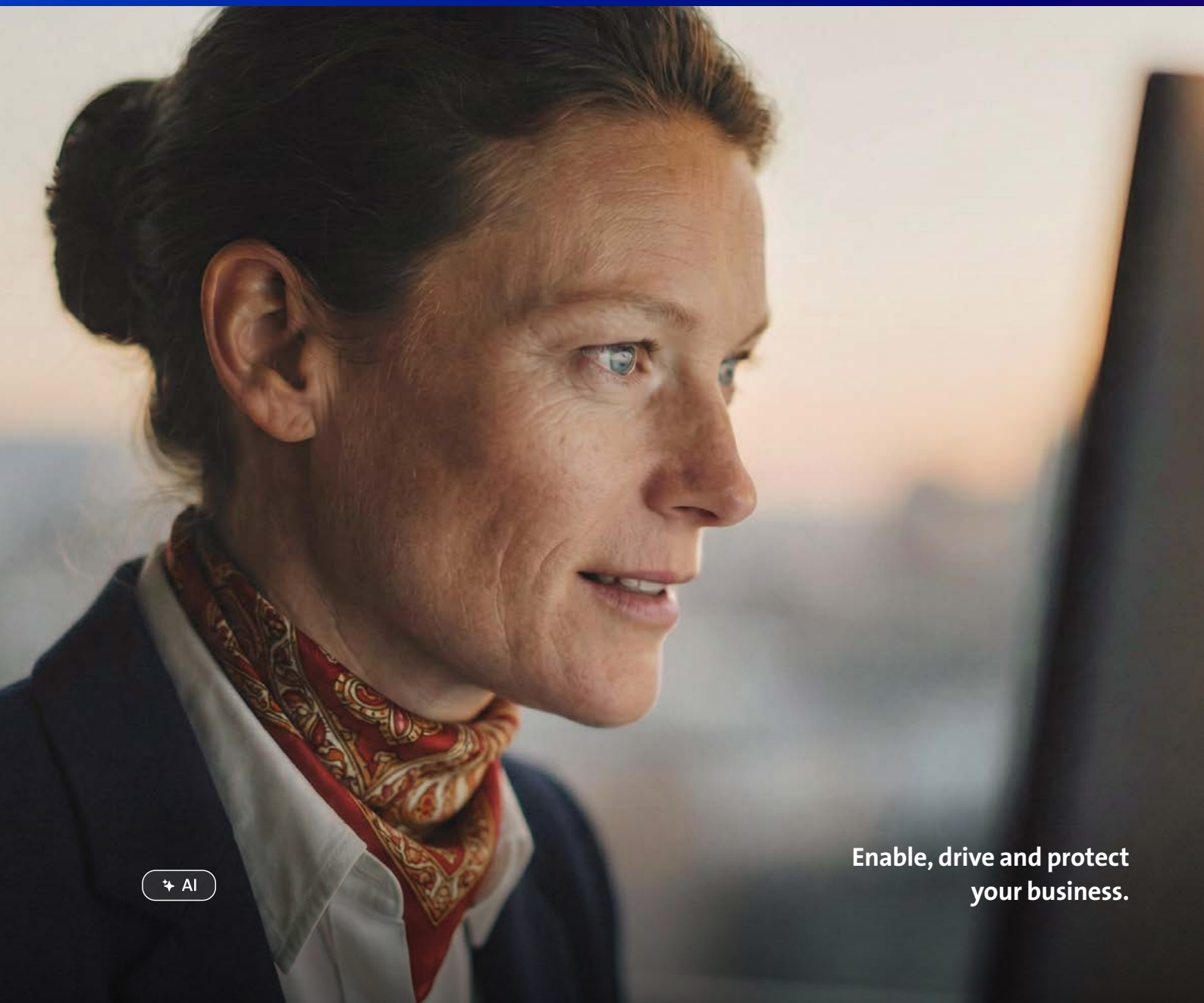
Ratgeber für Cybersicherheit



Cyberangriffe betreffen alle

Jedes sechste KMU wurde in den letzten fünf Jahren mindestens einmal oder gar mehrfach Opfer von einem Cyberangriff.[1]

Cyberkriminelle machen keinen Unterschied zwischen Gross und Klein. Cyberangriffe betreffen längst nicht mehr nur grosse Unternehmen. KMU sind mindestens genauso interessant für Angreifer, denn diese sind wegen mangelnden finanziellen Ressourcen und Know-how meist deutlich schlechter geschützt. Dank Automatisierungen und künstlicher Intelligenz spüren Angreifer ihre Opfer automatisiert auf.

