QUICK GUIDE

Lieferant oder Cloudanbieter meldet ein Sicherheitsproblem – was jetzt?

Sieben Fragen für die ersten Schritte

Ein Softwareanbieter informiert über eine kritische Schwachstelle. Ein Cloudanbieter meldet einen Cybervorfall. Ein Lieferant weist auf eine betroffene Komponente hin.

Solche Meldungen kommen von außen. Die entscheidenden Fragen entstehen aber im eigenen Unternehmen: Betrifft uns das konkret? Was wissen wir sicher? Welche Informationen fehlen? Und wer muss jetzt übernehmen?

Dieser Quick Guide hilft Ihnen bei der Erstaufnahme.

Er strukturiert die ersten Informationen, bevor Sie in eine detaillierte technische, vertragliche, regulatorische oder produktbezogene Bewertung einsteigen.

7	Fragen	1	Erstaufnahme	2	Vertiefungspfade

Fachstand: September 2026

Kostenloser Quick Guide · keine Registrierung erforderlich

WICHTIG VORAB

Bei einem akuten Vorfall gilt Ihr Incident-/Notfallprozess

STOP-HINWEIS

Wenn bereits ein laufender Angriff, ein erheblicher Ausfall, eine akute Gefährdung oder ein möglicher eigener Security Incident vorliegt, darf dieser Quick Guide den bestehenden Incident-/Notfallprozess nicht verzögern.

DIE SIEBEN FRAGEN AUF EINEN BLICK

1. **Was wurde konkret gemeldet?**
2. **Welcher Service, welches Produkt oder welche Komponente ist gemeint?**
3. **Wo nutzen wir das selbst?**
4. **Was ist bestätigt – und was ist noch unklar?**
5. **Welche Informationen brauchen wir noch vom Anbieter?**
6. **Wer muss intern übernehmen?**
7. **Was müssen wir dokumentieren – und wann prüfen wir erneut?**

LEISTUNGSGRENZE

Der Guide ersetzt keine technische Incident Response, Rechtsberatung oder fallbezogene CRA-, NIS2-, Datenschutz- oder sonstige Meldeprüfung.

FRAGEN 01-02

Eingangssignal und konkreten Bezug sichern

01 Was wurde konkret gemeldet?

Beginnen Sie mit der Originalinformation – noch ohne vorschnelle Bewertung.

ERFASSEN / PRÜFEN

- Datum und Uhrzeit des Eingangs
- Absender und Quelle
- Lieferant oder Anbieter
- Art der Meldung
- Advisory-ID, Ticket oder CVE, falls vorhanden
- vom Anbieter genannte Dringlichkeit
- Link bzw. Originalmeldung sichern

LEITFRAGE

Handelt es sich um eine Schwachstelle, einen bestätigten Vorfall, eine vorsorgliche Warnung, einen Patch-Hinweis oder eine allgemeine Information?

ZIEL: Später nachvollziehen können, was tatsächlich eingegangen ist.

02 Welcher Service, welches Produkt oder welche Komponente ist gemeint?

Eine allgemeine Anbieterwarnung wird erst handhabbar, wenn sie einem konkreten technischen oder vertraglichen Bezug zugeordnet werden kann.

ERFASSEN / PRÜFEN

- Produkt, Dienst oder Plattform
- betroffene Komponente
- Version, Build oder Firmware
- Hosting- oder Servicevariante
- betroffene Region, Umgebung oder Mandant, falls relevant

LEITFRAGE

Ist genau die von uns genutzte Variante betroffen – oder betrifft die Meldung einen anderen Produkt- oder Versionsstand?

FRAGEN 03-04

Eigene Betroffenheit und Informationslage trennen

03 Wo nutzen wir das selbst?

Jetzt wird aus der externen Meldung eine interne Betroffenheitsfrage.

