– Presseinformation der Controlware GmbH –

Proaktives Threat Hunting gegen Cyberangriffe – mit den Managed Services von Controlware

Dietzenbach, 08. Juni 2021 – Ob Computer-Sabotage oder Malware: Unternehmen jeder Branche und Größe müssen damit rechnen, Opfer eines Cyberangriffs zu werden. Proaktives Threat Hunting sorgt dafür, dass Cyberkriminelle schneller aufgespürt werden. Die passende Lösung bieten die Managed Services von Controlware.

Fast täglich berichten Medien über neue IT-Sicherheitsvorfälle in Unternehmen – von der Spionage bis zum Datendiebstahl. Firmen sollten sich daher mit dem Gedanken vertraut machen, selbst Opfer einer Cyberattacke zu werden – oder bereits zu sein. Benjamin Heyder, Cyber Defense-Experte bei Controlware verdeutlicht: „Je eher erkannt wird, dass ein Cyberangriff auf das Unternehmensnetzwerk stattgefunden hat, desto eher können größere Schäden verhindert werden." Entscheidend ist in diesem Zusammenhang die Dwell Time: die Zeitspanne zwischen dem Beginn eines Angriffs bis zu seiner Erkennung. Nach Angaben des Berichts „M-Trends 2020" von FireEye lag sie weltweit bei durchschnittlich 56 Tagen. „Automatisierte Erkennung muss durch weitere, proaktive Ansätze ergänzt werden, um diesen Wert zu senken", so Benjamin Heyder.

Einer dieser Ansätze ist proaktives Threat Hunting: Mithilfe dieser Methode lassen sich Angreifer identifizieren, die bereits im Netz unterwegs sind und nicht von vorhandenen Detektionsmechanismen erkannt wurden. In den Fokus genommen werden dabei spezifische Taktiken und Vorgehensweisen von Angreifern, die sogenannten TTPs (Tools, Techniques, Procedures). Nicht einzelne Merkmale, sondern eine Kombination aus verschiedenen Indikatoren ist hier der Schlüssel, um die Auffälligkeiten zu erkennen, erläutert Benjamin Heyder. „Die besondere Herausforderung besteht darin, dass diese Informationen an verschiedenen Orten erzeugt und sichtbar werden."

Telemetriedaten als Basis für spätere Analysen

Um einen Threat Hunting-Plan zu entwickeln, ist laut Benjamin Heyder ein tiefes Verständnis der wichtigen Angreifer-TTPs unverzichtbar. Dabei hilft das MITRE ATT&CK Framework: Die Wissensdatenbank aktueller „Real-world"-Angreifertechniken und -taktiken dient der Entwicklung

Sitz: Controlware GmbH Kommunikationssysteme ▪ Waldstraße 92 ▪ 63128 Dietzenbach ▪ GERMANY
Tel. +49 6074 858-00 ▪ Fax +49 6074 858-108 ▪ info@controlware.de ▪ www.controlware.de
Registergericht Offenbach a.M. ▪ HRB Nr. 6431 ▪ USt-IdNr. DE 113 539 225 ▪ Steuernummer 3523035235
Geschäftsführer: Bernd Schwefing, Oliver Thome

von Threat Hunting-Plänen und -Hypothesen. Unterstützt wird Threat Hunting außerdem von verschiedenen Technologiebausteinen in der Sicherheitsarchitektur. Dazu gehört Endpoint Detection and Response (EDR) – eine Technologie, die Endpunkte dauerhaft auf cyberkriminelles Verhalten überwacht. Neben Schutzfunktionen – zum Beispiel der Isolation eines infizierten Clients vom Netzwerk oder der Abschaltung verdächtiger Prozesse – gibt es zudem immer mehr Lösungen, die Telemetriedaten wie Netzwerkzugriffe als Basis für spätere Analysen kontinuierlich speichern.

Auch Cross-Layered Detection and Response (XDR)-Technologien können die Dwell Time verkürzen: XDR erweitert die Sichtbarkeit über einzelne Schichten wie Endpunkt und Netzwerk hinweg, indem es wichtige Metadaten wie E-Mails oder Cloud Workloads erfasst und korreliert. Dank automatischer Analysen dieser Daten werden Cyberbedrohungen früher entdeckt und abgewendet. „EDR und XDR sind neben SIEM-Systemen Technologiebausteine, die Threat Hunting effektiv unterstützen“, erklärt Benjamin Heyder, „aber letztlich ist es der Mensch, der Threat Hunting ausführt und weiterentwickelt.“

Cyber Defense-Technologien und Expertenwissen verzahnen

Wichtig für ein erfolgreiches Threat Hunting ist also das Zusammenspiel von technischen Lösungen und Expertenwissen. Anbieter wie der Systemintegrator und Managed Service Provider Controlware stehen Unternehmen dabei zur Seite – von der Beratung über die Umsetzung bis zum Betrieb der Threat Hunting-Lösung. Das Controlware Portfolio umfasst unter anderem individuelle Cyber Defense Services mit EDR- und XDR-Lösungen inklusive Threat Hunting als Managed Services. Benjamin Heyder: „Unsere Experten verfügen nicht nur über das technische Know-how, sondern profitieren auch von langjährigen Erfahrungen in unterschiedlichen Branchen. So können sie passgenau auf individuelle Kundenbedürfnisse eingehen.“

Sitz: Controlware GmbH Kommunikationssysteme ▪ Waldstraße 92 ▪ 63128 Dietzenbach ▪ GERMANY
Tel. +49 6074 858-00 ▪ Fax +49 6074 858-108 ▪ info@controlware.de ▪ www.controlware.de
Registergericht Offenbach a.M. ▪ HRB Nr. 6431 ▪ USt-IdNr. DE 113 539 225 ▪ Steuernummer 3523035235
Geschäftsführer: Bernd Schwefing, Oliver Thome

Über Controlware GmbH

Die Controlware GmbH, Dietzenbach, ist 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 rund 840 Mitarbeiter starke Unternehmen unterhält ein flächendeckendes Vertriebs- und Servicenetz 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)

fischerAppelt
Robert Schwarzenböck, Raphaela Sailer
Tel.: +49-89-747466-218
E-Mail: controlware@fischerappelt.de

Sitz: Controlware GmbH Kommunikationssysteme ▪ Waldstraße 92 ▪ 63128 Dietzenbach ▪ GERMANY
Tel. +49 6074 858-00 ▪ Fax +49 6074 858-108 ▪ info@controlware.de ▪ www.controlware.de
Registergericht Offenbach a.M. ▪ HRB Nr. 6431 ▪ USt-IdNr. DE 113 539 225 ▪ Steuernummer 3523035235
Geschäftsführer: Bernd Schwefing, Oliver Thome

Klassifizierung: ÖFFENTLICH