INCIDENT-PLAYBOOK SUP-05

Entwicklungsumgebung kompromittiert

Lieferanten & Softwareentwicklung

Es gibt Anzeichen, dass ein Entwicklerrechner, ein Build-Server oder eine Pipeline von Unbefugten genutzt oder verändert wurde. Über diese Systeme laufen Code, Zugangsdaten und Releases. Ein Eingriff kann damit bis in die Software reichen, die Kunden installieren.

- Commits oder Änderungen, die niemand im Team gemacht hat
- Pipeline-Konfiguration ohne Freigabe verändert
- Unbekannte SSH-Schlüssel oder Tokens im Konto
- Build-Ergebnis weicht vom geprüften Quellcode ab

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Keine Releases, Deployments oder Updates mehr auslösen, bis die IT die Umgebung geprüft hat.

02 Einen betroffenen Rechner vom Netzwerk trennen, aber nicht ausschalten und nicht neu aufsetzen.

03 Von dieser Umgebung aus keine Passwörter mehr ändern und keine weiteren Anmeldungen durchführen.

04 Auffällige Commits, Konfigurationsänderungen und Schlüssel notieren, ohne sie zu entfernen.

05 Sofort melden. Der Verdacht genügt.

Melden

SOFORT

WEN

IT-Verantwortliche oder IT-Dienstleister und die Leitung der Softwareentwicklung sofort. Bei möglicher Auslieferung an Kunden zusätzlich die Geschäftsführung.

WIE

Telefonisch oder über den internen Meldeweg aus dem Kontaktblatt, nicht über Konten oder Rechner aus der betroffenen Umgebung.

WAS BEREITHALTEN

- Welche Rechner, Server oder Pipelines betroffen sind
- Welche Auffälligkeit wann bemerkt wurde
- Welche Zugangsdaten in der Umgebung verfügbar waren
- Welche Releases seit dem möglichen Beginn erstellt wurden
- Ob Software oder Updates an Kunden ausgeliefert wurden

Nicht tun

HÄUFIGE FEHLER

- × Verdächtige Commits zurücksetzen oder Schlüssel löschen, bevor die IT den Stand gesichert hat.
- × Den Rechner neu aufsetzen, um schnell weiterarbeiten zu können.
- × Ein dringendes Release trotzdem freigeben.
- × Den Verdacht nur im Team besprechen und die Meldung aufschieben.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die IT stoppt betroffene Pipelines, sichert Spuren und klärt, seit wann die Umgebung verändert wurde.
- → Alle Zugangsdaten, Schlüssel und Signaturzertifikate der Umgebung werden gewechselt.
- → Releases seit dem möglichen Beginn werden mit dem geprüften Quellcode abgeglichen. Über die Information der Kunden entscheidet die Geschäftsführung.
- → Wesentliche und wichtige Einrichtungen nach NISG 2026 prüfen, ob ein erheblicher Cybersicherheitsvorfall vorliegt, der nach § 34 zu melden ist.

Verweise: Incident-Kontaktblatt (PDF) · Rechner verhält sich ungewöhnlich (MAL-02) · Zugangsdaten oder Secrets veröffentlicht (SUP-03) · Verdächtige Software oder Abhängigkeit (SUP-02) · 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