[1] Quelle: AXA

Inhaltsverzeichnis

1 Die Kosten und Folgen eines Cyberangriffs

Die Folgen eines Cyberangriffs sind schwerwiegend. Das zeigt ein Beispiel eines KMU aus der Westschweiz, das Opfer eines Ransomware-Angriffs wurde. Die Kosten des Angriffs betrugen mehrere hunderttausend Franken – für Lösegeld, IT-Wiederaufbau und den vierwöchigen totalen Produktionsausfall.[1]

Betriebsunterbruch
Plötzlich steht das Tagesgeschäft still: Aufträge, Einsatzpläne, Kundendaten oder Rechnungen sind nicht abrufbar. In der Fertigung kann nicht produziert werden, der Aussendienst weiss nicht, bei welchen Kunden er welche Produkte oder Dienstleistungen erbringen muss, die Buchhaltung kann keine Rechnungen verschicken. Bereits eine Woche Betriebsunterbruch kann bei einem mittleren Unternehmen zu finanziellen Schäden in fünfstelliger Höhe führen.[2]

Wiederherstellung der IT
Nach einem Angriff haben Sie einen enormen Aufwand: Systeme bereinigen, Daten wiederherstellen, Ursachen analysieren, Zugänge neu absichern und alle Hintertürchen der Angreifer entfernen, damit diese wirklich nicht mehr im Netzwerk sind. Dazu benötigen Sie meist externe Security-Spezialisten, zusätzlich zu den IT-Fachpersonen in Ihrem Unternehmen oder bei Ihren Partnern. Die Wiederherstellung dauert meist mehrere Wochen und erfordert mehrere Security-Experten – pro Woche können so schnell Kosten von 20'000 Franken entstehen.

Verlust von Daten und geistigem Eigentum
Wenn Daten verschlüsselt, gelöscht oder abgeflossen sind, fehlt oft mehr als nur ein Dokument: Es gehen Projektstände, Kundeninformationen oder sensible Unterlagen verloren. Da Backups häufig lückenhaft, veraltet oder von den Angreifern ebenfalls verschlüsselt sind, können Daten oft nur teilweise rekonstruiert werden – aus E-Mails, gedruckten Dokumenten oder mittels Nachfragen bei Partnern und Kunden. Daten landen dabei oft im Darknet, vor allem Kundeninformationen, Benutzer- und Logindaten, aber auch Patente und andere Geschäftsgeheimnisse.

Reputations- und Rechtsfolgen
Cybervorfälle können Sie selten verheimlichen. Kunden und Partner kriegen mit, wenn Ihr Betrieb stillsteht, Sie nicht mehr ausliefern oder kommunizieren können. Zudem sind Sie verpflichtet, sowohl Ihre Kunden als auch das Bundesamt für Cybersicherheit zu informieren, wenn ein Cybervorfall personenbezogene Daten betrifft – was bei den allermeisten Cyberangriffen der Fall ist. Unternehmen, die zur kritischen Infrastruktur gehören, müssen sämtliche Cybervorfälle melden. Diese Meldepflicht führt zu erheblichen Aufwänden bezüglich Dokumentation und kann auch rechtliche oder behördliche Konsequenzen haben. Häufig vergessen wird der Reputationsschaden, den Sie als Unternehmen bei Ihren Kunden und Partnern durch einen Cybervorfall erleiden.

[1] Quelle: Tagesanzeiger
[2] Quelle: AXA

2

So laufen Cyber-angriffe ab

Cyberkriminelle nutzen unterschiedliche Einfallstore und verschiedene Werkzeuge, um KMU anzugreifen. Dieses Kapitel gibt einen Überblick über gängige Einfallstore – also wo oder wie der Angreifer angreift, sowie typische Werkzeuge – also was sie nutzen, um Daten zu stehlen oder Schaden anzurichten.

2.1 Häufige Einfallstore von Cyberkriminellen

Cyberkriminelle finden viele Wege, um KMU anzugreifen.
Hier sind fünf typische Einfallstore:

1 **Phishing und Social Engineering**
Social Engineering ist der Überbegriff für Angriffe, bei denen Kriminelle mit unterschiedlichen Taktiken Menschen täuschen. Sie nutzen also keine technischen Schwachstellen, sondern unvorsichtige Mitarbeitende. Die bekannteste Taktik ist Phishing: gefälschte E-Mails oder SMS führen auf betrügerische Webseiten oder im Dateianhängen befindet sich versteckte Schadsoftware – häufig wird Phishing genutzt, um Benutzer auf gefälschte Login-Seiten zu leiten. Phishing ist heutzutage oft täuschend echt und gerade auf dem Smartphone oder in Eile hat man schnell auf einen bösartigen Link oder Anhang geklickt. Phishing ist mit 62% das häufigste Einfallstor von Cyberangriffen.[1]

2 **Fehlkonfigurationen und schlechte Einstellungen**
Fehlkonfigurationen entstehen oft durch Nachlässigkeit oder Unwissenheit. Beispiel dafür sind aus dem Internet zugreifbare Admin-Portale, öffentlich zugängliche Cloud-Speicher und SharePoint-Links, nicht geänderte Standardpasswörter auf Routern, Cloud-Konten oder Firewalls, zu weitreichende Benutzerrechte oder offene Ports in Firewalls. Solche vermeidbaren Lücken bieten Angreifern einfachen Zugriff auf Systeme, Daten und Geräte – ganz ohne komplexe Hacks.

3 **Physische Angriffe**
Eine oft unterschätzte Form von Cyberattacken sind Täter, die sich direkt Zugang zu Gebäuden oder Geräten verschaffen. Sie geben sich zum Beispiel als Techniker oder Lieferant aus und gelangen so in Büros. Dort können sie Geräte oder Dokumente entwenden, sich mit dem lokalen Netzwerk verbinden, präparierte USB-Sticks platzieren oder Abhörtechnik installieren. Ziel ist meist Betriebsspionage, das Sammeln sensibler Daten oder das Einschleusen von Schadsoftware. Schon eine unversperrte Bürotür, ein unbeaufsichtigter Laptop oder ein offener Netzwerkanschluss kann zum Einfallstor für Angreifer werden.

