Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/
Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: Hellwigstraße 8-10
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 4/2021

Datum: 03.03.2021

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Angriff auf Microsoft Exchange Server

Derzeit kommt es zu gezielten Angriffen auf Microsoft Exchange Server 2010, 2013, 2016 und 2019. Mehrere Schwachstellen, welche die Angriffe ermöglichen, werden als „kritisch“ eingestuft.

Nach erfolgreichen Angriffen, ist laut Microsoft, die Ausführung von Schadcode sowie das Lesen von internen E-Mails und Terminen möglich.

Die Angriffe auf die Exchange Server sind indes nicht ohne weiteres möglich.
Den Angreifern muss eine Verbindung zu Port 443 des Exchange Servers gelingen.

Gelingt dies, ist ein Ausnutzen der Sicherheitslücken **(CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)** möglich.

Betreiber von Exchange Servern sollten umgehend alle aktuellen Sicherheitsupdates installieren. Microsoft Exchange Online ist nicht von den Lücken betroffen.

Für Exchange Server haben die Entwickler folgende abgesicherte Versionen veröffentlicht:

- Exchange Server 2010 (RU 31 for Service Pack 3)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Laut Microsofteigenen Recherchen werden staatlich gesponserte Angreifer hinter den Angriffen vermutet. Demnach geht es bei den Angriffen insbesondere um Informationsgewinnung auf dem *Industriesektor, bei Bildungseinrichtungen und Nichtstaatlichen Organisationen(NGOs)*. Weitere Informationen können unter Quellen eingesehen werden.

Die Polizei rät

- Administratoren sollten Sicherheitsupdates so schnell wie möglich installieren.
- Werden erfolgreiche Angriffe festgestellt, sollte umgehend Strafanzeige bei der Polizei erfolgen.

Quellen:
https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2010-service-pack-3-march-2-2021-kb5000978-894f27bf-281e-44f8-b9ba-dad705534459

https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2010-service-pack-3-march-2-2021-kb5000978-894f27bf-281e-44f8-b9ba-dad705534459

https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2010-service-pack-3-march-2-2021-kb5000978-894f27bf-281e-44f8-b9ba-dad705534459

https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

https://www.heise.de/news/Jetzt-patchen-Angreifer-attackieren-Microsoft-Exchange-Server-5070309.html

Mit freundlichen Grüßen,

i.A.
KHK M.O. Schmitt
Zentrale Ansprechstelle
Cybercrime Saarland

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html