition der von einer Organisation zu erreichenden Sicherheitsziele unter Betrachtung geltender Regeln, Vorschriften und Gesetzte. Im Besonderen sind dabei personenbezogene Daten zu beachten.

Hierbei werden zwei grundsätzlich unterschiedliche Strategien bzw. Motivationen bevorzugt:

- Orientierung am Business (Minimalprinzip). Alle für die Sicherstellung der Vermögenssteigerung und -erhaltung nötigen Maßnahmen werden unter Berücksichtigung der Kosten und minimaler Störung des Betriebs, getroffen. Hier wird aktiv reagiert.
- Orientierung an der Sicherheit (Maximalprinzip). Alle aus Sicht der Datensicherheit sinnvollen Ziele werden umgesetzt. Ohne Einfluss auf Kosten, Komplikationen im Betrieb oder Berücksichtigug der aktuellen und vergangenen Bedrohungslage. Hier wird proaktiv gehandelt.

Die Sicherheitsziele sind:

- Verfügbarkeit. Unter der Sicherheitsbetrachtung spaltet sich die Verfügbarkeit in drei Gruppen auf:
  - Verfügbarkeit der Infrastruktur. Dazu zählen der Storage, die Server, die Netzwerkkomponenten und die zum Betrieb nötige Peripherie.
  - Verfügbarkeit der Dienste. Hier muss gewährleistet werden das die eingesetzten Programme einwandfrei und ohne Ausfall arbeiten
  - Datenverfügbarkeit. Es muss sicher gestellt sein das die Daten bis zu einem vorgegebenen Leistungsniveau unter allen Umständen – von normal bis katastrophal – verfügbar bleiben
- Integrität. Der Begriff Datenintegrität bezieht sich auf die Korrektheit, Vollständigkeit und Konsistenz von Daten. Auch die Sicherheit von Daten mit Blick auf regulatorische Anforderungen (CCPA, DSVGO, GDPR, HIPAA) und der Schutz der Daten vor unzulässigem Zugriff fallen unter diesen Begriff.
- Vertraulichkeit. Grundsätzlich wird hier gefordert das die unberechtigte Einsichtnahme in Daten und die Weitergabe von Informationen ausgeschlossen wird.
  - Personell: Für Mitarbeiter müssen im Umgang mit Daten Regeln und Maßnahmen verpflichtend sein.
  - Technisch: Dienste und Übertragungsstrecken müssen gegen Missbrauch geschützt sein.
- Verbindlichkeit. Hierbei muss sicher gestellt werden das die Identität authentifizieren ist.
  - Personell: Personen müssen nachweislich eindeutig identifizierbar sein.
  - Technisch: Anwendungen und Daten müssen nachweislich eindeutig identifizierbar sein.

- Informell: Die Quelle einer Information muss nachweislich eindeutig identifizierbar sein.

Thema: Datenschutz (personenbezogener Daten)
Aussage:
Das Ziel ist der Schutz schutzwürdiger Belange aller Bürger bei der Verarbeitung personenbezogener Daten.

Was sind personenbezogene Daten: Gesetzlich definiert wird der Begriff personenbezogene Daten in Artikel 4 der DSGVO als “alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen”.
Konkreter wird die Definition in §46 Abs. 1 des Bundesdatenschutzgesetzes: “Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)”

Quelle: https://www.piolo.de/datenschutz?msclkid=da8b9e94c60d1687798bffe6b1c4a3f5#Personenbezogene_Daten
https://datenschutzexperte.de/personenbezogene-daten/

Datenschutzgesetze
Beim Datenschutz gelten die Datenschutzgesetze
In Deutschland gilt die im Grundgesetz verankerte „informelle Selbstbestimmung“ die jedem Bürger das Recht einräumt über die Preisgabe personenbezogener Daten selbst zu bestimmen, solange andere Gesetzte dieses Recht nicht beschränken.

- Europäische Union: Datenschutz-Grundverordnung (DSGVO seit 25.05.2018)
- Deutschland: Bundesdatenschutzgesetz (BDSG und BDSG-neu seit 05.07.2017)
- Vereinigtes Königreich: Data Protection Act 2018 (DPA 2018) (Im August 2021 ist eine Reform beschlossen worden, die sich am DSVGO orientieren wird)
- Kalifornien: California Consumer Privacy Act (CCPA)
- Brasilien: Lei Geral de Proteção de Dados (LGPD)
- Singapur: Singapore Personal Data Protection Act (PDPA)
- Indien: Personal Data Protection Bill (PDPB)
- China: Personal Information Protection Law (PIPL)
- Schweiz: revidiertes Datenschutzgesetz (revDSG)

