IT-BASISWISSEN FÜR FÜHRUNGSKRÄFTE

IT-Sicherheit für Entscheider.

Verstehen. Vorleben. Vorbeugen.

Die wichtigsten Sicherheitsprinzipien verständlich erklärt – und was Sie als Führungskraft konkret tun können, damit Probleme gar nicht erst entstehen.

WORUM ES GEHT

Sicherheit ist Chefsache – kein Produkt

Die meisten IT-Schäden entstehen nicht, weil eine Schutzsoftware gefehlt hat. Sie entstehen durch Struktur- und Verhaltensfehler: zu viele Rechte, ungetestete Backups, ein unbedachter Klick, ein vergessenes Benutzerkonto.

Deshalb dreht sich diese Broschüre nicht um Produkte, sondern um Prinzipien. Wer sie versteht und im Unternehmen vorlebt, verhindert Sicherheitsprobleme, bevor sie entstehen – das ist wirksamer und günstiger als jede nachträgliche Verteidigung.

LEITPRINZIP DIESER BROSCHÜRE

Vermeiden statt verteidigen: Die beste Sicherheitslücke ist die, die es nie gab.

~90 %

der erfolgreichen Angriffe

beginnen mit menschlichem Verhalten – meist einer täuschend echten E-Mail

1 von 6

Unternehmen in Österreich

meldete bereits einen erfolgreichen Cyberangriff

1,2 Mio €

Schaden pro Woche Ausfall

so viel kostet eine Woche IT-Stillstand ein durchschnittliches Unternehmen

VERTIEFUNG · VERANTWORTUNG & RAHMENWERKE

NIS2 / NISG

Die EU-Richtlinie nimmt Geschäftsleitungen ausdrücklich in die Pflicht: Sicherheitsmaßnahmen müssen von der Führungsebene gebilligt und überwacht werden – persönliche Haftung inklusive. Betroffen sind auch viele Zulieferer.

CIS Controls

Priorisierte Maßnahmenliste aus der Praxis. Die Basisstufe (IG1) deckt bereits die häufigsten Angriffswege ab – ein realistisches erstes Zielbild für KMU.

ISO 27001

Der internationale Standard für Informationssicherheits-Management. Auch ohne Zertifizierung ein guter Maßstab: Risiken bewerten, Maßnahmen dokumentieren, regelmäßig prüfen.

Cyber-Versicherung

Versicherer verlangen zunehmend Nachweise: MFA, getestete Backups, Patch-Prozesse. Wer die Prinzipien dieser Broschüre umsetzt, erfüllt die üblichen Mindestanforderungen.

PRINZIP 01

01

Netzwerksegmentierung

Brandabschnitte für Ihre IT

Ein Gebäude hat Brandschutztüren, damit ein Feuer im Lager nicht das ganze Haus zerstört. Ihr Netzwerk braucht dasselbe: getrennte Bereiche, zwischen denen nur kontrollierter Verkehr fließt.

Ohne Segmentierung



Ein infizierter Bürorechner erreicht alles: Server, Produktionsmaschinen, Kassen. Ein Vorfall wird zum Totalausfall.

Mit Segmentierung



Der Vorfall bleibt im Bürobereich eingesperrt. Produktion und Server laufen weiter – der Schaden bleibt klein und beherrschbar.

> Fragen Sie Ihren IT-Verantwortlichen: „Was passiert, wenn ein Bürorechner infiziert wird – was erreicht er von dort aus?“

VERTIEFUNG · WIE SEGMENTIERUNG TECHNISCH UMGESETZT WIRD

VLANs & Firewall-Zonen

Logische Trennung im Switch (VLAN) plus eine Firewall, die den Verkehr zwischen den Zonen regelt – nach dem Prinzip: alles verboten, außer explizit erlaubt (Default Deny).

802.1X / NAC

Netzwerkzugangskontrolle: Nur bekannte, verwaltete Geräte bekommen überhaupt einen Netzwerkzugang – das fremde Notebook landet automatisch im Gästenetz.

OT/IT-Trennung

Produktions- und Steuerungstechnik (OT) gehört strikt vom Büronetz getrennt – Maschinen leben oft 15+ Jahre ohne Updates und brauchen deshalb besonders enge Zonen.

Ost-West-Verkehr

Nicht nur den Weg ins Internet kontrollieren, sondern auch den Verkehr zwischen internen Systemen – dort bewegen sich Angreifer nach dem Erstzugriff (Lateral Movement).

