CYBERSECURITY-SCHNELLTEST FÜR KMU

Hinweise und weiterführende Informationen für einen minimalen Schutz

Nachfolgende Erläuterungen zeigen auf, weshalb die im Schnelltest www.cybersecurity-check.ch genannten Punkte für einen minimalen Cybersecurity-Schutz essentiell sind. Die Hinweise und ergänzenden Informationen stammen mehrheitlich von folgenden Quellen:

- Publikation «Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU)», die 2016 von der Information Security Society Switzerland ISSS aktualisiert wurde[1]
- Informationen für KMU der Melde und Analysestelle Informationssicherung MELANI auf ihrem Portal sowie in der Publikation «Merkblatt Informationssicherheit für KMUs», 2018[2]

Weitere Quellen sind entsprechend vermerkt.

[1] https://www.kmu.admin.ch/dam/kmu/de/dokumente/savoir-pratique/Informatique-et-IT/InfoSurance_10_Points_Programme_FR.pdf
[2] https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

1. Aufgaben, Kompetenzen, Verantwortlichkeiten

Sind Aufgaben, Kompetenzen und Verantwortlichkeiten für IT-Sicherheit nicht geregelt, ist dies ein Anzeichen dafür, dass dem Thema Cybersecurity nicht die nötige Bedeutung beigemessen wird.

Mehr als ein Drittel der Schweizer KMUs waren bereits von Cyberattacken betroffen, selbst kleine Betriebe wie Restaurants und Coiffeure sind potentielle Angriffsopfer[3].
Viele Unternehmen unterschätzen das Risiko[4] und schützen sich ungenügend. Voraussetzung für einen wirkungsvollen Grundschutz ist die Ernennung eines Cybersecurity-Verantwortlichen, der den Bereich IT-Sicherheit kompetent leitet. Gerade kleinere KMU können hier mit externen Expertinnen und Experten zusammenarbeiten.

Weiterführende Informationen

ISSS
Pflichtenheft für IT-Verantwortliche erstellen
Informationssicherheit für KMU, Punkt 1

MELANI
Organisatorische Massnahmen zur Definition von Verantwortlichkeiten
Merkblatt für KMUs, S. 2-3

2. Sensibilisierung von Mitarbeitenden, Kundinnen und Kunden, Lieferanten und Dienstleistern

Die besten technischen Massnahmen zum Schutz vor Cyberrisiken sind nutzlos, wenn die Mitarbeitenden die Sicherheitsrichtlinien und Verhaltensregeln nicht kennen, verstehen und richtig umsetzen.

Erste Priorität haben Schulungen zur Erkennung von E-Mails, die schädliche Software oder Links auf kompromittierte Webseiten enthalten. Die meisten digitalen Angriffe werden über E-Mails ausgeführt. Allen E-Mails mit Anhängen oder Links, die man unaufgefordert erhält, ist grundsätzlich zu misstrauen. Aber auch bei anderen einfachen Tätigkeiten, die praktisch alle Mitarbeitenden ausüben, lauern Gefahren, die oft unterschätzt werden. So beispielsweise beim Surfen im Internet oder durch schlecht gewählte Passwörter. Ist bösartige Software erst einmal im System, kann dies weitreichende finanzielle und rechtliche Folgen haben.

Weiterführende Informationen

ISSS
Richtlinien für IT-Benutzerinnen und -Benutzer bekannt machen
Informationssicherheit für KMU, Punkt 8

Mitarbeitende sensibilisieren
Informationssicherheit für KMU, Punkt 15

MELANI
Wie schütze ich mich?
Verhaltensregeln
Portal MELANI

[3] KMU reagieren zu wenig auf Cyberkriminalität, Publikation KMU Portal des Eidgenössischen Departements für Wirtschaft, Bildung und Forschung, WBF: Link zur Publikation
[4] Cyberrisiken in Schweizer KMUs: Schlussbericht 2017, Gemeinsame Studie von SVV, SQS, ICTswitzerland, ISSS, ISB, Expertenkommission Bund: Link zur Studie

3. Datenschutz-Richtlinien

Bei Datenverlust oder Datenschutzverletzungen drohen strafrechtliche Folgen, hohe Geldstrafen und ein schwerwiegender Imageverlust. Die Konsequenzen können unter Umständen existenzbedrohend sein.

Ihr Unternehmen ist verantwortlich für den sicheren Umgang mit vertraulichen und personenbezogene Daten und muss sich insbesondere an die Bestimmungen des Datenschutzgesetzes (DSG), Urheberrechtsgesetzes (URG) und Obligationenrechts (OR) halten. Bereits durch das Erstellen der Gästeliste für einen Betriebsanlass sammeln Sie personenbezogene Daten, die Sie schützen müssen. 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.

