



Unsere IT läuft – oder?

10 IT-Sicherheitsfragen, die sich jedes KMU stellen sollte



WAS PASSIERT, WENN IHRE IT MORGEN NICHT MEHR FUNKTIONIERT?

Solange alles läuft, ist IT-Sicherheit für viele Unternehmen kein großes Thema. Erst wenn Systeme ausfallen, Daten fehlen oder der Betrieb stillsteht, wird klar, wie abhängig der Arbeitsalltag von funktionierender IT ist.

Cyberangriffe, Datenverluste und IT-Ausfälle betreffen längst nicht mehr nur große Konzerne. Gerade kleine und mittlere Unternehmen geraten zunehmend in den Fokus – oft, weil grundlegende Schutzmaßnahmen fehlen oder über Jahre gewachsen sind, ohne regelmäßig überprüft zu werden.

Genau hier setzt dieser IT-Check an. Er gibt Ihnen einen verständlichen, praxisnahen Überblick über die wichtigsten Sicherheitsbereiche und hilft Ihnen einzuschätzen, wie gut Ihre IT aktuell aufgestellt ist – ohne Fachchinesisch, ohne Blabla.

Und falls beim Durchgehen Fragen entstehen oder Sie tiefer einsteigen möchten: Wir unterstützen Sie gern unverbindlich dabei, Ihre individuelle Situation einzuordnen. Denn welche Maßnahmen sinnvoll sind, hängt stark von Branche, Unternehmensgröße und Arbeitsweise ab – und genau das lässt sich am besten persönlich klären.

