Cybersicherheit für kleine Unternehmen

Wie gut ist Ihr Unternehmen wirklich vorbereitet?

Referent: **Dr. Ralf C. Güstel**
IT-Security-Auditor · Wirtschaftsprüfer

KAPITEL 1

Cyberresilienz beginnt im Kopf

Warum heute nicht mehr die Frage ist, ob Sie Opfer eines Cyberangriffs werden, sondern wie schnell Sie danach wieder arbeitsfähig sind.

Die Realität

- Cyberangriffe gehören heute zum Unternehmensalltag.
- Jede Organisation verarbeitet digitale Informationen.
- Automatisierte Angriffe treffen Unternehmen jeder Größe.
- Gemeinnützige Organisationen sind keine Ausnahme.

Nicht die Größe entscheidet über das Risiko – sondern die Angriffsfläche.

MONTAG · 08:00 UHR

Unsere Geschichte

Montagmorgen – 08:00 Uhr

- Outlook funktioniert nicht.
- Telefonanlage fällt aus.
- Mitarbeitende können sich nicht anmelden.
- Buchhaltung steht still.
- Erste Lösegeldforderung erscheint.

Frage: Was würden Sie jetzt tun?

Was bedeutet Cyberresilienz?

Cybersicherheit → Angriffe verhindern
Cyberresilienz → Trotz eines Angriffs arbeitsfähig bleiben

Perfekte Sicherheit gibt es nicht. Gute Vorbereitung schon.

Die aktuelle Cyberlage

- Cyberkriminalität nimmt weiter zu.
- Ransomware bleibt eines der größten Risiken.
- KI verändert die Angriffsmethoden.
- Automatisierte Angriffe treffen jede Organisation.

Quellen: Bundeskriminalamt · Bundesamt für Sicherheit in der Informationstechnik (BSI)

Wie KI Cyberangriffe verändert

Früher

- Programmierkenntnisse
- Spezialwissen
- viel Erfahrung

Heute zusätzlich

- KI-Unterstützung
- automatisierte Analysen
- perfekte Phishing-Mails
- Deepfakes
- KI-Agenten

Warum gerade gemeinnützige Organisationen?

Sie verarbeiten häufig: Gesundheitsdaten · Sozialdaten · Personaldaten · Spendendaten · Finanzdaten

Oft bestehen gleichzeitig: begrenzte IT-Budgets · wenige IT-Spezialisten · viele Außenstellen · mobiles Arbeiten

Praxisbeispiel

Eine soziale Einrichtung verliert den Zugriff auf Klientendaten, Dienstpläne, Outlook, Buchhaltung und Telefonie.

Folge: Die Organisation kann ihren Auftrag nicht mehr erfüllen.

KI unterstützt heute sowohl Verteidiger als auch Angreifer.

Als das US-KI-Unternehmen Anthropic im April 2026 sein neues leistungsstarkes KI-Modell Mythos vorstellte, das Sicherheitslücken in Softwaresystemen identifizieren kann, war die Aufregung groß. Mythos sei zu leistungsfähig und damit zu gefährlich für die Öffentlichkeit, beschied Anthropic. Kürzlich erst verlangte die US-Regierung eine Sperre von Anthropics KI-Modellen Fable und Mythos. Nun hat das chinesische KI-Unternehmen Zhipu AI (bekannt als Z.ai) mit GLM-5.2 ein Open-Weight-Modell veröffentlicht, das sich bei der Erkennung von Sicherheitslücken offenbar mit Anthropics Opus 4.8 messen kann. Angreifer könnten GLM-5.2 möglicherweise ohne jede Aufsicht betreiben – ein Dilemma.

Informationssicherheit: Die drei Schutzziele

Vertraulichkeit

Nur Berechtigte erhalten Zugriff.

Integrität

Daten dürfen nicht verändert werden.

Verfügbarkeit

Informationen müssen verfügbar sein.

Das Spannungsdreieck

Sicherheit · Kosten · Funktionalität

Mehr Sicherheit bedeutet häufig höhere Kosten und geringeren Komfort.

Die Aufgabe der Geschäftsführung besteht darin, ein angemessenes Gleichgewicht herzustellen.

Verantwortung der Geschäftsführung

Die IT kann Aufgaben übernehmen. Die Verantwortung bleibt bei

- Vorstand
- Geschäftsführung

Entscheidungen betreffen u.a.

- Budget
- IT-Dienstleister
- Cyberversicherung
- Notfallplanung
- Restrisiken

Entscheidung der Geschäftsführung

Nach diesem Kapitel sollten Sie beantworten können:

- ✓ Ist Cyberresilienz Führungsaufgabe?
- ✓ Gibt es klare Verantwortlichkeiten?
- ✓ Existiert ein Cyber-Notfallplan?
- ✓ Sind Zuständigkeiten dokumentiert?
- ✓ Wären wir heute handlungsfähig?

Nicht der Cyberangriff entscheidet über die Zukunft einer Organisation. Sondern die Vorbereitung.

MONTAG · 08:30 UHR

Im Besprechungsraum fallen Sätze wie: *„Wir haben doch Microsoft 365." · „Wir haben doch einen Virenscanner." · „Wir haben doch Backups." · „Wir sind viel zu klein."* — Aber stimmt das wirklich?

KAPITEL 2

Die größten Mythen der Cybersicherheit

Mythos Nr. 1

„Uns trifft das nicht."

Tatsächlich:

- Angriffe erfolgen heute automatisiert.
- Gesucht werden Schwachstellen – nicht prominente Unternehmen.
- Jede erreichbare Organisation ist ein mögliches Ziel.

Nicht Ihr Name interessiert den Angreifer – sondern Ihre Schwachstelle.

Praxisbeispiel: Kleiner Verein – großer Schaden

- 18 Mitarbeitende · ungepatchte Firewall · automatisierter Scan · Ransomware

Ergebnis: Der Verein ist drei Wochen arbeitsunfähig.

Mythos Nr. 2: „Wir haben alles in der Cloud."

Cloud bedeutet

✓ professionelles Rechenzentrum

Cloud bedeutet nicht automatisch

- ✗ Backup
- ✗ Administratorenschutz
- ✗ Schutz vor Fehlkonfigurationen
- ✗ Schutz vor kompromittierten Konten

⚠ Cloud ≠ Backup

Auch Microsoft 365 benötigt

- Exchange-Backup
- SharePoint-Backup
- Teams-Backup
- OneDrive-Backup

Frage

Wie stellen Sie Microsoft 365 nach einem erfolgreichen Angriff wieder her?

Praxisbeispiel

Ein Administrator löscht versehentlich SharePoint, Teams und OneDrive. Erst jetzt stellt sich heraus: Es existiert kein eigenes Cloud-Backup.

Mythos Nr. 3 & 4

Mythos Nr. 3: „Unser IT-Dienstleister kümmert sich darum."

Ein guter Dienstleister ist wichtig. Aber entscheidend ist: Was wurde vertraglich vereinbart?