4 **Schwache Passwörter**
Angreifer lieben Logins, v.a. von Microsoft-Konten, Buchhaltungs-Softwares oder am besten gleich vom VPN-Zugriff. Dadurch erhalten sie Zugriff auf Unternehmensdaten und -systeme. Ein Passwort zu knacken ist einfacher, als man denkt: Cyberkriminelle nutzen dabei Listen aus dem Darknet mit bekannten Benutzernamen und Passwörtern aus früheren Hacks. Weil Benutzer gerne Passwörter mehrfach benutzen, kriegen Angreifer so einfach Zugriff auf unterschiedliche Logins. Alternativ nutzen Angreifer «Brute Force», d.h. lassen ein Computerprogramm automatisiert jede denkbare Kombination von Buchstaben, Zahlen und Zeichen durchprobieren – viele Passwörter sind innert Minuten geknackt. Selbst bei Multifaktor-Authentifizierung (MFA) über SMS-Codes oder Apps haben Angreifer Wege gefunden, diese zu hacken.

5 **Veraltete Software**
Jedes System kann Schwachstellen haben: das Windows Ihres Laptops, Android Ihres Smartphones, die Maschinensteuerung Ihrer Produktionsanlage, das Server-Betriebssystem oder Ihre Firewall. Mit 21% sind Schwachstellen das zweithäufigste Einfallstor und führen in 68% zur Installation von Schadsoftware durch die Angreifer.[1] Durch bekannte Schwachstellen können Angreifer beispielsweise Login-Mechanismen umgehen, aus der Ferne auf das System zugreifen, sich Admin-Rechte verschaffen oder Schadsoftware ausführen. Darum liefern die Anbieter regelmässig Security-Updates, die solche Schwachstellen schliessen. Wer diese Updates nicht installiert, macht es Angreifern einfach, diese auszunutzen. Cyberkriminelle scannen das Internet automatisch nach Systemen, Geräten und Software, die nicht aktuell sind und bekannte Sicherheitslücken aufweisen – ähnlich wie ein Dieb, der systematisch durch Quartier läuft, und nach offenen Fenstern Ausschau hält.

[1] Quelle: ENISA Threat Landscape 2025

2.2 Die Werkzeugkiste der Cyberkriminellen

Haben Angreifer einmal ein Einfallstor gefunden, nutzen sie unterschiedliche Werkzeuge, um in Systeme einzudringen, Daten zu stehlen oder sie unbrauchbar zu machen. Die Werkzeuge sind die Mittel, mit denen sie im Inneren Schaden anrichten oder den Angriff durchführen. Hier einige Beispiele – die Liste ist bei Weitem nicht abschliessend.

Ransomware
Schadsoftware, die Daten auf Computern oder Servern verschlüsselt und sie unbrauchbar macht. Häufig werden gleichzeitig auch Daten abgezogen (Double Extortion) oder auch Backups verschlüsselt (Triple Extortion). Die Angreifer fordern danach ein Lösegeld, oft in Kryptowährungen, um den Zugriff wieder freizugeben bzw. die Veröffentlichung von Daten zu verhindern. Bei KMU ist Ransomware in 88% der Cyberangriffe eine Komponente.[1]

Viren
Eine Schadsoftware, die sich selbständig kopiert, indem es sich in andere Programme oder Dateien einnistet. Viren können Daten löschen, verändern oder schwer zugänglich machen sowie Programme langsam machen oder zum Absturz bringen. Klassische Viren treten heute kaum noch isoliert auf. Ihre Funktionen – etwa Selbstverbreitung oder Dateiinjektion – sind meist Bestandteil komplexerer Schadsoftware wie Trojanern, Würmern oder Ransomware.

Spyware
Schadsoftware, die im Hintergrund Geräte ausspioniert und Daten sammelt (z. B. Kontakte, Mails, Dokumente, Passwörter) und an Angreifer übermittelt.

Keylogger
Schadsoftware, die sämtliche Tastatureingaben aufzeichnen – etwa Passwörter, Logins oder Texte – und diese an den Angreifer weiterleiten.

SEO Poisoning
Manipulation von Suchmaschinen-Ergebnissen, bei der Cyberkriminelle legitime oder kompromittierte Websites so optimieren, dass sie bei Suchanfragen möglichst weit oben erscheinen – um Nutzer gezielt auf schädliche Inhalte zu lenken. Solche Webseiten können einerseits vermeintlich nutzbare Tools zum Download anbieten, die in Wirklichkeit aber Schadsoftware sind, z.B. PDF-Konverter, VPNs oder Browser-Erweiterungen. Anderseits kann auch in legitimen Webseiten Schadcode eingebaut sein, der unbemerkt im Hintergrund heruntergeladen wird.

Cryptojacking
Schadsoftware, welche die Rechenleistung eines Gerätes nutzt, um Kryptowährungen zu schürfen, indem es komplizierte mathematische Probleme löst. Das kann dazu führen, dass der Lüfter des Gerätes stärker läuft als normal oder das Gerät langsam wird.