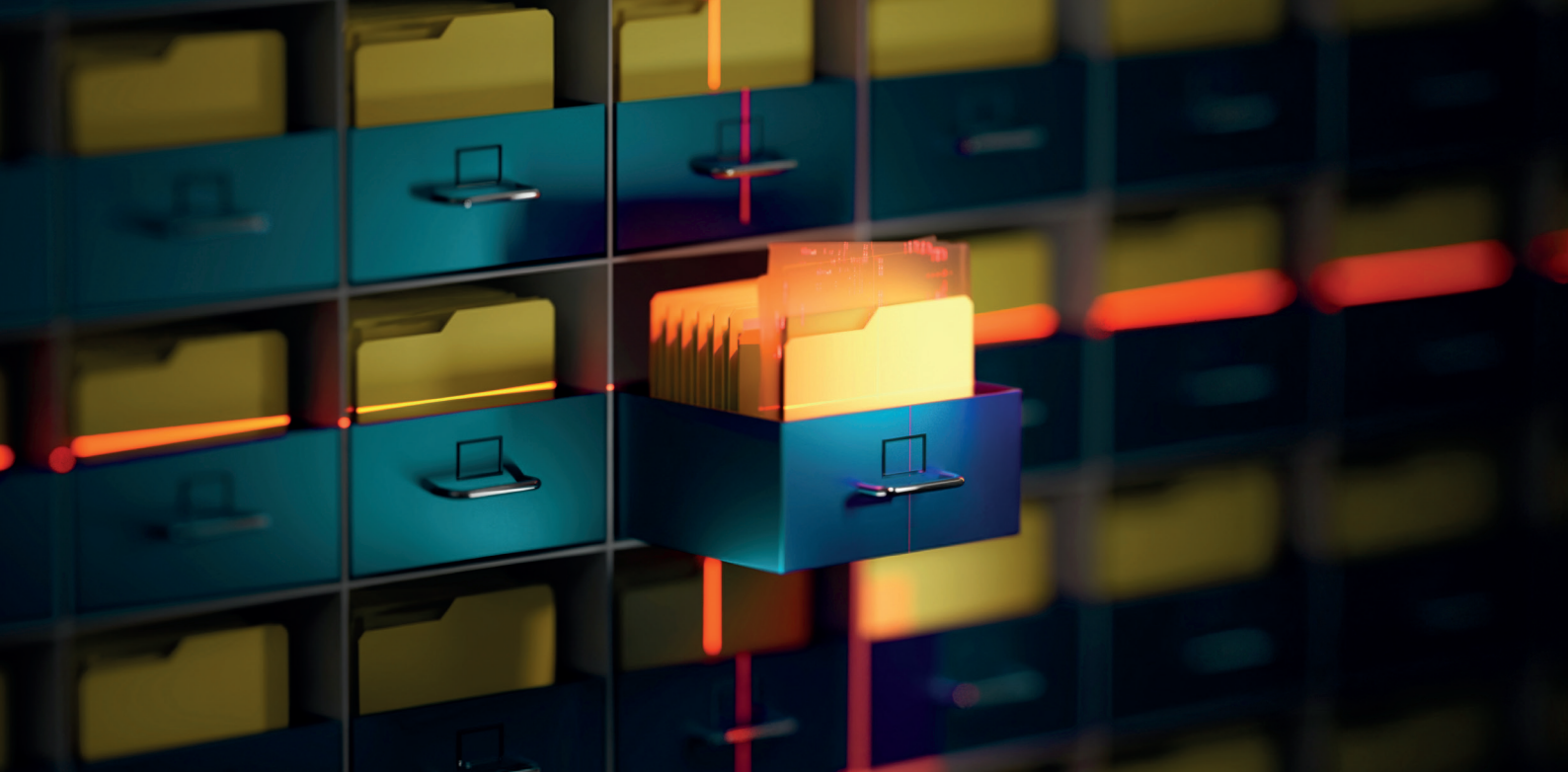
Was Sie in diesem IT-Check erwartet

- Datensicherung (Backup)
- Passwörter
- Multi-Faktor-Authentifizierung (MFA)
- Software-Updates
- Firewall & Netzwerksicherheit
- Virenschutz & Malware-Abwehr
- Mitarbeiter-Sensibilisierung
- Notfallplanung
- Verschlüsselung
- Zugriffsverwaltung

So nutzen Sie diesen IT-Check

Gehen Sie die Kapitel Schritt für Schritt durch und markieren Sie, wo Sie bereits gut aufgestellt sind – und wo Unsicherheiten bestehen. Nicht alles muss sofort perfekt sein. Wichtig ist, die größten Risiken zu erkennen und gezielt anzugehen.





1. DATENSICHERUNG (BACKUP) – IHR DIGITALER RETTUNGSANKER

Warum ist das wichtig?

Stellen Sie sich vor, morgen früh funktioniert keiner Ihrer Computer mehr. Alle Kundendaten, Rechnungen, Projekte – weg. Ein Albtraum, der leider Realität werden kann: durch Ransomware-Angriffe, Hardwaredefekte, Feuer oder einfach menschliche Fehler.

Die 3-2-1-Backup-Regel

Eine bewährte Methode für sichere Datensicherung ist die sogenannte 3-2-1-Regel:



3 Kopien Ihrer wichtigen Daten: Das Original plus zwei Backups



Auf 2 verschiedenen Speichermedien (z.B. lokale Festplatte und Cloud)



Mindestens 1 Kopie außer Haus (z.B. in einem Rechenzentrum oder Cloud-Speicher)

Moderne Erweiterung – die 3-2-1-1-0-Regel:

Zusätzlich zu den oben genannten Punkten:

- 1 unveränderliches Backup (immutable), das selbst von Administratoren nicht gelöscht werden kann – wichtig zum Schutz vor Ransomware
- 0 Fehler bei der Wiederherstellung – regelmäßige Tests sind Pflicht



Was Sie überprüfen sollten:



Werden regelmäßig Backups erstellt?

Tägliche Backups sind für die meisten Unternehmen sinnvoll. Überlegen Sie: Wie viel Datenverlust können Sie sich leisten? Die Daten von einem Tag, einer Woche oder einem Monat?



Sind die Backups automatisiert?

Manuelle Backups werden gerne vergessen. Automatische Lösungen sind zuverlässiger.



Wird ein Backup außer Haus aufbewahrt?

Bei einem Brand oder Einbruch vor Ort sollte mindestens eine Kopie Ihrer Daten sicher sein.



Wurden die Backups jemals getestet?

Ein Backup, das sich nicht wiederherstellen lässt, ist wertlos. Führen Sie regelmäßig (mindestens halbjährlich) Wiederherstellungstests durch.



