

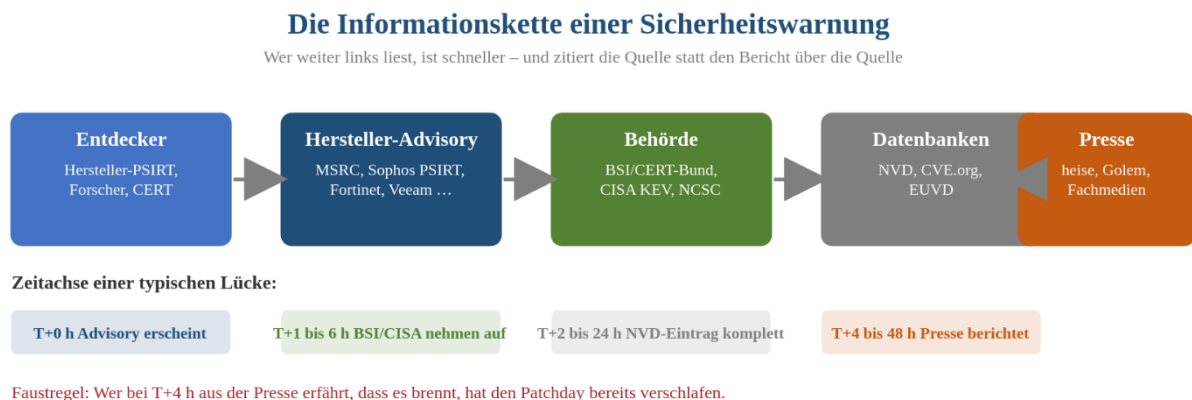
Wo informieren sich die Profis der IT-Gefahrenabwehr? Die Warnquellen, die einen Blick wert sind

Wenn du in einer Firma oder Behörde für die Abwehr von IT-Gefahren zuständig bist, hast du ein Problem, das nichts mit Technik zu tun hat: Du erfährst von den wichtigen Dingen zu spät und von den unwichtigen zu oft. Die Presse meldet die Exchange-Lücke, wenn sie schon 30 Stunden alt ist, und dazwischen liegen 400 CVEs zu Routern, die du nie besitzen wirst. Dieser Artikel sortiert, wer eigentlich warnt, wer davon schnell und verlässlich ist und wie du daraus eine Routine machst, die dich nicht auffrisst.

Die Kurzfassung für Eilige: Die Profis lesen **Hersteller und Behörden**, nicht die Presse. Sie schauen zuerst auf **aktiv ausgenutzte Lücken** (CISA KEV, BSI-Warnungen) und erst danach auf die große Masse. Und sie filtern nach dem, was sie tatsächlich betreiben, bevor sie überhaupt anfangen zu lesen.

Warum die Quelle über die Geschwindigkeit entscheidet

Jede Sicherheitswarnung durchläuft dieselbe Kette: Jemand entdeckt die Lücke, der Hersteller veröffentlicht ein Advisory, Behörden wie BSI oder CISA nehmen es auf und bewerten es, die Datenbanken (NVD, CVE.org, EUVD) füllen die Details nach, und irgendwann berichtet die Fachpresse. Jede Stufe kostet Stunden. Wer bei der Presse einsteigt, ist strukturell der Letzte – und zitiert obendrein den Bericht über die Quelle statt die Quelle selbst.



Skizze 1: Die Informationskette – je weiter links du liest, desto früher weißt du Bescheid.

Das ist kein Vorwurf an die Presse. heise, Golem und Kollegen leisten Einordnung, die ein Advisory nicht liefert. Aber Einordnung ist der zweite Schritt. Der erste ist die Frage „Muss ich heute noch etwas tun?“ – und die beantwortet dir ein Behördenfeed um 9:12 Uhr, nicht ein Artikel um 15:40 Uhr.

