Merkblatt Informationssicherheit für KMUs

MELANI

Version:	v2.0
Autor:	MELANI
Zuletzt aktualisiert:	25. Mai 2018

[1] http://creativecommons.org/licenses/by-nd/3.0/

Einleitung

Dieses Merkblatt richtet sich an Schweizer KMU und soll diesen dabei helfen, die Informationssicherheit in ihrer Systemlandschaft und im Unternehmensnetzwerk zu erhöhen[2].

Das Merkblatt ist in zwei Bereiche unterteilt:

- **Organisatorische Massnahmen**, um die Informationssicherheit zu erhöhen bzw. sicher zu stellen
- **Technische Massnahmen**, um die Sicherheit der IT-Infrastruktur zu erhöhen bzw. sicher zu stellen

Technische Massnahmen alleine genügen nicht, um die Informationssicherung in einem Unternehmensnetzwerk zu gewährleisten. Zusätzlich sind immer auch organisatorische Massnahmen notwendig. Gerade bei kosten- und/oder ressourcenintensiven Massnahmen muss jede Firma eine Abwägung treffen zwischen den Kosten dieser Massnahme und den Risiken, die bei einer Nichtumsetzung der Massnahme entstehen. Die Geschäftsleitung muss deshalb entscheiden, entsprechende Restrisiken zu tragen oder Ressourcen bereitzustellen, um diese zu minimieren. Obwohl die technischen Risiken der IT-Systeme einen wichtigen Teil die Informationssicherheit darstellen, sollte ein Unternehmen seinen Fokus nicht auf diesen Teil der Risiken beschränken oder gar die IT-Abteilung als alleinigen Risikoträger definieren. Die Verantwortung für das Risikomanagement, die Klassifikation und Einstufung der Informationen, sowie ein allenfalls abgestufter Aufwand an zur Verfügung gestellten Sicherungsmassnahmen sind Kernaufgaben der Geschäftsleitung.

Massnahmen auf organisatorischer Ebene

Organisatorische Massnahmen stellen sicher, dass die **Verantwortlichkeiten** im Unternehmen bezüglich Informationssicherheit definiert sind.

Auf organisatorischer Ebene lassen sich folgende Massnahmen treffen:

- **Überprüfung der Risiken im Bereich Informationssicherheit und Vorlage an die Geschäftsleitung**
  Beurteilen Sie die Abhängigkeit Ihrer Geschäftsprozesse von Ihrer Informatik. 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 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.

- **Verantwortlichkeiten bezüglich IT, insbesondere der IT-Sicherheit, sind geregelt.**
  Die Mitarbeitenden müssen wissen, an wen sie sich wenden sollen, wenn sie Fragen

[2] Sieht auch: "Informatik-, IT-Sicherheit und Infrastruktur: Empfehlungen" aus dem KMU Portal des Bundes: https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/infrastruktur-und-it.html

zur IT-Sicherheit haben (z.B. bei Erhalt eines verdächtigen E-Mails) oder wer bei einem IT-Sicherheitsvorfall zu informieren ist. Erarbeiten Sie frühzeitig einen Plan zur Bewältigung von Sicherheitsvorfällen (Incident Response Plan). Üben Sie dessen Umsetzung regelmässig und passen Sie den Plan aufgrund der Erkenntnisse aus diesen Übungen an.

- **Die Zuständigkeiten bezüglich IT-Sicherheit zwischen Ihrem Unternehmen und Ihrem IT-Dienstleister sind klar geregelt.**
  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 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.

- **Regelmässige Schulung der Mitarbeitenden im Umgang mit der IT-Infrastruktur hinsichtlich der IT-Sicherheit.**
  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. Entsprechende Verhaltensregeln im Umgang mit dem Internet finden Sie auf unserer Webseite[3].

- **Kenntnis der aktuellen Bedrohungslage**
  Halten Sie sich auf dem Laufenden betreffend neuen Bedrohungen der Informationssicherheit und geeigneter Massnahmen, um diese zu bewältigen.[4]

- **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[5].

- **Verfügbare Firmeninformationen auf dem Internet**
  Oft benutzen Betrüger Informationen, die sie auf dem Internet über eine Firma finden (zu Mitarbeitern, 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[6] helfen könnten, auf das nötige Mass zu reduzieren. Dabei muss eine Abwägung des Nutzens und des Risikos der Publikation von solchen Informationen erfolgen.

- **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

---

[3] MELANI Verhaltensregeln: https://www.melani.admin.ch/verhaltensregeln

[4] Alle sechs Monate behandelt MELANI in ihrem Halbjahresbericht die wichtigsten Cybervorfälle der Schweiz und International: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte.html

[5] Empfehlungen und Verordnungen in Sache Datenschutz finden sie auf den Portal des Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDöB): https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html

[6] Beispiele von Angriffen, welche Social Engineering verwenden, finden Sie auf unserer Website: https://www.melani.admin.ch/melani/de/home/themen/socialengineering.html

gesamten Lebenszyklus eines Systems inklusive Wartung und Ausserbetriebssetzung 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? usw.

