Information Security World 2022

Mit Ransomware leben lernen

Welche Maßnahmen Unternehmen zur Gefahrenabwehr ergreifen können, zeigte die Information Security World.

Die Information Security World ist zurück. Nach dreijähriger Corona-Abstinenz veranstalteten NTT Data und die NTT Gruppe die Cybersecurity-Konferenz und -Messe wieder als Präsenzevent. In Neu-Isenburg bei Frankfurt am Main trafen sich CIOs, CISOs, IT-Security-Verantwortliche und IT-Manager und diskutierten über Strategien und konkrete Lösungen für alle Herausforderungen in der Cybersicherheit. Mit welchen Bedrohungen müssen Firmen in den kommenden Jahren rechnen, welche neuen Regularien sind zu erwarten und wie sieht ein ganzheitlicher Schutzschirm gegen immer individuellere und komplexere Angriffe aus?

Ein 100-prozentiger Schutz vor Ransomware sei eine Illusion, zugleich könne aber eine Kapitulation auch nicht der Weisheit letzter Schluss sein, so der Tenor auf der Veranstaltung. Die neue Arbeitswelt nach der Pandemie hat neue Bedrohungslagen geschaffen, die sich durch den Konflikt in der Ukraine noch einmal verschärft haben. Weil sich gleichzeitig die Digitalisierung in Gesellschaft und Wirtschaft rasant beschleunigt, stoßen etablierte Sicherheitskonzepte an ihre Grenzen – es braucht neue Strategien zum Schutz vor Angriffen.

Foto: NTT

Bernhard Kretschmer, VP Service and Cybersecurity NTT in Deutschland (li.), und Patrick Schraut, SVP Cybersecurity DACH NTT Data, auf der ISW

„Ransomware und Phishing gehören weltweit zu den größten Bedrohungen für die IT-Sicherheit. Etliche Unternehmen schützen sich dabei immer noch unzureichend. Die Konsequenz kann ein Komplettausfall des Betriebs sein", betonte Bernhard Kretschmer, Vice President Service and Cybersecurity NTT in Deutschland, im Vorfeld der ISW. Da Ransomware nicht verschwinden wird, sollte ein Umdenken erfolgen: Unternehmen müssen Security-Strategien und -Lösungen nutzen, die nicht nur auf die Vermeidung von Ransomware-Angriffen abzielen, sondern auch die Reaktion auf erfolgreiche Attacken adressieren. Nur so kann die Business Continuity gewährleistet werden. „Mit Ransomware-Attacken werden Unternehmen auch in der Zukunft leben müssen", fasste Patrick Schraut, Senior Vice President Cybersecurity DACH bei NTT Data, zusammen.

NTT Data
www.nttdata.com

Schadensbegrenzung Schritt für Schritt

Welche Maßnahmen helfen, die Gefahren in den Griff zu bekommen? NTT nannte auf der ISW vier Bereiche, in denen Unternehmen tätig werden sollten:

1. Minimierung der Angriffsfläche: *Dazu zählen etwa die Implementierung einer Identity and Access Management-Lösung (IAM) für die Verwaltung von Identitäten, eine Mehr-Faktor-Authentifizierung und die regelmäßige Installation von Updates und Patches. Daneben bieten sich zudem gezielte Penetrations- und Vulnerability-Tests an. Auch eine Netzwerksegmentierung ist sinnvoll, um die Angriffsfläche möglichst gering zu halten. Nicht zuletzt ist auch die Sensibilisierung der Mitarbeiter Teil einer umfassenden Sicherheitsstrategie.*

2. Frühzeitige Angriffserkennung: *Eine klassische Maßnahme für die Angriffserkennung ist die Analyse von Log-Files. Hilfreich sind dabei SIEM (Security Information and Event Management)-Systeme, die einen ganzheitlichen Blick auf die IT-Sicherheit bieten. Wer noch einen Schritt weiter gehen will, nutzt auch eine Deception-Lösung. Diese leitet potenzielle Angreifer in die Irre und in eine überwachte Umgebung.*

3. Schnelle Reaktion: *Jedes Unternehmen sollte eine Incident-Response-Strategie etablieren, die konkrete Maßnahmen bei Sicherheitsvorfällen umfasst. Dazu gehören zum Beispiel die Festlegung von Verantwortlichkeiten, die Definition von Aufgaben, die Klassifizierung von Schadensfällen oder erforderliche Kommunikationsprozesse im Hinblick auf Strafverfolgungsbehörden – auch unter Beachtung etwaiger Meldepflichten.*

4. Optimierung der Infrastruktur: *Nach jedem Ransomware-Angriff muss die gesamte Infrastruktur auf den Prüfstand gestellt werden. Nur ausgehend von einer detaillierten forensischen Analyse des Angriffsszenarios können konkrete Abwehrmaßnahmen ergriffen werden, die eine Wiederholung verhindern.*