Cyber Security-Check.
Empfehlungen und Tipps – ausführlicher Bericht.

Sie können viele Angriffe verhindern, wenn Sie sich der Cyber-Risiken in der täglichen Arbeit und privat bewusst sind. Setzen Sie sich deshalb gezielt mit dem Thema auseinander. Der Security-Check gibt Ihnen einen Überblick wie es um die Sicherheitsmassnahmen in Ihrer Organisation steht. Der Security-Check stellt eine einfache, erste Hilfestellung zum Thema dar, kann jedoch eine systematische Analyse und Massnahmendefinition/-implementierung nicht ersetzen.

A) Organisation

1. Haben Sie eine interne oder externe Person bestimmt, die für die IT-Sicherheit Ihres Unternehmens verantwortlich ist?

Sind Aufgaben, Kompetenzen und Verantwortlichkeiten für IT-Sicherheit nicht geregelt, ist dies ein Anzeichen dafür, dass dem Thema Cyber-Security nicht die nötige Bedeutung beigemessen wird. Regeln Sie Verantwortlichkeiten/Zuständigkeiten (Aufgaben) für die IT-Sicherheit in Ihrer Organisation klar und leiten Sie allenfalls Massnahmen ab. Eine klare Zuteilung erhöht in der Regel die Qualität und Wichtigkeit des Sicherheitsthemas.

Die Mitarbeitenden müssen zudem wissen, an wen sie sich wenden sollen, wenn sie Fragen zur IT-Sicherheit haben (z.B. bei Erhalt eines verdächtigen E-Mails) oder wer bei einem IT-Sicherheitsvorfall zu informieren ist.

«Nutzen Sie Empfehlungen, um sich dort zu verbessern, wo Sie noch keine oder nur ungenügende Massnahmen getroffen haben.»

Die IT-Abteilung ist jedoch nie als alleiniger Risikoträger zu definieren. Die Verantwortung für das Risikomanage-ment, die Klassifikation und Einstufung der Informationen, sowie ein allenfalls abgestufter Aufwand an zur Verfügung gestellten Sicherungsmassnahmen sind Kernaufgaben der Geschäftsleitung. Delegierte Aufgaben an die IT-Verantwortliche Person sollen schriftlich festgehalten werden (Aufgaben- und Pflichtenheft). Zudem soll die Ge-schäftsleitung regelmässig kontrollieren, ob die Aufgaben erfüllt werden.

Der Verein ISSS (Information Security Society Switzerland) zeigt in einem ihrer Paper «Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU)» wie solche Richtlinien aussehen könnten:

- Sichern Sie die Daten auf Servern, Arbeitsstationen, Notebooks, Laptops und anderen mobilen Geräten regelmässig.
- Halten Sie Betriebssysteme, Antivirus-Programme, Firewalls und sonstige Software aktuell.
- Ändern Sie werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen sofort.
- Führen Sie eine Liste mit allen im Unternehmen vorhandenen Computern, mit den installierten Programmen sowie den ausgeführten Software-Aktualisierungen.
- Legen Sie die Zugriffsrechte fest: Welche Programme dürfen Mitarbeitende ausführen? Auf welche Daten haben Mitarbeitende Zugriff?
- Führen Sie eine Liste mit allen Personen, welche von aussen auf das Firmennetzwerk zugreifen, eventuell mit genauer Dauer der Berechtigung. Stellen Sie sicher, dass auch deren Schutzprogramme aktuell sind.
- Stellen Sie sicher, dass Datenschutz-Bestimmungen eingehalten werden, z.B. durch aktuelle Schutzprogramme und starke Passwörter.
- Kontrollieren Sie regelmässig, ob die Benutzerrichtlinien eingehalten werden.

Und auch wenn Sie technische Massnahmen wie Back-up, Virenschutz, Firewalls, Logfiles usw. an einen externen IT-Dienstleister auslagern, 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 Schadensfall). 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.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs & Information Security Society Switzerland ISSS (2008 und 2016): Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU)

2. Haben Sie und Ihre Mitarbeitenden je nach Funktion und Aufgabe unterschiedliche Berechtigungsstufen in den IT-Systemen (inkl. Administratorenrechte)?

Unklare Zugangs- und Administratorenrechte stellen ein erhebliches Sicherheitsrisiko dar, das leicht vermeidbar ist. Implementieren Sie ein Berechtigungsmanagement, dabei kann folgendes Prinzip verfolgt werden:
«Least privilege»: Die wenigsten Mitarbeitenden benötigen weitreichende Administratorenrechte. Erteilen Sie dem Mitarbeitenden nur so viele Rechte, wie für die Erledigung seiner Arbeit zwingend notwendig sind. Insbesondere sollten Sie die Rechte für die Installation jeglicher Software unterbinden.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Sie können dabei wie folgt vorgehen:

- Analysieren, wer respektive welche Funktion welche Zugriffe auf die Systeme benötigt
- Erstellen entsprechender Rollenprofile
- Implementieren und managen der jeweiligen Rollen
- Wer kann Sie bei diesem Thema supporten?
  (beispielhafte Aufzählung):
  – Ihr IT-Verantwortlicher
  – Ein anderer, externer IT-(Security)-Spezialist

Weitere Tipps zum Berechtigungsmanagement im Bereich Zahlungsverkehr:

Einschränkungen bei der E-Banking-Applikation: 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.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Sehen Sie dazu auch «eBanking – aber sicher!»

