

SICHERHEIT IST KEIN PRODUKT. SIE IST EINE STRATEGIE.



SECURITY FÜR GEMEINDEN

AGENDA

Überblick

- 01** Aktuelle Cyber-Risikolage
- 02** Bedeutung für Gemeinden
- 03** Prioritäten und Sofortmassnahmen
- 04** Nächste Schritte

Cyberangriffe sind längst Alltag

1'587

Meldungen zu Cyberattacken in der ersten Oktoberwoche 2026 – schweizweit.

Täglich

Cyberdelikte wurden der Kantonspolizei Solothurn gemeldet (Angabe aus 2025).

Sicherheit ist eine Führungsaufgabe

35 %

der befragten Schweizer Unternehmen behandeln Cybersicherheit regelmässig im Verwaltungsrat.

20 %

führen routinemässig eine Cyberrisikobewertung durch.

~1 Woche

bis Glutz nach dem Ransomware-Angriff 2022 wieder eingeschränkt im Normalbetrieb war.

WORAUF ORGANISATIONEN NICHT VORBEREITET SIND

Anteil der Sicherheitsverantwortlichen, die eine Vorbereitungslücke nennen.

50 % KI-Systeme

Transparenz über Assets, Risiken und Abhängigkeiten schaffen. Gebündelte Angriffe über KI-Systeme erfolgen 2-3 Minuten nach bekanntwerden der Schwachstellen!

40 % Cloud-Risiken

Priorisierte technische und organisatorische Massnahmen.

34 % Drittanbieter

Risiken bei deren Befall. Vorgehen, Verantwortlichkeiten und Eskalation definieren.

PwC Analyse 2027: 3'934 Führungskräfte in 71 Ländern befragt (Mai–Juli 2026).

NOTFALLPLANUNG: DIE GRÖSSTE LÜCKE

HERAUSFORDERUNG

Nur 39 % haben vollständig integrierte Betriebskontinuitätspläne für Cyberrisiken.

EMPFEHLUNG

Gemeinden: Krisenstab, Offline-Notfallpläne, Wiederanlauf und Übungen verbindlich regeln. Massnahme.

DREI PRIORITÄTEN FÜR GEMEINDEN

Aus internationalen Trends konkrete kommunale Massnahmen ableiten

01 Massnahmen umsetzen (organisatorisch, technisch)

02 Notfallbetrieb & Restore testen

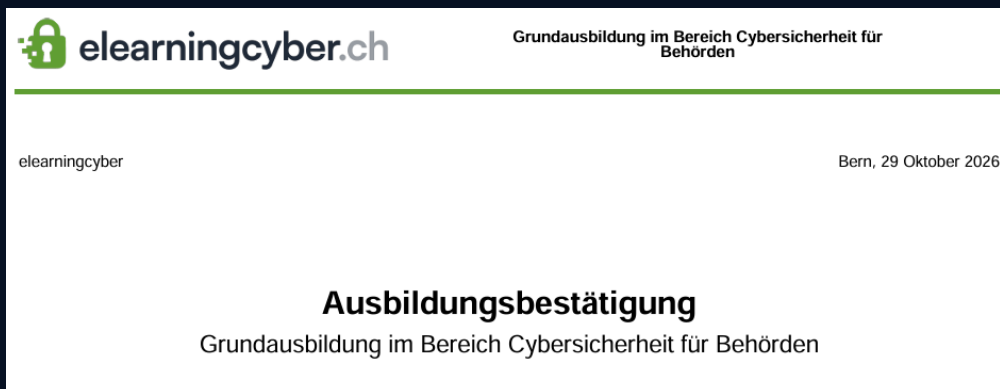
03 IT-Dienstleister & Lieferanten prüfen

01 Massnahmen umsetzen (organisatorisch, technisch)

Schulung des Personals



<https://www.elearningcyber.ch/de>



Schulungsliste

🔒 Melden Sie sich an, um Ihren Fortschritt in diesem Kurs zu verfolgen

- Training
1 **Informationssicherheit und Datenklassifizierung**
- Training
2 **Social Engineering**
- Training
3 **Phishing, Fake News**

01 Massnahmen umsetzen (organisatorisch, technisch)

Schulung des Personals

Wie kann man Fakes erkennen?

