**Vertraulichkeit (Maßnahmen und betriebliche Aufarbeitung)**

Inhalt

[Vertraulichkeit (Maßnahmen und betriebliche Aufarbeitung) 1](#_Toc93657010)

[Vertraulichkeit 1](#_Toc93657011)

[Technischen Maßnahmen: 2](#_Toc93657012)

[Firewall 2](#_Toc93657013)

[Verschlüsselung 2](#_Toc93657014)

[Datenschutzmanagementsystem (DSMS) 3](#_Toc93657015)

[Anonymisieren ist Verarbeitung 3](#_Toc93657016)

[Pseudonymisierung 3](#_Toc93657017)

[Organisatorische Maßnahmen: 4](#_Toc93657018)

[Zonenkonzept 4](#_Toc93657019)

[Dokumentklassifikation 4](#_Toc93657020)

[Zutrittskontrolle 4](#_Toc93657021)

[Datentransport 5](#_Toc93657022)

[Zugangskontrolle 5](#_Toc93657023)

[Denkaufgabe: wie werden Schutzobjekte ermittelt? 6](#_Toc93657024)

# Vertraulichkeit

Erhebe und beschreibe technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit von IV-Systemen.

Beispielhaft:

technisch: Firewall, Verschlüsselung (symmetrisch, asymmetrisch), ...

organisatorisch dazu: Zonenkonzept, Begleitpersonen, Dokumentklassifikation, ...

Unter Vertraulichkeit versteht man, dass Daten nur von den Personen eingesehen oder offengelegt werden dürfen, die dazu auch berechtigt sind. Will man Daten vertraulich behandeln, muss festgelegt sein, wer in welcher Art und Weise Zugriff auf diese Daten hat.

Zur Vertraulichkeit von Daten gehört auch, dass diese bei der Übertragung nicht von unautorisierten Personen gelesen werden! Das heißt, es muss dafür gesorgt sein, dass die Daten bei einer Übertragung in geeigneter Weise verschlüsselt werden.

Ein gutes Beispiel aus der Praxis ist der E-Mail-Verkehr. Vermutlich umfasst dieser wöchentlich mehrere tausend E-Mails. Darunter befinden sich mit Sicherheit Informationen, die vertraulich zu behandeln sind. Daher muss der E-Mail-Verkehr verschlüsselt sein! Andernfalls kann die Vertraulichkeit der Daten, die per E-Mail versendet wurden, nicht mehr garantiert werden.

Auch Räumlichkeiten, in denen vertrauliche Datenbestände wie. z.B. die Lohnbuchhaltung verarbeitet oder gelagert werden, müssen entsprechend gesichert sein. Wenn solche Räume frei zugänglich sind, kann man die Vertraulichkeit der dort befindlichen Daten vergessen!

# Technischen Maßnahmen:

* Firewall
* Verschlüsselung (symmetrisch, asymmetrisch)
* Datenschutzmanagementsystem
* Anonymisierung
* Pseudonymisierung

## Firewall

Die Firewall ist die Schnittstelle zwischen Netzwerk und dem Internet. Sie ist für den Austausch von Daten-Paketen zwischen den zwei Netzwerken zuständig. Dabei werden nicht die Dateninhalte von der Firewall überprüft, sondern das Verhaltensmuster von IP-Adressen, Ports und Protokollen des Versenders und Empfängers, um einen kontinuierlichen Schutz nach außen zu bieten. Um einen sicheren Schutz zu bieten, ist es möglich, Regeln zu erstellen um Daten, die als gefährlich eingestuft werden, zu blockieren.

Oft werden im Arbeitsalltag sensible Daten verwendet, die unter allen Umständen vor unautorisiertem Zugriff Unbefugter effektiv geschützt werden müssen. Auch beim Download oder Abruf jeglicher Daten aus dem Internet schützt die Firewall Ihr Netzwerk vor unerwünschten und gefährlichen Schadprogrammen. Sie überwacht den eingehenden und ausgehenden Datenaustausch und schütz Ihr Netzwerk so rund um die Uhr.

Mit Hardware-basierten Firewalls und der damit verbundenen intelligenten und lernenden Software wird vor komplexen Angriffen von Viren, Trojanern und Spyware auf Ihre Unternehmensinternen Daten geboten. Hierbei handelt es sich um eine Inhaltsfilterung zur Umsetzung von Internetschutzrichtlinien. Auch das Aufrufen bestimmter Webseiten kann damit komplett blockiert und gesperrt werden.