Zum Beispiel: Updates · Backups · Wiederherstellung · Reaktionszeiten · Administratoren

Lassen Sie sich jährlich schriftlich bestätigen: ✓ Updates aktuell · ✓ Backups geprüft · ✓ Administratoren überprüft · ✓ unterstützte Systeme · ✓ Test der Wiederherstellung

Mythos Nr. 4: „Wir haben Backups."

Die eigentliche Frage lautet: **Funktionieren sie?**
Ein Backup ist nur dann hilfreich, wenn es vollständig ist, getestet wurde, nicht mitverschlüsselt wurde und schnell zurückgespielt werden kann.

Praxisbeispiel: Backup vorhanden. Rücksicherung nie getestet. Nach dem Angriff stellt sich heraus: Die Sicherung war seit sechs Monaten fehlerhaft.

Mythos Nr. 5 & 6

Mythos Nr. 5: „Virenschutz reicht aus."

Moderne Angriffe nutzen häufig gestohlene Passwörter, kompromittierte Administratoren, Phishing, Social Engineering und legitime Programme.

Virenschutz bleibt wichtig. Er ist aber nur ein Baustein.

Mythos Nr. 6: „Unsere Cyberversicherung zahlt schon."

Eine Cyberversicherung ersetzt nicht: Patchmanagement · MFA · Backups · Notfallplanung · Dokumentation

Viele Versicherer verlangen Mindeststandards.

Wichtig im Schadenfall

Nicht sofort handeln. Zuerst: ✓ Cyberversicherung informieren · ✓ Weisungen beachten · ✓ Forensik abstimmen · ✓ Dokumentation beginnen

Erst anrufen – dann handeln.

Mythos Nr. 7 & 8: KI und Passwörter

Mythos Nr. 7: „KI macht unsere Organisation sicher."

KI unterstützt ✓ Administratoren · ✓ Datenschutz · ✓ Sicherheitsteams — aber auch ✓ Phishing · ✓ Deepfakes · ✓ Schadcode · ✓ Angriffsvorbereitung

KI verändert Cyberkriminalität

Heute unterstützt KI beim Erstellen von Phishing-Mails, Fake-Webseiten, Deepfake-Stimmen, Schadcode, Übersetzungen und Social Engineering.

> KI kennt keine Moral. Entscheidend ist, wer sie nutzt.

Praxisbeispiel: Die Buchhalterin erhält einen Anruf. Die Stimme klingt exakt wie die des Geschäftsführers. Er bittet um eine dringende Überweisung. Später stellt sich heraus: Es handelte sich um einen KI-generierten Deepfake.

Mythos Nr. 8: „Passwörter reichen aus."

Passwörter können erraten, gestohlen, gekauft und wiederverwendet werden. Deshalb gilt heute: **MFA (Multi-Faktor-Authentifizierung) ist Standard.** Für Administratoren: FIDO2-Sicherheitsschlüssel.

Social Engineering

Der Mensch bleibt das wichtigste Angriffsziel. Angriffe erfolgen heute über E-Mail, Telefon, SMS, Teams, WhatsApp, QR-Codes und Bewerbungen. Nicht jeder Angriff ist technisch. Viele sind psychologisch.

CEO-Fraud

Geschäftsführer bittet um Überweisung. Alles wirkt echt: richtige Signatur · perfektes Deutsch · hoher Zeitdruck. Erst später stellt sich heraus: Die Nachricht war gefälscht.

Browser werden unterschätzt

Heute beginnen viele Angriffe nicht auf Servern, sondern im Browser. Deshalb: ✓ Browser aktuell halten · ✓ Erweiterungen prüfen · ✓ keine unbekannten Plug-ins · ✓ Downloads kontrollieren

Entscheidung der Geschäftsführung

Nach diesem Kapitel sollten Sie beantworten können:

- ☐ Haben wir ein eigenes Cloud-Backup?
- ☐ Sind Verantwortlichkeiten vertraglich geregelt?
- ☐ Nutzen Administratoren FIDO2?
- ☐ Ist MFA verpflichtend?
- ☐ Gibt es einen Notfallplan?

Die wichtigste Erkenntnis

Cyberresilienz entsteht niemals durch eine einzelne Maßnahme. Sondern durch Technik · Organisation · Verträge · Schulungen · Kontrolle · Vorbereitung

---

MONTAG · 09:15 UHR

Der IT-Dienstleister sagt: *„Es handelt sich vermutlich um einen Ransomware-Angriff."* Die Geschäftsführung fragt: *„Wie konnte das überhaupt passieren?"*

KAPITEL 3

Wie Cyberangriffe heute funktionieren

„Große Schäden beginnen häufig mit kleinen Fehlern."

Die Realität

Cyberangriffe beginnen selten spektakulär. Sie beginnen häufig mit einer E-Mail, einem Passwort, einem Klick, einer Sicherheitslücke oder einer Fehlkonfiguration.

Schwachstelle

Lücke finden und ausnutzen

Zugriff

Ersten Zugang zum System bekommen

Aufspüren

Im Netzwerk lateral bewegen

Privilegien

Administratorrechte übernehmen

Phase 1 & 2: Informationsbeschaffung und erster Zugriff

Phase 1: Informationsbeschaffung

Angreifer suchen öffentlich erreichbare Systeme, bekannte Schwachstellen, kompromittierte Passwörter, veröffentlichte Informationen und schlecht geschützte Cloud-Zugänge. Oft geschieht dies vollständig automatisiert.

Praxisbeispiel: Auf der Internetseite der Organisation stehen Ansprechpartner, Organigramm, Telefonnummern und E-Mail-Adressen. Diese Informationen helfen Angreifern beim Social Engineering.

Phase 2: Der erste Zugriff

Typische Einfallstore: Phishing-Mail · gestohlenes Passwort · ungepatchte Firewall · kompromittiertes VPN · Remote-Zugang · schwache Administratorpasswörter

Praxisbeispiel

Eine Mitarbeiterin erhält eine E-Mail: *„Ihr Microsoft-Konto läuft ab."* Ein Klick genügt. Das Passwort wird auf einer gefälschten Webseite eingegeben. Der Angreifer besitzt jetzt gültige Zugangsdaten.

Phase 3 & 4: Orientierung und Administratorrechte

Phase 3: Orientierung im Netzwerk

Jetzt beginnt die eigentliche Arbeit des Angreifers. Er sucht Server, Administratoren, Cloud-Dienste, Datensicherungen und kritische Systeme. Oft bleibt dies tagelang unbemerkt.

Der eigentliche Angriff beginnt häufig lange bevor die Lösegeldforderung erscheint.

Phase 4: Administratorrechte

Das eigentliche Ziel sind selten Daten. Das eigentliche Ziel sind Administratorrechte. Denn damit können Angreifer Passwörter ändern, Benutzer anlegen, MFA deaktivieren, Backups löschen und Systeme kontrollieren.

Praxisbeispiel: Ein kompromittiertes Benutzerkonto führt nach mehreren Tagen zur Übernahme des globalen Administrators. Ab diesem Zeitpunkt kontrollieren die Angreifer die gesamte Microsoft-365-Umgebung.

