

MTI Technology bietet Schutzkonzepte auf Speicherebene gegen Ransomware-Attacken

Backup und Recovery als entscheidender Teil der Cybersecurity-Strategie

Wiesbaden, 16. März 2021 – Das bundesweit tätige IT-Systemhaus MTI Technology bietet ab sofort unter dem Schlagwort „Cyber Recovery“ spezielle Schutzkonzepte gegen Cyberangriffe auf Backup-Systeme. Gemeinsam mit seinen Technologiepartnern Dell Technologies und Quantum schützt MTI unternehmenskritische Daten mit bedarfsgerechten Lösungen, die wahlweise Tape-, Disk- als auch Cloud-basiert arbeiten. Damit haben Kunden die Gewissheit, dass auch bei einer erfolgreichen Cyberattacke auf valide Backup-Daten zurückgegriffen werden kann. Komplette Datenverluste, langwierige Ausfälle im Geschäftsbetrieb oder hohe Lösegeldforderungen sind damit weitestgehend ausgeschlossen.

1/4

Backup-Daten schützen und Bedrohungen identifizieren

Wesentliche Bestandteile der MTI Cyber-Recovery-Lösungen sind Komponenten in der Backup-Infrastruktur, welche die Daten entweder aus dem regulären Datenstrom im Netzwerk isolieren oder die Daten mit einer zusätzlichen Schicht vor einem unautorisierten Zugriff schützen. Zum Einsatz kommen Lösungen wie zum Beispiel der Quantum ActiveVault Tresor oder das Backup-2-Disk-System Data Domain von Dell Technologies. Zusätzlich helfen erprobte Technologien wie WORM (Write Once Read Many), eine Unveränderbarkeit der Backupdaten zu garantieren. Optional bietet MTI in Verbindung mit CyberSense von Index Engines eine Analyseplattform für die



zusätzliche Erkennung manipulierter Backupdaten. Die Software identifiziert Bedrohungen, diagnostiziert Angriffsvektoren mittels maschinellen Lernens und schützt so geschäftskritische Daten.

Nach individueller Anforderung des Kunden und je nach bereits vorhandener Infrastruktur stellt MTI Technology die optimalen Komponenten zusammen, um Unternehmen und Organisationen vor den Folgen einer Cyberattacke zu schützen. Der MTI Beratungsservice baut auf einen Workshop mit dem Kunden auf und ergänzt diesen durch die Entwicklung einer Cyber-Recovery-Strategie. Der aktuelle und gewünschte Sicherheitszustand des Kunden wird analysiert, um eine maßgeschneiderte Strategie für die Cyber-Recovery-Bereitschaft zu erstellen.

Die Gefahrenlage nimmt weiter zu

Laut den Analysten von Cybersecurity Ventures summierten sich die Schäden in Deutschland für Ausfall, Diebstahl, Schädigung der Produktionsabläufe oder die Erpressung mit gestohlenen oder verschlüsselten Daten bereits im Jahr 2019 auf rund 37,5 Milliarden Euro. Experten schätzen die Schadensbilanz für 2020 auf einem noch deutlich höheren Niveau. Insbesondere im Zusammenhang mit der Corona-Pandemie wurde ein zusätzlicher Anstieg von Ransomware-Attacken und Phishing-Angriffen beobachtet. Hacker werden aggressiver und greifen gezielt unternehmenskritische Systeme an, um die betroffenen Organisationen zur Zahlung hoher Lösegelder für die Entschlüsselung ihrer Daten zu nötigen. Betroffen sind nicht nur Unternehmen, sondern auch Behörden, Schulen, Krankenhäuser und Universitäten. In jüngster Zeit sind zudem Energie- und Wasserversorger immer öfter Opfer von Cyberattacken. Der Schaden reicht

2/4



vom Blockieren des Zugriffs von Benutzern auf benötigte Ressourcen bis hin zur Androhung von Offenlegung oder Vernichtung sensibler Unternehmensdaten.

„Das Backup ist eines der wichtigsten Elemente, um Unternehmen zuverlässig vor den Folgen einer Ransomware-Attacke zu schützen. Unternehmen müssen ihre Daten dort verteidigen, wo sie aufbewahrt werden: auf der Speicherebene“, erklärt Michael Babylon, Geschäftsführer der MTI Technology GmbH. „Ein einfaches Backup-System als Sicherungskopie reicht hier nicht mehr aus. Hackern ist bewusst, dass sie neben der Produktivdaten auch die Backup-Systeme ins Visier nehmen müssen, um den Wirkungsgrad ihres Angriffs zu maximieren. Damit Backups wirkungsvoll sind, müssen also die Kopien unveränderbar und vor der Verschlüsselung durch Ransomware geschützt sein. Unsere Konzepte sehen vor, unternehmenskritische Daten stärker abzusichern als andere Daten. Darüber hinaus gilt es, den Fokus auch auf die Prozesse der Wiederherstellung zu legen, um Unternehmen und Organisationen die schnelle Wiederaufnahme des Geschäftsbetriebs zu ermöglichen“, ergänzt Babylon.

3/4

Oster-Special für Backup Ransomware-Schutz

Damit in Zeiten einer hohen Gefahrenlage der Ransomware-Schutz für überlebenswichtige Backups rasch umgesetzt werden kann, hat MTI Technology zwei Oster-Aktionsangebote geschnürt. Die Specials, wahlweise mit EMC Data Domain oder mit Quantum Scalar i3 inklusive Active Vault, laufen bis zum 30. April 2021. Details zu den Specials sind zu finden auf: de.mti.com/specials.





Bild: Zum Schutz vor Ransomware-Attacken bietet MTI verschiedene Lösungen zur Speicherung unternehmenskritischer Daten in einem digitalen Datentresor [Copyright iStock / Petrovich9]

4/4

Über MTI Technology:

Das bundesweit tätige IT-Systemhaus MTI Technology GmbH (<http://de.mti.com>) ist seit über 30 Jahren auf Datacenter-Infrastrukturen, Cloud Solutions, Security und Managed Services spezialisiert. Mehr als 1.800 Kunden vertrauen auf die Expertise von MTI zur Speicherung, zum Schutz und zur Sicherung von Daten. Unternehmen aller Branchen profitieren von umfangreichen Full-Service-Konzepten und -Lösungen rund um das Rechenzentrum sowie verwandter IT-Prozesse. Dank enger Partnerschaften mit marktführenden Herstellern, wie u.a. Dell, Huawei, Quantum und SEP, bietet MTI ein Portfolio zukunftsicherer Technologien und verfügt über exzellentes Know-how. Mit seinen umfassend zertifizierten Servicemitarbeitern bietet MTI einen 24/7-Business-Support und IT-Services zu allen aktuell verfügbaren Technologien und Lösungen.

Pressekontakt:

MTI Technology GmbH
Uli Schunk
Telefon: +49 6122 995 155
uschunk@mti.com

Chris Cross Relations
Christine Vogl-Kordick
Telefon: +49 89 38 15 66 00
christinevk@chriscrossrelations.de