ADVANCED CYBER DEFENCE BY TELEKOM

Proaktive Gefahrenabwehr in Echtzeit

WISSENSBASIERTES SICHERHEITSMANAGEMENT

Mehr und mehr Unternehmen sehen sich hochprofessionellen Langzeitangriffen ausgesetzt. Sie bedrohen die gesamte Wertschöpfung von der Produktentwicklung bis zum Aftersales. Während die Angreifer zum Teil monatelang unerkannt bleiben, gewinnen sie Zugang zu dem Wissen, über das sich die Unternehmen von ihren Wettbewerbern abheben. Topziel dieser Advanced Persistent Threat (APT) genannten Angriffe sind international tätige Großkonzerne.

Herkömmliche, das heißt ereignisgetriebene Schutzkonzepte halten mit dem komplexen Vorgehen der Angreifer nicht mit: Wer das Verhalten von Netzwerk und IT-Systemen nicht Kontextbezogen und in Echtzeit überwacht, hinkt APT-Angriffen fortwährend hinterher. Um diese ebenso riskante wie frustrierende Verfolgerrolle zu überwinden, brauchen die Verantwortlichen ein wissensbasiertes Sicherheitsmanagement, das alle relevanten Informationen verknüpft und in Echtzeit auswertbar macht.

ANGRIFFE IM ANSATZ BEKÄMPFEN

Mit den Advanced Cyber Defense-Diensten (ACD) von T-Systems gewinnen Unternehmen die Fähigkeit, mit professionellen Angreifern wieder auf Augenhöhe zu sein. Die erkenntnisbasierten ACD-Dienste bilden die gesamte Sicherheitskette ab – von der Prävention über die Entdeckung und Aufklärung bis zur Vorfallsbehandlung. Im Zentrum der Arbeit steht das Next Generation Security Operation Center (NG SOC). Das NG SOC trägt Informationen zu allen relevanten Angriffsszenarien zusammen. Nach innen gerichtet untersuchen die im NG SOC tätigen Sicherheitsexperten, welche Unternehmenswerte wie viel Schutz brauchen, an welchen Stellen die unterstützenden IT/TK-Systeme angreifbar sind und angegriffen werden. Nach außen gerichtet klären die SOC-Experten die Motive, Methoden und Werkzeuge potenzieller Angreifer auf. Somit erkennen sie relevante Szenarien, noch bevor sie zum Einsatz kommen.

Mit diesem Wissen können die SOC-Experten den gesamten Datenverkehr des Unternehmens auf Anomalien untersuchen. Die umfassende Big Data-Analyse erfolgt gesetzeskonform und wo erforderlich anonymisiert. Erweist sich eine Anomalie als sicherheitsrelevant, bekämpft das NG SOC den Angriff im Initialstadium und begrenzt seine Wirkung auf ein Minimum.

T · · Systems ·

PROVIDERÜBERGREIFENDES LAGEBILD

Das NG SOC stützt sich auf eine Big Data-Umgebung, in der sich die gesamte Anwendungs- und IT-Landschaft und die Netzkommunikation des Kunden in Echtzeit überwachen lässt. Um entscheiden zu können, ob es sich bei einer Anomalie um einen Angriff handelt, erhalten die SOC-Experten Einblick in den Kontext der Anomalie. Hierzu restauriert das NG SOC eine Vielzahl von Daten, die bei unterschiedlichen Providern liegen können. Die Multiprovider-Sicht ist erforderlich, da Großkonzerne das Management von IT-Diensten, wie z. B. Netzen, Middleware oder Anwendungen, typischerweise an mehrere Dienstleister vergeben. T-Systems führt die entsprechend aufgetrennten Daten wieder zusammen und verschafft den SOC-Experten ein vollständiges Lagebild.

WAHLFREIHEIT

Das Advanced Cyber Defense-Portfolio umfasst 12 Dienste, die sich einzeln oder in Kombination nutzen lassen. Unternehmen können wählen, ob sie ein NG SOC von T-Systems aufbauen und betreiben lassen oder ob sie ihr bestehendes SOC durch den Zukauf einzelner ACD-Dienste stärken.