Kollektiv-Unterschrift beim E-Banking: 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 Mit-arbeitenden in allen Fällen eingehalten werden.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Sicherheit bei Zahlungen:

Setzen Sie für alle digital übermittelten Zahlungsaufträge (Offline-Zahlungssoftware, E-Banking) einen dedizierten Computer ein, mit dem Sie nicht im Internet surfen oder E-Mails empfangen.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Wer kann Sie bei diesem Thema supporten?

(beispielhafte Aufzählung):

- Ihr IT-Verantwortlicher oder
  ein anderer, externer IT-(Security)-Spezialist
  Ihre Bank

3. Arbeiten Sie in Ihrem Unternehmen mit Passwort-Richtlinien und werden diese auch angewandt?

Das Passwort ist einer der grössten Sicherheitsfaktoren in der IT-Sicherheit. Schwache Passwörter können von leistungsstarken Rechnern in kürzester Zeit enthüllt und für den unautorisierten Zugriff auf die IT- und OT-Systeme genutzt werden. Definieren Sie deshalb verbindliche Passwortregeln und setzen Sie diese konsequent durch (z.B. mind. 12 Zeichen mit Buchstaben, Zahlen und Sonderzeichen/werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IT-Verantwortlichen sofort geändert werden/regelmässige Änderung der Passwörter).

Passwörter alleine liefern jedoch keinen hinreichenden Schutz vor unbefugten Zugriffen. Setzen Sie, wo immer möglich, auf eine Zwei- bzw. Multi-Faktor-Authentisierung (Einmal Passwort, SMS-Token usw.). Dahinter steht das Prinzip, mehrere Authentifizierungstechniken miteinander zu verknüpfen.

Vermeiden Sie zudem die Mehrfachverwendung von Passwörtern. Stattdessen können Sie einen Passwort-Manager nutzen, der für jede Anwendung ein neues Passwort generiert und zur Übersicht für den jeweiligen Benutzer auch speichert.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Sehen Sie dazu auch die Empfehlungen von MELANI.
Testen Sie hier die Stärke Ihrer Passwörter.

Wer kann Sie bei diesem Thema supporten:

(beispielhafte Aufzählung)

- Ihr IT-Verantwortlicher
- externer IT-(Security)-Spezialist

4. Sensibilisieren Sie Ihre Mitarbeitenden zum Thema Cyber-Risiken und führen regelmässig Sicherheitstrainings in diesem Bereich durch?

Diverse Schadenfallanalysen zeigen, dass der Mensch oft das Einfallstor für Cyberkriminelle darstellt. Sind die Mitarbeitenden wie auch die Geschäftsleitung eines Unternehmens nicht im sicheren Umgang mit IT-Systemen geschult, sind viele der bekannten technischen Massnahmen wie

Firewall oder Virenscanner nutzlos. Daher hilft es, das Bewusstsein gegenüber Cyber-Risiken zu steigern.

Der Sensibilisierung aller Mitarbeitenden im Umgang mit der IT-Infrastruktur kommt eine zentrale Bedeutung zu. Schulen Sie Ihr Personal regelmässig im Umgang mit dem Internet und den damit verbundenen Gefahren z.B. in kurzen Workshops oder Online-Seminaren.
Definieren Sie zudem Verhaltensregeln und führen Sie regelmässig simulierte Cyber-Attacken durch, um die Sensibilisierung der Mitarbeitenden zu prüfen und um zu sehen, ob intern richtig reagiert wird. Dies kann z.B. ein gefaktes Phishing-Mail sein, in dem Benutzername und Passwort angefragt wird oder ein Mail mit einem Link auf eine fiktive Seite, bei dem kontrolliert werden kann, wie viele Mitarbei-tende auf diesen Link klicken.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Entsprechende Verhaltensregeln im Umgang mit dem Internet finden Sie auf der Homepage von MELANI.
MELANI publiziert hier zudem die aktuellsten Cyber-Gefahren (u.a. Social Engineering).

Wer kann Sie bei diesem Thema supporten?
(beispielhafte Aufzählung):

- Ihr IT-Verantwortlicher
- Ein anderer, externer IT-(Security)-Spezialist

B) Datenschutz

5. Verschlüsseln Sie im Unternehmen besonders schützenswerte Daten unter Berücksichtigung der gängigen Datenschutzgesetze?
und
6. Verwenden Sie im Unternehmen bei der Datenübermittlung gesicherte und verschlüsselte Kommunikationsverbindungen im Internet? (z.B. VPN)
Vertrauliche Informationen und geschäfts- oder personenbezogene Daten können schnell in falsche Hände geraten. Erlassen Sie deshalb 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.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Sehen Sie dazu auch die Beschreibung zum Datenschutz des Bundes.
Am 25. Mai 2018 ist zudem die neuen Datenschutz-Grundverordnung (DSGVO) der EU in Kraft getreten, die teilweise auch für Schweizer Unternehmen gilt. Prüfen Sie, ob Sie betroffen sind und initiieren Sie entsprechende Massnahmen, da bei Verstoss hohe Geldstrafen drohen.

