lehmann

# Leitfaden
# **IT-Security**

## Empfehlungen auf technischer Ebene

Eine 100-prozentige Sicherheit wird auch durch technische Massnahmen nicht erreicht. Jedoch trägt eine sinnvolle Kombination von technischen Massnahmen wesentlich zur IT-Sicherheit im Unternehmensnetzwerk bei und mindert die Gefahr von Infektionen mit Schadsoftware. Das schwächste Glied in der Kette ist in vielen Fällen nicht die Technik, sondern Benutzer:innen. Werden diese nicht im sicheren Umgang mit IT-Systemen geschult, sind viele der aufgezählten technischen Massnahmen nutzlos.

1

### Virenschutz

Stellen Sie sicher, dass auf jedem Computer ein Virenschutz installiert ist. Sorgen Sie auch dafür, dass dieser sich regelmässig aktualisiert (Pattern-Update) sowie regelmässig einen vollständige Systemscan durchführt (z.B. wöchentlich oder monatlich).

2

### Systemupdates + Periodische Wartung der Systeme

Es muss sichergestellt sein, dass die Clients, die Netzwerkkomponenten sowie auch die Server in regelmässigen Abständen gewartet werden. Dazu gehört, die wichtigsten Logdateien auf Unregelmässigkeiten zu prüfen, die Systemupdates oder die Sicherheitsupdates einzuspielen.

## Logdateien

Sogenannte «Logfiles» sind bei der Nachbearbeitung eines IT-Vorfalles enorm wichtig. Stellen Sie sicher, dass kritische Systeme wie Buchhaltungssoftware, Domain-Controller, Firewall oder E-Mail-Server solche Logdateien anlegen. Es ist empfehlenswert, die angefallenen Logdateien regelmässig auf Anomalien zu überprüfen. Bewahren Sie die Logdateien für mindestens 6 Monate auf und schliessen Sie diese in Ihren Backup-Prozess ein. Die Analyse der Logfiles setzt umfangreiche Kenntnisse voraus, weshalb die Auslagerung an einen IT-Dienstleister sinnvoll sein könnte.

3

## Regelmässige Datensicherung

Definieren Sie einen Prozess, der die regelmässige Datensicherung regelt und halten Sie diesen konsequent ein. Sie können die Datensicherung und weitere technische Massnahmen auch an eine spezialisierte IT-Dienstleistungsfirma auslagern. Überprüfen Sie die Datensicherung regelmässig auf ihre Funktionsfähigkeit. Bewahren Sie die Backups an einem sicheren Ort auf (offline). Stellen Sie sicher, Vorgängerversionen der Backups über einen bestimmten Zeitraum aufzubewahren. Üben Sie von Zeit zu Zeit das Einspielen von Backups, so dass Sie mit dem Prozess vertraut sind, wenn Sie einmal darauf angewiesen sein sollten.

4

5

## «Least privilege» Prinzip

Die wenigsten Mitarbeitenden benötigen weitreichende Administratorenrechte. Erteilen Sie den Mitarbeitenden nur so viele Rechte, wie für die Erledigung ihrer Arbeit zwingend notwendig sind. Insbesondere sollten Sie die Rechte für die Installation jeglicher Software unterbinden.

6

## Firmenhandy mit Daten

Sind die Firmenhandys mit einem Passwort versehen damit die Daten nicht ausgelesen werden können?

7

## Netzwerksegmentierung

Spezifische Server oder Computer sollten in einem separaten Netzwerk stehen und von den anderen Computern in Ihrem Netzwerk nicht erreichbar sein. Denken Sie auch daran, dass sich die Malware auch über Netzwerk-Shares weiterverbreiten kann.

