Merkblatt IT-Sicherheit für KMUs

MELANI / GovCERT.ch

Version:	v1.03
Autor:	MELANI / GovCERT.ch
Zuletzt aktualisiert:	24. Juli 2016

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

Einleitung

Dieses Merkblatt richtet sich an Schweizer KMUs und soll diesen dabei helfen die IT-Sicherheit im Unternehmensnetzwerk zu erhöhen.

Das Merkblatt ist in zwei Bereiche unterteilt:

- Massnahmen, welche auf **organisatorischer Ebene** getroffen werden können, um die IT-Sicherheit zu erhöhen bzw. sicher zu stellen
- Massnahmen, welche auf **technischer Ebene** getroffen werden können, um die IT-Sicherheit zu erhöhen bzw. sicher zu stellen

Wir weisen darauf hin, dass technische Massnahmen alleine nicht genügen, um die IT-Sicherheit in einem Unternehmensnetzwerk zu gewährleisten. Zusätzlich sind immer auch organisatorische Massnahmen notwendig. Gerade bei kosten- und/oder ressourcenintensiven Massnahmen muss jede Firma, konkret die Geschäftsleitung, eine Abwägung treffen zwischen den Kosten dieser Massnahme und den Risiken, die bei einer Nichtumsetzung der Massnahme entstehen. Die Geschäftsleitung muss deshalb entscheiden, entsprechende Risiken zu tragen oder Ressourcen bereitzustellen, um diese zu minimieren.

Massnahmen auf organisatorischer Ebene

Ziel von organisatorischen Massnahmen ist es, sicher zu stellen, dass die **Verantwortlichkeiten** im Unternehmen bzgl. IT-Sicherheit definiert sind.

Auf organisatorischer Ebene lassen sich folgende Massnahmen treffen:

- **Stellen Sie sicher, dass die Verantwortlichkeiten bzgl. IT, insbesondere der IT-Sicherheit, geregelt sind.** Dies umfasst beispielsweise an wen sich die Mitarbeitenden wenden sollen, wenn diese Fragen zur IT-Sicherheit haben (z.B. bei Erhalt eines verdächtigen E-Mails) oder wer bei einem IT-Sicherheitsvorfall zu informieren ist.

- **Schulen Sie die Mitarbeitenden regelmässig im Umgang mit der IT-Infrastruktur hinsichtlich der IT-Sicherheit.** Entsprechende Verhaltensregeln im Umgang mit dem Internet finden Sie auf unserer Webseite:

  Verhaltensregeln:
  https://www.melani.admin.ch/verhaltensregeln

- **Stellen Sie sicher, dass bezüglich IT-Sicherheit die Zuständigkeiten zwischen Ihnen und Ihrem IT-Dienstleister klar geregelt sind.** Dies betrifft insbesondere die technischen Massnahmen, wie Backup, Virenschutz, Logfiles. Überprüfen Sie die Einhaltung dieser Massnahmen regelmässig, 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).

- **Überprüfen Sie regelmässig Ihre Risiken im Bereich Informationssicherheit und legen Sie diese der Geschäftsleitung vor.** Beachten Sie dabei die Abhängigkeit Ihrer Geschäftsprozesse von Ihrer Informatik, beispielsweise welche Auswirkungen es hat, wenn ein bestimmtes System für längere Zeit ausfällt oder wenn eine Datenablage nicht mehr verfügbar ist.

- **Definieren Sie eine Passwort-Policy und setzen Sie diese technisch um** (z.B.: Passwortwechsel alle 3 Monate, mind. 12 Zeichen mit Buchstaben, Zahlen und Sonderzeichen).

- **Nutzen Sie Einschränkungen Ihrer 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.

- **Bei den meisten E-Banking-Systemen gibt es die Möglichkeiten von Kollektiv-E-Banking-Verträgen.** Hierbei wird eine Zahlung 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.

Seien Sie sich zudem bewusst, dass in jedem Fall die Geschäftsleitung die IT-Risiken trägt. Diese lassen sich nicht delegieren.