ITC Switzerland (2018): CYBERSECURITY-SCHNELLTEST FÜR KMU.
URL: https://ictswitzerland.ch/media/dateien/Cyber_Security/Minimalstandards/Hinweise_Cybersecurity_Minimalschutz.pdf (abgerufen am 16.12.18)

Folgende Homepages können Ihnen bei Thema DSGVO helfen:

- MELANI: Datenschutz: Neue EU-Verordnung
- ECONOMIE SUISSE: Datenschutz «Online-Check» sowie Faktenblatt EU Datenschutz

Wichtiger Hinweis zum Thema Cloud-Dienste:
Cloud-Dienste haben u.a. den Vorteil, dass Sie keine teure IT-Infrastruktur betreiben müssen. Seien Sie aber vorsichtig bei der Verwendung von Cloud-Diensten. Sensible Daten sollten nur selektiv und wenn, dann zumindest immer verschlüsselt in der Cloud abgelegt werden. Ausserdem sollten Sie sich vor Abschluss eines Vertrags beim Anbieter erkundigen, wer Zugriff auf die Daten hat, wie die Datensicherung geregelt ist usw.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Wer kann Sie bei diesem Thema supporten?
(beispielhafte Aufzählung):

- Ihr IT-Verantwortlicher
- Ein anderer, externer IT-(Security)-Spezialist
- Juristen mit Spezialgebiet Datenschutz

7. Ist in Ihrem Unternehmen der physische Zugang zur Rechner-, Server- und Netzwerkinfrastruktur vor dem Zugriff von Dritten zweckmässig geschützt?
Die IT-Sicherheit eines Unternehmens wird auch über eine gute Absicherung der Hardware und des Zugangs zu den Firmenräumen gewährleistet. Dieser Schutz wird in der digitalen Zeit aber leider häufig unterschätzt und vernachlässigt.

Folgende Massnahmen helfen, sich vor unerlaubtem physischen Zugang Dritter zu schützen:
- Kundenempfang instituieren
- Unkontrollierte Zugänge zum Gebäude bzw. zu Firmenräumen abschliessen
- Regel für Mitarbeitende definieren: z.B. beim Verlassen des Arbeitsplatzes den Bildschirm sperren
- Kleinere Rechnergehäuse abschliessen

- Bei Server- und Netzwerkinfrastrukturräumen Zutrittskontrollsysteme installieren und Zutrittsrecht auf ein Minimum von Personen beschränken (für die Zutrittskontrolle können unter anderem elektronische Zutrittscodes, Magnetkarten oder biometrische Daten verwendet werden)
- Überwachungs- und Alarmanlagen installieren

8. Kennen und erfüllen Sie die PCI-DSS Standards?

Der Missbrauch von gestohlenen Kreditkartendaten ist ein Thema, welches in regelmässigen Abständen durch die Presse geht. Wenn es bei der Zahlungsabwicklung mit Zahlungskarten zu Datenpannen kommt, kann die Situation schnell kritisch werden. Ihre Kunden werden verunsichert und verlieren das Vertrauen in Ihre Fähigkeit, die persönlichen Daten Ihrer Kunden zu schützen. Im schlimmsten Fall wenden sich die Kunden von Ihnen ab und wechseln den Händler. Das führt wiederum zu finanziellen Verlusten bei Ihrem Unternehmen.

Um das Vertrauen der Verbraucher in die Bezahlform Kreditkarte zu stärken, haben die Kreditkartenorganisationen (VISA und Mastercard) gemeinsame Sicherheitsstandards beim Umgang mit Karten- und Transaktionsdaten geschaffen. Die Payment Card Industry Data Security Standards, kurz PCI DSS, umfassen eine Reihe von verbindlichen Regeln für alle Parteien, die Kartendaten verarbeiten, speichern oder weiterleiten. Diese Standards sind für sämtliche Kartenakzeptanzstellen – damit auch für einen Webshop – verbindlich. Alle an diesem Prozess beteiligten Firmen (Payment Service Provider wie Internet-Händler mit eigenem Payment-Gateway) müssen ihre Systeme den Sicherheitsstandards anpassen und sich durch speziell lizenzierte Institutionen zertifizieren lassen.

PCI Security Standards Council (2016): Sichere Kartenzahlung für Kleinhändler: Leitfaden für sichere Zahlungsverfahren., ibi research an der Univer-sität Regensburg (2009): E-Commerce-Special zum Thema PCI veröffentlicht. & Datatrans (2018): PCI-Zertifizierung (Zahlungssicherheit),URL: https://www.datatrans.ch/pci (abgerufen am 14.12.18)

Im Folgenden finden Sie eine übergeordnete Übersicht über die zwölf PCI-DSS-Anforderungen:

1. Installation und Wartung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten
2. Keine vom Anbieter gelieferten Standardeinstellungen für Systemkennwörter und andere Sicherheitsparameter verwenden
3. Schutz gespeicherter Karteninhaberdaten
4. Verschlüsselung bei der Übertragung von Karteninhaberdaten über offene, öffentliche Netze
5. Schutz sämtlicher Systeme vor Malware und regelmässige Aktualisierung von Antivirensoftware und Program-men
6. Entwicklung und Wartung sicherer Systeme und Anwendungen
7. Beschränkung des Zugriffs auf Karteninhaberdaten je nach Geschäftsinformationsbedarf
8. Identifizierung und Authentifizierung des Zugriffs auf Systemkomponenten
9. Physischen Zugriff auf Karteninhaberdaten beschränken
10. Verfolgung und Überwachung des gesamten Zugriffs auf Netzwerkressourcen und Karteninhaberdaten
11. Regelmässiges Testen der Sicherheitssysteme und -prozesse Pflege einer Informationssicherheitsrichtlinie
12. Pflegen Sie eine Informationssicherheitsrichtlinie für das gesamte Personal.