Anmerkung: Die DSVGO gilt Europaweit, die BDSG konkretisiert Teile des Datenschutzes, im Besonderen im Arbeitsrecht, siehe: https://keyed.de/blog/datenschutz-im-arbeitsvertrag/

Prinzipien des Datenschutz
Artikel 5 DSGVO beschreibt die 7 Grundprinzipien der Datenverarbeitung:

1. Rechtmäßigkeit: Verarbeitung nach Treu und Glauben, Transparenz. Die Verarbeitung der Daten erfordert eine Rechtsgrundlage. Die betroffene Person muss darüber informiert werden, was mit den Daten passiert.
2. Zweckbindung: Der Zweck der Datenverarbeitung müssen bereits bei der Erhebung personenbezogener Daten festgelegt, eindeutig und legitim sein.
3. Datenminimierung: Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden. D.h. z.B. dass die Anmeldung zu einem Newsletter sich auf Emailadresse und ggf. Geschlecht und Nachnamen als Pflichtfelder beschränken muss.
4. Richtigkeit: Daten müssen korrekt und auf dem neuesten Stand sein. Fehlerhafte Daten sind unverzüglich zu korrigieren oder zu löschen.

5. Speicherbegrenzung: Daten müssen gelöscht werden, wenn sie für den Zweck der Verarbeitung nicht mehr benötigt werden.
6. Integrität und Vertraulichkeit: Schutz gegen unbefugte oder unberechtigte Verarbeitung, insbesondere die Weitergabe an unberechtigte Dritte.
7. Rechenschaftspflicht: Unternehmen sind gegenüber den Aufsichtsbehörden in der Nachweispflicht. Verstöße gegen die Grundprinzipien fallen in die höchste Strafkategorie von bis zu € 20 Millionen oder 4 % des Konzernumsatzes.

Quellen:
Informelle Selbstbestimmung von Unternehmen: https://www.wbs-law.de/medienrecht/persoenlichkeitsrecht/unternehmenspersoenlichkeitsrecht/
Internationale Datenschutzgesetzte: https://www.boxcryptor.com/de/blog/post/data-protection-laws-worldwide/
Prinzipien des Datenschutz: https://fokus.genba.org/grundsaetze-der-dsgvo

Anmerkung: Der Begriff Datenschutz hat mehrere Bedeutungen:
- Schutz vor missbräuchlicher Datenverarbeitung
- Recht auf informelle Selbstbestimmung
- Schutz der Privatsphäre
- Schutz des Persönlichkeitsrechts bei der Datenverarbeitung

Obwohl der Schutz personenbezogener Daten länger besteht als es Computer gibt, ist der Begriff Datenschutz erst in der zweiten Hälfte des 20. Jahrhunderts aufgekommen.

Beispiel einer guten Information: https://www.piolo.de/datenschutz?msclkid=da8b9e94c60d1687798bffe6b1c4a3f5#Personenbezogene_Daten

Thema: Ausgewählte Maßnahmen zur Datensicherheit
Aussage: Ein umfängliches Datensicherheitskonzept beginnt mit der Einweisung und Schulung der Mitarbeiter, beschreibt Autorisierungs- und Authentifizierungsverfahren, definiert den technisch sicheren Umgang mit Daten und sorgt für sichere Übertragungskanäle.

Verschlüsselung (Kryptografie)
Kryptografie (altgriechisch: krypto für "verborgen, geheim" und grafie für "schreiben, Schrift") ist ein Teilgebiet der Kryptologie und befasst sich mit dem Verschlüsseln von Informationen.

Exkurs: Informationen zu verschlüsseln ist eine etwa 3000 Jahre alte Technik. Die ersten „geheimen“ Texte sind aus der Zeit 1500 vor Christus bekannt. Julius Cäsar setzte 60 vor Christus als symmetrische Verschlüsselung eine einfache Buchstabenverschiebung ein, und die Enigma aus dem 2. Weltkrieg, eine der letzten großen mechanischen Chiffriergeräte, verwendete eine asymmetrische Verschlüsselungstechnik. Schon mit der Erfindung der ersten Computer (zB Zuse 2) wurde die „moderne Kryptographie“ ins Leben gerufen. Sie verwendet mathematische Algorythmen die zu ihrer Zeit im Ruf standen nicht rückwärts rechenbar zu sein. Das heute noch gängige PKI-Modell (Public Key Infrastruktur) verwendet zum Verschlüsseln einen öffentlichen Schlüssel und zum entschlüsseln einen privaten Schlüssel. Somit kann jeder verschlüsseln, aber nur die Besitzer des privaten Schlüssel können entschlüsseln.

