CISOs CONNECT

in Zusammenarbeit mit

AimPoint Group | W2Communications

Ransomware im Fokus

CISOs kommen zu Wort

Im Bemühen, jenseits aller Schlagzeilen und Sensationsmeldungen die Faktenlage zu klären, befragte Zscaler im August 2021 über 250 Chief Information Security Officers (CISOs) zu ihren bisherigen Erfahrungen, aktuellen Befürchtungen und zukünftigen Plänen für einen zukünftigen Schutz vor Ransomware.

Keine Besserung in Sicht

Insgesamt		Mittelständische Unternehmen mit 1.000 bis 10.000 Mitarbeitern
53 %	Waren in den letzten 12 Monaten mindestens einmal von einem Ransomware-Angriff betroffen	66 %
69 %	Rechnen in den nächsten 12 Monaten mit mindestens einem Ransomware-Angriff	80 %

3 Branchen, die in den nächsten 12 Monaten am stärksten mit einem Ransomware-Angriff rechnen

Bauwesen und Maschinenbau | Einzelhandel und Gebrauchsgüter | Fertigung

Lösegeldkosten nur von nachrangiger Bedeutung

Am *stärksten beunruhigende* Ransomware-Auswirkungen

Nr. 1
Offenlegung sensibler oder geschützter Daten

Nr. 2
Kosten der Wiederherstellung des Normalbetriebs

Nr. 3
Verlorene Einnahmen aufgrund von Betriebsunterbrechungen

Am *wenigsten beunruhigende* Ransomware-Auswirkungen

Nr. 9
Verlust von Mitarbeiterproduktivität

Nr. 10
Kosten für die Zahlung des Lösegelds

Nr. 11
Kosten für regulatorische/ Compliance-Bußgelder

Ransomware-Roulette

55 % Die Zahlung des Lösegelds führte zur *VOLLSTÄNDIGEN* Wiederherstellung von Daten

34 % Die Zahlung des Lösegelds führte zur *TEILWEISEN* Wiederherstellung der Daten

11 % Die Zahlung des Lösegelds führte zu *KEINER* Wiederherstellung der Daten

Jedes 5. ..... Ransomware-Opfer erlitt Verluste über ..... >5 Mio. USD

Jedes 20. ..... Ransomware-Opfer erlitt Verluste über ..... >50 Mio. USD

Wehrhafte Sicherung

Effektivste technische Gegenmaßnahmen zur Abwehr von Ransomware-Angriffen

Datensicherung und Wiederherstellung

Endpoint Protection Platform (EPP)

E-Mail-Sicherheit (mit Phishing-Erkennung)

Sensibilisierung und Schulung der User

Wichtigste technische Gegenmaßnahmen, die in den nächsten 12 Monaten zum Schutz vor Ransomware geplant sind

User and Entity Behavior Analytics (UEBA)

Netzwerksegmentierung/ Zero-Trust-Zugriff

Data Loss/Leak Prevention (DLP)

Ein kleiner Hoffnungsschimmer?

Allem Anschein nach hat das mediale Interesse an erfolgreichen Ransomware-Angriffen zusammen mit ihrer finanziellen Tragweite dafür gesorgt, dass Cybersicherheit zunehmend zur Chefsache erklärt wird.

Bedeutendste **Hindernisse bei der Realisierung einer effektiven Ransomware-Abwehr**

Schwierigkeit der Implementierung von Tools/Technologien

Mangel an qualifiziertem Personal zur Implementierung von Lösungen

Andere konkurrierende Prioritäten

Weniger schwerwiegende **Hindernisse bei der Realisierung einer effektiven Ransomware-Abwehr**

Schwierigkeit der Rechtfertigung entsprechender Budgetanfragen

Mangelnde Unterstützung durch den Vorstand

Hier den vollständigen Report herunterladen >>>>

zscaler