Viele kleinere Shopbetreiber stellen sich die Frage, ob sie sich mit der PCI-Zertifizierung überhaupt auseinandersetzen müssen oder ob dies nicht der Zahlungsanbieter übernimmt. Ein Online-Händler kann jedoch die Pflicht zur PCI-Zertifizierung nur dann umgehen, wenn er an keiner Stelle im eigenen System Daten der Karteninhaber oder Peripherie-Daten, wie der dreistellige Sicherheitscode der Kreditkarte, verarbeitet oder speichert.

Das Verarbeiten und Speichern von Karteninhaberdaten ohne PCI-Zertifizierung kann weitreichende Folgen nach sich ziehen, von Strafzahlungen seitens Bank, die für den Online-Händler die Kreditkarten abrechnet, bis zur Entnahme der Zulassung von Kreditkartenzahlungen.
Die betreffenden Online-Händler werden zudem nie wieder Kartenzahlung akzeptieren können, da voraussichtlich kein anderer Acquirer, also die Bank, die für den Online-Händler die Kreditkarten abrechnet, einen Akzeptanzvertrag unterschreiben wird.

Bosk, Holger (2014): Was ist eine PCI-Zertifizierung? URL: https://www.novalnet.de/magazin/was-ist-eine-pci-zertifizierung (abgerufen am 20.11.2018)

Wer kann Sie bei diesem Thema supporten?

(beispielhafte Aufzählung):

- Ihr Online-Webshop Entwickler
- Acquirer: Aduno, Six, PostFinance, etc.
- Payment Service Provider (PSP): Datatrans, Aduno, Six Payment Services, Innocard, CCV, PostFinance, etc.

C) Datensicherung

9. Sichern Sie im Unternehmen Ihre Daten täglich (Backup)?

und

10. Überprüfen Sie die Backup-Daten regelmässig auf die Qualität?

und

11. Bewahren Sie das Backup sicher auf?

und

12. Wird das Backup physisch getrennt (offline) abgelegt?

Es kann nie ausgeschlossen werden, dass Daten durch Fehlmanipulation, wegen technischer Defekte oder durch Malware teilweise zerstört werden oder gar ganz verloren gehen. Dieser Datenverlust kann für ein Unternehmen verheerende Folgen haben. Ein gutes Backup Konzept sorgt da vor und ist deshalb dringend zu empfehlen.

- Definieren Sie einen Prozess, der die regelmässige Datensicherung regelt (am besten automatisiert) und halten Sie diesen konsequent ein. Sie können die Datensicherung und weitere technische Massnahmen auch an eine spezialisierte IT-Dienstleistungsfirma auslagern.
- Diese Regel und die Zuständigkeit sollen schriftlich festgelegt werden.
- Erstellen Sie mindestens ein Back-up pro Tag. Ein tägliches Backup sorgt für die gesetzeskonforme Archivierung Ihrer Daten gemäss Obligationenrecht und der «Verordnung über die Führung und Aufbewahrung der Geschäftsbücher» (GeBüV)
- Überprüfen Sie die Datensicherung regelmässig auf ihre Funktionsfähigkeit.
- Bewahren Sie Backups an einem sicheren Ort auf (optimalerweise offline).
- Stellen Sie sicher, Vorgängerversionen des Backups über einen bestimmten Zeitraum aufzubewahren. (mind. 1 Woche – Generationenprinzip))
- Üben Sie von Zeit zu Zeit das Einspielen von Backups (Restore), so dass Sie mit dem Prozess vertraut sind, wenn Sie einmal darauf angewiesen sein sollten.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs) & Information Security Society Switzerland ISSS (2008 und 2016): Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU)

Sie können sich für die Zusammenstellung der Regel für den Backup Prozess folgende Fragen stellen:

- Wie oft wird gesichert? – Wie viele Backups erstellt werden. Einmal täglich, mehrmals täglich, etc.
- Wie viele Backups werden angelegt? – Mindestens eine Spiegelung des Backups sollte vorhanden sein.
- Wohin wird gesichert? – Die Backups sollen örtlich getrennt sein und mindestens ein Backup dezentral (ausser Haus) aufbewahrt sein.
- Was wird gesichert? – Klare Definition, welche Daten und welche Server gesichert werden.
- Wie wird gesichert? – Mit welchem Backup Programm und auf welches Medium die Sicherungen gemacht werden.
- Mehrere Generationen? – Mittels Generationenprinzip auch auf Daten von vorgestern und von letztem Jahr zugreifen können.
- Funktioniert das Backup? – Regelmässige Überprüfung, ob die Daten und Systeme gesichert werden.
- Wiederherstellbar? – Mittels Simulation die Wiederherstellung von Daten und Systemen periodisch testen.
- Wie umfangreich? – Klare Strategie für: Voll Backups, inkrementelle Backups, differentielle Backups
- Wer ist zuständig? – Festlegen, wer für die Durchführung und wer für die Kontrolle verantwortlich ist.
- Wer ist berechtigt? – Definieren, welche Personen, externe Dienstleister auf die Sicherungen zugreifen dürfen.
- Wie sicher? – Schutz der Backups vor Diebstahl und Missbrauch. Zusätzliche Verschlüsselung prüfen.

