Presseinformation

16. November 2017 – Unternehmensmeldung

Pressesprecherin:
Petra Sauer-Wolfgramm

Telefon: 04 31 / 39 93 - 525
Telefax: 04 31 / 39 93 - 999
E-Mail: sauer-wolfgramm@consist.de

Sicherheitsinformations- und Ereignismanagement: Kosten- und Nutzenaspekte

Ist IT-Security ohne ein SIEM noch zeitgemäß?

IT-Sicherheit ist ein Muss, das ist allen Unternehmen klar. Jetzt ist nur die Frage, wie gelangt man zu einem geeigneten Sicherheitsniveau? Was ist zuviel, was ist zu wenig?

Kiel – Sicherheitsinformations- und Ereignismanagement (SIEM) - Systeme werden im Kontext einer Sicherheitsstrategie oft genannt. Beim SIEM-Workshop der Consist Software Solutions GmbH auf der diesjährigen Rethink! Security in Hamburg kamen auch Fragen auf zur Sinnhaftigkeit eines SIEM und ab wann sich dessen Einsatz für ein Unternehmen lohnt.

Braucht jedes Unternehmen ein SIEM?

IT-Security wird immer gerne an technischen Komponenten fest gemacht: Firewalls, Intrusion Detection, Schwachstellen-Scanner, Virenscanner, Anti-Viren-Software und Web-Filter. In Sicherheitskonzepte müssen aber immer auch Prozesse und Mitarbeiter einbezogen werden, damit sie funktionieren. Ohne Zweifel lässt sich mit einem SIEM eine hohe Transparenz über die Aktivitäten auf den genutzten Systemen herstellen. Man erkennt auf einen Blick, wo sicherheitskritische Aktivitäten ablaufen, kann diese nachverfolgen, die Bearbeitung dokumentieren und über die aktuelle Lage berichten: bei heutigen komplexen Systemumgebungen eine große Hilfe. Für Unternehmen stellt sich in diesem Kontext die Frage: „Brauche ich ein SIEM und wenn ja, in welcher Form?“

Consist Software Solutions GmbH
A Consist World Group Company

Falklandstraße 1-3, 24159 Kiel
Postfach 93 28, 24152 Kiel

Pressekontakt:
Petra Sauer-Wolfgramm

Telefon: 04 31 / 39 93 - 525
Telefax: 04 31 / 39 93 - 999
E-Mail: sauer-wolfgramm@consist.de
Internet: www.consist.de/presse

Sitz der Gesellschaft: Kiel
HRB Kiel Nr. 3983

Geschäftsführung:
Daniel Ries
Martin Lochte-Holtgreven

Bedrohung

Das hängt von der Bedrohungssituation und den Nachweisverpflichtungen aus gesetzlichen Regelungen ab. Nahezu 100% aller Angriffe erfolgen mit gültigen Zugangsdaten. Durchschnittlich sind 40 IT-Systeme betroffen. Noch erstaunlicher ist, dass Angriffe im Mittel erst nach mehr als 200 Tagen entdeckt werden und der Hinweis auf Kompromittierungen bei 67 % aller Fälle durch Dritte erfolgt. Eine permanente Überwachung von Systemzugriffen und Datenströmen der eigenen IT ist ein Schlüsselfaktor, um Angriffe, oder das Fehlverhalten von Usern (Insider Threats) schnell entdecken und handeln zu können.

Vereinfachung

Bis zu einem gewissen Grad lässt sich solch eine Überwachung durch ein zentrales Log- und Berechtigungsmanagement abbilden. Bei größeren Systemlandschaften sollte man sich jedoch fragen, ob automatisierte Abläufe nicht kostensparender sind, da manuelle Prüfungen reduziert werden können. Wird ein SIEM eingesetzt, muss sich die IT-Sicherheit nur noch um Verdachtsfälle (Incidents) kümmern und kann diese im SIEM sowohl untersuchen als auch bearbeiten.

Gesetzeskonformität

Gesetzliche Regelungen können eventuell ohne ein SIEM nicht erfüllt werden. Noch schreibt das IT-Sicherheitsgesetz zwar kein solches vor. Doch spätestens mit der Anwendung der EU-DSGVO ab Mai 2018 dürfte es vor allem für KRITIS-Unternehmen schwierig werden, die gestiegenen Anforderungen ohne eine Automatisierung der Erkennungs- und Meldeprozesse zu erfüllen. Eine zugleich arbeitnehmer- und datenschutzkonforme Überwachung von Aktivitäten ist durch ein SIEM möglich, da Alarmierungen für Sicherheitsvorfälle nur bei Ausreißern aus der normalen IT-Systemnutzung erfolgen.