## Verschlüsselung

Mit einer Verschlüsselung kann das Schutzziel der Vertraulichkeit erfüllt werden. Der Zugriff von Unbefugter auf personenbezogene Daten durch Verschlüsselung soll verhindert werden. Sinn und Zweck des Verschlüsselns ist es, den Schutz der personenbezogenen Daten, die verarbeitet werden, zu erhöhen oder zu gewährleisten. Wenn nur Befugte den Schlüssel zur Entschlüsselung haben, bedeutet das auch, dass Unbefugte keinen Zugriff haben. Unbefugte sind alle, die die entsprechenden Daten nichts angehen.

Durch Verschlüsselung von personenbezogenen Daten wird auch das Risiko von Datenpannen, Schadensersatzansprüchen oder Bußgeldern vermindert. Wenn nämlich durch die Verschlüsselung das Schutzziel der Vertraulichkeit auch bei unbeabsichtigtem Verlust gewährleistet, bleibt.

Man sollte immer verschlüsseln, wenn man personenbezogene Daten transportieren oder weitergeben. Denn auf ihrer „Reise“ sind die Risiken für personenbezogene Daten immer höher. Überall wo Sie Zugriffe von Dritten nicht (ausreichend) ausschließen oder kontrollieren können, soll ebenfalls verschlüsselt werden.

Die Transportverschlüsselung sichert die Daten vor fremde Kenntnisnahme auf dem Weg, bzw. bei der Übertragung. Hier bieten sich Protokolle wie SSL/TLS oder VPN Verbindungen an.

Bei der Ende zu Ende Verschlüsselung können nur Sender und Empfänger die (verschlüsselten) Daten lesen.

## Datenschutzmanagementsystem (DSMS)

Der Kern eines DSMS bildet ein Rahmenwerk zum Datenschutz – das können Vorgaben für die Beschäftigten sein – zum Beispiel Richtlinien. Richtlinien sind eine einfache Möglichkeit der Umsetzung. Darin stehen notwendige technische und organisatorische Maßnahmen zur Umsetzung von Datenschutzanforderungen. Beschäftigte erfahren so, was sie tun müssen, um die Anforderungen aus dem Datenschutz umzusetzen. Sie erhalten diese Vorgaben oder auch Weisungen von der für den Datenschutz verantwortlichen Geschäftsführung. Damit die Beschäftigten von den Richtlinien erfahren, teilt die Geschäftsführung ihnen das in einer Leitlinie mit. Darin steht also, dass es Richtlinien zum Datenschutz gibt. An die sollen sich alle Mitarbeiter halten.

## Anonymisieren ist Verarbeitung

Durch die Anonymisierung verlieren die personenbezogenen Daten ihren Personenbezug – danach sagen sie nichts mehr über eine bestimmte Person aus. Eine gelungene Anonymisierung macht eine Zuordnung unmöglich. Es handelt sich um eine sehr wirksame Maßnahme im Datenschutz.

Personenbezogene Daten richtig anonymisieren geht nur, indem eine „Entanonymisierung“, also eine Umkehr des Vorgangs, nicht mehr machbar ist.

Denken man an demokratische geheime Wahlen. Durch das Aushändigen der Wahlzettel und das Setzen der Kreuze ohne Personenbezug ist jeder Stimmzettel anonym. Nachvollziehbar ist nur, wer zur Wahl erschienen ist, wobei sogar das auf einem anderen Zettel steht – die Daten werden voneinander getrennt. Wichtig ist, dass durch das anonyme Wahlverfahren nicht nachvollziehbar ist, wer wen gewählt hat.

## Pseudonymisierung

Ein Pseudonym verschleiert die tatsächliche Identität einer Person für alle nicht eingeweihten. Zum Beispiel haben alle Mitarbeit in einem Unternehmen eine Personalnummer. Wenn man ein Vergleich der Gehälter macht und hier nur die Personalnummer, Art der Stelle und das Gehalt gegenüberstellen, ist diese Aufstellung pseudonymisiert. Genauso ist es mit Kunden- und Lieferantennummern. Durch die Vergabe einer solchen Nummer, wird die Identität für Unbefugte verschleiert.