Das ACD-Portfolio adressiert drei zentrale Aufgabengebiete:
1. Prozess-/Architekturgestaltung und -integration
2. Experteneinsatz und Wissen
3. Betrieb von SOC-Systemen.

1. PROZESS-/ARCHITEKTURGESTALTUNG UND -INTEGRATION

1. 1 Strategy & Roadmap
T-Systems überprüft das bestehende Cyber-Sicherheitsmanagement des Kunden. Der Kunde erhält belastbare Informationen, inwieweit er relevanten Bedrohungen technisch und organisatorisch gewachsen ist.

1.2 Next GenSOC Design & Implementation
T-Systems klärt in einem umfassenden Vorgehensmodell, wie sich das NG SOC in die bestehende IT/TK-Sicherheitsarchitektur des Kunden einbetten lässt. Gleichzeitig schlüsselt das Modell die personelle und technische Ausstattung des NG SOC auf.

1.3 Security Operations Management
T-Systems Experten konzipieren und pilotieren den Einsatz eines Expertensystemen für Security Operations Management in einer vom Kunden definierten Umgebung.

1.4 Vulnerability & Risk Management
T-Systems zeigt kundenspezifisch auf, welche Berichtspflichten sich aus IT/TK-Sicherheitsvorfällen ergeben und wie sich die damit einhergehenden Compliance-Abläufe im Unternehmen aufsetzen lassen.

1.5 Penetration Testing
T-Systems greift die geschäftskritischen IT/TK-Lösungen des Kunden mit fortge-schrittenen Methoden an. Der Kunde erfährt, ob sein bestehendes SOC die An-griffe erkennt. Zudem erhält er eine Schwachstellenanalyse zu den IT/TK-Systemen, die er im Einsatz hat.

2. EXPERTENEINSATZ UND WISSEN

2.1 Cyber Threat Intelligence
Der Kunde erhält aktuelle Informationen über relevante Angreifer und ihr Vorgehen. Gleichzeitig gibt T-Systems Empfehlungen zur Gefahrenabwehr.

2.2 Incident Response
Sicherheitsexperten von T-Systems unterstützen das SOC des Kunden bei Sicherheitsvorfällen aus der Ferne und vor Ort.

2.3 Forensics
Im Falle eines entdeckten Vorfalls rekonstruieren Experten von T-Systems das Vorgehen der Angreifer und deren Ziele.

3. BETRIEB VON SOC-SYSTEMEN

3.1 Security Incident Detection & Response
T-Systems stellt alle personellen NG SOC-Ressourcen, um rund um die Uhr Sicherheitsvorfälle zu entdecken, aufzuklären und professionell zu lösen.

3.2 Cyber Situational Awareness
Die SOC-Experten von T-Systems erschließen kundenspezifisches Wissen zu relevanten Cyber-Bedrohungen. Hierbei ergänzen sie die Informationen offener Quellen durch den bilateralen Austausch mit IT/TK-Produktherstellern, Sicherheitsorganisationen und den Computer Emergency Response Teams (CERTs) anderer Unternehmen.

3.3 SOC Content Engineering
Werden neue Angriffstechniken aufgeklärt, erstellt T-Systems neue bzw. veränderte Regeln und Verfahrensweisen zum Umgang mit den damit einhergehenden Sicherheitsvorfällen. Diese Best Practices beschleunigen die Vorfallsbehandlung und begrenzen die Abwehrkosten auf ein Minimum. Insbesondere werden so die Fähigkeiten des NG SOC kontinuierlich den weiterentwickelten Angriffsmethoden und -techniken angepasst.

3.4 SOC Platform Operations
T-Systems hostet und betreibt sämtliche Systeme, auf die das Advanced Security Operations Center seine Arbeit stützt.

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

EXPERTENKONTAKT
T-Systems International GmbH
Dr. Karl-Friedrich Thier
Deutsche-Telekom-Allee 7
64295 Darmstadt

HERAUSGEBER
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt
Deutschland

Stand 2/2014 | Änderungen und Irrtümer vorbehalten