IT-NUNWEILER
CYBER SECURITY & AI

FÜR GESCHÄFTSFÜHRER IM MITTELSTAND

Cyber *Report* 2027

INKLUSIVE 20 FRAGEN SCHNELLCHECK



53 %

mehr Angriffsversuche
auf Unternehmen in Deutschland

August 2026 gegenüber August 2025
Quelle: Check Point Research

Marcel Nunweiler

Cyber-Security-Experte
Founder & CEO der
IT-Nunweiler GmbH

Über 20 Jahre Erfahrung

Mit Notfallkarte für den Ernstfall

SEITE 17

„Wir sind im Cyberkrieg."

IHR MASSNAHMENPLAN 2027

Drei Schritte,

die Sie als Geschäftsführer jetzt umsetzen müssen.

VORWORT

„Bei uns ist doch nichts zu holen.“

Diesen Satz höre ich seit über 20 Jahren. Er war nie richtig. Seit 2026 ist er gefährlich.

Angreifer suchen ihre Ziele nicht mehr von Hand aus. Das erledigt Software, immer öfter mit künstlicher Intelligenz. Sie fragt nicht, wie groß Ihr Unternehmen ist. Sie prüft nur, ob irgendwo eine Lücke offen steht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Lage im November 2026 deshalb hochgestuft: von „angespannt“ auf „angespannt bis kritisch“.

Die meisten Unternehmer, mit denen ich spreche, haben einen IT-Dienstleister und gehen davon aus, dass damit alles geregelt ist. Oft stimmt das. Oft aber auch nicht, und den Unterschied sieht man von außen kaum.

Genau dafür ist dieser Report da. Er zeigt Ihnen das ganze Bild: wie sich die Lage verändert hat, was das für Ihre Verantwortung als Geschäftsführung bedeutet und woran Sie erkennen, ob Ihre IT wirklich geschützt ist. In klarer Sprache und mit belegten Zahlen.

Nehmen Sie sich eine halbe Stunde. Danach wissen Sie, wo Ihr Unternehmen steht und was 2027 zu tun ist.





Marcel Nunweiler

Cyber-Security-Experte · Founder & CEO

Über 20 Jahre Erfahrung

Die IT-Nunweiler GmbH hat über 2.600 Unternehmen betreut.

Warum ich von Cyberkrieg spreche

Von Marcel Nunweiler

Ein Konflikt kann im Postfach eines Zulieferers ankommen.

Im Mai 2025 warnten deutsche und internationale Sicherheitsbehörden vor einer Spionagekampagne des russischen Militärnachrichtendienstes GRU. Sie richtete sich gegen westliche Logistik- und Technologieunternehmen, darunter Firmen, die Hilfslieferungen an die Ukraine organisierten. Für einen Nachrichtendienst können schon ein Transportplan, Lieferzeiten oder die Namen von Partnern wertvoll sein.

Spionage und Erpressung treffen Betriebe auf unterschiedliche Weise.

Mit „Cyberkrieg" beschreibe ich auf dem Titel, wie Staaten ihre Konflikte auch über digitale Netze austragen. Das BSI dokumentiert Cyberspionage und Cybersabotage. Daneben gibt es Täter, die Unternehmen erpressen, um Geld zu verdienen. Ein verschlüsselter Server allein verrät Ihnen nicht, wer dahintersteckt. Die Praxisfälle in diesem Heft belegen wirtschaftliche Schäden. Wer die Angriffe verübt hat, ist damit offen.

Was das für Ihren Betrieb bedeutet.

Denken Sie an einen Maschinenbauer, dessen Kunde ein Rüstungszulieferer ist. Eine ausgespähte Mail kann technische Zeichnungen oder Liefertermine offenlegen. Fällt sein externer IT-Partner aus, kann sich der Schaden auf mehrere Betriebe verteilen. Ihre Rolle in der Lieferkette zählt ebenso wie die Größe Ihres Unternehmens.

Mein Rat: Legen Sie fest, welche Daten und Abläufe Ihre Kunden Ihnen anvertrauen. Vereinbaren Sie dann mit Ihrer IT, wer diese schützt, wer bei Alarm entscheidet und welcher Auftrag zuerst wieder laufen muss.

Quellen: BSI, Lagebericht 2026, Kapitel Cyberconflict und Cyberspionage; Gemeinsame Behördenwarnung zur GRU-Kampagne, 21. Mai 2025.

INHALT

Ihr Weg durch den Report

DIE LAGE

Warum ich von Cyberkrieg spreche 3
Die Lage in vier Zahlen 5
Was sich 2026 verändert hat 6
Das 8-Tage-Problem 7
Echte Cyberfälle 8
Ihre Verantwortung als Geschäftsführung 10

DER SCHUTZ

Schnell patchen: welcher Zeitraum? 11
EDR, XDR, MDR 12
Backup, das zurückkommt 13
Microsoft 365 und Google Workspace 14
Domainsicherheit 15

DIE UMSETZUNG

Die ersten 60 Minuten nach einem Angriff 16
Die Notfallkarte 17
Worauf es beim IT-Dienstleister ankommt 18
Der 20-Fragen-Schnellcheck 19–20
Ihre Auswertung 21
Drei Schritte. Drei klare Aufträge. 22
Ihr Maßnahmenplan für 2027 23
Das Protokoll für Ihren ersten Probelauf 24
Ihr nächster Schritt 25
Quellen und Impressum 26–27

Lesen

Jedes Thema steht auf einer Seite. Sie können vorne beginnen oder direkt zu dem Thema springen, das Sie beschäftigt.

Ankreuzen

Der Schnellcheck auf Seite 19 zeigt in zehn Minuten, wo Ihr Unternehmen steht.

Aufhängen

Die Notfallkarte auf Seite 17 drucken Sie aus und füllen sie von Hand aus.

Vier Zahlen, die Sie kennen sollten

Diese vier Zahlen zeigen, wie stark sich die Lage von 2025 auf 2026 verschärft hat. Hier steht, was sie bedeuten, woher sie stammen und was sie nicht aussagen.

+53 %

mehr Cyberangriffe auf Unternehmen in Deutschland

Im August 2026 zählte Check Point Research im Schnitt 1.834 Angriffe pro Woche auf jedes Unternehmen in Deutschland. Das sind 53 % mehr als im August 2025 und der stärkste Anstieg im deutschsprachigen Raum.

Wichtig: Gezählt werden Angriffsversuche, die von Sicherheitssystemen erkannt wurden. Es sind keine erfolgreichen Einbrüche.

Quelle: Check Point Research, Monthly Cyber Threat Report August 2026

8 Tage

bis Angreifer eine neue Sicherheitslücke ausnutzen

So lange dauerte es im 2. Quartal 2026 im Schnitt vom Bekanntwerden einer Sicherheitslücke bis zum ersten bekannten Angriff. Im Berichtszeitraum davor waren es im Schnitt 53 Tage.

Wichtig: Das ist ein Durchschnitt. Manche Lücken werden nach Stunden angegriffen, viele nie. Mehr dazu auf Seite 7.

Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2026

≈ 310

neue Sicherheitslücken pro Tag

Bis zum 13. November 2026 wurden weltweit 100.222 Sicherheitslücken veröffentlicht. Das sind im Schnitt mehr als 310 pro Tag und schon jetzt mehr als doppelt so viele wie im gesamten Vorjahr.

Wichtig: Das BSI nennt für seinen Berichtszeitraum bis Juni 2026 im Schnitt 160 pro Tag (plus 35 %). Die Zeiträume sind verschieden, die Richtung ist dieselbe.

Quelle: VulnCheck, zitiert nach The Register vom 13.11.2026

Alle 2-4 Wochen

Wiederherstellungstest für eine verlässliche Datensicherung

Unsere Empfehlung für geschäftskritische Systeme: Die Datensicherung wird alle zwei bis vier Wochen vollständig zurückgespielt und das Ergebnis festgehalten. Nur so wissen Sie, dass Ihr Backup im Ernstfall funktioniert.

Wichtig: Das ist ein Richtwert aus der Praxis und keine gesetzliche Frist. Mehr dazu auf Seite 13.

Quelle: Empfehlung der IT-Nunweiler GmbH

> **Mehr Lücken, schnellere Angriffe, kleinere Ziele. In dieser Lage treffen Sie 2027 Ihre Entscheidungen.**

DIE LAGE 2026

Was sich 2026 verändert hat

Am 19. November 2026 hat das BSI seinen Lagebericht vorgestellt. Die Behörde stuft die Lage jetzt als „angespannt bis kritisch“ ein. Drei Entwicklungen stehen dahinter.

Die Suche nach Lücken läuft automatisch

Früher musste ein Mensch jede Schwachstelle von Hand finden und den Angriff selbst bauen. Heute übernimmt künstliche Intelligenz einen wachsenden Teil dieser Arbeit, und zwar auf beiden Seiten: Hersteller finden mehr Lücken, Angreifer nutzen sie schneller aus.

Das BSI sieht in selbstständig arbeitenden KI-Programmen den wichtigsten Treiber. An den Sensoren der Behörde nahmen automatische Suchläufe nach Schwachstellen um 57 % zu, Angriffsversuche auf gefundene Lücken um 48 %.

160

neue Schwachstellen pro Tag im Berichtszeitraum des BSI. Das sind 35 % mehr als im Jahr davor.

Es trifft die Kleinen

Angegriffen wird, wer ein leichtes Ziel ist. Von den angezeigten Fällen mit Erpressungssoftware (Ransomware) betrafen zuletzt 90 % kleine und mittlere Unternehmen. Ein Jahr zuvor waren es 80 %.

Dazu passt eine zweite Zahl des BSI: Nur etwa die Hälfte der kleinen und mittleren Unternehmen, die ihren Stand prüfen ließen, erfüllt die Mindestanforderungen an IT-Sicherheit.

90 %

der angezeigten Ransomware-Fälle treffen kleine und mittlere Unternehmen.

Der Schaden entsteht durch Stillstand

Nach einer Umfrage des Versicherers Hiscox standen betroffene kleine und mittlere Unternehmen in Deutschland nach einem Cyberangriff im Schnitt 41,7 Stunden still. Im internationalen Vergleich waren es 31,6 Stunden.

Der Digitalverband Bitkom beziffert den Schaden der deutschen Wirtschaft durch Diebstahl, Spionage und Sabotage für 2025 auf rund 289 Milliarden Euro. Etwa 70 % davon gehen auf Cyberangriffe zurück.

41,7 Std.

Stillstand im Schnitt nach einem Cyberangriff auf ein deutsches KMU.

DIE GUTE NACHRICHT

Die meisten Angriffe sind nicht raffiniert, sondern schnell und automatisch. Wer die Grundlagen im Griff hat, ist für diese Angriffe kein leichtes Ziel mehr: schnelle Updates, ein Schutz, der Angriffe erkennt, und ein Backup, das nachweislich zurückkommt. Um genau diese drei Grundlagen geht es ab Seite 11.

DAS TEMPO

Angreifer brauchen 8 Tage. Wie lange braucht Ihre IT?

Sobald ein Hersteller eine Lücke schließt, ist öffentlich bekannt, wo sie war. Ab diesem Moment läuft die Uhr.

ZEIT VOM BEKANNTWERDEN EINER LÜCKE BIS ZUM ERSTEN BEKANNTEN ANGRIFF, IM DURCHSCHNITT



Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2026, vorgestellt am 19.11.2026. Die 8 Tage sind ein Durchschnitt und keine sichere Frist.

Warum der Monatslauf nicht mehr reicht

Viele Unternehmen spielen Updates einmal im Monat ein. Das war lange ein vernünftiger Rhythmus. Heute bedeutet er: Eine gefährliche Lücke kann bis zu 30 Tage offen stehen, während Angreifer im Schnitt 8 Tage brauchen.

Wo ein fertiger Angriffscode öffentlich wird, geht es noch schneller. Der Sicherheitsanbieter CrowdStrike hat das erste Halbjahr 2026 ausgewertet: 88 % dieser Angriffe begannen innerhalb von 48 Stunden nach Veröffentlichung des Codes.

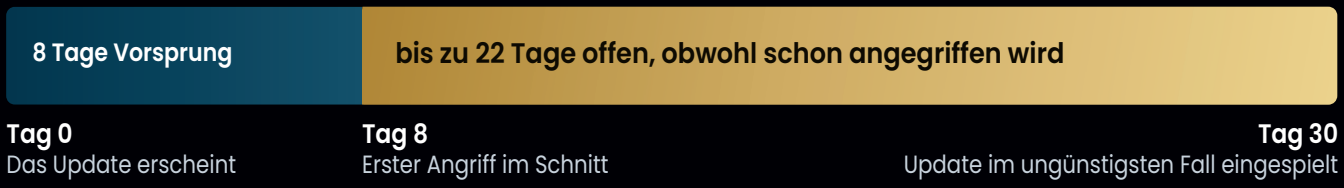
Sie müssen nicht alles sofort patchen

Von den über 100.000 Lücken des Jahres 2026 stehen bisher 1.363 im Verzeichnis nachweislich ausgenutzter Lücken des Anbieters VulnCheck. Das sind rund 1,4 %. Es kommt also darauf an, die gefährlichen Lücken zuerst zu erkennen:

- Wird die Lücke bereits angegriffen?
- Ist das betroffene System aus dem Internet erreichbar?
- Lässt sich der Angriff automatisieren?

Nach diesen Kriterien sortiert seit Juni 2026 auch die US-Behörde für Cybersicherheit (CISA).

RECHENBEISPIEL: DAS OFFENE FENSTER BEIM MONATLICHEN UPDATE



Tag 0
Das Update erscheint

Tag 8
Erster Angriff im Schnitt

Tag 30
Update im ungünstigsten Fall eingespielt

> **Die Frage lautet nicht mehr: Sind alle Updates installiert? Sie lautet: Wie schnell ist die gefährlichste Lücke zu?**

AUS DER PRAXIS

Echte Cyberfälle

„Die Produktion steht fast sechs Wochen still.“

Drei Fälle aus Deutschland. Keiner davon ist ein Konzern, alle sind öffentlich belegt. Wir erzählen sie nicht, um mit dem Finger zu zeigen. Jeder dieser Fälle hätte auch ein anderes Unternehmen treffen können.