Wirksam ist die Pseudonymisierung nur so lange, wie Unberechtigte die Verbindung zur betroffenen Person nicht herstellen können. In den genannten Beispielen gibt es Dateien oder Datenbanken, in denen die Zuordnung der Nummer zu Namen erfolgt. Wer Zugriff auf diese „Schlüsseldateien“ hat, kann die Personen hinter dem Pseudonym ganz einfach identifizieren. Die Identitätsverschleierung kann damit also recht einfach aufgehoben werden. Deshalb ist eine Pseudonymisierung nur so wirksam wie die Maßnahmen zum Schutz der Schlüsseldatei stark sind.

# Organisatorische Maßnahmen:

* Zonenkonzept
* Dokumentklassifikation
* Zutrittskontrolle
* Datentransport
* Zugangskontrolle

## Zonenkonzept

Eine netzbasierte Sicherheitszone ist ein IP-Netzwerk, das aus Sicherheitsgründen von anderen Netzen getrennt wird.

Die Kommunikation in eine Sicherheitszone hinein oder aus einer Sicherheitszone heraus, wird durch Sicherheitsmaßnahmen kontrolliert. Hierzu werden die Sicherheitszonen durch Firewalls oder Intrusion Prävention Systeme (je nach Anforderung) zusammen verbunden.

Innerhalb einer Sicherheitszone wird auf Ebene des Netzes die Kommunikation nicht eingeschränkt.

Eine Firewall kann an mehrere Sicherheitszonen angebunden werden und eine Sicherheitszone kann ebenso mit mehreren Firewalls verbunden werden.

## Dokumentklassifikation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Öffentlich** | **Intern** | **Vertraulich** | **Geheim** | **Streng vertraulich** |
| Daten sind für jedermann, auch außerhalb der Firma, zugänglich. | Daten sind für jedermann, auch außerhalb der Firma, zugänglich. | Vertraulich definierte Daten sind lediglich einer begrenzten Anzahl an Mitarbeitern zugänglich, z.B. Personaldaten, Kundenlisten, Kalkulationen. | Zwischenebene zwischen Vertraulich und Strenggeheim. Verursacht mehr Kosten als Vertraulich aber weniger streng vertraulich. | Streng vertrauliche Daten sind punktuell und ausschließlich bestimmten definierten Personen zugänglich. Eine Weitergabe kann das Unternehmen nachhaltig schädigen. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Öffentlich | Intern | Vertraulich | Geheim | Streng geheim |
| Wirtschaft | Firmenbuch | Gewinn und Verlust |  |  | Aktien |
| Rechtlich | Verhalten im Notfall | Regelwerke, Arbeitsanweisung | Personenbezogen Daten | Passwörter | NDA |
| Organisatorisch | Geschäftsführer-in | Interne Veranstaltungen | Treffen der Geschäftsführer |  |  |
| Technisch | Webseite | Kommunikation | E-Mail |  |  |
| Baulich | Lager, Büro | Pausenhof | Spind | Server-Raum |  |

## Zutrittskontrolle

Es geht damit also um Maßnahmen, die verhindern, dass unberechtigte Personen Bereiche, Grundstücke, Gebäude, Gebäudeteile oder Räume betreten.

Aus einem anderen Blickwinkel betrachtet kann man auch sagen, dass durch die Anwendung der Zutrittskontrolle nur berechtigten Personen Zutritt zu Datenverarbeitungsanlagen, oder Bereichen, in denen diese aufgestellt sind, gewährt wird. Es handelt sich tatsächlich um den physischen Zutritt, also das körperliche Herantreten an Datenverarbeitungsanlagen.

Unberechtigte dürfen keinen räumlichen Zugriff auf Anlagen haben, mit denen personenbezogene Daten verarbeitet werden. Das gleiche gilt auch für analoge Daten (z.B. Akten mit personenbezogenen Daten). Wer berechtigt, oder unberechtigt ist, steht in einem Zutrittskonzept.

Zur Nachvollziehbarkeit der Zutrittsberechtigung müssen als nächstes Regeln erstellen werden. Wie hoch der Schutz sein muss, hängt wie immer vom Schutzbedarf der Daten ab. Je nach Art der personenbezogenen Daten kann der Schutz unterschiedlich ausfallen.

