Datenschutz im Home Office: Macht Zero-Trust-Technologie die Cloud sicher?

16.04.2020 – München: Rund ein Viertel der Deutschen arbeitet derzeit von Zuhause aus[1]. Rosige Zeiten für Hacker: Sie nutzen die Krise um COVID-19 für gezielte Cyberangriffe. Sicherheitsforscher sprechen im Rahmen der Corona-Pandemie von einer der größten E-Mail-Kampagnen durch Cyberkriminelle, die jemals unter einem einzigen Thema durchgeführt wurde[2]. Auch die deutsche Verbraucherzentrale warnt explizit vor Malware und Phishing[3].

E-Mail als Einfallstor für Hacker

Gerade E-Mails sind für die Angestellten im Home Office eine immer noch unterschätzte Gefahr. So verbreiten Cyberkriminelle etwa Dokumente mit Malware als angebliche Informationen rund um SARS-CoV-2 und nutzen so die Angst der Empfänger für kriminelle Zwecke aus. Wenn Mitarbeiter diese Dokumente dann auf Firmenrechnern oder privaten Rechnern mit Zugang zum Firmennetzwerk öffnen, ist es bereits zu spät.

Darüber hinaus missbrauchen Cyberkriminelle Mails häufig für Social Engineering. Auf diese Weise können Angreifer zum Beispiel Zugangsdaten erbeuten. Besonders problematisch ist das in Verbindung mit privilegierten Nutzerkonten, wie sie in den Rechenzentren vieler Unternehmen für Administrationsaufgaben vorgesehen sind. Denn diese Konten verfügen häufig über uneingeschränkte Zugriffsrechte. So verschaffen sich die Hacker Zugriff zu den Systemen des Unternehmen entwenden oder manipulieren dort sensible Daten und Dokumente.

VPN oder lieber in die Cloud?

Trotz dieser bekannten Gefahren versenden viele Angestellte immer noch sensible Dateien per Mail oder öffnen unwissentlich gefährliche Dateianhänge. Unternehmen sollten ihre Mitarbeiter im Home Office daher sensibilisieren und dafür sorgen, dass die Angestellten beim Austausch schützenswerter Daten auf sichere und erprobte Methoden setzen.

Ideal sind beispielsweise geschützte VPN-Verbindungen oder – noch einfacher in der Anwendung – hochsichere Business-Clouds mit virtuellen Datenräumen. Hier empfehlen sich Dienste wie die Versiegelte Cloud der Deutschen Telekom oder idgard® der TÜV SÜD-Tochter uniscon, die vollständig auf privilegierte Zugänge für Administratoren verzichten und auf sogenannte Zero-Trust-Technologie setzen.

Dabei sorgen verschiedene ineinander verzahnte technische Maßnahmen für die nötige Sicherheit. Sie stellen zuverlässig sicher, dass Daten und Anwendungen innerhalb der Infrastruktur gegen Attacken und unbefugte Zugriffe geschützt sind. Dies gilt sowohl für gespeicherte Daten als auch für die Datenübertragung und -verarbeitung. Nicht einmal der Betreiber des Dienstes hat hier Zugang.

---

[1] https://www.uni-mannheim.de/gip/corona-studie/
[2] https://www.sueddeutsche.de/digital/it-sicherheit-coronavirus-hacker-cybercrime-1.4859962
[3] https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/achtung-phishing-wie-betrueger-die-coronakrise-in-emails-nutzen-45714

Anwendung findet diese hochsichere Sealed-Cloud-Technologie[4] bereits in Kliniken, staatlichen Einrichtungen und in Unternehmen mit besonders hohen Sicherheitsansprüchen; etwa als File-Sharing-Ersatz zum sicheren Datenaustausch oder für die sichere Verarbeitung von IoT-Daten. Im Home Office sorgt die Sealed Cloud für das Extra-Maß an Sicherheit – ohne, dass die Angestellten sich mit komplizierten Schlüsseln, VPN-Verbindungen und Erweiterungen befassen müssen.

Weiterführende Informationen erhalten Sie auf Anfrage bei presse@uniscon.de.

Lesenswertes aus den Bereichen Cloud-Security und Datenschutz im Internet finden Sie auf www.privacyblog.de

uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund ist uniscon in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen: www.uniscon.com

Pressekontakt

uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.com
Telefon: 089 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Markus Reck
Auf der Eierwiese 1
82031 Grünwald
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20

[4] https://de.wikipedia.org/wiki/Sealed_Cloud