

– Presseinformation der Controlware GmbH –

Erpressungstrojanern keine Chance geben – Controlware unterstützt mit individuellen Security-Lösungen

Dietzenbach, 27. Oktober 2021 – Ransomware zählt zu den häufigsten Cyberbedrohungen, mit denen Unternehmen jederzeit rechnen müssen. Die Security-Experten von Controlware helfen dabei, Netzwerke gegen Erpressersoftware zu schützen.

Statt dem Startbildschirm grinst dem User ein Totenkopf entgegen. Oder ein Erpresserbrief klärt ihn auf, was passiert ist: Cyberkriminelle haben Daten auf dem Computer oder im Netzwerk so codiert, dass sie für den Nutzer unbrauchbar sind. Den Entschlüsselungsschlüssel liefern die Erpresser erst, wenn sie ihr Lösegeld kassiert haben. Ransomware-Attacken können Unternehmen Millionen kosten. Laut des „2021 Unit 42 Ransomware Threat Report“ von UNIT 42 stieg das im Durchschnitt bezahlte Lösegeld von 94.137 Euro im Jahr 2019 auf 255.527 Euro in 2020 – also um 171 Prozent. Das höchste gezahlte Lösegeld belief sich 2020 auf 8,18 Millionen Euro.

„Vor allem die Zunahme von Homeoffice in Pandemie-Zeiten und die stetig steigende Zahl der Cloud-Anwendungen haben das Risiko, Opfer von Cybererpressern zu werden, erhöht“, sagt Angelika Stiehl, Senior Business Development Manager Application Delivery bei Controlware. Die Verbreitung neuer Ransomware-Varianten und Ransomware-as-a-Service-Lösungen lassen laut Angelika Stiehl zudem vermuten, dass Cybererpressungen künftig weiter zunehmen. Sie rät: „Unternehmen sollten ihre Mitarbeiter frühzeitig für Themen wie Phishing sensibilisieren und den Zugriff auf Daten und Dateien über Administratorrechte und Zugriffsmanagement sichern. Außerdem ist es sinnvoll, Daten regelmäßig zu speichern und Sicherheitslücken so schnell wie möglich auffindig zu machen und zu schließen.“ Denn hohe Lösegeldzahlungen lassen sich vermeiden – mit der richtigen Strategie und der passgenauen Sicherheitslösung.

Backups und Air Gap gegen Malware-Attacken

Wichtig zu wissen: Nicht immer reichen bestehende IT-Security-Lösungen aus, um Ransomware-Angriffe zu verhindern. Vor allem Backups werden häufig das Ziel von Cyberattacken – und sollten am besten regelmäßig offline gespeichert werden, um Daten nach einem Hackerangriff wiederherstellen zu können. Denn erst eine zweite Backup-Ebene oder eine Air Gap-Lösung, die Rech-



ner untereinander und von Netzwerken isoliert, schützt die Unternehmensdaten vor der vollständigen Zerstörung durch Cyberkriminelle. Darüber hinaus kann beispielsweise ein unveränderbares Filesystem gegen Angriffe verteidigen: Es kontrolliert die Prüfsummen von Files und löst bei Abweichungen durch einen Cyberangriff Alarm aus.

Entsprechend ausgelegte Speichermedien bieten darüber hinaus besonderen Schutz gegen Ransomware. „Primär- oder Plattenspeicher etwa sind mit Features ausgestattet, um Malware abzuwehren“, so Angelika Stiehl „zudem schützen Lösungen wie SafeMode-Snapshots Backup-Daten und -Metadaten, indem sie eine sichere Kopie erstellen, die Ransomware nicht löschen, ändern oder verschlüsseln kann. Auch einbruchssichere Backup-Architekturen lassen sich nicht verschlüsseln oder löschen. Sie ermöglichen es Unternehmen, den letzten Zustand ihres Netzwerks wiederherzustellen und liefern zusätzliche Informationen über den Cyberangriff.“

Als Systemintegrator und Managed Service Provider unterstützt Controlware Data Center und Unternehmen dabei, ihre IT-Security vor Ransomware-Attacken zu schützen. Gemeinsam mit den Kunden entwickeln die Controlware Experten passgenaue Lösungen, die Erpressungstrojaner zuverlässig abwehren und Daten sichern. So können Unternehmen möglichen Lösegeldforderungen gelassen entgegentreten.

Über Controlware GmbH

Die Controlware GmbH, Dietzenbach, ist mit mehr als 800 Mitarbeitern und einem Umsatz von ca. 330 Mio. Euro einer der führenden unabhängigen Systemintegratoren und Managed Service Provider in Deutschland. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden. Das Portfolio erstreckt sich von der Beratung und Planung über Installation und Wartung bis hin zu Management, Überwachung und Betrieb von Kundeninfrastrukturen durch das firmeneigene ISO 27001-zertifizierte Customer Service Center. Zentrale Geschäftsfelder der Controlware sind die Bereiche Network Solutions, Collaboration, Information Security, Application Delivery, Data Center & Cloud sowie IT-Management. Controlware arbeitet eng mit national und international führenden Herstellern zusammen und verfügt bei den meisten dieser Partner über den höchsten Zertifizierungsgrad. Das Unternehmen unterhält ein flächendeckendes Vertriebs- und



Servicenetzt mit 16 Standorten in DACH. Im Bereich der Nachwuchsförderung kooperiert Controlware mit renommierten deutschen Hochschulen und betreut durchgehend um die 50 Auszubildende und Studenten. Zu den Unternehmen der Controlware Gruppe zählen die Controlware GmbH, die ExperTeach GmbH, die Networkers AG und die productware GmbH.

Pressekontakt:

Stefanie Zender

Controlware GmbH

Tel.: +49 6074 858-246

Fax: +49 6074 858-220

E-Mail: stefanie.zender@controlware.de

www.controlware.de (Homepage)

Juliane Heermeier

fischerAppelt, relations GmbH

Tel.: +49 89 74 74 66 338

E-Mail: controlware@fischerappelt.de

