

Der Betrieb muss laufen.

7 digitale Schutzschalter für KMU

Wie Unternehmen Cyberangriffe erschweren,
die Ausbreitung begrenzen und nach einem Vorfall
schneller wieder arbeitsfähig werden.

Steffen Kraus · SURFBOXX IT-SOLUTIONS GmbH
2. Juli 2026 · Elektro-Fink · Teterow



Keep IT Simple & Secure.

EINSTIEG

Eine einfache Frage.

Wie lange kann Ihr Unternehmen weiterarbeiten, wenn ab jetzt E-Mail, Dateiablage und zentrale Anwendungen ausfallen?

Viele KMU beantworten diese Frage nicht in Tagen, sondern in Stunden.

Deshalb geht es heute nicht um Hackerfilme, sondern um Lieferfähigkeit, Kommunikation mit Kunden und tägliche Arbeit.

30 Minuten

erste Abläufe stocken

3 StundenKunden und
Mitarbeitende warten**1 Arbeitstag**Liefer- und
Rechnungsfähigkeit
gefährdet

IT-Sicherheit ist eine Frage
der Betriebsfähigkeit.

— WARUM KMU?

„Wir sind doch zu klein.“

Angriffe starten häufig automatisiert.

Gesucht werden erreichbare Systeme, schwache Passwörter, offene Fernzugänge und ungepatchte Geräte - nicht zuerst die Unternehmensgröße.

Nicht die Größe schützt,
sondern wirksame Begrenzungen.

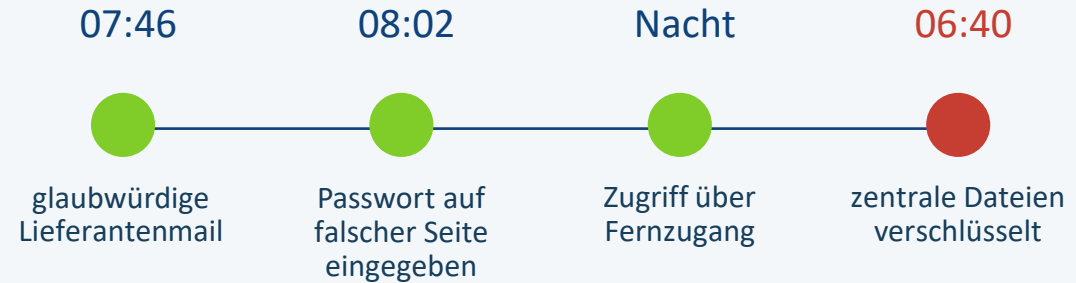
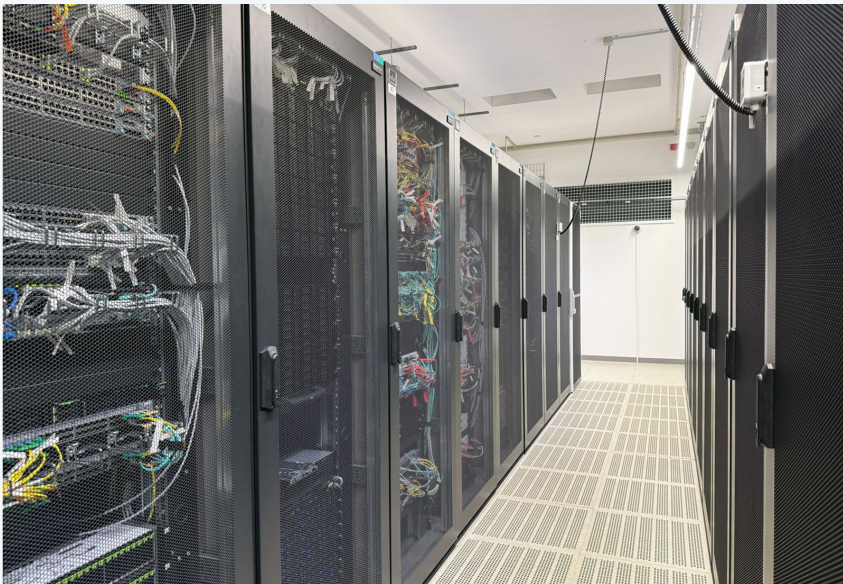
Typische Einstiegspunkte

- 1 E-Mail und Zugangsdaten
- 2 Fernwartung und VPN
- 3 veraltete Systeme
- 4 fehlende Segmentierung
- 5 Backup ständig erreichbar

PRAXISFALL, ZUSAMMENGESETZT

Ein typischer Montagmorgen.

38 Mitarbeitende, Büro, Werkstatt, Außendienst, Warenwirtschaft und zentrale Dateiablage.



Der Schaden entsteht nicht durch einen Klick, sondern durch eine Kette fehlender Begrenzungen.

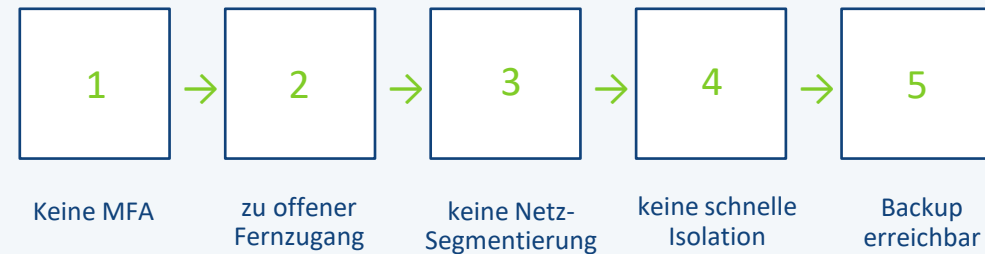
Zusammengesetztes Szenario - kein konkreter Kundenfall.