- **Passwort-Policy**
  Definieren Sie verbindliche Passwortregeln und setzen Sie diese konsequent durch (z.B.: mind. 12 Zeichen mit Buchstaben, Zahlen und Sonderzeichen oder Prüfung der Passworthashes gegen bekannte Datenlecks). Setzen Sie wo immer möglich auf eine Zwei-Faktor-Authentisierung[7]. 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.**
  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[8].

- **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 Mitarbeitenden in allen Fällen eingehalten werden.

- **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.

Massnahmen auf technischer Ebene

Eine 100prozentige 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 Benutzerinnen und Benutzer Sind diese nicht im sicheren Umgang mit IT-Systemen geschult, sind viele der aufgezählten technischen Massnahmen nutzlos.

Auf technischer Ebene lassen sich folgende Massnahmen treffen:

- **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 vollständiger Systemscan durchführt (z.B. wöchentlich oder monatlich).

  Im privaten Bereich und 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

[7] Sieht z.B. die Empfelungen von MELANI in Sache Password Erstellung: https://www.melani.admin.ch/melani/it/home/schuetzen/verhaltensregeln.html

[8] Sieht z.B "eBanking aber sicher! Ihr Wegbegleiter für sicheres eBanking" von der Hochschule Luzern: https://www.ebankingabersicher.ch/de/

bieten jedoch meistens Zusatzfunktionen wie z.B. einen Anti-Spam-Filter oder einen Werbeblocker.

- **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 Backups an einem sicheren Ort auf (offline). Stellen Sie sicher, Vorgängerversionen des 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.

- **Sicherheitsupdates**
  Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. **Stellen Sie sicher, dass sämtliche Computer und Server in Ihrem Netzwerk Sicherheitsupdates automatisch einspielen (Aktivierung von Automatischen Updates).** Patchen Sie Drittsoftware wie z.B. Adobe Reader, Adobe Flash, Java etc. ebenfalls regelmässig. Das gilt auch für die eingesetzte Hardware wie z.B. Drucker, Router usw.

- **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 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.

- **„Least privilege“ Prinzip[9].**
  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.

- **Netzwerksegmentierung[10].**
  Mindestens die Computer der Buchhaltung und der Personalabteilung (HR) sollten in einem separaten Netzwerk stehen und von den anderen Computern in Ihrem Netzwerk nicht erreichbar sein. Denken Sie auch daran, dass sich Malware auch über Netzwerk-Shares weiterverbreiten kann. Ihr IT-Dienstleister kann Sie bei der Planung und Umsetzung beraten.

- **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 be-

---

9 Sieht z.B. "Restriktive Berechtigungsvergabe bei Client-Betriebssystemen ab Windows Vista" von deutschen Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04247.html
Und/oder "Netzwerksicherheit in der Bundesverwaltung" von Informatiksteuerungsorgan des Bundes: https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/sicherheit/si003-netzwerksicherheit_in_der_bundesverwaltung.html

10 Sieht z.B "Geeignete logische Segmentierung" von deutschen Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05062.html

stimmten Ländern (welche z.B. bekannt für ein hohes Spamaufkommen sind) abzuweisen.

Potenziell schädliche Email Anhänge sollten bereits auf Ihrem Email-Gateway bzw. Spam-Filter blockiert bzw. gefiltert werden. Gefährliche Email Anhänge verwenden verschiedene Dateiendungen, vor welchen MELANI auf ihrer Webseite warnt[11].

- 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.

- **Makros**
  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.

- **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, Google Authenticator usw.).

- **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 nie in der Cloud abgelegt, sondern nur lokal gespeichert werden. Ausserdem sollten Sie sich vor Abschluss eines Vertrags beim Anbieter erkundigen, wer Zugriff auf die Daten hat, wie die Datensicherung geregelt ist usw.

- **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 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 auf unserer Webseite[12]. Ist Ihr

[11] MELANI Verhaltensregeln E-Mail:https://www.melani.admin.ch/melani/de/home/schuetzen/verhaltensregeln.html

[12] Massnahmen zum Schutz von Content Management Systemen (CMS):

Unternehmen stark vom Internetauftritt abhängig (z.B. Onlineshop), dann machen Sie sich auch Gedanken darüber, wie Sie einem allfälligen DDoS Angriff begegnen können.[13] Die grossen Internet Service Provider in der Schweiz bieten einen DDoS-Schutz an, den Sie schon jetzt einkaufen können, aber erst dann bezahlen müssen, wenn Sie ihn tatsächlich brauchen.

MELANI empfiehlt zudem bei einem Virenbefall oder bei einem Verdacht auf einen solchen, den betroffenen Computer neu aufzusetzen (Neuinstallation des Betriebssystems). Somit lässt sich verhindern, dass Teile der Schadsoftware auf dem Computer verbleiben und den Computer wieder infizieren können. Zudem besteht die Gefahr, dass bei einem Virenscan nicht alle Malware identifiziert und entfernt werden kann. Eine Neuinstallation ist daher immer die sicherste Lösung. Ändern Sie alle Passwörter, die auf dem infizierten System eingegeben wurden. Vor der Neuinstallation sind zwingend alle Daten zu sichern, da diese beim Neuaufsetzen verloren gehen.

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

[13] Massnahmen gegen DDoS Attacken: https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html