2026

ZEGO Textil-veredelungszentrum

Aschaffenburg
Textilveredelung
rund 60 Beschäftigte
37 Jahre am Markt

Am 29. März 2026, einem Sonntag, trifft ein Cyberangriff das Unternehmen. Die Produktion steht fast sechs Wochen still. Im Juli 2026 teilt das Unternehmen mit, dass es Insolvenz angemeldet hat. In der Mitteilung an Kunden und Lieferanten heißt es sinngemäß: Die Folgen des Angriffs ließen sich trotz aller Anstrengungen nicht mehr ausgleichen. Der Betrieb soll im Verfahren weiterlaufen.

Welche Art von Angriff es war und wie die Täter hineinkamen, hat das Unternehmen nicht veröffentlicht.

WAS UNTERNEHMER DARAUS LERNEN KÖNNEN

Gefährlich ist nicht nur das Lösegeld, gefährlich ist der Stillstand. Die entscheidende Frage lautet deshalb nicht „Haben wir ein Backup?“, sondern „Nach wie vielen Tagen arbeiten wir wieder?“

Mehr dazu: Seite 13, Backup und Wiederanlauf

Quellen: Mitteilung des Unternehmens vom Juli 2026; The Register vom 13.07.2026

2026

Autohaus Pichel

Chemnitz
Autohandel und Werkstatt
35 Beschäftigte am Standort
Familienunternehmen seit 2000

Im Dezember 2025 greifen Unbekannte gezielt die IT des Ford-Autohauses an. Die gesamte elektronische Datenverarbeitung ist rund zwei Monate weitgehend lahmgelegt, ein regulärer Geschäftsbetrieb kaum möglich. Anfang März 2026 stellt das Unternehmen Insolvenzantrag.

Das Autohaus war schon vorher angeschlagen: Der Abschluss für 2024 weist rund 530.000 Euro Verlust aus. Der vorläufige Insolvenzverwalter nennt den Angriff trotzdem als wesentlichen Auslöser. Werkstatt und Service laufen im Verfahren weiter.

WAS UNTERNEHMER DARAUS LERNEN KÖNNEN

Wer wenig finanziellen Puffer hat, übersteht wochenlangen Stillstand nicht. Gerade in schwierigen Zeiten ist IT-Sicherheit keine Ausgabe, die man verschieben kann.

Mehr dazu: Seite 10, Ihre Verantwortung, und Seite 13, Backup

Quellen: it-daily.net vom 06.03.2026 unter Berufung auf die Sächsische Zeitung

AUS DER PRAXIS

2026

Metzgerei in der Oberpfalz

Landkreis Neustadt an der Waldnaab
Fleischerhandwerk
Name nicht veröffentlicht

In der Nacht zum Montag, 2. November 2026, verschaffen sich Unbekannte Zugriff auf die Fernsteuerung der Kühlanlagen. Sie stellen mehrere Kühlhäuser auf bis zu 150 Grad. Der Schaden liegt laut Polizei im fünfstelligen Eurobereich, die Kripo ermittelt.

Der Fall steht nicht allein: Seit Oktober 2026 melden mehrere EU-Staaten Angriffe auf gewerbliche Kühlanlagen. In Niederbayern heizte sich das Kühlregal eines Supermarkts auf bis zu 50 Grad auf.

WAS UNTERNEHMER DARAUS LERNEN KÖNNEN

Angreifer brauchen keinen Server. Jedes Gerät, das sich aus der Ferne steuern lässt, ist ein Zugang: Kühlung, Heizung, Kameras, Maschinen. Auch diese Geräte brauchen Updates, sichere Zugänge und jemanden, der sie überwacht.

Mehr dazu: Seite 11, schnell patchen, und Seite 18, IT-Dienstleister

Quellen: dpa, u. a. Abendzeitung München und nordbayern.de vom 04.11.2026; ms-aktuell.de vom 05.11.2026

Was die drei Fälle gemeinsam haben

Es waren keine Konzerne

Ein Textilbetrieb mit 60 Beschäftigten, ein Autohaus mit 35, eine Metzgerei. Größe schützt nicht, und Kleinsein auch nicht.

Zwei der drei Angriffe kamen am Wochenende

Angreifer schlagen zu, wenn niemand hinsieht. Wer sieht bei Ihnen am Sonntag um 3 Uhr einen Alarm, und wer darf dann handeln?

Der größte Schaden entstand nach dem Angriff

Wochen und Monate Stillstand, verlorene Ware, verlorene Aufträge. Zwei der drei Betriebe mussten Insolvenz anmelden.

Was das Risiko senkt, ist bekannt

Schnelle Updates, sichere Zugänge von außen, Überwachung rund um die Uhr und ein Backup, das nachweislich zurückkommt. Nichts davon ist Geheimwissen.

40+

deutsche Unternehmen allein im Oktober 2026

So viele deutsche Opfer listet Security-Insider allein für Oktober 2026, darunter Bauunternehmen, eine Anwaltskanzlei, ein Seniorenwohnheim und eine Brauerei. Die drei Fälle oben sind keine Ausnahme. Es sind nur die, über die öffentlich berichtet wurde.

IHRE VERANTWORTUNG

IT-Sicherheit lässt sich beauftragen. Die Verantwortung nicht.

Sie müssen keine Firewall einrichten können. Sie müssen aber wissen, ob es jemand tut, und es sich belegen lassen.

Das Gesetz nennt die Geschäftsleitung beim Namen

Seit dem 6. Dezember 2025 gilt das neue BSI-Gesetz, mit dem Deutschland die EU-Richtlinie NIS-2 umsetzt. Für rund 29.500 Einrichtungen ist Cybersicherheit damit ausdrücklich Chefsache: Die Geschäftsleitung muss die Schutzmaßnahmen umsetzen, ihre Umsetzung überwachen und sich selbst schulen lassen (§ 38 BSIG). Bei Pflichtverletzungen kann sie gegenüber dem eigenen Unternehmen haften.

Auch wenn Ihr Unternehmen nicht direkt darunter fällt: Kunden, die betroffen sind, müssen ihre Lieferkette absichern und reichen die Fragen an Sie weiter.

Die Uhr läuft ab dem ersten Verdacht

Sind personenbezogene Daten betroffen, muss der Vorfall in der Regel innerhalb von 72 Stunden der Datenschutzaufsicht gemeldet werden (Art. 33 DSGVO). Für Einrichtungen nach dem BSI-Gesetz kommt bei erheblichen Vorfällen eine erste Meldung an das BSI innerhalb von 24 Stunden hinzu (§ 32 BSIG).

Wer in diesem Moment erst klärt, wer zuständig ist, verliert die Frist. Deshalb gehört die Notfallkarte von Seite 17 an die Wand.

Die Versicherung fragt vorher und nachher

Cyberversicherer verlangen vor Vertragsabschluss in der Regel Auskunft über Mehr-Faktor-Anmeldung, Datensicherung und Update-Stand. Im Schadenfall wird geprüft, ob die Angaben stimmten und die vereinbarten Pflichten eingehalten wurden.

