Pressemitteilung

IT-Sicherheit 8. Oktober 2020

Rückkehr ins Büro: TÜV SÜD gibt Tipps zur IT-Sicherheit

München. Das Arbeiten im Home-Office während der Corona-Pandemie hat die Angriffsfläche für Cyberkriminelle spürbar vergrößert. Doch auch der Wechsel vom Home-Office zurück ins Büro bringt einige Risiken für die IT-Sicherheit mit sich. Die Experten von TÜV SÜD Sec-IT geben einen Überblick zu den wichtigsten Regeln für die IT-Sicherheit.

„Grundsätzlich besteht die größte Gefahr darin, dass sich Mitarbeiter im Home-Office unbemerkt Schadsoftware eingefangen haben. Diese bringen sie dann am ersten Arbeitstag unabsichtlich mit ins Büro und somit in das Firmennetzwerk“, sagt Stefan Vollmer, CTO bei der TÜV SÜD Sec-IT GmbH. Falls Mitarbeiter ihre Firmenrechner zudem auch für private Zwecke nutzen, können z.B. durch externe Speichermedien oder unerlaubt installierte Software zusätzliche Sicherheitsrisiken entstehen.

Diese IT-Sicherheitscheckliste fasst die wichtigsten Punkte für die Rückkehr ins Büro zusammen:

- **Schrittweise Rückkehr:** Wenn alle Mitarbeiter gleichzeitig ins Büro wechseln, dann könnte das die IT-Abteilung überfordern. Ein handlungsunfähiges und überfordertes IT-Team aber birgt hohe Risiken, da im Ernstfall nicht schnell reagiert werden kann.
- **Inventarisierung:** Bei der Entscheidung, alle Mitarbeiter mit sofortiger Wirkung ins Home-Office zu schicken, blieb meist keine Zeit für ein geordnetes Vorgehen. Umso wichtiger ist es jetzt, dass Geräte, welche nun wieder in die Firma zurückgebracht werden, akribisch erfasst und inventarisiert werden. Damit ist man bei einem Zwischenfall in der Lage, sehr schnell Rückschlüsse auf den Ursprung zu ziehen.
- **Verpflichtender Passwortwechsel:** Bei der Rückkehr sollten alle Mitarbeiter dazu angehalten werden, die Passwörter ihrer Firmenzugänge und Hardware zu ändern. Es kann nicht ausgeschlossen werden, dass im Zuge eines Phishings die Zugangsdaten gestohlen wurden und somit nun ein Zugang zum Firmennetzwerk möglich ist.
- **Private IT-Geräte nicht erlauben:** Zuhause wird gerne private Hardware für Geschäftszwecke genutzt. Die Gefahr besteht, dass diese Hardware nun auch ins Büro gebracht wird, um weiter,

wie nun gewohnt, arbeiten zu können. Dies sollte im Zuge der zuvor angesprochenen Inventarisierung verhindert werden.

- **End Point Scan:** Falls eine phasenweise Rückführung der Mitarbeiter ins Büro möglich ist, sollte während und nach jeder Phase ein Scan der mitgebrachten Hardware durchgeführt werden. Dies dient nicht nur der Erkennung von Schadsoftware, sondern auch der Validierung und Inventarisierung von selbst installierter Software, welche nicht zuvor vom Unternehmen freigegeben wurde.
- **Patching:** Bei allen Geräten, die in das Firmennetz eingebracht werden, müssen sofort und zwingend alle Updates eingespielt werden, ohne die Möglichkeit, diese zu verschieben oder abzubrechen.

„Wenn Unternehmen diese Punkte beachten, können sie die mitgebrachten, möglicherweise schon tickenden Cyberbomben rechtzeitig entschärfen“, sagt Vollmer. „Letztlich stellt die aktuelle Situation auch eine Chance dar, die Belegschaft besser für Cyberrisiken zu sensibilisieren und ihr Verantwortungsgefühl beim Arbeiten im Home-Office zu stärken.

Mehr über die Leistungen der TÜV SÜD Sec-IT GmbH im Bereich IT-Sicherheit : https://www.tuvsud.com/de-de/dienstleistungen/cyber-security.

Pressekontakt:

Sabine Krömer TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 29 35 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail sabine.kroemer@tuvsud.com Internet www.tuvsud.com/de

Im Jahr 1866 als Dampfkesselrevisionsverein gegründet, ist TÜV SÜD heute ein weltweit tätiges Unternehmen. Mehr als 25.000 Mitarbeiter sorgen an über 1.000 Standorten in rund 50 Ländern für die Optimierung von Technik, Systemen und Know-how. Sie leisten einen wesentlichen Beitrag dazu, technische Innovationen wie Industrie 4.0, autonomes Fahren oder Erneuerbare Energien sicher und zuverlässig zu machen. www.tuvsud.com/de