Wie lange würde eine vollständige Wiederherstellung dauern?

Kennen Sie die Antwort? Falls nicht, sollten Sie das mit Ihrem IT-Dienstleister klären.



2. PASSWÖRTER – IHRE ERSTE VERTEIDIGUNGSLINIE

Warum ist das wichtig?

Passwörter sind nach wie vor der häufigste Weg, um auf Unternehmenssysteme zuzugreifen. Schwache oder kompromittierte Passwörter sind eine Einladung für Cyberkriminelle. Laut aktuellen Studien sind über 80% aller erfolgreichen Hackerangriffe auf kompromittierte Anmeldedaten zurückzuführen.

Was macht ein sicheres Passwort aus?

Moderne Empfehlungen:

- Mindestens 12 Zeichen lang (besser 16 oder mehr)
- Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Keine Wörter aus dem Wörterbuch oder persönliche Informationen (Namen, Geburtsdaten)
- Keine mehrfache Verwendung – jedes System bekommt ein eigenes Passwort
- Keine regelmäßigen Änderungen erzwingen – nur bei Verdacht auf Kompromittierung (viele Menschen neigen sonst zu leicht zu erratenden Variationen)

Tipp für merkbare Passwörter:

Denken Sie sich einen Satz aus und nehmen Sie die Anfangsbuchstaben: „Mein Sohn wurde 2015 in Lüneburg geboren!“ wird zu „MSw2015iLg!“.

Was Sie überprüfen sollten:



Gibt es eine Passwortrichtlinie in Ihrem Unternehmen?

Alle Mitarbeiter sollten wissen, wie ein sicheres Passwort aussieht.



Werden Passwörter sicher aufbewahrt?

Post-its am Monitor sind tabu! Ein Passwort-Manager ist die bessere Lösung.



Nutzen Sie einen Passwort-Manager?

Es gibt verschiedene Tools, die dabei helfen, viele komplexe Passwörter sicher zu verwalten.



Ist die Multi-Faktor-Authentifizierung (MFA) aktiviert?

Besonders für E-Mail-Konten, Cloud-Dienste und administrative Zugänge ist MFA unverzichtbar (mehr dazu im nächsten Kapitel).





3. MULTI-FAKTOR-AUTHENTIFIZIERUNG (MFA) – DIE DOPPELTE SICHERHEIT

Warum ist das wichtig?

Selbst das beste Passwort kann gestohlen werden – durch Phishing-E-Mails, Datenlecks oder Keylogger. Die Multi-Faktor-Authentifizierung fügt eine zusätzliche Sicherheitsebene hinzu: Selbst wenn Ihr Passwort in falsche Hände gerät, können Angreifer ohne den zweiten Faktor nicht auf Ihre Systeme zugreifen.

Wie funktioniert MFA?

MFA kombiniert mindestens zwei der folgenden Faktoren:

1

Wissen

Etwas, das Sie wissen (z.B. Passwort, PIN)

2

Besitz

Etwas, das Sie haben (z.B. Smartphone, USB-Token)

3

Identität

Etwas, das Sie sind (z.B. Fingerabdruck, Gesichtserkennung)

Typisches Beispiel:

Sie melden sich mit Ihrem Passwort an und erhalten dann einen Bestätigungscode auf Ihr Smartphone, den Sie zusätzlich eingeben müssen.



Was Sie überprüfen sollten:



Ist MFA für E-Mail-Konten aktiviert?

E-Mails sind oft das Einfallstor für Angriffe – schützen Sie sie besonders gut.



Nutzen Sie MFA für Cloud-Dienste?

Microsoft 365, Google Workspace und andere Cloud-Anwendungen bieten MFA – aktivieren Sie sie.



Sind administrative Zugänge mit MFA geschützt?

Konten mit weitreichenden Berechtigungen sollten höchste Priorität haben.



Ist MFA für VPN-Zugänge aktiv?

Fernzugriffe auf Ihr Netzwerk sollten durch MFA abgesichert sein.



Gibt es einen Plan für verlorene MFA-Geräte?