Consist Software Solutions GmbH
A Consist World Group Company

Falklandstraße 1-3, 24159 Kiel
Postfach 93 28, 24152 Kiel

Pressekontakt:
Petra Sauer-Wolfgramm

Telefon: 04 31 / 39 93 - 525
Telefax: 04 31 / 39 93 - 999
E-Mail: sauer-wolfgramm@consist.de
Internet: www.consist.de/presse

Sitz der Gesellschaft: Kiel
HRB Kiel Nr. 3983

Geschäftsführung:
Daniel Ries
Martin Lochte-Holtgreven

Presseinformation

Mit einem SIEM ist es wesentlich leichter, Transparenz zu erzielen. Die Möglichkeiten, um Sicherheitsvorfälle klären zu können, sind vielfältiger und einfacher zu handhaben. Moderne Methoden, wie Machine Learning, User Behavior Analysis oder Threat Lists in SIEMs erlauben es gezielt Incidents (Alarme) auf Abweichungen, Ausreißer zu generieren. Weniger Regelpflege, weniger Fehlalarme sind die angenehme Konsequenz hieraus.

Diese Pressemitteilung enthält 3.205 Zeichen (inkl. Leerzeichen) bei durchschnittlich 59 Zeichen pro Zeile.

Sie finden sie auch unter www.consist.de/presse

Weitere Informationen:

- Über Consist: www.consist.de
- Zum SIEM: www.consist.de/de/produkte/security_bigdata/splunk/

Consist Software Solutions GmbH
A Consist World Group Company

Falklandstraße 1-3, 24159 Kiel
Postfach 93 28, 24152 Kiel

Pressekontakt:
Petra Sauer-Wolfgramm

Telefon: 04 31 / 39 93 - 525
Telefax: 04 31 / 39 93 - 999
E-Mail: sauer-wolfgramm@consist.de
Internet: www.consist.de/presse

Sitz der Gesellschaft: Kiel
HRB Kiel Nr. 3983

Geschäftsführung:
Daniel Ries
Martin Lochte-Holtgreven

Unternehmensporträt

Die Consist Software Solutions GmbH ist Spezialist für IT-Services und Software. Seine Kunden unterstützt der IT-Dienstleister im gesamten Software-Lifecycle, von Entwicklungsprojekten über die Wartung in der Betriebsphase, bis hin zu ergänzenden Big Data- und Security-Produkten.

Mit mehr als 180 Mitarbeitern an den Standorten Kiel, Berlin und Frankfurt setzt Consist bundesweit qualitative Maßstäbe in den Bereichen Data Analytics, IT-Security und Managed Services.

Gegründet 1994 am Stammsitz Kiel führt das Unternehmen seinen Wachstumskurs nachhaltig fort, der Consist zu einem der erfahrensten IT-Dienstleister macht, dank ausgewiesener Mainframe-Kompetenz und hochqualifizierter Spezialisten für innovative Technologien. Ausgezeichnet mit dem großen Preis des Mittelstandes erhielt Consist in 2016 erneut den Premier-Sonderpreis.

IT that works.

Gründung:	1983 Profitcenter der Krupp MAK 1994 Ausgründung als Mak DATA SYSTEM Kiel GmbH
Geschäftsführer:	Martin Lochte-Holtgreven, Daniel Ries
Umsatz, Mitarbeiter:	26 Mio. € (2016), 190 Mitarbeiter (01.01.2017)
Standorte:	Kiel, Berlin, Frankfurt (Main), Braunschweig
Beteiligungen:	Consist ITU Environmental Software GmbH, Hamburg TeamWork GmbH, Kiel

Consist Software Solutions GmbH
A Consist World Group Company

Falklandstraße 1-3, 24159 Kiel
Postfach 93 28, 24152 Kiel

Pressekontakt:
Petra Sauer-Wolfgramm

Telefon: 04 31 / 39 93 - 525
Telefax: 04 31 / 39 93 - 999
E-Mail: sauer-wolfgramm@consist.de
Internet: www.consist.de/presse

Sitz der Gesellschaft: Kiel
HRB Kiel Nr. 3983

Geschäftsführung:
Daniel Ries
Martin Lochte-Holtgreven