PRINZIP 02

02

Least Privilege & Admin-Tiering

Nicht jeder braucht den Generalschlüssel

Jede Person bekommt genau die Rechte, die sie für ihre Arbeit braucht – nicht mehr. Und wer viel darf, arbeitet mit getrennten Konten: eines für den Alltag, eines nur für Verwaltungsaufgaben.

Tier 0 · Generalschlüssel
Zentrale Systeme (z. B. Benutzerverwaltung)

Nur wenige Spezialkonten, nie für E-Mail & Web

Tier 1 · Abteilungsschlüssel
Server & Anwendungen

Eigene Admin-Konten, protokolliert

Tier 2 · Büroschlüssel
Arbeitsplätze & Alltag

Hier arbeiten alle – auch die Chefs

WENIGER KONTEN ↑ · MEHR RECHTE – NIE MISCHEN

Warum der Chef kein Admin sein sollte

Angreifer zielen auf die Konten mit den meisten Rechten – und Führungskräfte sind die sichtbarsten Ziele. Wer als Geschäftsführer mit Admin-Rechten E-Mails liest, macht aus jedem Phishing-Klick einen Vollzugriff. Trennen Sie konsequent: Alltagskonto für die Arbeit, Admin-Konto (falls überhaupt nötig) nur für den Ausnahmefall.

> Faustregel: Ein Konto, das E-Mails empfangen kann, darf keine Server verwalten.

VERTIEFUNG · WERKZEUGE FÜR SAUBERES RECHTEMANAGEMENT

PAW

Privileged Access Workstation: Verwaltungsaufgaben nur von eigens gehärteten Geräten ohne E-Mail und Web – der Admin-Zugang teilt sich nie ein Gerät mit dem Alltag.

Just-in-Time-Admin

Rechte werden nicht dauerhaft vergeben, sondern zeitlich befristet angefordert und automatisch wieder entzogen – stehende Privilegien verschwinden.

LAPS

Automatisch verwaltete, pro Gerät einzigartige lokale Admin-Passwörter – ein gestohlenes Passwort öffnet nicht mehr jeden Rechner im Haus.

Service-Konten

Konten für Programme und Dienste sind beliebte Hintertüren: nie mit Domain-Admin-Rechten betreiben, Passwörter verwalten lassen (z. B. gMSA), Nutzung protokollieren.

PRINZIP 03

03

Multi-Faktor-Authentifizierung (MFA)

Schlüssel + Alarmcode

Ein Passwort ist ein Schlüssel – und Schlüssel werden gestohlen, erraten oder abgephisht. MFA verlangt einen zweiten, unabhängigen Nachweis: eine Bestätigung am Handy, einen Sicherheitsschlüssel, einen Fingerabdruck.

1
Passwort
etwas, das Sie wissen

→

2
Bestätigung
etwas, das Sie haben

→

✓
Zugang
erst wenn beides stimmt

Was MFA abfängt

- Gestohlene oder erratene Passwörter werden allein wertlos
- Passwort-Listen aus Datenlecks laufen ins Leere
- Angriffsversuche werden sichtbar: unerwartete Bestätigungsabfrage = Alarmzeichen

Wo MFA Pflicht ist

- E-Mail-Konten (das Haupteinfallstor)
- VPN- und Fernzugänge
- Microsoft 365 / Cloud-Dienste
- Alle Admin-Konten – ohne Ausnahme

Achtung Ermüdungstaktik: Angreifer lösen absichtlich viele Bestätigungsabfragen aus, bis jemand genervt „Ja“ drückt. Regel: Unerwartete Anfrage → immer ablehnen und der IT melden.

VERTIEFUNG · NICHT JEDES MFA IST GLEICH STARK

FIDO2 / Passkeys
Phishing-resistent: Der Schlüssel funktioniert nur auf der echten Website – eine nachgebaute Anmeldeseite geht leer aus. Goldstandard für Admin- und Führungskonten.

App-Push mit Number Matching
Statt blindem „Bestätigen“ muss eine angezeigte Zahl eingetippt werden – wirksam gegen die Ermüdungstaktik. SMS-Codes gelten dagegen als schwächste Variante.

AiTM / Token-Diebstahl
Moderne Phishing-Kits schalten sich zwischen Nutzer und echte Anmeldung und stehlen die Sitzung trotz MFA – Gegenmittel: Passkeys plus Richtlinien, die Anmeldungen nur von verwalteten Geräten erlauben.