⚠ Achtung: Die Presse-Falle

Wer seine Gefahrenabwehr auf Nachrichtenseiten stützt, lernt zwei Dinge zu spät: dass etwas passiert ist und dass es ihn betrifft. Beides steht Stunden früher im Hersteller-Advisory. Presse gehört in die Kaffeepause, nicht in den Alarmpfad.

Drei Klassen von Quellen – und was sie dir jeweils liefern

Es lohnt sich, die Quellenlandschaft in drei Klassen zu denken. Jede hat einen anderen Job, und du brauchst alle drei – aber in unterschiedlicher Dosierung.

Klasse	Beispiele	Was sie liefert	Was sie nicht liefert
Hersteller	MSRC Update Guide, Sophos PSIRT, Fortinet PSIRT, Veeam KB, Broadcom/VMware	Die Lücke selbst, betroffene Versionen, den Patch, oft Workarounds – am schnellsten überhaupt	Einordnung, ob es dich trifft; Priorisierung gegenüber anderen Lücken
Behörden	BSI/CERT-Bund, CISA, NCSC UK, NCSC-NL, CERT-EU, CERT.at	Bewertung, Warnstufe, den entscheidenden Hinweis „wird aktiv ausgenutzt“, Handlungsempfehlungen	Produkttiefe; sie sind eine Stufe langsamer als der Hersteller
Threat-Intel-Labore	Microsoft Threat Intelligence, Sophos X-Ops, Unit 42, Talos, Huntress	Kampagnen, Angriffstechniken, Indikatoren – die Geschichte hinter der Lücke	Vollständigkeit; sie schreiben über das, was sie selbst gesehen haben

i Warum Threat-Intel-Labore keine Presse sind

Unit 42, Talos oder Sophos X-Ops sind Hersteller-Research: Sie haben die Kampagne selbst entdeckt und dokumentiert. „Laut Microsoft Threat Intelligence nutzt die Gruppe aktuell Device-Code-Phishing gegen Entra-Tenants“ ist saubere Quellenarbeit – der Bericht ist die Primärquelle. Eine Zeitschrift, die denselben Bericht zusammenfasst, ist es nicht.

Deutschland und der deutschsprachige Raum

Das **BSI** ist mehr als eine Behörde, es sind mehrere Kanäle, die du getrennt abonnieren solltest. Die Cyber-Sicherheitswarnungen (CSW) sind die seltenen, lauten Warnungen bei akuter Lage – wenn das BSI eine CSW herausgibt, ist das ein Termin für heute. Der **Warn- und Informationsdienst (WID) von CERT-Bund** liefert dagegen den täglichen Strom an Sicherheitshinweisen mit CVSS-Bewertung, mehrere pro Tag, als RSS abrufbar. Dazu kommen die Lageberichte und der IT-Grundschutz als Referenz für das „Wie sollte es sein“.

Faktenkasten: Die BSI-Kanäle

- **Cyber-Sicherheitswarnungen (CSW):** selten, hohe Dringlichkeit, eigener RSS-Feed – der Alarmkanal
- **CERT-Bund WID:** tägliche Sicherheitshinweise mit Risikoeinstufung, RSS unter wid.cert-bund.de
- **Allianz für Cyber-Sicherheit:** Praxishilfen und Erfahrungsaustausch für Unternehmen, kein Alarmkanal
- **Lagebericht und Grundschutz:** jährlich bzw. fortlaufend, Referenz statt Warnung

