Mit dem Intel Security „Threat Defense Lifecycle“ gegen aktuelle IT-Sicherheitsrisiken

intel Security | solutionIT

Abwehr gezielter Angriffe – die Zeit ist reif für ein adaptives Sicherheitsmodell

In einer umfassenden Sicherheitsumfrage[1] deckte Intel® Security unter Sicherheitsverantwortlichen die Hürden und Chancen auf, die Spezialisten bei der Analyse gezielter Angriffe sehen. Vor dem Hintergrund immer größerer Angriffsflächen und der Industrialisierung der Internetkriminalität wurde offengelegt, dass Sicherheitsteams mit der schieren Zahl immer neuer Bedrohungen meist überfordert sind.

Die Umfrage zeigte auch, dass sich die Befragten darüber bewusst sind, dass sie ihre Effizienz steigern würden, wenn sie eine verbesserte Erkennung mithilfe von besseren Analysen sowie Schulungen erreichen könnten. Auch wünschen sie sich eine engere Vernetzung der Sicherheitsdaten mit den Systemen, welche die IT-Infrastruktur betreibt, um die Zusammenführung von Sicherheits- und Betriebsdaten sowie Prozessen zu erleichtern. Ferner wurde offenkundig, dass bei den meisten Erkennungs- und Korrekturmaßnahmen Spezialisten-Knowhow mit Tools und Daten kombiniert werden.

Was also bremst die Sicherheitsteams?

Das Thema IT-Sicherheit wurde bisher in Unternehmen oft nur als notwendiges Übel mit einigen wenigen Metriken und einer begrenzten Risikoanalyse behandelt. Sicherheitsprojekte wurden nur im Kontext eines bestimmten Problems ausgewählt, implementiert und betrieben: Schutz, Erkennung, Korrektur und (separat) Compliance. Im Gegensatz zu anderen langfristigen Infrastrukturen in der IT beinhalteten Sicherheitsprodukte bis vor Kurzem weder ein allgemeines Datenfreigabemodell, noch eine Messaging-Infrastruktur oder eine effiziente Möglichkeit, Prozessintegrationen arbeitsgruppenübergreifend zu verknüpfen oder zu verwalten.

Statt dessen wählten Desktop-, Netzwerk- oder Compliance-Kunden Sicherheitsprodukte aus, ohne einen bewussten Plan für die erforderliche Integration, Datenfreigabe oder Widerstandsfähigkeit zu haben, um den immer komplexeren Bedrohungen gerecht zu werden. Die Produkte wurden nur rudimentär verwaltet und ausgetauscht, sobald die Verträge ausliefen. Auf veränderte Geschäftsabläufe und Technologien wurde nicht reagiert. Eine schnelle Einrichtung und Wartungsfreiheit waren gängige Prämissen für bestimmte Sicherheitskomponenten.

[1]Tackling Attack Detection and Incident Response (Research and Analysis by Intel Security and ESG)

Wenn Sie Ihr Unternehmen in dieser Beschreibung wiedererkennen, sollten Sie davon ausgehen, dass Angreifer genau diesen veralteten Ansatz gegen Sie verwenden. Die Angreifer haben schon mehrfach bewiesen, dass punktuelle Produktentscheidungen ein Vakuum erzeugen und dieses für gezielten Angriffe nutzen.

Der Lebenszyklus zur Bedrohungsabwehr

Intel Security empfiehlt, die Schutz-, Erkennungs- und Korrekturschritte zur Bedrohungsabwehr zu verknüpfen, um ein umfassendes Sicherheitsmodell für den Kampf gegen gezielte Angriffe aufzubauen.

Jede Phase besitzt zwar ihre eigenen taktischen Methoden, arbeiten jedoch zusammen, wenn es um die Bereitstellung des Kontexts und die Nutzung von Erkenntnissen geht. Dieses Konzept – ein adaptives Sicherheitsmodell – wendet Erkenntnisse in der gesamten gemeinsamen Architektur an und bietet damit die erforderliche umfassende Internetsicherheit, um Gegner auszuschalten, Eindringungsversuche schneller einzudämmen und finanziellen Schaden abzuwenden.

Wenn Sie Ihre Schutz-, Erkennungs- und Korrekturaufgaben effizienter wahrnehmen möchten, prüfen Sie Ihr Sicherheitsprogramm darauf, wie gut es als „System“ funktioniert. Ist es ein Netzwerk aus separaten Komponenten oder ein integriertes, durchgängig verfügbares Hochleistungssystem? Wie gut sind die einzelnen Prozesse miteinander vernetzt und wie gut ergänzen sie sich gegenseitig? Arbeitet es in einer geschlossenen Dauerschleife? Gibt es einen Informationsaustausch zwischen den einzelnen Produkten?

