INCIDENT-PLAYBOOK SUP-01

Verdacht auf kompromittierten Lieferanten

Lieferanten & Softwareentwicklung

Ein Lieferant, Dienstleister oder Softwareanbieter meldet einen Sicherheitsvorfall, oder seine Kommunikation wirkt plötzlich auffällig. Der Angriff trifft ein anderes Unternehmen, die Auswirkungen landen trotzdem im eigenen Betrieb.

- Lieferant informiert über einen Sicherheitsvorfall
- Bekannter Ansprechpartner schickt plötzlich seltsame Anhänge
- Mail mit geänderten Bankdaten eines Lieferanten
- Softwareanbieter warnt vor manipuliertem Update

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Keine Zahlung freigeben und keine Stammdaten ändern, solange der Vorfall nicht geklärt ist.

02 Aktuelle Mails und Anhänge dieses Lieferanten nicht öffnen und nichts installieren, was von dort kam.

03 Rückfragen ausschließlich über eine bekannte Telefonnummer aus dem eigenen System, nie über Kontaktdaten aus der verdächtigen Nachricht.

04 Festhalten, welche Zugänge dieser Lieferant zu internen Systemen hat, etwa Fernwartung, Portal oder Schnittstelle.

05 Sofort melden, auch wenn der Vorfall beim anderen Unternehmen passiert ist.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister und die für den Lieferanten zuständige Fachabteilung. Bei Zahlungsbezug zusätzlich Buchhaltung und Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Verdächtige Nachrichten als Anhang weitergeben, nicht als Weiterleitung mit anklickbaren Links.

WAS BEREITHALTEN

- Um welchen Lieferanten es geht
- Woher die Information über den Vorfall stammt
- Welche Zugänge oder Schnittstellen bestehen
- Ob offene Zahlungen oder Bestellungen laufen
- Ob zuletzt Software oder Updates von dort kamen

Nicht tun

HÄUFIGE FEHLER

- × Geänderte Bankdaten übernehmen, weil die Mail vom bekannten Ansprechpartner kommt.
- × Die Rückfrage über die Kontaktdaten aus der verdächtigen Nachricht stellen.
- × Den Fernwartungszugang des Lieferanten stillschweigend offen lassen, bis sich jemand meldet.
- × Andere Kunden oder Partner des Lieferanten eigenständig warnen.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT sperrt oder beschränkt die Zugänge des Lieferanten und prüft die Protokolle auf Zugriffe über diesen Weg.
- → Die Fachabteilung klärt über einen gesicherten Kanal, welche Daten und Prozesse betroffen sind, und dokumentiert die Antworten.
- → Sind eigene personenbezogene Daten betroffen, folgt die Bewertung nach Art. 33 DSGVO durch die Datenschutz-Ansprechperson.
- → Wesentliche und wichtige Einrichtungen nach NISG 2026 prüfen, ob daraus ein erheblicher Cybersicherheitsvorfall im eigenen Haus wird, der nach § 34 zu melden ist.

Verweise: Incident-Kontaktblatt (PDF) · Verdacht auf Datenschutzverletzung (DAT-05) · Insights zu Drittparteien und Lieferkette · Interne Kontakte siehe Incident-Kontaktblatt

Playbooks sind der Anfang. Der Prozess dahinter ist Führungsarbeit.

Alle Playbooks, Kontaktblatt und Hintergründe online — kostenfrei und ohne Anmeldung.

wermescher.com/tools/it-notfallplan