Ein Nachweis, den Sie jeden Monat bekommen, ist dann viel wert.

Stillstand kostet ab der ersten Stunde

Gehälter, Miete und Leasing laufen weiter, der Umsatz nicht. Rechnen Sie es für Ihr Unternehmen einmal durch:

Umsatz pro Arbeitstag _____ Euro

mal Tage Stillstand _____

ergibt _____ Euro

DREI FRAGEN, DIE SIE ALS GESCHÄFTSFÜHRUNG BEANTWORTEN KÖNNEN SOLLTEN

- Wer ist bei uns für IT-Sicherheit verantwortlich, mit Namen?
- Wann habe ich zuletzt einen Bericht über Update-Stand und Backup-Test gesehen?
- Wie lange dauert es, bis wir nach einem Totalausfall wieder arbeiten?

Diese Seite dient der Orientierung und ersetzt keine Rechtsberatung. Ob Ihr Unternehmen unter das BSI-Gesetz fällt, klären Sie bitte mit Ihrem Rechtsberater.

SCHUTZ 1 · UPDATES

Schnell patchen: welcher Zeitraum?

Ein Patch ist ein Update, das eine Sicherheitslücke schließt. Welcher Zeitraum richtig ist, hängt von der Lücke ab. Wir empfehlen drei Stufen.

48 Stunden
SOFORT

Wann: Die Lücke wird bereits angegriffen und das System ist aus dem Internet erreichbar. Das betrifft vor allem Firewall, VPN, Mailserver, Fernzugriff und Website.

Was: Schließen oder absichern, auch außerhalb der Wartungszeit. Gibt es noch kein Update, wird der Zugang gesperrt oder der Dienst abgeschaltet.

7 Tage
DIESE WOCHE

Wann: Kritische Sicherheitsupdates für alle übrigen Systeme, also Server, Arbeitsplätze und Programme.

Was: Einspielen im nächsten Wartungsfenster, einschließlich Neustart.

30 Tage
MONATSLAUF

Wann: Sicherheitsupdates, zu denen keine Angriffe bekannt sind.

Was: Automatisch und überwacht. Niemand muss eingreifen, aber jemand prüft das Ergebnis.

Die Fristen sind Richtwerte aus der Praxis und keine gesetzlichen Vorgaben. Verbindlich ist, was Sie mit Ihrem IT-Dienstleister schriftlich vereinbaren.

Was alles aktuell sein muss

Betriebssysteme	Windows, macOS, Server
Programme	Browser, Office, PDF, Branchensoftware
Geräte am Netzrand	Firewall, Router, VPN, WLAN
Geräte im Netz	Netzwerkspeicher, Drucker, Telefonanlage, Kameras, Anlagen mit Fernzugriff
Website	Redaktionssystem, Shop, Erweiterungen

Automatische Update-Routinen decken oft nur die ersten beiden Zeilen ab.

Woran es in der Praxis scheitert

- **Der Neustart fehlt.** Ein Update, das auf den Neustart wartet, schützt nicht.
- **Niemand kennt alle Geräte.** Was auf keiner Liste steht, wird auch nicht aktualisiert.
- **Alte Systeme.** Wofür der Hersteller keine Updates mehr liefert, lässt sich nicht patchen. Solche Systeme werden ersetzt oder vom Netz abgeschottet.

DAS KÖNNEN SIE VERLANGEN: EINEN MONATSBERICHT MIT DREI ZAHLEN

Anteil der Geräte, auf denen alle Sicherheitsupdates installiert sind	Offene kritische Lücken und seit wann sie offen sind	Geräte, die auf einen Neustart warten

EDR, XDR, MDR: Was hinter den Kürzeln steckt

Kein Schutz hält jeden Angriff auf. Entscheidend ist deshalb, wie schnell ein Angriff bemerkt und gestoppt wird. Dafür gibt es vier Stufen, die aufeinander aufbauen.

Klassischer Virenschutz	Erkennt bekannte Schadsoftware an ihren Mustern. Gegen neue Angriffe und gegen Täter, die sich mit gestohlenen Zugangsdaten anmelden, hilft das wenig.	**Reicht allein nicht mehr aus.**
EDR	**Endpoint Detection and Response** Beobachtet das Verhalten auf jedem PC und Server. Fällt etwas auf, etwa ein Programm, das massenhaft Dateien verschlüsselt, wird der Vorgang gestoppt und das Gerät vom Netz getrennt.	**Heute der Mindeststandard.**
XDR	**Extended Detection and Response** Verknüpft die Signale aus Geräten, E-Mail, Benutzerkonten und Netzwerk. So wird ein Angriff sichtbar, der an jeder einzelnen Stelle harmlos aussieht.	**Wichtig, sobald Sie Cloud-Dienste nutzen.**
MDR	**Managed Detection and Response** Ein Sicherheitsteam überwacht die Meldungen rund um die Uhr und greift ein. Die Technik meldet, Menschen entscheiden und handeln.	**Der Unterschied zwischen Alarm und Hilfe.**

Woran Sie guten Schutz erkennen

- Der Schutz läuft auf allen Geräten, auch auf Servern und auf Notebooks im Homeoffice.
- Alarme gehen an Menschen und nicht nur in ein Postfach.
- Ein befallenes Gerät lässt sich aus der Ferne sofort vom Netz trennen.
- Es ist schriftlich geregelt, wer nachts was entscheiden darf.
- Sie bekommen einen Bericht über erkannte und gestoppte Vorfälle.

> **Zwei der drei Angriffe aus diesem Report kamen am Wochenende.**

Die Frage an Ihre IT lautet deshalb: Wer sieht den Alarm am Sonntag um 3 Uhr, und wer darf dann handeln?

Hersteller verwenden die Kürzel unterschiedlich. Lassen Sie sich deshalb den Ablauf erklären: Was passiert, wenn nachts ein Alarm kommt?

SCHUTZ 3 · DATENSICHERUNG

Ein Backup zu haben reicht nicht. Es muss zurückkommen.

Angreifer wissen, dass ein gutes Backup ihr Geschäft zerstört. Deshalb suchen sie häufig zuerst die Sicherung und löschen oder verschlüsseln sie mit. Drei Fragen entscheiden, ob Ihr Backup den Ernstfall übersteht.

FRAGE 1

Vorhanden?

Werden alle wichtigen Daten täglich gesichert? Dazu gehören Server, Arbeitsplätze und Cloud-Dienste.

FRAGE 2

Geschützt?

Liegt eine Kopie außer Haus, und ist sie unveränderbar (englisch: immutable)? Unveränderbar heißt: Für eine festgelegte Zeit kann niemand diese Sicherung löschen oder überschreiben. Auch kein Administrator und kein Angreifer mit Administratorrechten.

FRAGE 3

Getestet?

Wurde die Sicherung vollständig zurückgespielt und das Ergebnis festgehalten? Unsere Empfehlung für geschäftskritische Systeme: alle zwei bis vier Wochen.

