CNEXT SECURITY SERVICES · ABSCHLUSSBERICHT · IM VORFALL

Abschlussbericht

KUNDE
Muster AG, Bern (erfunden)

VORFALL
INC-2026-041, Schwachstelle in SharePoint Server

DAUER
14. April 2026, 21:40 bis 15. April 2026, 16:10

ERGEBNIS
Geschlossen, keine Ausnutzung festgestellt

18 h	4	0	3
von Meldung bis Abschluss	Massnahmen	Meldungen an Behörden nötig	Lehren

Wann Sie dieses Dokument erhalten: Innerhalb einer Woche nach Abschluss des Vorfalls.

Zusammenfassung

Die Lücke wurde 2 Stunden 10 Minuten nach Veröffentlichung gemeldet, das betroffene Portal 40 Minuten nach der Erstmeldung gesperrt und der Server am nächsten Morgen aktualisiert. Die Prüfung der Protokolle seit 1. April ergab keine Spuren einer Ausnutzung. Personendaten sind nach unserer Prüfung nicht abgeflossen; eine Meldung an den EDÖB oder das BACS war nicht angezeigt. Das Portal ist seit 16:10 wieder erreichbar.

Zeitlinie

ZEIT	EREIGNIS	WER
14.4. 19:30	Microsoft veröffentlicht das Sicherheitsupdate; der Agent liest den Eintrag im Security Update Guide	Agent
14.4. 19:34	Abgleich mit dem Inventar: SRV-SP01 betroffen, aus dem Internet erreichbar; Vorschlag kritisch	Agent
14.4. 21:25	Einstufung geprüft und bestätigt, Erstmeldung geschrieben	CNEXT
14.4. 21:40	Erstmeldung per Mail und Anruf an IT-Leitung und Stellvertretung	CNEXT
14.4. 22:20	Partnerportal gesperrt	IT Muster AG
15.4. 07:50	Update installiert, Konfigurations-Assistent durchgelaufen	IT Muster AG mit CNEXT
15.4. 15:40	Protokollprüfung abgeschlossen, keine Spuren	CNEXT
15.4. 16:10	Portal freigegeben, Vorfall geschlossen	IT Muster AG

Lehren und Änderungen

- Der Reverse Proxy kannte keine vorbereitete Regel für das Sperren einzelner Sites; die Regel ist jetzt angelegt und im Alarmplan verlinkt.
- SharePoint Server 2019 erreicht am 14. Juli 2026 das Ende des Supports; die Ablösung durch SharePoint Online steht als Vorhaben im Inventar mit Termin.
- Die Stellvertretung der IT-Leitung war am Abend nur per Mail erreichbar; der Alarmplan führt neu eine zweite Telefonnummer.

So geht es weiter

Dieser Bericht geht an Geschäftsleitung und IT-Leitung und wird im Monatsbericht April unter den Fällen geführt.

Alle Namen, Systeme und Zahlen in diesem Dokument sind erfunden. Ihr Bericht enthält Ihre Umgebung am Tag der Prüfung.