ALLIANZ
DIGITALE SICHERHEIT
SCHWEIZ

Cybersecurity Leitfaden für KMU

Version 2.1 | 8. Februar 2022

Dieser Leitfaden wurde entwickelt, um KMU eine Hilfestellung zu geben, wie sie eine minimalen Cybersecurity erreichen und sich so besser vor den häufigsten Cyber-Attacken schützen können.

KMU sind immer häufiger das Ziel von Cyber-Attacken, die gravierende Auswirkungen haben können. Schon wenige wichtige Massnahmen helfen, einen minimalen Schutz gegen Cyberbedrohungen zu erreichen. Diese Massnahmen sind im vorliegenden Leitfaden erläutert. Die Sprache des Leitfadens ist klar, die Handlungen einfach und konkret – spezifisch abgestimmt auf die Bedürfnisse von KMU.

Der Leitfaden ergänzt den Cybersecurity-Schnelltest für KMU und folgt der darin eingeführten Themenstruktur. Für eine Selbstbeurteilung, wie das eigene Unternehmen in Sachen Cybersecurity aufgestellt ist, empfehlen wir das Ausfüllen des Schnelltests.

Der Leitfaden sowie der vorgelagerte Schnelltest für KMU sind Teil der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken. Eine Fachgruppe hat die Inhalte entwickelt und explizit auf die Bedürfnisse von KMU abgestimmt.

Die an der Erarbeitung des Leitfadens involvierten Partner setzen sich gemeinsam dafür ein, dass sich die Schweizer KMU-Landschaft bestmöglich vor Cyberrisiken schützen kann.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

ICTSWITZERLAND ISSS Information Security Society Switzerland satw it's all about technology SNV standards connect the world SQS ASA | SVV

Übersicht

Sicherheit im Bereich Organisation und Prozesse

Wieso ist es wichtig?

Bei einem Cyber-Vorfall sind die richtige Vorbereitung und Reaktion zentral und entscheiden darüber, ob und wie schnell Sie Ihr Business nach einem Vorfall weiter betreiben können.

Eine rasche und richtige Reaktion kann Schäden entscheidend verringern oder sogar vermeiden. Dazu ist es wichtig, Ihre Organisation auf diese Bedrohungen auszurichten und entsprechende Prozesse zu definieren, wie z.B. ein regelmässiges Backup Ihrer Daten durchzuführen, Zugriffsrechte selektiv zu vergeben sowie einen Notfallplan zu erstellen.

Was kann ich tun?

☐ Sichern Sie Ihre Informationen mit einem regelmässigen **Backup**.

☐ Sorgen Sie für eine geeignete **Benutzeradministration**.

☐ Erstellen Sie einen **Notfallplan**.

Wie gehe ich vor?

Informationen sichern: Backup als Routine

- Erstellen Sie regelmässig und falls möglich automatisiert ein Backup auf einem Sicherheitsmedium (Festplatte, Online, etc. – je nach Geschäftsmodell und regulatorischen Vorgaben des KMU).
- Bewahren Sie das Backup an einem externen, geschützten Ort und vom Netzwerk getrennt auf (Offline-Backup).
- Überprüfen Sie regelmässig, ob sich die Daten von den Sicherheitsmedien zurückspielen lassen.

Angriffsfläche minimieren: Geeignete Benutzeradministration

Mit einer erfolgreiche Benutzeradministration kann Kriminellen der Zugriff auf besonders wichtige Informationen erschwert werden.

- Erstellen Sie getrennte Konten (Login) für Admin-Aufgaben (besonders schützenswerte Daten, Informationen und Systeme) und «normale» Aufgaben.
- Geben Sie jeder Benutzerin und jedem Benutzer nur die notwendigsten Zugriffsrechte. So kann verhindert werden, dass sich Angreifer unbeschränkten Zugriff auf alle Systeme verschaffen.
- Verwenden Sie, wenn möglich nur persönliche Konten (keine Konten verwenden, die von mehreren Benutzerinnen und Benutzern mit gleichem Benutzernamen/Kennwort verwendet werden).
- Legen Sie fest, wer auf bestimmte IT-Anwendungen/Informationen Zugriff hat. Vergeben Sie die Zugriffsrechte rollenbasiert (z.B. Buchhaltung/Personal-Admin/Sekretariat/System-Admin/ Verkauf)
- Sperren Sie bei Austritten aus dem Unternehmen die Benutzerkonten/Zugangsdaten der entsprechenden Personen.

Vorsorgen für den Ernstfall: Notfallplan

Erstellen Sie einen Notfallplan, damit Sie im Bedarfsfall wissen, wie Sie vorgehen müssen.

