strategisch-sicher.de

certified IT
ein Whitepaper von

EIN SURVIVAL-GUIDE FÜR GESCHÄFTSFÜHRER UND INHABER

Die 7 unsichtbaren Brandherde in gewachsenen IT-Infrastrukturen

Was heute reibungslos läuft, kann morgen für Tage stillstehen. Dieser Guide zeigt Ihnen, wo Sie hinschauen sollten — ruhig, konkret und ohne Panikmache.

Mit Firewall-Schnellcheck und NIS2-Kurzcheck zum Selbsttest.

Christian Enderle
IT-Consultant & Managed Service Provider, certified IT
20+ Jahre Erfahrung · Vertrauter Ansprechpartner für den Mittelstand

20+	KMU	NIS2
Jahre Praxis	Fokus Mittelstand	Compliance-Blick

01 · EINLEITUNG

„Es läuft ja irgendwie.“

Ihr Firmenwagen bekommt alle zwei Jahre eine Hauptuntersuchung. Ihre Bilanzen prüft der Steuerberater einmal im Jahr. Nur Ihre IT-Infrastruktur läuft munter weiter — ohne TÜV, ohne Plakette, ohne dass je jemand unabhängig unter die Haube geschaut hat.

Das Tückische: Wie beim Auto merkt man den Verschleiß erst, wenn es kracht. Eine Firewall ohne Updates, ein Server, den niemand mehr patcht, ein Backup, das im Ernstfall leer läuft — jedes für sich unauffällig. In Kombination genügt oft ein einziger Auslöser, um den Betrieb für Tage lahmzulegen.

Die gute Nachricht: Anders als beim TÜV entscheidet hier kein Prüfsiegel über Stilllegung — sondern Sie. Sie müssen nur wissen, wo Sie hinschauen sollten.

Warum dieses Dokument?

Dieser Guide bündelt, was certified IT bei Bestandsaufnahmen im Mittelstand immer wieder sieht — sieben Muster, ehrlich benannt, ohne Verkaufsdruck. Am Ende wissen Sie genau, wo Sie stehen und was als Nächstes zu tun ist.

ÜBER DEN AUTOR

Christian Enderle

Christian Enderle begleitet seit über 20 Jahren mittelständische Unternehmen durch genau diese Themen — in der Fertigung, im Gesundheitswesen, in Hotellerie und Kommunen. Sein Fokus: Netzwerksicherheit, Virtualisierung, Backup-Strategien und NIS2-Compliance, mit dem nüchternen Blick eines Praktikers, nicht eines Verkäufers.

02 · DIE 7 BRANDHERDE

Brandherde 1–2: Architektur & Altsysteme

1 Das „Klingeldraht“-Netzwerk

Architektur ohne Segmentierung

DAS RISIKO

Gäste-WLAN, Büro und Produktionsanlage hängen an einem Strang. Ein Klick im Gästenetz reicht, um bis in die Fertigung durchzudringen.

WARUM ES NIEMAND BEMERKT

Es läuft ja — und was läuft, wird selten hinterfragt.

SO SCHÜTZEN SIE SICH

Sauber getrennte VLANs sorgen dafür, dass ein Zwischenfall genau da bleibt, wo er entsteht.

2 Der Zombie-Server

Windows-Altsysteme im Dauerbetrieb

DAS RISIKO

Windows Server 2012 / 2016 werkeln weiter, obwohl Microsoft seit Jahren keine Sicherheitsupdates mehr liefert.

WARUM ES NIEMAND BEMERKT

„Never touch a running system“ — der Umzug wirkt riskanter als das Nichtstun. Ein Trugschluss mit Ablaufdatum.

SO SCHÜTZEN SIE SICH

Eine priorisierte Migrationsliste schließt bekannte Lücken, bevor es jemand anderes für Sie tut.

02 · DIE 7 BRANDHERDE

Brandherde 3–4: Firewall & Linux

3 Die vergessene Zeitbombe

Firewalls ohne Firmware-Updates

DAS RISIKO

Firewall-Geräte ohne Firmware-Update seit Jahren stehen unverändert am Netzwerkrand — im Dienst rund um die Uhr, aber längst blind.

WARUM ES NIEMAND BEMERKT

Die Firewall „läuft“ ja — ein Update-Fenster wird gefühlt jeden Monat verschoben.

SO SCHÜTZEN SIE SICH

End-of-Life-Geräte konsequent austauschen. Ein wacher Posten macht am Ende den Unterschied.

4 Der unsichtbare Mitspieler

Ungepatchte Linux-Systeme

DAS RISIKO

NAS-Systeme, Datenbank- und Monitoring-Server auf Linux-Basis laufen oft jahrelang unbeaufsichtigt mit.

WARUM ES NIEMAND BEMERKT

Linux gilt als pflegeleicht — und wird deshalb gern komplett vergessen.

SO SCHÜTZEN SIE SICH

Eine vollständige Inventarisierung holt jedes System aus dem Halbschatten.