Conditional Access
Anmelderegeln nach Kontext: Zugriff nur von verwalteten Geräten, riskante Anmeldungen (unbekanntes Land, unmögliche Reisezeit) werden blockiert oder erneut geprüft.

PRINZIP 04

04

Backup richtig gedacht

Ein ungetestetes Backup ist ein Gerücht

Backups sind Ihre letzte Verteidigungslinie – gegen Angriffe, aber auch gegen Brand, Diebstahl und schlichte Fehler. Entscheidend sind zwei Fragen: Ist eine Kopie außer Reichweite der Angreifer? Und startet sie im Ernstfall wirklich?

3 Kopien Ihrer Daten (Original + zwei Sicherungen)

2 verschiedene Speicherarten (z. B. Server + Cloud)

1 Kopie außer Haus und vom Netz getrennt

DIE 3-2-1-REGEL

Moderne Erpresser-Software sucht und verschlüsselt zuerst die Backups – erst dann die Daten. Eine getrennte Kopie ist deshalb nicht Kür, sondern Pflicht.

Testen statt hoffen

SO MACHEN WIR DAS

Ein „grüner" Backup-Bericht heißt nur: Die Sicherung lief durch. Ob sie sich im Ernstfall auch starten lässt, zeigt nur der Test. Wir starten Server-Backups deshalb regelmäßig automatisiert in einer geschützten Testumgebung – mit Screenshot des Anmeldebildschirms als Nachweis.

> Die eine Frage an Ihre IT: „Wann wurde zuletzt eine komplette Wiederherstellung geprobt – und wie lange hat sie gedauert?"

VERTIEFUNG · WORAN GUTE BACKUP-KONZEPTE ERKENNBAR SIND

Immutable Storage

Unveränderbare Sicherungen: Einmal geschrieben, kann das Backup für eine definierte Zeit weder gelöscht noch verschlüsselt werden – auch nicht mit Admin-Rechten.

Getrennte Zugangsdaten

Das Backup-System braucht eigene Konten mit eigenem MFA, unabhängig von der Benutzerverwaltung – sonst löscht ein kompromittierter Domain-Admin auch die Sicherungen.

RPO & RTO

Die zwei Kennzahlen, die Sie als Entscheider festlegen: Wie viele Stunden Datenverlust sind tragbar (RPO)? Wie schnell muss alles wieder laufen (RTO)? Daraus folgt die Technik – nicht umgekehrt.

Wiederherstellungs-Reihenfolge

Ein Notfallplan legt fest, welche Systeme zuerst zurückkommen (z. B. Benutzerverwaltung → ERP → Mail) – das unterscheidet Stunden von Wochen.

UNTERSCHÄTZTE GEFAHREN

Die Risiken, an die niemand denkt

Nicht die spektakulären Angriffe sind das größte Risiko – sondern die unscheinbaren Gewohnheiten und Altlasten.

01 Konten ausgeschiedener Mitarbeiter

Wer gegangen ist, aber noch Zugänge hat, ist ein unsichtbares Einfallstor. Austritt = Konto noch am selben Tag sperren.

02 „Temporäre“ Ausnahmen

Die schnell geöffnete Firewall-Regel, das kurz deaktivierte Update – Provisorien werden vergessen und bleiben Jahre offen.

03 Fernwartungszugänge

Jeder Wartungszugang von Lieferanten ist eine Tür in Ihr Netz. Ohne MFA und Protokoll ist sie unbewacht.

04 Gefundene USB-Sticks & Werbegeschenke

Ein „verlorener“ Stick am Parkplatz ist ein Klassiker gezielter Angriffe. Fremde Datenträger gehören nie in Firmenrechner.

05 Private Geräte & Schatten-IT

Das private Notebook mit Firmenzugang, der selbst eingerichtete Cloud-Speicher – gut gemeint, aber außerhalb jeder Kontrolle.

06 Vergessene Geräte im Netz

Drucker, Kameras, Zeiterfassung: Geräte, die nie Updates bekommen, sind beliebte Hintertüren – Segmentierung hilft (Prinzip 01).

VERTIEFUNG · DIE ANGRIFFSFLÄCHE SYSTEMATISCH VERKLEINERN

Asset-Inventar

Man kann nur schützen, was man kennt: eine automatisch gepflegte Liste aller Geräte, Konten und Cloud-Dienste ist die Grundlage jeder Sicherheitsarbeit – und deckt Schatten-IT auf.

