**Vertrauen ist gut, Kontrolle ist (un)möglich**

IT-Sicherheit spielt in Zeiten von Digitalisierung eine tragende Rolle, um gezielte Cyber-Angriffe abzuwenden.

KONVERTO, eines der führenden IT-Unternehmen Südtirols, hat in seinem Event „talks Thinking Security“ gemeinsam mit dem internationalen Security-Spezialisten Fortinet auf die zunehmende Wichtigkeit der Sicherheit im IT-Umfeld reagiert und Lösungen aufgezeigt, die den wachsenden Bedrohungen durch äußere Einflüsse standhalten. In einem anregenden Gespräch mit Sandro Moretti, Division Manager Teleconduction & Telecommunication von Alperia, Christian Pezzei, Geschäftsführer von Eurotherm, und Enrico Dorigatti, Key Account Manager BU Enterprise von KONVERTO, hat Moderator Markus Frings über ihre Erfahrungen mit digitalen Bedrohungen sowie über Chancen, aber auch Risiken, die die Digitalisierung mit sich bringt, diskutiert.

Mit einem Fahrerlebnis auf dem Gelände des Safety Park in Bozen mit Elektro- und Hybrid-Autos wurden die Gäste von der IT-Welt in die Realität der Verkehrssicherheit auf den Straßen zurück katapultiert.

Im Mittelpunkt der Veranstaltung standen die Sicherheitssysteme Security Information and Event Management SIEM und Network Access Control NAC – Mechanismen, die alle Sicherheitsereignisse überwachen und kontrollieren.

„Bei Eurotherm legen wir hohen Wert auf die Sicherheit unserer Systeme, und auch die Sensibilisierung der Mitarbeiter für dieses Thema spielt im heutigen Geschäftsleben eine zentrale Rolle. Seit Langem ist KONVERTO unser Partner und Berater in Sachen IT-Sicherheit und Cloud-Lösungen. Die verlässliche, kompetente und innovative Denk- und Arbeitsweise hat uns seit jeher Überzeugt“, unterstreicht Christian Pezzei, Geschäftsführer von Eurotherm.

„Die Sicherheit des Unternehmensnetzes im Blick zu haben, die Geräte zu kontrollieren, mit denen Mitarbeiter sich ans Netz anschließen und die Systeme vor Angriffen von außen zu schützen, sind Aspekte, die bei Alperia von größter Bedeutung sind. Zu wissen, dass es Mechanismen gibt, die für mehr Sicherheit und Kontrolle sorgen, ist essenziell, um sich den zunehmenden Herausforderungen der Digitalisierung zu stellen“, sagt Sandro Moretti, Division Manager Teleconduction & Telecommunication von Alperia. „KONVERTO hat innovative Lösungen, die den Sicherheitsanforderungen von Unternehmen gerecht werden.“

**Doch was genau versteht man unter SIEM und NAC?**

Security Information and Event Management SIEM heißen die Systeme, die genau diese Aufgabe übernehmen; die Ereignisdaten von unterschiedlichsten heterogenen IT-Systemen werden zentral gesammelt, interpretiert, klassifiziert und daraus werden Schlüsse gezogen. Die Analyse der Ereignisse verläuft dabei in Echtzeit, sodass im Ernstfall sofort ein Alarm ausgelöst wird und dadurch ein Schaden noch abgewendet oder eingegrenzt werden kann.

**Korrelation der Ereignisse**

Die Kernfunktion eines SIEM besteht in der Korrelation der Ereignisse. Dabei werden Vorfälle auf unterschiedlichsten Systemen untereinander in Verbindung gebracht und daraus eine Sicherheitsbedrohung abgeleitet. Die Einzelereignisse auf den verschiedenen Systemen sind nämlich oft für sich allein betrachtet recht unkritisch, im Zusammenhang über die Systemgrenzen hinweg betrachtet kann daraus aber eine klare Verletzung der IT-Sicherheit erkannt werden. Das Erstellen eines neuen Kontos auf einem System durch einen Administrator ist eigentlich ein unbedeutendes Ereignis, wenn allerdings dieser Vorgang an einem unüblichen Ort stattfindet oder über ein unübliches Gerät ausgeführt wurde, so kann dies auf ein gehacktes Administratorkonto hinweisen. Das belanglose Ereignis wird durch die Korrelation zu einem kritischen Alarm eskaliert.

