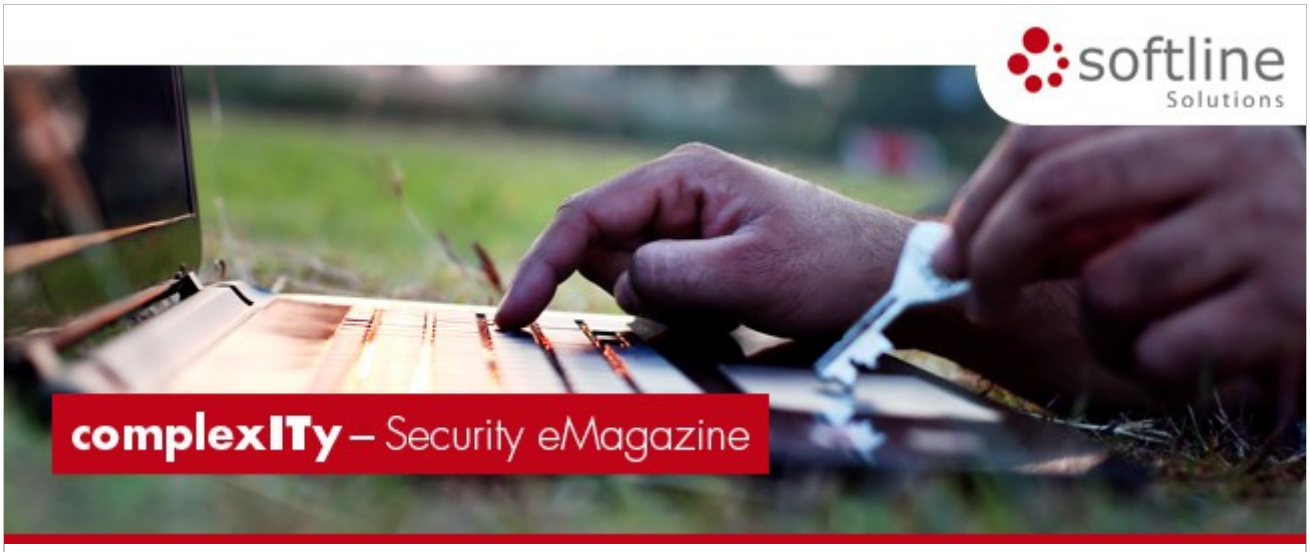

Leipzig, 14.12.2017

Liebe Leserinnen und Leser,

im aktuellen **IT-Security eMagazine – »complexITy«** beleuchten unsere Consultants für Sie das Thema **Security Monitoring** und wie man als Unternehmen oder Organisation die Gefahren und Bedrohungen des Internets im Blick behält. Um den Kontext des Security Monitorings und die Brisanz des Themas darzustellen, erläutern wir grundlegende Eigenschaften. In unseren Best Practices geben wir Ihnen fundierte Tipps rund um die Nutzung des **Security Information and Event Managements (SIEM) und des Security Operation Centers (SOC).** Ausgewählte Breaking News aus dem Security-Umfeld runden das eMagazine für Sie ab.

Wir wünschen Ihnen besinnliche Weihnachtsfeiertage und einen guten Rutsch ins neue Jahr sowie nun noch einmal viel Freude beim Lesen!

Security Monitoring in a Nutshell

Die Informations- und Kommunikationstechnik ist heutzutage nicht mehr nur ein notwendiges Übel für Unternehmen und Organisationen, sondern viel mehr ein Business Enabler, um flexibel am Markt zu überleben. Technologien und Services entwickeln sich permanent weiter, sodass Unternehmen (und Anwender selbst) die eigenen Aufgaben immer effizienter lösen können. Damit einhergehend ergeben sich jedoch stets neue Einfallstore für Angreifer.

Was für Unternehmen oft enorme Mehrwerte liefert, stellt IT-Abteilungen vor riesige Herausforderungen. Unzählige Informationen und Daten durchqueren das Unternehmensnetzwerk. Doch welche Informationen sind gewollt und welche haben möglicherweise einen schädigenden Hintergrund? Um dies herauszufinden, müssen alle Ereignisse im Netzwerk erfasst und mitgeschrieben werden. Auf diesen Ansatz baut das **Security Monitoring** auf und unterstützt folglich den IT-Betrieb, um stets verfügbar und handlungsfähig zu bleiben. Hierzu müssen kritische Ereignisse detektiert, frühzeitig erkannt und proaktive Maßnahmen eingeleitet werden.

Wissenswertes rund um das Security Monitoring

»Kontinuierliche Überwachung der IT-Systemumgebung«

Die Echtzeitüberwachung der IT-Systemumgebung führt zu einer wirksamen Früherkennung von modernen Cyber-Attacken. Dies erfolgt durch Sammlung von Ergebnisdaten aus unterschiedlichen operativen Ebenen und deren Echtzeitanalyse. Durch diese Ergebnisdaten ist es möglich, eine umfassende Abschätzung des Risikos von Cyber-Attacken zu ermitteln. Daraus resultieren zielgerichtete Maßnahmen zur Eindämmung von Angriffen.