1. Der Kontext- und Plausibilitätscheck (Menschliche Ebene)

KI kann Sprache perfekt imitieren, kennt aber die internen Abläufe Ihres Unternehmens nicht.

- **Ungewöhnliche Kanäle:** Bittet der CEO plötzlich per E-Mail um eine dringende Überweisung, obwohl solche Freigaben intern *immer* über das ERP-System oder Microsoft Teams laufen?
- **Künstlicher Zeitdruck:** KI-Prompts werden oft darauf optimiert, Dringlichkeit zu erzeugen ("Sofort handeln", "Bis 16:00 Uhr erledigen"). Prüfen Sie, ob der Grund für den Zeitdruck logisch nachvollziehbar ist.
- **Fehlendes Insider-Wissen:** Die Mail klingt zwar professionell, nutzt aber generische Floskeln statt der firmeninternen Abkürzungen, Projektnamen oder des üblichen kollegialen Tons.
- **Zu perfekte Höflichkeit:** KI-Mails wirken oft steril, übertrieben formell oder untypisch distanziert für eine Person, mit der man regelmässig arbeitet.

[Quiz: WR Test Quiz](#)

2. Technische Indikatoren (System-Ebene)

Da der Text täuschend echt ist, liefert die Technik oft die verlässlichsten Warnsignale.

- **Die Absenderadresse (Spoofing):** Der Anzeigename lautet zwar "Logistik AG", die tatsächliche E-Mail-Adresse lautet aber `info@logistik-ag-portal-ch.com`. Details in der Domain genau prüfen.
- **Versteckte Link-Ziele:** KI generiert perfekten Begleittext für Links. Bewegen Sie den Mauszeiger über den Link (**Hover-Effekt**), ohne zu klicken. Führt die URL wirklich auf die offizielle Schweizer Website des Partners oder zu einer unbekannten Domain?