Symmetrische Verfahren:
Eine symmetrische Verschlüsselung verwendet den gleichen Vorgang. Dies kann zum Beispiel eine einfache Buchstabenverschiebung des Alphabets sein (siehe die Cäsarische Verschlüsselung). Jedem der Kenntnis dieses Schlüssels hat, ist es möglich die Nachricht zu entschlüsseln. Werden

komplexere Funktionen verwendet, fällt es dem zufälligen Betrachter der verschlüsselten Nachricht deutlich schwerer den Code zu knacken.
Daher muss der Krypto-Key komplex und geheim sein. Der Vorteil dieses Verfahrens ist das es sehr schnell arbeitet und daher für große Datenmengen geeignet ist.
Beispiel: Verschlüsselung von Datenträgern
Bei der Verschlüsselung eines Datenträgers wird eine bekannte mathematische Funktion (Algorithmus) mit mehreren Variablen verwendet. Alle Variablen, bis auf eine, werden beim Initialvorgang automatisch und zufällig gefüllt. Die verbleibende Variable wird von Anwender manuell eingegeben – das ist das Passwort. Zum Entschlüsseln wird die bekannte Funktion mit allen eingesetzten Variablen verwendet. Die letzte Unbekannte wird wieder von Anwender eingegeben und die Daten können entschlüsselt werden.

Asymmetrische Verschlüsselungsverfahren
Asymmetrische Verschlüsselungsverfahren verwenden zum chiffrieren und dechiffrieren unterschiedliche Vorgänge. Ein gängiges Verfahren ist PKI

Wesentliche Bestandteile einer PKI sind:
Digitale Zertifikate: Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen.
Zertifizierungsstelle (Certificate Authority, CA): Organisation, welche das CA-Zertifikat bereitstellt und die Signatur von Zertifikatsanträgen übernimmt.
Registrierungsstelle (Registration Authority, RA): Organisation, bei der Personen Zertifikate beantragen können. Diese prüft die Richtigkeit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag der dann durch die Zertifizierungsstelle signiert wird.
Zertifikatsperrliste (Certificate Revocation List): Eine Liste mit Zertifikaten die vor Ablauf der Gültigkeit zurückgezogenen wurden z.B. weil das Schlüsselmaterial kompromittiert wurde. Prinzipell muss eine PKI immer eine Zertifikatsstatusprüfung anbieten. Hierbei können jedoch neben der CRL (Offline-Statusprüfung) auch s.g. Online-Statusprüfungen wie OCSP zum Einsatz kommen.
Verzeichnisdienst: ein durchsuchbares Verzeichnis, welches ausgestellte Zertifikate enthält, meist ein LDAP-Server, seltener ein X.500-Server.
Dokumente: Eine PKI führt eines oder mehrere Dokumente, in denen die Arbeitsprinzipien der PKI beschrieben sind. Kernpunkte sind der Registrierungsprozess, Handhabung des Secret-Key-Materials, zentrale oder dezentrale Schlüsselerzeugung, technischer Schutz der PKI-Systeme sowie evtl. rechtliche Zusicherungen. In X.509-Zertifikaten kann das CPS in den Extensions eines Zertifikates verlinkt werden. Nachfolgende Dokumente sind teilweise üblich.

- **CP** (Certificate Policy): In diesem Dokument beschreibt die PKI ihr Anforderungsprofil an ihre eigene Arbeitsweise. Es dient Dritten zur Analyse der Vertrauenswürdigkeit.
- **CPS** (Certificate Practice Statement): Hier wird die konkrete Umsetzung der Anforderungen in die PKI beschrieben. Dieses Dokument beschreibt die Umsetzung der CP.
- **PDS** (Policy Disclosure Statement): Dieses Dokument ist ein Auszug aus dem CPS, falls das CPS nicht veröffentlicht werden soll.

Eine PKI bietet ein hierarchisches Gültigkeitsmodell an. Wird einer Zertifizierungsstelle vertraut, wird damit allen von ihr signierten Zertifikaten auch vertraut. Da eine CA untergeordnete CAs haben kann (Mehrstufigkeit), wird auch allen untergeordneten CAs vertraut.

Arbeitsweise einer PKI
Die Zertifizierungsstelle bekommt einen Antrag auf Ausstellung eines CA-Zertifikats. Nach positiver Prüfung der Daten wird ein Zertifikatspärchen erstellt, ein öffentliches und ein privates. Das öffentliche Zertifikat ist über die Zertifikatsserver öffentlich erreichbar. Damit kann eine Datei verschlüsselt werden und der Empfänger (der Eigner des privaten Schlüssels) verifiziert werden, solange der private Schlüssel gültig ist. Verliert das Zertifikat seine Gültigkeit aufgrund

abgelaufenem Datum oder einem Eintrag in einer Sperrliste, verliert auch das öffentliche Zertifikat seine Gültigkeit. Nur mit dem privaten Zertifikat kann die Information wieder entschlüsselt werden. Somit lässt sich eine Infrastruktur aufbauen mit unendlich vielen Sendern, aber nur einer Zentralen Entschlüsselungseinheit.
Anmerkung: Eine Root-CA lässt sich auch selbst erstellen, diese Zertifikate sind dann „Eigenzertifiziert“. Hierbei fehlt die Letzte Vertrauensstelle (Trustcenter).