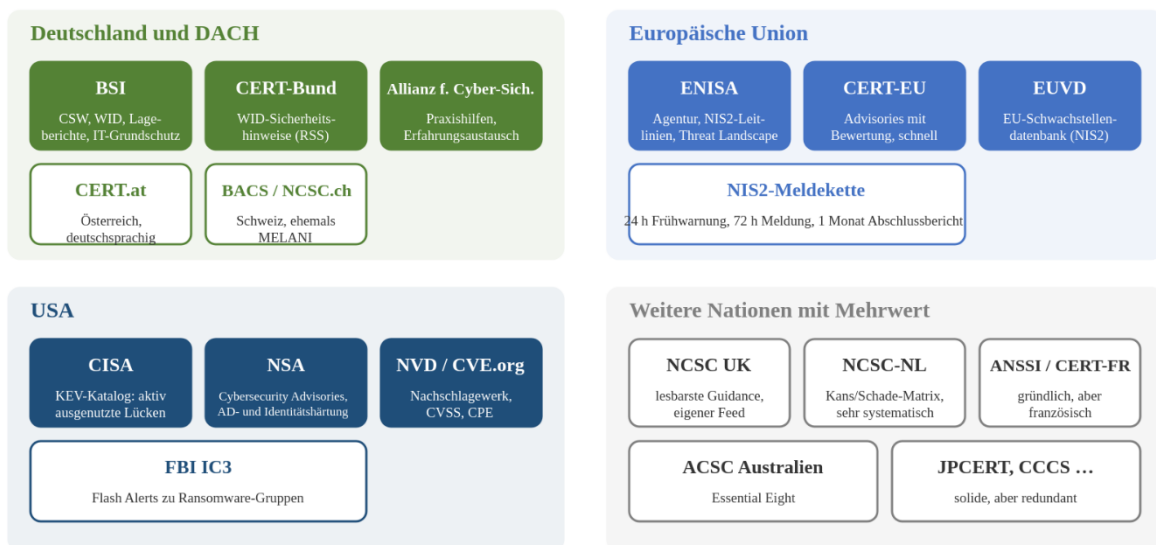
Im deutschsprachigen Umfeld lohnen zwei Ergänzungen: **CERT.at** in Österreich bringt gelegentlich Warnungen früher oder mit anderer Gewichtung als das BSI und schreibt auf Deutsch. Das Schweizer **BACS** (Bundesamt für Cybersicherheit, die frühere MELANI, heute unter NCSC.ch) ist bei Phishing-Wellen und Betrugsmaschen oft die klarste Stimme im Raum.

Europa: ENISA, CERT-EU und die neue EUVD

Auf EU-Ebene sind drei Namen relevant, die man leicht verwechselt. **ENISA**, die Agentur der Europäischen Union für Cybersicherheit, ist kein Alarmdienst, sondern die Instanz für Leitlinien, den jährlichen Threat-Landscape-Bericht und die technische Ausgestaltung von NIS2. **CERT-EU** dagegen ist das operative CERT der EU-Institutionen und veröffentlicht Security Advisories mit eigener Bewertung – häufig schneller und pointierter als nationale Stellen, weil die Redaktion klein ist und klar priorisiert.

Neu und für europäische Unternehmen perspektivisch wichtig ist die **EU Vulnerability Database (EUVD)**, betrieben von ENISA als europäisches Gegenstück zur amerikanischen NVD. Sie ist aus NIS2 hervorgegangen und bündelt Schwachstelleninformationen samt Herstellerhinweisen und Ausnutzungsstatus. Noch ist sie im Aufbau, aber sie hat zwei Vorteile: Sie ist nicht von der Finanzierung einer US-Behörde abhängig, und ein Verweis auf die EUVD klingt in einem Bericht an eine deutsche Geschäftsführung schlicht richtiger als einer auf das NIST.

Wer warnt wovor – die staatlichen Warnquellen im Überblick



Skizze 2: Wer warnt wovor – die staatlichen Quellen nach Region und Aufgabe.

Faktenkasten: NIS2 und die Meldekette

- Betroffene Einrichtungen müssen erhebliche Sicherheitsvorfälle in drei Stufen melden: **Frühwarnung innerhalb von 24 Stunden, Meldung innerhalb von 72 Stunden, Abschlussbericht innerhalb eines Monats**
- Zuständige Stelle in Deutschland ist das BSI; die Umsetzung erfolgt über das NIS2-Umsetzungsgesetz
- Wer melden muss, muss vorher wissen – die Meldepflicht ist damit auch eine Pflicht, Warnquellen systematisch zu lesen
- Die EUVD und die ENISA-Leitlinien sind die europäische Referenz, auf die sich Prüfer künftig beziehen