Implementierung

Um Security Monitoring in das Unternehmen einzubinden, wird zunächst der aktuelle Stand der IT-Systemumgebung aufgezeichnet. Dieser bildet die Grundlage für die Definition des gewünschten Sicherheitslevels, welche wiederum in die Analyse einfließt. Die Umsetzung erfolgt durch Einbindung diverser Produkte (Programme), die das automatisierte Überwachen und Analysieren eines definierten Datenverkehrs übernehmen.

Brisanz für Unternehmen und Organisationen

Im Fokus dieses Security-Ansatzes steht der Schutz vor externen und internen Bedrohungen. Durch die schnellere Angriffserkennung können potenzielle Schäden stark reduziert werden. Zudem erzeugen die Einrichtung und der Betrieb der Security-Lösung einen umfassenden Einblick in die eigene IT-Systemlandschaft. Da Nachvollziehbarkeit und Aufzeichnung von Vorgängen fester Bestandteil des Ansatzes sind, wird die Erkennung von Anomalien im täglichen IT-Betrieb vereinfacht und Ausfallzeiten der Infrastruktur werden verringert.

Was kann überwacht bzw. getrackt werden?

- Malware
- Verdächtig gekennzeichnete externe Webseiten
- Kritische Kontexte
- Systeme
- Ungewöhnliche Verbindungen
- Anormales Verhalten innerhalb des Netzwerkes
- Anmeldungen an IT-Systemen
- Auslastung von Systemen
- Verfügbarkeit von Diensten
- Zutrittskontrollen zu Räumen oder Bereichen, wenn diese durch IT-Technik gesteuert werden

Welche Daten Sie individuell erfassen sollten, variiert je nach relevanter Information und Klassifikation bzw. was wichtig für den Betrieb oder die Schutzbedürftigkeit Ihrer Daten ist. So sollte z. B. gewährleistet sein, dass nur berechtigte Personen Zugriff zu klassifizierten Räumen haben oder dass Systeme nur durch bestimmte Konten administriert werden können. Um Gefahren aufzudecken, sollte eine unautorisierte Anmeldung in einem sicherheitsrelevanten System zwingend aufgezeichnet und zeitnah ausgewertet werden. Es besteht die Möglichkeit, regelmäßige Reports von Fortschritten und Verläufen zu erstellen und abzurufen.

Gründe für das »Tracken«

- Vertraulichkeit von Daten zu gewährleisten
- Systeme aufrecht erhalten
- Bei Problemen reagieren
- Vorbeugende Maßnahmen treffen
- Wahren der Datenintegrität
- Schutz vor Manipulation

Wie werden die gesammelten Daten weiterverarbeitet?

Proaktive Aufgaben können automatisch definiert werden, sodass z. B. eine E-Mail an einen Administrator versandt wird, sobald eine Anmeldung durch einen Dritten an einem sicherheitsrelevanten System erfolgt. Für reaktive Maßnahmen geben die getrackten Daten einen Hinweis für nächste Schritte, sind eine gute Vorbereitung für Folgetätigkeiten und gewährleisten einen reibungslosen Informationsfluss.

Weitere Informationen rund um die Informationssicherheit und IT-Security finden Sie hier. >>

Best Practices

Um einen passenden Ansatz zum effektiven Security Monitoring aufzustellen, werden zunächst zwei wesentliche Tools beschrieben: **SIEM und SOC.** Ein bewährte Möglichkeit zur Erfassung wichtiger Informationen ist die Nutzung eines ***Security Information and Event Managements (SIEM).*** Das Grundprinzip eines SIEM besteht darin, Ereignisse aus den verschiedensten Stellen eines Informationsverbundes aufzuzeichnen, um diese in Echtzeit zu analysieren und zu verarbeiten. Sicherheitsrelevante Daten werden in den nachfolgenden Schritten verarbeitet und gemeldet. Die Alarmierung spielt dabei eine wesentliche Rolle, da in der Folge ein kontinuierliches Reporting erstellt und noch wichtiger notwendige Abwehrmaßnahmen eingeleitet und durchgeführt werden.