Quelle: https://kryptografie.de/kryptografie/index.htm
https://www.exploit-db.com/docs/deutsch/13598-[deutsch]-kryptographie---die-magie-der-asymmetrischen-verschl%C3%BCsselung.pdf
PKI: https://www.security-insider.de/was-ist-eine-pki-public-key-infrastruktur-a-696659/

Authentifizierung
In der digitalen Welt besteht eine starke Authentifizierung aus:

- Etwas was ich weis, wie zB ein Passwort
- Etwas was ich habe, wie zB ein Token
- Etwas was ich bin, zB ein Retina- oder Fingerabdruck

Mit diesen Informationen kann die Identität einer Person eindeutig und wiederholbar sichergestellt werden. Es ist die Voraussetzung Personen zu autorisieren.

Autorisierung
Eindeutig authentifiziere Personen können Berechtigungen zugewiesen bekommen. Dies geschieht zB mit ACL-Listen (Access Control List) oder Benutzerkontenverwaltungen. Es gibt zentrale Systeme wie eine AD-Domäne oder lokale Berechtigungen wie zB in Linux die etc/passwd
Mit diesen Berechtigungen lässt sich steuern wer welche Dateien, Dienste oder andere Funktionen in einem Rechnernetz bedienen darf. Auch eine Zutrittskontrolle kann so geregelt werden.

Firewall-Systeme
Eine Firewall ist ein aktiver Netzwerkfilter. Einfache Systeme regeln den Datenverkehr zwischen zwei Netzwerksegmenten durch öffnen und schließen der Ports.
Beispiel: Üblicherweise werden Datenpakete des Protokolls http über den Port 80 übermittelt. Möchte ich aus meinem lokalen Netz (LAN) mit meinem Webbrowser über einen Router im Internet eine Webseite abrufen, muss mein PC die Berechtigung haben mit dem Protokoll http über den Port 80 kommunizieren zu dürfen

http://www.yahoo:80 – so sähe die vollständige Zeile im Browser dafür aus

Schließe ich nun den Port 80 (dazu ist idealerweise mein Router auch eine Firewall) wird die Übertragung der IP-Pakete unterbunden. Ein Austausch von Daten ist nicht mehr möglich.
Bessere Firewalls erkennen den Inhalt eines IP-Pakets und können es einem Protokoll zuweisen. Mit solch einem Paketfilter können unabhängig des verwendeten Port unerwünschte Inhalte gefiltert und gelöscht werden.
Erstellt man einen Verbund aus zwei gegenüberliegenden Firewalls erhält man eine DMZ (demilitarisierte Zone). Ein besonderer Bereich im Netzwerk indem man alles darf, aber niemand hinein kommt. Eine Seite steht dabei im eigenen LAN und die andere Seite hat Zugang zu anderen Netzwerksegmenten, wie zB das Internet. Dazwischen ist ein eigenes Netzwerk mit besonderen Eigenschaften.

Anmerkung: Ein Penetrationstest, kurz Pentest, ist ein empirischer Sicherheitscheck unter definierten Rahmenbedingungen. Die Ergebnisse des Penetrationstests werden in einem Bericht zusammengefasst und die identifizierten Schwachstellen, Konfigurationsfehler und Best Practice Empfehlungen aufgelistet. .

Thema: Ausgewählte Maßnahmen zur Überwachung
Aussage: Ein starkes Sicherheitskonzept verlangt nach ständiger Kontrolle. Diese können erfolgen durch regelmäßige Pentests, Anti-Viren-und Malware- Scanner. Werden dazu wichtige Logdateien protokoliert und ausgewertet, ist man auch zukünftigen Angriffen nicht schutzlos ausgeliefert.

IDS (Intrusion Detection Systems)
Intrusion Detection Systems (IDS) helfen, Cyberbedrohungen zu erkennen, damit sie vom System und seinen Inhalten isoliert werden und Schäden am System verhindert werden können.

