uniscon
SEALED CLOUD TECHNOLOGIES
A member of TÜV

Data protection when working from home: Do zero trust technologies make the cloud secure?

April 20, 2020 - Munich: With approximately 25% of Germans currently working from home[1], the COVID-19 crisis has turned into the perfect breeding grounds for hackers, who are exploiting the context to conduct targeted cyber-attacks. Security researchers even speak of one of the largest email campaigns ever carried out by cyber-criminals on a single topic: The Corona pandemic[2]. The German consumer advice center also explicitly warns of malware and phishing[3].

Emails as a gateway for hackers

Emails, in particular, are still an underestimated danger for employees working from home. For example, cyber-criminals usually spread documents containing malware as alleged information about SARS-CoV-2, thus exploiting the fear of the recipients for criminal purposes. Once employees open these documents on their computers—be it the company computers or the personal ones with access to the company network—it is already too late.

In addition, cyber-criminals often misuse emails for social engineering. For instance, attackers can loot access data. This poses a particularly high risk when it comes to privileged user accounts since they are often intended for administrative tasks in the data centers of many companies and have unlimited access permissions. Hackers can thus gain access to the company's systems and steal or manipulate sensitive data and documents.

VPN or the cloud?

Despite these known threats, many employees still email sensitive files or unknowingly open dangerous file attachments. Companies should therefore raise awareness among those working from home and make sure that they use secure and proven methods to exchange sensitive data.

Ideally, they should use protected VPN connections or highly secure business clouds—which are even easier to use—with virtual data rooms. In this regard, services such as Sealed Cloud from Deutsche Telekom or idgard® from TÜV SÜD's subsidiary uniscon are very suitable for this purpose, since they completely dispense administrators from privileged access and rely on zero-trust technologies.

Various interlinked technical measures provide the necessary security. They reliably ensure that data and applications within the infrastructure are protected against attacks and unauthorized access. This applies to data storage, transmission and processing. Not even the service operator has access.

[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

This highly secure sealed cloud technology[4] is already being used in hospitals, government institutions and companies with particularly high security requirements, for example, for secure data exchange or the secure processing of IoT data. When working from home, the sealed cloud provides the extra level of security without employees having to deal with complicated keys, VPN connections and extensions.

For further information contact us at presse@uniscon.de

Learn more about cloud security and data protection on the Internet at www.privacyblog.de

uniscon — a company of the TÜV SÜD Group

uniscon GmbH is a company of the TÜV SÜD Group. As part of TÜV SÜD's digitalization strategy, uniscon offers high-security cloud applications and solutions for secure, legally compliant data traffic. TÜV SÜD is one of the world's leading technical service providers with over 150 years of industry-specific experience and more than 24,000 employees at around 1,000 locations in 54 countries. Within this strong network, uniscon can reliably implement large-scale international projects in the IoT and Industry 4.0 sectors with the Sealed Cloud and its products.

Further information on the company and its solutions at www.uniscon.com

Press contact

uniscon GmbH, Claudia Seidl
Ridlerstr. 57
80339 Munich (Germany)
email: presse@uniscon.de
Internet: www.uniscon.com
Phone: +49 (0)89 / 41 615 988 104

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

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