01 Massnahmen umsetzen (organisatorisch, technisch)

Schulung des Personals

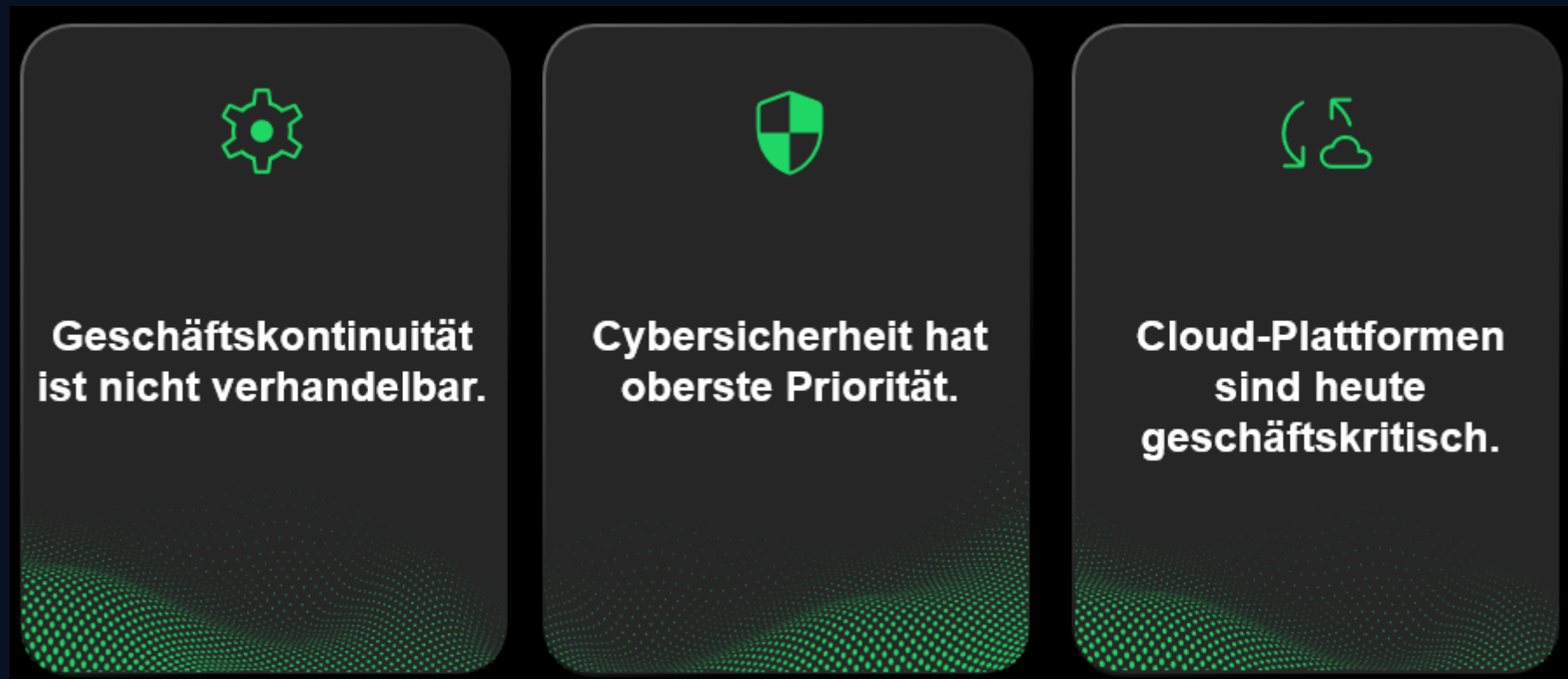
Sicher am Arbeitsplatz

- Keine Dokumente auf dem Schreibtisch liegen lassen (Clean Desk)
- Beim Verlassen des Schreibtischs immer den Bildschirm sperren (Windows L)



01 Massnahmen umsetzen (technisch)

Schutz der Geräte, welche mit dem Internet verbunden sind (Firewall)



01 Massnahmen umsetzen (technisch)

Wieso brauche ich eine Firewall?