Massnahmen auf technischer Ebene

Mit technischen Massnahmen lässt sich die Gefahr einer Infektion mit Schadsoftware mindern und die IT-Sicherheit im Unternehmensnetzwerk steigern. Eine 100prozentige Sicherheit wird dadurch aber nie erreicht. Das schwächste Glied in der Kette ist in vielen Fällen nicht die Technik, sondern der Benutzer. Ist dieser nicht mit dem sicheren Umgang mit IT-Systemen geschult, sind viele der aufgezählten technischen Massnahmen nutzlos.

Auf technischer Ebene lassen sich folgende Massnahmen treffen:

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

- **Vergewissern Sie sich, dass regelmässig (täglich) ein Backup aller Daten durchgeführt wird.** Überprüfen Sie das Backup regelmässig auf seine Funktionsfähigkeit. Bewahren Sie Backups an einem sicheren Ort auf (offline). Stellen Sie sicher, Vorgängerversionen des Backups über einen bestimmten Zeitraum aufzubewahren.

- **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.

- **Arbeiten Sie nach dem „least privilege“ Prinzip[2].** Es gilt Mitarbeitenden nur diejenigen Rechte zu gewähren, welche diese für die Ausführung der Ihnen zugetragenen Arbeit benötigen. Mitarbeitende sollten standardmässig über keine Administratorenrechte verfügen.

[2] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04247.html

- **Segmentieren Sie Ihr Netzwerk.** 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.

- **Verwenden Sie einen 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 Spamaufkommen sind) abzuweisen.

- **Stellen Sie sicher, dass potenziell schädliche Email Anhänge bereits auf Ihrem Email-Gateway bzw. Spam-Filter blockiert bzw. gefiltert werden.** Gefährliche Email Anhänge verwenden unter anderem folgende Dateiendungen:
  .js (JavaScript)
  .jar (Java)
  .bat (Batch file)
  .exe (Windows executable)
  .cpl (Control Panel)
  .scr (Screensaver)
  .com (COM file)
  .pif (Program Information File)
  .vbs (Visual Basic Script)
  .ps1 (Windows PowerShell)
  .wsf (Windows Script File)
  .docm (Microsoft Word mit Makros)
  .xlsm (Microsoft Excel mit Makros)
  .pptm (Microsoft PowerPoint mit Makros)

- **Versichern Sie sich, dass solche gefährlichen E-Mail-Anhänge auch dann blockiert werden, wenn diese in Archiv-Dateien wie Beispielsweise ZIP, RAR** oder aber auch in geschützten Archiv-Dateien (z.B. in einem passwortgeschützten ZIP) an Empfänger in Ihrem Unternehmen versendet werden.

- **Zusätzlich sollten sämtliche E-Mail-Anhänge blockiert werden, welche Makros enthalten (z.B. Word, Excel oder PowerPoint Anhänge mit Makros).**

- **Verwenden Sie auf jedem Computer eine Firewall. Schützen Sie zudem Ihr Unternehmensnetzwer**k gegenüber dem Internet mit einer zusätzlichen Firewall. Das Standardverhalten der Firewall sollte sein, dass sämtlicher eingehender und ausgehender Datenverkehr unterbunden wird, ausser demjenigen, welcher explizit (durch eine Firewall-Regel) zugelassen wird.

- **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 etc.).

- **Definieren Sie eine Passwort-Policy und setzen Sie diese technisch um.**

- Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. **Stellen 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.

- **Seien Sie vorsichtig bei der Verwendung von Cloud-Diensten.** Sensible Daten sollten nie in der Cloud abgelegt sondern nur lokal gespeichert werden.

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

- Falls Ihr Unternehmen über ein 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:

  Massnahmen zum Schutz von Content Management Systemen (CMS):
  https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

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 Rückstände der Schadsoftware 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.

Weiterführende Links

- Verhaltensregeln im Umgang mit dem Internet
  https://www.melani.admin.ch/verhaltensregeln

- Massnahmen zum Schutz von Content Management Systemen (CMS)
  https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

- KMU Portal des Bundes: Sicherheitsvorkehrungen für die IT-Infrastruktur
  http://www.kmu.admin.ch/kmu-betreiben/03710/03712/03715/index.html?lang=de