NIDS (Network Intrusion Detection Systems)
Ein Network Intrusion Detection System (NIDS) ist eine unabhängige Plattform, die den Netzwerkverkehr überwacht und Hosts untersucht, um Eindringlinge zu identifizieren. NIDSs verbinden sich mit Netzwerk-Hubs oder Netzwerk-Taps und werden oft an Datenengpässen platziert – normalerweise in einer demilitarisierten Zone (DMZ) oder Netzwerkgrenze –, um den Netzwerkverkehr zu erfassen und einzelne Pakete auf bösartige Inhalte zu analysieren.

HIDS (Host based Intrusion Detection Systems)
Ein hostbasiertes Intrusion Detection System (HIDS) ist ein direkt auf dem Host installierter Agent, der bösartigen Datenverkehr erkennt, der durch Systemaufrufe, Anwendungsprotokolle und Dateisystemänderungen geht. Es analysiert beispielsweise Passwortprotokollversuche und vergleicht diese mit bekannten Brute-Force-Angriffsmustern, um festzustellen, ob es sich um einen Angriffsversuch handelt.

Da HIDSs lokale Ereignisse auf Hosts überwachen, können sie Angriffe erkennen, die ein NIDS möglicherweise übersieht. HIDS ist auch ein effektives Werkzeug zum Erkennen und Verhindern von Softwareintegritätsverletzungen wie Trojanischen Pferden . Sie können auch in einer Umgebung betrieben werden, in der der Netzwerkverkehr verschlüsselt ist, was sie ideal für den Schutz hochsensibler Informationen wie rechtliche Dokumente, persönliche Informationen und geistiges Eigentum macht.

PIDS (Perimeter intrusion detection systems)
Ein Perimeter Intrusion Detection System (PIDS) erkennt und lokalisiert Einbruchsversuche an „Perimeter Zäunen“ wichtiger Systeminfrastrukturen wie dem Hauptserver. Ein PIDS-Setup kommt normalerweise in Form eines elektronischen oder faseroptischen Geräts, das auf den digitalen Zaun eines Servers montiert wird. Wenn es Störungen erkennt, die darauf hinweisen, dass ein Zugriff über andere Wege als den regulären Kanal versucht wird, löst es einen Alarm aus.

PIDS dient als Frühwarngerät und verhält sich wie ein Wachposten, der beim ersten Anzeichen eines Eindringlings das Hauptverteidigungskorps aufweckt. Es ist eine kostengünstige erste Verteidigungslinie, da es ohne große Änderungen oder Anpassungen einfach an Ihrem bestehenden System angebracht werden kann.

VMIDS (VM-based intrusion detection systems)
Ein auf virtuellen Maschinen basierendes Intrusion Detection System (VMIDS) ähnelt einem oder einer Kombination aus einem der drei oben genannten IDS, wird jedoch remote über eine virtuelle Maschine (VM) bereitgestellt. Er ist der neueste der vier IDS-Typen und wird derzeit noch verbessert. Die meisten Managed IT Services Provider (MSPs) verwenden ein VMIDS-Setup.

Quelle: https://www.outsourceitcorp.com/the-four-types-of-ids-and-how-they-can-protect-your-business/

Anti-Viren Programme und Malware
Zitat: „Malware (zusammengesetzt aus dem engl. malicious: bösartig und ware von Software) bezeichnet ein schädliches Programm (Schadsoftware). Dies sind Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte bzw. schädigende Funktionen auszuführen. Der Begriff bezeichnet keine schadhafte Software, obwohl auch diese Schaden anrichten kann.“

Malwarescanner können und sollen zentral und lokal installiert werden. Die zentrale Instanz überwacht den Datenverkehr im LAN, wobei die lokalen Scanner jeden einzelnen PC schützen, auch wenn er sich nicht im eigenen lokalen Netzwerk befindet.
Malwarescanner arbeiten auf zwei unterschiedliche Weisen:
Bei der reaktiven Erkennung sucht der Scanner nach auffälligen Code-Schnipsel, sogenannte Signaturen. Diese werden vom Hersteller in Datenbanken erstellt und dienen als Suchmuster-Referenz.
Die heuristische oder proaktive Erkennung bewertet potenzielle Schadprogramme aufgrund ihres Verhaltens. Diese so genannte proaktive Erkennung findet Verwendung in statischen und dynamischen Scannern (Sandbox-Technik).

Wird eine Schadsoftware gefunden, verhindert der Scanner die vollständige Ausführung des Schadcodes und stellt infizierte Dateien unter Quarantäne.

Quelle: https://wirtschaftslexikon.gabler.de/definition/malware-53410/version-276503

Anmerkung: Viren sind auch Malware, daher ist jedes Antivirenprogramm auch ein Malwarescanner.