02 · DIE 7 BRANDHERDE

Brandherde 5–6: Backup & Berechtigungen

5 Die trügerische Backup-Illusion

Backup ist nicht gleich Schutz

DAS RISIKO

Ein tägliches Backup existiert — liegt aber online, veränderbar, im selben Netz wie die Produktivsysteme.

WARUM ES NIEMAND BEMERKT

„Wir sichern ja täglich“ fühlt sich an wie Schutz, ist aber nur die halbe Miete.

SO SCHÜTZEN SIE SICH

Eine unveränderliche Offline-Kopie hält auch dann, wenn Angreifer versuchen, das Backup gleich mitzuverschlüsseln.

6 Das Berechtigungs-Chaos

Active Directory außer Kontrolle

DAS RISIKO

Langjährige Mitarbeitende sammeln über die Jahre „aus Versehen“ Admin-Rechte über weite Teile der Infrastruktur an.

WARUM ES NIEMAND BEMERKT

Rechte werden großzügig vergeben — und beim Rollenwechsel so gut wie nie wieder entzogen.

SO SCHÜTZEN SIE SICH

Ein Berechtigungs-Audit nach dem Least-Privilege-Prinzip stutzt jeden Generalschlüssel auf Normalmaß.

02 · DIE 7 BRANDHERDE

Brandherd 7: Der Notfallplan

7

Der blinde Fleck beim Notfallplan

Fehlender Incident-Response-Plan

DAS RISIKO

Niemand im Haus weiß verbindlich, wer im Ernstfall in welcher Reihenfolge was übernimmt.

WARUM ES NIEMAND BEMERKT

Ein Notfall bleibt abstrakt — bis er es plötzlich nicht mehr ist.

SO SCHÜTZEN SIE SICH

Ein schriftlicher, eingeübter Notfallplan macht aus tagelangem Stillstand einen Vorfall, der in Stunden erledigt ist.

Zwischenfazit: Sieben Brandherde, ein Bild

- ✓ 1. Netzwerk ohne Segmentierung
- ✓ 2. Windows-Altsysteme ohne Patches
- ✓ 3. Firewalls ohne Firmware-Updates
- ✓ 4. Ungepatchte Linux-Systeme
- ✓ 5. Backup ohne Offline-Kopie
- ✓ 6. Berechtigungs-Chaos im AD
- ✓ 7. Fehlender Notfallplan

Jeder Punkt für sich ist beherrschbar. Gemeinsam betrachtet ergeben sie ein klares Bild — und das ist bereits der erste Schritt zu echtem Schutz.

03 · DER QUICK-CHECK

Wie viele Brandherde schwelen bei Ihnen?

Sechs Fragen, ehrlich beantwortet — mehr braucht es nicht für einen ersten, realistischen Eindruck.

Können Sie mit 100%iger Sicherheit sagen, dass heute Nacht ein unveränderliches (offline/immutable) Backup gezogen wurde?	JA	NEIN
Sind alle Windows- und Linux-Server in Ihrem Netz aktuell gepatcht (jünger als 30 Tage)?	JA	NEIN
Läuft Ihre Firewall auf einer Firmware, die noch aktiv vom Hersteller aktualisiert wird?	JA	NEIN
Sind Gästenetz, Büro-IT und Produktionsanlagen durch VLANs sauber voneinander getrennt?	JA	NEIN
Gibt es eine dokumentierte, regelmäßig geprüfte Liste, wer welche Admin-Rechte im Active Directory besitzt?	JA	NEIN
Existiert ein schriftlicher Notfallplan, der jedem Verantwortlichen seine Rolle im Ernstfall zuweist?	JA	NEIN

Zwei oder mehr „Nein“? Dann ist jetzt ein guter Zeitpunkt.

Das ist kein Armutszeugnis — gewachsene Infrastrukturen sehen fast immer so aus. Es bedeutet nur: Jetzt lohnt sich ein genauer Blick, bevor der Zufall die nächste Entscheidung trifft.

04 · DER NÄCHSTE SCHRITT

Rote Flaggen entdeckt? Warten Sie nicht, bis es brennt.

Dieser Guide zeigt die Symptome. Das 14-Tage-Audit von certified IT ist die Hauptuntersuchung, die Ihre IT nie hatte — Diagnose plus priorisierter Fahrplan, den Sie sofort umsetzen können. Kein Verkaufsgespräch, sondern eine ehrliche Bestandsaufnahme, die Ihnen zeigt, wo Sie wirklich stehen.

Bestandsaufnahme

Netzwerk, Server, Firewall und Backup im Detail geprüft.

Priorisierter Fahrplan

Konkrete Schritte nach Dringlichkeit statt Empfehlungen von der Stange.

NIS2-Einordnung

Klarheit, wo regulatorischer Handlungsbedarf wirklich besteht.

Jetzt für das 14-Tage-Audit bewerben →

Terminbuchung & Details unter strategisch-sicher.de

Christian Enderle · certified IT

strategisch-sicher.de · certifiedit.net · Blaubeuren / Region Ulm