Wer den Administrator kontrolliert, kontrolliert die Organisation.

Phase 5, 6 & 7: Datendiebstahl, Verschlüsselung, Erpressung

Phase 5: Datendiebstahl

Heute werden Daten häufig vor der Verschlüsselung kopiert. Dadurch entsteht doppelter Druck: Betriebsunterbrechung und Androhung einer Veröffentlichung.

Was wird gestohlen? Je nach Organisation: Personaldaten · Gesundheitsdaten · Spenderdaten · Verträge · Finanzdaten · E-Mails · Klientendaten

Phase 6: Verschlüsselung

Erst jetzt werden Systeme verschlüsselt – oft innerhalb weniger Minuten. Die eigentliche Vorbereitung dauerte jedoch Tage oder Wochen.

Phase 7: Erpressung

Typische Forderungen: Lösegeld · Veröffentlichung von Daten · Fristen · Druck auf die Geschäftsführung

⚠ Über eine Zahlung sollte niemals unüberlegt entschieden werden. Ziehen Sie frühzeitig die Cyberversicherung, spezialisierte IT-Forensik, Rechtsberatung und – soweit sinnvoll – die Strafverfolgungsbehörden hinzu.

Warum KI Angriffe verändert

KI unterstützt heute

- Phishing
- Übersetzungen
- Deepfakes
- Codeanalyse
- Recherche
- Automatisierung

Dadurch werden Angriffe schneller, professioneller und glaubwürdiger.

Ransomware ist heute ein Geschäftsmodell

Viele Tätergruppen arbeiten arbeitsteilig. Es gibt Entwickler, Betreiber, Vermittler, Geldwäschestrukturen und Verhandlungsführer. Cyberkriminalität ist heute häufig professionell organisiert.

Der Faktor Mensch

Technik allein genügt nicht. Angriffe richten sich häufig gegen Vertrauen, Hilfsbereitschaft, Zeitdruck und Routine. Deshalb bleiben Schulungen unverzichtbar.

Praxistipps

Sensibilisieren Sie Mitarbeitende regelmäßig. Schwerpunkte:

- ✓ Phishing
- ✓ CEO-Fraud
- ✓ Passwortsicherheit
- ✓ Deepfakes
- ✓ Meldewege

Nicht einmalig. Sondern regelmäßig.

Entscheidung der Geschäftsführung

Nach diesem Kapitel sollten Sie beantworten können:

- ☐ Wie gelangen Angreifer typischerweise in unsere Organisation?
- ☐ Welche Systeme wären besonders kritisch?
- ☐ Wer besitzt Administratorrechte?
- ☐ Werden Mitarbeitende regelmäßig sensibilisiert?
- ☐ Gibt es einen Meldeweg für verdächtige Vorfälle?

Die wichtigste Erkenntnis

Cyberangriffe bestehen nicht aus einem einzigen Ereignis. Sondern aus Vorbereitung · Informationsbeschaffung · Datendiebstahl · Erpressung

Je früher ein Angriff erkannt wird, desto geringer ist der Schaden.

MONTAG · 09:50 UHR

Der IT-Dienstleister sagt: *„Wir müssen jetzt prüfen, ob auch unsere Administratoren betroffen sind."* Die Geschäftsführung fragt: *„Wie hätten wir das verhindern können?"*

KAPITEL 4

Die wichtigsten Schutzmaßnahmen

Was jede Organisation sofort umsetzen sollte

MONTAG · 10:00 UHR

Der IT-Dienstleister berichtet:

- ✓ Backups vorhanden
- ? Administratoren noch unklar
- ? Umfang des Schadens unbekannt

Die Geschäftsführung fragt: *„Wie hätten wir uns besser schützen können?"*

Die wichtigste Erkenntnis

Cybersicherheit entsteht nicht durch ✕ eine Firewall · ✕ einen Virenscanner · ✕ eine Software
Sondern durch ✓ Organisation · ✓ Menschen · ✓ Prozesse · ✓ Technik

Schutzmaßnahme Nr. 1: Verantwortung übernehmen

Cyberresilienz ist Führungsaufgabe.

Die Geschäftsführung entscheidet über Budget · IT-Strategie · Restrisiko · Notfallplanung · Cyberversicherung

Verantwortung kann delegiert werden. Haftung häufig nicht.

Entscheidung der Geschäftsführung

- ✓ Gibt es einen Cyber-Notfallplan?
- ✓ Gibt es einen Krisenstab?
- ✓ Sind Zuständigkeiten geregelt?
- ✓ Ist Cyberresilienz regelmäßiger Tagesordnungspunkt?

Schutzmaßnahme Nr. 2 & 3: IT kennen und Patchmanagement

Schutzmaßnahme Nr. 2: Kenne Deine IT

Man kann nur schützen, was man kennt. Dazu gehören Server · Clients · Cloud · Software · Administratoren · Benutzer · mobile Geräte

⚠ Praxisbeispiel: Der IT-Dienstleister fragt: „Wo befindet sich Ihr Backup?" Antwort: „Das weiß unser ehemaliger Administrator." Problem: Er ist seit drei Jahren nicht mehr im Unternehmen.

Schutzmaßnahme Nr. 3: Patchmanagement

Viele Angriffe nutzen keine neuen, sondern bekannte Schwachstellen. Deshalb: Sicherheitsupdates zeitnah installieren.

Praxistipp

Fragen Sie Ihren IT-Dienstleister nicht *„Haben wir Updates?"* sondern *„Wann wurden die letzten Sicherheitsupdates installiert?"* und *„Liegen dafür Protokolle vor?"*

Typische Fehler

- ❌ Updates werden verschoben.
- ❌ Niemand kontrolliert.
- ❌ Alte Software.
- ❌ Betriebssysteme ohne Support.
- ❌ Keine Dokumentation.

Schutzmaßnahme Nr. 4: Administratoren besonders schützen

Administratoren sind die Kronjuwelen jeder Organisation.

Wer Administratorrechte besitzt, kontrolliert häufig u.a. auch Microsoft 365 · Benutzer · Passwörter · Backups · Server

Goldene Regeln

- ✓ Administrator ≠ Benutzer
- ✓ getrennte Konten
- ✓ kein Surfen
- ✓ kein Outlook
- ✓ keine Office-Arbeiten
- ✓ Adminrechte nur bei Bedarf

Least Privilege

Jeder erhält nur die Rechte, die tatsächlich benötigt werden. Nicht mehr. Nicht dauerhaft.

Microsoft z.B. empfiehlt

Administratorrechte nicht dauerhaft vergeben. Stattdessen Just-in-Time-Administration, beispielsweise mit Microsoft Entra Privileged Identity Management (PIM). Dadurch werden Administratorrechte nur für einen begrenzten Zeitraum aktiviert.

Break-Glass-Konto

Jede Organisation sollte mindestens ein Notfall-Administratorkonto besitzen.