Den Zutritt kontrollieren Sie, beispielsweise

* mit abschließbaren Türen (Schlösser die auch benutzt werden)
* Zutritt nur für bestimmte Personen (mit Schlüssel) zu bestimmten Bereichen
* durch Verhindern des Betretens von Sicherheitsbereichen (durch Wachschutz)
* Kontrolle des Eingangs zum Betriebsgelände

Das bedeutet nicht, dass jedes Unternehmen einen Wachschutz mit Schäferhund benötigt. Generell sind die Maßnahmen immer abhängig von der Notwendigkeit und Wirksamkeit in der Gesamtheit, bzw. Kombination. (Es nützt nichts, wenn man zwar Schlösser hat, aber niemand wusste, dass man abschließen sollte.)

## Datentransport

Mit Regelungen zur Weitergabe vermeidet man, dass personenbezogene Daten während des Transports von Unbefugten gelesen, kopiert, verändert oder entfernt werden können. Genau das ist auch das Ziel: man möchte nicht, dass Informationen in irgendwo landen. Vielmehr steuern und legt man fest, was passieren soll.

Zum Transport zählt neben dem physischen Transport auch die elektronische Übertragung. Anschließend auch die Speicherung auf einem Datenträger oder Speichermedium.

Sie müssen überprüfen und feststellen können, wo (an welcher Stelle) eine Datenübertragung stattfinden soll, bzw. eine Übertragung geplant ist.

Der Begriff Weitergabekontrolle ist etwas missverständlich. Es ist tatsächlich nicht die Kontrolle oder Protokollierung der Datenweitergabe. Es geht vielmehr darum die Weitergabe von Daten vorhersehbar, und damit kontrollierbarer zu machen.

Empfänger und die Übertragungswege vorab. Man legt also vorher Regeln fest.

## Zugangskontrolle

„Den Zugang berechtigter Personen kontrollieren“, bedeutet zu verhindern, dass unberechtigte Personen sich an Systemen anmelden können. Der Zugang zu Systemen wird also eingeschränkt. Möglicherweise wird der Zugang sogar verhindert.

* Verwaltung von Berechtigungen
* Vorgaben zu Passwörtern (Passwortrichtlinie)
* Automatische Bildschirmsperre

Wer berechtigt, oder unberechtigt ist, steht im Berechtigungskonzept – alternativ können Berechtigungen auch über Rollen festgelegt werden, dann nennt sich das Ganze Rollenkonzept (gerne auch in Kombination Berechtigungs- und Rollenkonzept). Wem Konzepte zu überdimensioniert erscheinen, regelt den Zugang in Benutzerprofilen.

Berechtigte sind Personen, die bestimmte Daten zur Erfüllung ihrer Aufgaben benötigen. Diese ergeben sich wiederum aus Aufgabenbeschreibungen oder Positionen.

# Denkaufgabe: wie werden Schutzobjekte ermittelt?

Ziel der Strukturanalyse ist es, diejenigen Objekte zu identifizieren und in ihrem Zusammenwirken zu beschreiben, für die in einem Sicherheitskonzept angemessene Schutzmaßnahmen festgelegt werden müssen. Daher ist es wichtig, diese Schutzobjekte vollständig und hinreichend zu erfassen.

Ziel der Strukturanalyse ist es nicht, ein vollständiges Inventar über alle eingesetzten technischen Komponenten zu erhalten. Vielmehr sollten Sie bei allen Teilerhebungen Objekte sinnvoll zu Gruppen zusammenfassen, die Sie in den Folgeschritten der Konzeptentwicklung als ein einziges Objekt behandeln können. Zum Beispiel ist es zweckmäßig, IT-Systeme, die gleich oder ähnlich konfiguriert sind und für die gleichen Aufgaben genutzt werden, zu einer Gruppe zusammenzufassen.

Generell gilt, dass Sie Komponenten zusammenfassen sollten, die

* vom gleichen Typ sind,
* gleich oder nahezu gleich konfiguriert sind,
* gleich oder nahezu gleich in das Netz eingebunden sind,
* den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen,
* die gleichen Anwendungen bedienen und
* den gleichen Schutzbedarf aufweisen.

In der Regel bietet sich an, Clients in Gruppen zusammenzufassen. Gruppierungen sind aber auch für Server möglich, wenn diese die oben genannten Kriterien erfüllen. Dies trifft z. B. auf redundant ausgelegte Server zu. Weitere typische Beispiele für Gruppierungen sind gleich ausgestattete und genutzte Büroräume oder die Kommunikationsverbindungen zwischen einem Switch und den Clients einer Gruppe. In den nachfolgenden Abschnitten werden weitere Beispiele für zweckmäßige Gruppenbildungen genannt.