Weiterführende Informationen

ISSS
Vorgaben zu Vertraulichkeit einhalten
Informationssicherheit für KMU, Punkt 11

Daten vertraulich behandeln
Informationssicherheit für KMU, Punkte 13, 14

Eidg. Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Umgang mit personenbezogenen Daten
Portal EDÖB

Eidg. Departement für Wirtschaft, Bildung und Forschung WBF
Herausforderung DSGVO
KMU-Portal WBF

Economiesuisse
«DSGVO- Ist Ihr Unternehmen betroffen?»
Online-Check und Faktenblatt DSGVO

4. Passwort-Richtlinien und Benutzeradministration

Schwache und/oder mehrfach verwendete Passwörter sowie unklare Zugangs- und Administratorenrechte stellen ein erhebliches Sicherheitsrisiko dar, das leicht vermeidbar ist.

Leiten Sie Ihre Mitarbeitenden an, starke Passwörter zu verwenden und für jeden Dienst ein anderes Passwort zu nutzen. Verwenden Sie einen Passwortmanager, schreiben Sie die Passwörter nicht auf und geben Sie sie zu keiner Zeit an Dritte weiter. Nutzen Sie wo möglich Zwei-Faktor-Authentifizierung. Regeln Sie den Zugriff auf Daten durch eine übergeordnete Benutzeradministration, die Ihre Mitarbeitenden kennen, verstehen und konsequent einhalten. Beachten Sie dabei, dass jeder Benutzer, jede Benutzerin nur die notwendigsten Zugriffsrechte hat und löschen Sie diese beim Austritt von Mitarbeitenden aus dem Unternehmen.

Weiterführende Informationen

ISSS
Starke Passwörter verwenden
Informationssicherheit für KMU, Punkt 6

Zugriffschutz auf Daten regeln
Informationssicherheit für KMU, Punkt 12

MELANI
Wie schütze ich mich?
Verhaltensregeln
Portal MELANI

Passwortcheck
So testen Sie die Stärke Ihrer Passwörter
Portal Passwortcheck.ch

5. Aktueller Schutz vor schädlicher Software

Ein aktuelles Antivirus-Programm ist auf jedem IT-Gerät unverzichtbar und gehört zum Grundschutz gegen Viren, Würmer und Trojaner.

Computerviren gelangen oft clever getarnt über bekannte Absender per E-Mail-Anhänge ins System[5]. Schädliche Software kann so leicht in Ihr System gelangen und dort Daten zerstören, manipulieren und die gesamte IT-Infrastruktur lahmlegen. Schlecht geschützte Computer können zum Instrument für gezielte Angriffe von Hackern werden und schädliche Software weiterverbreiten. Dies gefährdet nicht nur Ihr Unternehmen, sondern auch Dritte.

Weiterführende Informationen

ISSS
Virenschutz-Programme aktuell halten
Informationssicherheit für KMU, Punkt 3

MELANI
Wie schütze ich mich?
Software und Einstellungen
Portal MELANI

Massnahmen auf technischer Ebene
Merkblatt für KMUs, S. 4-5

Liste Antivirensoftware
Website MELANI

6. Konfigurierte und aktualisierte Firewall

Der Einsatz einer leistungsfähigen Firewall verringert das Risiko von Angriffen erheblich. Zusammen mit der Antivirus-Software gehört sie zum Grundschutz für jedes IT-Gerät und ist oftmals kostenfrei als Zusatzsoftware von Antiviren-Programmen erhältlich.

Weiterführende Informationen

ISSS
Internetzugang mit Firewall schützen
Informationssicherheit für KMU, Punkt 4

MELANI
Wie schütze ich mich?
Software und Einstellungen
Portal MELANI

Informationen zur Firewall
Merkblatt für KMUs, S.6

[5] Publikation der Melde- und Analysestelle Informationssicherung MELANI zum Thema Schadsoftware: Zur Publikation

7. Mit dem Internet verbundene Geräte und Systeme aktuell halten

Werden Betriebssysteme, Antivirus-Software, Firewall und andere Anwendungen nicht aktuell gehalten, können Angreifer durch bekannte Sicherheitslücken eindringen. Daten können vernichtet und manipuliert werden oder Ihre Infrastruktur kann für kriminelle Zwecke missbraucht werden.

Bringen Sie Computer regelmässig auf den neusten Stand und überprüfen Sie alle Software-Produkte regelmässig auf Updates, um Sicherheitslücken zu schliessen – dies gilt auch für sämtliche mobile Geräte, die in Ihrem Firmenumfeld verwendet werden. Nutzen Sie wann immer möglich automatische Update-Funktionen. Legen Sie systematisch fest, in welchem Turnus alle Geräte diesbezüglich überprüft werden.