Beispielregeln gemäss URL: https://boegli-ict.ch/local-it/Back-up-loesungen/ (abgerufen am 20.11.2018)

Wer kann Sie bei diesem Thema supporten?
(beispielhafte Aufzählung):

- Ihr IT-Verantwortlicher
- Ein anderer, externer IT-(Security)-Spezialist

D) Technische Schutzmassnahmen

13. Haben Sie im Unternehmen aktuelle und branchenübliche technische Schutzmassnahmen installiert?

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.

Die wichtigsten technischen Schutzmassnahmen sind nachstehend kurz beschrieben:

Virenschutz
Stellen Sie sicher, dass auf jedem mit dem Internet verbunden Gerät ein Virenschutz installiert ist. Sorgen Sie auch dafür, dass dieser sich regelmässig aktualisiert sowie regelmässig einen vollständigen Systemscan durchführt (z.B. wöchentlich oder monatlich). bei kleinen Unternehmen ist übrigens ein kostenloser Virenschutz in der Regel ausreichend. Die Erkennungsrate von Schadsoftware ist bei kostenlosen Programmen nicht schlechter als bei kostenpflichtigen Lösungen. Letztere bieten jedoch meistens Zusatzfunktionen wie z.B. einen Anti-Spam-Filter oder einen Werbeblocker.

Spam-Filter
Es gibt eine Vielzahl 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 z.B. bekannt für ein hohes Spam-aufkommen sind) abzuweisen. Potenziell schädliche E-Mail-Anhänge sollten bereits auf Ihrem E-Mail-Gateway bzw. Spam-Filter blockiert bzw. gefiltert werden. Gefährliche E-Mail-Anhänge verwenden verschiedene Dateiendungen, vor welchen u.a. MELANI auf ihrer Webseite warnt.

Solche E-Mail-Anhänge müssen auch dann blockiert werden, wenn diese in Archiv-Dateien wie beispielsweise ZIP, RAR, ISO oder aber auch in geschützten Archiv-Dateien (z.B. in einem passwortgeschützten ZIP) an Empfänger in Ihrem Unternehmen versendet werden.

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. Lassen Sie proxyfähige Protokolle wie HTTP/HTTPS usw. über einen Proxy laufen. Werten Sie die Logs des Proxys regelmässig aus.

Remote-Zugänge
Mitarbeitende, die oft unterwegs sind, sind darauf angewiesen, von ausserhalb der Firma auf das Firmennetz zugreifen zu können. Falls Sie einen Remote-Zugang verwenden (z.B. RAS, VPN), stellen Sie sicher, dass dieser stark authentisiert ist, z.B. mit einem zweiten Faktor (One-Time-Password, SMS-Token usw.).

W-LAN
Schränken Sie den Zugriff auf Ihren Access Point so ein, dass lediglich Ihre Endgeräte mit ihm kommunizieren dürfen. Dies kann durch Erfassen der MAC-Adresse der Endgeräte erreicht werden.
Aktivieren Sie an Ihrer W-LAN-Hardware die WPA- oder WPA2-Verschlüsselung und wählen Sie dafür ein starkes, schwer zu ratendes Passwort.
Falls vertrauliche Daten über Ihr W-LAN übermittelt werden, empfiehlt sich der Einsatz von Protokollen, bei denen die Daten (zusätzlich) verschlüsselt übertragen werden (z. B. VPN, https, ssh, usw.).

Content Management Systeme (CMS)
Falls Ihr Unternehmen über einen Webauftritt verfügt, stellen Sie sicher, dass ein gegebenenfalls eingesetztes Content Management System (CMS) stets auf dem aktuellsten Stand ist. Verwenden Sie eine Web Application Firewall (WAF), um Ihre Webseite gegen Angriffe zu schützen. Eine Liste von weiteren Massnahmen zum Schutz von Content Management Systemen (CMS) finden Sie hier.

Ist Ihr Unternehmen stark vom Internetauftritt abhängig (z.B. Onlineshop), dann machen Sie sich auch Gedanken darüber, wie Sie einem allfälligen DoS-Angriff begegnen können.

Logdateien
sogenannte «Logfiles» sind bei der Nachbearbeitung eines IT-Vorfalles enorm wichtig. Stellen Sie sicher, dass kriti-sche Systeme wie Buchhaltungssoftware, Domain-Controller, Firewall oder E-Mail-Server solche Logdateien anlegen. Es ist empfehlenswert, die angefallen Logdateien regelmässig auf Anomalien hin zu überprüfen. Bewahren Sie 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.

Netzwerksegmentierung
Mindestens die Computer der Buchhaltung und der Personalabteilung (HR) sowie allfällige Maschinen-Steuerungen (Operational Technologie - OT) sollten jeweils in einem separaten Netzwerk stehen und von den anderen Compu-tern/Geräten in Ihrem Netzwerk nicht erreichbar sein. Denken Sie auch daran, dass sich Malware auch über Netzwerk-Shares weiterverbreiten kann.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Wer kann Sie bei diesem Thema supporten?