Protokollierung
Um sicherheitsgefärdende Ereignisse zu dokumentieren schreiben fast alle Systeme sogenannte Log-Dateien. Selbst in einfachen Zutrittskontrollen wird in der Regel ein Logbuch geführt.
IPS (Intrusion Prevention Systems)
In rechnergestützten Systemen können diese Logdateien zentralisiert und automatisch ausgewertet werden. Durch ein Filter initiiert, meldet dann das IPS sicherheitsrelevante Ereignisse und verhindert durch ein Regelwerk die weitere Durchführung. So kann schnell reagiert werden und die Sicherheitsverletzung gestoppt.
Ziel solch eines Programms kann sein, alle Serverdienste gegen Angriffe des Typs Denial of Service (DoS) abzusichern. Allerdings darf man nicht vergessen, dass die Grundfunktion (Sperren einzelner IP-Adressen) insbesondere bei "Distributed Denial of Service"-Angriffen (DDoS) durch Bot-Netze an ihre Grenzen stoßen wird.

Siehe: https://www.graylog.org/ , https://www.splunk.com/ und https://wiki.ubuntuusers.de/fail2ban/

Thema: Organisatorische Sicherheitsmaßnahmen
In Rechnergestützten Systemen definiert das Betriebskonzept die Vorgaben der organisatorischen Sicherheitsmaßnahmen.

Das Betriebshandbuch
Ein Betriebshandbuch beschreibt “Wer, Was, Wann, Wie, Wie oft” tun muss, um den operativen Betrieb einschließlich der erforderlichen Kontroll- und Wartungsarbeiten sicherzustellen, d.h. die operativen Tätigkeiten.

Wichtig sind u.a. Beschreibungen aller notwendigen Maßnahmen und deren Einhaltung zur Gewährleistung des ordnungsgemäßen Anwendungsbetriebs sowie der Betriebsbedingungen und Voraussetzungen. Auch Anleitungen und Workarounds für das Störungsmanagement können in die Betriebshandbücher aufgenommen werden. In der Praxis besteht ein Betriebshandbuch deshalb häufig aus einem Set an Dokumenten, das zum einen Ablaufbeschreibungen und zum anderen Arbeitshilfen für die täglichen Routinearbeiten umfasst. Hierbei kann es sich um textliche Anleitungen, bei komplexeren Abläufen auch um Handbücher handeln. Hilfreich sind auch Zeitpläne, Formulare und Checklisten. Checklisten und Formulare können während der Ausführung der Aktivität ausgefüllt und abgezeichnet werden und dienen dann als Nachweisdokumente.

GRC-Dokumentation
GRC steht für Governance-, Risk- und Compliance-Management und beschreibt die drei wichtigsten Handlungsebenen eines Unternehmens. IT-GRC dient dazu die IT transparent und damit steuerbar zu machen, Risiken zu identifizieren und zu behandeln und sicherzustellen, dass die IT sich konform (compliant) zu externen Regelwerken, insbesondere Gesetzen verhält. Für diese Bereiche müssen Maßnahmen, Prozesse und Kontrollen implementiert und nachvollziehbar dokumentiert werden.
Beispiel: https://www.sap.com/germany/products/erp-financial-management/grc.html

Notfallkonzept
Der Notfallplan ist das zentrale Dokument um auf Notfälle in der IT angemessen unverzüglich und juristisch korrekt reagieren zu können und hilft den möglichen Schaden einzugrenzen. Ein Notfallplan ist dabei ein Leitfaden, der Handlungsanweisungen und zu ergreifende Maßnahmen bei IT-Notfällen definiert. Solche Notfälle sind z.B.:

- Hackerangriffe
- technische Störungen
- Stromausfälle
- Feuer
- Hochwasser oder Rohrbrüche
- Personalausfälle
- Einbrüche und Diebstahl

Achtung: Versicherungstechnisch wird unterschieden in

- Höhere Gewalt (Wetterereignisse, Erdbeben, Meteoriteneinschlag...)
- unverschuldet (Unfälle, unvorhersehbare technische Defekte, Diebstahl...)
- Selbstverschuldet / Teilschuld (unsachgemäße Bedienung/Verwendung, unzureichende Sicherheitskonzepte...)

Handlungsanweisung für einen bestimmten Notfall in Form einer Checkliste (Welche Gegenmaßnahmen sind zu ergreifen?)

- Festlegung von Verantwortlichkeiten und Alarmierungsketten (Wer ist zu benachrichtigen? Interne Personen oder externe Dienstleister? Wie ist die Person zu erreichen? Wer ist der Stellvertreter?)
- Handlungsanweisung zur Wiederherstellung der Funktion der Systeme
- Liste über ggf. zusätzlich relevante Dokumentationen
- Auflistung über erforderliche Zugangsdaten

- Liste über zu informierende Personen im Nachgang an den Vorfall (Vorgesetzter, Geschäftsleitung, Datenschutzbeauftragter etc.)

