Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Generalsekretariat

Nationales Zentrum für Cybersicherheit NCSC
www.ncsc.admin.ch

NCSC

Merkblatt Informationssicherheit für KMUs

Inhaltsverzeichnis

1 Einleitung 2
2 Organisatorische Massnahmen 2
3 Technische Massnahmen 4

1 Einleitung

Dieses Merkblatt richtet sich an Schweizer KMU und soll ihnen helfen, die Informationssicherheit in Ihrem Unternehmen zu erhöhen.[1].

Das Merkblatt ist in zwei Bereiche unterteilt:

- **Organisatorische Massnahmen** erhöhen oder stellen die Informationssicherheit sicher.
- **Technische Massnahmen** erhöhen oder stellen die Sicherheit der IT-Infrastruktur sicher.

Technische Massnahmen leisten einen wesentlichen Beitrag zur Gewährleistung der Informationssicherheit. Jedoch müssen diese technische Massnahmen durch organisatorische Massnahmen ergänzt werden. Insbesondere bei kosten- und/oder personalintensiven Massnahmen muss jedes Unternehmen zwischen den Kosten dieser Massnahmen und den bei einer Nichtumsetzung der Massnahmen entstehenden Risiken abwägen. Nicht umgesetzte Massnahmen hinterlassen so genannte Restrisiken. Deshalb muss die Geschäftsleitung entscheiden, diese Restrisiken zu tragen oder Ressourcen bereitzustellen, um diese zu weiter 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 benennen. 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.

2 Organisatorische Massnahmen

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

Information der Geschäftsleitung über Risiken
Beurteilen Sie die Abhängigkeit Ihrer Geschäftsprozesse von Ihrer Informatik. Welche Auswirkungen hat der Ausfall eines Systems oder die Nicht-Verfügbarkeit der Datenablage? Mit welchen finanziellen Folgen ist zu rechnen? Welche Massnahmen können dagegen ergriffen werden? usw.

Risiken als Bestandteil der Governance und des Kontinuitätsmanagements
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.

Die Verantwortlichkeiten sind geregelt
Die Mitarbeitenden müssen 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. Erarbeiten Sie frühzeitig einen Plan zur Bewältigung von Sicherheitsvorfällen (Incident Response Plan). Prüfen Sie die Wirksamkeit des Plans regelmässig, beispielsweise mit Übungen, und passen Sie den Plan aufgrund der Erkenntnisse

[1] 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

aus diesen Übungen an.

Zuständigkeiten von Unternehmen und IT-Dienstleister
Viele kleinere Unternehmen lagern die IT an spezialisierte Dienstleister aus. Die Zuständigkeiten zwischen Ihnen und dem IT-Dienstleistungsunternehmen müssen klar geregelt sein. Regeln Sie im Vertrag Haftungsfragen für den Fall, dass Sicherheitsvorschriften missachtet oder die IT-Sicherheit anderweitig vernachlässigt wird. Der Vertrag muss klar und unmissverständlich formuliert sein. Wenn beispielsweise aufgrund eines Missverständnisses keine Datensicherungen erstellt werden, kann das verheerende Folgen haben.[2]

Mitarbeitersensibilisierung
Der Sensibilisierung aller Mitarbeitenden im Umgang mit der IT-Infrastruktur kommt eine zentrale Bedeutung zu. Schulen Sie Ihr Personal regelmässig im Umgang mit potenziellen Gefahren in der digitalen Welt. Sensibilisieren Sie Ihre Mitarbeitenden im Umgang mit E-Mails und Internet. Entsprechende Verhaltensregeln finden Sie auf unserer Webseite.

Kenntnis der aktuellen Bedrohungslage
Halten Sie sich auf dem Laufenden betreffend neuen Bedrohungen der Informationssicherheit und geeigneter Massnahmen, um diese zu bewältigen.[3]

Umgang mit sensiblen Daten
Erlassen Sie verbindliche Regeln zur Klassifizierung von Daten und setzen Sie diese Regeln konsequent durch. Regeln Sie insbesondere, wie klassifizierte Daten elektronisch gespeichert und/oder übermittelt werden dürfen.[4] Definieren Sie Richtlinien zur Weitergabe von Unternehmensinformationen. Über anonyme Kanäle (zum Beispiel Telefon oder E-Mail) sollten grundsätzlich keine vertraulichen Informationen weitergegeben werden.

Firmeninformationen im Internet
Kriminelle suchen laufen Informationen über potenzielle Opfer. Überlegen Sie sich deshalb genau, welche Informationen Sie zum Beispiel auf der eigenen Website oder in sozialen Medien verbreiten. Reduzieren Sie das Mass an im Internet verfügbaren Informationen über das Unternehmen auf ein Minimum. Wägen Sie Nutzen und Risiko der verfügbaren Informationen ab. Erstellen Sie Richtlinien, wie Ihre Mitarbeitenden beispielsweise bei der privaten Nutzung sozialer Medien mit Unternehmensinformationen umzugehen haben.