(beispielhafte Aufzählung):

- Ihr IT-Verantwortlicher
- Ein anderer, externer IT-(Security)-Spezialist

14. Verfügt Ihr Unternehmen über ein systematisches Patch- und Update-Management, das für eine zeitnahe Installation von Patches/Sicherheits-Updates bei allen mit dem Internet verbundenen Geräten und Systemen sorgt?
oder
15. Nutzen Sie die Möglichkeit der automatischen Softwareaktualisierung?
Falls vorherige mit Nein beantwortet wurde:
16. Wird bei Geräten und Systemen, deren Software nicht automatisch aktualisiert wird, diese regelmässig auf den neusten Stand gebracht (z.B. durch den Hersteller)?
Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. Angreifer können einfach durch bekannte Sicherheitslücken in das System eindringen. Daten können vernichtet und manipuliert werden oder Ihre Infrastruktur kann für kriminelle Zwecke missbraucht werden.

Stellen Sie sicher, dass sämtliche Geräte (Computer, Server, Drucker, Firewall, Router, Mobile Geräte, Maschinen-Steuerungen, etc.) in Ihrem Netzwerk auf dem neusten Stand sind und überprüfen Sie alle Software-Produkte regelmässig auf Sicherheitsupdates. Nutzen Sie wann immer möglich automatische Update-Funktionen. Patchen Sie auch Drittsoftware wie z.B. Adobe Reader, Adobe Flash, Java etc. ebenfalls regelmässig.

Legen Sie zudem systematisch fest, in welchem Turnus alle Geräte und Software diesbezüglich überprüft werden.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Spezieller Hinweis zu Maschinen-Steuerungen (OT, ICS, SCADA):

Das Patchmanagement bei Maschinen-Steuerungen ist teilweise heikel und kann (aus Gewährleistungsgründen) meist nur in Zusammenarbeit mit dem Lieferanten gemacht werden. Das heisst, dass in der Regel längere Zeitfenster vorhanden sind, während denen ein System angreifbar ist.

Das Risiko kann durch ein Whitelisting von ausführbaren Anwendungen reduziert werden. Bei fast jedem Angriff muss auf dem angegriffenen Gerät Software gestartet werden. Durch ein Whitelisting soll erreicht werden, dass nur noch zugelassene Programme ausgeführt werden können.

Melde- und Analysestelle Informationssicherung MELANI (2013): Massnahmen zum Schutz von Industriellen Kontrollsystemen (ICS)

Wer kann Sie bei diesem Thema supporten?

(beispielhafte Aufzählung):

- Ihr IT-Verantwortlicher
- Ein anderer, externer IT-(Security)-Spezialist
- Anbieter der eingesetzten Hardware/ Software

17. Haben Sie bei Servern und wichtigen zentralen Infrastrukturkomponenten einen Überspannungsschutz/USV (unterbrechungsfreie Stromversorgung) installiert?

Die zuverlässige Funktion elektronischer Systeme hängt von einer guten Stromversorgung ab. Viele Unternehmen schützen aber ihr Netzwerk nicht mit einer unterbrechungsfreien Stromversorgung (USV).

Viele Anwender sind der Meinung, dass man sich nur bei den seltenen totalen Stromausfällen über die Stromversorgung bei Computern und anderen elektronischen Systemen Sorgen machen muss. Die grösste Wirkung haben jedoch die Schwankungen und Störungen in der Netzspannung, die nicht wahrnehmbar sind, aber Leistung und Verhalten eines Systems beeinflussen können.

«45 Prozent aller nicht erklärbaren Computer-Probleme, wie beispielsweise Datenverlust, Netzwerkabsturz, mysteriöse Fehlermeldungen oder beschädigte Dateien, gehen nach neuesten Untersuchungen auf Probleme bei der Eingangsspannung zurück», sagen die USV-Experten der Karlsruher Powerware GmbH. Viele Anwender sind der Meinung, dass der Strom aus der Steckdose «sauber» ist, was aber nicht der Fall ist. Die Netzeingangsspannung kann beispielsweise eine bestimmte Zeit erheblich variieren. Hinzu kommen weitere Spannungsprobleme, wie Spannungseinbruch, Spanungsspitzen oder Kurzschluss im Netz oder Überspannungen.

Viele Faktoren können die Qualität der Spannung beeinflussen. So kann die Benutzung der Aufzüge in einem Gebäude oder sogar das Einschalten eines Fotokopierers zu Schwankungen in der Stromversorgung führen. Sensible elektronische Systeme, wie Computer, Hubs und Router, reagieren besonders empfindlich auf Spannungsschwankungen. Deshalb ist es sehr wichtig für ein Unternehmen, sich auch mit diesem Thema vertieft auseinander zu setzen und für zentrale Infrastrukturelemente wie Server oder Router Massnahmen gegen dieses Risiko zu ergreifen.

Spannungsschutz-Spezialisten können Sie beraten, welches System für den Schutz der Last geeignet ist und welche speziellen Massnahmen zu berücksichtigen sind.

Unbekannter Autor (2000): USV-Anlagen schützen vor Datenverlusten. Eine wichtige Komponente bei der IT-Strategie. URL: https://industrieanzeiger.industrie.de/allgemein/eine-wichtige-komponente-bei-der-it-strategie/(abgerufen am 16.12.2018)

E) Notfallbewältigung

18. Sind Sofortmassnahmen im Falle eines Cyber-Vorfalls definiert?

oder

19. Ist eine IT-Verantwortliche Person sowie eine Ansprechperson im Falle eines Cyber-Vorfalls (z.B. Fehlfunktion, Angriff o.ä.) definiert und jederzeit verfügbar (Stellvertretung)?