USA: CISA, NSA und die Datenbanken

Die amerikanische **CISA** ist für deine Praxis aus einem einzigen Grund unverzichtbar: dem **Known-Exploited-Vulnerabilities-Katalog (KEV)**. Darin stehen ausschließlich Lücken, für die eine aktive Ausnutzung nachgewiesen ist – mit Frist, bis wann US-Bundesbehörden sie schließen müssen. Das ist die beste Priorisierungshilfe, die es kostenlos gibt. Ein CVE mit CVSS 9.8 ohne KEV-Eintrag ist ein Thema für die nächste Wartung. Ein CVE mit CVSS 7.5 im KEV ist ein Thema für heute Nachmittag.

Faktenkasten: CISA KEV

- Gestartet im November 2021 mit der Binding Operational Directive 22-01
- Aufnahmekriterien: CVE-ID vorhanden, aktive Ausnutzung nachgewiesen, Behebungsmaßnahme verfügbar

- Als JSON und CSV frei abrufbar, täglich aktualisiert, mit Feld „knownRansomwareCampaignUse“
- Faustregel: KEV-Eintrag plus eigenes Produkt im Bestand = Patch heute

Die **NSA** veröffentlicht seltener, dafür tiefer: Ihre Cybersecurity Advisories behandeln regelmäßig Active-Directory- und Identitätshärtung, Kerberos, Zertifikatsdienste und Konfigurationen, die im Alltag niemand hinterfragt. Wer Windows-Infrastruktur betreibt, sollte sie kennen. Die **NVD** schließlich ist kein Nachrichtenkanal, sondern das Nachschlagewerk: CVSS-Bewertung, betroffene Produkte (CPE), Verweise. Man liest sie nach, nicht vor.

✓ Praxis-Tipp: NVD als Gedächtnis, nicht als Alarm

Behandle NVD und EUVD wie ein Lexikon: Du schlägst nach, wenn eine andere Quelle eine CVE nennt. Wer die NVD als Feed abonniert, bekommt 30 bis 60 Einträge am Tag, von denen 90 Prozent Produkte betreffen, die es im eigenen Haus nicht gibt. Als Nachschlagewerk ist sie unschlagbar, als Alarmquelle ein Lärmgenerator.

Weitere Nationen: Wo sich der Blick über den Tellerrand lohnt

Fast jedes Land hat ein CERT oder ein NCSC. Die meisten melden dasselbe wie BSI und CISA, nur später und in Landessprache. Vier Ausnahmen haben einen eigenen Blick, der sich lohnt:

Quelle	Land	Warum ein Blick lohnt	Sprache
NCSC UK	Vereinigtes Königreich	Die lesbarsten Advisories und Guidance-Dokumente überhaupt; Priorisierung ohne Behördendeutsch	Englisch
NCSC-NL	Niederlande	Jedes Advisory trägt eine Matrix aus Eintrittswahrscheinlichkeit und Schaden (Kans/Schade) – methodisch vorbildlich	Niederländisch, Bewertung sprachneutral
ANSSI / CERT-FR	Frankreich	Gründlich und schnell; wer französisch liest, findet hier oft die beste technische Tiefe in Europa	Französisch
ACSC	Australien	Die „Essential Eight“ sind weltweit Referenz für pragmatische Härtung; Advisories oft gemeinsam mit CISA	Englisch

JPCERT/CC in Japan, das kanadische Cyber Centre oder die CSA in Singapur sind solide, bringen für den deutschen Mittelstand aber kaum etwas, was nicht schon in den genannten Quellen steht. Beobachten kann man sie – priorisieren sollte man sie nicht.