Was passiert, wenn ein Mitarbeiter sein Smartphone verliert? Haben Sie Backup-Codes oder alternative Verfahren?

4. SOFTWARE-UPDATES – SCHLIESSEN SIE DIE SICHERHEITSLÜCKEN

Warum ist das wichtig?

Software-Hersteller entdecken ständig Sicherheitslücken in ihren Produkten und veröffentlichen Updates (Patches), um diese zu schließen. Ohne regelmäßige Updates bleiben diese Lücken offen – und Cyberkriminelle wissen genau, wo sie ansetzen können.

Wichtige Bausteine:

1 Automatische Updates

Viele Systeme (Windows, macOS, Browser, Office, Antivirus) installieren Sicherheitsupdates automatisch.

2 Geplante Wartungsfenster

Bei Servern, Fachanwendungen oder geschäftskritischen Systemen empfiehlt sich ein festes „Wartungsfenster“ – z. B. Mittwohabend 20–22 Uhr.

3 Auch „unsichtbare“ Systeme nicht vergessen

Nicht nur Programme am PC benötigen Updates. Vieles läuft im Hintergrund – und genau dort entstehen oft die größten Risiken. Dazu gehören z. B.: Router und Firewalls, Netzwerk-Switches und WLAN-Access-Points, Drucker und Scanner, Telefonanlagen, Zeiterfassung und Zutrittssysteme sowie Fachanwendungen auf Servern



Was Sie überprüfen sollten:



Sind automatische Updates aktiviert?

Für Betriebssysteme (Windows, macOS) und wichtige Software sollten automatische Updates eingeschaltet sein.



Gibt es einen Verantwortlichen für Updates?

Jemand sollte regelmäßig überprüfen, ob alle Systeme aktuell sind – besonders Server und Netzwerkgeräte.



Wie schnell werden kritische Sicherheitsupdates installiert?

Für kritische Updates sollten Sie einen Prozess haben, um sie innerhalb von 48 Stunden einzuspielen.



Werden auch Anwendungen von Drittanbietern aktualisiert?

Denken Sie an Adobe Reader, Java, Browser, Buchhaltungssoftware etc.



Setzen Sie noch veraltete Software ein?

Software ohne Sicherheitsupdates (z.B. alte Windows-Versionen) ist ein massives Sicherheitsrisiko und sollte ersetzt werden.

Handlungsempfehlung:

Etablieren Sie einen geregelten Update-Prozess. Bei größeren Systemen macht es Sinn, Updates zunächst in einer Testumgebung zu prüfen, bevor sie im Produktivsystem eingespielt werden.



5. FIREWALL UND NETZWERKSICHERHEIT – DER SCHUTZWALL UM IHRE DATEN

Warum ist das wichtig?

Eine Firewall kontrolliert den Datenverkehr zwischen Ihrem Netzwerk und dem Internet. Sie ist wie ein Türsteher, der entscheidet, wer rein und raus darf.

Router-Firewall vs. professionelle Firewall – wo liegt der Unterschied?

Viele Router – egal ob von der FritzBox bis zum Business-Router – besitzen eine eingebaute „Firewall“. Das führt schnell zu dem Gedanken: „Wir haben doch schon eine Firewall, warum brauchen wir noch eine zusätzliche?“

Aber es gibt dabei entscheidende Unterschiede:

Router-Firewall (Basis-Schutz)

Die Firewall im Router übernimmt nur grundlegende Aufgaben: Sie blockiert ungewollte Verbindungen aus dem Internet ins Firmennetz („Stateful Inspection“). Sie sorgt dafür, dass interne Geräte sicher ins Internet kommen. Sie schützt vor einigen Standardangriffen wie Port-Scans.

Das ist gut – aber sehr begrenzt. Router-Firewalls können nicht erkennen, welche Anwendungen kommunizieren, ob sich Malware versteckt oder ob verdächtige Muster im Datenverkehr auftreten. Diese Firewall ist dafür gebaut, Privatanutzer zu schützen – nicht Unternehmensdaten.