Teil jedes Notfallplans muss immer die Notfall-Simulation sein. Hierbei wird der Ernstfall simuliert und dabei die Vorgehensweise laut Notfallplan auf Vollständigkeit wund Wirksamkeit geprüft. Hierzu hat der BSI Standarts entwickelt:

- BSI-Standard_1004 beschreibt allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS)
- BSI-Standard 100-2 [BSI2] beschreibt die IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3 [BSI3] stellt eine Methode für die Durchführung einer Risikoanalyse vor, die für die
  Vorgehensweise nach IT-Grundschutz optimiert ist.
- BS 25999-1 / BS 25999-2 vom British Standards Institute veröffentlicht, beschreibt den Aufbau eines Management-
  Systems für das Notfallmanagement [BS259991].
- BS 25999-2 Part 2: Specification“ legt die
  Punkte fest, die zur Zertifizierung eines Business Continuity Managements vorhanden sein müssen
  [BS259992].
- Good Practice Guidelines” (GPG) des Business Continuity
  Institute (BCI) [GPG08]. Das BCI wurde 1994 gegründet und hat in mehr als 85 Ländern über 4000
  Mitglieder (Stand Februar 2008). Sein Ziel ist es, einen hohen Standard und Kompetenz im Bereich
  des Business Continuity Management zu setzen.
- ISO / PAS 22399 ist die Vornorm „Sicherheit und
  Schutz des Gemeinwesens - Leitfaden für Planung, Vorbereitung und operationelle Kontinuität“
- ISO 27001 / ISO 27002 ist die erste internationale Norm zum Management
  von Informationssicherheit, die auch eine Zertifizierung ermöglicht
- NIST SP 800-34 ist ein Leitfaden zur Notfallvorsorgeplanung für IT-Systeme [NIST34].
- PAS 77 / BS 25777 beschreibt die Prinzipien und Methoden für den Aufbau und die Umsetzung eines IT Service Continuity Managements.
- ISO / IEC 24762 beschäftigt
  sich mit den Anforderungen an die Wiederanlauf-Services für die Informations- und Kommunikationstechnologie.
- ITIL hat sich inzwischen als weltweit akzeptierter De-facto-Standard für
  Gestaltung, Implementierung und Management wesentlicher Steuerungsprozesse in der IT etabliert.
- ISO/IEC 20000 ermöglicht eine Zertifizierung des IT Service Managements einer Institution.

Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=1

Link:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungsrahmenwerk/odt/Modul_Notfallhandbuch.html Modul Notfallhandbuch des BSI

Datensicherheitskonzept
Ein Datensicherheitskonzept regelt den Umgang mit Daten, sowohl im Normal- als auch im Fehlerfall. Hierbei wird der technische Umgang sowie der organisatorische Umgang festgelegt.

Ziel eines Datensicherungskonzeptes ist es, klar und verständlich zu dokumentieren, welche Maßnahmen IT-Systeme und Daten vor versehentlichem Verlust schützen und wie im Verlustfall Daten schnell rekonstruiert werden können.
Um diese Ziele erreichen zu können, muss/sollte das Datensicherungskonzept folgende Punkte berücksichtigen:

- Verantwortliche Personen
- Betrachtete IT-Systeme (Server, Clients, ggf. mobile Geräte)
- Betrachtete Datenspeicherarten (Datenbanken, Files oder auch ganze Festplatten)
- Betroffene Daten und Datenarten (Personaldaten, Kundendaten etc.)
- Art der Datensicherung (Vollsicherung, Inkrementell oder Differenziell)
- Häufigkeit der Sicherungen (täglich, wöchentlich, jährlich)
- Kombinationen aus Art und Häufigkeit
- Verwendetes Raid im Backup-Server
- Sicherungen der Backup Server: Bandsicherungen, Co-Location, etc.
- Sicherungsmaßnahmen für den Backup-Server
    - Räumlichkeiten (Zugang, Gefahr von Brand- und Wasserschäden)
    - Hardware Monitoring (Speicherkapazität, Temperatur, allgemein Zustand, Benachrichtigung über fehlgeschlagene Backups)
    - Zutritts- und Zugangsberechtigungen
    - Verschlüsselung der Datenträger des Backup-Servers
- Prozesse zum Zurückspielen/Wiederherstellen von Daten (ggf. in Kombination zum Notfallhandbuch)
- Vorgaben zur Nutzung der Daten für andere Zwecke (Beweissicherung, Abgleich von Versionsständen, Erfüllung von Nachweispflichten etc.)