## Spam-Filter

8

Es gibt eine Vielzahl von Möglichkeiten, Spam-E-Mails zu blockieren. Falls Ihr Unternehmen beispielsweise nur in der Schweiz tätig ist, wäre es eine Option, E-Mails aus bestimmten Ländern (welche bekannt sind für ein hohes Spamaufkommen) abzuweisen. Potenziell schädliche E-Mail-Anhänge sollten bereits auf Ihrem E-Mail-Gateway bzw. Spam-Filter blockiert bzw. gefiltert werden.

## Makros

9

Makros sind eigentlich dafür gedacht, Office-Dokumente zu automatisieren. Leider verwenden immer mehr Angreifer Makros, um ihre Schadsoftware zu verteilen. Sämtliche E-Mail-Anhänge, die Makros enthalten (z.B. Word, Excel oder PowerPoint Anhänge mit Makros), sollten blockiert werden.

10

## Firewall

Verwenden Sie auf jedem Computer eine Firewall. Schützen Sie zudem Ihr Unternehmensnetzwerk gegenüber dem Internet mit einer zusätzlichen Firewall. Die Firewall sollte standardmässig sämtlichen eingehenden und ausgehenden Datenverkehr unterbinden, ausser demjenigen, welcher explizit (durch eine Firewall-Regel) zugelassen wird. Werten Sie die Logs des Proxys regelmässig aus.

11

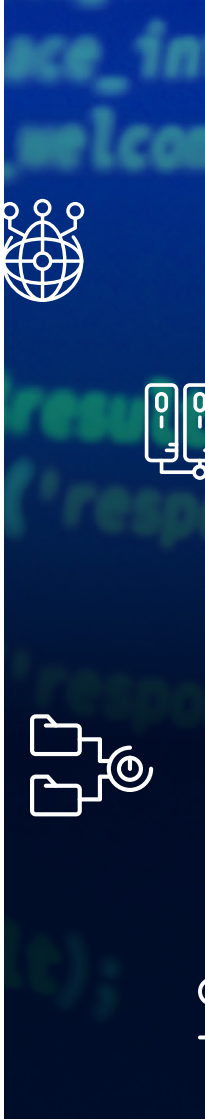
## Cloud-Dienste

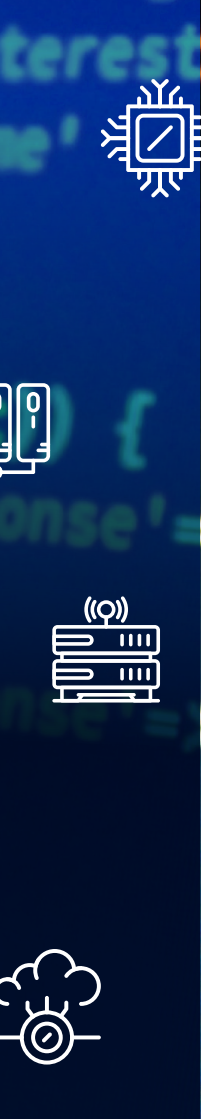
Cloud-Dienste haben u.a. den Vorteil, dass Sie keine teure IT-Infrastruktur im Hause betreiben müssen. Seien Sie aber vorsichtig bei der Verwendung von Cloud-Diensten.
Vertrauen Sie Ihre Daten und Dienste nur seriösen Anbietern auf dem Markt an. Erkundigen Sie sich beim Anbieter, wer Zugriff auf die Daten hat und wie die Datensicherung geregelt ist.

12

## Verschlüsselung

Verschlüsseln Sie wichtige Daten, insbesondere bei der Nutzung von Clouddiensten und auf mobilen Geräten.





## Content Management Systeme (CMS)

Falls Ihr Unternehmen über einen Webauftritt verfügt, stellen Sie sicher, dass das eingesetzte Content Management System (CMS) stets auf dem aktuellsten Stand ist. Ist Ihr Unternehmen stark vom Internetauftritt abhängig (z.B. Onlineshop), dann machen Sie sich auch Gedanken darüber, wie Sie einem allfälligen gezielten DDoS-Angriff begegnen können.

