Adesso Deutschland verschwieg Cyberangriff lange

Von Philipp Anz, 20. April 2023 um 13:37

SECURITY CYBERANGRIFF DEUTSCHLAND ADESSO

Foto: Engyn Arkut / Unsplash

Kunden wurden nicht über die gefährliche Situation informiert. Erst ein Whistleblower machte Medien und Security-Behörden auf den Fall aufmerksam.

Anfang Februar 2023 wurde ein Cyberangriff auf Adesso Deutschland publik. Systeme seien kompromittiert worden, Daten abgeflossen. Man habe die Situation aber im Griff und sofort Massnahmen ergriffen, beruhigte das Unternehmen. Informationen und Systeme von Kunden seien "nach aktuellem Kenntnisstand" nicht vom Angriff betroffen.

Schon damals wurden Vorwürfe laut, Adesso habe nicht schnell genug mit ausreichenden Massnahmen reagiert. Wie die 'Süddeutsche Zeitung' (Paywall) jetzt schreibt, begann der Angriff bereits im Frühsommer 2022. Ab dann seien die Netze ausgekundschaftet worden. Über eine Schwachstelle in der Software Confluence von Atlassian hätten die Hacker Ende Mai Malware eingeschleust. Kurz bevor Atlassian Patches für die kritische Lücke zur Verfügung stellte. Security-Experten warnten, die Schwachstelle könnte "Solarwinds-Ausmasse" annehmen.

Gefahr durch VPN-Verbindungen

Adessos Sicherheitsteam entdeckte den Angriff erst am 11. Januar. Zwar seien danach laut 'SZ' ein Microsoft-Ermittlerteam informiert und einige kompromittierte Nutzerkonten geschlossen worden. Doch Behörden oder Kunden erfuhren nicht, dass sie in Gefahr sind. In Deutschland zählen zu diesem Kreis grosse Konzerne wie BMW, RWE und EON, das Bundeskriminalamt, die Finanzaufsicht Bafin und die Bundesbank. Zu vielen Firmen unterhält Adesso VPN-Verbindungen, die durch einen Angriff zum Problem werden können.

Am 19. Januar schickte schliesslich ein Whistleblower Informationen zum Vorfall an 'Heise', die 'Süddeutsche Zeitung' und die Cybersecurity-Behörde BSI. Diese wurde sofort aktiv und bot Hilfe an. Adesso schrieb später, das Unternehmen "habe das BSI informiert". Tatsächlich musste das Amt erst nachfragen, um informiert zu werden.

Adesso informierte erst nach Medienberichten

Der Sicherheitschef von Adesso habe in einer internen Gruppe ein Memo verschickt: "Kurze Info an alle: Am Freitag wurde ich vom BSI angerufen, da über 'Wege' an sie durchgestochen wurde, dass wir einen Vorfall hatten." Ein ähnliches Muster wiederholte sich in den folgenden Wochen mehrfach, schreibt die Zeitung. "Adesso beherzigt offenbar die Strategie: 'Gib zu, was du nicht leugnen kannst, aber leugne, was du nicht zugeben kannst.'"

Adessos Kunden erfuhren von der Gefahr erst, als die Medien den Fall am 1. Februar publik machten und Adesso im Anschluss ebenfalls mit einer Mitteilung an die Öffentlichkeit ging. "Ein Datenabfluss von Kundendaten ist nicht nachweisbar", beschwichtigte das Unternehmen. Was Adesso aber gemäss 'SZ' verschwieg: "Das Unternehmen hat keine Ahnung, wie viel die Cyberkriminellen seit Mitte vergangenen

Jahres gesehen oder heruntergeladen haben, weil Adesso diese Datenflüsse gar nicht überwacht."

Geheimdokumente von Behörden erbeutet?

Ein Sprecher des Bundesverwaltungsamts erklärte jetzt, "es sei nicht auszuschliessen", dass die Hacker geheime Dokumente der Behörde zu Gesicht bekamen. Auch das BSI war nicht glücklich über die Taktik von Adesso. Am 9. März verschickte die Behörde eine vertrauliche Warnung an Betreiber kritischer Infrastrukturen in Deutschland: Kunden, die noch VPN-Verbindungen zu Adesso hatten, sollten sie umgehend kappen.

Doch zu diesem Datum waren schon zwei Monate seit der Entdeckung des Hacks und noch mehr Zeit seit dem Eindringen der Angreifer vergangen. Viel Zeit, in denen die Cyberkriminellen vermutlich die Möglichkeit hatten, Adessos Kunden auszuspionieren.