**Sicherheit durch Maschinelles Lernen**

Moderne SIEM Lösungen verbessern ihre Aussagekraft durch Funktionen welche aus dem Bereich von Big Data, Maschinellem Lernen und Künstlicher Intelligenz stammen.

Damit erkennt ein SIEM nicht nur Angriffe, welche nach einem bekannten Muster ablaufen, sondern es ist auch in der Lage, eigenständig verdächtige Abweichungen von Normalwerten ausfindig zu machen.

Die dynamischen Normalwerte werden in der jeweiligen Umgebung selbständig durch die Beobachtung über einen gewissen Zeitraum gelernt und sie werden auf Tages-, Wochen- oder Monatsbasis ausgewertet.

Eine verdächtig hohe Anzahl von Datenbankänderungen zu einer gewissen Uhrzeit, seltsame Anmeldevorgänge eines Benutzers am Wochenende oder ein ungewöhnlicher Netzwerkverkehr: all dies kann auf eine potenzielle Sicherheitsverletzung hinweisen; moderne SIEM Systeme erkennen solche Ausreißer ganz von allein.

**Wertvoller Datenschatz**

Aufgrund der umfassenden Datensammlung ist ein SIEM auch der ideale Startpunkt für forensische Analysen im Falle einer Sicherheitsverletzung. Zu den Standardfunktionen von SIEM Lösungen zählen selbstverständlich auch Berichte auf unterschiedlichen Detailebenen, von punktuellen Ereignissen bis hin zu längerfristigen Trendanalysen.

Die aktuellen SIEM Produkte der verschiedenen Hersteller interpretieren Protokolldaten von allen gängigen Server-Betriebssystemen, Netzwerkprodukten, Firewallsystemen, Datenbanken, Standardapplikationen und Cloudanwendungen.

Die SIEM-Lösung selbst kann in unterschiedlicher Hardwareausstattung, als Software oder selbst als Cloudlösung aktiviert werden.

**Schwachpunkt Netzwerkzugang**

Nicht minder herausfordernd als die Überwachung der Ereignisse auf den unterschiedlichsten IT-Systemen ist die Regulierung des Netzwerkzuganges im Unternehmen.

Eine Haustür ist dafür da, nur bekannte und vertrauenswürdige Wesen ein- und auszulassen und einen genauen Überblick über die anwesenden Personen zu haben.

Eine ähnliche Funktion sollte es auch für den Zugang zum Unternehmensnetzwerk geben, schließlich sind darüber äußerst kritische und schützenswerte Informationen zu erreichen.

Die Realität ist im Allgemeinen aber recht ernüchternd, meistens reicht eine Netzsteckdose oder ein WLAN Passwort (vielleicht von einem Mitarbeiter weitergegeben), um sich erfolgreich mit dem Unternehmensnetzwerk zu verbinden.

Dabei ist der Zugang zum Netzwerk noch viel kritischer zu betrachten: nicht nur externe Personen müssen erkannt, sondern auch die internen Personen und deren Geräte müssen laufend überprüft werden. Nach wie vor passieren nämlich die meisten Sicherheitsverletzungen durch Innentäter.

**Der digitale Türsteher**

Ein Network Access Control NAC System übernimmt die Aufgabe eines digitalen Türstehers: die Objekte werden vor dem Zustandekommen einer Netzwerkverbindung eingehend überprüft und nur was vertrauenswürdig erscheint wird durchgelassen. Geräte welche nicht den vorgegebenen Richtlinien entsprechen werden ausgesperrt oder für das Erreichen der Konformität in eine Quarantäne gesetzt.

Ohne diese Kontrolle könnte ein kompromittiertes Gerät ganz von allein, ohne Zutun einer Person und ohne irgendwelche Eingabe von Passwörtern, tief ins Netzwerk eindringen und sensible Informationen (etwa Zugangsdaten) stehlen und beträchtlichen Schaden anrichten.