Sicherheit von der Beschaffung bis zur Entsorgung der IT-Infrastruktur
Sicherheitsüberlegungen sollten immer in den Beschaffungsprozess eingebunden werden. Dabei sind nicht nur die Anforderungen bei der Inbetriebnahme, sondern über den gesamten Lebenszyklus eines Systems inklusive Wartung und Ausserbetriebssetzung zu berücksichtigen. Informieren Sie sich insbesondere vor dem Kauf, wie lange beispielsweise Sicherheitsupdates zur Verfügung gestellt werden. Werden diese automatisch installiert? Wie erfahren Sie, das neue Updates vorhanden sind? Legen Sie die Vorgehensweise bei der Ausserbetriebssetzung von Teilen der IT-Infrastruktur fest (z.B. wie vertrauliche Informationen zuverlässig von den betroffenen Systemen zu entfernen sind).

---

[2] Weitere Informationen siehe hier Zusammenarbeit mit IT-Dienstleistern: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/zusammenarbeit-it-provider.html

[3] Alle sechs Monate behandelt NCSC in ihrem Halbjahresbericht die wichtigsten Cybervorfälle der Schweiz und International. Auch werden die Top 5 Bedrohungen auf der Webseite von NCSC regelmässig aktualisiert.

[4] 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

Passwort-Policy
Definieren Sie verbindliche Passwortregeln und setzen Sie diese konsequent durch. Die Mindestlänge des Passwortes sollte bei zwölf Zeichen liegen und sowohl aus Gross- und Kleinbuchstaben, Zahlen wie auch Sonderzeichen bestehen. Setzen Sie wenn möglich auf eine Zwei-Faktoren-Authentisierung. Vermeiden Sie unbedingt die Mehrfachverwendung von gleichen Passwörtern. Verwenden Sie einen Passwortmanager und generieren Sie für jede Anwendung ein eigenes Passwort. Sie finden auf dem Markt unterschiedliche Passwortmanagement-Systeme für die verschiedenen Betriebssysteme und Geräte; es gibt sowohl kostenlose als auch lizenzpflichtige Programme. Passwörter und Zugangsdaten dürfen niemals weitergegeben werden.

Zugriffsberechtigungen
Die wenigsten Mitarbeitenden benötigen weitreichende Administratorenrechte. Erteilen Sie dem Mitarbeitenden nur so viele Rechte, wie für die Erledigung seiner Arbeit zwingend notwendig sind (beispielsweise benötigen Mitarbeitende des Marketings nicht zwingend Zugriff auf die Informationen in der Personalabteilung). Insbesondere sollten Sie die Rechte für die Installation jeglicher Software unterbinden.

E-Banking
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. Regeln Sie sämtliche den Zahlungsverkehr betreffenden Vorgänge und setzen Sie deren Einhaltung konsequent um (Vier-Augen-Prinzip, Kollektivunterschrift usw.). Dies gilt insbesondere, wenn mehrere Mitarbeitende zahlungsberechtigt sind. Unter Umständen lassen sich nicht benötigte Funktionen in Ihrer e-Banking Applikation abschalten oder einschränken. Sprechen Sie mit Ihrer Bank über mögliche Sicherheitsmassnahmen z. B. über allfällige Länderbeschränkungen.

3 Technische Massnahmen

Eine 100prozentige Sicherheit lässt sich durch technische Massnahmen nie erreichen. Oft sind nicht die technischen Massnahmen das schwächste Glied in der Kette, sondern der Mensch. Sind die Mitarbeitenden im sicheren Umgang mit IT-Systemen nicht geschult, kann dies die Wirksamkeit der im Folgenden beschriebenen technischen Massnahmen wesentlich beeinflussen. Jedoch trägt eine sinnvolle Kombination verschiedener technischer Massnahmen wesentlich zur IT-Sicherheit im Unternehmensnetzwerk bei und mindert die Gefahr von Infektionen mit Schadsoftware.

Regelmässige Datensicherung
Definieren Sie einen Prozess für die regelmässige Datensicherung (Backup) und setzen Sie die Einhaltung konsequent durch. Sie können die Datensicherung und weitere technische Massnahmen auch an eine spezialisierte IT-Dienstleistungsfirma auslagern.

Überprüfen Sie die Datensicherung regelmässig auf ihre Funktionsfähigkeit. 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.

Die Sicherungskopie sollte offline, das heisst auf einem externen Medium wie Beispielsweise einer externen Festplatte gespeichert werden. Stellen Sie daher sicher, dass Sie das Medium, auf welche Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer trennen. Ansonsten werden bei einem Befall durch Ransomware möglicherweise auch

die Daten auf dem Backup-Medium verschlüsselt und unbrauchbar. Bewahren Sie auch ältere Backups über einen bestimmten Zeitraum auf.