- ✓ nur Notfälle
- ✓ sehr langes Passwort
- ✓ FIDO2
- ✓ Zugang im Tresor
- ✓ regelmäßige Prüfung

Schutzmaßnahme Nr. 5: Multi-Faktor-Authentifizierung

Passwort + zweiter Faktor = MFA

Der zweite Faktor kann sein: Smartphone-App · Push-Nachricht · Hardware-Token · FIDO2 - Stick 2FA-Stick

Warum MFA?

Ein Passwort kann erraten, gestohlen, gekauft und wiederverwendet werden. MFA erschwert den Missbrauch erheblich.

Warum FIDO2?

Für privilegierte Konten empfohlen: ✓ phishing-resistent · ✓ keine SMS · ✓ keine TAN · ✓ kryptografische Anmeldung
Beispiele: YubiKey · Feitian · Google Titan

Entscheidung der Geschäftsführung

Fragen Sie Ihren IT-Dienstleister:

- ✓ Sind Administratoren ausschließlich mit FIDO2 abgesichert?
- ✓ Gibt es noch SMS als zweiten Faktor?
- ✓ Welche privilegierten Konten existieren?

Schutzmaßnahme Nr. 6: Passwortmanager

Keine Passwörter

- in Excel
- im Browser
- im Outlook
- auf Notizzetteln

Nutzen Sie professionelle Passwortmanager.

Recovery-Mail

Die Recovery-Mail (E-Mail zum zurücksetzen des Passwortes) sollte nicht die normale (gleiche) E-Mail-Adresse sein.

Empfehlung

- ✓ separate Mailadresse (außerhalb des Unternehmenskosmos, z.B. www.posteo.de)
- ✓ MFA
- ✓ FIDO2
- ✓ nur für Passwort-Rücksetzungen

Schutzmaßnahme Nr. 7: Microsoft 365 absichern

Fragen Sie Ihren IT-Dienstleister

- Wie hoch ist unser Secure Score?
- Ist MFA verpflichtend?
- Nutzen wir Conditional Access?
- Ist Legacy Authentication deaktiviert?
- Wird Microsoft Defender genutzt?

Microsoft Secure Score

Der Secure Score zeigt, wie gut Microsoft 365 abgesichert ist. Er ersetzt keine Risikoanalyse, liefert aber wertvolle Hinweise auf Verbesserungspotenzial.

Conditional Access

Nicht jede Anmeldung sollte erlaubt sein. Beispiele: ✓ nur bekannte Geräte · ✓ nur bestimmte Länder · ✓ nur verwaltete Endgeräte · ✓ Sperrung riskanter Anmeldungen

KI-Härtung

Microsoft integriert KI zunehmend in seine Sicherheitslösungen.

Wichtige Fragen

- ✓ Wer darf Copilot nutzen?
- ✓ Sind Berechtigungen aktuell?
- ✓ Sind vertrauliche Daten geschützt?
- ✓ Gibt es Data-Loss-Prevention-Regeln?
- ✓ Sind Sensitivity Labels eingerichtet?

Was steckt dahinter?

Data-Loss-Prevention-(DLP)-Regeln

Verhindern in Microsoft 365 den unbeabsichtigten oder unzulässigen Abfluss sensibler Daten – etwa das versehentliche Versenden vertraulicher Informationen per E-Mail oder das Teilen in der Cloud.

Sensitivity Labels

Klassifizieren Dokumente, E-Mails und andere Inhalte anhand ihrer Schutzbedürftigkeit und versehen diese automatisch mit Sicherheitsmaßnahmen wie Verschlüsselung oder Zugriffsbeschränkungen.

Mitarbeitende sensibilisieren

> **Mitarbeitende sind das Schutzschild des Unternehmens.**

Technik allein genügt nicht. Regelmäßige Schulungen zu folgenden Themen machen Mitarbeitende zu einem wichtigen Bestandteil der Sicherheitsstrategie:

Phishing

Deepfakes

CEO-Fraud

Passwörter

Meldewege

Schulungsangebote

Folgende Schulungen werden regelmäßig von der **Gem.DataSecure GmbH Wirtschaftsprüfungsgesellschaft** angeboten:

KOSTENLOS

Datenschutzschulung

„Die häufigsten Datenschutzpannen und deren Vermeidung"

Kostenlos für alle Mitarbeitenden

KOSTENLOS

KI-Datenschutzschulung

„Datenschutzrisiken beim Einsatz von KI"

Kostenlos für alle Mitarbeitenden

PFLICHTSCHULUNG

KI-Kompetenzschulung

„KI-Schulung für Mitarbeitende – Kompetenzerwerb gemäß Artikel 4 KI-Verordnung"

Pflicht für Mitarbeitende, die mit KI arbeiten (EU-KI-Verordnung)

Praxistipp & Entscheidung der Geschäftsführung

Praxistipp

Lassen Sie sich jährlich schriftlich bestätigen:

- ✓ Administratoren geprüft
- ✓ Updates aktuell
- ✓ Datensicherung getestet
- ✓ Secure Score bewertet
- ✓ kritische Risiken dokumentiert

Diese Dokumentation kann gegenüber Versicherern, Aufsichtsbehörden und im Rahmen einer Prüfung wertvoll sein.

Entscheidung der Geschäftsführung

Nach diesem Kapitel sollten Sie beantworten können:

- ☐ Wer besitzt Administratorrechte?
- ☐ Nutzen Administratoren FIDO2?
- ☐ Ist MFA verpflichtend?
- ☐ Ist Microsoft 365 gehärtet?
- ☐ Gibt es einen Passwortmanager?
- ☐ Gibt es eine Recovery-Mail?
- ☐ Werden Mitarbeitende regelmäßig geschult?

Cyberresilienz entsteht nicht durch möglichst viel Technik. Sondern durch klare Verantwortlichkeiten, sichere Administratoren, aktuelle Systeme, geschulte Mitarbeitende und regelmäßige Kontrolle.

MONTAG · 10:40 UHR

Der IT-Dienstleister sagt: *„Die gute Nachricht: Wir haben Backups."* Kurze Erleichterung. Dann folgt der nächste Satz: *„Jetzt müssen wir prüfen, ob wir sie überhaupt wiederherstellen können."* Nicht die Firewall entscheidet, ob Sie weiterarbeiten können – sondern Ihre Wiederherstellungsstrategie.

KAPITEL 5

Datensicherung, Cloud und Wiederherstellung

Warum Backups heute wichtiger sind als Firewalls

MONTAG · 10:40 UHR

Der IT-Dienstleister sagt: *„Die gute Nachricht: Es gibt Backups."*
Kurze Erleichterung. Dann folgt: *„Jetzt müssen wir prüfen, ob wir sie auch wiederherstellen können."*

Die wichtigste Erkenntnis

Backups schützen nicht vor einem Cyberangriff. Backups sorgen dafür, dass Ihre Organisation wieder arbeitsfähig wird.

Backups verhindern keinen Angriff – sie verkürzen die Betriebsunterbrechung.

Die eigentliche Währung: Zeit

Nach einem Cyberangriff zählt vor allem

Zeit

Nicht ✕ Server · ✕ Software · ✕ Hardware
Je schneller die Wiederherstellung, desto geringer der Schaden.