SIEM klingt gut? Überlegen wir nun, wie es im Unternehmen Anwendung findet und welche Schnittstellen genutzt werden. Wichtig ist, im Vorfeld ein Konzept zu erstellen, welches die Gegebenheiten des Unternehmens aufgreift und daraus folgend den Umfang der Analyse definiert. SIEM kann als eigenständige Lösung in Form einer Software im Unternehmen betrieben und gepflegt werden, um aus den verschiedensten Quellen (Server, Clients, Netzwerkhardware, Firewalls etc.) notwendige Informationen zu beziehen. Nicht selten kommt dabei eine große Menge an Daten und Informationen zusammen, welche ausgewertet und behandelt werden müssen. Außerdem fallen hierbei oft Investitionen für die Anschaffung von Hardware-Ressourcen und Software-Lizenzen an. Sind die Gegebenheiten eines Unternehmens diesem Aufwand nicht gewachsen und ist die Geschäftsleitung dennoch bestrebt, alle kritischen Ereignisse zu entdecken, um mögliche Schäden zu vermeiden, besteht die Möglichkeit ‚SIEM-Dienste als Service zu nutzen. Externe Dienstleister übernehmen dabei die Verwaltung und Pflege des SIEM und werten alle aufgezeichneten Informationen im eigenen Umfeld aus.

SIEM-as-a-Service kann immer häufiger auch als Cloud-Service genutzt werden. Die Verantwortlichkeiten werden bei dieser Methode nahezu komplett zum Service-Provider ausgelagert. Für den Kunden wirkt sich das in vielerlei Hinsicht positiv aus. Zum einen kümmert sich ein speziell darauf geschultes Team um die Erfüllung des Services und zum anderen entstehen für Unternehmen kalkulierbare Kosten im Vergleich zur Realisierung im eigenen IT-Umfeld.

In einigen Organisationen und Unternehmen ist die Notwendigkeit zur Überwachung der eigenen IT-Landschaft besonders hoch. Hierfür wird ein sogenanntes ***Security Operations Center (SOC)*** gebildet. Dieses zeichnet sich dadurch aus, dass an einem zentralen Ort alle Informationen gesammelt werden (auch jene, welche ein SIEM zur Verfügung stellt). Der Unterschied zwischen einem SOC und einem SIEM besteht darin, dass in einem SOC Angriffe erkannt, entsprechende Prozesse eingeleitet und mögliche Nachfolgeschäden verhindert werden. SIEM ist im Grund nur eine Softwarelösung, welche ein SOC mit Informationen versorgt. Entsprechend geschulte Mitarbeiter werten diese aus und leiten Folgeprozesse ein.

Wie ein Security Operations Center konzipiert sein muss und in welchem Umfang es Ihr Unternehmen schützt, können wir Ihnen in Zusammenarbeit mit unserem Partner Radar Services gern in einem Workshop näherbringen. Sie wollen Ihre IT sicherer gestalten und die Möglichkeiten eines SIEM oder SOC nutzen? Dann sprechen Sie uns an! Wir beraten Sie gern in allen Angelegenheiten rund um das Thema Security Monitoring**.** Kontaktieren Sie uns dazu unter it-sicherheit@softline-group.com oder telefonisch unter +49 341 24051-0.

FAQ – Was bedeutet eigentlich …?

SIEM – Security Information & Event Management

Das *Security Information & Event Management* ist eine Softwarelösung, die Protokolle und Dokumente zur Analyse der Systemumgebung sammelt, verknüpft und analysiert. Dadurch können sicherheitsrelevante Ereignisse identifiziert und bewertet werden, sodass die daraus gezogenen Informationen zum Schutz Ihrer Unternehmenswerte beitragen.

SOC – Security Operation Center

Ein *Security Operations Center* bildet eine zentrale Anlaufstelle in Ihrem Unternehmen zur Erkennung und Abwehr von Angriffen auf die IT-Infrastruktur und IT-Systeme. Das SOC überwacht die IT-Infrastruktur auf Grundlage von Logdaten. Informationen werden live ausgewertet und Gegenmaßnahmen zur Minimierung von auftretenden Schäden eingeleitet.

Breaking News

IT-Grundschutz wurde modernisiert

Das Bundesamt für Sicherheit in der Informationstechnik hat schrittweise den bestehenden IT-Grundschutz und dessen zugehörige BSI-Standards aktualisiert.

Studien zufolge ist jedes zweite Unternehmen aus Deutschland einem Cyberangriff zum Opfer gefallen, wobei viele diesen nicht aufgedeckt oder gemeldet haben. Unter anderem sah sich das BSI aus diesem Grund in der Pflicht, die veröffentlichten Standards und das IT-Grundschutzkompendium zu aktualisieren. Der IT-Grundschutz richtet sich an Behörden und Unternehmen aller Branchen sowie Unternehmensgröße. Aktuell wird am neuen *BSI-Standard 200-2* zur IT-Grundschutz-Vorgehensweise gearbeitet; neu sind dabei drei Vorgehensweisen:

- **Basis-Absicherung:** Einstieg zur Initiierung eines Managementsystems für Informationssicherheit (ISMS)
- **Standard-Absicherung**: Implementierung eines kompletten Sicherheitsprozesses
- **Kern-Absicherung:** Betrachtet einen kleinen Teil eines größeren Informationsverbundes

Ziel dieser aktualisierten Vorgehensweise ist es, kleine und mittelständische Unternehmen (KMU) stufenweise an das vielschichtige und komplexe IT-Management heranzuführen.