Virenschutz
Auf jedem Computer im Unternehmen muss ein Virenschutz installiert sein. Dieser ist regelmässig zu aktualisieren. Führen Sie regelmässig vollständige Systemscans durch (z.B. wöchentlich oder monatlich.

Firewall
Verwenden Sie auf jedem Computer eine Firewall. Schützen Sie zudem Ihr Unternehmensnetzwerk gegenüber dem Internet mit einer zusätzlichen Firewall. Definieren Sie mittels Firewall-Regeln, welche ein- und ausgehenden Verbindungen erlaubt sein sollen. Lassen Sie proxyfähige Protokolle wie HTTP/HTTPS usw. über einen Proxy laufen. Werten sie die Logdateien des Proxy regelmässig aus.

Sicherheitsupdates
Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. Stellen Sie sicher, dass sämtliche Computer und Server in Ihrem Netzwerk Sicherheitsupdates automatisch einspielen. Jede installierte Software ist unverzüglich zu aktualisieren, sobald Sicherheitsupdates vorhanden sind. Auch Hardware wie z.B. Drucker, Router usw. ist immer auf dem aktuellsten Stand zu halten.

Content Management Systeme (CMS)
Content Management Systeme (CMS) für die Erstellung und Aktualisierung von Internetseiten sind stets auf dem aktuellsten Stand zu halten. Die meisten CMS bieten eine einfach zu aktivierende automatische Updatefunktion an. Verwenden Sie eine «Web Application Firewall» (WAF), um Ihre Webseite gegen Angriffe zu schützen. Eine Liste von weiteren Massnahmen zum Schutz CMS) finden Sie auf unserer Webseite[5]. Ist Ihr Unternehmen stark vom Internetauftritt abhängig (z.B. Onlineshop), dann machen Sie sich auch Gedanken darüber, wie Sie einem allfälligen DDoS Angriff begegnen können.[6] 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.

Logdateien
Sogenannten «Logdateien» kommt bei der Nachbearbeitung eines IT-Vorfalles zentrale Bedeutung zu. Stellen Sie sicher, dass kritische Systeme wie Buchhaltungssoftware, Domain-Controller, Firewall oder E-Mail-Server solche Logdateien anlegen. Prüfen Sie die verfügbaren Logdateien regelmässig auf Unstimmigkeiten. Bewahren Sie Logdateien für mindestens sechs 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[7]
Unterteilen Sie Ihr Unternehmensnetz in einzelne Bereiche (z.B. separate Netze für Produktion, Personal, Buchhaltung usw.). Es gibt keinen Grund, weshalb Mitarbeitende des Perso-

---

5 Massnahmen zum Schutz von Content Management Systemen (CMS): https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ics.html

6 Massnahmen gegen DDoS Attacken: https://www.ncsc.admin.ch/ /ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ddos.html

7 "Geeignete logische Segmentierung" vom deutschen Bundesamt für Sicherheit in der Informationstechnik BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05062.html

naldienstes auf Ihre Produktionsanlage zugreifen sollten. So vermeiden Sie, dass beispielsweise Steuerungscomputer von Werksanlagen, die nicht mehr aktualisiert werden können, zum Einfallstor für Angreifende werden.

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.

Filtern potenziell schädlicher E-Mails
Potenziell schädliche E-Mail Anhänge sollten bereits auf Ihrem Email-Gateway bzw. Spam-Filter blockiert bzw. gefiltert werden. Eine Liste potenziell schädlicher Dateiendungen finden Sie auf der Website von NCSC[8]. 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 dienen der Automatisierung von Office-Dokumenten. Sie können aber auch zur Verbreitung von Schadsoftware zum Einsatz kommen.
Sämtliche E-Mail-Anhänge, die Makros enthalten (z.B. Word, Excel oder PowerPoint Anhänge mit Makros), sollten blockiert werden. Sensibilisieren Sie Ihre Mitarbeitenden dahingehend, dass entsprechende Warnhinweise in Office-Programmen nicht ignoriert werden dürfen.

Fernzugriffe
Müssen Mitarbeitende von aussen auf Ihr Firmennetz zugreifen (z.B. auf Geschäftsreisen, Home Office usw.) sollte dies nur durch ein virtuelles privates Netzwerk (VPN) möglich sein, das durch eine Zwei-Faktor-Authentisierung geschützt ist. Dies gilt auch für den Zugriff von externen IT-Dienstleistern und Administratoren.

Cloud-Dienste
Bei der Nutzung von Cloud-Diensten müssen Sie keine teure IT-Infrastruktur selber betreiben. Seien Sie aber vorsichtig bei der Verwendung von Cloud-Diensten. Sensible Daten sollten nie in der Cloud abgelegt, sondern nur lokal gespeichert werden. Erkundigen Sie sich vor Vertragsabschluss beim Anbieter über die wichtigsten Sicherheitsvorkehrungen (Zugriff auf die Daten, Datensicherung usw.).

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

[8] NCSC Verhaltensregeln E-Mail: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/verhalten-bei-e-mail.html