Eine **professionelle Firewall (vollwertiger Unternehmensschutz)** bietet vollwertigen Unternehmensschutz, indem sie den gesamten Datenverkehr überwacht und intelligent steuert. Sie filtert Anwendungen – etwa indem Microsoft 365 erlaubt und unbekannte Apps blockiert werden – und erkennt mit IDS/IPS Angriffsmuster in Echtzeit. Gleichzeitig stoppt sie Malware- und Botnet-Verbindungen automatisch und schützt per Webfilter vor gefährlichen Websites.

Sichere VPN-Zugänge ermöglichen den geschützten Zugriff von außen, während feingranulare Regeln festlegen, welcher PC wann wohin darf. Tägliche Updates gegen neue Bedrohungen halten das Sicherheitsniveau konstant hoch. Durch umfassende Protokollierung und Monitoring werden verdächtige Aktivitäten sichtbar und Angriffe überhaupt erst erkennbar.



Was Sie überprüfen sollten:



Ist eine professionelle Firewall im Einsatz?

Die Firewall im WLAN-Router reicht für Unternehmen meist nicht aus. Professionelle Firewalls bieten mehr Schutz und Kontrolle.



Wird die Firewall regelmäßig aktualisiert?

Auch Firewalls benötigen Updates, um neue Bedrohungen abwehren zu können.



Ist Ihr WLAN verschlüsselt?

Nutzen Sie WPA3 oder mindestens WPA2-Verschlüsselung. Ältere Standards wie WEP sind unsicher.



Gibt es ein separates Gäste-WLAN?

Gäste sollten nicht im gleichen Netzwerk sein wie Ihre Geschäftsdaten.



Ist die Firewall korrekt konfiguriert?

Eine falsch konfigurierte Firewall bietet oft nur Scheinsicherheit. Lassen Sie die Konfiguration regelmäßig überprüfen.



6. VIRENSCHUTZ UND MALWARE-ABWEHR

Warum ist das wichtig?

Schadsoftware (Malware) wie Viren, Trojaner und Ransomware können Ihre Systeme lahmlegen, Daten stehlen oder verschlüsseln. Ein moderner Virenschutz erkennt und blockiert die meisten Bedrohungen.



Was passiert, wenn Malware durchkommt?



Verschlüsselte Systeme (Ransomware)

Ihre Server und Daten werden unbenutzbar gemacht. Kriminelle verlangen ein Lösegeld für die Entschlüsselung – oft mit der Drohung, Daten zu veröffentlichen. Ohne funktionierendes Backup stehen Produktion und Geschäftsabläufe im schlimmsten Fall still.



Datendiebstahl (z. B. Kundendaten)

Personenbezogene Daten werden abgegriffen und verkauft oder zur Erpressung genutzt. Das ist ein Datenschutzvorfall mit Meldepflicht an die Aufsichtsbehörde und potenziellen Bußgeldern, Schadensersatzforderungen und Image-Schäden.



Betriebsunterbrechung

IT-gestützte Abläufe funktionieren nicht mehr – vom Warenwirtschaftssystem bis zur Produktion. Stillstand, Lieferverzug und Umsatzverluste sind die Folge.



Doppelte Erpressung

Immer häufiger drohen Angreifer nicht nur mit Verschlüsselung, sondern zusätzlich mit der Veröffentlichung zuvor gestohlener Daten („Double Extortion“). Selbst mit Backups bleibt man erpressbar.

Was Sie überprüfen sollten:



Ist auf allen Geräten ein Virenschutz installiert?

Jeder Computer, jedes Notebook und idealerweise auch Server und Smartphones sollten geschützt sein.



Wird der Virenschutz regelmäßig aktualisiert?

Neue Bedrohungen entstehen täglich – nur ein aktueller Virenschutz kann sie erkennen.



Laufen regelmäßige Scans?

Automatische tägliche oder wöchentliche Scans sollten Standard sein.



Werden erkannte Bedrohungen dokumentiert?

Sie sollten wissen, wenn etwas Verdächtiges erkannt wurde.



7. MITARBEITER-SENSIBILISIERUNG – DER MENSCHLICHE FAKTOR

Warum ist das wichtig?