Lifecycle-Management

Jedes Gerät braucht ein definiertes Lebensende (EOL): Wer Windows-Versionen oder Geräte ohne Hersteller-Support weiterbetreibt, betreibt dokumentiert unschützbare Systeme.

Externes Attack-Surface-Scanning

Regelmäßig von außen prüfen, was vom Internet aus sichtbar ist: offene Fernwartungsports, vergessene Subdomains, veraltete Geräte – Angreifer scannen genau das, nur täglich.

ALLTAG

Do's & Don'ts in alltäglichen Situationen

Sicherheit entscheidet sich in kleinen Momenten. Diese Regeln kosten nichts – und verhindern die häufigsten Schäden.

	✗ VERMEIDEN	✓ STATTDESSEN
E-Mail & Anhänge	Anhänge und Links öffnen, weil der Absender bekannt wirkt – Absender lassen sich fälschen.	Bei unerwarteten Mails: kurz anrufen und nachfragen. 30 Sekunden Rückruf schlagen jede Schutzsoftware.
Zahlungsfreigaben	Überweisungen freigeben, weil „der Chef“ es per E-Mail eilig anordnet – das ist das Muster des CEO-Frauds.	Zahlungen ab definierter Höhe immer über einen zweiten Kanal bestätigen (Anruf, persönlich). Ohne Ausnahme – auch beim Geschäftsführer.
Passwörter	Ein Passwort für mehrere Dienste verwenden oder im Team teilen.	Passwort-Manager nutzen: ein starkes Passwort pro Dienst, automatisch erzeugt. Plus MFA (Prinzip 03).
Unterwegs & Homeoffice	Über offenes Hotel- oder Flughafen-WLAN direkt auf Firmendaten zugreifen.	Immer über die gesicherte Firmenverbindung (VPN) arbeiten – oder den Handy-Hotspot nutzen.
Datenweitergabe	Kundenlisten oder Verträge über private Mail oder Gratis-Cloud-Dienste verschicken.	Nur die vom Unternehmen bereitgestellten Wege nutzen – die sind kontrolliert, protokolliert und DSGVO-konform.

VERTIEFUNG · TECHNIK, DIE GUTES VERHALTEN FLANKIERT

SPF / DKIM / DMARC

E-Mail-Echtheitsprüfung: Richtig konfiguriert, wird der gefälschte Absender „Ihres“ Geschäftsführers schon vom Mailserver abgewiesen – CEO-Fraud verliert sein Hauptwerkzeug.

Makro- & Anhang-Richtlinien

Office-Makros aus dem Internet zentral blockieren, riskante Anhangstypen (ISO, LNK, HTA) aussperren – die häufigsten Infektionswege verschwinden per Richtlinie.

Externe-Mail-Banner

Ein deutlicher Hinweis auf Mails von außerhalb der Organisation macht den „Chef von der Privatadresse“ sofort erkennbar – minimaler Aufwand, große Wirkung.

DER ERNSTFALL

Richtig reagieren, wenn etwas passiert

Ob Verschlüsselungsmeldung am Bildschirm, verdächtiger Klick oder verlorenes Notebook: Die ersten Minuten entscheiden über die Schadenshöhe. Dieser Ablauf gehört ausgedruckt neben jeden Arbeitsplatz.

1 **Ruhe bewahren**

Hektik erzeugt Folgefehler. Ein gemeldeter Verdacht ist nie peinlich – ein verschwiegener wird teuer.

2 **Gerät vom Netz trennen – nicht ausschalten**

Netzwerkkabel ziehen, WLAN aus. Nicht herunterfahren: Im laufenden Zustand bleiben Spuren erhalten, die Experten für die Analyse brauchen.

3 **Sofort melden**

Intern an die definierte Stelle und an Ihren IT-Partner. Lieber fünfmal falscher Alarm als einmal zu spät.

4 **Nichts löschen, nichts zahlen, nichts verhandeln**

Keine Dateien aufräumen, keine Lösegeldkontakte. Jede eigenmächtige Aktion kann Beweise vernichten oder den Schaden vergrößern.

5 **Dokumentieren**

Was ist wann passiert, wer wurde informiert? Fotos vom Bildschirm genügen. Wichtig für Versicherung, Behörden und Aufarbeitung.

