ADVANCED CYBER DEFENCE – UNIFIED SECURITY MANAGEMENT

Sicherheit durch Innovation, Transparenz und Kompetenz

UMFASSENDER SCHUTZ

In Zeiten wachsender Cyber-Kriminalität ist es unverzichtbar, das Sicherheitsniveau der eigenen ICT-Infrastruktur realistisch einzuschätzen. Mit welchem Aufwand können Angreifer zum Beispiel über ein Webportal in die Backend-Systeme eindringen? Wie gut sind Kunden- und Geschäftsdaten geschützt? Werde ich gerade angegriffen? Sind diese Angriffe geglückt oder haben die Schutzmaßnahmen die gewünschte Wirkung gezeigt?

Um diese Fragen beantworten zu können, ist ein umfassender Gesamtüberblick über die aktuelle Lage sowie alle Vorgänge erforderlich. An verfügbaren Sicherheitslösungen mangelt es heute nicht mehr. Für jeden Anwendungsfall steht eine Vielzahl an Produkten zur Verfügung, die jedoch meist nur Inselsysteme darstellen. Eine übergreifende Analyse von Daten, die Sicherheitsprobleme erkennen, erfolgt jedoch meist nicht. Mit Unified Security Management stellt Ihnen T-Systems eine Management Plattform zur Verfügung, mit der Sie in der Lage sind, Ihre Risiken ganzheitlich entdecken sowie bewerten zu können und im Falle eines Angriffs bestmöglich darauf reagieren zu können.

SCHWACHSTELLEN AUFSPÜREN

Mitarbeiter kommen und gehen. Neue Hardware wird hinzugefügt, alte Hardware wird entfernt. Ständig werden neue Software-Bugs gefunden. Dies bedeutet, dass sich Ihr Netzwerk mit all seinen Komponenten und somit auch mögliche Angriffsflächen ständig verändern. Was gestern ein sehr sicheres Netzwerk war, könnte heute voller Lücken sein, trotz der besten Hardware- und Sicherheitsrichtlinien. Automatisierte Schwachstellen-Scans ermöglichen Ihnen, regelmäßig Ihre gesamte IT auf Verwundbarkeiten zu analysieren. Nur wer seine Schwachstellen kennt, kann diese auch beheben!

ANGRIFFE ENTDECKEN UND ANALYSIEREN

Über das Internet sind Systeme weltweit erreichbar. Kriminelle Organisationen und Hacker haben es daher in der virtuellen Welt weitaus leichter Angriffe durchzuführen, als dies physisch möglich ist. Cyber-Crime hat sich mittlerweile zu einem Geschäftsmodell entwickelt. Intelligente Intrusion Detection (IDS) Systeme überwachen und analysieren die Aktivitäten in einem Netzwerk. Diese Systeme können sowohl typische Angriffs-Muster erkennen, als auch Anomalien aufspüren, und Verletzungen der Unternehmensrichtlinien feststellen. IDS-Systeme erzeugen meist eine Vielzahl an Fehlalarmen. Durch die übergreifende Auswertung verschiedenster Datenquellen können diese Fehlalarme bei USM meist vermieden werden.

T · · Systems ·

„UNIFIED SECURITY“ - VORSPRUNG DURCH INNOVATION, TRANSPARENZ UND KOMPETENZ

ANOMALIEN IM NETZWERK ERKENNEN.

Jedes Netzwerk wird für verschiedenste Applikationen und Dienste genutzt. Durch eine ständige Analyse des Netzwerkverkehrs ist es möglich, stark veränderte Datenströme zu identifizieren. Kombiniert mit Log-Informationen oder Meldungen aus dem Intrusion Detection System können Angriffe oder unauthorisierte Datenübertragungen leichter erkannt werden.

ASSETS BEWERTEN.

IT-Netzwerke beinhalten meist eine Vielzahl an Systemen. Nicht selten sind einige davon weder dokumentiert, bekannt ist, welcher Mitarbeiter diese Systeme betreut. USM stellt einerseits die Möglichkeit zur Verfügung, nicht dokumentierte Systeme entdecken zu können. Ebenso kann jeder Komponente eine Kritikalität zugewiesen werden, die in weiterer Folge in die Bewertung von entdeckten Sicherheitsproblemen mit einfließt.

LOGDATEN ANALYSIEREN.