DIE 3-2-1-1-0-REGEL ALS MERKHILFE

3	2	1	1	0
Kopien Ihrer Daten	verschiedene Speicher	Kopie außer Haus	Kopie unveränderbar	Fehler beim Wiederherstellungstest

WAS GESICHERT WERDEN MUSS

Arbeitsplätze	Dokumente, die lokal auf PC oder Notebook liegen. Besser noch: Daten liegen gar nicht lokal, sondern zentral, und werden dort gesichert.
Server	Das komplette System und nicht nur einzelne Dateien. Täglich, mit einer Kopie im Rechenzentrum und einem regelmäßigen Wiederherstellungstest.
Cloud-Dienste	Postfächer, Dateien und Teams in Microsoft 365 oder Google Workspace. Warum das nötig ist, steht auf Seite 14.

Der Nachweis für Ihre Server

Lassen Sie die vollständigen virtuellen Maschinen aus einem geprüften Sicherungsstand wiederherstellen. Ihre IT prüft die Datenbank auf Konsistenz. Das Fachteam gleicht bekannte Auftragsdaten mit einem verlässlichen Beleg ab.

> „Wann haben Sie unser Backup zuletzt komplett wiederhergestellt?“

Wer auf diese Frage kein Datum nennen kann, hat eine Hoffnung und kein Backup. Lassen Sie sich außerdem zwei Zahlen nennen: Wie viele Stunden Arbeit gehen im schlimmsten Fall verloren? Und nach wie vielen Stunden oder Tagen arbeiten Sie wieder?

Die Cloud sichert sich nicht von selbst



Microsoft und Google betreiben die Rechenzentren und schützen ihre Plattformen. Für Ihre Daten, Zugänge, Freigaben und Aufbewahrungsfristen bleiben Sie verantwortlich.

Microsoft 365
Exchange Online, OneDrive, SharePoint und Teams

Google Workspace
Gmail, Google Drive, geteilte Ablagen und Kalender

Was Sie bei beiden Diensten prüfen sollten

Konten und Freigaben

Mehr-Faktor-Anmeldung für alle Konten, auch für die Geschäftsführung. Getrennte Administrator-Konten für die Verwaltung nutzen. Alte Anmeldeverfahren ohne zweiten Faktor abschalten. Auffällige Anmeldungen, Weiterleitungen und externe Freigaben regelmäßig prüfen.

E-Mail-Schutz und gesetzliche Archivierung

Links und Anhänge prüfen. Legen Sie fest, wer auf Phishing-Meldungen reagiert. Archivieren Sie aufbewahrungspflichtige E-Mails und Belege für die jeweilige Frist. Änderungen müssen nachvollziehbar bleiben.

Backup und Wiederherstellung

Gelöschte Daten bleiben im Papierkorb nur begrenzte Zeit verfügbar. Werden Dateien verschlüsselt, synchronisiert die Cloud auch die verschlüsselten Fassungen. Halten Sie eine getrennte, unveränderbare Sicherung vor, die Sie unabhängig zurückspielen können.

DER TEST / DATENSTAND VOR DREI MONATEN

Lassen Sie Ihre IT eine Wiederherstellung vorführen.

Microsoft 365
Ein Postfach, einen Ordner und ein Team wiederherstellen.

Google Workspace
Ein Gmail-Postfach und einen Ordner aus einer geteilten Ablage zurückholen.

Welche Fristen und Funktionen gelten, hängt von Ihrem Tarif und Ihren Einstellungen ab. Lassen Sie sich den Stand für Ihr Unternehmen zeigen.

Domainsicherheit

Wer nutzt den Namen Ihrer Firma?

Ihr Kunde erhält eine Rechnung mit Ihrem Firmennamen und einer fremden Bankverbindung. Gleichzeitig meldet ein Lieferant, dass seine E-Mail an Sie zurückkommt. Ihre IT muss beide Hinweise einordnen können.

BEISPIEL / SICHTBARER ABSENDER

rechnung@ihre-firma.example

01 Zugriff auf Ihre Domain sichern

Schützen Sie das Konto beim Domainanbieter mit Mehr-Faktor-Anmeldung. Halten Sie fest, wer Änderungen freigibt, wer vertritt und wie die Domain rechtzeitig verlängert wird.

02 Berechtigte Versender erkennen

Erfassen Sie Buchhaltung, Newsletter und weitere Versanddienste. SPF und DKIM helfen beim Prüfen der Herkunft. Werten Sie DMARC-Berichte aus. Sobald alle legitimen Versender korrekt erkannt werden, können Sie die Ablehnung gefälschter Absender vorgeben.

03 Vertrauliche Post auf dem Transportweg schützen

Mit MTA-STS können Sie unterstützende Mailserver verpflichten, eingehende E-Mails verschlüsselt an die vorgesehenen Server zuzustellen. TLS-Berichte zeigen gemeldete Zustellprobleme, etwa ein ungültiges Zertifikat.

04 Änderungen früh erkennen und darauf reagieren

Überwachen Sie die DNS-Einträge für Ihren E-Mail-Verkehr. Bei einer Änderung muss die zuständige Person erfahren, was sich geändert hat. Lassen Sie unbekannte Versender und gemeldete Verschlüsselungsfehler prüfen.

Prüfpunkt für Ihre IT

DNSSEC macht manipulierte DNS-Antworten erkennbar. Bei unterstützter Mailinfrastruktur kann DANE über signierte DNS-Einträge festlegen, welches Zertifikat Ihr Mailserver verwenden darf.

Ihr Nachweis als Geschäftsführer

Wer erhält den Alarm? Lassen Sie sich die letzte Änderung zeigen und erklären, wer sie geprüft hat.

Die ersten 60 Minuten

Minute 0 bis 5

Nicht ausschalten

Betroffene Geräte nicht ausschalten und nicht neu starten. Sonst gehen Spuren verloren, die für die Aufklärung wichtig sind. Nicht weiterarbeiten, nichts anklicken.

Minute 5 bis 15

Netzwerk trennen

Netzwerkkabel ziehen, WLAN aus. So breitet sich der Angriff nicht weiter aus. Im Zweifel die Internetverbindung des ganzen Betriebs trennen. Auch das Backup vom Netz nehmen.

Minute 15 bis 30

Anrufen

IT-Dienstleister oder interne IT, Geschäftsführung, Cyberversicherung, falls vorhanden. Per Telefon und nicht über das betroffene E-Mail-System. Danach: Datenschutzbeauftragter und Polizei.

Minute 30 bis 60

Aufschreiben

Was ist wann passiert, wer hat es bemerkt? Welche Geräte, welche Meldungen? Bildschirme mit dem Handy fotografieren. Wer wurde wann informiert?

Das lassen Sie bleiben: Geräte ausschalten oder neu aufsetzen. Dateien löschen oder selbst aufräumen. Mit Erpressern verhandeln oder zahlen, ohne sich beraten zu lassen. Den Vorfall verschweigen. Sind personenbezogene Daten betroffen, gilt in der Regel eine Meldefrist von 72 Stunden an die Datenschutzaufsicht (Art. 33 DSGVO).