Was empfiehlt das BSI?

Datensicherungen müssen:

- ✓ regelmäßig erstellt werden
- ✓ getrennt gespeichert werden
- ✓ regelmäßig getestet werden
- ✓ dokumentiert werden
- ✓ gegen Veränderungen geschützt werden

Typische Fehler

- ✕ Backup nie getestet
- ✕ Backup dauerhaft mit dem Netzwerk verbunden
- ✕ Niemand kontrolliert den Erfolg
- ✕ Nur Daten gesichert
- ✕ Cloud nicht gesichert
- ✕ Administrator besitzt alleinigen Zugriff

Was ist das BSI? Das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** ist die Cybersicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. Weitere Informationen unter: **www.bsi.bund.de**

Die 3-2-1-1-0-Regel & Immutable Backups

⚠ Praxisbeispiel: Backup vorhanden. Nach dem Angriff stellt sich heraus: Die Datensicherung war seit sechs Monaten fehlerhaft. Niemand hatte jemals eine Rücksicherung getestet.

3 Kopien der Daten	**2** unterschiedliche Speichermedien	**1** Kopie außerhalb des Produktivsystems
1 unveränderbare (Immutable) Sicherung	**0** Fehler nach erfolgreichem Wiederherstellungstest	

Immutable Backups

Immutable bedeutet: Die Sicherung kann ✓ nicht verändert · ✓ nicht überschrieben · ✓ nicht gelöscht werden – auch dann nicht, wenn Administratorrechte kompromittiert wurden.

Cloud ersetzt kein Backup: Microsoft 365 sichern

Microsoft schützt

- ✓ Rechenzentrum
- ✓ Hardware
- ✓ Plattform

Sie bleiben verantwortlich für

- ✓ Ihre Daten
- ✓ Benutzer
- ✓ Berechtigungen
- ✓ Wiederherstellung

Microsoft 365 sichern – eigene Datensicherung für

- ✓ Exchange Online
- ✓ Outlook
- ✓ Teams
- ✓ SharePoint
- ✓ OneDrive
- ✓ Benutzer
- ✓ Gruppen
- ✓ Konfigurationen

⚠ Praxisbeispiel: Ein globales Administratorkonto wird übernommen. Innerhalb weniger Minuten werden Benutzer, Teams, SharePoint, OneDrive und Postfächer gelöscht. Frage: Wie stellen Sie diese Daten wieder her?

Wiederherstellung testen & Wiederanlaufplanung

Die wichtigste Frage lautet nicht „Haben wir Backups?" Sondern „Haben wir die Wiederherstellung erfolgreich getestet?"

Entscheidung der Geschäftsführung

Fragen Sie Ihren IT-Dienstleister:

- ✓ Wann wurde zuletzt zurückgesichert?
- ✓ Wie lange dauert die Wiederherstellung?
- ✓ Wer dokumentiert den Test?
- ✓ Welche Systeme wurden getestet?

Wiederanlaufplanung

Nicht alle Systeme gleichzeitig starten. Prioritäten festlegen.

1. Firewall / Internet
2. Identitätsmanagement
3. Microsoft 365
4. Telefonanlage
5. Fachverfahren
6. Buchhaltung
7. Archivsysteme

RPO, RTO und Passwortmanager

RPO – Wie viel Datenverlust ist akzeptabel?

Stellen Sie sich vor, Ihr System fällt aus. Wie weit darf die Wiederherstellung zurückgehen?

- RPO = 15 Minuten → maximal 15 Minuten Datenverlust
- RPO = 24 Stunden → maximal 1 Tag Datenverlust

Je kürzer das RPO, desto häufiger muss gesichert werden.

RTO – Wie lange darf ein System ausfallen?

Nicht jedes System ist gleich wichtig.

- Telefonanlage: max. 2 Stunden
- Buchhaltung: max. 24 Stunden
- Archiv: max. 3 Tage

Legen Sie Prioritäten fest – bevor der Ernstfall eintritt.

Passwortmanager

Passwörter gehören nicht in:
❌ Outlook · ❌ Excel · ❌ Browser · ❌ Notizzettel
Empfehlung:
✓ Professioneller Passwortmanager
✓ Rollen- und Rechtekonzept
✓ Notfallzugriff geregelt

Recovery-Mail

Passwort-Rücksetzungen niemals über die normale Firmen-E-Mail abwickeln.

Empfehlung:
✓ Separate Recovery-Mail-Adresse
✓ Mit MFA gesichert
✓ FIDO2-Stick
✓ Nur wenige Berechtigte

Die Cyber-Notfallliste

Nicht digital. Sondern zusätzlich in Papierform. Inhalt

- ✓ Ansprechpartner
- ✓ Cyber-Versicherungsnummer
- ✓ Administratoren
- ✓ IT-Dienstleister
- ✓ Internetprovider
- ✓ Telefonanbieter
- ✓ Datenschutzbeauftragter
- ✓ Wiederanlaufplan

Unser Praxistipp

Viele Organisationen speichern alle Kontakte nur in Outlook. Nach einem Cyberangriff ist Outlook häufig nicht mehr erreichbar.

Empfehlung: Die wichtigsten Notfallkontakte zusätzlich analog vorhalten.

Service für Mandanten

- Auf Wunsch unterstützen wir Sie dabei, eine aktuelle Cyber-Notfallkontaktliste zu erstellen.
- Diese muss außerhalb der eigenen IT aufbewahrt werden – so bleiben wichtige Ansprechpartner auch dann erreichbar, wenn Ihre EDV vollständig ausgefallen ist.
- Ihre Notfallliste können Sie uns gern zusenden – wir hinterlegen diese sicher in unserem Datenschutzmanagementsystem. Wir sind 365 Tage im Jahr für Sie erreichbar.

Entscheidung der Geschäftsführung

Nach diesem Kapitel sollten Sie beantworten können:

- ☐ Besitzen wir ein eigenes Cloud-Backup?
- ☐ Testen wir regelmäßig die Wiederherstellung?
- ☐ Kennen wir unser RPO?
- ☐ Kennen wir unser RTO?
- ☐ Gibt es einen Wiederanlaufplan?
- ☐ Gibt es eine Cyber-Notfallliste?
- ☐ Brauchen wir eine Cyberversicherung?

Die wichtigste Erkenntnis

Die Frage lautet nicht *„Haben wir Backups?"*
Sondern *„Wie schnell können wir morgen wieder arbeiten?"*

MONTAG · 11:30 UHR

Die ersten Systeme lassen sich vermutlich wiederherstellen. Doch jetzt stellt der Geschäftsführer die nächste Frage: *„Wen müssen wir jetzt informieren?"* Die Antwort entscheidet häufig über Versicherungsschutz, Datenschutz, Kommunikation und den weiteren Verlauf des Vorfalls.
„Was tun wir eigentlich, wenn es passiert ist?"

KAPITEL 6

Cyberangriff – Die ersten 24 Stunden

Wer muss wann informiert werden?

