0800 400 510 1

AKTUELLE INFORMATION
EXCHANGE-SERVER MIT WENIGEN KLICKS ABSICHERN

Datenschutz - Nr. 03/2021

Datenschutz

Wir entlasten Führungskräfte und schützen Mitarbeiter. Seit 1997.

Schwere Sicherheitslücken in Microsoft Exchange Servern locken Hackergruppen an

Es wird geschätzt, dass allein in Deutschland 60.000-75.000 Server kompromitiert wurden, von denen vermutlich aktuell noch ca. 9.000 Systeme offen sind.
Der Angriff auf Microsoft Exchange ist einer der schwersten Cyberattacken der jüngsten Vergangenheit. Zwar hat Microsoft Patches herausgegeben, aber die Schwachstellen locken Nachahmer an und noch immer sind weltweit auf zehntausenden von Servern keine Patches installiert.

Sowohl die Schwachstellen selbst als auch der Zugriff, der durch deren Ausnutzung erreicht werden kann, sind erheblich. Es ist daher nicht überraschend, dass mehrere Angreifer versuchten und weiterhin versuchen, anfällige Systeme zu kompromittieren, bevor diese von Netzwerkadministratoren gepatcht werden. Diese Angriffe geschahen in einem noch nie dagewesenen Ausmaß.

Das Aufspielen des Patches ist ein notwendiger erster Schritt, aber nicht ausreichend, wenn man bedenkt, wie lange die Schwachstelle in der freien Wildbahn war. Das Aufspielen des Patches beseitigt nicht den Zugang, den Angreifer möglicherweise bereits zu anfälligen Systemen erlangt haben. **Quelle: ZDNet**

Admins werden mit neuem Tool unterstützt

Mit dem jüngst veröffentlichten On-premises Mitigation Tool (EOMT) können Admins Exchange-Server mit wenigen Klicks innerhalb kürzester Zeit gegen die aktuellen Attacken absichern. Damit will Microsoft vor allem Admins helfen, die mit Patch-Routinen noch nicht so vertraut sind. Das Tool ersetzt die Sicherheitspatches aber nicht.

Tool umgehend ausführen

Das Tool kann man gratis auf der Github-Website von Microsoft herunterladen.
In einem Beitrag beschreiben die Entwickler, dass das EOMT Exchange-Server durch URL Rewrite Server vor der Initial-Attacke ProxyLogon (CVE-2021-26855) schützt. Dabei versuchen Angreifer eine nicht vertrauenswürdige Verbindung zum Server (Port 443) auszubauen. Klappt das, nutzen Angreifer weitere Lücken aus und nisten sich unter anderem mit einer Backdoor auf Servern ein.
Sind Server abgesichert, lädt das Tool den Microsoft Security Scanner herunter. Die-

Leistungsangebot Datenschutz

AKTUELL & WICHTIG!

Datenschutzrechtliche Beratung Krisenmanagement

Externer Datenschutzbeauftragter gemäß DSGVO

Sicher zum Verarbeitungsverzeichnis

Betroffenenrechte & Mitteilungspflichten steuern

Webseiten rechtskonform gestalten

Audits & Bestandsaufnahmen durchführen

Informationspflichten praktikabel umsetzen

WIE KÖNNEN WIR IHNEN HELFEN?

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck
www.fkc-gmbh.de

datenschutzanfrage@fkc-gmbh.de

AKTUELLE INFORMATION EXCHANGE-SERVER MIT WENIGEN KLICKS ABSICHERN

Datenschutz - Nr. 03/2021

Datenschutz

ser untersucht Server auf Schadcode von Angreifer. Wird er fündig, versucht er im Zuge der Attacke verbogene Servereinstellung geradezubiegen. Inwieweit das verlässlich funktioniert, ist bislang nicht bekannt.

Nur eine erste Schutzmaßnahme

Microsoft gibt an, dass diese Absicherung Exchange-Server effektiv vor derzeitig bekannten Attacken schützt. Neuartige Angriffsszenarien könnten den Schutz des Tools aber aushebeln. Deswegen gilt es nicht als allumfassende Schutzmaßnahme und Admins sollten **die verfügbaren Sicherheitspatches** zügig installieren.
Den Entwicklern zufolge funktioniert das EOMT mit Exchange-Server 2013, 2016 und 2019. Nachdem das Tool gestartet wurde, können Admins unter C:\EOMTSummary.txt einsehen, was das Werkzeug getan hat. Mit dem **Skript Test-ProxyLogon.ps1** können Admins prüfen, ob Server bereits kompromittiert sind.

Quelle: heise online

Sollten Sie feststellen, dass Ihre Systeme kompromittiert wurden, sind Sie verpflichtet eine forensische Untersuchung durchführen zu lassen. Melden Sie dies bitte umgehend Ihrem Datenschutzbeauftragten.
Falls die forensische Untersuchung einen Datenabfluss bestätigt, beginnt in diesem Fall die 72 Stunden Frist zur Meldung einer Datenpanne nach Art. 33 DSGVO gegenüber den Aufsichtsbehörden und es muss geprüft werden, ob auch Ihre Kunden/Mitarbeiter und sonstige Betroffenen informiert werden müssen.

Bitte patchen/aktualisieren Sie, wenn der Sachverhalt auf ihre Systeme zutrifft!
Bei weiteren Rückfragen kontaktieren Sie möglichst Ihren internen oder externen IT-Administrator.

datenschutzanfrage@fkc-gmbh.de

Bilder von Canva.