ZUM AUSDRUCKEN

Die Notfallkarte

Diese Seite ausdrucken, die Nummern von Hand eintragen und neben das Telefon hängen. Im Ernstfall kommen Sie möglicherweise nicht mehr an Ihre Dateien.

Die ersten 60 Minuten nach einem Angriff

Minute 0 bis 5	**Nicht ausschalten**
Minute 5 bis 15	**Netzwerk trennen**
Minute 15 bis 30	**Anrufen**
Minute 30 bis 60	**Aufschreiben**

Unsere Notfallnummern

IT-Dienstleister

Geschäftsführung · mobil

Cyberversicherung · Schaden-Hotline

Versicherungsnummer

Datenschutzbeauftragter

Polizei · Zentrale Ansprechstelle Cybercrime

Bank · Konten sperren

Telefon- und Internetanbieter

Ausgefüllt am: _____

Ein Exemplar gehört auf Papier ins Büro, eines nach Hause zur Geschäftsführung.
IT-Nunweiler GmbH, Stand November 2026.

Worauf es beim IT-Dienstleister ankommt

Ob Updates installiert werden, sagt wenig. Es zählt, wie schnell gefährliche Lücken geschlossen werden und ob Sie das nachprüfen können. Diese acht Fragen dürfen Sie jedem Dienstleister stellen. Auch uns.

1 Wie schnell schließen Sie kritische Lücken?

Gute Antwort: Feste Fristen je Dringlichkeit, schriftlich vereinbart. Siehe Seite 11.

2 Was genau halten Sie aktuell?

Gute Antwort: Nicht nur Windows, sondern auch Programme, Firewall, Server und Netzwerkgeräte. Mit einer Geräteliste.

3 Wer überwacht unsere Systeme nachts und am Wochenende?

Gute Antwort: Ein Sicherheitsteam rund um die Uhr, das befallene Geräte sofort isolieren darf.

4 Wann haben Sie unser Backup zuletzt vollständig zurückgespielt?

Gute Antwort: Ein Datum aus den letzten vier Wochen und ein Protokoll dazu.

5 Ist eine Kopie unserer Sicherung unveränderbar und außer Haus?

Gute Antwort: Ja, getrennt von Ihrem Netz und vor Löschung geschützt.

6 Sind unsere Cloud-Dienste gesichert und abgesichert?

Gute Antwort: Eigenes Backup für Microsoft 365 oder Google Workspace und Mehr-Faktor-Anmeldung für alle Konten.

7 Wie schützen Sie Ihre eigenen Zugänge zu unseren Systemen?

Gute Antwort: Mehr-Faktor-Anmeldung, persönliche Konten, Protokollierung jedes Zugriffs.

8 Was bekommen wir schwarz auf weiß?

Gute Antwort: Einen Monatsbericht zu Update-Stand, Backup-Tests und Vorfällen. Dazu einen Notfallplan mit Namen und Nummern.

BEI DIESEN SÄTZEN SOLLTEN SIE NACHFRAGEN

- „Bei uns ist noch nie etwas passiert."
- „Das Backup läuft jede Nacht durch." Durchlaufen heißt nicht, dass es sich zurückspielen lässt.
- „Die Updates laufen automatisch."
- „Einen Bericht brauchen Sie nicht. Wir melden uns, wenn etwas ist."

> **Gute Dienstleister freuen sich über diese Fragen. Sie zeigen, dass ihre Arbeit gesehen wird.**

Der 20-Fragen-Schnellcheck

Kreuzen Sie ehrlich an. Bei „Weiß ich nicht“ kreuzen Sie Nein an, denn auch das ist eine Antwort. Jedes Ja zählt einen Punkt.

	A Updates und Patches	Ja	Nein
01	Gibt es eine aktuelle Liste aller Geräte und Programme in Ihrem Unternehmen?	☐	☐
02	Werden kritische Sicherheitsupdates innerhalb von 7 Tagen eingespielt?	☐	☐
03	Werden auch Firewall, Router, Server und Programme aktualisiert und nicht nur Windows?	☐	☐
04	Bekommen Sie regelmäßig einen Bericht über den Update-Stand?	☐	☐

	B Erkennen und reagieren	Ja	Nein
05	Läuft auf allen PCs und Servern ein Schutz, der verdächtiges Verhalten erkennt (EDR oder XDR)?	☐	☐
06	Werden Warnmeldungen rund um die Uhr von Menschen geprüft (MDR)?	☐	☐
07	Kann ein befallenes Gerät sofort vom Netz getrennt werden, auch nachts?	☐	☐
08	Ist mit Ihrem IT-Dienstleister eine Reaktionszeit für Sicherheitsvorfälle vereinbart?	☐	☐

	C Backup und Wiederherstellung	Ja	Nein
09	Werden Server und wichtige Daten täglich gesichert?	☐	☐
10	Liegt eine Kopie der Sicherung außer Haus, und ist sie unveränderbar?	☐	☐
11	Wurde in den letzten vier Wochen eine vollständige Wiederherstellung getestet?	☐	☐
12	Sind Microsoft 365 oder Google Workspace zusätzlich gesichert?	☐	☐

Weiter mit Frage 13 auf Seite 20.

Der 20-Fragen-Schnellcheck

Kreuzen Sie auch für die letzten beiden Bereiche Ja oder Nein an. Zählen Sie danach die Punkte beider Seiten zusammen.

D Zugänge und Konten		Ja	Nein
13	Ist für alle Zugänge von außen eine Mehr-Faktor-Anmeldung Pflicht (E-Mail, VPN, Fernzugriff)?	☐	☐
14	Haben Administratoren getrennte Konten für Verwaltung und Tagesgeschäft?	☐	☐
15	Werden Konten ausgeschiedener Mitarbeiter am selben Tag gesperrt?	☐	☐
16	Wissen Sie, welche externen Dienstleister Zugriff auf Ihre Systeme haben?	☐	☐

E Notfall und Verantwortung		Ja	Nein
17	Gibt es einen Notfallplan auf Papier mit allen wichtigen Telefonnummern?	☐	☐
18	Ist festgelegt, wer im Ernstfall entscheidet und wer wen informiert?	☐	☐
19	Wissen Sie, wie lange der Wiederanlauf nach einem Totalausfall dauert?	☐	☐
20	Hat sich die Geschäftsführung in den letzten 12 Monaten über den Stand der IT-Sicherheit berichten lassen?	☐	☐

Ihre Punkte

Zählen Sie alle Ja-Antworten zusammen. Die Auswertung steht auf der nächsten Seite.

____ / 20

Ihre Auswertung

Die Summe zeigt, wo Sie insgesamt stehen. Wichtiger ist Ihr schwächster Bereich, denn Angreifern genügt eine offene Stelle.

17 bis 20 · Grün

Gut aufgestellt

Ihre Grundlagen stehen. Lassen Sie sich die Ja-Antworten einmal im Jahr belegen und wiederholen Sie den Check alle sechs Monate.

11 bis 16 · Gelb

Lücken mit Ansage

Sie haben eine Basis, aber sie hat Löcher. Gehen Sie jedes Nein einzeln durch. Beginnen Sie mit den Zugängen (Bereich D) und dem Backup (Bereich C).

