telekom +it Report

Ausgabe 06 | 2021

BERUFSBILDER IN DER IT

18

Die Initiative WOMENinICT holt weibliche Role Models vor den Vorhang und setzt auf den Austausch mit Frauen in der IT-Branche.

P. b. b. Verlagspostamt 1170 Wien, Vertriebskennzahl 02 Z030627M, Preis: EUR 4,–

Warum man die Lösegeldforderung nicht bezahlen sollte

Bei Ransomware-Attacken können Datenretter betroffenen Unternehmen mitunter wieder zu einem produktiven Zustand verhelfen. Die Erpresser werden so bei ihren kriminellen Machenschaften gestört.

Ein Kommentar Markus Häfele

»Zeit ist Geld. Das wissen beide Seiten.«

Markus Häfele
Geschäftsführer
Attingo Datenrettung

Als professionelle Datenretter erhalten wir regelmäßig Anfragen von Betroffenen, deren Produktivsysteme, Back-ups und Archive mit Ransomware verschlüsselt oder gelöscht wurden.

Die Täter werden zunehmend perfider in ihrem Vorgehen. Sie sind technisch versierter, organisierter und wissen meist, was sie tun. Ein Cyberangriff bedeutet oftmals, dass sich die Angreifer ausgiebig innerhalb der Daten umsehen und somit wissen, welche Daten wichtig sind und tunlichst nicht geleakt werden dürfen. Wenig verwunderlich also, dass die Erpresser genau hier ansetzen, um eine schnelle Zahlungsbereitschaft zu erzeugen.

Doch warum gehen Menschen auf die Forderungen der Erpresser ein? Immerhin begünstigt es die Motivation der Kriminellen, damit fortzufahren, da es sich als lukrativ erweist. Zudem bringt es weitere kriminelle Strukturen hervor, durch die sie sich über diesen »Geschäftszweig« bereichern wollen.

>> Abwägen von Kosten <<

Zeit ist Geld; das wissen beide Seiten. Jede Minute, in der Produktivsysteme, Produktionsanlagen oder landesweite Kassensysteme nicht mehr funktionieren, kann den Betroffenen Unsummen kosten. In solchen Momenten muss abgewogen werden. Was geht schneller, um alles wieder zum Laufen zu bekommen und Verluste möglichst gering zu halten: Das Einspielen gegebenenfalls noch vorhandener älterer Datenbestände? Eine professionelle Datenrettung – zum Beispiel durch Attingo? Oder die Entschlüsselung der Daten mit dem durch die Lösegeldzahlung erhaltenen Decryptor?

Um Folgsamkeit zu gewährleisten und die dritte Option zu forcieren, drohen Erpresser unter anderem mit dem Abbruch des Kontakts, der unwiederbringlichen Vernichtung aller Dateien oder gar deren Veröffentlichung. Die Täter wollen mit diesen Druckmitteln eine Alternativlosigkeit schaffen. In vielen Situationen funktioniert dies leider hervorragend. Bei einer derartigen Ausnahmesituation sind Stress, Panik und Verzweiflung die treibenden Kräfte und sorgen für Kurzschlussreaktionen. Das Eingehen auf die Lösegeldforderung muss aber mit allen Mitteln vermieden werden. Da man sonst das »Geschäft« ankurbelt und die Erpresser bei ihren kriminellen Machenschaften unterstützt.

Aus diesem Grund ist es elementar, jederzeit auf einen potenziellen Angriff vorbereitet zu sein und eine sichere sowie vom Netzwerk gelöste Offline-Back-up-Strategie für den Worst Case zu entwickeln. Denn selbst Online-Back-ups sind oft betroffen; aber auch hier gibt es Möglichkeiten. Wenn RAID-Server oder NAS-Systeme und virtuelle Laufwerke teilweise verschlüsselt, Daten gelöscht oder teilweise überschrieben wurden, sollte man nicht sofort das Handtuch werfen und das Lösegeld zahlen. Vorher sollte man Kontakt mit einem Spezialisten aufnehmen.

Bevor Sie das Handtuch werfen, sollten Sie Kontakt mit einem Spezialisten aufnehmen.

Je nach Umfang kann die Analyse eines befallenen Systems zwar einige Tage dauern und mehrere tausend Euro kosten. Einigen Opfern kann so jedoch zu einem ausreichend produktiven Zustand geholfen werden – zu weitaus geringeren Kosten als den horrenden Lösegeldforderungen. ■

Fotos: iStock, fotostudio-marion.at