© APA/dpa/Oliver Berg

Indirekt
Oft gelingt es Hackern, über die Infiltration von IT-Endgeräten von Mitarbeitern Zugriff auf berufliche Passwörter und Datenbankzugänge zu erlangen.

Haftungsrisiken von Cyberhacking

Eintrittswahrscheinlichkeit und Folgekosten von Cyberangriffen sind vielen noch nicht bewusst.

Gastbeitrag
••• *Von Martin Schiefer und Ralf Blaha*

WIEN. Cyberhacking ist in den letzten Jahren mehr und mehr in das Bewusstsein der Öffentlichkeit gedrungen. Vielen Geschäftsführungen von Unternehmen und öffentlichen Organisationen sind jedoch die Eintrittswahrscheinlichkeit und Folgekosten von Cyberangriffen nicht bewusst, weshalb sie für die Prävention nur geringe Ressourcen einsetzen.

Gerade das wirtschaftliche Risiko von Cyberhacking wird von vielen Unternehmern jedoch unterschätzt: In einer Studie bemisst das Ponemon Institute die durchschnittlichen Kosten eines „Data Breaches" im Jahr 2018 mit 3,86 Mio. USD und sieht die Wahrscheinlichkeit einer Wiederholung bei knapp 28%.

Durch die Einführung der DSGVO hat sich der Druck auf Unternehmen in ihrer Funktion als Datenverarbeiter dramatisch erhöht. Bei (mit)verschuldeten Datenlecks drohen nun nicht nur hohe Strafen, sondern kann die Datenschutzbehörde auch verfügen, dass die betroffene Datenverarbeitung nicht mehr fortgeführt werden darf – also die IT des betroffenen Unternehmens „abdrehen" ...

Oft ist es ganz einfach …
Direkte Angriffe auf die IT der Zielunternehmen stellen jedoch nicht den einzigen Ansatzpunkt von Internet-Kriminellen dar. Oft gelingt es Hackern, über die Infiltration von IT-Endgeräten von Mitarbeitern Zugriff auf berufliche Passwörter und Datenbankzugänge zu erlangen.

Anfällig für den Angriffsvektor bei der aktuellen Hackingwelle, bei der vorgebliche Mitarbeiter von Microsoft die User zum Installieren einer Fernwartungssoftware verleiten, sind laut Angaben von Microsoft zudem nicht nur ältere Menschen, sondern auch die Altersklasse zwischen 18 und 34 Jahren.

Fokus auf Sensibilisierung
Eine proaktive interne Datenschutzpolitik sollte daher die umfassende Sensibilisierung und Schulung der Mitarbeiter und Führungskräfte umfassen.

Gefordert ist eine ganzheitliche IT-Sicherheitsstrategie, die technische Maßnahmen, Schulungsmaßnahmen und auch rechtliche Maßnahmen umfasst. Übersehen wird nämlich oft, dass ein Datenleck nicht nur Daten des eigenen Unternehmens, sondern auch personenbezogene Daten sowie Geschäfts- und Betriebsgeheimnisse von Auftraggebern, Kunden und Kooperationspartnern exponieren kann. Ohne vertragliche Absicherung eröffnet dies enorme Haftungsrisiken gegenüber diesen Vertragspartnern, zumal die Judikatur zur Haftung bei Cyberhacking noch spärlich ist.

Als Spezialisten für Vergaberecht realisieren Martin Schiefer und sein Rechtsanwaltsteam ein Kanzleikonzept der Zukunft mit den Marken procureSEC, procureLAB und procureACT.

© Nik Pichler (2)

Martin Schiefer und Ralf Blaha, Schiefer Rechtsanwälte GmbH, Wien.