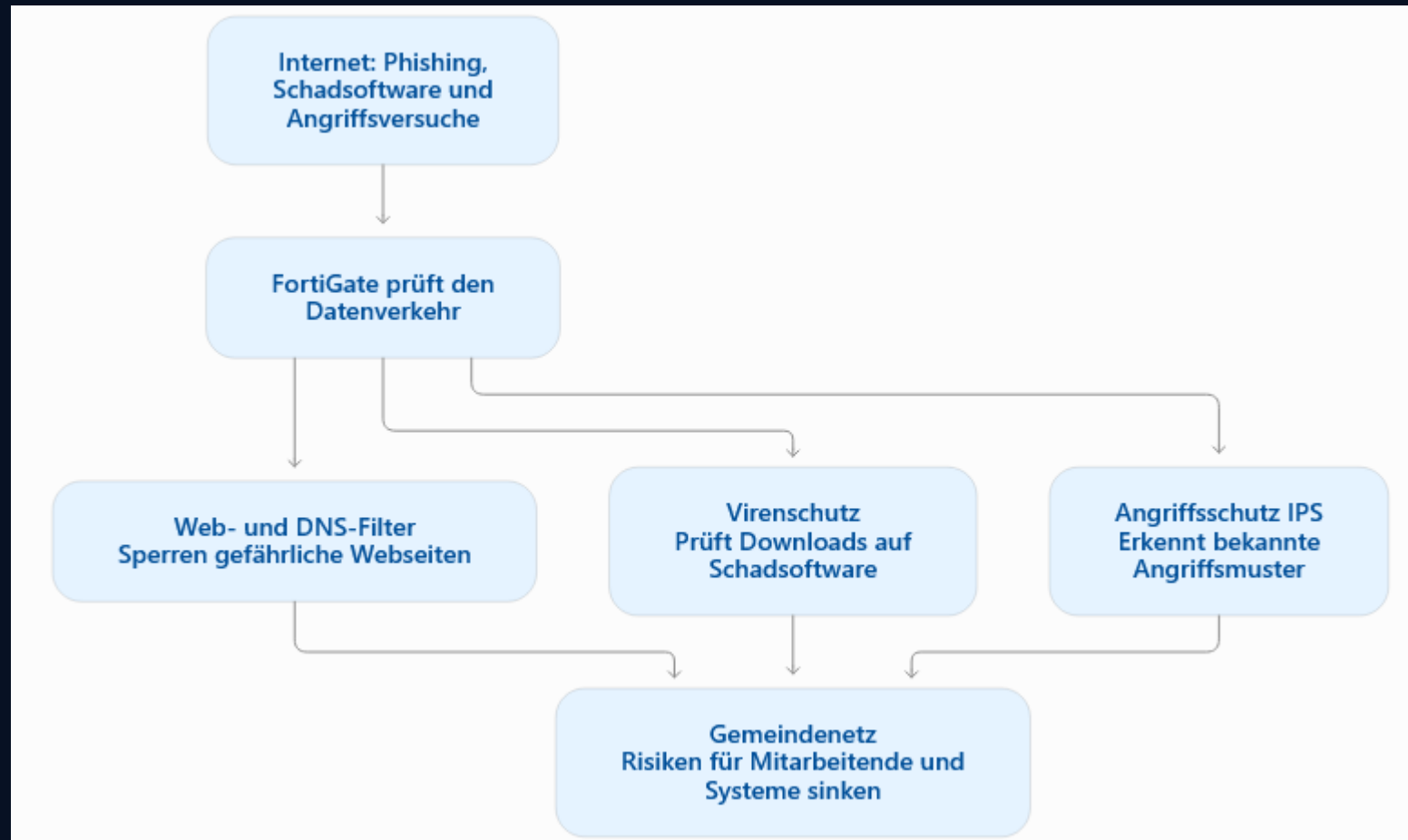
<https://fortiguard.fortinet.com/threat-map>



01 Massnahmen umsetzen (technisch)

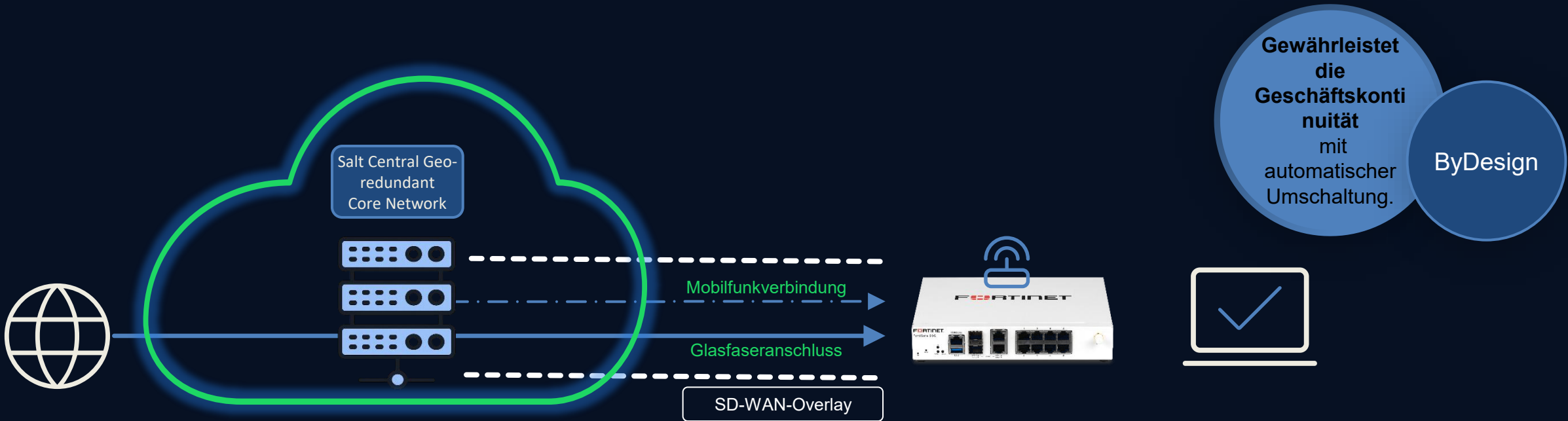
Wieso brauche ich eine Firewall?