- Identifizieren Sie notfallkritische Systeme, z.B. Adressdatenbank, Mailsystem, Terminkalender etc., sowie persönliche Daten und Kundendaten.
- Definieren Sie Rückfallebenen (Bereitstellung Ersatz-PCs; Ausrüstung aller Arbeitsplätze mit mindestens zwei Browsern; Vereinbarung über Reaktionszeiten und Lieferfristen mit Lieferanten).
- Halten Sie fest, wer mit welchem System arbeitet (Namen und Telefonnummern), um im Notfall zielgerichtet informieren zu können
- Definieren Sie die erste Reaktion bei einem Vorfall: Trennen Sie die Netzwerkverbindungen (Kabel und WLAN) der betroffenen Systeme.
- Definieren Sie Massnahmen zur schnellen Wiederherstellung Ihrer Systeme und überlegen Sie sich, wie Sie bei einem Ausfall der kritischen Systeme die Arbeit weiterführen können (z.B. Ausdruck der wichtigsten Kontaktdaten, etc.)
- Definieren Sie Zuständigkeiten und Rollen, d.h. wer ist bei einem Vorfall (z.B. bei einer Lösegeldforderung oder beim Ausfall eines notfallkritischen Systems) wie zu informieren:
    - Person/Firma zur Behebung des IT-Vorfalls.
    - Person/Firma für rechtliche Sofortmassnahmen. Sind z.B. Personendaten betroffen, empfiehlt sich die Kontaktaufnahme mit einer Rechtsberatung bzw. einer juristischen Fachperson.
    - Person/Firma für kommunikative Sofortmassnahmen.
    - Person für die Meldung des Vorfalls: Diese informiert den nächstgelegenen Polizeiposten sowie das nationale Zentrum für Cybersicherheit des Bundes (NCSC) über das entsprechende Meldeformular. In einem Cyber-Betrugsfall mit finanziellem Schaden ist die sofortige Kontaktaufnahme mit der Bank, Polizei und/oder einer spezialisierten Firma dringend empfohlen, um allfällige Zahlungen stoppen zu können.
    - Üben Sie den Notfall in Ihrem Unternehmen.

Sicherheit dank dem Faktor «Mensch»

Wieso ist es wichtig?

Trotz aller technischen Hilfsmittel sind es schliesslich die Mitarbeitenden, welche für die Sicherheit Ihres Unternehmens entscheidend sind. Dazu ist es wichtig, dass Sie und alle Mitarbeitenden die aktuellen Gefahren kennen, mit den technischen Mitteln umgehen können, sowie die wichtigsten Regeln einhalten.

Was kann ich tun?

☐ Verankern Sie die **Sensibilisierung** der Mitarbeitenden im Unternehmensalltag.

☐ Sorgen Sie mit sicheren **Passwörtern** für bestmöglichen Schutz Ihrer Anwendungen.

☐ Definieren Sie **Benutzerrichtlinien** für einen sicheren Umgang mit Internet und E-Mails.

Wie gehe ich vor?

Sicherheit zum Thema machen: Sensibilisierung

- Machen Sie die Sicherheit und insbesondere ein sicheres Verhalten im Internet im Unternehmen immer wieder zum Thema.
- Organisieren Sie eine Basisausbildung für Ihre Mitarbeitenden, mit folgendem Inhalt:
    - Was ist der Nutzen der IT-Sicherheit?
    - Was sind starke Passwörter? (siehe unten)
    - Was bedeutet ein sicherer Umgang mit Internet und E-Mail? (siehe unten)

Bestmöglicher Schutz Ihrer Anwendungen: Starke Passwörter

- Wählen Sie sichere Passwörter, d.h. verwenden Sie möglichst lange Passwörter mit mindestens 12 Zeichen, die aus Klein- und Grossbuchstaben, Zahlen und Sonderzeichen bestehen
- Verwenden Sie einen Passwortmanager und automatisch generierte Passwörter.
- Als Alternative nutzen Sie den Passsatz: Wählen Sie einen persönlichen Satz, den niemand einfach erraten kann. Von diesem Satz nehmen Sie jeweils den ersten oder die ersten zwei Buchstaben jedes Wortes und bilden so ein Passwort. Achten Sie darauf, keine allgemein bekannten Sätze wie Buchtitel, Redewendungen, etc. zu nutzen.
- Verwenden Sie Passwörter nicht mehrfach, d.h. nutzen Sie für jeden Dienst wie E-Mail-Account, Online-Banking, Buchhaltungssoftware, CRM-Anwendungen, etc. ein anderes Passwort.
- Verwenden Sie möglichst Zwei-Faktor Authentifizierung zum Schutz des Zugangs zu Ihren Internetdiensten (z.B. Einmal-Passwort, SMS-Token, etc.).
- Geben Sie ihr Passwort nicht auf einer Internetseite ein, die Sie über einen Link aufgerufen haben, sondern geben Sie die Adresse (URL) zur entsprechenden Seite manuell in der Adresszeile des Browsers ein.
- Ändern Sie unpersönliche Passwörter im Betrieb, wenn Mitarbeitende die Firma verlassen.