Bei einem Cyber-Vorfall müssen Sie schnell handeln können, um den Schaden zu begrenzen und die Kosten zu minimieren.

Beurteilen Sie die Abhängigkeit Ihrer Geschäftsprozesse von Ihrer Informatik. Analysieren und klassifizieren Sie die Risiken im Bereich der Informationensicherheit und legen Sie diese der Geschäftsleitung vor. Dabei sind insbesondere folgende Frage zu beantworten:

Welche Auswirkungen hat der Ausfall eines Systems oder die Nicht-Verfügbarkeit der Datenablage? Welche Massnahmen können dagegen ergriffen werden? Mit welchen finanziellen Folgen ist zu rechnen? usw.

Die wichtigsten Arbeiten müssen auch erledigt werden können, wenn die gesamte IT oder ein Teil davon vorübergehend nicht funktioniert. Das gleiche gilt für das OT-System (Maschinen). Dies muss nicht einmal unbedingt die Folge eines Cyber-Angriffs sein. Auch Stromausfälle, Naturereignisse und weitere Szenarien können einen vollständigen oder teilweisen Ausfall Ihrer IT oder OT provozieren. Legen Sie fest, wie sich Mitarbeitende im Notfall verhalten sollen und welche Aktionen auszulösen sind. Definieren Sie frühzeitig mögliche Alternativen und/oder Rückfallebenen für die jeweiligen Systeme. Bestimmen Sie Ansprechpersonen und stellen Sie deren Erreichbarkeit im Notfall sicher.

Melde- und Analysestelle Informationssicherung MELANI (2018): Merkblatt Informationssicherheit für KMUs

Wer kann Sie bei diesem Thema supporten?

(beispielhafte Aufzählung):

- Ihr IT-Verantwortlicher
- Ein anderer, externer IT-(Security)-Spezialist
- Grössere Telecom- und Internet-Provider
- Weitere kleinere Unternehmen, welche solche DoS Schutz-lösungen anbieten.

20. Besitzt ihr Unternehmen eine Abwehrstrategie gegen DoS-Attacken?

Ein DoS-Angriff kann jede Organisation treffen. Wenn eine Webseite (z.B. Reservierungsplattform oder Onlineshop) oder ein gesamter Server nicht erreichbar ist, kann dies für den Besitzer einen grossen Gewinnausfall aber auch einen Reputationsverlust bedeuten, insbesondere wenn der angegriffene Dienst kommerzieller Natur ist. Eine DoS-Attacke wird vielfach von einer Geldforderung begleitet. Der Erpresser verlangt Geld, damit er einen bereits gestarteten Angriff stoppt oder keinen startet. Die Angreifer hoffen, dass das Opfer bezahlt, um keine negativen Folgen eines solchen Angriffs zu erleiden.

Idealerweise setzen Sie sich mit der DoS-Problematik schon vorgängig auseinander, um eine gewisse DoS-Abwehrbereitschaft zu erreichen.

Folgende Punkte können ihnen dabei helfen:

- Sie kennen Ihre Infrastruktur und deren Schwächen. Welche Dienste sind so wichtig, dass deren Ausfall weitreichende Auswirkungen auf Ihre Organisation haben könnte. Versuchen Sie dabei auch an Basis Systeme zu denken, ohne die Ihre kritischen Geschäftsanwendungen nicht funktionieren.
- Sie kennen den «Normalzustand» Ihrer Netze und Systeme und erkennen Anomalien (IDS (Intrusion Detection Systeme), zentralisierte Logauswertung). Eine DoS-Attacke sollte ent-

deckt werden, bevor Ihre Kunden sie bemerken können.
- Überwachen Sie die Verfügbarkeit Ihrer Kundenanwendungen auch aus der Sicht Ihrer Kunden, das heisst vom Internet her.
- Ihre Systeme sind gehärtet (keine unnötigen Dienste, strikte Rechtevergabe, starke Authentisierung, usw.) und auf aktuellem Patch-Level. SYN-Cookies sind aktiviert etc.
- Eine vorgelagerte Firewall lässt nur benötige Protokolle zum System durch. Die Firewall verfügt über genügend Systemressourcen, um auch im Falle eines DoS funktionsfähig zu bleiben. Dabei ist ein grosses Augenmerk auf die Connection Table sowie auf eine gute Regelverwaltung zu legen, damit sie im Notfall zusätzlich viele Blockierungsregeln implementieren können.
- Prüfen Sie die Möglichkeiten eines GeoIP Blockings. Wenn Ihre Kunden vorwiegend aus der Schweiz und dem nahen Ausland stammen, können Sie ein Profil vordefinieren, welches IP Adressen aus diesem Raum entweder Priorität einräumt oder andere IP Adressen blockiert. Im Angriffsfall können Sie dieses Profil aktivieren und ge-winnen so sehr schnell an Handlungsoptionen und zusätzlichem Schutz.
- Eine Web-Application Firewall minimiert die Angriffsfläche auf webbasierte Dienste.
- Systeme, die potentiell Opfer einer DoS Attacke werden könnten (z.B. Webauftritt), sollten an einem anderen Internet-Uplink hängen als die übrigen Systeme der Organisation. Die betroffenen Systeme können so einfacher unter den Schutzschild eines DoS-Mitigation-Providers gestellt werden, ohne dabei die restlichen Systeme zu tangieren, die für das Tagesgeschäft nötig sind.
- Stellen Sie Ausweichlösungen bereit, z.B. eine statische Website mit minimalen Informationen, welche bei einem anderen Provider bereit steht und die Sie mit einer einfachen Änderung im DNS aktivieren können.
- Achten Sie generell darauf, eine gute Balance in den TTLs der DNS Server zu haben, so dass Sie genügend schnell eine Domänenauflösung umstellen können.
- Sie haben eine Strategie für den Fall einer DoS Attacke. Die zuständigen Personen kennen das Vorgehen sowie die internen und externen Kontakte (Service Provider, Polizeistellen etc.).
- Im Fall der Fälle können Sie auf interne oder vertraglich zugesicherte externe Ressourcen zugreifen (insbesondere Personal und Infrastruktur).
- Sie haben den Fall einer DoS Attacke mit Ihren internen Stellen und den externen Partnern besprochen und auch geübt. Jeder kennt seine Rolle und Ansprechpartner!

