IT-Unternehmenssicherheit:
Ein einfacher Leitfaden für KMU

Viele kleine und mittlere Unternehmen glauben, Unternehmenssicherheit sei nur etwas für Konzerne mit grossen Budgets und eigenen Security-Abteilungen. Die Realität ist meist einfacher: Die meisten Vorfälle entstehen nicht durch hochkomplexe Angriffe, sondern durch fehlende Zuständigkeiten, schwache Passwörter, mangelnde Awareness, fehlende Prozesse oder schlicht Zeitdruck. Dieser Leitfaden soll helfen, die eigene Sicherheitslandschaft mit einfachen Mitteln strukturiert zu überprüfen.

Unser Grundsatz: Sicherheit muss praktikabel sein

Ein gutes Sicherheitsniveau bedeutet nicht maximale Kontrolle oder maximale Technik. Ein gutes Sicherheitsniveau bedeutet:

- Risiken verstehen und kritische Bereiche erkennen
- Einfache Schutzmassnahmen konsequent umsetzen
- Verantwortlichkeiten klar definieren
- Im Ernstfall jederzeit handlungsfähig bleiben

Der 15-Minuten-Selbsttest

Wenn Sie mehrere der folgenden Fragen mit „Nein“ beantworten, besteht in Ihrem Unternehmen akuter Handlungsbedarf:

- **Zuständigkeit:** Gibt es im Unternehmen eine klar verantwortliche Person für Sicherheitsthemen?
- **Passwörter:** Werden Passwörter sicher verwaltet und regelmässig geändert?
- **Schutzfaktor:** Ist die Multi-Faktor-Authentifizierung (MFA) überall aktiviert?
- **Datensicherung:** Gibt es regelmässige Datensicherungen (Backups)?
- **Funktionstest:** Werden diese Backups auch regelmässig auf ihre Wiederherstellung getestet?
- **Sensibilisierung:** Wissen alle Mitarbeitenden, wie eine Phishing-Mail aussieht?
- **Verdachtsfälle:** Gibt es klare, bekannte Prozesse bei einem Sicherheitsverdacht?
- **Offene Zugänge:** Sind alle Zugänge ehemaliger Mitarbeitenden konsequent deaktiviert?
- **Dokumentation:** Werden kritische Zugänge und Administrator-Rechte dokumentiert?
- **Notfall:** Gibt es einen sofort erreichbaren Notfallkontakt für IT- und Cybervorfälle?

Netfon Solutions AG
info@netfon.ch
www.netfon.ch

Thurgauerstrasse 119
8152 Glattpark (Opfikon)
+41 44 497 11 11

Samstagernstrasse 45
8832 Wollerau
+41 43 888 00 22

Häufige Fragen und Antworten zur Unternehmenssicherheit

Was sind die häufigsten Schwachstellen in kleinen und mittleren Unternehmen?

Es sind meist vier klassische Schwachpunkte, die Angreifern das Leben leicht machen:

1. **Schwache Passwörter:** Einfache oder mehrfach verwendete Passwörter zählen nach wie vor zu den grössten Risiken. *Unsere Empfehlung:* Nutzen Sie konsequent einen Passwortmanager, aktivieren Sie MFA und trennen Sie private sowie berufliche Passwörter strikt.
2. **Keine klaren Zuständigkeiten:** Oft fühlt sich „irgendwie jeder" zuständig – tatsächlich aber niemand. *Unsere Empfehlung:* Definieren Sie eine feste verantwortliche Person, legen Sie klare Eskalationswege fest und dokumentieren Sie Notfallkontakte.
3. **Fehlende Awareness:** Mitarbeitende sind keine Schwachstelle – wenn man sie richtig vorbereitet. *Unsere Empfehlung:* Setzen Sie auf kurze, verständliche Sensibilisierungen mit praxisnahen Beispielen statt auf Angstkommunikation.
4. **Ungeschützte Zugänge:** Offene Fernwartungen, alte Benutzerkonten oder fehlende Software-Updates sind häufige Einfallstore. *Unsere Empfehlung:* Deaktivieren Sie ungenutzte Konten sofort, halten Sie alle Software-Systeme aktuell und prüfen Sie externe Zugriffe regelmässig.

Müssen wir sofort in neue, teure Sicherheitssoftware investieren?
Nein, die meisten Unternehmen benötigen nicht sofort neue Technik. Sie benötigen zuerst klare Abläufe, eindeutige Verantwortlichkeiten und funktionierende Kommunikationswege. Selbst die beste und teuerste Technik hilft im Ernstfall wenig, wenn im Moment des Angriffs niemand weiss, wer die Entscheidungen trifft.