Erfahren Sie mehr, wie Sie im Zuge der Optimierung Ihrer Schutz-, Erkennungs- und Korrekturschritte Ihren IT-Betrieb und Ihre Sicherheitskontrollen in einer flexiblen, zunehmend automatisierten Architektur vereinen können: bit.ly/1ViQExK

Der Lebenszyklus zur Bedrohungsabwehr

Kontinuierliche Abwehr von Bedrohungen durch „Schützen. Erkennen. Korrigieren“

Schützen

Wirksame Abwehr von bekannten und unbekannten Bedrohungen sowie Verhinderung derer Verbreitung.

Erkennen

Herausfiltern von unauffälligen bzw. versteckten Bedrohungen durch hochentwickelte Analysemöglichkeiten.

Korrigieren

Gezieltes Korrigieren von Problemen durch Priorisierung als Teil einer kontinuierlichen Recherche.

Lernen/Anpassen

Erkenntnisse durch integrierte Sicherheit unmittelbar umsetzen.

Intel Security Innovation Alliance (SIA)

Integration von Sicherheitstechnologien anderer Anbieter

Datenschutz

McAfee Complete Data Protection
Mehrstufiger Schutz dank Verschlüsselung zur Erfüllung von Compliance-Vorgaben.

McAfee Device Control
Verhinderung der nicht-autorisierten Nutzung von Datenträgern.

McAfee DLP Endpoint
Integrierter Datenschutz für Endgeräte.

Weitere McAfee DLP-Lösungen:
McAfee DLP Discover, McAfee DLP Monitor und McAfee DLP Prevent

Datenbanksicherheit

McAfee Data Center Security Center for Databases
Zuverlässiger Echtzeitschutz für geschäftskritische Datenbanken.

McAfee Vulnerability Manager for DB
Schwachstellen-Management für Datenbanken.

Web-Sicherheit

McAfee Web Gateway
Schützt alle Aspekte des Web 2.0-Datenverkehrs, inkl. leistungsstarker Web-Filterung und proaktiven Anti-Malware-Schutz.

Endgerätesicherheit

McAfee Complete Endpoint Protection
Zuverlässiger Schutz für alle Endgeräte.

McAfee MOVE AntiVirus
Optimierter Virenschutz für virtuelle Umgebungen.

McAfee Application Control
Blockiert nicht-autorisierte Anwendungen und Code auf Servern, Desktops sowie Fixed Function Devices.

McAfee Change Control (File Integrity Monitoring)
Verhindert nicht-autoriserte Veränderungen auf Clients und Servern.

Netzwerksicherheit

McAfee Network Security Platform
Echtzeitabwehr von Angriffen sowie Schutz vor Zero-Day- und DDos-Angriffen, Botnetzerkennung sowie umfangreicher Malware-Schutz auf Netzwerkebene.

Intel Security Controller
Schafft eine Abstraktionsebene zwischen Sicherheitsinfrastruktur und Virtualisierungsverwaltung der Softwaredefinierten Infrastruktur (SDI) im Rechenzentrum.

Cloud-Sicherheit

McAfee Public Cloud Security Suite
Bietet Unterstützung bei der Durchsetzung sowie Verwaltung von Sicherheitsrichtlinien für Server in der öffentlichen Cloud (darunter AWS, Microsoft Azure)

Endgerätesicherheit

McAfee Active Response
Ein Erkennungs- und Reaktions-Tool für hochentwickelte Bedrohungen (inklusive APTs) auf Endgeräten.

Netzwerksicherheit

McAfee Advanced Threat Defense
Führt dynamische sowie statische Analysen potenziell gefährlicher Objekte in einer anwenderspezifischen, virtuellen Umgebung durch (Sandboxing).

Sicherheits-Management

McAfee ePolicy Orchestrator
Zentrale Management-Konsole zur Optimierung und Kontrolle der gesamten IT-Sicherheit.

McAfee ePO Deep Command
Bietet per Fernzugriff abgesicherte Sicherheitsverwaltung für ausgeschaltete oder defekte Computer.

SIEM & Log-Management

McAfee Enterprise Security Manager
Echtzeitüberblick über sämtliche Aktivitäten auf Systemen, Netzwerkkomponenten, Datenbanken und Anwendungen sowie Korrelation der Events zur Bedrohungserkennung und Risiko-Management.

McAfee Enterprise Log Manager
Revisionssichere Speicherung und Verwaltung von Original-Log-Dateien.

Sicherheits-Management

McAfee Threat Intelligence Exchange
Optimiert die Erkennung und Reaktion auf Bedrohungen (inklusive Advanced Persitant Threats).