Falls es dann doch zu einem DoS kommen sollte, geht es primär darum, dem Angreifer zu signalisieren, dass er sein Ziel nicht erreicht. Halten Sie genügend lange durch, wird der Angreifer sich typischerweise von Ihnen abwenden.

1. Protokollieren Sie den Angriff (Netflows, Server-Logs, Mail-Verkehr mit den Erpressern usw.). Sie sind für eine spätere Analyse und allfällige Anzeige wichtig.

2. Stellen Sie sicher, dass Sie minimale Informationskanäle gegen aussen offen halten können, z.B. ein statischer Webauftritt, auf dem Sie Ihre Kunden informieren und Ihnen alternative Kontaktmöglichkeiten (z.B. Telefon, Fax, E-Mail) anbieten.

3. Analysieren Sie den Angriff und legen Sie eine Abwehrstrategie fest:

a) Ist der Ursprung der Attacke eine beschränkte Anzahl von IP-Adressen, dann genügt evtl. das Filtern dieser Adressen an Ihrem Router oder Firewall. Übersteigt das Datenvolumen die Ihnen zur Verfügung stehende Bandbreite, dann muss dies Ihr ISP erledigen.

b) Verschieben Sie ggf. Ihr angegriffenes System in ein anderes Subnetz (Bei rein IP-basierten Angriffen). Typischerweise suchen Sie hier eine Lösung in enger Zusammenarbeit mit Ihrem ISP und/oder einem spezialisierten DDoS-Mitigation-Provider.

c) Es handelt sich um eine Attacke, deren Source-IP-Adressen wahrscheinlich gefälscht sind: Dies ist typischerweise bei SYN-, UDP-, BGP- und SNMP-Flooding der Fall. Ein Filtern der IP-Adressen macht hier keinen Sinn und kann sogar legitime Benutzer aussperren. Typischerweise suchen Sie hier eine Lösung in Zusammenarbeit mit Ihrem ISP. Er kann diesen Verkehr umlenken und ausfiltern. Dazu sollten Sie aber vorher schon wissen, welche Protokolle bei Ihnen eingesetzt werden und welche schadlos ausgefiltert werden können. Öffentliche Auftritte beschränken sich in der Regel auf TCP-basierte Protokolle (HTTP, HTTPS, SMTP etc.) so dass stateless Protokolle wie UDP bedenkenlos gefiltert werden können (evt. Ausnahme: DNS).

d) Angriffe auf eine Applikation: Hier wird Ihre Applikation durch eine grosse Anzahl von (komplexen) Anfragen lahmgelegt. Die Attacken nutzen in der Regel TCP als Netzwerk-Protokoll. Die Absender Adresse ist also nur schwer fälschbar und kann daher nach diversen Kriterien gefiltert werden.

e) Attacken auf das SSL/TLS Protokoll: Mögliche Abhilfe ist das Terminieren der SSL-Verbindung bei einem Cloud-Dienst, der die gefilterte Verbindung danach an Ihre Systeme weiterreicht.

f) Falls sich der Grossteil der Kundschaft in bestimmten Ländern befindet, kann nach GEO-IP gefiltert bzw. priorisiert werden. So bleibt der Dienst möglichst lange verfügbar, obwohl vielleicht der eine oder andere legitime Benutzer ausgefiltert bzw. niedrig priorisiert wird.

4. Analysieren Sie den Angriff und legen Sie eine Abwehrstrategie fest: Stellen Sie sich darauf ein, dass der Angreifer versuchen wird, sich auf Ihre Abwehrmassnahmen einzustellen und dass er neue Taktiken anwenden wird. Analysieren Sie in einem solchen Fall den DoS erneut und wenden Sie entsprechende Gegenmassnahmen an.

5. Melden Sie den Vorfall an MELANI und erstatten Sie Anzeige bei der zuständigen Polizei, wegen (versuchter) Datenbeschädigung (Art. 144 bis Strafgesetzbuch) und gegebenenfalls (versuchter) Erpressung (Art. 156 Strafgesetzbuch). Eine Datenbeschädigung liegt auch dann vor, wenn Daten durch einen Angriff über eine gewisse Zeit nicht verfügbar und deshalb «unbrauchbar» sind.

6. MELANI wie auch die Polizei raten dringend davon ab, auf die Forderungen der Erpresser einzugehen.

Melde- und Analysestelle Informationssicherung MELANI & GovCERT.ch (2015): Massnahmen gegen DDoS Attacken