DIE FEHLERKETTE

Nicht ein Klick. Eine Kette.

Gute Security geht davon aus, dass Menschen Fehler machen.

Die Aufgabe der Technik ist, diesen Fehler aufzufangen und seine Wirkung zu begrenzen.



Menschen sind Teil der Verteidigung –
aber sie dürfen nicht die einzige Verteidigung sein.

KISS IN DER PRAXIS

Die 7 digitalen Schutzschalter.

KISS: Keep IT Simple & Secure.

Wenige klare Maßnahmen –
sauber umgesetzt und betreut.

Keine Produktliste, sondern sieben Aufgaben,
die zusammenwirken.

1 Überblick & Updates**2** Identitäten & MFA**3** Firewall & Zonen**4** Endpoint-Isolation**5** Backup & Restore**6** Notfallplan**7** Physische Sicherheit

SCHUTZSCHALTER 1 UND 2

Wissen, was da ist. Schützen, wer rein darf.

Erste Frage für Montag:

Welche Konten haben Zugriff von außen?

Ein gestohlenes Passwort darf allein nicht reichen,
reichen, um ins Unternehmen zu kommen.

1 Überblick & Updates

Server, Clients, Router, WLAN, Kameras
und Fachsysteme erfassen.

Verantwortliche und Updatefristen festlegen.

2 Identitäten & MFA

E-Mail, VPN, Fernwartung und Administration
nicht nur mit Passwort schützen.

Admin-Konten vom Alltag trennen.

SCHUTZSCHALTER 3 UND 4

Trennen, erkennen, isolieren.



3 Firewall & Netzwerkzonen

Büro, Server, Produktion, Gäste-WLAN sowie Video und Zutritt nicht ungeprüft in einem gemeinsamen Netz betreiben.

4 Endpoint-Schutz

Auffälliges Verhalten erkennen und betroffene Geräte schnell vom restlichen Netzwerk trennen.

Sämtliche Schutzebenen müssen miteinander kommunizieren. Die Architektur ist wichtiger als das einzelne Produkt.

SCHUTZSCHALTER 5 UND 6

Backup ist erst fertig, wenn Restore funktioniert.

Grüne Häkchen im Backup-System helfen wenig!

Wenn niemand getestet hat, ob die wichtigsten Daten und Anwendungen rechtzeitig wiederhergestellt werden können.

Ein Backup, das nie zurückgesichert wurde,
ist kein Wiederanlaufplan, sondern Hoffnung.

Wiederanlauf bedeutet:

- ✓ geschützte Sicherung
- ✓ getestete Rücksicherung
- ✓ Prioritätenliste der Systeme
- ✓ Notfallkontakte auf Papier
- ✓ klare Entscheidungskette

SCHUTZSCHALTER 7

Physische Sicherheit ist heute auch IT.

Kameras, Zutrittssysteme und Intercoms sind vernetzte vernetzte Geräte.

Sie brauchen Updates, klare Konten, minimale Rechte Rechte und einen eigenen Netzwerkbereich.

Video und Zutritt erhöhen Sicherheit -
wenn sie nicht selbst zur Angriffsfläche werden.



 GASTGEBER-BEZUG

Warum das zu Elektro-Fink passt.

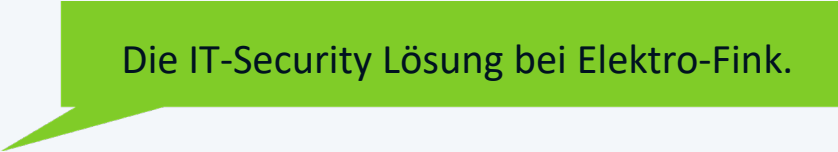
Schaltanlagenbau, Engineering und Automation leben von Verfügbarkeit, sauberer sauberer Dokumentation und klaren Zuständigkeiten.

Genau diese Logik lässt sich auf IT-Sicherheit übertragen.

Analogie

Elektrische Selektivität: ein Fehler soll gezielt abgeschaltet werden.

Digitale Selektivität: ein Vorfall soll begrenzt werden, bevor er den ganzen Betrieb stoppt.



Die IT-Security Lösung bei Elektro-Fink.

MONTAG UM 9 UHR

Drei Schritte, die sofort Wirkung bringen.

Wer diese drei Punkte ehrlich beantwortet,
kennt meist bereits den wichtigsten
Handlungsbedarf.

- 1** MFA prüfen
E-Mail, VPN, Fernwartung und Admin-Konten.
Konten.
- 2** Restore testen
Eine Datei, eine Anwendung oder eine VM
wirklich zurückholen.
- 3** Netz skizzieren
Büro, Server, Produktion, Gäste-WLAN,
WLAN, Kameras, und Fernzugänge auf einer
einer Seite darstellen.

NÄCHSTER SCHRITT

Wie viele digitale Schutzschalter sind aktiv?

Sieben Fragen. Drei Minuten.

Eine erste Einschätzung - direkt im Browser, ohne automatische Datenübertragung.

Web: surfboxx.it/check

Kostenfreies 30-Minuten-Auswertungsgespräch auf Wunsch.



Check starten und Ergebnis auf Wunsch mit SURFBOXX besprechen.

SCHLUSS

IT-Sicherheit ist kein Zustand. Sie ist ein Prozess.

Beginnen Sie nicht mit allem gleichzeitig.

Starten Sie mit dem nächsten wirksamen
Schutzschalter.

Vielen Dank.