0 bis 10 · Rot

Handeln Sie jetzt

Mehrere Grundlagen fehlen oder sind nicht belegt. Holen Sie sich Unterstützung, bevor jemand anderes die Lücken findet. Die Reihenfolge steht auf Seite 23.

Ihr schwächster Bereich zuerst

Haben Sie in einem Bereich weniger als drei Ja, fangen Sie dort an.

A	Geräteliste erstellen lassen und Fristen für Updates schriftlich vereinbaren.	**S. 11**
B	Klären, wer nachts und am Wochenende einen Alarm sieht und handeln darf.	**S. 12**
C	Einen vollständigen Wiederherstellungstest beauftragen und das Protokoll zeigen lassen.	**S. 13–14**
D	Mehr-Faktor-Anmeldung für alle Zugänge von außen einschalten.	**S. 14**
E	Notfallkarte ausfüllen und festlegen, wer im Ernstfall entscheidet.	**S. 17**

Ein Ja zählt nur mit Beleg

„Das macht unser Dienstleister“ ist erst dann ein Ja, wenn Sie den Bericht dazu gesehen haben. Fragen Sie nach, bevor Sie ankreuzen. Die acht Fragen von Seite 18 helfen dabei.

In sechs Monaten noch einmal

Notieren Sie Ihr Ergebnis und das Datum. Wer den Check zweimal im Jahr wiederholt, sieht, ob sich etwas bewegt. Datum: _____ Punkte: ____ / 20

Sie möchten Ihr Ergebnis mit jemandem besprechen, der täglich mit diesen Fragen arbeitet? Auf Seite 25 steht, wie das geht.

Drei Schritte. Drei klare Aufträge.

Geben Sie jedem Auftrag einen Verantwortlichen, einen ersten Termin und einen Nachweis. Auf Seite 23 sehen Sie, wie Sie diese drei Aufgaben über das Jahr verteilen.

1 Kritische Lücken schließen

Lassen Sie die von außen erreichbaren Systeme erfassen. Vereinbaren Sie Update-Fristen und wer bei einer akut ausgenutzten Lücke sofort entscheiden darf.

Nachweis: Liste offener kritischer Lücken mit Frist und Zuständigkeit.

2 Auf Angriffe reagieren

Lassen Sie einen Testalarm bis zum Menschen verfolgen. Wer sieht ihn nachts? Wer darf ein Konto sperren oder einen Rechner isolieren?

Nachweis: dokumentierter Alarmweg mit Vertretung und Eingriffsbefugnis.

3 Den Betrieb wieder zum Laufen bringen

Lassen Sie die vollständigen virtuellen Maschinen für einen Kundenauftrag in einer isolierten Umgebung wiederherstellen – mit Datenbank, Anwendung und benötigten Diensten. Ihre IT prüft die Datenbank auf Konsistenz. Das Fachteam gleicht Auftragsdaten ab und speichert einen Testauftrag. Messen Sie die Zeit vom simulierten Ausfall bis zur fachlichen Freigabe.

Nachweis: zulässige Ausfallzeit, gemessene Dauer und Freigabe durch das Fachteam.

INKLUSIVE

Ihr Maßnahmenplan für 2027

Vier Quartale, jedes mit einer klaren Aufgabe. Wer die Reihenfolge einhält, hat Ende 2027 einen belegbaren Stand statt eines guten Gefühls.

Q1 JANUAR BIS MÄRZ
Klarheit schaffen

- [ ] Schnellcheck ausfüllen und mit dem IT-Dienstleister besprechen
- [ ] Mehr-Faktor-Anmeldung für E-Mail, VPN und Fernzugriff einschalten
- [ ] Einen vollständigen Wiederherstellungstest durchführen lassen
- [ ] Notfallkarte ausfüllen und aufhängen

Q2 APRIL BIS JUNI
Lücken schließen

- [ ] Geräteliste erstellen: alles, was im Netz hängt
- [ ] Update-Fristen schriftlich vereinbaren: 48 Stunden, 7 Tage, 30 Tage
- [ ] Unveränderbare Backup-Kopie außer Haus einrichten
- [ ] Microsoft 365 oder Google Workspace eigens sichern
- [ ] Schutz mit Verhaltenserkennung auf alle Geräte bringen und Überwachung rund um die Uhr klären

Q3 JULI BIS SEPTEMBER
Den Ernstfall üben

- [ ] Notfallübung am Tisch: Montagmorgen, nichts geht mehr. Wer tut was?
- [ ] Wiederanlauf eines kompletten Servers testen und die Zeit messen
- [ ] Systeme ohne Hersteller-Updates ersetzen oder abschotten
- [ ] Mitarbeiter unterweisen: Verdächtiges melden statt verschweigen

Q4 OKTOBER BIS DEZEMBER
Belegen und nachschärfen

- [ ] Jahresbericht anfordern: Update-Stand, Backup-Tests, Vorfälle
- [ ] Cyberversicherung und Verträge mit dem tatsächlichen Stand abgleichen
- [ ] Schnellcheck wiederholen und mit dem Ergebnis vom Januar vergleichen
- [ ] Budget und Prioritäten für 2028 festlegen

Jeden Monat: 15 Minuten

Lassen Sie sich drei Dinge zeigen: den Update-Stand, das Protokoll des letzten Wiederherstellungstests und die Vorfälle des Monats. Mehr braucht es nicht, um als Geschäftsführung den Überblick zu behalten.

Der Plan ist ein Vorschlag für ein Unternehmen, das bei den Grundlagen beginnt. Wenn Ihr Schnellcheck in einem Bereich rot zeigt, ziehen Sie die passenden Punkte vor.

Das Protokoll für Ihren ersten Probelauf

Wählen Sie einen Geschäftsprozess, etwa die Auftragsannahme. Testen Sie die vollständige Wiederherstellung in einer isolierten Umgebung. Tragen Sie Zielzeit und Prüfergebnisse ein.

01 Auftrag, Systeme und Verantwortliche

Welcher Auftrag muss wieder laufen? Welche virtuellen Maschinen, Datenbanken und Dienste braucht er? Wer gibt ihn fachlich frei?

---

02 Zielzeit und Sicherungsstand

Maximale Ausfallzeit: _____ Tolerierbarer Datenverlust: _____
Wie wurde der Sicherungsstand vor der vermuteten Manipulation geprüft?

---

03 Wiederanlauf messen

Simulierter Ausfall: _____ VM-Rückspielung von _____ bis _____
Anwendung verfügbar: _____ Fachlich freigegeben: _____
Gesamtausfallzeit: _____ Zielzeit eingehalten? _____

---

04 Datenbank und Geschäftsvorgang prüfen

Konsistenzprüfung bestanden? Stimmen bekannte Auftragswerte mit einem unabhängigen Beleg überein? Testauftrag gespeichert und erneut geöffnet?
Abnahme durch: _____ Nacharbeit / nächster Test: _____

IHR NÄCHSTER SCHRITT

Besprechen Sie Ihr Ergebnis mit mir

KOSTENLOSES ERSTGESPRÄCH | 30 MINUTEN

Sie haben den Schnellcheck gemacht und möchten wissen, womit Sie anfangen sollen? Dann sprechen wir darüber. Sachlich, auf Augenhöhe und ohne Verkaufsdruck.