Für einen sicheren Umgang mit Internet und E-Mail: Benutzerrichtlinien

Definieren Sie Benutzerrichtlinien für einen sicheren Umgang mit Internet und E-Mail. Diese können u.a. folgende Punkte beinhalten:

- Geben Sie Login-Daten (Benutzername und Passwort) zu keinem Zeitpunkt und unter keinen Umständen an Dritte weiter.
- Übermitteln Sie Kreditkartennummern ausschliesslich bei vertrauenswürdigen Webseiten, achten Sie z.B. darauf, dass https:// vor der Adresse im Browser steht.
- Laden Sie keine unbekannten Programme aus dem Internet herunter.
- Nutzen Sie das Smartphone als Hotspot, statt ein öffentliches, ungeschütztes WLAN. Dies gilt insbesondere fürs Online-Banking. Ungeschützte Verbindungen sind nicht sicher und es besteht die Gefahr, dass Dritte auf Ihre Daten zugreifen.

- Seien Sie beim Erhalt von E-Mails vorsichtig und achten Sie insbesondere auf folgende Punkte:
    - Bei zweifelhaften E-Mails (z.B. untypische Absenderadressen, Schreibfehler, Tonalität und Logos) keine angefügten Dokumente oder Programme öffnen und keine Links anklicken.
    - Im Zweifelsfall niemals vertrauliche Informationen preisgeben und versuchen, den Absender auf andere Weise (z.B. telefonisch) zu kontaktieren, um die Vertrauenswürdigkeit der E-Mail zu überprüfen.
    - Auch Nachrichten kritisch prüfen, die von einer bekannten Person oder einem leitenden Mitarbeitenden der Firma stammen. Betrügerinnen und Betrüger könnten Zugriff auf das Postfach dieser Person haben und in deren Namen E-Mails verschicken.

Sicherheit dank geeigneter technischer Massnahmen

Wieso ist es wichtig?

Durch Sicherheitslücken können Unbefugte in Ihre Systeme eindringen. So können Daten vernichtet und manipuliert werden oder Ihre IT-Infrastruktur kann für kriminelle Zwecke manipuliert werden. Software-Updates schliessen diese Sicherheitslücken.

Eine aktuelle Firewall kann Ihren Computer vor unerlaubten Zugriffen schützen. Mit einer aktualisierten Antiviren-Software schützen Sie Ihre Daten vor Viren, Würmern und Trojanern.

Kriminelle können den Datenverkehr mitlesen und sogar manipulieren, wenn Ihre Kommunikation nicht verschlüsselt ist.

Was kann ich tun?

☐ Nutzen Sie geeignete **Software** (z.B. Firewall, Antiviren-Software) um Ihre Sicherheit zu erhöhen.

☐ Achten Sie auf eine **regelmässige Aktualisierung** Ihrer Software.

☐ Verbinden Sie **veraltete Geräte**, bei denen kein Softwareupdate verfügbar ist, nicht mit dem Internet.

Wie gehe ich vor?

Mit technischen Hilfsmitteln die Sicherheit erhöhen: Geeignete Soft- und Hardware

- Aktualisieren Sie Betriebssysteme, Firewall und andere Anwendungen regelmässig.
- Überprüfen Sie Ihren Computer regelmässig auf Updates und bringen Sie ihn auf den neusten Stand, um Sicherheitslücken zu schliessen.
- Nutzen Sie wo immer möglich automatische Update-Funktionen. Dies gilt auch für alle Softwareprodukte und mit dem Internet verbundenen Geräte, wie z.B. Anlagen, Drucker, Gebäudesteuerungen, Haushaltgeräte oder Smartphones.
- Trennen Sie Geräte, für die keine Updates ausgeliefert werden, vom Internet oder nehmen sie ausser Betrieb.
- Installieren Sie eine aktuelle Antiviren-Software und aktualisieren Sie diese regelmässig (geschieht meist automatisch). Für einen noch grösseren Schutz setzen Sie einen Virenscanner von zwei unterschiedlichen Herstellern ein, um ein möglichst breites Spektrum an Gefahren zu erkennen.
- Schützen Sie Ihre Kommunikation mit einer guten Verschlüsselung (z.B. Virtual Private Network, VPN).

Cybersicherheit als Teil des Datenschutzes

Wieso ist es wichtig?