MONTAG · 11:30 UHR

Der Angriff ist bestätigt.

- Server verschlüsselt
- Microsoft 365 kompromittiert
- Administratoren betroffen
- Betrieb steht weitgehend still

Die Geschäftsführung fragt: *„Was machen wir jetzt zuerst?"*

Die wichtigste Erkenntnis

Ein Cyberangriff ist nicht nur ein IT-Vorfall. Er ist gleichzeitig Unternehmenskrise · Datenschutzvorfall · Kommunikationskrise · Organisationskrise

Ein Cyberangriff ist zuerst eine Managementaufgabe – erst danach ein IT-Problem.

Die ersten 15 Minuten

> **Ruhe bewahren. Nicht hektisch handeln.**

✓ Sofort handeln

- Krisenstab bilden: Geschäftsführung, IT-Dienstleister, Datenschutzbeauftragter
- Angriff dokumentieren
- Systeme isolieren

✗ Was Sie NICHT tun sollten

- Server sofort ausschalten
- Festplatten formatieren
- Benutzer löschen
- Beweise vernichten
- Lösegeld vorschnell bezahlen

Wer muss informiert werden?

1. Geschäftsführung
2. IT-Dienstleister
3. Cyberversicherung
4. Datenschutzbeauftragter
5. IT-Forensik (falls erforderlich)
6. ZAC – Zentrale Ansprechstelle Cybercrime?

ZAC – Zentrale Ansprechstelle Cybercrime

Die ZAC gibt es in jedem Bundesland und ist die zentrale Ansprechstelle Cybercrime der Polizeien für Wirtschaftsunternehmen.

Die ZAC unterstützt Sie **kostenlos** durch eine erste Einschätzung der Lage, Beratung im Ernstfall, Einleitung notwendiger Schritte zur Strafverfolgung, Koordination mit Ermittlungsbehörden.
⚠ **Wichtiger Hinweis:** Die ZAC ist zur Sicherung von Beweismitteln berechtigt – dies kann bedeuten, dass Server oder andere Geräte mitgenommen werden. Deshalb gilt: Nur wer ein aktuelles, funktionsfähiges Backup besitzt, kann in diesem Fall die Arbeitsfähigkeit schnell wiederherstellen.
Weitere Informationen: **www.polizei.de – ZAC**

Cyberversicherung, ZAC und IT-Forensik

Cyberversicherung – Warum zuerst informieren?

Viele Versicherer organisieren:

✓ IT-Forensiker
✓ Spezialanwälte
✓ Krisenkommunikation
✓ Verhandlungsexperten
✓ Wiederherstellung

Erst die Versicherung informieren – dann weitere Maßnahmen abstimmen.

Zentrale Ansprechstelle Cybercrime (ZAC)

Die ZAC bietet Ihnen ein umfangreiches Beratungsangebot zu Präventionsmöglichkeiten an und unterstützt bei strafrechtlich relevanten Fällen.

Praxistipp: Hinterlegen Sie die Kontaktdaten der für Ihre Organisation zuständigen ZAC bereits heute in der Cyber-Notfallliste.

IT-Forensik – Wann ist sie sinnvoll?

- ✓ Ransomware
- ✓ Datendiebstahl
- ✓ kompromittierte Administratoren
- ✓ unbekannter Angriffsweg
- ✓ möglicher Versicherungsfall

Datenschutz und Bußgelder

Datenschutz

Ein Cyberangriff kann gleichzeitig eine Datenschutzverletzung sein durch Zugriff auf Personaldaten, Gesundheitsdaten, Klientendaten , Spendendaten, E-Mail-Archive, Geschäftsgeheimnisse

DSGVO – Prüfen Sie frühzeitig

- ✓ Liegt eine Datenschutzverletzung vor?
- ✓ Welche Daten sind betroffen?
- ✓ Welche Risiken bestehen?
- ✓ Muss die Datenschutzaufsichtsbehörde informiert werden?
- ✓ Müssen Betroffene informiert werden?

Benachrichtigung Betroffener

Die Information an Betroffene gestaltet sich häufig schwierig – da nach einem Cyberangriff der Zugriff auf Kontaktdaten oft nicht mehr möglich ist. Diesen Zeitvorsprung nutzen Angreifer für Phishing-Attacken.

Bußgelder

Nicht jeder Cyberangriff führt zu einem Bußgeld. Aber: Fehlende oder unzureichende technische und organisatorische Maßnahmen (TOM) können aufsichtsrechtliche Konsequenzen haben.

Die Datenschutzaufsichtsbehörden fragen grundsätzlich:

✓ Warum war der Angriff möglich?
✓ Welche TOM bestanden?
✓ Gab es MFA?
✓ Wurden sicherheitsrelevante Updates installiert? Wann?
✓ Gab es getestete Backups?
✓ Liegen Auftragsverarbeitungsverträge vor?
✓ Welche Maßnahmen zur Vermeindung werden künftig umgesetzt?

Folgen einer Datenschutzverletzung

Bußgelder

Die Datenschutzaufsichtsbehörde kann empfindliche Bußgelder verhängen – auch bei kleinen Organisationen.

Schadensersatzklagen

Sofern Betroffene einen immateriellen oder materiellen Schaden durch die Datenschutzpanne erleiden, können Schadensersatzklagen folgen.

Reputationsverlust

Datenschutzpannen führen nahezu immer zu einem erheblichen Reputationsverlust – bei Klienten, Spendern, Mitarbeitenden und der Öffentlichkeit.

Kommunikation und Dokumentation

Kommunikation – Wer spricht?

Nicht jeder. Nur benannte Personen. Kommunikation mit: ✓ Mitarbeitenden · ✓ Klienten · ✓ Angehörigen · ✓ Spendern · ✓ Fördermittelgebern · ✓ Presse

Mitarbeitende informieren

Mitarbeitende müssen wissen: ✓ Welche Systeme dürfen genutzt werden? · ✓ Welche Passwörter sind zu ändern? · ✓ Wer ist Ansprechpartner? · ✓ Welche Informationen dürfen weitergegeben

"Pressearbeit" - Kommunikation nach außen

Keine Spekulationen. Keine Schuldzuweisungen. Nur bestätigte Informationen. Ein einheitlicher Ansprechpartner. Oft können Informationen nur über die Homepage des Unternehmens veröffentlicht werden. Sie sind ja nicht erreichbar.

Aktueller Fall: Das Institut der Wirtschaftsprüfer war vor kurzem Ziel eines Cyberangriffs und konnte dies nur über Ihre Homepage mitteilen. Nach 4 Wochen kam eine E-Mail an rd. 8.000 Wirtschaftsprüfer, das man nicht ausschließen könne, das hochsensible Daten abgeflossen seien und man Wachsam sein sollte.

Dokumentation – Von Beginn an dokumentieren

- ✓ Uhrzeit
- ✓ Entscheidungen
- ✓ Ansprechpartner
- ✓ Maßnahmen
- ✓ Meldungen
- ✓ Wiederherstellung

Diese Dokumentation hilft später der Versicherung, der Datenschutzaufsicht, der Polizei und der Geschäftsführung.

