PRESSEMITTEILUNG

Secutec und SOCRadar analysieren die Auswirkungen des groß angelegten Cyberangriffs auf den Firewall-Hersteller Fortinet in Österreich

Zusammenfassung:

- Eine Untersuchung von Secutec und SOCRadar zeigt, wie Hacker massenhaft in Unternehmensnetzwerke eindringen, auch in Österreich.
- Im Februar 2026 wurden insgesamt 374 Firewalls von österreichischen Unternehmen gehackt. Umfangreiche Analysen von Secutec haben ergeben, dass 199 davon derzeit noch über das Internet mit den gestohlenen Administratorrechten zugänglich sind.
- Auf einigen untersuchten Firewalls hat Secutec bereits neue Accounts gefunden, die Hacker selbst erstellt haben.
- Unternehmensdaten werden abgezogen, wofür Hacker in einer späteren Phase Lösegeld fordern können: Das ist das neue Ransomware-Modell.

Hohenzell, 22. Juni 2026

Mindestens 374 Firewalls von österreichischen Unternehmen sind von dem groß angelegten Cybervorfall «FortiBleed» betroffen , bei dem Kriminelle Zugangsdaten zu Fortinet-Firewalls erbeutet haben und diese aktiv missbrauchen. Dies geht aus einer Analyse des Cybersicherheitsunternehmens Secutec hervor, das die Auswirkungen in Österreich gemeinsam mit der Threat Research Unit von SOCRadar, einem Spezialisten für *Darknet-Überwachung,* erfasst hat. Bei fast 200 österreichischen Organisationen haben Angreifer auch heute noch Administratorzugriff auf die Firewall sowie auf das Netzwerk der betroffenen Organisationen.

FortiBleed gilt als einer der grössten Vorfälle, die es je bei einem Sicherheitsanbieter gegeben hat. Weltweit haben Secutec und SOCRadar mehr als 75'000 kompromittierte Firewalls identifiziert. Über 110 Millionen Anmeldedaten wurden im Rahmen einer groß angelegten Kampagne abgegriffen, die bereits seit Anfang 2026 läuft und bis heute aktiv ist.

Der Angriff nutzt das Fortinet-Partnerportal aus, über das IT-Dienstleister Zugriff auf die Umgebungen ihrer Kunden haben. Durch eine Sicherheitslücke konnten Hacker die Zugangsdaten von Zehntausenden von Partnern erbeuten, wodurch sie nicht nur in eine einzelne Organisation, sondern in eine ganze Kette von Kundennetzwerken eindringen konnten. Das erklärt, warum sich die Auswirkungen gleichzeitig auf verschiedene Branchen ausbreiten und warum auch kleinere Organisationen betroffen sind.

Erhebliche Auswirkungen in Österreich

Die detaillierte Analyse zeigt, dass die Auswirkungen umfangreich sind. Die gestohlenen Zugangsdaten betreffen Unternehmen aus unterschiedlichsten Branchen wie Anwaltskanzleien, lokale Behörden, Schulen und andere Dienstleister. In 213 Fällen sind die betroffenen Firewalls

nach wie vor direkt über das Internet erreichbar. Bei 199 dieser Firewalls kann man sich immer noch mit den Administratorrechten anmelden.

Die Ursache liegt häufig in mangelhaften Sicherheitspraktiken. So zeigt sich, dass bei keiner der untersuchten Firewalls die Multi-Faktor-Authentifizierung aktiviert war, während IT-Partner in vielen Fällen identische Passwörter für mehrere Kunden verwenden. Zudem laufen ein Großteil der betroffenen Systeme nicht mit der neuesten Firmware, wodurch bekannte Schwachstellen weiterhin für Missbrauch offenstehen.

Hacker weiterhin aktiv

Den Untersuchungen der beiden Cybersicherheitsorganisationen zufolge zeigt FortiBleed eine deutliche Weiterentwicklung in der Vorgehensweise von Cyberkriminellen. *«Während Ransomware-Angriffe früher vor allem auf die Verschlüsselung von Daten abzielten, verlagert sich der Fokus nun auf den Diebstahl und Handel mit Zugriffsrechten und Daten. Das bezeichnen wir als Initial Access Brokerage. In der Analyse wurde festgestellt, dass Hacker bei einigen Fällen bereits neue Konten angelegt haben, was darauf hindeutet, dass der Zugriff für den Verkauf im Dark Web vorbereitet wird. Wir haben festgestellt, dass es bei verschiedenen Organisationen weltweit bereits zu Datenexfiltration gekommen* ist», sagt Daniel Rossgatterer, Geschäftsführer von Secutec.