Botnets
Netzwerke aus infizierten Geräten (z.B. Computer, IoT- und Smarthome-Geräte, Drucker, Smart TVs), die von Angreifer ferngesteuert werden können. Sie werden genutzt, um z.B. Spam zu verschicken oder grosse Angriffswellen (Distributed Denial of Service, DDoS) durchzuführen.

Comand-and-Control Server (C2)
Viele Schadsoftware (z.B. Ransomware oder Trojaner) sind von Angreifern so programmiert, dass sie automatisch eine Verbindung zu einem sogenannten Command-and-Control Server des Angreifers aufbauen. Die Schadsoftware wartet so auf Anweisungen des Servers oder sendet gesammelte Daten an den Server. Der Angreifer kann über den C2 Anweisungen an die Schadsoftware schicken, z.B. den Befehl, Daten zu verschlüsseln.

[1] Quelle: Verizon Data Breach Investigation Report 2025

2.3 Beispiel eines Cyberangriffs

Cyberkriminelle sind kreativ. Sie kombinieren verschiedene Einfallstore und Werkzeuge, um Schritt für Schritt tiefer in Ihr Unternehmen einzudringen und Schaden anzurichten. Ein typischer Cyberangriff läuft beispielsweise wie folgt ab:

1. Phishing-Mail

Der Angreifer schickt ein täuschend echtes Phishing-Mail, das auf eine gefälschte Microsoft Login-Seite linkt. Der Benutzer gibt Benutzername und Passwort ein – und nun hat auch der Angreifer Zugriff.

2. Interne Verbreitung

Wegen Fehlkonfigurationen hat der gehackte Benutzer deutlich mehr Rechte, als nötig wäre. Der Angreifer nutzt dies, um sich im Netzwerk auszubreiten und seine Berechtigungen zu erhöhen und schlussendlich Admin-Rechte zu erlangen. Dadurch kann er Sicherheitsmechanismen wie Antivirus oder Backups deaktivieren.

3. Hintertürchen einrichten

Der Angreifer richtet sich einen dauerhaften Zugang zum Netzwerk ein, falls das Unternehmen das gehackte Benutzer-Login entdeckt. Das erreicht er beispielsweise durch Erstellen neuer Benutzerkonten, Ändern von bestehenden Konten oder die Installation von Fernwartungsprogrammen.

4. Datenanalyse und Datenklau

Der Angreifer erkundet das Netzwerk, identifiziert besonders wertvolle Geschäftsdaten und Backups und zieht Daten ab.

5. Verschlüsselung der Daten

Der Angreifer installiert Ransomware und verschlüsselt die Daten sowie die gefundenen Backups.

Ransomware as a Service von «LockBit»

Cyberkriminelle sind keine Einzeltäter, sondern ein gut organisiertes Netzwerk. LockBit ist eine der bekanntesten Ransomware-Gruppen weltweit und arbeitet nach dem Prinzip «Ransomware-as-a-Service». Das bedeutet: Die Gruppe stellt die Schadsoftware und Infrastruktur bereit, während sogenannte Affiliate-Partner die eigentlichen Angriffe durchführen.

Steckbrief zu LockBit

- 10–20 Mitarbeitende bei LockBit
- 200 Affiliate-Partner, die Angriffe durchführen
- 70-80% des Lösegeldes geht an Partner, der Rest an LockBit
- Jährliche Umsatz von USD 20 Mio. durch bezahltes Lösegeld

3

Was Sie jetzt konkret tun können

Cybersicherheit ist kein einzelner Schutzschild, sondern ein Zusammenspiel verschiedener Komponenten. Keine einzelne Massnahme kann umfassenden Schutz bieten – Sicherheit entsteht erst, wenn mehrere Schutzvorkehrungen ineinandergreifen und sich gegenseitig absichern.

Wird eine Barriere überwunden, verhindern andere, dass ein Angriff grösseren Schaden anrichtet. Wenn also eine Schutzmassnahme einmal versagt – etwa, weil ein Passwort in falsche Hände gerät oder ein Angreifer eine Sicherheitslücke entdeckt – verhindern andere Vorkehrungen, dass der Angreifer Zugriff auf Unternehmensdaten oder auf das ganze Unternehmensnetzwerk bekommt. Dieser mehrstufige Ansatz sorgt dafür, dass aus einem Fehler kein Desaster wird.

Die folgenden **fünf Themenbereiche** zeigen Ihnen, wie Sie robuste, aufeinander abgestimmte Sicherheitsmassnahmen aufbauen können – so, dass Ihr Unternehmen auch dann geschützt bleibt, wenn irgendwo eine Schwachstelle übersehen wird.

3.1 Cybersicherheit in der Geschäftsführung verankern

Cybersicherheit funktioniert nicht, wenn die Geschäftsleitung lediglich darauf vertraut, dass IT oder externe Partner sich darum kümmern. Wer Verantwortung, Massnahmen und Prioritäten nicht festlegt, reagiert meist erst im Krisenfall. Und spätestens dann wird es zur Chefsache – denn wenn Ihr Betrieb stillsteht, sind Sie und Ihre Geschäftsführung betroffen – nicht Ihr IT-Partner.

Darum gehört Cybersecurity in die Führungsagenda. Heisst nicht, dass Sie Cybersecurity im Detail verstehen müssen oder gar umsetzen – aber Sie sollten einen Überblick Ihrer Risiken haben, Verantwortlichkeiten und Aufgabenbereiche klären, den aktuellen Fokus Ihrer Massnahmen definieren und folgende Punkte regelmässig prüfen.