ERFASSEN / PRÜFEN

- betroffene Anwendung oder Geschäftsprozess
- eigenes Produkt oder technische Lösung
- Standort, Bereich oder Kunde
- relevante Daten oder Schnittstellen
- angebundene oder abhängige Systeme
- kritische betriebliche Funktion

LEITFRAGE

Welche konkrete eigene Abhängigkeit könnte betroffen sein, wenn die Meldung zutrifft?

ZIEL: Nicht nur wissen, dass der Anbieter betroffen ist, sondern die eigene Nutzung verstehen.

04 Was ist bestätigt – und was ist noch unklar?

Trennen Sie bestätigte Fakten, Annahmen und offene Informationen.

BESTÄTIGT

- betroffene Version bekannt
- Patch verfügbar
- konkreter Service bestätigt
- Nicht-Betroffenheit einer Variante bestätigt

ANNAHMEN

- „Wir nutzen vermutlich eine andere Version."
- „Unsere Daten dürften nicht betroffen sein."
- „Der Provider wird das vollständig beheben."

OFFEN

- keine eindeutige Versionsangabe
- unklare Ausnutzbarkeit
- keine Aussage zu Unterauftragnehmern
- keine Aussage zu Daten / Zeitraum
- kein Update-Termin

LEITFRAGE

Welche Aussage können wir belegen – und welche Information fehlt noch für unsere eigene Bewertung?

FRAGEN 05-06

Fehlende Anbieterinformationen und interne Verantwortung

05 Welche Informationen brauchen wir noch vom Anbieter?

Nicht jede Situation benötigt dieselbe Prüftiefe. Je nach Nutzung und Kritikalität können insbesondere relevant sein:

ERFASSEN / PRÜFEN

- genaue betroffene Produkte, Services oder Versionen
- technische Beschreibung der Schwachstelle oder des Vorfalls
- Zeitpunkt, Zeitraum und bekannte Ausnutzung
- Patches oder Risikominderungsmaßnahmen
- mögliche Auswirkungen und betroffene Daten/Services
- Unterauftragnehmer- oder Komponentenbezug
- SBOM-/VEX-Informationen
- nächstes Provider-Update und Abschlussinformation

LEITFRAGE

Welche fehlende Information benötigen wir für unsere eigene Bewertung oder Entscheidung?

06 Wer muss intern übernehmen?

Eine Provider-Mail darf nicht zwischen Postfächern verloren gehen.

ERFASSEN / PRÜFEN

- IT / Informationssicherheit
- Product Security / Entwicklung
- Einkauf / Supplier Management
- Datenschutz
- Qualität / Compliance
- Incident Management
- Produktverantwortliche
- Management oder Freigabestelle

LEITFRAGE

Wer besitzt die benötigten fachlichen Informationen – und wer darf über Maßnahmen, Risiko, Freigabe oder Eskalation entscheiden?

ZIEL: Einen eindeutigen Owner festlegen, statt die Meldung nur weiterzuleiten.

FRAGE 07

Dokumentieren, entscheiden und erneut prüfen

07

Was müssen wir dokumentieren – und wann prüfen wir erneut?

Ein Vorgang ist nicht erledigt, nur weil die erste E-Mail beantwortet wurde.

ERFASSEN / PRÜFEN

- Eingangssignal
- Anbieter, Service oder Komponente
- eigener Bezug
- bestätigte Fakten
- offene Fragen
- angeforderte Informationen
- verantwortlicher Owner
- eingeleitete Sofortmaßnahmen
- Entscheidung oder Eskalation
- nächster Review-Termin
- Abschlussinformation, sobald vorhanden

LEITFRAGE

Woran erkennen wir später, warum wir so entschieden haben – und ob neue Informationen eine Neubewertung auslösen?

ERSTAUFNAHME ABGESCHLOSSEN?

Ein kontrollierter Erststand bedeutet nicht, dass der Fall fachlich abgeschlossen ist.