Die Operation wird mit einer russischen Gruppe in Verbindung gebracht, ist auffallend gut organisiert und koordiniert und von beispiellosem Ausmaß. Den Untersuchungen zufolge haben sich die Angreifer mittels «Brute-Force»-Angriffen Zugang verschafft, indem sie automatisiert große Mengen an Passwörtern und Benutzernamen kombiniert haben. Einmal im System, installierten sie *«FortigateSniffer*», die über die Firewall den gesamten Netzwerkverkehr überwachen und Anmeldedaten über Dutzende von Protokollen abfangen kann.

Die erbeuteten Daten werden anschließend geknackt, angereichert und genutzt, um weiter in interne Systeme vorzudringen, woraufhin sensible Daten systematisch entwendet werden. Die Ermittler stellen fest, dass die Infrastruktur der Angreifer nach wie vor in Betrieb ist und täglich neue Kompromittierungen stattfinden.

Österreichische Behörden informiert

Secutec hat inzwischen das österreichische CERT als auch weitere europäischen CERTs informiert. Die beiden Unternehmen fordern Organisationen, die Fortinet-Lösungen nutzen, dazu auf, dringend Maßnahmen zu ergreifen, darunter die Aktualisierung von Systemen, die Aktivierung der Multi-Faktor-Authentifizierung sowie die Überprüfung von Zugriffsrechten und Konten.

«FortiBleed verdeutlicht, wie anfällig das aktuelle Ökosystem der IT-Dienstleistungen geworden ist, in dem ein einziges schwaches Glied den Zugriff auf Hunderte von Organisationen gleichzeitig ermöglichen kann. Wir gehen davon aus, dass diese Art von gross angelegten Kettenangriffen in den kommenden Jahren nur noch zunehmen wird», warnt Rossgatterer.

Ein Foto von Daniel Rossgatterer befindet sich im Anhang.
Er steht auch für Interviews zur Verfügung; bitte wenden Sie sich direkt an den u.a Kontakt.

***

Über Secutec

Secutec zählt zu den führenden europäischen Herstellern im Bereich Cyber Threat Intelligence und unterstützt Unternehmen und Organisationen im Kampf gegen Cyberkriminalität - von der Prävention bis zur akuten Krisenbewältigung.

Mit einem klaren Fokus auf die externe Sicht und den frühzeitigen Schutz vor Bedrohungen, entwickelt Secutec innovative Technologien, die Angriffe erkennen, bevor sie Schaden anrichten. Secutec ist besonders stolz darauf, mit Technologie und Expertise nicht nur Unternehmen, sondern auch hochsensible Institutionen zu unterstützen, darunter das CCB - Centre for Cybersecurity in Belgien und die NATO. Diese Zusammenarbeit unterstreicht den hohen Anspruch, die technologische Qualität und das Vertrauen, das Secutec sich auf internationaler Ebene erarbeitet hat.

Durch die Begleitung von mehreren hundert realen Cyberangriffen gehört Secutec zu den erfahrensten Akteuren der Branche. Im Worst Case profitieren Kunden zudem von langjähriger Erfahrung in Verhandlungen mit Cyberkriminellen. Das ist ein entscheidender Faktor, wenn es um schnelle, sichere und strategisch geführte Reaktionen geht.

Weitere Informationen unter https://www.secutec.com.

Medienkontakt

Mag. Daniel Rossgatterer MBA
Geschäftsführer
Mobil: +43 664 2050686
daniel.rossgatterer@secutec.com

Pressefoto, Secutec-Logo und weiteres Bildmaterial stehen unter folgendem Link zum Download bereit:
PRESSE - FortiBleed | Secutec

Die Verwendung ist im Zusammenhang mit redaktioneller Berichterstattung über Secutec und FortiBleed honorarfrei möglich.