«Wenn Ihr Betrieb stillsteht, ist die Geschäftsführung betroffen – nicht der IT-Partner.»

Siegfried Bernath,
Security-Berater für KMU bei Swisscom

Ihre Checkliste

- **Cybersecurity in der Geschäftsleitung verankern**
  Cybersecurity ist ein fixes Traktandum in jeder Geschäftsleitungssitzung, nicht erst nach einem Vorfall. Risiken und Schwachstellen sind den Geschäftsleitungsmitgliedern bewusst und Sie haben ein Budget für Security-Massnahmen.
- **Massnahmenpakete definieren, priorisieren und prüfen**
  Die Geschäftsleitung definiert Massnahmen bzw. Aufgabenpakete, priorisiert diese und kontrolliert deren Status.
- **Verantwortlichkeiten klar definieren**
  Es ist klar definiert, wer was macht und was zum Aufgabenbereich der Zuständigen gehört. Es ist klar geregelt, was der Partner und was die interne IT macht. Es ist geregelt, wer was entscheiden darf und soll – v.a. im Krisenfall.
- **Sicherheitsrichtlinien definieren**
  Sicherheitsvorschriften sind schriftlich definiert und intern kommuniziert. Dazu gehören z.B. die Pflichten im Umgang mit Kundendaten, Passwortrichtlinien, Nutzung von privaten Geräten, Nutzung von Online-Services wie Dropbox oder ChatGPT.
- **Mitarbeitende schulen**
  Mitarbeitende werden zu Cyberangriffen sensibilisiert. Dazu gehört u.a., dass Mitarbeitende Cyberangriffe erkennen können und wissen, wie und wo sie einen Cyberangriff melden müssen.

3.2 Geräte von Mitarbeitenden schützen

Jedes Arbeitsgerät ist ein mögliches Einfallstor: Laptop, Smartphone oder Tablet. Je mobiler der Arbeitsalltag, desto wichtiger ist es, Geräte konsequent zu schützen. Im Büro, im Homeoffice und unterwegs.

Smartphones werden dabei häufig übersehen – sie werden aber immer häufiger zum Ziel von Cyberkriminellen. Die Angriffe auf Smartphones sind im Jahr 2025 um 29% gestiegen.[1] Bei vielen Firmen nutzen Mitarbeitende Smartphones, um auf Geschäftsdaten wie Mails, Kalender oder Dokumente zuzugreifen – häufig über private Geräte, die meist noch schlechter geschützt sind als Firmengeräte. Häufige Risiken bei Smartphones sind, dass Benutzer schädliche Apps von Webseiten oder inoffiziellen App-Stores herunterladen, bösartige Anhänge in Mails öffnen oder Schwachstellen im Betriebssystem. Die wenigsten Smartphones und Tablets haben einen Schutz vor Phishing und Schadsoftware. 50% der Smartphones haben ein veraltetes Betriebssystem und 25% der Geräte sind so alt, dass sie keine Updates mehr vom Hersteller erhalten.[2]

Der Schutz von Geräten ist für viele KMU eine Herausforderung, da sie häufig darauf angewiesen sind, dass ihre Mitarbeitenden sorgfältig mit den Geräten umgehen und selbst auf deren Sicherheit achten. Eine Geräteverwaltung kann hier Abhilfe schaffen – sie ermöglicht, alle Computer, Smartphones und Tablets zentral zu verwalten, aktuell zu halten und zu schützen – leider sind Geräteverwaltungslösungen gerade für kleine Unternehmen häufig zu teuer.

Ihre Checkliste

- **Alle Geräte aktuell halten**
  Betriebssysteme (Android, Windows, iOS) auf allen Computern, Tablets und Smartphones sind stets aktuell.
- **Software auf Geräten aktuell halten**
  Nicht nur das Betriebssystem des Gerätes, sondern auch alle darauf installierten Tools sind stets aktuell, z.B. Browser, Office-Programme, Fachanwendungen und Apps.
- **Nur firmenintern geprüfte Anwendungen nutzen**
  Mitarbeitende nutzen nur Anwendungen oder Tools, die von Ihrem Unternehmen geprüft und freigegeben sind. Programme wie Video-Player, ZIP-Software oder Browser-Erweiterungen sollten nicht eigenständig installiert werden, da sie Schadsoftware enthalten oder unbemerkt Sicherheitslücken öffnen können.
- **Schutz vor Phishing und Schadsoftware**
  Alle Dateien, die über das Internet, einen USB-Stick oder per Mail auf ein Gerät gelangen, werden auf überprüft, z.B. mit einer Antivirus-Software sowie Spam- und Phishing-Filter auf Ihrem E-Mail-Dienst. Diese Schutz-Software sollte mehrmals täglich aktualisiert werden. Denken Sie unbedingt an Smartphones und Tablets!
- **Geräte mit Login schützen**
  Alle Computer, Tablets und Smartphones sind mit Login geschützt z.B. mit PIN, Passwort oder biometrischem Schutz. Bei einer bestimmten Inaktivität auf dem Gerät, sperrt sich das Gerät automatisch.
- **Geräte aus der Ferne löschen können**
  Geräte können aus der Ferne gelöscht werden, für den Fall, dass ein Gerät gestohlen wird oder verloren geht, z.B. über eine zentralisierte Geräteverwaltung.
- **Speicher von Geräten verschlüsseln**
  Die Festplatte oder der interne Speicher aller Geräte ist verschlüsselt, damit Dritte Daten auf dem Gerät nicht einfach auslesen können, z.B. manuell beim Aufsetzen des Gerätes oder über eine Geräteverwaltung.