Ihr Unternehmen ist verantwortlich für den sicheren Umgang mit Personendaten und geistigem Eigentum. Bei Datenverlust oder Datenschutzverletzungen drohen strafrechtliche Folgen, hohe Geldstrafen und schwerwiegender Imageverlust. Die Konsequenzen können existenzbedrohend sein.

Seit 2018 ist die neue Datenschutzgrundverordnung (DSGVO oder GDPR) der EU in Kraft, die teilweise auch für Schweizer Unternehmen gilt. Von der DSGVO betroffen sind Schweizer Firmen und Webseiten, die mit Daten von EU-Bürgerinnen und -Bürgern hantieren oder solche als Zielgruppe haben. Dies gilt z.B. auch für Webseiten, die mittels sog. Cookies das Surfverhalten ihrer Besucher aus dem EU-Ausland auswerten.

Cybersicherheit und Datenschutz gehen Hand in Hand: Durch einen Cyberangriff können Kriminelle an sensible Daten gelangen.

Was kann ich tun?

☐ Mit Massnahmen zur Cybersicherheit leisten Sie einen Beitrag zur gesetzlich festgelegten Einhaltung des Datenschutzgesetzes.

Wie gehe ich vor?

Mit Daten gesetzeskonform umgehen: Datenschutz

- Sobald Sie Daten von Personen (z.B. Kunden oder Mitarbeitende) auf irgendeine Art und Weise bearbeiten, müssen Sie diese hinreichend schützen (bzw. die Daten nur sammeln).
- Als Verarbeitung gilt jeder Umgang mit Personendaten, also insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten.
- Prüfen Sie, ob Sie vom DSGVO betroffen sind: Online-Check Economiesuisse, Faktenblatt DSGVO

Sicherheit dank geeignetem Umfeld

Wieso ist es wichtig?

Wenn einer Ihrer Lieferanten oder Dienstleister von einem Hackerangriff betroffen ist, können Sie mitbetroffen sein, z.B. wenn die eigenen Kundendaten verloren gehen. Es ist daher wichtig, dass auch Drittparteien, mit denen Sie zusammenarbeiten, die wichtigsten Cybersecurity-Massnahmen umsetzen.

Falls Sie die IT- oder die IT-Security an eine Drittpartei auslagern, ist es wichtig, dass Sie Ihrem Anbieter genau auf die Finger schauen und die wichtigsten Punkte mit ihm klären.

Was kann ich tun?

☐ Fordern Sie bei **Outsourcing-Partnern und Lieferanten** die Umsetzung minimaler Cybersecurity-Massnahmen ein.

☐ Achten Sie beim Auslagern von **IT- und IT-Security-Dienstleistungen** auf Zertifikate und die Einhaltung der wichtigsten Sicherheitsmassnahmen.

Wie gehe ich vor?

Sicherheit ausserhalb des eigenen Unternehmens einfordern: Outsourcing-Partner und Lieferanten

Gehen Sie mit Lieferanten und Dienstleistern (Outsourcing-Partnern) den Cybersecurity-Schnelltest durch und stellen Sie sicher, dass diese die Anforderungen, die ans eigene Unternehmen gestellt werden, auch erfüllen. Klären Sie u.a. folgende Punkte:

- Werden regelmässig Backups durchgeführt und an einem externen Ort gespeichert?
- Gibt es einen Notfallplan?
- Gibt es Benutzerrichtlinien und werden diese eingehalten?
- Sind Vorgaben für die Benutzeradministration vorhanden?
- Werden die Mitarbeitenden fürs Thema Cybersecurity sensibilisiert (z.B. Phishing-E-Mail, Verwendung von Passwörtern)?
- Werden Betriebssysteme, Firewall und andere Anwendungen regelmässig aktualisiert?
- Wird eine verschlüsselte Kommunikation verwendet?
- Wird Antivirensoftware genutzt und regelmässig aktualisiert?

Sicherheit bei Auslagerung von Security-Dienstleistungen: IT-Security-Provider

Stellen Sie sicher, dass der IT oder der IT-Security-Provider die wichtigsten Sicherheits-Anforderungen erfüllt: Gehen Sie mit ihm den Schnelltest durch oder prüfen Sie, ob er ein entsprechendes Zertifikat (z.B. CyberSeal für IT-Dienstleister, ISO 27001 für IT-Security-Provider) besitzt.

Worauf wir uns beziehen

Referenzen

BNC: Cybersecurity und Datenschutz

EDOEB: Datenschutz

IT-Sicherheit für KMU

KMU-Portal: Zehn Regeln für die Informationssicherheit im KMU

NCSC: Merkblatt Informationssicherheit für KMU

NCSC: Informationen für Unternehmen

Tagblatt: Datenschutzgesetz

UBS: Phishing