Warum das hilft: Die Firewall kann Angriffe an mehreren Stellen stoppen: beim Aufruf einer Phishing-Seite, beim Herunterladen einer schädlichen Datei oder beim Versuch, eine Sicherheitslücke auszunutzen. FortiGuard aktualisiert die dafür verwendeten Bedrohungsinformationen.



Business Continuity by Design.

Ihre Dienste bleiben auch im Falle eines Ausfalls der Hauptverbindung betriebsbereit.



Stets betriebsbereit – Schutz für alle Ihre aktiven Dienste.

Teambesprechungen, Telefonate, VPN, Fernzugriff, IPv4- und IPv6-Adressierung: Alles wird nahtlos auf die mobile Verbindung umgeschaltet.

Security by Design: Cybersicherheit. Eine wachsende Bedrohung in der Schweiz

Erweiterter Schutz mit IPS-Software und Malware – by design.

+63.000

Cybervorfälle in der Schweiz im Jahr 2024
(+28 % im Vergleich zum Vorjahr).

Unternehmen sind die
Prioritätsziele.

Malware
führt die Angriffe an.



Dank der globalen Bedrohungsentelligenz von Fortinet bietet unsere Spitzentechnologie Schweizer Unternehmen

**eine fortschrittliche
Erkennung und Abwehr von
Malware.**

**Schützen Sie Ihr
Netzwerk mit
fortschrittlicher
Bedrohungsanalyse
vor Malware.**

ByDesign

AB CHF
118.- /Monat

FortiClient – sicher arbeiten, überall

SICHERER ZUGRIFF

Verschlüsselte VPN-Verbindungen für Homeoffice und Aussendienst.

ZERO TRUST

Gerätestatus und Zugriffsregeln mit FortiClient EMS und FortiGate.

ZENTRALE KONTROLLE

Clients, Richtlinien und Sicherheitsstatus, Patches zentral verwalten. Dies auch für nicht Microsoft Produkte

MOBILE ARBEITSPLÄTZE

Auch Notebooks ausserhalb des Gemeinde-Netzes einbeziehen.

NUTZEN: Einheitliche Sicherheitsstandards – bei allen Teams. Kann als Service eingekauft werden

Minimal Umsetzen: Patch My PC – Sicherheitslücken schneller schliessen

AUTOMATISIEREN

Updates für unterstützte Drittanbieter-Software werden zentral vorbereitet und verteilt.

RISIKEN REDUZIEREN

Veraltete Anwendungen bleiben weniger lange ungepatcht; CVE-Bezug unterstützt Priorisierung.

RESSOURCEN SPAREN

Weniger manuelles Paketieren und Aktualisieren – wichtig für kleine Gemeinde-IT-Teams.

Empfehlung: Patch-Management durchsetzen – Patch My PC ergänzt Intune, oder WSUS, ersetzt diese aber nicht.

VIELEN DANK

Fragen & Diskussion

info@securetime.ch

www.securetime.ch