[1] Quelle: Kaspersky Mobile Statistics Q2 2025
[2] Quelle: Zimperium Global Mobile Threat Report 2025

3.3 IT-Infrastruktur und Standorte schützen

Die IT-Infrastruktur – Server, Datenbanken, Cloud-Dienste, Business-Anwendungen – bildet das Rückgrat jedes Unternehmens. Darauf haben es die meisten Angreifer abgesehen: Sie wollen Ihre Daten stehlen oder Ihren Betrieb zum Stillstand bringen.

Angriffe lassen sich mit keiner Lösung gänzlich verhindern. Ziel ist es daher nicht nur, Angriffe abzuwehren, sondern auch, ihre Ausbreitung zu verhindern und kritische Systeme besonders abzusichern. Hier fühlen sich viele KMU in falscher Sicherheit, weil sie eine Firewall haben. Firewalls schützen aber meist nur den Übergang von aussen ins Netzwerk, aber nicht innerhalb des Netzwerks. Zudem bieten sie meist keinen Schutz vor Phishing und Schadsoftware und bei vielen KMU werden Firewalls nur sporadisch aktualisiert. Regelmässige Updates für alle Systeme sind grundsätzlich ein Muss. Denn bekannte Schwachstellen in Firewalls, Server-Betriebssystemen und Anwendungen machen es Angreifern einfach.

Zu einem wirksamen Schutz der IT-Infrastruktur und von lokalen Standorten und Netzwerken gehört ein Mix aus Security-Massnamen, unter anderem eine aktuelle, moderne Firewall, klar getrennte Netzwerkbereiche sowie regelmässige Updates.

«Viele Firewalls werden oft monate- oder jahrelang nicht aktualisiert.»

Siegfried Bernath,
Security-Berater für KMU bei Swisscom

Limitierungen klassischer Firewalls

- Schützt meistens nur am Standort oder wenn der Benutzer per VPN mit dem Firmennetzwerk verbunden ist
- Kein Schutz vor Phishing
- Limitierter Schutz vor Schadsoftware – Dateien, E-Mails oder Programme werden nicht geprüft, nur verdächtiger Datenverkehr blockiert
- Kein Schutz vor Angreifern, die bereits im Netzwerk sind
- Fehlende oder späte Updates machen die Firewall verwundbar
- Falsche Konfigurationen sind eine häufige Schwachstelle

Ihre Checkliste

- **Moderne, stets aktuelle Firewall – oder eine alternative Lösung**
  Eine moderne Firewall schützt Standorte und alle dort verbundenen Geräte und Mitarbeitenden umfassend vor Gefahren. Die Firewall ist stets aktuell.

- **Nur absolut notwendige Dienste ins Internet exponieren**
  Nur Dienste, die von extern zugreifbar sein müssen, sind ins Internet exponiert (z.B. Kundenportal, VPN-Zugriff oder Mail-Dienste). Dazu werden selektiv Ports für diese Dienste auf der Firewall geöffnet und mit starken Zugriffsmechanismen abgesichert. Alle anderen Ports sind geschlossen und nicht aus dem Internet zugreifbar, z.B. veraltete Dateiablagen, Zugriffe für Fernwartung, Verwaltungsoberflächen für Router oder Drucker.

- **Netzwerk in sichere Bereiche aufteilen (Netzwerksegmentierung)**
  Je nach Unternehmen ist es sinnvoll, ein Netzwerk in mehrere Bereiche aufzuteilen z.B. für Unternehmensbereiche (Produktionsanlagen, Server, Büro-PCs), Gäste-WLAN oder für Systeme mit besonders schützenswerten Daten (Lohnbuchhaltung, Kundendaten oder Patente). So kann sich ein Angriff weniger einfach im ganzen Unternehmen ausbreiten und zentrale Systeme sind besser geschützt.

- **Server und Systeme stets aktuell halten**
  Updates und Sicherheits-Patches für Server, Datenbanken oder selbstverwaltete Clouds werden zeitnah installiert.

- **Business-Software stets aktuell halten**
  Security-Updates von Business-Anwendungen werden zeitnah eingespielt. Business-Anwendungen, die keine Security-Updates erhalten, sollten abgestellt, erneuert oder isoliert betrieben werden.

- **Sichere Konfiguration von Systemen und Anwendungen**
  Konfigurationen – von Computer-Betriebssystemen, Netzwerkgeräten, Cloud-Umgebungen oder Microsoft 365 – werden sorgfältig gemacht und von Experten geprüft. Mögliche Konfigurationsanpassungen sind z.B. Security-Standardeinstellungen, nicht benötigte Dienste abschalten, Logging und Monitoring aktivieren.

- **WLAN schützen**
  Auch beim WLAN ist ein starkes Passwort notwendig. Die Verschlüsselung ist aktiviert (WPA2 oder WPA3), damit nicht jeder in Funkreichweite Ihren Datenverkehr mithören kann. Gäste nutzen ein separates WLAN, das vom Unternehmensnetzwerk getrennt ist.