Hersteller: Wer den Patch baut, weiß es zuerst

Für Microsoft-Umgebungen ist der **MSRC Security Update Guide** die erste Adresse. Er liefert jede Schwachstelle mit CVE, Bewertung, betroffenen Produkten und – wichtig – dem Feld „Exploited: Yes/No“. Am zweiten Dienstag im Monat (Patchday) kommen 80 bis 120 Einträge auf einmal; zwischendurch tröpfeln Out-of-Band-Updates und Cloud-Meldungen ein. Der **Microsoft Security Blog** und **Microsoft Threat Intelligence** liefern die Kampagnenberichte dazu – Midnight Blizzard, ToolShell, Teams als Einfallstor.

Für den Rest deines Stacks gilt dieselbe Logik: Der PSIRT-Feed deines Firewall-Herstellers (Sophos, Fortinet), die Knowledge Base deines Backup-Anbieters (Veeam), die Advisories deines Hypervisors (Broadcom/VMware) und deines Load Balancers. Wer diese vier bis sechs Feeds abonniert hat, deckt 90 Prozent der Angriffsfläche eines typischen Mittelständlers ab.

i Wenn der Hersteller keinen Feed mehr anbietet

Einige Hersteller haben ihre Advisory-Seiten in Portale verlegt, die nur noch per JavaScript laden – Feed weg, Beobachtung schwierig. Dann hilft der Umweg über KEV und NVD mit einem Filter auf den Herstellernamen: Die CVE kommt an, nur der Workaround nicht. Den holst du dir dann gezielt beim Hersteller.

Aus Quellen eine Routine machen: der Triage-Trichter

Alle genannten Quellen zusammen liefern mehrere hundert Meldungen pro Woche. Niemand liest das. Die Profis lesen es auch nicht – sie filtern in drei Stufen, und die Reihenfolge ist entscheidend.

Vom Rauschen zur Handlung – der Triage-Trichter der Gefahrenabwehr



Skizze 3: Vom Rauschen zur Handlung – drei Filter, die aus 300 Meldungen ein bis drei Aufgaben machen.

Filter 1 – Betrifft uns das überhaupt? Eine Positivliste der Hersteller und Produkte, die du tatsächlich betreibst. Das ist reine Fleißarbeit, aber sie sortiert 85 Prozent des Rauschens aus, bevor du eine Zeile gelesen hast. **Filter 2 – Wird es ausgenutzt?** KEV-Eintrag, BSI-Warnstufe, Herstellerhinweis auf aktive Ausnutzung. Das trennt „heute“ von „nächste Wartung“. **Filter 3 – Ist das System erreichbar und kritisch?** Internet-exponiert, Identitätsdienst, Admin-Rechte im Spiel? Hier entscheidet dein eigenes Inventar, nicht die Quelle.

✓ Praxis-Tipp: Die 15-Minuten-Routine

Jeden Morgen, in dieser Reihenfolge: 1. CISA KEV – neue Einträge seit gestern? 2. BSI-Cyber-Sicherheitswarnungen – gibt es eine? 3. MSRC Update Guide gefiltert auf „Exploited: Yes“. 4. Die PSIRT-Feeds deiner vier bis sechs Kernhersteller. Alles andere – NVD, Threat-Intel, Presse – liest du, wenn Zeit ist. Wer diese Viertelstunde durchhält, ist besser informiert als die meisten IT-Abteilungen, die stundenlang Newsletter lesen.

Wer das automatisieren will, braucht keinen SIEM-Anbieter: Ein Dienst, der die Feeds abholt, nach Positivliste filtert, gleiche CVEs aus verschiedenen Quellen zu einem Ereignis zusammenfasst und bei KEV-Treffern eine Nachricht schickt, ist ein Wochenendprojekt. Der Mehrwert liegt nicht in der Technik, sondern in der Disziplin, nur Hersteller und Behörden als Auslöser zuzulassen.

Häufige Fragen

Reicht es nicht, das BSI zu abonnieren?

Für den Alarmfall ja – eine Cyber-Sicherheitswarnung des BSI wirst du nicht verpassen. Für den Alltag nein: Das BSI bewertet, aber es ist eine Stufe hinter dem Hersteller, und es priorisiert nicht nach deinem Bestand. Die Kombination aus BSI, CISA KEV und den PSIRT-Feeds deiner Kernhersteller ist das Minimum.