Der Vergleich mit einem Türsteher betrifft aber nur einen Teil eines NAC Systems: die verbundenen Geräte werden nicht nur beim Verbindungsaufbau, sondern regelmäßig überprüft. Beim Abweichen von den vorgegebenen Richtlinien wird sofort eingegriffen, um die Sicherheit kontinuierlich aufrechtzuerhalten.

Genauso wie SIEM Systeme haben auch moderne NAC Systeme Funktionen von Big Data und Künstlicher Intelligenz entliehen, um noch effizienter auf bestimmte Bedrohungen hinzuweisen. Dabei wird der von den einzelnen Geräten erzeugte Netzwerkverkehr unter die Lupe genommen, um Auffälligkeiten und verdächtige Abweichungen vom Normalverhalten zu identifizieren und zu melden.

**Erhöhte Sichtbarkeit**

Eine klare Übersicht darüber, was sich zu einem gegebenen Zeitpunkt alles im eigenen Netzwerk tummelt, ist eigentlich eine Grundvoraussetzung für jedes Sicherheitsmanagement; ohne ein modernes NAC System beruht eine solche Übersicht aber mehr auf vagen Vermutungen als auf zuverlässigen Daten. Manchmal ist schon allein dieser Umstand der erhöhten Sichtbarkeit im Netzwerk der Hauptgrund dafür, dass sich Unternehmen für ein NAC System entscheiden.

„Mit dieser Veranstaltung wollten wir die Relevanz von IT-Sicherheit im digitalen Geschäftsumfeld aufzeigen und verdeutlichen, dass sicherheitsorientierte Netzwerke und und KI-gesteuerte Bedrohungsabwehrmechanismen in einer stark vernetzten Welt wesentlicher Bestandteil einer IT-Infrastruktur sein müssen“, betonen die beiden KONVERTO-Direktoren Peter Nagler und Peter Werth. „IT-Sicherheit zu thematisieren, die Faktoren aufzeigen, die Schwachstellen im Unternehmensnetz ausnutzen und wie man Lösungen integriert, die für mehr Kontrolle und Transparenz sorgen, ist unser Ziel. Dies den Unternehmern nahe zu bringen, ist uns mit KONVERTO talks gelungen.“, sind sich beide Direktoren einig.

KONVERTO AG

Bruno-Buozzi-Str. 8

39100 Bozen

800 031 031, 0471 064 500

info@konverto.eu

konverto.eu

**Konverto verbindet Mensch und Technik**

Konverto ist aus dem Zusammenschluss der IT-Unternehmen Raiffeisen OnLine und RUN Raising Unified Network hervorgegangen. Der innovative IT-Player blickt auf langjährige Erfahrung in der IT-Branche zurück und bedient dank seines hochgradigen Know-hows den Markt mit einem breiten IT-Angebot. Mit 130 spezialisierten Mitarbeiten verfügt dasUnternehmen über äußerst breit aufgestellte IT-Kompetenzen. Das Service-Angebot bedient sowohl Unternehmen als auch Privatpersonen und reicht von Internetanbindungen, Security, Modern Workplace, Business Continuity, Cloud-Lösungen, bis hin zu Software-Entwicklung und Digitalisierung.

**La fiducia è buona, il controllo è (im)possibile**

In tempi di digitalizzazione, la sicurezza informatica svolge un ruolo importante per evitare attacchi informatici mirati.

KONVERTO, una delle aziende IT leader in Alto Adige, ha reagito alla crescente importanza della sicurezza nell'ambiente IT nel suo evento "talks Thinking Security" insieme allo specialista internazionale della sicurezza Fortinet e ha presentato soluzioni che resistono alle crescenti minacce di influenze esterne. In una stimolante conversazione con Sandro Moretti, Division Manager Teleconduction & Telecommunication di Alperia, Christian Pezzei, Amministratore Delegato di Eurotherm, ed Enrico Dorigatti, Key Account Manager BU Enterprise di KONVERTO, il moderatore Markus Frings ha discusso le loro esperienze con le minacce digitali e le opportunità e i rischi della digitalizzazione.

