INCIDENT-PLAYBOOK SUP-02

Verdächtige Software oder Abhängigkeit

Lieferanten & Softwareentwicklung

Ein Programm, eine Bibliothek, ein Paket oder eine Erweiterung verhält sich anders als erwartet oder stammt aus einer zweifelhaften Quelle. Der Verdacht entsteht oft beim Installieren, beim Build oder durch eine Sicherheitswarnung zu einer Komponente, die bereits im Einsatz ist.

- Paket mit Tippfehler oder ungewohnter Schreibweise installiert
- Neue Version einer Bibliothek baut unerwartete Verbindungen auf
- Sicherheitswarnung zu einer genutzten Abhängigkeit
- Tool oder Erweiterung aus inoffizieller Quelle installiert

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Nicht weiter bauen, nicht ausrollen und nichts veröffentlichen, was die verdächtige Komponente enthält.

02 Name, Version und Herkunft der Komponente notieren, ebenso wann und auf welchem System sie installiert wurde.

03 Den aktuellen Stand sichern: Lockfile, Build-Protokoll und Warnmeldung nicht verändern und nicht löschen.

04 Zugangsdaten, die auf dem betroffenen Rechner oder in der Pipeline verfügbar waren, nicht mehr verwenden, bis die IT entschieden hat.

05 Sofort melden, auch wenn sich die Warnung später als Fehlalarm herausstellen könnte.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister und die Leitung der Softwareentwicklung. Wurde bereits an Kunden ausgeliefert, zusätzlich die Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt. Komponente und Fundstelle genau benennen, keine Installationsdatei per Mail weiterleiten.

WAS BEREITHALTEN

- Name, Version und Bezugsquelle der Komponente
- Auf welchen Rechnern, Servern oder Pipelines sie läuft
- Seit wann sie im Einsatz ist
- Ob sie in ausgelieferte Software oder Updates eingeflossen ist
- Was konkret auffällig war

Nicht tun

HÄUFIGE FEHLER

- × Die Komponente still entfernen oder ersetzen und den Fall damit für erledigt halten.
- × Den Build noch schnell abschließen, weil ein Termin ansteht.
- × Die verdächtige Datei an Kolleginnen und Kollegen schicken, damit sie sich das ansehen.
- × Die Datei bei einem Online-Virenscanner hochladen, wenn sie internen Code oder Daten enthalten könnte.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT prüft, wo die Komponente überall eingesetzt wird, und isoliert betroffene Systeme und Pipelines.
- → Zugangsdaten und Schlüssel, die der Komponente zugänglich waren, werden gewechselt.
- → Ist die Komponente in ausgelieferte Software gelangt, entscheidet die Geschäftsführung über die Information der Kunden.
- → Wesentliche und wichtige Einrichtungen nach NISG 2026 prüfen, ob ein erheblicher Cybersicherheitsvorfall vorliegt, der nach § 34 zu melden ist.

Verweise: Incident-Kontaktblatt (PDF) · Zugangsdaten oder Secrets veröffentlicht (SUP-03) · Rechner verhält sich ungewöhnlich (MAL-02) · Verdacht auf kompromittierten Lieferanten (SUP-01) · 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