Die beste Technik hilft nichts, wenn Mitarbeiter auf Phishing-E-Mails hereinfallen oder USB-Sticks unbekannter Herkunft anschließen. Der Mensch bleibt oft das schwächste Glied in der Sicherheitskette – aber auch das stärkste, wenn er richtig geschult ist.

Was bedeutet „Social Engineering“?

Social Engineering beschreibt Angriffe, bei denen nicht die Technik, sondern Menschen gezielt manipuliert werden. Cyberkriminelle nutzen typische Verhaltensmuster aus: Hilfsbereitschaft, Stress, Höflichkeit oder den Wunsch, schnell zu reagieren.

Typische Beispiele:

- Phishing-Mails, die vertraut wirken („Ihr Paket konnte nicht zugestellt werden...“)
- Gefälschte Chef-Anweisungen („Bitte dringend diese Zahlung freigeben...“)
- Anrufe, bei denen sich jemand als IT-Support oder Dienstleister ausgibt
- USB-Sticks, die absichtlich liegen gelassen werden („Fundstück“)

Das Ziel ist immer dasselbe: Zugangsdaten stehlen, Vertrauen ausnutzen oder jemanden zu einer Handlung bewegen, die der Angreifer sonst nicht durchführen könnte. Social Engineering ist deshalb so gefährlich, weil dabei keine technischen Hürden überwunden werden müssen. Gut geschulte und wachsame Mitarbeitende sind hier der wichtigste Schutzfaktor.



Was Sie überprüfen sollten:



Werden Mitarbeiter regelmäßig zu IT-Sicherheit geschult?

Mindestens einmal jährlich sollten alle Mitarbeiter ein Security-Awareness-Training absolvieren.



Können Ihre Mitarbeiter Phishing-E-Mails erkennen?

Typische Warnsignale: Dringlichkeit, verdächtige Absender, unerwartete Anhänge, Rechtschreibfehler.



Gibt es klare Regeln für den Umgang mit sensiblen Daten?

Alle sollten wissen: Was darf per E-Mail verschickt werden? Wie werden Daten sicher ausgetauscht?



Wissen die Mitarbeiter, an wen sie sich bei IT-Problemen wenden?

Es sollte eine klare Anlaufstelle geben.



Gibt es einen Prozess für das Melden von Sicherheitsvorfällen?

Mitarbeiter müssen wissen, dass sie Fehler melden können, ohne Angst vor Konsequenzen zu haben.



8. NOTFALLPLANUNG – VORBEREITET AUF DEN ERNSTFALL

Warum ist das wichtig?

Trotz aller Vorsichtsmaßnahmen kann es zu einem Sicherheitsvorfall kommen. Dann zählt jede Minute. Ein durchdachter Notfallplan hilft Ihnen, schnell und richtig zu reagieren und die Auswirkungen zu minimieren.

Warum ein Backup noch kein Notfallplan ist

Viele Unternehmen fühlen sich sicher, weil sie ein Backup haben. Aber ein Backup allein beantwortet nur eine Frage: „Haben wir unsere Daten irgendwo gesichert?“

Ein Notfallplan beantwortet eine ganz andere – viel entscheidendere – Frage: „Wie schnell können wir nach einem Angriff oder Ausfall wieder arbeitsfähig sein?“

Denn im Ernstfall müssen viele Dinge geklärt sein: Wie spielen wir die Daten zurück? Wer darf entscheiden, dass wir auf das Backup zurückgehen? Welche Systeme starten wir zuerst wieder? Wer informiert Kunden, Mitarbeitende und Dienstleister? Wie lange können wir ohne IT arbeiten, bevor es kritisch wird? Genau dafür gibt es einen Notfallplan: Er sorgt dafür, dass die Disaster-Recovery-Time – also die Zeit bis zur Wiederaufnahme des Geschäftsbetriebs – so kurz wie möglich bleibt.

Was Sie überprüfen sollten:



Gibt es einen IT-Notfallplan?

Ein dokumentiertes Vorgehen für verschiedene Szenarien (Ransomware, Serverausfall, Datenverlust) sollte existieren.



Sind Verantwortlichkeiten klar definiert?

Wer entscheidet was? Wer führt welche Maßnahmen aus?



Gibt es eine Notfall-Kontaktliste?