85% aller Angriffe hinterlassen eindeutige Spuren in Logfiles. Meist werden diese jedoch nicht erkannt, da die große Anzahl an dezentralen Log-Daten eine zentrale Speicherung und Analyse erfordert. USM bietet Ihnen eine zentrale Logfile-Analyse sowie Archivierung. Zusätzlich werden alle entgegengenommenen Log-Files auf Sicherheitsprobleme analysiert. So können beispielsweise auch verteilte Angriffe direkt aus dem internen Netz auf mehrere Systeme schnellstmöglich entdeckt werden.

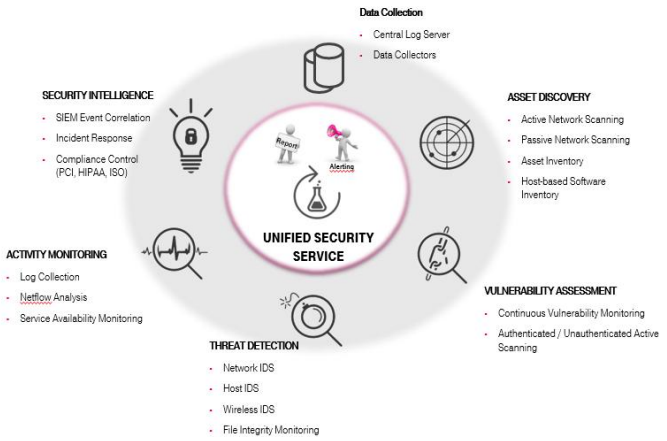
SECURITY BIG DATA ANALYSE.

Angriffe zu erkennen, ist vielfach die Suche nach der Nadel im Heuhaufen. Terrabyte von Daten werden täglich über das Netzwerk übertragen. Angreifer versuchen auch häufig, ihre Angriffe in einer Vielzahl an Verbindungsversuchen zu verstecken oder diese zu tarnen. Ebenso sind Virenscanner heute meist nicht mehr in der Lage die sich ständig verändernden Trojaner, Würmer und Viren durchgängig zu erkennen. Durch die übergreifende Analyse verschiedenster Datenquellen ist es mit Unified Security Management möglich, „echte“ Angriffe sowie eine Schadsoftware, die eine Verbindung zu einem Command & Control-Server aufbaut, zu erkennen und darauf reagieren zu können.

FLEXIBILITÄT

Die Lösung Unified Security Management ist entweder als Cloud-Service oder als eigene Installation am Kundenstandort zur Verfügung. Durchgängige Skalierbarkeit gewährleistet eine bestmögliche Anpassung an die Anforderungen des Kunden.

UNIFIED SECURITY MANAGEMENT.



KOMPETENZ & SERVICE.

T-Systems verfügt über viele Jahre Erfahrung im Betrieb hochkomplexter IT-Landschaften. Diese Erfahrungswerte fließen in Form von optimierten Konfigurationen und bestmöglichen Implementierungsformen auch in unsere Sicherheits-Lösungen ein. Mit dem Security Operations Center steht eine 7x24 besetzte und erreichbare Service-Stelle zur Verfügung, die Sie im Fall von Sicherheitsvorfällen unterstützt und Vorfälle bewertet.

DAS WICHTIGSTE AUF EINEN BLICK

- **Schwachstellen Scans** ermöglichen die Erkennung und Behebung von Sicherheitsproblemen
- **Intrusion Detection Systeme** erkennen Angriffe auf die eigene IT-Infrastruktur
- Durch eine **Anomalie-Analyse** des Netzwerk-Verkehrs können abnormale Datentransfers erkannt werden
- Regelmäßige **Asset-Analysen** ermöglichen die Erkennung unauthorisierter IT-Komponenten im Netzwerk.
- Die Nutzung aller verfügbaren **Datenquellen** ermöglicht eine schnellere und genauere Erkennung von Hacker-Angriffen und damit eine rasche und zielgerichtete Reaktion darauf.
- **USM** ist entweder als Cloud-Service, als auch als eigene Installation am Kundenstandort verfügbar.

HABEN SIE NOCH FRAGEN?
Internet: www.t-systems.de/security
oder schreiben Sie eine E-Mail an
security-info@t-systems.at

EXPERTENKONTAKT
T-Systems Austria GesmH
Thomas Masicek
Head of Security Management
thomas.masicek@t-systems.at

HERAUSGEBER
T-Systems Austria GesmbH
Rennweg 97-99
1030 Wien