# US-Sicherheitsbehörde äussert heftige Kritik an Microsoft

Von Hans Joerg Maron, 3. April 2024 um 14:37

SECURITY BREACH CYBERANGRIFF VERWALTUNG MICROSOFT


## Beim Softwareriesen müsse "eine schnelle Kulturänderung" geschehen, fordert die CISA.

Ein Komitee der Cybersecurity and Infrastructure Security Agency (CISA) der USA hat untersucht, wie die chinesische Hackergruppe "Storm-0558" vor einem Jahr von Microsoft gehostete E-Mail-Konten von US-Offiziellen knacken und Informationen daraus stehlen konnte. In ihrem Bericht zur Untersuchung (PDF) wird der Softwarehersteller scharf kritisiert.

Dies hätte nie passieren sollen und wäre verhinderbar gewesen, schreibt die CISA. Microsofts Security-Kultur sei ungenügend und müsse grundlegend verändert

werden. Zum Hack habe eine "Kaskade von unnötigen Fehlern" von Seiten Microsofts geführt.

### Schlampiges Schlüsselmanagement

Beispielsweise habe Microsoft es nicht geschafft, selbst zu entdecken, dass einer seiner kryptographischen Schlüssel kompromittiert worden war. Dieser 2016 kreierte Schlüssel, der eigentlich längst hätte ungültig gemacht werden sollen, ermöglichte es Storm-0558, von Heimanwendern verwendete Outlook-Web-Access-Accounts zu knacken. Wegen einer weiteren Sicherheitslücke konnten die Hacker mit dem Schlüssel aber auch Token kreieren, die ihnen Zugang zu E-Mail-Accounts von Unternehmen und Behörden gaben. Microsoft merkte dies erst, nachdem ein Kunde den Cloud-Riesen darauf aufmerksam gemacht hatte.

In diesem Zusammenhang verweist die CISA auf das mangelhafte Schlüsselmanagement bei Microsoft für seine Consumer-Services. Das Identity-Management-System für Comsumer-Services wurde Anfang der 2000er-Jahre entwickelt. Dabei verzichtete Microsoft darauf, ein System zum automatischen Austausch von veralteten Schlüsseln einzurichten. Stattdessen wurde dies manuell erledigt – aber nur bis 2021, als ein missglückter Schlüsseltausch einen Ausfall der Microsoft-Cloud verursachte. Danach und bis zum Breach im letzten Jahr verwendete Microsoft gar kein Tool mehr, dass seine Mitarbeitenden auf veraltete Schlüssel hinwies.

Des Weiteren habe es Microsoft versäumt, seine anfänglichen Statements zum Vorfall, die einige Unwahrheiten enthielten, in vernünftiger Zeit zu korrigieren.

### Umfangreiche Kulturänderung gefordert

Das mangelhafte Schlüsselmanagement ist für die CISA aber nur eines von mehreren Indizien für die schlechte Security-Kultur bei Microsoft, die auch zu anderen Security-Vorfällen geführt habe. Andere Cloud-Provider seien in Sachen Security sorgfältiger. Gleichzeitig seien die weit verbreiteten Microsoft-Produkte grundlegend wichtig für die Ökonomie, das Gesundheitssystem und die Verwaltung und damit auch die Sicherheit der USA.

Die Forderungen der Agentur an Microsoft gehen daher weit über ein verbessertes Schlüsselmanagement hinaus. Die Microsoft-Führung sollte Entwicklerteams anweisen, die Entwicklung neuer Features vorerst zurückzustellen, schreibt sie. Stattdessen sollten sie sich zuerst auf substantielle Verbesserungen der Security in der Cloud-Infrastruktur und über die ganze Produktpalette hinweg konzentrieren. Zudem sollten Security-Risiken auch in Zukunft voll analysiert und behoben werden, bevor neue Features veröffentlicht werden.

Um eine schnelle Änderung der Security-Kultur sicher zu stellen, so die CISA weiter, sollten sich auch der CEO und das Management viel stärker darauf fokussieren. Dazu gehöre die Erarbeitung und Veröffentlichung eines spezifischen und für das Management verbindlichen Zeitplans für Security-Reformen in der Produktpalette und im gesamten Unternehmen.