Meldepflichten nicht vergessen

DSGVO Sind personenbezogene Daten betroffen: Meldung an die Datenschutzbehörde binnen 72 Stunden.

NIS2 / NISG Fällt Ihr Unternehmen unter NIS2: Frühwarnung an das nationale CSIRT binnen 24 Stunden, detaillierte Meldung binnen 72 Stunden.

Auch deshalb gilt: sofort melden statt intern abwarten – Ihr IT-Partner hilft bei der Einordnung.

IHRE IT-NOTFALLNUMMER

Hier eintragen und die Seite gut sichtbar aushängen.

BETRIEBSSICHERHEIT

Auch Verfügbarkeit ist IT-Sicherheit

Nicht jeder Ausfall ist ein Angriff: Ein defektes Netzteil, ein Wasserschaden oder ein Software-Fehler legen ein Unternehmen genauso still wie Erpresser-Software. Betriebssicherheit heißt, diese Frage VOR dem Ausfall zu beantworten – nicht währenddessen.

Wie lange darf ein Ausfall in Ihrem Unternehmen dauern?

Die ehrliche Antwort ist je nach System verschieden: Die Telefonanlage darf vielleicht einen Tag stehen, die Produktionssteuerung keine Stunde. Genau diese Einstufung – System für System – ist die Grundlage jeder Investitionsentscheidung.

RTO — **Wiederanlaufzeit**
Wie schnell muss ein System wieder laufen? „Recovery Time Objective" – die wichtigste Kennzahl Ihrer Betriebssicherheit.

RPO — **Max. Datenverlust**
Wie viele Stunden Arbeit dürfen schlimmstenfalls verloren gehen? Bestimmt, wie oft gesichert werden muss.

Was kostet Sie eine Stunde Stillstand?

Personalkosten (20 MA × ø 45 €)	**900 €**
Entgangene Wertschöpfung / Umsätze	**1.500 €**
Lieferverzug, Vertragsstrafen, Express-Kosten	**400 €**
Pro Stunde Stillstand	**≈ 2.800 € / Stunde**

Beispielrechnung für einen 20-Personen-Betrieb – setzen Sie Ihre eigenen Zahlen ein. Aber ehrlich rechnen: Kosten × Eintrittswahrscheinlichkeit. Ein Server-Cluster (z. B. 50.000 € statt 15.000 €) rechnet sich bei diesen Zahlen selten – ein Hersteller-Wartungsvertrag mit Ersatzteil am nächsten Arbeitstag (z. B. 1.300 € für 5 Jahre) fast immer.

VERTIEFUNG · VERFÜGBARKEIT IN ZAHLEN

Verfügbarkeitsklassen

99 % klingt gut, bedeutet aber ~87 Stunden Ausfall pro Jahr. 99,9 % ≈ 8,8 h; 99,99 % ≈ 53 min. Jede „Neun" mehr kostet deutlich – kaufen Sie nur die Neunen, die Ihr Geschäft braucht.

Single Point of Failure

Jede Komponente, deren Ausfall alles stoppt (die eine Firewall, der eine Switch, die eine Internetleitung). Der erste Schritt jeder Analyse: diese Punkte auflisten.

MTBF & MTTR

Mittlere Zeit zwischen Ausfällen bzw. bis zur Reparatur. Entscheidend für die Praxis ist MTTR: Ein seltener Ausfall, der zwei Wochen dauert, ist schlimmer als drei kurze.

Business Impact Analyse

Die systematische Form der Frage links: jedes System nach Ausfallfolgen in Stunden/Euro bewerten – Grundlage für NIS2 und jedes Notfallhandbuch.

BETRIEBSSICHERHEIT

Wie viel Redundanz brauche ich – und was kostet sie?

Redundanz heißt: Eine Komponente darf ausfallen, ohne dass der Betrieb steht. Die Kunst ist das richtige Maß – zu wenig riskiert Stillstand, zu viel bezahlt Sicherheit, die niemand braucht. Drei Stufen im Vergleich:

Stufe 1 · Keine Redundanz — €

WIEDERANLAUF: TAGE BIS WOCHEN

- Ein Server, eine Leitung, ein Switch
- Ersatz muss erst bestellt werden
- Wiederherstellung aus Backup – hoffentlich getestet

Vertretbar nur, wenn Tage Stillstand nachweislich verkraftbar sind.