WAS WIR GEMEINSAM KLÄREN

1 **Ihr Ergebnis**
Wir gehen Ihre Nein-Antworten aus dem Schnellcheck durch.

2 **Ihre größte Lücke**
Wo käme ein Angreifer bei Ihnen heute am leichtesten hinein?

3 **Ihre ersten 30 Tage**
Sie bekommen die drei Schritte, die bei Ihnen zuerst dran sind. In klarer Reihenfolge.

Den Plan können Sie mit uns umsetzen, mit Ihrer eigenen IT oder mit Ihrem bisherigen Dienstleister. Das entscheiden Sie.



Marcel Nunweiler
Founder + CEO der IT-Nunweiler GmbH
Seit über 20 Jahren Experte für Cyber Security

Ihre ersten 30 Tage

Sie bekommen die drei Schritte, die bei Ihnen zuerst dran sind.

Gespräch buchen

SO ERREICHEN SIE MICH

TELEFON	0511 51 51 69 14
E-MAIL	info@it-nunweiler.de
WEB	it-nunweiler.de
ADRESSE	Rendsburger Str. 18, 30659 Hannover

ÜBER UNS

Die IT-Nunweiler GmbH betreut Unternehmen mit 10 bis 250 IT-Arbeitsplätzen und hat bisher über 2.600 Unternehmen begleitet. Unsere Schwerpunkte sind Cyber Security, Managed IT und KI.

Quellen

Alle Zahlen in diesem Report stammen aus den folgenden Quellen. Wo es keine belegte Zahl gibt, steht im Report auch keine.

1 **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

Die Lage der IT-Sicherheit in Deutschland 2026, vorgestellt am 19.11.2026. Berichtszeitraum 1. Juli 2025 bis 30. Juni 2026. Ergänzend die Berichte von it-daily.net, Deutscher Handwerks-Zeitung und ZDFheute vom selben Tag.

Verwendet für: Einstufung „angespannt bis kritisch“; 160 neue Schwachstellen pro Tag (plus 35 %); 53, 25 und 8 Tage bis zur ersten Ausnutzung; 90 % der angezeigten Ransomware-Fälle bei KMU; Mindestanforderungen bei KMU; Suchläufe plus 57 %, Angriffsversuche plus 48 %; Seiten 2 bis 7.

2 **Check Point Research**

Monthly Cyber Threat Report August 2026, veröffentlicht im September 2026.

Verwendet für: 1.834 Angriffe pro Woche je Unternehmen in Deutschland, plus 53 % gegenüber August 2025. Seite 5.

3 **The Register, 13.11.2026**

Bericht zum Stand der veröffentlichten Sicherheitslücken, mit Zahlen von VulnCheck und CrowdStrike sowie Hinweis auf die CISA-Richtlinie BOD 26-04 vom Juni 2026.

Verwendet für: 100.222 veröffentlichte Lücken bis 13.11.2026; 1.363 nachweislich ausgenutzte Lücken (rund 1,4 %); 88 % der Angriffe mit öffentlichem Angriffscode binnen 48 Stunden; Kriterien der CISA. Seiten 5 und 7.

4 **Hiscox**

Cyber Readiness Report 2026, zitiert nach Versicherungsbote.

Verwendet für: 41,7 Stunden Stillstand bei betroffenen deutschen KMU, 31,6 Stunden im internationalen Vergleich. Seite 6.

5 **Bitkom e. V.**

Studie Wirtschaftsschutz 2025.

Verwendet für: rund 289 Milliarden Euro Schaden im Jahr 2025, davon etwa 70 % durch Cyberangriffe. Seite 6.

Quellen und Impressum

6 ZEGO Textilveredelungszentrum GmbH

Mitteilung des Unternehmens an Kunden und Lieferanten, Juli 2026; The Register vom 13.07.2026.

Verwendet für: Angriff am 29.03.2026, fast sechs Wochen Produktionsausfall, Insolvenzantrag. Seite 8.

7 Autohaus Pichel GmbH, Chemnitz

it-daily.net vom 06.03.2026, unter Berufung auf die Sächsische Zeitung und Angaben des vorläufigen Insolvenzverwalters.

Verwendet für: Angriff im Dezember 2025, rund zwei Monate weitgehender IT-Ausfall, Verlust 2024, Insolvenzantrag März 2026, 35 Beschäftigte. Seite 8.

8 Metzgerei im Landkreis Neustadt an der Waldnaab

Polizeiangaben, verbreitet durch dpa, u. a. Abendzeitung München und nordbayern.de vom 04.11.2026; ms-aktuell.de vom 05.11.2026.

Verwendet für: Manipulation der Kühlanlagen in der Nacht zum 2. November 2026, bis zu 150 Grad, Schaden im fünfstelligen Bereich, Angriffe auf Kühlanlagen in mehreren EU-Staaten seit Oktober 2026, Supermarkt in Niederbayern. Seite 9.

9 Security-Insider

Übersicht „Cyberangriffe auf Unternehmen in Deutschland 2026“, Stand 17.11.2026.

Verwendet für: über 40 deutsche Unternehmen als Opfer im Oktober 2026. Seite 9.

10 Gesetze

BSI-Gesetz in der Fassung des NIS-2-Umsetzungsgesetzes, in Kraft seit 06.12.2025, §§ 32 und 38; Zahl von rund 29.500 Einrichtungen nach Angaben des BSI. Datenschutz-Grundverordnung, Art. 33.

Verwendet für: Pflichten der Geschäftsleitung, Meldefristen von 24 und 72 Stunden. Seiten 10 und 16.

Hinweise

Dieser Report gibt den Stand von November 2026 wieder. Die genannten Fristen für Updates und Wiederherstellungstests sind Empfehlungen der IT-Nunweiler GmbH und keine gesetzlichen Vorgaben. Der Report ersetzt keine individuelle Beratung und keine Rechtsberatung.

Herausgeber

IT-Nunweiler GmbH, Rendsburger Str. 18, 30659 Hannover. Telefon 0511 51 51 69 14, info@it-nunweiler.de, it-nunweiler.de. Verantwortlich für den Inhalt: Marcel Nunweiler.



MARCEL NUNWEILER / ZUM SCHLUSS

„Die entscheidende Frage lautet deshalb nicht ›Haben wir ein Backup?‹, sondern ›Nach wie vielen Tagen arbeiten wir wieder?‹“

DIE NOTFALLKARTE AUF SEITE 17

Wen rufen Sie an, wenn die IT ausfällt?

Tragen Sie die direkten Nummern Ihrer IT und Ihrer Geschäftsführung auf der Notfallkarte ein. Legen Sie die ausgefüllte Karte neben das Telefon.

KONTAKT ZUM REPORT

Marcel Nunweiler

IT-Nunweiler GmbH

Rendsburger Str. 18 · 30659 Hannover

info@it-nunweiler.de

0511 51 51 69 14

it-nunweiler.de