



Informationssicherheit und Datenschutzkonzept

Metainformationen

Info	Beschreibung
Version	1.0
Author	Mattia Gallicchio
Datum	5. September 2023
Klassifizierung	S3

Dokumentinhalt

Dieses Dokument wurde durch den oben genannten Autor verfasst. Alle Texte stammen von ihm. Für einzelne Definitionen wie zum Bsp. Begriffserklärungen wurden externe Inhalte einbezogen, diese sind jedoch mit einer Quelle markiert.

Zuständigkeiten des ISDS-Konzept

Dieses ISDS ist stetig auf dem neusten Stand zu halten. Sollten Vorfälle im Zusammenhang mit der Informationssicherheit geschehen, so muss sich auf dieses Konzept verlassen werden können. Sollten Änderungen vorgenommen werden, so müssen alle Mitarbeitenden darüber informiert werden, dass das ISDS aktualisiert worden ist. Gemacht wird das durch ein Mail an alle betroffenen Personen (Mail-Verteiler: isds@mammatus.ch), in dem die Änderungen zusammengefasst beschrieben sind. Dies ist ein endloser Prozess, wie folgende Abbildung aufzeigt:

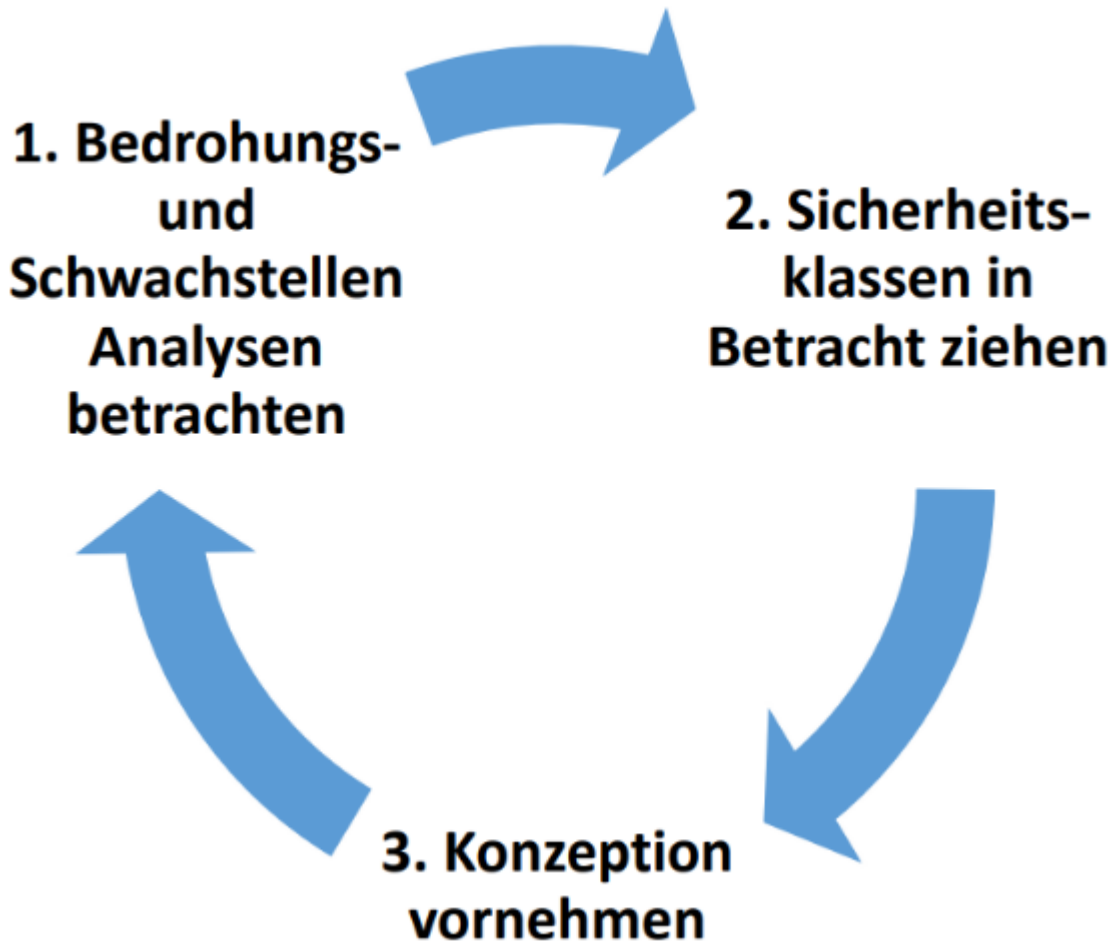


Abbildung 1. Mattia Gallicchio. (2023). - Sicherheits-Cycle

Die oben beschriebene Zuständigkeit liegt beim aktuellen CISO(Chief Information Security Officer), dieser ist nur dafür zuständig und darf für die Ausführung von Änderungen an seine Mitarbeitenden delegieren!

Gültigkeit des ISDS-Konzeptes

Die Gültigkeit des ISDS-Konzepts beträgt maximal 5 Jahre.

Ziele des Konzepts

Ziel dieses Konzepts ist es Standards für Prozesse und Umgang mit Daten in Zusammenhang mit der Informationssicherheit aufzuzeigen.

Vertraulichkeit

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 klar festgelegt sein, wer in welcher Art und Weise Zugriff auf diese Daten hat. Doch man muss noch einen weiteren Aspekt beachten, den viele gerne vergessen!

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. Zu den verschiedenen Verschlüsselungsverfahren erfahren Sie hier mehr.

Ein gutes Beispiel aus der Praxis stellt hier vor allem Ihr E-Mail-Verkehr dar. Vermutlich umfasst dieser wöchentlich mehrere tausend E-Mails. Darunter befinden sich mit Sicherheit Informationen, die vertraulich zu behandeln sind. Aber können Sie auch garantieren, dass diese Informationen nur die Augen erreichen, für die sie bestimmt sind? Ihr E-Mail-Verkehr muss verschlüsselt sein! Andernfalls können Sie die Vertraulichkeit Ihrer Daten, die per E-Mail versendet wurden, nicht mehr garantieren!