Stufe 2 · Kalte Reserve — €€

WIEDERANLAUF: STUNDEN

- Ersatzgerät konfiguriert im Schrank – oder Vorhaltung beim Dienstleister
- Backup läuft auf Zweitsystem an
- Wechsel erfordert Handgriffe der IT

Der Sweet Spot für viele KMU. Die Ersatzgeräte-Vorhaltung kann auch ein externer Dienstleister übernehmen: Bei aktivem Vertrag weiß er, was im Einsatz ist, und tauscht schnellstmöglich.

Stufe 3 · Hochverfügbar — €€€

WIEDERANLAUF: MINUTEN BIS NULL

- Alles doppelt: Server-Cluster, zwei Leitungen, zwei Firewalls
- Übernahme automatisch, ohne Handgriff
- Auch Strom & Kühlung abgesichert

Pflicht, wo jede Stunde fünfstellig kostet – Produktion, Handel, Medizin.

Faustregel: Redundanz muss sich gegen Ausfallkosten × Eintrittswahrscheinlichkeit rechnen – nicht gegen den schlimmsten denkbaren Tag. Für viele KMU ist deshalb Stufe 2 oder ein Wartungsvertrag mit garantierter Wiederherstellung (Seite 12) wirtschaftlicher als volle Redundanz.

VERTIEFUNG · WORAUS REDUNDANZ TECHNISCH BESTEHT

N+1-Prinzip

Von allem eines mehr als nötig: zweites Netzteil, zweiter Lüfter, zweite USV. Die billigste Redundanz – viele Geräte können das ab Werk, es muss nur bestellt werden.

Cluster & Replikation

Zwei Server, die denselben Stand halten: Fällt einer aus, übernimmt der andere (Failover). Virtualisierung macht das heute auch für KMU bezahlbar.

Zweite Internetleitung

Verschiedene Technologien kombinieren (Glasfaser + Mobilfunk), sonst fällt beides mit demselben Bagger aus. Die Firewall schaltet automatisch um.

USV & Notstrom

Die übersehene Basis: Ohne überbrückten Stromausfall nützt der schönste Cluster nichts – und ungeplante Stromabschaltungen beschädigen Server-Daten.

Wartungsvertrag & Software-Support: Was ist wirklich zugesichert?

Für alles, was nicht redundant ist, ist der Wartungsvertrag Ihre einzige Absicherung. Entscheidend ist das Kleingedruckte – denn „Reaktionszeit“ und „Wiederherstellung“ sind zwei völlig verschiedene Zusagen:

✗ HÄUFIGSTER IRRTUM IN WARTUNGSVERTRÄGEN

Nur Reaktionszeit zugesichert

„Wir melden uns binnen 4 Stunden“ heißt: Nach 4 Stunden ruft jemand an. Ob das Ersatzteil in 3 Tagen oder 3 Wochen kommt, ist NICHT geregelt.

✓ DAS SOLLTE IM VERTRAG STEHEN

Wiederherstellung zugesichert

„Entstörung binnen 8 Stunden“ oder „Ersatzgerät am nächsten Arbeitstag“ heißt: Der Betrieb läuft nachweisbar wieder – dafür haftet der Partner.

Und die Software?

Hardware ist nur die halbe Betriebssicherheit. Prüfen Sie für jede geschäftskritische Anwendung – auch für Sonderentwicklungen und Branchensoftware:

- Gibt es aktiven Herstellersupport – oder ist das Produkt abgekündigt (End of Life)?
- Liegt der Quellcode / eine Doku vor, falls der Hersteller ausfällt?
- Wer hilft bei einem Fehler – mit welcher zugesicherten Zeit?
- Läuft die Software auf aktuellen, gepatchten Systemen – oder erzwingt sie veraltete?

Prüfen Sie heuer noch: Welche Ihrer Verträge garantieren nur eine Reaktion – und welche die Reparatur?

VERTIEFUNG · VERTRAGSBEGRIFFE, AUF DIE ES ANKOMMT

SLA

Service Level Agreement: die messbare Zusage (Zeiten, Verfügbarkeit, Pönale). Ohne Messgröße und Konsequenz ist es nur eine Absichtserklärung.

Reaktions- vs. Entstörzeit

Reaktion = jemand beginnt zu arbeiten. Entstörung = das System läuft wieder. Nur Letzteres schützt Ihren Betrieb.

NBD / 4h-Vor-Ort

Hersteller-Servicelevel für Hardware: Ersatzteil „Next Business Day“ oder Techniker binnen 4 Stunden vor Ort. Kostet beim Kauf wenig – nachrüsten ist teuer.