Con un'esperienza di guida nel parco di sicurezza di Bolzano con auto elettriche e ibride, gli ospiti sono stati catapultati dal mondo IT nella realtà della sicurezza stradale su strada.

L'evento si è focalizzato sui sistemi di sicurezza Security Information and Event Management SIEM e Network Access Control NAC - meccanismi che monitorano e controllano tutti gli eventi di sicurezza.

"In Eurotherm attribuiamo grande importanza alla sicurezza dei nostri sistemi e la sensibilizzazione dei dipendenti su questo tema gioca un ruolo centrale nell'attuale contesto imprenditoriale. KONVERTO è da tempo nostro partner e consulente per la sicurezza informatica e le soluzioni cloud. Il modo di pensare e lavorare affidabile, competente e innovativo ci ha sempre convinto", sottolinea Christian Pezzei, Amministratore Delegato di Eurotherm.

"L'attenzione alla sicurezza della rete aziendale, il controllo dei dispositivi con cui i dipendenti si collegano alla rete e la protezione dei sistemi da attacchi esterni sono aspetti della massima importanza in Alperia. Sapere che esistono meccanismi per aumentare la sicurezza e il controllo è essenziale per affrontare le crescenti sfide della digitalizzazione", afferma Sandro Moretti, Division Manager Teleconduzione & Telecomunicazioni di Alperia. "KONVERTO ha soluzioni innovative che soddisfano le esigenze di sicurezza delle aziende".

**Cosa si intende con SIEM und NAC?**

Security Information and Event Management SIEM è il nome dei sistemi che svolgono proprio questo compito; i dati degli eventi provenienti da un'ampia varietà di sistemi informatici eterogenei vengono raccolti, interpretati, classificati e le conclusioni tratte centralmente. L'analisi degli eventi avviene in tempo reale, in modo che in caso di emergenza scatti immediatamente un allarme e i danni possano essere evitati o limitati.

**Correlazione degli eventi**

La funzione principale di un SIEM è la correlazione degli eventi. Gli incidenti su sistemi diversi sono collegati tra loro e ne deriva una minaccia per la sicurezza. I singoli eventi sui vari sistemi sono spesso di per sé poco critici, ma se visti in un contesto che supera i confini del sistema, è possibile rilevare una chiara violazione della sicurezza informatica. La creazione di un nuovo account su un sistema da parte di un amministratore è in realtà un evento insignificante, ma se questo processo si svolge in un luogo insolito o è stato eseguito tramite un dispositivo insolito, questo può indicare un account amministratore violato. L'evento insignificante viene incrementato dalla correlazione con un allarme critico.

**Sicurezza grazie all'apprendimento automatico**

Le moderne soluzioni SIEM migliorano il loro significato attraverso funzioni provenienti dai campi dei Big Data, Machine Learning e Artificial Intelligence.

In questo modo, un SIEM non solo rileva gli attacchi che si verificano secondo un modello noto, ma è anche in grado di rilevare autonomamente le deviazioni sospette dai valori normali.

I valori normali dinamici sono appresi indipendentemente nel rispettivo ambiente attraverso l'osservazione per un certo periodo di tempo e sono valutati su base giornaliera, settimanale o mensile.

Un numero sospettosamente elevato di modifiche al database in un determinato momento, strani login degli utenti nel fine settimana o un traffico di rete insolito: tutto questo può indicare una potenziale violazione della sicurezza; i moderni sistemi SIEM rilevano da soli questi valori anomali.

**Prezioso tesoro di dati**

Grazie alla sua ampia raccolta di dati, il SIEM è anche il punto di partenza ideale per le analisi forensi in caso di violazione della sicurezza. Le caratteristiche standard delle soluzioni SIEM comprendono report a vari livelli di dettaglio, dagli eventi puntuali all'analisi delle tendenze a lungo termine.

Gli attuali prodotti SIEM di vari produttori interpretano i dati di log di tutti i comuni sistemi operativi per server, prodotti di rete, sistemi firewall, database, applicazioni standard e applicazioni cloud.

La soluzione SIEM stessa può essere attivata in varie configurazioni hardware, come software o addirittura come soluzione cloud.

