– Presseinformation der Controlware GmbH –

Umfassende Erkennung von Cyber-Gefahren durch Managed SIEM Services von Controlware

Dietzenbach, 07. Juli 2020 – Viele Unternehmen setzen zur Abwehr von Cyber-Gefahren auf Security Information & Event Management (SIEM)-Lösungen. Basis für die Erkennung sind dabei „Use Cases“, also vorab definierte Ereignisse, die mit einer kontinuierlichen Suche erkannt werden und nach definierten Regeln einen Alarm auslösen. Controlware erweitert diesen Ansatz um Cyber Use Cases – basierend auf dem MITRE ATT&CK™-Modell, womit sich die Aufdeckungsraten erheblich erhöhen lassen.

Die Einrichtung und der Betrieb von SIEM-Lösungen setzt tiefes Fachwissen und Erfahrung bei der Erkennung von Cyber-Gefahren voraus – und zwar bei der Formulierung ebenso wie bei der Implementierung der Erkennungsmechanismen. Denn zur Erkennung von Ereignissen, also Security-relevanten Vorfällen, verwenden diese Systeme üblicherweise sogenannte Use Cases. Durch den Use Case-Ansatz ist es möglich, sehr schnell aus der großen Anzahl täglicher Events potenzielle sicherheitsrelevante Vorfälle herauszufiltern. Der Systemintegrator und Managed Service Provider Controlware hat diesen Ansatz weiterentwickelt und kann so weitaus mehr Cyber-Gefahren erkennen und Attacken erfolgreich stoppen oder verhindern. Denn: In der Praxis beschränken sich die Use Cases der gängigen SIEM-Lösungen meist auf Compliance-getriebene Use Cases. Darunter sind Basis Use Cases zu verstehen, die Verstöße gegen Compliance-Richtlinien erkennen oder Auffälligkeiten in System-Protokollierungen bzw. Logdaten feststellen, die eventuell auf Security Incidents hindeuten. Diese Use Cases stellen eine Basisüberwachung sicher, eignen sich jedoch nicht zur vollständigen Erkennung „echter“ Cyber-Gefahren und Attacken.

Controlware hat deshalb seinen Use Case-Katalog um Cyber Security Use Cases auf Basis des MITRE ATT&CK™-Modells erweitert. Bei diesen Use Cases liegt der Fokus auf der Erkennung von Cyber-Gefahren bzw. Cyber-Angriffen. Hier wird versucht, die typischen Angreifer-Techniken in den unterschiedlichen Phasen eines Cyber-Angriffs über die Auswertung der entsprechenden Logdaten zu erkennen. Diese sind erheblich komplexer als Basis Use Cases und erfordern bei der Formulierung ein sehr profundes Verständnis der Techniken und Vorgehensweisen von Angreifern sowie Erfahrung bei der individuellen Anpassung an die

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 (CEO) Bernd Schwefing

Kundenumgebung. Zudem sind erweiterte Logquellen wie Sysmon- oder Powershell-Logs erforderlich.

Die Controlware Cyber Use Cases können als wirtschaftliche Alternative zu Systemen zur Anomalie-Erkennung eingesetzt werden, die auf Untersuchungen des Netzwerkdatenverkehrs oder des Benutzerverhaltes zurückgreifen. Diese Systeme bieten zwar eine hohe Erkennungsrate, sind jedoch aufgrund der dazu benötigten leistungsstarken Sensorik und Datenverarbeitung sowie der KI-Technologie meist erheblich kostenintensiver.

Zwar ersetzen auch die Controlware Cyber Use Cases nicht die anschließende manuelle Bewertung der erkannten Vorfälle durch ausgebildete Security-Analysten, sie sind jedoch eine wesentliche Grundlage für den wirtschaftlichen Betrieb eines Security Operations Centers: Die Qualität der Ergebnisse hat einen erheblichen Einfluss darauf, wie viele Events manuell überprüft werden müssen und wie oft es zu falschem Alarm kommt.

Darüber hinaus lassen sich die Managed SIEM Services mit weiteren Cyber Defense-Modulen – beispielsweise Vulnerability Management oder Advanced Threat Detection – je nach Bedarf kombinieren. Installation, Konfiguration und Betrieb aller Module und des Security Operations Centers übernimmt Controlware als Service Provider. Zudem ist ein Service Provider in der Lage, zusätzlich auf Erkenntnisse aus anderen Kundenumgebungen zuzugreifen – im Gegensatz zu den hauseigenen IT-Spezialisten der Unternehmen. So kann Controlware erstens schneller auf Vorfälle reagieren und zweitens Maßnahmen vorschlagen, die sich in anderen Security-Vorfällen als sinnvoll erwiesen haben. Damit werden Schäden bereits verhindert, ehe sie eintreten.

(4.028 Zeichen inkl. Leerzeichen)

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

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 (CEO) Bernd Schwefing

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.: +49-89-747466-23
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 (CEO) Bernd Schwefing

Klassifizierung: ÖFFENTLICH