Und hier noch ein weniger technisches Beispiel: 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!

Quelle: Brandmauer IT. (10.10.2022) Vertraulichkeit, Integrität und Verfügbarkeit - Schutzziele der Informationssicherheit. Abgerufen am 05.09.2023 von: <https://www.brandmauer.de/blog/it-security/schutzziele-der-informationssicherheit>

Geheimhaltung

Alle Mitarbeitende müssen bei Antritt ihrer Stelle eine Geheimhaltung unterzeichnen.

Geheimhaltungen:

- Geheimhaltungsvereinbarung_mab - für alle MAB
- Geheimhaltungsvereinbarung_s3 - für alle Personen mit Zugriff auf Daten der Klassifizierung S3
- Geheimhaltungsvereinbarung_s4 - für alle Personen mit Zugriff auf Daten der Klassifizierung S4
 - Hier ist zusätzlich ein Background Check durch die IT Sicherheit durchzuführen. Für den Background-Check muss der MAB noch eine "Zustimmung für den Background-Check" unterzeichnen

Integrität

Viele verwechseln Integrität mit Vertraulichkeit. Integrität bedeutet allerdings, dass es nicht möglich sein darf, Daten unerkannt bzw. unbemerkt zu ändern. Es geht hierbei also um das Erkennen von Datenänderungen, wohingegen bei Vertraulichkeit der Fokus auf der Berechtigung liegt. Oft wird mit Integrität (man spricht dann von starker Integrität) sogar gefordert, dass Daten überhaupt nicht unberechtigt verändert werden können. Da sich dies aber selten sinnvoll umsetzen lässt, empfehle ich die erste Definition.

Nehmen wir einmal Forschungs- und Entwicklungsdaten. Wenn die Integrität solcher Daten zerstört ist, weil eine winzige Änderung unerkannt vorgenommen wurde, können Sie sämtlichen Daten nicht mehr trauen! Man muss niemandem erklären, dass dies eine Katastrophe wäre.

Quelle: Brandmauer IT. (10.10.2022) Vertraulichkeit, Integrität und Verfügbarkeit - Schutzziele der Informationssicherheit. Abgerufen am 05.09.2023 von: <https://www.brandmauer.de/blog/it-security/schutzziele-der-informationssicherheit>

Verfügbarkeit

Die Verfügbarkeit eines Systems beschreibt ganz einfach die Zeit, in der das System funktioniert. Im Sinne der Schutzziele geht es hier selbstverständlich darum, die Verfügbarkeit möglichst hoch zu halten. Anders gesagt: Es gilt, das Risiko von Systemausfällen zu minimieren!