**Accesso alla rete di punti deboli**

Non meno impegnativo del monitoraggio degli eventi su una vasta gamma di sistemi IT è la regolazione dell'accesso alla rete all'interno dell'azienda.

Una porta d'ingresso permette solo a persone conosciute e affidabili di entrare e uscire e di avere una visione d'insieme precisa delle persone presenti.

Una funzione analoga dovrebbe essere prevista anche per l'accesso alla rete aziendale, che può essere utilizzata per raggiungere informazioni estremamente critiche e sensibili.

Nella maggior parte dei casi, una presa di corrente o una password WLAN (magari fornita da un dipendente) è sufficiente per connettersi con successo alla rete aziendale.

L'accesso alla rete è ancora più critico: non solo le persone esterne devono essere rilevate, ma anche le persone interne e i loro dispositivi devono essere continuamente controllati. La maggior parte delle violazioni della sicurezza sono ancora commesse dagli autori interni.

**Il portiere digitale**

Un sistema Network Access Control NAC assume il ruolo di un portiere digitale: gli oggetti vengono accuratamente controllati prima di stabilire una connessione di rete e solo ciò che appare affidabile è consentito. I dispositivi non conformi alle linee guida specificate sono bloccati o messi in quarantena per la conformità.

Senza questo controllo, un dispositivo compromesso potrebbe penetrare in profondità nella rete, rubando informazioni sensibili (come le credenziali) e causando danni significativi, tutto da solo, senza l'intervento di nessuno e senza inserire alcuna password.

Il confronto con un portiere, tuttavia, riguarda solo una parte di un sistema NAC: i dispositivi collegati non solo durante il collegamento, ma anche regolarmente. Se un dispositivo si discosta dalle linee guida specificate, vengono intraprese azioni immediate per mantenere la sicurezza su base continuativa.

Proprio come i sistemi SIEM, i moderni sistemi NAC hanno preso in prestito le funzioni dei Big Data e dell'Intelligenza Artificiale per allertare in modo più efficiente le minacce specifiche. Il traffico di rete generato dai singoli dispositivi viene analizzato per identificare e segnalare anomalie e deviazioni sospette dal comportamento normale.

**Maggiore visibilità**

Una chiara panoramica di ciò che accade nella propria rete in un dato momento è in realtà un requisito fondamentale per qualsiasi gestione della sicurezza; senza un moderno sistema NAC, tuttavia, tale panoramica si basa più su ipotesi vaghe che su dati affidabili. A volte questo fatto di maggiore visibilità nella sola rete è la ragione principale per cui le aziende scelgono un sistema NAC.

"Con questo evento, abbiamo voluto dimostrare l'importanza della sicurezza informatica nell'ambiente di business digitale e chiarire che le reti orientate alla sicurezza e i meccanismi di difesa dalle minacce controllate dall'intelligenza artificiale devono essere parte integrante di un'infrastruttura IT in un mondo altamente interconnesso", sottolineano i due direttori di KONVERTO Peter Nagler e Peter Werth. "Il nostro obiettivo è quello di affrontare la sicurezza informatica, identificare i fattori che sfruttano le vulnerabilità della rete aziendale e come integrare soluzioni che offrano maggiore controllo e trasparenza. Con i colloqui KONVERTO, siamo riusciti ad avvicinare questo aspetto agli imprenditori", concordano entrambi i direttori.

KONVERTO S.p.A.

Via Bruno Buozzi 8

39100 Bolzano

800 031 031, 0471 064 500

info@konverto.eu

konverto.eu

**Konverto connette persone e tecnologia**

Konverto è il risultato della fusione delle società IT Raiffeisen OnLine e RUN Raising Unified Network. L'innovativo player IT può vantare un'esperienza pluriennale nel settore IT e, grazie al suo know-how di alto livello, serve il mercato con una vasta gamma di prodotti IT. Con 130 dipendenti specializzati, l'azienda ha competenze informatiche estremamente ampie. L'offerta di servizi è rivolta sia alle aziende che ai privati e spazia dalle connessioni Internet, alla sicurezza, ai moderni ambienti di lavoro, alla business continuity e alle soluzioni cloud, allo sviluppo software e alla digitalizzazione.