13

## Externer Zugriff auf Dateien oder Dienste

Ist der Zugriff von extern auf Ihre IT-Umgebung möglich? Ist dieser direkt möglich oder nur mit VPN? Gibt es eine Zwei-Faktor-Authentifizierung neben dem gewöhnlichen Passwort?

14

## Empfehlungen auf organisatorischer Ebene

Cybersicherheit ist vielschichtig. Neben grundlegenden technischen Massnahmen erhöhen zusätzliche organisatorische Massnahmen die IT-Sicherheit in Ihrer Unternehmung. Welche Massnahmen können dagegen ergriffen werden? Mit welchen finanziellen Folgen ist zu rechnen? Die Risiken im Bereich Informationssicherheit müssen Bestandteil des Risikomanagements der übergeordneten Governance und des Kontinuitätsmanagements sein. Die anfallenden Arbeiten müssen auch erledigt werden können, wenn die gesamte IT oder ein Teil davon vorübergehend nicht funktioniert. Dies muss nicht unbedingt die Folge eines Cyber-Angriffs sein. Auch Stromausfälle, Naturereignisse und weitere Szenarien können einen vollständigen oder teilweisen Ausfall Ihrer IT provozieren. Definieren Sie frühzeitig mögliche Alternativen und/oder Rückfallebenen für die jeweiligen Systeme.

1

### Physische Sicherheit

Es ist an allen Standorten definiert, wer Zugriff zum Serverraum hat. Die Server/Firewall/NAS/Switches sind abgeschlossen und nur autorisierte Personen haben darauf Zugriff.

2

### Verantwortlichkeiten bezüglich IT, insbesondere der IT-Sicherheit, sind geregelt.

Die Mitarbeitenden müssen wissen, an wen sie sich wenden sollen, wenn sie Fragen zur IT-Sicherheit haben (z.B. bei Erhalt einer verdächtigen E-Mail) oder wer bei einem IT-Sicherheitsvorfall zu informieren ist. Erarbeiten Sie frühzeitig einen Plan zur Bewältigung von Sicherheitsvorfällen. Üben Sie dessen Umsetzung regelmässig und passen Sie den Plan aufgrund der Erkenntnisse aus diesen Übungen an. Verantwortlichkeiten sollten zudem auch schriftlich festgehalten werden.

## Regeln Sie die Zuständigkeiten bezüglich IT-Sicherheit zwischen Ihrem Unternehmen und Ihrem IT-Dienstleister klar.

3

Wenn Sie technische Massnahmen wie Backup, Virenschutz, Logfiles usw. an einen IT-Dienstleister auslagern, dann überprüfen Sie regelmässig, ob diese Massnahmen korrekt durchgeführt werden, falls nötig durch einen (spezialisierten) Dritt-Dienstleister. Legen Sie im Vertrag auch fest, was eine Vernachlässigung der IT-Sicherheit für Konsequenzen hat (Haftung im Schadenfall). Achten Sie darauf, dass der Vertrag eindeutig formuliert ist und keine Missverständnisse bestehen. Wenn z.B. aufgrund eines Missverständnisses keine Datensicherungen erstellt werden, kann das verheerende Folgen haben.

## Regelmässige Schulung der Mitarbeitenden im Umgang mit der IT-Infrastruktur hinsichtlich der IT-Sicherheit

4

Der Sensibilisierung aller Mitarbeitenden im Umgang mit der IT-Infrastruktur kommt zentrale Bedeutung zu. Schulen Sie Ihr Personal regelmässig im Umgang mit dem Internet und den damit verbundenen Gefahren. Hier ist z.B auch den Mitarbeitern mitzuteilen, wer Ihre externen IT-Partner sind. Es gibt Fälle, wo sich böswillige Angreifer als IT-Dienstleister ausgeben, um so an Daten zu kommen.