Die Cyber-Notfallliste sollte enthalten

✓ Cyberversicherung · ✓ IT-Dienstleister · ✓ Geschäftsführer · ✓ Datenschutzbeauftragter · ✓ Internetprovider · ✓ Telefonanbieter · ✓ Administratoren · ✓ Microsoft-Partner · ✓ ZAC · ✓ Datenschutzaufsichtsbehörde

Praxistipps: Notfallkontakte und Notfallübung

💡 Praxistipp 1: Notfallkontakte

Viele Organisationen stellen erst im Ernstfall fest, dass sämtliche Telefonnummern nur noch in Outlook gespeichert waren.

Empfehlung:

- ✓ Wichtigste Notfallkontakte ausgedruckt vorhalten
- ✓ Sicher außerhalb der eigenen IT aufbewahren

🔥 Praxistipp 2: Notfallübung

Ein Notfallplan, der nie getestet wurde, ist im Ernstfall häufig wertlos.

Empfehlung:

- ✓ Mindestens einmal jährlich eine Cyber-Notfallübung durchführen
- ✓ Realistische Szenarien simulieren
- ✓ Ergebnisse dokumentieren und Maßnahmen ableiten

□ Service für Mandanten

Auf Wunsch unterstützen wir Sie dabei, eine aktuelle Notfallkontaktliste zu erstellen und diese – nach entsprechender Vereinbarung – in unserem Datenschutzmanagementsystem vertraulich außerhalb Ihrer IT zu hinterlegen.

- ✓ Erreichbarkeit wichtiger Ansprechpartner auch bei Ausfall von Outlook, Microsoft 365 oder Intranet

Entscheidung der Geschäftsführung

Nach diesem Kapitel sollten Sie beantworten können:

- ☐ Gibt es einen Krisenstab?
- ☐ Wer informiert die Cyberversicherung?
- ☐ Wer informiert den Datenschutzbeauftragten?
- ☐ Wer kommuniziert nach außen?
- ☐ Wo befinden sich die wichtigsten Notfallkontakte?
- ☐ Wurde der Notfallplan bereits geübt?

Die wichtigste Erkenntnis

Ein Cyberangriff lässt sich nicht immer verhindern. Chaos dagegen schon.

Gute Organisation ist die beste Krisenbewältigung.

MONTAG · 17:45 UHR

Die ersten Systeme laufen wieder. Der Geschäftsführer fragt: *„Wie verhindern wir, dass uns das noch einmal passiert?"* Der IT-Dienstleister antwortet: *„Hundertprozentige Sicherheit gibt es nicht."*

KAPITEL 7

Cyberresilienz:
Warum es keinen 100-%-Schutz gibt

MONTAG · 17:45 UHR

Die ersten Systeme funktionieren wieder.

- Outlook läuft.
- Die Telefonanlage ist erreichbar.
- Die Buchhaltung arbeitet.
- Die ersten Klientendaten sind wieder verfügbar.

Der Geschäftsführer fragt: *„Wie verhindern wir, dass uns das noch einmal passiert?"*

Die Antwort

Der IT-Dienstleister antwortet: *„Gar nicht."* Kurze Pause. Dann ergänzt er: *„Wir können das Risiko deutlich reduzieren. Einen hundertprozentigen Schutz wird es aber niemals geben."*

Warum?

Jeden Tag entstehen neue Sicherheitslücken · neue Schadprogramme · neue Betrugsmaschen · neue KI-Werkzeuge

Hinzu kommen menschliche Fehler · Fehlkonfigurationen · Lieferkettenangriffe · Angriffe auf Ihre Auftragsverarbeiter - Insider · Hardwaredefekte

Es gibt keinen 100-%-Schutz

Es gibt

- ❌ keine perfekte Firewall
- ❌ keinen perfekten Virenschutz
- ❌ keine perfekte Cloud
- ❌ keine perfekte Software

Es gibt nur

✓ gut vorbereitete Organisationen

Cyberresilienz bedeutet

Nicht ❌ niemals angegriffen werden.
Sondern: ✓ Angriffe erkennen · ✓ Schäden begrenzen · ✓ schnell reagieren · ✓ Systeme wiederherstellen · ✓ aus jedem Vorfall lernen.

Unsere Geschichte – Warum hat unsere Organisation überlebt?

Nicht wegen ❌ der Firewall · ❌ des Virenscanners
Sondern weil ✓ Backups vorhanden waren · ✓ Verantwortlichkeiten geregelt waren · ✓ Entscheidungen getroffen wurden · ✓ Systeme wiederhergestellt werden konnten.

Was wäre ohne Vorbereitung passiert?

Keine Backups. Keine Administratorübersicht. Keine Verantwortlichkeiten. Keine Cyberversicherung. Keine Ansprechpartner. Kein Notfallplan. Bußgelder. Schadensersatzklagen. Reputationsverlust.

⚠ Ergebnis: Aus einer Krise wäre schnell eine existenzbedrohende Situation geworden.

Die 10 goldenen Regeln der Cyberresilienz

01

Cyberresilienz ist Führungsaufgabe.

02

Administratoren besonders schützen.

03

Cloud ersetzt kein Backup.

04

Backups regelmäßig testen.

05

Sicherheitsupdates zeitnah installieren.

06

MFA ist heute Standard.

07

FIDO2 für privilegierte Konten.

08

Mitarbeitende regelmäßig sensibilisieren.

09

Cyber-Notfallplan regelmäßig üben.

10

Aus jedem Vorfall lernen.

Was können Sie morgen tun?

- ✓ Administratorrechte überprüfen
- ✓ MFA verpflichtend einführen
- ✓ FIDO2 für Administratoren bestellen
- ✓ Cloud-Backup prüfen
- ✓ Notfallkontakte ausdrucken
- ✓ Cyberresilienz auf die Agenda der nächsten Vorstandssitzung setzen

Die wichtigsten Fragen

Nicht *„Werden wir angegriffen?"* Sondern *„Wie schnell arbeiten wir danach wieder?"*
Nicht *„Haben wir Backups?"* Sondern *„Haben wir die Wiederherstellung getestet?"*
Nicht *„Haben wir Microsoft 365?"* Sondern *„Können wir Microsoft 365 vollständig wiederherstellen?"*
Nicht *„Haben wir Administratoren?"* Sondern *„Sind Administratoren besser geschützt als alle anderen Benutzer?"*
Nicht *„Ist unsere IT sicher?"* Sondern *„Ist unsere Organisation resilient?"*

Entscheidung der Geschäftsführung

Nach diesem Webinar sollte beschlossen werden:

- ✓ **Cyberresilienz als festen Tagesordnungspunkt aufnehmen**
- ✓ **Administratorrechte überprüfen**
- ✓ **Microsoft 365 absichern**
- ✓ **Wiederherstellung testen**
- ✓ **Cyber-Notfallplan erstellen bzw. aktualisieren**
- ✓ **Mitarbeitende regelmäßig sensibilisieren**

Unser Fazit

Praxistipp

Cyberresilienz ist heute Bestandteil einer ordnungsgemäßen Unternehmensführung. Dokumentieren Sie Entscheidungen, Risiken, Maßnahmen, Kontrollen und Notfallübungen.