Wichtige Telefonnummern sollten auch ohne Zugriff auf das IT-System verfügbar sein (z.B. gedruckt).



Wurde der Notfallplan jemals getestet?

Ein ungetesteter Plan ist oft das Papier nicht wert, auf dem er steht.



Gibt es Kommunikationspläne?

Wie informieren Sie Kunden, Lieferanten und Mitarbeiter im Notfall?



Handlungsempfehlung:

Erstellen Sie einen Notfallplan und testen Sie ihn mindestens einmal jährlich in einer Übung.

9. VERSCHLÜSSELUNG – SCHÜTZEN SIE IHRE DATEN

Warum ist das wichtig?

Verschlüsselung macht Daten für Unbefugte unlesbar. Auch wenn jemand physischen Zugriff auf ein Gerät oder eine Festplatte erhält, kann er ohne den Entschlüsselungsschlüssel nichts mit den Daten anfangen.

Verschlüsselung ist Schutz...**aber auch genau das, was Angreifer gegen uns einsetzen (Ransomware)**

Verschlüsselung ist eines der wichtigsten Sicherheitswerkzeuge: Sie sorgt dafür, dass Daten selbst bei Verlust eines Geräts oder beim Abfangen im Internet unlesbar bleiben. Nur wer den richtigen Schlüssel besitzt, kann sie entschlüsseln und wieder nutzbar machen. Genau diese Stärke wird bei modernen Cyberangriffen allerdings auch gegen Unternehmen eingesetzt – vor allem durch Ransomware. Bei einem Ransomware-Angriff passiert im Kern Folgendes: Angreifer verschlüsseln Ihre eigenen Daten und Systeme so, dass Sie selbst keinen Zugriff mehr haben – und verlangen anschließend ein Lösegeld für den Entschlüsselungsschlüssel. Technisch gesehen machen Angreifer also dasselbe wie Sie bei BitLocker oder verschlüsselten Backups – nur mit dem Unterschied, dass Sie den Schlüssel nicht besitzen.

Was Sie überprüfen sollten:**Sind Notebooks und mobile Geräte verschlüsselt?**

Gerade Geräte, die außer Haus genutzt werden, sollten vollständig verschlüsselt sein (z.B. BitLocker für Windows).

**Werden sensible E-Mails verschlüsselt?**

Für besonders vertrauliche Informationen sollten Sie E-Mail-Verschlüsselung nutzen.

**Sind Backups verschlüsselt?**

Auch Ihre Sicherungskopien sollten vor unberechtigtem Zugriff geschützt sein.

**Wird eine sichere Verbindung (HTTPS) verwendet?**

Ihre Website und alle Online-Anwendungen sollten über HTTPS laufen.





10. ZUGRIFFSVERWALTUNG – WER DARF WAS?

Warum ist das wichtig?

Nicht jeder Mitarbeiter braucht Zugriff auf alle Daten und Systeme. Das Prinzip der minimalen Berechtigung (Need-to-Know) reduziert Risiken: Je weniger Zugriffsrechte unnötig vergeben sind, desto kleiner ist die Angriffsfläche.

Admin-Konten: praktisch – aber hochriskant

Viele Unternehmen nutzen Admin-Konten im Alltag, weil es bequem ist: Man kann alles installieren, alles ändern und muss sich keine Gedanken über Berechtigungen machen. Doch genau diese Bequemlichkeit ist ein großes Risiko.

Ein Admin-Konto hat vollständige Kontrolle über das System:

- Dateien löschen
- Programme installieren
- Sicherheitseinstellungen ändern
- Backups überschreiben
- Benutzer anlegen oder entfernen

Wenn ein solches Konto missbraucht wird – egal ob durch einen Fehler, Malware oder einen Angreifer – kann der gesamte Schaden ungebremsst durch das Unternehmen laufen.

Deshalb gilt in der IT-Sicherheit ein einfacher Grundsatz: „Mit Admin-Rechten arbeitet man nicht.“ Stattdessen nutzt man ein normales Benutzerkonto für die tägliche Arbeit und ein separates Admin-Konto nur dann, wenn es wirklich gebraucht wird.

