Sicherheitslücken 2026: Was passiert ist und was jetzt zählt

Seit dem Frühjahr 2026 finden KI-Systeme Schwachstellen in Software so schnell, dass die alten Spielregeln nicht mehr gelten. Das betrifft jedes Unternehmen, das einen Rechner, einen Router oder einen Online-Shop betreibt. Dieses Blatt sagt in Kürze, was passiert ist, warum das anders ist als frühere Lücken, und was Sie jetzt tun können. Die sieben Schritte stehen weiter unten; die ersten drei, Updates, zweiter Faktor und Sicherung, erledigen das meiste.

129.000	31 Min.	59 → 222
Lücken meldet der KI-Hersteller für April bis Juli 2026, aus Partnerberichten	vom Windows-Update bis zum Nachweis, dass sich die Lücke auslösen lässt, Messung des KI-Herstellers	Erpressungsfälle in Deutschland im Vergleich zum Vorjahr, von Microsoft erfasst, laut Presseberichten

Die 129.000 sind eine Herstellerangabe; unabhängige Zähler ordnen bislang nur einige hundert Lücken eindeutig zu. Die Richtung ist unstrittig, die genaue Zahl nicht.

Was passiert ist

Im April 2026 hat der Anbieter Anthropic ein KI-Modell vorgestellt, das Sicherheitslücken in Software selbständig findet. Innerhalb weniger Wochen fand es nach Angaben des Herstellers kritische Lücken in jedem großen Betriebssystem und jedem großen Browser, dazu tausende Lücken in über tausend Open-Source-Bausteinen, die in fast jeder Firmensoftware stecken. Eine davon war 27 Jahre alt und bis dahin niemandem aufgefallen.

Seitdem reißt die Kette nicht ab. Allein 2026 gab es ernste, zum Teil aktiv ausgenutzte Lücken in Windows, Linux, Apple-Systemen und Firefox, in Netzwerkgeräten von Cisco, Fortinet, Citrix, Ivanti, Palo Alto und SonicWall, in Microsoft Exchange und in PHP, der Technik hinter den meisten Online-Shops und Websites. Nicht jede davon stammt aus der KI-Suche, aber alle treffen auf Angreifer, die mit ihr arbeiten. Microsoft hat allein im Oktober 2026 über 1.400 Lücken an einem Tag geschlossen. Im ganzen Jahr 2025 waren es nie mehr als 177 auf einmal.

Warum das für Unternehmen alles ändert

Bisher galt: Ein Hersteller veröffentlicht ein Update, und man hat einige Wochen Zeit, es einzuspielen, bis Angreifer die Lücke ausnutzen. Erstens ist diese Zeit weg. Kriminelle nutzen dieselbe Technik, und laut BSI lässt sich aus einem veröffentlichten Update binnen Minuten bis Stunden ableiten, wie ein Angriff aussehen kann. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht von einer neuen Zeitrechnung der Cybersicherheit und schreibt in seiner Sicherheitsinformation vom 22. Juni 2026 wörtlich, „wenige Tage sind dabei keine angemessene Reaktionsgeschwindigkeit“.

Zweitens trifft es nicht mehr nur große Konzerne. Angriffe laufen automatisiert gegen alles, was im Internet erreichbar ist: Router, VPN-Zugänge (der Fernzugang ins Büro), Mailserver, Online-Shops. Ob dahinter ein Weltkonzern oder ein Fünf-Mann-Betrieb steht, spielt für den Automaten keine Rolle. Deutschland ist das einzige EU-Land unter den zehn Ländern, die in Microsofts Daten am häufigsten angegriffen werden, laut Berichterstattung zum Microsoft-Bericht.

Wie lange das so bleibt. Oft ist von 18 Monaten die Rede. Die Zahl stammt aus einer Einschätzung des Anbieters vom April 2026: In sechs bis 18 Monaten hätten auch andere Anbieter Modelle mit denselben Fähigkeiten. Inzwischen sagt derselbe Anbieter, dass frei verfügbare Modelle eine kritische Schwelle überschritten haben. Die 18 Monate sind also keine Frist, nach der es vorbei ist. Eine Entwarnung hat bisher niemand ausgesprochen. Unsere Einschätzung: mindestens bis Ende 2027 mit deutlich erhöhter Gefahr rechnen und die Abläufe so einrichten, dass sie dauerhaft tragen.

Was Sie selbst tun können, ohne Fachwissen

1. **Updates am selben Tag einspielen.** Automatische Updates überall einschalten: Windows, Mac, Handy, Browser, Router, Online-Shop. Zuerst alles, was aus dem Internet erreichbar ist (Router, VPN, Mailserver, Online-Shop). Ein Update, das eine Woche wartet, ist heute ein offenes Fenster.
2. **Zweiten Faktor überall anschalten.** E-Mail, Online-Banking, Cloud-Speicher, Verwaltung des Online-Shops, Social Media: Anmeldung nur mit Passwort plus Code aus einer App oder einem Sicherheitsschlüssel. Das stoppt den größten Teil aller Kontoübernahmen.

