Cybersecurity 2025

Die Digitalisierung bietet enorme Chancen – für Unternehmen, Behörden und Privatpersonen. Doch sie birgt auch Risiken, die heute größer sind als je zuvor.

Moderne Cyberangriffe sind professionell, automatisiert und global vernetzt.
Wer glaubt, von Cyberkriminalität nicht betroffen zu sein, der irrt gewaltig.
Daten werden weltweit gesammelt, gespeichert und verkauft – häufig ohne Wissen der Betroffenen.
Viele Nutzer fühlen sich sicher, sind es aber nicht.

Clear Net, Deep Web und Darknet – Was steckt dahinter?

Das Internet besteht aus weitaus mehr als dem sichtbaren Teil, den wir täglich nutzen.
Die drei Ebenen:

- **Clear Net**: Öffentlich sichtbare Webseiten wie Google oder Microsoft
- **Deep Web**: Interne Unternehmensnetzwerke, Cloud-Datenbanken, geschützte Inhalte
- **Darknet**: Ein abgeschotteter Bereich, der mithilfe spezieller Software anonym nutzbar

Diese Struktur zeigt: Nur ein Bruchteil unserer digitalen Welt ist sichtbar – der Großteil befindet sich unter der Oberfläche und enthält riesige Mengen sensibler Daten.

Cyberangriffe? Ein globales Dauerfeuer

Wie bedrohlich die Situation ist, zeigen internationale Monitoring-Dienste:
Auf einer Weltkarte für Cyberbedrohungen laufen Angriffe permanent und weltweit – von privaten Hackern bis hin zu kriminellen Organisationen.

Ausserdem können angreifbare Systeme online leicht gefunden werden.
Tools wie shodan.io zeigen öffentlich erreichbare Geräte, Server, Überwachungskameras oder industrielle Steuerungen – oft ohne ausreichende Absicherung.

Für Angreifer war es noch nie so einfach, Sicherheitslücken aufzudecken und auszunutzen.

Passwörter: Das unterschätzte Risiko

Ein weiteres Problem: Schlechte oder wiederverwendete Passwörter.
Auf Plattformen wie dehashed.com oder weakpass.com sind gestohlene oder schwache Passwörter öffentlich einsehbar.

Daraus lässt sich ein klarer Trend ableiten:
Viele Angriffe müssen nicht einmal hochkomplex sein.
Oft reicht ein einziges Passwort – und ein Netzwerk fällt wie ein Kartenhaus zusammen.

Ransomware – wenn der Zugriff plötzlich weg ist

Einer der drastischsten Angriffsvektoren unserer Zeit heißt Ransomware.
Dabei werden Systeme verschlüsselt, Unternehmen lahmgelegt und Lösegeldforderungen gestellt.

Ransomware Statistiken belegen, dass Ransomware-Gruppen jeden Tag neue Opfer treffen und ihre Aktivitäten öffentlich im Darknet präsentieren. Das Geschäftsmodell dahinter ist erschreckend erfolgreich – und wächst weiter.

Was Unternehmen jetzt tun müssen: Defense-in-Depth Prinzip

Ein wichtiges Sicherheitskonzept: Defense in Depth – Sicherheit in mehreren Schichten.

Empfehlungen gibt es von
➢ ISO/IEC 27001
➢ IEC 62443
➢ BSI
➢ NIS-2-Richtlinie
➢ und viele weitere

Empfohlene Maßnahmen sind unter anderem:

- Netzwerksegmentierung
- Firewalls & Datendioden
- Physikalische Sicherheit
- Backup & Recovery

Diese Verteidigungspunkte bilden ein mehrstufiges Schutzsystem, das Cyberangreifern das Eindringen maximal erschwert.

Cybersecurity beginnt bei den Menschen

Neben Technik zählt vor allem eines: Bewusstsein.
Handlungsempfehlungen für Mitarbeiter:

- Absender überprüfen, bevor Anhänge geöffnet werden
- Besucher registrieren
- Sensible Informationen schützen
- Sicherheitsvorfälle sofort melden
- Fehlverhalten vermeiden, z.B. keine fremden USB-Sticks nutzen oder ungesicherte Webseiten öffnen

Fazit: Sicherheit ist kein Zustand, sondern ein Prozess

Cybersecurity ist kein Produkt, das einmal gekauft und dann vergessen werden kann.
Daten werden gesammelt, verkauft und missbraucht – weltweit und jederzeit.
Unternehmen wie Privatnutzer müssen akzeptieren, dass Angriffe nicht mehr die Ausnahme, sondern die Regel sind.
Sicherheit entsteht aus:

- Wissen
- Vorbereitung
- Kontinuierlichen Maßnahmen
- Verantwortungsbewusstsein

„Wenn du den Feind und dich kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten.“
Sunzi / Chinesischer General, Militärstratege und Philosoph um 500 v. Chr.

Wir kennen Cyber Security Experten

Die erfolgreiche Umsetzung eines Cybersecurity-Projektes benötigt nebst vielen Aspekten immer zwei Grundvoraussetzungen: Kompetenz und Kapazität.

Bei uns finden Sie Beides!

Planen Sie ein Projekt zur Optimierung der Cybersecurity und haben Sie Interesse, dieses mit uns durchzuführen?
Wir unterstützen Sie gern mit professionellen und qualitätsgeprüften Interim Managern und Beratern.

Über eine Kontaktaufnahme freuen wir uns.

hpm human power management ag
Brunnenrain 23
5735 Pfeffikon LU

+41 44 994 23 46
info@hpmag.ch
www.hpmag.ch