So verhindern Sie, dass ein falscher Klick oder eine Phishing-Mail plötzlich Zugriff auf das ganze Unternehmen bekommt. Das Prinzip ist einfach – aber extrem wirksam, um Schaden zu begrenzen und Angreifern den Weg abzuschneiden.



Was Sie überprüfen sollten:



Haben alle Mitarbeiter nur die Berechtigungen, die sie wirklich benötigen?

Prüfen Sie regelmäßig, ob Zugriffsrechte noch aktuell sind.



Werden Berechtigungen bei Wechsel oder Ausscheiden entzogen?

Ehemalige Mitarbeiter sollten sofort alle Zugänge verlieren.



Gibt es administrative Konten für spezielle Aufgaben?

Normale Arbeit sollte nicht mit Admin-Rechten erfolgen.



Werden Zugriffe dokumentiert?

Bei kritischen Systemen sollten Sie nachvollziehen können, wer wann worauf zugegriffen hat.

ZUSAMMENFASSUNG: IHRE NÄCHSTEN SCHRITTE

Sie haben nun einen Überblick über die wichtigsten IT-Sicherheitsbereiche. Lassen Sie uns gemeinsam schauen, wie Sie vorgehen können:

1. Schritt: Bestandsaufnahme

Gehen Sie die Checklisten in diesem Dokument durch und notieren Sie, wo Unsicherheiten oder Lücken bestehen.

2. Schritt: Prioritäten setzen

Nicht alles muss sofort perfekt sein. Konzentrieren Sie sich zunächst auf:

- Funktionierende Backups
- Starke Passwörter und MFA
- Aktuelle Software
- Mitarbeiter-Sensibilisierung

3. Schritt: Expertenrat einholen

Für eine fundierte Einschätzung Ihrer individuellen Situation empfehlen wir ein persönliches Gespräch mit IT-Sicherheitsexperten. Jedes Unternehmen ist anders, und branchenspezifische Anforderungen (wie KRITIS, NIS2 oder DORA) können zusätzliche Maßnahmen erfordern.



4. Schritt: Maßnahmen umsetzen

Erstellen Sie einen realistischen Plan mit konkreten Terminen und Verantwortlichkeiten.

5. Schritt: Regelmäßig überprüfen

IT-Sicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. Planen Sie jährliche Reviews ein.

BRANCHENSPEZIFISCHE HINWEISE

Abhängig von Ihrer Branche können zusätzliche regulatorische Anforderungen gelten, z.B.:

Kritische Infrastrukturen (KRITIS): Betreiber kritischer Infrastrukturen unterliegen besonderen gesetzlichen Anforderungen nach dem IT-Sicherheitsgesetz.

NIS2-Richtlinie: Die europäische NIS2-Richtlinie erweitert die Anforderungen an die Cybersicherheit für viele Unternehmen – sprechen Sie uns an, ob Sie betroffen sind.

DORA (Digital Operational Resilience Act): Finanzunternehmen müssen ab 2025 strengere Vorgaben zur digitalen Betriebsstabilität erfüllen.

DSGVO: Unabhängig von der Branche müssen alle Unternehmen, die personenbezogene Daten verarbeiten, angemessene technische und organisatorische Maßnahmen zum Datenschutz treffen.

u.v.m.

IHR PARTNER FÜR IT-SICHERHEIT IM RAUM LÜNEBURG

Sie haben Fragen zu Ihrer IT-Sicherheit? Sie möchten wissen, wie Ihr Unternehmen konkret aufgestellt ist?

Kontaktieren Sie uns für eine unverbindliche Erstberatung.

Wir analysieren Ihre individuelle Situation, zeigen Ihnen konkrete Handlungsempfehlungen auf und begleiten Sie bei der Umsetzung – ohne Blabla, auf Augenhöhe.

LUENE.IT

Systempartner IT-Vertriebs GmbH & Co. KG
Moldenweg 3
21339 Lüneburg

Tel. 04131 20 76 110
E-Mail: info@luene.it
www.luene.it

Stand: November 2025

Dieses Dokument dient der allgemeinen Information und ersetzt keine individuelle IT-Sicherheitsberatung.

