

Cybersecurity

Minimale Vorkehrungen – grosse Wirkung

Thurgauer Technologietage | 22. März 2019

Andreas Kaelin
Geschäftsführer ICTswitzerland
Präsident ICT-Berufsbildung Schweiz

Cyberisiken – Unbewusste Inkompetenz

Die zunehmende Vernetzung mit dem Internet ist eine Voraussetzung, um die Vorteile der Digitalisierung nutzen zu können. Dies erhöht die Risiken aus dem Cyberspace und bedingt, dass sich die Unternehmen sowie Privatpersonen mit Cyberisiken kompetent auseinandersetzen.

Repräsentative Studien zeigen

Überraschend hohes Sicherheitsgefühl

im Widerspruch

zur Schadensrealität

Beispiele: Digitale Überfälle (Trojaner, «CEO-Trick», Erpressung,...)

Repräsentative Umfrage bei 300 CEOs von KMU¹

- Risiko von Cyberangriffen wird stark unterschätzt
 - Die Mehrheit fühlen sich gut bis sehr gut geschützt
 - Nur 4% der CEOs sehen es als grosse oder sehr grosse Gefahr, durch einen Cyberangriff in der Existenz gefährdet zu werden
- Studienergebnisse zeigen eine andere Realität
 - Mehr als ein Drittel sind von Cyberattacken betroffen
 - Die Anzahl der von Erpressung betroffenen Firmen wird auf 23'000 (4%) geschätzt
 - Nur 60% geben an, Grundschutzmassnahmen wie Malware-Schutz, Firewall, Patch-Management und Backup voll und ganz umgesetzt zu haben
 - Systeme zur Erkennung von Cybervorfällen wurden nur von jedem fünften Unternehmen vollständig umgesetzt
 - Prozesse zur Behandlung von Cybervorfällen wurden nur von 18% der Unternehmen vollständig umgesetzt
 - Mitarbeiter-Schulungen über den sicheren Gebrauch IT wurden lediglich bei 15% der KMU vollständig umgesetzt

¹ Studie von SVV, SQS, ICTswitzerland, ISSS, ISB, Expertenkommission Bund: Publikation 12.12.2017, <https://ictswitzerland.ch/publikationen/studien/cyberisiken-in-schweizer-kmu/>

Und bei Ihnen / sowie bei der breiten Bevölkerung?

- Schädigung durch Cyberangriffe
 - Waren Sie schon einmal von einem Angriff aus dem Internet betroffen, der bei Ihnen entweder einen finanziellen Schaden angerichtet hat, Ihnen viel Mühe für die Bereinigung gemacht hat, oder Ihnen emotional sehr zu schaffen gemacht hat?
- Passwörter (Anmelden beim Computer, Onlinedienste, Social Media, Hotel- , Flugbuchungen usw.)
 - Wird ein Passwort mehrfach benutzt?
 - Passwörter mindestens 10 Zeichen lang?
- Publikation der Resultate der Bevölkerungsumfrage «Sicherheit im Internet» am 28.3.2019¹
 - Der hohe Betroffenheitsgrad steht im Widerspruch zum hohen Sicherheitsgefühl, genauso wie der hohe selbst eingeschätzte Informationsgrad im Widerspruch zu gewissem Verhalten steht (z.B. Länge und Verwendung Passwort)

1) Im Auftrag von ICTswitzerland, ISSS, ISB, SATW, SISA, SwissICT und Switch befragte das Markt- und Sozialforschungsinstitut gfs-zürich vom 25. Januar bis 15. Februar 2019 1000 erwachsene Personen der Deutsch- und Westschweiz zum Thema «Sicherheit im Internet». Die nach wissenschaftlichen Methoden erfolgte Auswahl erlaubt es, die Resultate auf die Gesamtheit der erwachsenen Schweizer Bevölkerung zu übertragen.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

ICTSWITZERLAND



satw it's all about
technology

SNV

SQS

ASA | SVV

Cybersecurity-Schnelltest für KMU

Initiative von BWL, Expertenkommission Bund zur Datenbearbeitung und Datensicherheit, ICTswitzerland,
ISB - MELANI, ISSS, SATW, SNV, SQS, SVV

www.cybersecurity-check.ch



Jeder Computer ist ein lohnenswertes Angriffsziel

- Ausrichtung auf kleinere Unternehmen mit wenig ausgeprägten Kompetenzen bezüglich Informatik und IT-Sicherheit
- Instrument zur Selbstbeurteilung
- Kurz und einfach
- Begleitdokument mit weiterführenden Hinweisen zu jedem Thema

Wie gut ist Ihr Unternehmen vor Angriffen aus dem Cyberspace geschützt
und darauf vorbereitet?

Testen Sie jetzt, ob Sie die Minimalstandards für KMU erfüllen!

www.cybersecurity-check.ch

Der Cybersecurity Schnelltest für KMU in Kürze

- Breit abgestützte Initiative von von BWL, Expertenkommission Bund zur Datenbearbeitung und Datensicherheit, ICTswitzerland, ISB - MELANI, ISSS, SATW, SNV, SQS, SVV
- Fragebogen mit Spezialisten aus verschiedenen Fachbereichen entwickelt. Deckt thematisch die aktuellen, modernen Standards zu Security ab
- Fokus und Eigenheiten eines KMU berücksichtigt → kurzer, dennoch umfassender Fragebogen

Beispiele der Fragen:

People

Aufgaben, Kompetenzen, Verantwortlichkeiten;
Sensibilisierung von Mitarbeitenden

Process

Richtlinien, Abläufe (Backup!), Vorgaben, Outsourcing;
gesetzliche Vorgaben (Datenschutz)

Technology

Firewalls und Anti-Malware, Updates, WLAN, Verschlüsselung

Minimale Vorkehrungen – grosse Wirkung

- Für jeden Dienst ein anderes Passwort mit mehr als 10 Zeichen
- Allen E-Mails mit Anhängen oder Links, die man unaufgefordert erhält, ist grundsätzlich zu misstrauen, auch wenn der Absender auf den ersten Blick bekannt erscheint
- Updates
 - Computer regelmässig auf den neusten Stand bringen
 - Alle Software-Produkte regelmässig auf Updates prüfen, um Sicherheitslücken zu schliessen
 - Gilt auch für alle mit dem Internet verbundene Geräte, wie z. B. Haushaltsgeräte, Drucker oder Smartphones
 - Geräte, für die keine Updates ausgeliefert werden, sind aus Sicherheitsgründen vom Internet zu trennen oder ausser Betrieb zu nehmen
- WLAN-Netzwerk mit Passwörtern (mindestens 10 Zeichen) schützen. Separaten Gäste Zugang einrichten
- Regelmässige Datensicherung. Diese an einem externen, geschützten Ort aufbewahren. Regelmässig prüfen, ob sich die Daten von den Sicherheitsmedien zurückspielen lassen

¹⁾ Hinweise und Informationen für einen minimalen Schutz: https://ictswitzerland.ch/media/dateien/Cyber_Security/Minimalstandards/Hinweise_Cybersecurity_Minimalschutz.pdf