Weiterführende Informationen

ISSS
IT-Systeme überprüfen und warten
Informationssicherheit für KMU, Punkt 16

Software regelmässig aktualisieren
Informationssicherheit für KMU, Punkt 5

Mobile Geräte schützen
Informationssicherheit für KMU, Punkt 7

MELANI
Wie schütze ich mich?
Software und Einstellungen
Portal MELANI

8. Geschütztes und verschlüsseltes WLAN-Netzwerk

Ungesicherte und unverschlüsselte oder mit veralteten Protokollen gesicherte WLAN-Netzwerke ermöglichen Unbefugten und Hackern Zugang. Alle Geräte, die mit Ihrem WLAN verbunden sind, sowie die darauf gespeicherten Daten, können gelesen, manipuliert und für kriminelle Handlungen missbraucht werden.

Schützen Sie Ihr WLAN-Netzwerk durch Firewall, Verschlüsselung und mit starken Passwörtern. Richten Sie einen separaten Zugang für Ihre Kundinnen und Kunden sowie Gäste ein.

Weiterführende Informationen

ISSS
Internetzugang mit einer Firewall schützen
Informationssicherheit für KMU, Punkt 4

Mobile Datenträger und Übermittlung verschlüsseln
Informationssicherheit für KMU, Punkt 13

CHIP.de
5 Tipps, um den Internetzugang wirksam zu schützen
Website CHIP.de

MELANI
Wie schütze ich mich?
Geräte und Peripherie
Portal MELANI

9. Verschlüsselung von (Daten-) Übermittlung (z.B. VPN)

Vertrauliche Informationen und geschäfts- oder personenbezogene Daten können bei der Übermittlung in falsche Hände geraten.

Eine zuverlässige Verschlüsselung Ihrer Kommunikation sowie der Daten während der Übermittlung reduziert dieses Risiko.

Weiterführende Informationen

ISSS
Mobile Datenträger und Übermittlung verschlüsseln
Informationssicherheit für KMU, Punkt 13

Computerwoche
Methoden für die Verschlüsselung von Festplatten, E-Mail, Dateienübertragung
Website Computerwoche

10. Backup

Datenverluste sind nicht immer auf kriminelle Handlungen zurück zu führen, bereits ein Wasserschaden kann wichtige Daten und Informationen zerstören. Sichern Sie Ihre Daten regelmässig, um einen dauerhaften Datenverlust zu vermeiden – denn für manche Daten gilt eine gesetzlich vorgeschriebene Aufbewahrungspflicht.

Führen Sie eine regelmässige Datensicherung durch, die Sie an einem externen, geschützten Ort aufbewahren und überprüfen Sie regelmässig, ob sich die Daten von den Sicherheitsmedien zurückspielen lassen. Jedes KMU sollte täglich ein Backup erstellen. Definieren Sie einen Prozess, der regelt, in welchem Turnus Sie bestimmte Daten sichern und halten Sie sich konsequent daran.

Weiterführende Informationen

ISSS
Daten mit Backup sichern
Informationssicherheit für KMU, Punkt 2

MELANI
Wie schütze ich mich?
Software und Einstellungen
Portal MELANI

11. Mindestvorkehrung für die Notfallbewältigung

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

Legen Sie fest, wie sich Mitarbeitende im Notfall verhalten sollen und welche Aktionen auszulösen sind.Definieren Sie Rückfallebenen für einen vorübergehenden Totalausfall der IT, damit die wichtigsten Arbeiten weiterhin erledigt werden können. Bestimmen Sie Ansprechpersonen und stellen Sie deren Erreichbarkeit im Notfall sicher.

Weiterführende Informationen

ISSS

Für unterbruchsfreie Stromversorgung sorgen
Informationssicherheit für KMU, Punkt 17

Wichtige Elemente redundant halten
Informationssicherheit für KMU, Punkt 18

Notfallvorsorge planen
Informationssicherheit für KMU, Punkt 19

12. Outsourcing

Prüfen Sie, ob in den Verträgen mit Ihren Outsourcing-Partnern alle Punkte des Schnelltest geregelt sind.

Sie haben sich mit den wichtigsten Fragen für einen minimalen Cybersecurity-Schutz auseinandergesetzt. Eine Zusammenstellung mit weiterführenden Informationen – speziell für KMU – finden Sie auf www.cybersecurity-check.ch.

Impressum

Autoren:

Umberto Annino (ISSS) | Norbert Bollow (SNV) | Maya Bundt (SVV) | Daniel Caduff (BWL) | Lucius Dürr (SQS) | Xaver Edelmann (SQS) | Andreas Kaelin (ICTswitzerland) | Marcel Knecht (SNV) | Arié Malz (EFD) | Felix Müller (SQS) | Gunthard Niederbäumer (SVV) | Reinhard Niederer (Druckerei AG Suhr) | Peter Reber (SQS) | Daniel Rudin (ISB – MELANI) | Ronald Trap (SNV)

Redaktion:

Annalena Kassner (ICTswitzerland) | Lena Schneider (ICTswitzerland) | Adrian Sulzer (SATW) | Nicole Wettstein (SATW)