Ein Leitfaden stellen die Umsetzungshinweise zum „Baustein CON.3 Datensicherungskonzept“ des BSI dar

Link:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_CON_3_Datensicherungskonzept.html Umsetzungshinweise zum Baustein CON.3 Datensicherungskonzept

Thema: Aufbau- und ablauforganisatorische Maßnahmen im Hinblick auf IT-Security
Frage:
Welche Maßnahmen gibt es und deren Betrachtung auf Nutzbarkeit, Effizienz, Kosten und Risiken.

Personelle Massnahmen

Datenschutzbeauftragter:

Aufgaben: Zitat: „Zu den Aufgaben des Datenschutzbeauftragten zählen: Das Hinwirken auf die Einhaltung aller relevanten Datenschutzvorschriften, die Überwachung bestimmten Prozesse wie der Datenschutz-Folgenabschätzung oder der Sensibilisierung und Schulung der Mitarbeiter sowie die Zusammenarbeit mit der Aufsichtsbehörde.“ Quelle: https://dsgvo-gesetz.de/themen/datenschutzbeauftragter/

Ab diesen Gegebenheiten ist ein DSB laut DSGVO verpflichtend:

- Das Unternehmen beschäftigt mindestens neun Mitarbeiter, die personenbezogene Daten automatisiert verarbeiten
- Das Unternehmen übermittelt personenbezogene Daten geschäftsmäßig, erhebt oder verarbeitet diese.
- Das Unternehmen verarbeitet besonders sensible Daten

Der DSB kann intern oder extern besetzt werden.

Sicherheitsbeauftragter: (Optional)

Aufgaben, klassisch:

- Prüfung des Zustandes der Schutzeinrichtungen und der persönlichen Schutzausrüstungen
- Information der Mitarbeiter über den sicheren Umgang mit Arbeitsstoffen und Maschinen
- Meldung von sicherheitstechnische Mängel an den Vorgesetzten
- Teilnahme an regelmäßigen Betriebsbegehungen
- Untersuchungen von Unfall- und Berufskrankheiten

Die Aufgaben eines Sicherheitsbeauftragten werden von der Deutschen Gesetzliche Unfallversicherung in der DGUV Vorschrift 1 - Grundsätze der Prävention, §20 Bestellung und Aufgaben von Sicherheitsbeauftragten genau definiert

Link: https://www.dguv.de/fb-org/sachgebiete/sicherheitsbeauftragte/aufgaben/index.jsp

In einem IT-Umfeld ergibt sich eine modernere Auslegung der Tätigkeiten:

- Prüfung der vorhandenen Datenschutzeinrichtungen von Server und Client
- Schulung der Mitarbeiter im Umgang mit vertraulichen Daten
- Meldung von Datenschutzverletzungen an den vorgesetzten und Datenschutzbeauftragte.
- Teilnahme an regelmäßigen Schulungen und Weiterbildungen
- Mithilfe bei der Untersuchung, Vermeidung und Behebung von Datenschutzverletzungen

Compliance-Manager (Optional)

Ein Compliance Manager stellt rechtlich und ethisch korrektes Verhalten in einem Unternehmen sicher. Dazu erarbeiten sie mit der Geschäftsleitung und dem Betriebsrat Verhaltensrichtlinien, die ein rechtlich und ethisch korrektes Verhalten von Unternehmen, Organisationen und Mitarbeitern gewährleisten soll und optimieren die eingeführten Maßnahmen und Normen kontinuierlich. Sie organisieren auch deren Umsetzung und überwachen diese. Dazu gehört auch der korrekte Umgang mit vertraulichen Daten und sicherheitsrelevanten Verhaltensweisen.

Quelle: https://wirtschaftslexikon.gabler.de/definition/compliance-27721/version-333143

Compliance-Richtlinien

International: Practices Act (FCPA) (USA) und UK Bribary Act (GB)

Quelle:

FCPA: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act

und https://www.sec.gov/investor/alerts/fcpa.pdf

UK Bribary Act: https://www.legislation.gov.uk/ukpga/2010/23/contents

Deutschland: Deutsche Corporate Governance Kodex (DCGK)

Quelle: https://dcgk.de/de/

Anmerkung: In Betrieben, in denen ein Betriebsrat besteht, sind generelle Verhaltensregelungen gemäß § 87 Abs.1 Nr.1 BetrVG mitbestimmungspflichtig.

Anmerkung: Es ist für alle drei Positionen anzuraten, diese als Stabsstelle zu etablieren. So ist gewährleistet das sie unabhängig, frei und mit genügend hoher Weisungsbefugnis agieren können.

Die Position ist zwar optional und rechtlich nicht vorgeschrieben, aber im besonderen unter börsennotierten Unternehmen unumgänglich.

Anmerkung: Weitere Infos:
https://www.validatis.de/kyc-prozess/news-fachwissen/compliance/