Was wirklich gegen Ransomware hilft

Nach einer aktuellen Studie von Sophos sind 60 Prozent der Schweizer Unternehmen im vergangenen Jahr Opfer von Ransomware geworden. Wie man sich vor Ransomware schützen kann und welche letzte Verteidigungslinie wirklich hilft, erklärt Wolfgang Huber, Regional Director DACH, beim Data Management-Spezialisten Cohesity.

Herr Huber, wie gross ist die Gefahr durch Ransomware wirklich?
Weltweit wird alle elf Sekunden ein Unternehmen von Ransomware befallen. Dabei steigen die Angriffe zunehmend in Bezug auf Häufigkeit und Raffinesse. Auch in der Schweiz wurden bereits in diesem Jahr zahlreiche Fälle bekannt, unter anderem beim Logistikkonzern M+R Spedag, der Zeitungspapierfabrik CPH-Gruppe, der Stadtverwaltung von Yverdon-les-Bains oder dem Internationalen Roten Kreuz in Genf. Daher müssen sich heute Unternehmen aller Branchen vor Ransomware schützen.

Sind die Angreifer besser oder die Verteidigung schlechter geworden?
Beides, einmal sind viele Unternehmen anfälliger geworden, weil ihre Daten auf immer mehr Orte im Rechenzentrum, in der Cloud und am Edge verteilt sind und sich so die Angriffsfläche vergrössert. Firmen wollen diese isolierten Daten mit mehreren Legacy-Produkten schützen, die untereinander kaum interagieren. Das erhöht die Komplexität weiter, reisst Sicherheitslücken, durch die Hacker leichter eindringen können. Gleichzeitig hat sich das Geschäft mit Ransomware weiter professionalisiert und dank as-a-Service-Konzepten kann jeder in das kriminelle Geschäft einsteigen.

Welche Security-Ansätze schützen davor?
Unternehmen benötigen heute einen umfassenden Ansatz zum Schutz ihrer Daten, der im Idealfall alle Systeme und Speicherorte abdeckt – on-premises und in der Cloud. Das Next-Gen-Data-Management von Cohesity bricht diese Datensilos auf und führt die heterogenen Datenquellen zusammen. Es schützt diese Daten, indem sie als unveränderliche Backup-Snapshots abgelegt werden und setzt künstliche Intelligenz ein, um die abgelegten Backups zu beobachten und Symptome für Angriffe aufzuspüren. Bei Alarmen können die Firmen sofort automatisierte Abwehrmassnahmen einleiten. Die Workloads und Applikationen selbst lassen sich ebenfalls automatisch und schnell wiederherstellen.

Ist das nicht alles sehr kompliziert?
Überhaupt nicht, die Plattform von Cohesity lässt sich mit einer einzigen Konsole verwalten. Zudem stehen bereits viele Funktionen als as-a-Service bereit wie Backup oder Disaster Recovery. Unternehmen können absolut frei wählen, ob sie die Lösungen selbst im Rechenzentrum oder in der Cloud betreiben, einen unserer Partner für diese Aufgabe einspannen oder den entsprechenden Dienst nutzen, der von Cohesity selbst betrieben wird. Ein Unternehmen kann all diese Betriebsmodi beliebig mischen und jederzeit auf ein anderes Modell umsteigen.

Warum scheitern so viele Firmen daran, Ransomware-Attacken aufzuhalten?
Entscheidend ist, wie schnell IT-Teams Attacken erkennen und Gegenmassnahmen einleiten. Jede Verzögerung kann zu längeren Ausfallzeiten und höheren Datenverlusten führen. Daher arbeitet Cohesity mit führenden Anbietern wie Palo Alto Networks zusammen und vernetzt die Plattformen untereinander. Sobald unsere KI-basierte Helios-Plattform Anomalien in den Backup-Daten entdeckt, die auf einen Angriff hindeuten, leitet sie den Alarm an die Plattform Cortex XSOAR von Palo Alto Networks weiter.

Mit welchen weiteren Anbietern kooperieren Sie?
Wir bieten zum Beispiel auch Integrationen mit Cisco SecureX, Entrust, Fortanix oder Parablu. Die Lösungen sind über unseren Marketplace erhältlich, der ständig erweitert wird. Das gemeinsame Ziel mit unseren Partnern ist es, die Abwehr von Gefahren über KI-basierte Automatisierungen und die Priorisierung von Warnmeldungen zu erleichtern. Die Sicherheitsanalysten werden so rechtzeitig und detailliert über mögliche Gefahren informiert und können selbst schnell bestimmen, wie sie am besten auf den Vorfall reagieren müssen.

Wie lässt sich ein externes Backup nutzen?
Wir bieten mit Cohesity FortKnox eine Software-as-a-Service-Lösung zur Datenisolierung und -wiederherstellung. Diese zusätzliche Ebene des Offsite-Schutzes bildet sozusagen die letzte Verteidigungslinie, wenn alle anderen Massnahmen fehlschlagen. Die Daten sind dank eines Virtual Air Gap vor unbefugtem Zugriff geschützt und lassen sich aus dem von Cohesity verwalteten Cloud-Tresor an die ursprüngliche Source Location oder alternative Ziele zurückspielen. ■

COHESITY

Cohesity Inc.
300 Park Avenue, Suite 1700, 95110 San José, CA, USA
✆ +41 (0)77 965 69 79
swisscontact@cohesity.com, www.cohesity.com/de