Warum soll ich eine amerikanische Behörde lesen?

Weil der KEV-Katalog der CISA die einzige frei verfügbare, laufend gepflegte Liste nachweislich ausgenutzter Lücken ist. Das BSI verweist selbst darauf. Ob die Lücke in Washington oder Dortmund ausgenutzt wird, ist dem Angreifer egal.

Was ist der Unterschied zwischen CVSS und KEV?

CVSS misst, wie schlimm eine Lücke theoretisch ist. KEV sagt, dass sie tatsächlich ausgenutzt wird. Eine 9.8 ohne Ausnutzung ist weniger dringend als eine 7.5 mit. Wer nur nach CVSS priorisiert, patcht die falschen Dinge zuerst.

Darf ich in einem Bericht an die Geschäftsführung heise als Quelle nennen?

Du kannst, aber du solltest nicht. Nenne das Hersteller-Advisory und die Behördenwarnung – das sind die Primärquellen, auf die sich auch ein Prüfer beziehen würde. Die Presse hat dieselben Quellen gelesen wie du, nur früher.

Wie gehe ich mit Herstellern um, die keine Feeds mehr anbieten?

Über KEV und NVD mit einem Filter auf den Herstellernamen. Die CVE erreicht dich dann trotzdem, nur der Workaround nicht – den holst du dir gezielt auf der Herstellerseite. Und du nimmst das in die nächste Beschaffungsentscheidung mit: Ein Hersteller ohne Advisory-Feed macht dir die Arbeit schwerer.

Was ändert NIS2 an meinen Lesegewohnheiten?

Die Meldepflicht in 24, 72 Stunden und einem Monat setzt voraus, dass du einen Vorfall überhaupt als solchen erkennst. Wer Warnquellen systematisch liest, erkennt früher, dass eine gemeldete Lücke im eigenen Haus zum Vorfall geworden sein könnte – und kann die Frühwarnung fristgerecht abgeben.

Wie viel Zeit muss ich täglich investieren?

Mit der beschriebenen Reihenfolge – KEV, BSI-Warnungen, MSRC gefiltert, Kernhersteller – etwa 15 Minuten. Am Patchday eine Stunde. Alles darüber ist Lektüre, keine Gefahrenabwehr.

Primärquellen

- [BSI – Cyber-Sicherheitswarnungen und Lageberichte](#)
- [CERT-Bund – Warn- und Informationsdienst \(WID\)](#)
- [CISA – Known Exploited Vulnerabilities Catalog](#)
- [NSA – Cybersecurity Advisories and Guidance](#)
- [Microsoft Security Response Center – Security Update Guide](#)
- [ENISA – Agentur der Europäischen Union für Cybersicherheit](#)
- [CERT-EU – Security Advisories](#)
- [EU Vulnerability Database \(EUVD\)](#)
- [NCSC UK – National Cyber Security Centre](#)
- [NCSC-NL – Nationaal Cyber Security Centrum](#)
- [CERT.at – Computer Emergency Response Team Austria](#)
- [BACS – Bundesamt für Cybersicherheit \(Schweiz\)](#)

Weiter im Kompetenzbereich Microsoft 365 Security

- › [Microsoft 365 Security – der Kompetenzbereich im Überblick](#)
- › [Tenant-Härtung: die Checkliste für Microsoft 365](#)

- › [TerminalFix Berlin: Was der Fall für Microsoft-365-Tenants bedeutet](#)
- › [Microsoft 365 Security Beratung](#)
- › [Microsoft 365 Security Schulung](#)

Stand dieses Artikels

Stand: 12. September 2026. Behördenstrukturen und Feed-Adressen ändern sich; die genannten Institutionen und ihre Aufgaben sind stabil, einzelne Kanäle solltest du vor dem Abonnieren kurz prüfen.