Quelle: Brandmauer IT. (10.10.2022) Vertraulichkeit, Integrität und Verfügbarkeit - Schutzziele der Informationssicherheit. Abgerufen am 05.09.2023 von: <https://www.brandmauer.de/blog/it-security/schutzziele-der-informationssicherheit>

Zurechenbarkeit / Verbindlichkeit

Diese zwei erweiterten Schutzziele lassen sich recht gut anhand des Identitätsmanagements veranschaulichen. Verbindlichkeit bedeutet nämlich, dass es nicht möglich sein darf, ausgeführte Handlungen abzustreiten. Unter Zurechenbarkeit versteht man, dass es möglich sein muss, Handlungen eindeutig dem zuzuordnen, der sie ausgeführt hat. Die beiden Begriffe gehen also Hand in Hand. Vor allem hängen diese Eigenschaften an den im Unternehmen vorhandenen Identitäten!

Ein kleines Beispiel aus dem Unternehmensalltag: Es existiert ein Datenbestand, auf den über eine Applikation zugegriffen werden kann. Oftmals werden aus Kostengründen nur wenige Lizenzen gekauft. Dann sind auch nur wenige Benutzerkonten mit Passwort vorhanden, die anschließend von mehreren Personen benutzt werden (gerne „Shared User Accounts“ genannt). Offensichtlich ist hier Zurechenbarkeit nicht mehr gegeben, da Datenänderungen von mehreren Personen, die jedoch dieselbe digitale Identität benutzen, vorgenommen werden können. Mit solchen „Shared User Accounts“ zerstören Sie ganz leicht die Zurechenbarkeit, weshalb Sie diese Accounts schnellstmöglich eliminieren sollten! Wenn dies nicht ohne weiteres möglich ist, sollten Sie wenigstens entsprechende Dokumentationspflichten für Datenänderungen einführen.

Quelle: Brandmauer IT. (10.10.2022) Vertraulichkeit, Integrität und Verfügbarkeit - Schutzziele der Informationssicherheit. Abgerufen am 05.09.2023 von: <https://www.brandmauer.de/blog/it-security/schutzziele-der-informationssicherheit>

Aufbau der Informationssicherheit

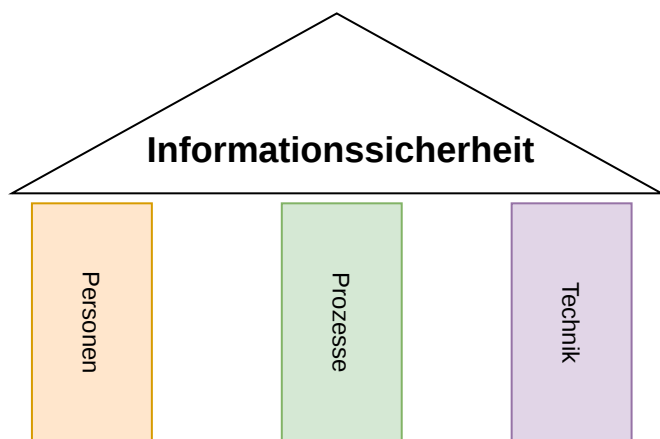


Abbildung 2. Mattia Gallicchio. (2023). - Aufbau der Informationssicherheit

Personen

Die Sicherheit um Personen und die dazugehörigen Daten. Die Garantie der Zurechenbarkeit / Verbindlichkeit.

Prozesse

Prozesse welche bei Mammatus genutzt werden um die Informationssicherheit aufrecht zu halten.

Technik

Technische Sicherheitsmassnahmen bei Mammat wie zum Bsp. Schutz der Räumlichkeiten (Physischer Zugang), Virtueller Schutz, Schutz von Kundendaten, Isolation von Kunden Umgebungen etc.

Faktor Mensch

Faktor Mensch ist in der IT Welt die grösste sicherheitslücke und ist nicht umgehbar. Jedoch ist es möglich auch hier das Risiko auf ein Minimum zu verkleinern.

