Wunderwaffe SIEM?

SIEM Tools und Remote Access VPN im Zusammenspiel

Im Schnitt dauert es rund 256 Tage (Ponemon Institute) bis eine erfolgreiche Cyberattacke erkannt wird – falls sie denn überhaupt auffällt. Der damit verbundene Schaden kostet die deutsche Wirtschaft laut VDI jährlich über 50 Milliarden Euro. Betroffen von der steigenden Zahl immer raffinierterer Angriffe sind nicht nur Konzerne oder bestimmte Branchen, sondern Unternehmen aller Größen. Dies zeigt, dass die Motivation der Angreifer nicht immer offensichtlich und klar ist. Welche Daten schützenswert sind und wer Systeme über welchen Weg attackiert sollte aus Unternehmenssicht unbedingt erfasst werden – zusammen mit definierten Prozessen, die im Angriffsfall ablaufen müssen.

Das Problem ist meist nicht, dass keine hilfreichen Daten zu möglichen oder erfolgreichen Attacken vorliegen, sondern eher die schwierige Auswertung einer viel zu großen und unstrukturierten Informationsflut. Die Datenmengen resultieren aus steigenden Zahlen an Nutzern, Endgeräten und Anwendungen, die für Menschen unüberschaubare Berge an Protokolldaten produzieren. SIEM-Systeme (Security Information and Event Management) zur besseren Analyse und Verwaltung von Angriffsindikatoren setzen genau hier an.

Aus gesammelten Daten von Netzwerk-Komponenten, Betriebssystemen und Applikationen werden Zusammenhänge zwischen einzelnen Ereignissen hergestellt und als Warnungen und Berichte an Verantwortliche wie z.B. IT-Administratoren ausgegeben. Durch die Dokumentation und Archivierung sicherheitsrelevanter Vorfälle können Sicherheitslücken geschlossen und ähnliche Angriffe künftig besser verhindert werden. Auf diese Weise leistet ein SIEM-System einen wesentlichen Beitrag zur kontinuierlichen Verbesserung der Standards für Sicherheit, Compliance und Qualität des IT-Betriebes.

Remote Access als beliebtes Einfallstor

Über Remote-Verbindungen versuchen Angreifer den Zugriff auf Firmendaten zu erlangen. In diesem Zusammenhang können v.a. Nutzer- und Zugriffsdaten analysiert werden, um Anomalien im Log-Aufkommen sowie Angriffe aufzudecken. Im ersten Schritt muss allerdings bekannt sein, wie normale Netzaktivitäten aussehen, um Abweichungen in Echtzeit als solche zu erkennen. Diese unterscheiden sich firmen- oder sogar abteilungsspezifisch. Während beispielsweise eine doppelte Anmeldung von Benutzern in der Regel auf ungewöhnliche Aktivitäten hinweist, ist dies unter Umständen völlig normal, wenn ein Vorgesetzter und sein Assistent dieselben Login-Daten nutzen, um gemeinsam auf ein E-Mail-Konto zuzugreifen.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Wunderwaffe SIEM?

Die meisten Attacken werden statistisch gesehen von ehemaligen Mitarbeitern oder Dienstleistern mit Administratoren-Zugang verübt. Unternehmen müssen daher heute ihr Augenmerk ganz besonders nach innen richten, um bekannte Sicherheitssünden möglichst auszumerzen:

- Nachlässige Kontrolle mobiler Endgeräte und Wechselmedien wie USB-Sticks
- Nutzung schlecht abgesicherter privater Geräte für den Firmengebrauch (BYOD) sowie leichtsinnige Verwendung von Firmengeräten für private Zwecke
- Unzureichende Schulung der Anwender bzgl. möglicher Gefahrenquellen oder z.B. aktueller Schadsoftware
- Lückenhafte Kontrolle von Updates und Co. bei personenunabhängigen Geräten im Netzwerk, die auch als Einfallstor dienen können (z.B. Drucker)
- Mangelnde Kontrolle und Übersicht, welche Anwendungen im Firmennetz welche Verbindung aufbauen und Daten übertragen dürfen

SIEM und NAC – Quarantänezone anstatt Netzwerkzugang

Wichtig ist also u.a. ein kompletter Überblick über die Geräte, die sich im Netzwerk befinden oder die über VPN zugreifen – PCs, Laptops, Drucker, technische Geräte und Maschinen, Smartphones sowie Tablets. Eine Möglichkeit zur besseren Absicherung externer Netzwerkzugänge ist die Netzzugangskontrolle (Network Access Control) als Technologie zur Abwehr von Schadsoftware und unautorisierten Zugriffen. Bei der einfachsten Form wird überprüft, ob sich die MAC- oder IP-Adresse eines Gerätes auf der Whitelist für den Netzwerkzugang befindet.