Eine gute Dokumentation hilft der Geschäftsführung, der Cyberversicherung, der Datenschutzaufsicht und Ihrer eigenen Organisation.

Unser Fazit

Cyberresilienz ist kein Projekt. Keine Software. Kein Produkt.

Cyberresilienz ist eine dauerhafte Führungsaufgabe.

Nicht der Cyberangriff entscheidet über die Zukunft Ihrer Organisation. Sondern Ihre Vorbereitung.

PRAXISBLOCK

Cyberresilienz in der Praxis

Das können Sie morgen umsetzen

Teil 1: Die 10 häufigsten Fehler nach einem Cyberangriff

Fehler Nr. 1: Die Cyberversicherung zu spät informieren

Viele Versicherungsverträge verlangen eine unverzügliche Schadenmeldung. Verspätete Meldungen können die Schadenregulierung erschweren.

Erst informieren – dann handeln.

Fehler Nr. 2: Sofort alle Server ausschalten

Dadurch können Beweise verloren gehen, Wiederherstellungen erschwert werden und forensische Untersuchungen beeinträchtigt werden. Nur abgestimmt handeln.

Fehler Nr. 3: Lösegeld vorschnell bezahlen

Eine Zahlung garantiert keine Entschlüsselung, keine Datenrückgabe und keine Nichtveröffentlichung. Die Entscheidung sollte niemals ohne Abstimmung mit Cyberversicherung, IT-Forensik und Rechtsberatung erfolgen.

Die 10 häufigsten Fehler (Fortsetzung)

Fehler Nr. 4: Den Datenschutzbeauftragten vergessen

Bereits der Verdacht auf einen Datenschutzvorfall kann eine Prüfung erforderlich machen. Nicht erst Tage später informieren.

Fehler Nr. 5: Administratorpasswörter nicht ändern

Nach erfolgreicher Wiederherstellung müssen Administratoren, privilegierte Konten und Servicekonten überprüft und gegebenenfalls neu abgesichert werden.

Fehler Nr. 6: Mitarbeitende nicht informieren

Unsicherheit erzeugt Gerüchte. Informieren Sie frühzeitig, was passiert ist, was zu tun ist und welche Systeme genutzt werden dürfen.

Fehler Nr. 7: Wiederherstellung nie getestet

Ein Backup ist erst dann wertvoll, wenn die Rücksicherung funktioniert.

Fehler Nr. 8: Nur die Technik betrachten

Cyberangriffe betreffen Organisation · Kommunikation · Datenschutz · Personal · IT

Fehler Nr. 9: Nach dem Angriff nichts ändern

Jeder Vorfall muss ausgewertet werden. Fragen Sie: Was hat funktioniert? Was müssen wir verbessern?

Fehler Nr. 10: Glauben, dass es uns nicht noch einmal trifft

Cyberresilienz ist kein einmaliges Projekt. Sie ist ein kontinuierlicher Verbesserungsprozess.

Teil 2: Die 10 wichtigsten Fragen an Ihren IT-Dienstleister

1. **Wann wurden zuletzt Sicherheitsupdates installiert?**
2. **Wann wurde zuletzt eine Rücksicherung erfolgreich getestet?**
3. **Wie viele Administratoren besitzen wir?**
4. **Sind Administratoren mit FIDO2 abgesichert?**
5. **Existiert ein Microsoft-365-Backup?**
6. **Wie hoch ist unser Microsoft Secure Score?**
7. **Ist Conditional Access eingerichtet?**
8. **Welche Systeme besitzen keinen Herstellersupport mehr?**
9. **Wie lange dauert eine vollständige Wiederherstellung?**
10. **Welche Maßnahmen empfehlen Sie uns kurzfristig?**

Ein guter IT-Dienstleister erklärt verständlich, transparent und nachvollziehbar, welche Risiken bestehen und welche Maßnahmen sinnvoll sind.

Teil 3: 10 Maßnahmen, die Sie morgen umsetzen können

- ✓ Administratorrechte überprüfen
- ✓ FIDO2-Sticks bestellen
- ✓ Passwortmanager prüfen
- ✓ Vorstand informieren
- ✓ Cyberversicherung griffbereit halten
- ✓ Recovery-Mail einrichten
- ✓ Notfalltelefonnummern ausdrucken
- ✓ Cloud-Backup hinterfragen
- ✓ Patchmanagement prüfen
- ✓ Mitarbeitende sensibilisieren

Die Cyber-Notfallliste

Die Cyber-Notfallliste sollte enthalten

- ✓ Cyberversicherung
- ✓ Ansprechpartner
- ✓ IT-Dienstleister
- ✓ Datenschutzbeauftragter
- ✓ Internetprovider
- ✓ Administratoren
- ✓ Wiederanlaufplan
- ✓ Notfalltelefonnummern

Unser Praxistipp

Viele Organisationen stellen erst im Ernstfall fest, dass alle wichtigen Telefonnummern nur digital gespeichert waren. Wir empfehlen, eine aktuelle Notfallkontaktliste zusätzlich analog vorzuhalten.

Auf Wunsch unterstützen wir unsere Mandanten bei der Zusammenstellung und sicheren Hinterlegung dieser Kontakte ggf. in unserem 2FA abgesichertem Datenschutzmanagementsystem.

Der Gem.Sicherheitscheck

> „Wie gut sind Sie wirklich vorbereitet?"

Was ist der Gem.Sicherheitscheck?

Auf Basis eines standardisierten Fragenkatalogs werden Schwachstellen in Ihrer IT-Infrastruktur schnell und systematisch erkannt.

Anbieter: Gem.IT GmbH – aus unserem Netzwerk

Was passiert danach?

- ✓ Auswertung der Ergebnisse
- ✓ Identifikation konkreter Handlungsfelder
- ✓ Stärkung Ihrer Cyberresilienz durch Ihren EDV-Dienstleister oder die **Gem.IT GmbH** (bei gesonderter Beauftragung)
- ✓ Systematische Weiterentwicklung Ihrer IT-Sicherheit

Weitere Informationen: www.gem-gruppe.de/it-digitalisierung

> ***„Cyberresilienz ist kein Zustand – sondern ein kontinuierlicher Verbesserungsprozess."***

Ich wünsche Ihnen, dass Ihre Organisation niemals Opfer eines Cyberangriffs wird. Sollte es dennoch passieren, wünsche ich Ihnen vor allem eines: Dass Sie vorbereitet sind und Ihren Auftrag schnell wieder erfüllen können.

Kontakt

Dr. Ralf C. Güstel

IT-Security-Auditor · Wirtschaftsprüfer

Gem.DataSecure GmbH Wirtschaftsprüfungsgesellschaft
Weidestrasse 134 · 22083 Hamburg

r.guestel@gem-gruppe.de
040 - 879 779 513
www.gem-gruppe.de