PSTN-Calling Germany

In Deutschland befindet sich das Produkt **PSTN-Calling Germany** (aus dem Hause Microsoft) innerhalb der »Office 365«-Welt aktuell noch in der Preview-Phase. Diesen Status wird es jedoch in den kommenden Monaten verlassen.

Mittels PSTN-Calling wird es möglich, eine Telefonanlage in der Cloud von Microsoft abzubilden. Dieses Vorgehen wird auch *Cloud-PBX* genannt. Dadurch können Unternehmen PSTN-Anrufdienste direkt über Microsoft beziehen. Ohne die OnPremise-Sever von Lync/ Skype for Business können über den Office 365 Skype for Business Client Anrufe ins Fest- und Mobilfunknetz durchgeführt werden. Nutzer erhalten eine deutsche Telefonnummer für ein- und ausgehende Anrufe. Die Audio-/ Video-Verbindung, wie in Skype for Business bekannt, bleibt unabhängig von PSTN-Calling möglich. Die Abrechnung erfolgt über Microsoft, welche dadurch wie andere Konkurrenten (z. B. Vodafone, QSC und Telekom) zum Carrier werden.

Skype for Business fasst als Software Client von Microsoft die Kommunikationsformen Instant Messaging, Konferenzen, Telefonie, Voice-Mail etc. unter einer einheitlichen Benutzeroberfläche zusammen.

Die Softline Solutions GmbH unterstützt Sie bei der Entwicklung eines Notfallplans oder der Erstellung eines Notfallhandbuches sowie deren Umsetzung im Unternehmen. Kontaktieren Sie uns dazu unter it-sicherheit@softline-group.com oder telefonisch unter +49 341 24051-0.

ISDN-Abschaltung

Bis Ende 2018 soll laut der Telekom ISDN gänzlich abgeschaltet werden. Im Zuge der Umstellung gab es diverse Bedenken, was die Sicherheit von *Voice over IP (VoIP)* anbelangt.

An dieser Stelle kommen das ***Session Initiation Protocol Security (SIPS)*** und ***Secure Real-Time Transport Protocol (SRTP)*** ins Spiel.

Bei **SIPS** handelt es sich um eine Erweiterung für SIP. Diese wurde zusätzlich um eine Verschlüsselung mit TLS/ SSL ergänzt. Mithilfe der Erweiterung kann der Verbindungsaufbau zwischen IP-Telefonanlage und VoIP-Telefon per Handshake-Verfahren verschlüsselt erfolgen. Ist die Verbindung aufgebaut, kommt das Protokoll **SRTP** zum Tragen. Zum Transport werden die

RTP-Pakete in SRTP-Pakete eingebettet. Zur Verschlüsselung des RTP-Datenstroms wird der *Advanced Encryption Standard (AES)* mit einer Schlüssellänge bis zu 256 Bit verwendet. Damit der Empfänger die Daten auch wieder entschlüsseln kann, wird bei der Initialisierung der Verbindung ein Master-Key über SIPS versendet. Dies ermöglicht dem Empfänger, die verschlüsselten Datenpakete wieder in »hörbare« Pakete umzuwandeln.

Für die Einrichtung kann z. B. der *Session Border Controller* von Ferrari electronic genutzt werden. Dieser verwendet intern ein virtuelles Vermittlungssystem als *back-to-back user agent (B2BUA)*, bei dem externe und interne SIP-Verbindungen komplett unabhängig voneinander sind. Beispielweise können so keinerlei SIP-Header einfach durchgereicht werden. Unterstützung für eine sichere IP-Kommunikation bieten bspw. eine vielfältig konfigurierbare Firewall, flexible Listenverarbeitung (replizierbare Black-/ Whitelists) und *TLS, SRTP* – u. a. auch mit *QSC SIP-Trunks.*

Falls Sie Fragen oder Hinweise zu gewünschten Magazininhalten haben oder unsere Unterstützung in IT-Sicherheitsprojekten benötigen, dann kontaktieren Sie uns unter it-sicherheit@softline-group.com oder telefonisch unter +49 341 24051-0.

Mit freundlichen Grüßen
Ihr Softline Team

Weitere Blog-Beiträge unserer IT-Experten zu den Themen SAM, IT-Sicherheit und Informationssicherheit finden Sie hier >>

Softline Solutions GmbH // Geschäftsführer: Martin Schaletzky // Sitz der Gesellschaft: Leipzig // Handelsregister Leipzig: HRB 26058 // Steuer Nr.: 232/118/06001 // USt ID: DE270894910