EOL / EOS

End of Life / End of Support: Ab diesem Datum gibt es keine Sicherheitsupdates mehr – das Produkt wird planbar zum Risiko. Gehört in jede Inventarliste.

Folgen einer falschen Einschätzung – zwei Betriebe im Vergleich

Gleiche Branche, gleicher Vorfall, unterschiedliche Vorbereitung. Die Szenarien sind fiktiv – die Muster sehen wir in der Praxis ständig:

Szenario 1 · Der zentrale Server fällt aus (Netzteil-Defekt, Freitag 14 Uhr)

Betrieb A · unvorbereitet — **4 Tage**

Kein Ersatz, kein Vertrag mit Wiederherstellungszusage. Ersatzteil kommt Mittwoch, Backup-Rücksicherung ungeprobt. 4 Arbeitstage Stillstand ≈ 90.000 € Schaden.

Betrieb B · Stufe 2 vorbereitet — **2 Stunden**

Zweites Netzteil ab Werk + Ersatzsystem im Schrank + geübter Wechsel. Betrieb läuft nach 2 Stunden wieder – die Reparatur passiert ohne Zeitdruck.

Szenario 2 · Die Branchensoftware stürzt nach einem Update ab

Betrieb A · Software abgekündigt — **1–2 Wochen**

Hersteller existiert nicht mehr, niemand kennt das System. Externe Analyse dauert Tage, Rückbau unmöglich – Notbetrieb auf Papier, Datenverlust droht.

Betrieb B · Support gesichert — **Selber Tag**

Aktiver Supportvertrag mit Entstörzusage, dokumentierte Umgebung, Snapshot vor jedem Update. Hersteller spielt Vorgängerversion ein – am selben Tag wieder produktiv.

> Der Unterschied war in keinem Fall Glück – sondern drei Entscheidungen, die Monate vorher getroffen wurden: realistische Einschätzung der Ausfalltoleranz, passende Redundanzstufe, Verträge mit echter Wiederherstellungszusage.

VERTIEFUNG · SO WIRD AUS DEN SZENARIEN EIN PLAN

Notfallhandbuch

Pro kritischem System eine Seite: Wer macht was, in welcher Reihenfolge, mit welchen Passwörtern (versiegelt)? Muss auch OHNE die IT-Systeme lesbar sein – gedruckt.

Jährliche Übung

Ein halber Tag pro Jahr: einen Ausfall durchspielen, Zeiten stoppen, Lücken notieren. Nach der zweiten Übung ist der Ablauf Routine statt Krise.

Wiederanlauf-Reihenfolge

Nicht alles kann gleichzeitig starten: erst Netzwerk und Benutzerverwaltung, dann Daten, dann Anwendungen. Die Reihenfolge einmal festlegen spart im Ernstfall Stunden.

KLEINE ÄNDERUNGEN, GROSSE WIRKUNG

Womit Sie morgen anfangen können

Sortiert nach Verhältnis von Aufwand zu Wirkung – die ersten vier kosten fast nichts.

01	**MFA aktivieren** AUFWAND: GERING	Für E-Mail, VPN und Cloud – der wirksamste Einzelschritt überhaupt.		96
02	**Alt-Konten löschen** AUFWAND: GERING	Alle Zugänge ausgeschiedener Mitarbeiter prüfen und sperren – heute.		88
03	**Zahlungs-Doppelfreigabe einführen** AUFWAND: GERING	Zweiter Kanal ab definierter Summe. Stoppt CEO-Fraud zuverlässig.		82
04	**Updates automatisieren** AUFWAND: GERING	Bekannte Lücken sind das Lieblingsziel – automatisches Patchen schließt sie ohne Zutun.		78
05	**Admin-Rechte trennen** AUFWAND: MITTEL	Alltagskonten ohne Admin-Rechte, Verwaltung über eigene Konten (Prinzip 02).		90
06	**Backup-Test vereinbaren** AUFWAND: MITTEL	Regelmäßige, automatisierte Wiederherstellungs-Proben mit Nachweis (Prinzip 04).		85
07	**Notfallplan aushängen** AUFWAND: MITTEL	Die 5 Schritte von Seite 9 ausdrucken, Zuständigkeiten benennen, einmal durchspielen.		80
08	**Netzwerk segmentieren** AUFWAND: GRÖSSER	Brandabschnitte einziehen (Prinzip 01) – das Projekt mit der nachhaltigsten Wirkung.		92

WIRKUNG AUF IHR SICHERHEITSNIVEAU (RELATIV)

VERTIEFUNG · FORTSCHRITT MESSBAR MACHEN

Kennzahlen statt Gefühl

Drei Zahlen, die Sie sich quartalsweise berichten lassen sollten: MFA-Abdeckung in Prozent, Patch-Latenz in Tagen (kritische Lücken), Alter des letzten erfolgreichen Restore-Tests.