Darüber hinaus spielt es eine Rolle, welches Betriebssystem die Geräte verwenden, welche Anwendungen installiert sind oder ob Antivirenprogramme aktuell sind. Und dies sind nur einige Beispiele der Risiken, die durch eine gezielte Prüfung der Richtlinienkonformität während der Authentisierung verringert werden können. Weicht ein System von den Sicherheitsrichtlinien ab, kann es in eine Quarantänezone mit beschränktem Serverzugriff z.B. nur zur Software-Aktualisierung geleitet werden. Solche Lösungen sind vom Mitarbeiter nicht manipulierbar und können auch nicht umgangen werden. Keine Erfüllung der Richtlinien, kein Zugang.

SIEM- Systeme liefern beispielsweise über Zugangs- und Protokolldaten zahlreiche Informationen zu den im Netz befindlichen Geräten oder der Authentisierung derselben. Sie dienen u.a. als Grundlage für die Netzzugangskontrolle. Durch das Zusammenspiel einer Analyse von SIEM-Daten und NAC kann die Sicherheit im Unternehmensnetzwerk beim lokalen Zugang oder von extern über VPN enorm erhöht werden. Bedenkt man, dass Mitarbeiter und von ihnen verwendete Geräte eines der größten Sicherheitsrisiken darstellen, setzt diese Kontrolle den Hebel hier genau an der richtigen Stelle an.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Wunderwaffe SIEM?

Bessere Absicherung von VPN Verbindungen

Zahlreiche Funktionen der VPN Software von NCP ermöglichen im Bereich Remote Access ein hohes Sicherheitslevel und können gleichzeitig relevante Informationen für SIEM-Tools liefern. Durch eine zentral vorgegebene Parametersperre kann z.B. ausgeschlossen werden, dass Anwender Konfigurationen manipulieren oder unabsichtlich deaktivieren. Im Rahmen der Endpoint Security kann der Administrator über das Management System sicherheitsrelevante Parameter festlegen anhand derer die VPN Clients dann vor jedem Zugriff auf das Firmennetz überprüft und gegebenenfalls in eine Quarantänezone geleitet werden.

Da User-Name und Passwort heute viel zu leicht durch Hacker ausgespäht werden können, legt NCP großen Wert auf zahlreiche unterschiedliche Technologien (auch zusammen mit Technologiepartnern) für eine starke Authentifizierung:

- Integrierte Advanced Authentication über SMS
- OTP-Token (dynamisch generierte Einmalpasswörter)
- Elliptische Kurven (ECC) und digitale Zertifikate (Software oder Smartcard) in einer PKI (Public Key Infrastructure)
- Biometrische Technologien

Sämtliche Meldungen (Log-Ausgaben, Warnungen, Systemmeldungen, etc.) der zentralen NCP - Komponenten (VPN Management und VPN-Gateways) können in die SIEM-Tools einfließen und die automatisierte Analyse und proaktive Erkennung von Anomalien erleichtern. Um das Zusammenspiel von SIEM-Tools und der NCP Enterprise-Lösung noch effektiver zu gestalten, arbeitet NCP kontinuierlich an der Weiterentwicklung der Schnittstellen zu diesen Werkzeugen. Wichtige Voraussetzung beim Einsatz intelligenter Software ist aber immer, dass Administratoren und auch Anwender geschult sind und sich nicht alleine auf diese Tools verlassen.

Lehren aus SIEM-Daten ziehen

Vier Schritte zur Abwehr von Cyberattacken

1. Bestandsaufnahme und Risikobewertung vornehmen	Wissen, welche Daten und Informationen schützenswert sind und mögliche Schäden bei Verlust oder Diebstahl kennen
2. Netzaktivitäten analysieren	Normales Nutzer- und Netzverhalten kennen, um Anomalien zu erkennen
3. Sicherheitsrelevante Daten auswerten und Prozesse für den Angriffsfall festlegen	Verantwortliche und Abläufe für Angriffsszenarien definieren, um reaktionsfähig zu sein
4. Mitarbeiter regelmäßig schulen	Mitarbeiter regelmäßig auf aktuelle Schadsoftware und Cyberangriffe hinweisen, um sie so zu sensibilisieren

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Wunderwaffe SIEM?

Haftungsausschluss
Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen
Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

Stand März 2016

Next Generation Network Access Technology

www.ncp-e.com

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Phone: +1 (650) 316-6273 · www.ncp-e.com