## Kenntnis der aktuellen Bedrohungslage

5

Halten Sie sich auf dem Laufenden betreffend neuen Bedrohungen der Informationssicherheit und geeigneter Massnahmen, um diese zu bewältigen.

6

## Umgang mit sensiblen Daten

Erlassen Sie verbindliche Regeln zur Klassifizierung von Daten und setzen Sie diese Regeln konsequent durch. Legen Sie einen Prozess für den Umgang mit sensiblen Daten fest. Diese sollten auf speziell gesicherten Systemen, wenn möglich vom Internet getrennt, aufbewahrt werden. Sollen solche Informationen mit Dritten geteilt werden, sind diese Daten ausschliesslich verschlüsselt zu übermitteln.

7

## Verfügbare Firmeninformationen auf dem Internet

Oft benutzen Betrüger Informationen, die sie im Internet über eine Firma finden (zu Mitarbeitenden, Firmenstruktur, Geschäftspartnern etc.), um ihre Angriffe vorzubereiten. Es empfiehlt sich deshalb, die publizierten Informationen (auf der Firmenwebseite, auf Social Media usw.) und Informationen, welche dem Angreifer bei seiner Tat, beispielsweise bei einem Social Engineering Angriff, helfen könnten, auf das nötige Mass zu reduzieren. Dabei muss eine Abwägung des Nutzens und des Risikos der Publikation von solchen Informationen erfolgen.

8

## Sicherheit von der Beschaffung bis zur Entsorgung

Sicherheitsüberlegungen sollten fix in den Beschaffungsprozess eingebunden werden. Dabei sind nicht nur die Anforderungen bei Inbetriebnahme, sondern über den gesamten Lebenszyklus eines Systems inklusive Wartung und Ausserbetriebsetzung zu berücksichtigen. Informieren Sie sich insbesondere vor dem Kauf, wie z.B. Sicherheitsupdates zur Verfügung gestellt werden. Werden diese automatisch installiert? Wie erfahren Sie, das neue Updates vorhanden sind?

## Passwort-Policy

9

Definieren Sie verbindliche Passwortregeln und setzen Sie diese konsequent durch (z.B.: mind. 10 Zeichen mit Buchstaben, Zahlen und Sonderzeichen oder Prüfung der Passworthashes gegen bekannte Datenlecks). Setzen Sie, wo immer möglich, auf eine Zwei-Faktor-Authentisierung. Vermeiden Sie unbedingt die Mehrfachverwendung von Passwörtern. Stattdessen benutzen Sie einen Passwort-Manager und generieren für jede Anwendung ein neues Passwort.

## Einschränkungen bei der E-Banking-Applikation

10

Unter Umständen lassen sich nicht benötigte Funktionen in Ihrer E-Banking Applikation abschalten oder einschränken. Sprechen Sie mit Ihrer Bank über entsprechende Möglichkeiten, zum Beispiel über allfällige Länderbeschränkungen.

## Kollektiv-Unterschrift beim E-Banking

11

Hierbei wird eine Zahlung unter Berücksichtigung des Vier-Augen-Prinzips über einen zweiten E-Banking-Vertrag freigegeben. Sprechen Sie mit Ihrer Bank über entsprechende Möglichkeiten. Sämtliche Prozesse, welche den Zahlungsverkehr betreffen, sollten firmenintern klar geregelt sein und von den Mitarbeitenden in allen Fällen eingehalten werden.

**Haben Sie noch Fragen oder dürfen wir Sie bei Ihrer IT-Security unterstützen? Melden Sie sich ganz unverbindlich bei uns.**

**Ihre direkten Ansprechpartner:**


**Marco Lehmann**

Security Engineer
BSc FHO in Elektrotechnik

marco.lehmann@lehmann.ch
071 388 24 80



**Ralf Zeller**

Bereichsleiter Informatik
& Telekommunikation

ralf.zeller@lehmann.ch
071 388 24 79