Wie sieht ein einfacher IT-Notfallplan für den Ernstfall aus?
Jedes Unternehmen sollte die folgenden fünf Punkte zwingend schriftlich festhalten und offline (ausgedruckt) griffbereit haben:

- **Wer entscheidet?** Definition der Geschäftsführung oder der verantwortlichen Person.
- **Wer wird informiert?** Liste für IT-Abteilung, externe Dienstleister, Kunden und Behörden.
- **Welche Systeme sind kritisch?** Priorisierung von ERP, E-Mail, Produktion, Telefonie und Buchhaltung.
- **Was passiert bei einem Ausfall?** Vorab definierte Ersatzprozesse für den Notbetrieb.
- **Wo liegen wichtige Kontakte?** Telefonnummern und Verträge müssen analog verfügbar sein.

Netfon Solutions AG
info@netfon.ch
www.netfon.ch

Thurgauerstrasse 119
8152 Glattpark (Opfikon)
+41 44 497 11 11

Samstagernstrasse 45
8832 Wollerau
+41 43 888 00 22

Warum wird die physische Sicherheit oft vergessen?
Unternehmenssicherheit bedeutet nicht nur Schutz vor Hackern aus dem Internet. Einbrecher oder unbefugte Besucher vor Ort können denselben Schaden anrichten. Achten Sie daher zwingend auf:

- Eine funktionierende Zutrittskontrolle und ein klares Besuchermanagement.
- Eine gelebte Clean-Desk-Policy (keine Passwörter auf Post-it's, keine sensiblen Dokumente auf dem Tisch).
- Sichere Schlüsselverwaltung und die geschützte Entsorgung von Dokumenten (Schredder).
- Reisesicherheit für Aussendienstmitarbeiter (z. B. Blickschutzfolien für Laptops).

Was ist „Social Engineering" und wie schütze ich mein Team?
Angreifer attackieren heute immer seltener direkt die IT-Systeme – sie manipulieren stattdessen Menschen. Typische Warnsignale für solche Angriffe sind künstlich erzeugter Zeitdruck, ungewöhnliche Zahlungsaufforderungen (bspw. der angebliche „Chef-Betrug" per Mail), spontane Passwortabfragen oder emotionale Druckmittel. Es gilt die goldene Grundregel: Lieber einmal zu viel intern nachfragen als einmal falsch reagieren.

Welche Sofortmassnahmen bringen den grössten Nutzen bei geringstem Aufwand?
Konzentrieren Sie sich für den Start auf diese 10 wirksamen Schritte:

1. Multi-Faktor-Authentifizierung (MFA) überall aktivieren
2. Zentralen Passwortmanager einführen
3. Regelmässige Updates für alle Systeme erzwingen
4. Das bestehende Backup-Konzept real testen
5. Mitarbeitende aktiv und praxisnah sensibilisieren
6. Alte und ungenutzte Zugänge konsequent entfernen
7. Sicherheitsverantwortliche Person benennen
8. Externe Zugriffe (VPN, Fernwartung) streng kontrollieren
9. Notfallkontakte schriftlich dokumentieren
10. Sicherheitsrelevante Prozesse einfach und verständlich festhalten

---

Fazit: Sicherheit ist kein Projekt, sondern ein Prozess
Unternehmenssicherheit ist keine einmalige Massnahme, die man abhaken kann. Bedrohungen verändern sich, Unternehmen wachsen und Prozesse passen sich an. Deshalb sollte IT-Sicherheit regelmässig überprüft, pragmatisch angepasst und wirtschaftlich vertretbar umgesetzt werden.
Die meisten Unternehmen benötigen keine hochkomplexen Sicherheitskonzepte. Sie benötigen Klarheit, Struktur, Awareness und einfache, umsetzbare Massnahmen. Mehr Sicherheit entsteht fast immer durch bessere Organisation, nicht durch zusätzliche Komplexität.

Gute Unternehmenssicherheit ist minimal invasiv, maximal effektiv und wirtschaftlich vertretbar.

Netfon Solutions AG
info@netfon.ch
www.netfon.ch

Thurgauerstrasse 119
8152 Glattpark (Opfikon)
+41 44 497 11 11

Samstagernstrasse 45
8832 Wollerau
+41 43 888 00 22