Massnahmen

- Personen die sich nicht besonders gut mit IT auskennen wie Administration, Kundenberatung usw. sind nicht im gleichen Netz wie Techniker. Ihr Netz ist isoliert und macht den Zugriff auf jegliche interne Systeme unmöglich!
- Alle Techniker werden alle 6 Monate an einem Halbtages Workshop von der IT-Sicherheit auf die neusten Attacken geschult. Es gibt jeweils zwei Daten, Teilnahme ist Pflicht!
- Kunden haben ihre Ressourcen in einem Isolierten Subnetz. Kommunikation nach aussen ist nur über gewisse Ports möglich. Jegliche Kommunikation in andere Zonen(Subnetzte) werden durch Firewalls Unterbunden.

Daten klassifizierung

Alle Daten bei Mammat müssen Klassifiziert werden:

- Zu Beginn der Datensammlung
- Bei Änderungen von Datenquellen
- Bei Veränderungen der Datenart

Achtung

Dazu zählen auch Dokumente. Ein Dokument das ein Mitarbeiter erstellt muss klassifiziert werden!

Als Datenquellen zählen auch Personen: Wird zum Beispiel eine Datenbank mit Benutzerdaten erweitert durch einen neuen Benutzerkreis so muss die Klassifizierung erneut erfolgen.

Klassifizierungsstufen

Stufe	Beschreibung
S1	Die Daten sind öffentlich verfügbar.
S2	Die Daten sind intern aber ohne eine weitere Sicherheitsstufe. Abgabe an Externe ist nicht erlaubt. Es sei denn, von den Externen wurde eine Geheimhaltung unterzeichnet.
S3	Speziell sichere Daten. Die Daten sind nicht für alle Interne zugänglich und müssen gut geschützt

werden.

- | | |
|----|---|
| S4 | Die Daten sind streng geheim und dürfen unter keinen Umständen zu unbefugten Personen kommen. Der Befugte-Bereich ist so klein wie möglich zu halten! |
|----|---|

Vorgehen im Notfall / Gefahrensituation

Definition Notfall :

Als Notfall gelten folgende Situationen:

- Dokumente ab Datenklassifizierungs Stufe S3 sind an unbefugte Personen übergegangen.
- Ein unbefugter Zugriff auf unsere Infrastruktur wurde festgestellt durch:
 - Überwachungssysteme
 - Personen der IT
 - Personen ausserhalb der IT - bestätigt durch die IT-Sicherheit
- Ein Mitarbeitender hat einen Fehler begangen (Phishing, SPAM etc.)

Definition Gefahr :

Als Gefahr gelten folgende Situationen

- Ein Konkurrent wurde Opfer eines Angriffs.
- Drohung an die Firma Mammatus oder einzelne Mitarbeitende
- Ein Sicherheitssystem ist ausgestiegen
- Viele Externe Personen im Gebäude (Tag der Offenen Tür etc.)

Sollte ein Notfall eintreffen ist umgehend die IT-Sicherheit zu informieren.

1. CISO
2. CISO Stellvertretung
3. IT-Sicherheit MAB

Die IT-Sicherheit wird sich dann um den Fall kümmern. Im Notfall ist die IT-Sicherheit befugt Systeme aus sicherheitsgründlichen umgehend Offline zu nehmen.

Achtung

Sollten Geräte infiziert sein diese umgehend vom Netzwerk nehmen. Ethernet ausziehen, Wifi Karte deaktivieren, Gerät Herunterfahren usw.

Sollte eine Gefahrensituation eintreffen so muss die IT-Sicherheit die ganze Firma per Mail über die aktuelle Gefahrenlage informieren. Sollte die Gefahr aufgrund einer technischen Störung sein, so muss an der Störungstelle manuell überwacht werden!

Die IT-Sicherheit ist für das Informieren und umsetzen allfälligen Massnahmen verantwortlich. Im Gefahrenfall ist die IT-Sicherheit befugt Systeme aus sicherheitsgründen Offline zu nehmen. Dabei gilt eine 2 Stündige Vorlaufzeit.

Ansprechpersonen

- Bei Fragen zu diesem Dokument wenden sie sich bitte an den Author.
- Bei Fragen zur IT Sicherheit wenden sie sich bitte an den CISO.