3.4 Zugriffe und Berechtigungen einschränken

32% der Cyberangriffe nutzen Login-Daten von Benutzerkonten.[1] Es sind also keine komplexen Hacks, sondern schwache Passwörter, im Darknet gekaufte Zugangsdaten aus früheren Hacks oder ein nie geänderten Standardpasswort.

Ein gutes Zugriffsmanagement bedeutet klare Zuordnung: Jede Person hat ihr eigenes Login, starke Authentifizierungsmethoden, jeder Zugriff ist nachvollziehbar und jede Berechtigung ist gerechtfertigt. Das schützt nicht nur vor Angriffen, sondern auch vor internen Fehlbedienungen oder Datenverlust.

Bei Zugriffen wird zunehmend das Zero-Trust-Prinzip angewendet. Jeder Zugriff auf Business-Software – z.B. die Buchhaltungssoftware, M365 oder das ERP – wird geprüft, auch wenn der Zugriff aus dem lokalen Netzwerk am Standort erfolgt. Jeder Zugriff wird umfassend geprüft – nicht nur mit Benutzername und Passwort, sondern auch der Kontext, beispielsweise der geografische Ort des Zugriffs oder von welchem Gerät.

Besonders für KMU gilt: Zugriffe sind die erste Verteidigungslinie. Wenn diese Linie sauber und diszipliniert umgesetzt ist – mit starken Login-Mechanismen, kontextbasiertem Zugriff und minimalen Rechten – können Sie viele Cyberangriffe abwehren oder den Schaden eines Angriffs eindämmen.

Was sind Passkeys?

Passkeys ersetzen Passwörter durch digitale Schlüsselpaare, die sicher auf den Geräten Ihrer Mitarbeitenden, im einem Passwort-Manager oder auf einem physischen Stick gespeichert sind. Das Login erfolgt einfach per Fingerabdruck, Gesichtserkennung oder PIN – kein Passwort nötig.

Da der private Schlüssel das Gerät nie verlässt bzw. nicht über das Internet übermittelt wird, sind Phishing und Kontoübernahmen praktisch ausgeschlossen. Das Ergebnis: schnellere Logins, weniger Verwaltungsaufwand und deutlich höhere Sicherheit.

[1] Quelle: IBM X-Force Threat Intelligence Index 2026

Ihre Checkliste

- **Für jeden Mitarbeitenden sein eigenes Login**
  Keine geteilten Logins – jeder Mitarbeitende hat für jedes Tool sein persönliches Login.

- **Einmalige, starke Passwörter – oder Passkeys**
  Jedes Passwort wird nur einmal verwendet. Passwörter sind lang und stark – oder noch besser: Passkeys. Passwörter gehören nicht auf Post-it oder in Excel-Listen, sondern höchstens in einen sicheren Passwortmanager.

- **Multifaktor Authentifizierung bei kritischen Anwendungen**
  Bei kritischen Anwendungen (z.B. Passwort-Manager, Microsoft-Login, Buchhaltungssoftware) nutzen Sie zusätzlich zum Passwort einen zweiten Faktor, z.B. ein SMS-Code, Authenticator-Apps oder Passkeys.

- **Zugriffsrechte und Berechtigungen minimieren**
  Mitarbeitende haben nur Zugriff auf Daten und Systeme, die sie wirklich brauchen. Nicht alle Mitarbeitenden müssen auf Buchhaltungssoftware, CRM oder die ganze Dateiablage zugreifen können. Berechtigungen auf Geräten sind eingeschränkt, sodass Benutzer nicht einfach Programme installieren können.

- **Zugriffe basierend auf Kontext einschränken**
  Nur Benutzername und Passwort reichen nicht, um sich einzuloggen. Kontext-Informationen, z.B. von welchem Gerät, Ort oder zu welcher Zeit ein Login erfolgt, werden genutzt, um Zugriffe einzuschränken, z.B. keine Zugriffe auf das CRM aus dem Ausland, kein Zugriff auf Admin-Tools ausserhalb des Standortes.

- **Standardpasswörter sofort ändern**
  Vom Hersteller gesetzte Standardpasswörtern auf IT-Geräte und -Tools werden sofort und vor der Inbetriebnahme geändert, z.B. auf Firewalls, Drucker, Routern. Passwörter werden nicht als Klartext in Business-Software oder Automatisierungen gespeichert.

3.5 Gewappnet sein für den Ernstfall

Keine Security-Lösung gibt Ihnen 100%-ige Sicherheit.
Seien Sie also gewappnet für den Ernstfall.

Angreifer tummeln sich meist ein paar Stunden bis mehrere Monate in einem System rum, bis sie zuschlagen.[1] Die effektive Verschlüsselung der Daten dauert dann nur noch wenige Minuten oder Stunden – das machen Cyberkriminelle oft freitag-abends, am Wochenende oder an Feiertagen.

Darum sind zwei Punkte wichtig:

1. **Überwachen Sie Ihre Systeme kontinuierlich,** um Auffälligkeiten frühzeitig zu erkennen und Krisen möglichst zu verhindern. Stellen Sie sicher, dass zuständige Personen jederzeit informiert sind.
2. **Im Ernstfall wird sofort ein Alarm ausgelöst,** sodass Ihre Spezialisten unverzüglich reagieren können.