Wiederkehrend statt einmalig

Jede Maßnahme dieser Liste braucht einen Rhythmus (monatlich, quartalsweise) und einen namentlich Verantwortlichen – sonst degradiert sie zur einmaligen Aufräumaktion.

CIS IG1 als Zielbild

Die Basisstufe der CIS Controls (~56 Maßnahmen) ist ein realistisches, prüfbares Erstziel für KMU – besser als eine selbst zusammengestellte Maßnahmenliste.

SELBSTEINSCHÄTZUNG

Wo steht Ihr Unternehmen?

Sechzehn Fragen, die Sie ohne IT-Wissen beantworten können. Jedes „Nein“ und jedes „Weiß nicht“ ist ein konkreter Handlungspunkt – und ein guter Gesprächseinstieg mit Ihrer IT.

- Ist MFA für alle E-Mail- und Cloud-Zugänge aktiv?
- Arbeiten Führungskräfte im Alltag ohne Admin-Rechte?
- Werden Konten ausgeschiedener Mitarbeiter am Austrittstag gesperrt?
- Gibt es eine Backup-Kopie außer Haus und vom Netz getrennt?
- Wurde eine komplette Wiederherstellung in den letzten 6 Monaten geprobt?
- Ist das Gäste-WLAN vom Firmennetz getrennt?
- Erreicht ein Bürorechner Ihre Produktion / Server NICHT direkt?
- Gibt es eine Doppelfreigabe für Zahlungen ab definierter Höhe?
- Werden Updates automatisch und zeitnah eingespielt?
- Sind Fernwartungszugänge mit MFA gesichert und protokolliert?
- Wissen alle Mitarbeiter, wem sie einen Vorfall melden?
- Hängt der Notfallplan griffbereit aus?
- Wissen Sie, wie lange jedes kritische System ausfallen darf (RTO)?
- Sind Ihre Single Points of Failure bekannt – und bewusst so entschieden?
- Garantieren Ihre Wartungsverträge die Wiederherstellung – nicht nur eine Reaktion?
- Hat jede geschäftskritische Software aktiven Herstellersupport (kein EOL)?

13–16 × Ja
Solide Basis – Feinschliff mit einem Sicherheits-Check.

7–12 × Ja
Gute Ansätze, klare Lücken – die Quick Wins von Seite 14 zuerst.

0–6 × Ja
Handlungsbedarf – aber jeder Punkt ist lösbar. Reden wir.

VERTIEFUNG · WAS EIN PROFESSIONELLER SICHERHEITS-CHECK ZUSÄTZLICH PRÜFT

Außensicht
Schwachstellen-Scan von außen: Was sieht ein Angreifer von Ihrem Unternehmen im Internet – offene Zugänge, veraltete Dienste, geleakte Zugangsdaten aus Datenlecks?

Innensicht
Analyse der Benutzerverwaltung (Active Directory / Entra ID): stehende Admin-Rechte, Passwort-Richtlinien, verwaiste Konten, riskante Delegierungen.

Belastungsprobe
Ein begleiteter Restore-Test und ein durchgespielter Vorfall (Tabletop-Übung) zeigen, ob Pläne auch unter Druck funktionieren – auf dem Papier besteht jeder.

Vorbeugen ist günstiger als reparieren.

Gerne gehen wir die Selbsteinschätzung gemeinsam mit Ihnen durch – unverbindlich, auf Augenhöhe und ohne Fachchinesisch. Sie erfahren ehrlich, wo Sie stehen und welche Schritte sich für Ihr Unternehmen wirklich lohnen.

Jetzt Kontakt aufnehmen

www.t2.at

T2 IT Systeme GmbH

Bräuweg 15, 5252 Aspach
info@t2.at · +43 7755 22022

Ihre IT-Sicherheit ist unsere Mission.
Sie kümmern sich ums Geschäft – wir uns um den Rest.