- ein eindeutiger Owner ist benannt
- die eigene Nutzung oder Abhängigkeit ist identifiziert
- bestätigte Fakten und Informationslücken sind getrennt
- eine nächste Maßnahme oder Eskalation ist festgelegt
- ein Review-Zeitpunkt oder Abschlusskriterium ist bekannt

MERKSATZ

Neue Informationen des Anbieters, eine geänderte Version, ein Patch, ein zusätzlicher Incident-Befund oder eine regulatorische Bewertung können eine erneute Prüfung auslösen.

ARBEITSBLATT

Erstaufnahme

Kompakter Arbeitsblock zum Ausfüllen oder Ausdrucken.

Ereignis / Meldung

Datum / Uhrzeit

Lieferant / Anbieter

Betroffener Service / Produkt / Komponente

Version / Konfiguration

Owner

Eigene Nutzung / Abhängigkeit

Bestätigte Fakten

Annahmen

Offene Fragen / fehlende Nachweise

Sofortmaßnahmen

Nächster Review

Status / Abschluss

NÄCHSTER THEMENPFAD

Welcher Weg ist danach relevant?

Die Erstaufnahme hilft, die weitere Bearbeitung in den passenden Kontext zu überführen.

A · LIEFERANT / SAAS / CLOUD / SERVICE

Lieferanten- und Drittanbieter-Cybersicherheit

Wenn es primär um eine betriebliche Abhängigkeit von einem externen Anbieter geht, folgen typischerweise Fragen zu:

- Kritikalität
- Lieferantenprüfung
- vertraglichen Anforderungen
- Nachweisen
- Schwachstellen-/Incident-Schnittstellen
- Monitoring und Änderungen
- Exit und Resilienz

Mehr zur Lieferanten-Cybersicherheit

B · DRITTKOMPONENTE IM EIGENEN PRODUKT

Cyber Resilience Act

Wenn Software, Firmware oder Komponente Bestandteil eines eigenen Produkts mit digitalen Elementen ist, können insbesondere relevant werden:

- Produkt- und Versionsbezug
- Produktsicherheit
- Schwachstellenbewertung
- Security Updates
- Nachweise
- gegebenenfalls CRA-Reporting

Mehr zum Cyber Resilience Act

ABGRENZUNG

Beide Themen können sich überschneiden. Entscheidend ist, ob die Sicherheitsmeldung primär eine externe Unternehmensabhängigkeit betrifft oder ob eine betroffene Drittkomponente Bestandteil Ihres eigenen Produkts mit digitalen Elementen ist.

GRENZEN UND NÄCHSTE SCHRITTE

Wann reicht dieser Quick Guide nicht aus?

Ziehen Sie den passenden internen Prozess oder Fachunterstützung hinzu, wenn beispielsweise:

- ein laufender Angriff oder erheblicher Security Incident möglich ist
- die technische Betroffenheit nicht beurteilt werden kann
- kritische Systeme oder Services ausfallen
- sensible oder personenbezogene Daten betroffen sein könnten
- eine gesetzliche, regulatorische oder vertragliche Meldepflicht möglich ist
- eine aktiv ausgenutzte Schwachstelle im Raum steht
- Lieferanteninformationen widersprüchlich oder wesentlich unvollständig bleiben
- trotz offener wesentlicher Risiken eine Freigabe- oder Weiterbetriebsentscheidung erforderlich ist

NÄCHSTER SCHRITT

Lieferanten-Cybersicherheit vertiefen

Für Lieferanten, SaaS-/Cloud-Dienste, Softwareanbieter und andere externe Abhängigkeiten.

www.sp-services-gmbh.de/de/lieferanten-cybersicherheit/

Cyber Resilience Act für den eigenen Produktfall

Wenn die betroffene Software, Firmware oder Komponente Teil eines eigenen Produkts mit digitalen Elementen ist.

www.sp-services-gmbh.de/de/cyber-resilience-act/

HINWEIS

Dieser Quick Guide dient der strukturierten Erstaufnahme. Er ersetzt keine technische Incident Response, individuelle Rechtsberatung oder fallbezogene CRA-, NIS2-, Datenschutz-, Vertrags- oder sonstige Fachprüfung.