«Die Wiederherstellung von Systemen ist komplex und aufwändig, da zuerst sämtliche Hintertürchen der Angreifer gefunden und beseitigt werden müssen.»

Adrian Kress,
Security-Experte bei Swisscom

Ihre Checkliste

- **Regelmässige Backups nach dem 3-2-1 Prinzip mit mehreren physisch getrennten Kopien**
  Mindestens 3 Backups, auf 2 unterschiedlichen Speichermedien, davon 1 Kopie extern (z.B. Cloud oder anderer Standort). Backups werden wöchentlich, einmal oder mehrmals täglich durchgeführt – je nach Anforderung Ihres Unternehmens.
- **Automatische Überwachung von sicherheits-relevanten Aktivitäten**
  Analysieren Sie den Datenverkehr und Aktivitäten in Ihrem Firmennetzwerk automatisiert. Stellen Sie sicher, dass die zuständige Person bei Auffälligkeiten benachrichtigt wird. Nutzen Sie dafür z.B. ein Monitoring-Tool oder einen externen Dienstleister.
- **Klar definierter und schriftlicher Notfallplan**
  Im Notfall ist klar, wer was macht, wer was entscheiden darf und muss. Verantwortlichkeiten sind klar definiert, z.B. wer wann wen informiert, wer welche Systeme abschalten darf, welche externen Security-Experten im Notfall involviert werden.
- **Regelmässiges Üben des Notfallszenarios**
  Sie üben den Ernstfall regelmässig und testen, ob die Wiederherstellungsmechanismen wirklich funktionieren, z.B. Wiederherstellen eines vollständigen Backups testen, Wiederherstellen einzelner kritischer Anwendungen üben und Durchspielen der Alarm- und Kommunikationskette.
- **Unterstützung durch Security-Experten im Krisenfall**
  Sie wissen, wen Sie sich im Krisenfalls zur Hilfe holen, denn hier ist meist spezifisches Security-Wissen benötigt. Security-Experten helfen Ihnen, alle Systeme und Konfigurationen wieder zu bereinigen und sämtliche «Hintertürchen» der Angreifer zu entfernen.

[1] Quelle: Barracuda Threat Report 2026

4

Cybersicherheit jetzt pragmatisch anpacken

Der Security Markt ist riesig und undurchsichtig. Viele Anbieter versprechen «Rundumschutz», auch wenn sie in Wirklichkeit nur einen kleinen Security-Bereich abdecken: Es gibt keine einzelne Lösung, die alle Risiken abdeckt. Verschiedene Lösungen schützen oft vor derselben Bedrohung – aber auf unterschiedliche Art und Weise und mit ihren eigenen Limitierungen.

Genau darum braucht es ein abgestimmtes Zusammenspiel von Security-Lösungen: Mehrere Bausteine, die sich ergänzen statt überschneiden. Für KMU heisst das: Sie brauchen keine zwanzig High-End-Lösungen, sondern drei bis fünf aufeinander abgestimmte Tools, welche mit vertretbarem Aufwand die meisten Ihrer Risiken abdecken.

Unser Angebot

Swisscom hilft Ihnen, in diesem Security Dschungel den Überblick zu bewahren – ohne dass Sie selbst IT-Sicherheitsprofi werden müssen. Mit wenigen, auf Schweizer KMU zugeschnittenen Lösungen, die sich optimal ergänzen.

beem

Unsere Sicherheitslösung «beem» vereint zentrale Sicherheitsfunktionen in einer einfachen Lösung – speziell konzipiert für KMU.

✓ Sicher surfen

Anonym im Internet surfen sowie Schutz vor Phishing und Schadsoftware – von überall und jedem Gerät.

✓ Geschützte Standorte

Schutz Ihrer Unternehmensstandorte und aller Geräte vor Ort – stärker als jede klassische Firewall.

✓ Geschützte Geräte

Computer, Tablets und Smartphones zentral verwalten, schützen oder aus der Ferne löschen.

✓ Sichere Zugriffe

Von überall sicher auf Unternehmensdaten zugreifen, mit starken Logins und genauer Einstellung und Prüfung von Zugriffen – sicherer als VPNs.

✓ Immer aktuell

Das Sicherheitswissen von über 300 Security-Fachpersonen von Swisscom stellt sicher, dass beem täglich aktuell ist.

→ **beem entdecken**

Backup

Automatisierte Datensicherung auf Schweizer Cloud-Servern von Swisscom und Wiederherstellung der Backups bei Verlust durch IT-Experten.

Mitarbeiter-Schulungen

Sensibilisierung Ihrer Mitarbeitenden durch Online-Schulungen, Phishing-Simulationen sowie Erfolgsmessung und Reporting.

Früherkennung von Cyberangriffen

Automatisierte Überwachung der Datenströme von beem und Alarmierung Ihrer Fachpersonen durch unsere Security-Experten.

Soforthilfe bei Cyberangriffen

Unterstützung durch unsere Security-Experten im Angriffsfall inklusive Forensik und Wiederherstellung Ihrer Systeme.

Lassen Sie sich beraten

→ **Kontaktformular**

Gratis-Telefonnummer: 0800 000 515