Vodafone GmbH, 40543 Düsseldorf

29 42C4 57F1 B9 3000 071A
DV 03.21 0,80 Deutsche Post

Abteilung: Enterprise Security
Telefon: 0800 5035 845
E-Mail: TE.Security@vodafone.com

Datum: 24.03.2021
Kundennummer: [redacted]

[redacted]

Sicherheitshinweis zu Ihrem Internetanschluss

Sehr geehrte Damen und Herren,

das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat uns mitgeteilt, dass Ihr genutzter **Microsoft Exchange Server** ein **gravierendes Sicherheitsproblem aufweist und kompromittiert wurde**. Auf Ihrem System wurde von Angreifern eine Web-Shell installiert. Diese Web-Shell kann genutzt werden, um beliebigen Programmcode mit hohen Rechten auf dem Exchange-Server auszuführen. Angreifer könnten darüber auf alle E-Mails auf dem Server zugreifen und betroffene Systeme auch mittels Ransomware verschlüsseln.

Leiten Sie diesen Sicherheitshinweis bitte umgehend an Ihre IT-Abteilung weiter.

Scannen Sie den QR-Code für weitere Informationen zu diesem Sicherheitshinweis:

https://kundensicherheit.unitymedia.de/8W2ZBX

Für das Einschleusen der Web-Shells wurden vermutlich die aktuellen kritischen Schwachstellen in Exchange (CVE-2021-26855, et al.) ausgenutzt.

Auf Ihrem System wurde zum angegebenen Zeitpunkt unter dem im Feld "webshell_path" genannten Pfad eine entsprechende Web-Shell identifiziert.

Neben Systemen, auf denen die Schwachstellen noch nicht geschlossen wurden, sind auch Systeme betroffen, auf denen bereits entsprechende Sicherheitsupdates eingespielt wurden. Diese Systeme wurden vor der Installation der Updates kompromittiert und offenbar nicht ausreichend auf bereits erfolgte Kompromittierungen geprüft.

Vodafone GmbH
Ferdiand-Braun-Platz 1, 40549 Düsseldorf, Postfach: 40543 Düsseldorf
Tel.: 0800 5035 845, Fax: +49 (0) 211/533-2200, **vodafone.de**
Geschäftsführung: Dr. Johannes Ametsreiter (Vorsitzender), Anna Dimitrova, Bettina Karsch, Andreas Laukenmann, Gerhard Mack, Alexander Saul
Vorsitzender des Aufsichtsrats: Frank Rövekamp, Sitz der Gesellschaft: Düsseldorf, **Amtsgericht Düsseldorf, HRB 38062**

Kompromittierung

Um eine Überprüfung auf eine Kompromittierung zu ermöglichen, sollte kurzfristig technisch und organisatorisch sichergestellt werden, dass relevante Logs auf dem Server nicht gelöscht oder überschrieben werden. Die Verfahren des jeweils gültigen Notfallprozesses (Datenschutz/Betriebs- oder Personalrat) sind dabei zu berücksichtigen.

Eine mögliche Shell wurde z. B. unter %PROGRAMFILES %\Microsoft\ExchangeServer\V15\FrontEnd\HttpProxy\owa\auth\ als RedirSuiteServerProxy.aspx abgelegt. Generell sind alle kürzlich erzeugten .aspx-Dateien verdächtig. Allerdings könnte eine Webshell auch in bestehende Dateien hinzugefügt werden, indem eine einzige Zeile eingefügt wird. Hinweis: Die RedirSuiteServiceProxy.aspx ist grundsätzlich legitim.

Falls eine Webshell gefunden wird, sollte die Organisation in den Incident Response Modus übergehen. Um nachzuvollziehen, welche Befehle über die Webshell abgesetzt wurden, sollte zeitnah ein Arbeitsspeicher-Image erstellt werden. Dazu sollte das ganze System forensisch gesichert werden, um prüfen zu können, ob von diesem System ein Lateral Movement ins eigene Netzwerk erfolgte. Es sind die begleitenden Maßnahmen dieser Eskalation zu berücksichtigen. (Wirkungsbewertung, Ausweichmaßnahmen, Kunden-/MA-Kommunikation, ...) Sie finden eine Übersicht zu Incident Response Maßnahmen auf den Webseiten des BSI.

Weitere Informationen finden Sie unter:

https://www.bsi.bund.de/Exchange-Schwachstellen
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-march-2-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

Haben Sie noch Fragen?
Unsere Kontaktdaten finden Sie oben im Briefkopf.

Freundliche Grüße

Vodafone Enterprise Security

Aufgrund des am 25.07.2015 in Kraft getretenen IT-Sicherheitsgesetzes informieren wir Sie gemäß des §109a Abs.4 TKG

Vodafone GmbH
Ferdiand-Braun-Platz 1, 40549 Düsseldorf, Postfach: 40543 Düsseldorf
Tel.: 0800 5035 845, Fax: +49 (0) 211/533-2200, **vodafone.de**
Geschäftsführung: Dr. Johannes Ametsreiter (Vorsitzender), Anna Dimitrova, Bettina Karsch, Andreas Laukenmann, Gerhard Mack, Alexander Saul
Vorsitzender des Aufsichtsrats: Frank Rövekamp, Sitz der Gesellschaft: Düsseldorf, **Amtsgericht Düsseldorf, HRB 38062**