3. **Sicherung getrennt aufbewahren.** Eine Kopie aller wichtigen Daten auf einer Festplatte, die nach der Sicherung abgezogen wird, oder in einem Speicher, den der Rechner nicht löschen kann. Einmal im Quartal probehalber eine Datei zurückholen. Eine Sicherung, die nie geprüft wurde, ist eine Hoffnung.
4. **Alte Technik abschalten.** Windows 10 ohne die bezahlte Verlängerung von Microsoft, Windows Server 2012, Exchange 2016 und 2019, PHP 8.1 und älter bekommen keine Korrekturen mehr. Was keine Updates mehr erhält, gehört vom Netz oder wird ersetzt.
5. **Administratorrechte nur, wo sie nötig sind.** Im Alltag mit einem normalen Benutzerkonto arbeiten. Schadsoftware kann dann nur so viel, wie der Benutzer darf.
6. **Anrufe und Mails misstrauisch prüfen.** KI-Stimmen klingen inzwischen wie der Chef, die Bank oder der Lieferant. Bei Zahlungsaufträgen oder Kontoänderungen immer über eine bekannte Nummer zurückrufen, nie über die Nummer aus der Nachricht.
7. **Notfallkarte an die Wand.** Wen rufe ich an, wenn der Bildschirm eine Erpressung zeigt? Vom Netz trennen (Kabel ziehen, WLAN aus), nichts bezahlen, nichts löschen, Hilfe rufen. Das BSI stellt dafür eine IT-Notfallkarte kostenlos zum Ausdrucken bereit.

Was darüber hinaus sinnvoll ist

MIT ÜBERSCHAUBAREM AUFWAND

CyberRisikoCheck des BSI. Ein vom BSI geschulter Dienstleister geht in ein bis zwei Stunden 27 Punkte mit Ihnen durch. Der Ergebnisbericht nennt passende Förderprogramme von Bund, Ländern und Kommunen; Höhe und Bedingungen unterscheiden sich. Das Ergebnis zeigt, welche Punkte bei Ihnen fehlen.

Überwachung der Geräte. Ein Schutzprogramm, das Angriffe erkennt und meldet (Fachbegriff EDR), statt nur klassischer Virenscanner. Gibt es für kleine Betriebe als Monatsdienst.

Notfallplan und eine Übung. Einmal durchspielen: Was tun wir, wenn morgen nichts mehr geht? Wer meldet es der Versicherung, den Kunden, der Polizei?

WENN IHR BETRIEB OHNE INTERNET STILLSTEHT

Netz trennen. Kasse, Büro, Gäste-WLAN und Maschinen in getrennten Netzen, damit ein befallenes Gerät nicht alles erreicht.

Protokolle außerhalb speichern. Gemeint sind Aufzeichnungen, wer wann was getan hat. Wer einen Einbruch später nachvollziehen will, braucht sie an einem Ort, den der Angreifer nicht löschen kann.

Externe Hilfe fest vereinbaren. Ein IT-Dienstleister, der die Updates überwacht und im Notfall binnen Stunden erreichbar ist. Das BSI führt Listen qualifizierter Anbieter.

Cyberversicherung prüfen. Sie ersetzt keinen Schutz, deckt aber je nach Vertrag Betriebsunterbrechung und Wiederherstellung. Versicherer fragen die Punkte von oben häufig beim Abschluss ab.

Wie S&S Connect unterstützt. Wer die sieben Punkte nicht allein durchgehen möchte, bekommt bei uns eine Durchsicht von ein bis zwei Stunden. Das ist eine eigene Durchsicht von uns, kein CyberRisikoCheck des BSI. Anfrage per Mail oder Telefon, Kontakt siehe unten. Dieses Blatt ist eine Information, kein Angebot mit Preis.

KONTAKT

S&S Connect GbR
Nobelstraße 3-5,
41189 Mönchengladbach
info@sundsconnect.de
+49 151 40322125
Dieses Blatt im Netz:
sundsconnect.de/sicherheit-2026/

QUELLEN

1. BSI, Sicherheitsinformation 2026-262788-1032, 22.06.2026 (PDF) bsi.bund.de, Cybersicherheitswarnung 2026-262788-1032
2. BSI-Blog „Eine neue Zeitrechnung der Cybersicherheit“, 08.05.2026 bsi.bund.de, Blog 08.05.2026
3. Anthropic, Project Glasswing, 07.04.2026 anthropic.com/glasswing
4. Anthropic, Zwischenbericht Glasswing, 22.05.2026 anthropic.com/news/glasswing-initial-update
5. Anthropic, Messung vom Update bis zum Nachweis, 08.06.2026 anthropic.com/research/n-days
6. Anthropic, Cyber Verification Program mit der Zahl 129.000, 06.10.2026 anthropic.com/news/cyber-verification-program
7. Anthropic, frei verfügbare Modelle und die kritische Schwelle, 2026 anthropic.com/research/glm-5-3-and-the-spread-of-advanced-cyber-capabilities
8. Microsoft Digital Defense Report 2026, 01.10.2026, Berichterstattung dazu bei Trending Topics, 01.10.2026 microsoft.com/security/blog, trendingtopics.eu
9. Zero Day Initiative, Microsoft-Updates Oktober 2025 (177 Lücken), 14.10.2025 zerodayinitiative.com/blog, 14.10.2025
10. BSI, CyberRisikoCheck für kleine Unternehmen bsi.bund.de, Seite „CyberRisikoCheck“
11. BSI, IT-Notfallkarte zum Ausdrucken bsi.bund.de, Seite „IT-Notfallkarte“

S&S Connect GbR, Mönchengladbach. Weitergabe und Ausdruck in unveränderter Form sind ausdrücklich erwünscht, auch an Kollegen, Kunden und Lieferanten. Änderungen und Ausschnitte bitte mit uns abstimmen. Diese Information fasst öffentliche Quellen zusammen, ist allgemein gehalten und ersetzt weder eine Prüfung Ihrer Systeme noch eine Beratung im Einzelfall. Vor Änderungen an Servern, Online-Shop und Geschäftsanwendungen bitte zuerst sichern. Lizenz für den Text dieses Blatts: CC BY-ND 4.0; ausgenommen sind Logo, Marken und wörtliche Zitate aus den genannten Quellen.