McAfee GTI

Cloud-basierter Dienst zur Bedrohungsanalyse in Echtzeit

Complete Endpoint Protection Suites

Produkt	Kleine Unternehmen	Mittelständische & Groß-Unternehmen			
	Endpoint Protection for SMB Essential (TSH)	Endpoint Protection Suite (EPS)	Endpoint Protection Advanced (EPA)	Complete Endpoint Protection – Business (CEB) (bis zu 2.000 Nodes)	Complete Endpoint Protection – Enterprise (CEE)
ePO (on premise)	✔	✔	✔	✔	✔
ePO Cloud	✔				
Desktop & Server Anti-virus	✔	✔	✔	✔	✔
Email Server Anti-virus		✔	✔	✔	✔
Desktop Firewall	✔	✔	✔	✔	✔
Endpoint URL + Web Filtering	✔	✔	✔	✔	✔
Host IPS for Desktops	✔ limitiert		✔	✔	✔
Device Control	✔	✔	✔	✔	✔
Desktop Policy Auditing			✔		
Full Disk Encryption (Windows & Mac)				✔	
File & Rem Media Encryption (Windows & Mac)				✔	
Native Encryption Management				✔	
Multi-platform AV (Linux/Unix/Mac)	✔ nur MAC	✔	✔	✔	✔
Anti-virus for Storage Servers				✔	
Anti-virus for SharePoint				✔	
Application Control for Desktop					✔

Threat Intelligence Exchange (TIE) ist nicht in einer der Suites enthalten und muss separat erworben werden

Complete Data Protection Suites

	McAfee Complete Data Protection – Advanced (CDA)	McAfee Complete Data Protection (CDB)	McAfee Complete Data Protection – Essential (CDE)
Data Loss Prevention			
Data Loss Prevention Endpoint	✔		
Device Control	✔		
Full Disc Encryption			
Drive Encryption – for Windows	✔	✔	
Management of Native Encryption – for FileVault & BitLocker	✔	✔	✔
File, Folder & Removable Media			
File & Removable Media Protection – for Windows	✔	✔	✔
Management and Intel vPro Support			
ePO Deep Command – for Intel vPro and Intel AMT	✔	✔	
ePolicy Orchestrator – deployed on ePO Server only	✔	✔	✔
End User Password Recovery App			
Endpoint Assistant App* – for iOS and Android	✔	✔	✔

Complete Server Security Suites

	McAfee Server Security Suite Essentials	McAfee Server Security Suite Advanced
VirusScan Enterprise (VSE)	✔	✔
VirusScan Enterprise for Linux (VSEL)	✔	✔
VirusScan Command Line	✔	✔
MOVE AV for Servers	✔	✔
MOVE Scheduler	✔	✔
Host IPS for Servers	✔	✔
Deep Defender for Servers	✔	✔
Data Center Connector for VMware vSphere	✔	✔
Data Center Connectors for AWS, OpenStack, Microsoft Azure	✔	✔
ePolicy Orchestrator	✔	✔
Application Control for Servers		✔
Change Control for Servers		✔
McAfee Agentless Firewall		✔

Über Intel Security

Intel Security verbindet die Erfahrung und das Know-how von McAfee mit der Innovationsstärke und bewährten Leistungsfähigkeit von Intel, um Sicherheit zu einem wesentlichen Bestandteil jeder Architektur und jeder Computerplattform zu machen. Mit seinem integrierten Sicherheitssystem unterstützt Intel Security durch starken Schutz, hervorragende Erkennung und schnelle Behebung Unternehmen bei der Bedrohungsabwehr. Dank Vernetzung der Architektur und zentraler Verwaltung wird die Komplexität verringert und die betriebliche Effizienz der gesamten Sicherheitsinfrastruktur gesteigert.

McAfee Data Exchange Layer (DXL)

McAfee DXL vereint getrennte Technologielösungen verschiedener Anbieter und ermöglicht so eine sofortige Kommunikation und Zusammenarbeit. Dabei verbindet diese bidirektionale, offene Kommunikationsplattform Ihre Sicherheitslösungen zu einem zentralen Ökosystem.
Weitere Informationen: http://intel.ly/1ROBM5Z

McAfee Global Threat Intelligence (GTI)

Auf Grundlage von Millionen Sensoren weltweit und der Arbeit eines großen Forschungsteams veröffentlicht McAfee Labs über McAfee GTI zeitnah relevante Informationen zu Bedrohungsaktivitäten. Durch die direkte Integration von McAfee GTI in die Sicherheitsprodukte von Intel Security sind Systeme unmittelbar vor neuen Bedrohungen geschützt, der Arbeitsaufwand wird verringert und die Zeit zwischen Erkennung bis zur Eindämmung wird verkürzt.
Weitere Informationen: http://intel.ly/1UMiCQX

Intel Security Innovation Alliance (SIA)

Die Intel Security Innovation Alliance ist ein Programm für Technologiepartnerschaften, die die Entwicklung interoperabler Sicherheitsprodukte beschleunigt, die Integration dieser Produkte in komplexe Kundenumgebungen vereinfacht und Lösungen zur Maximierung des Wertes bestehender Kundeninvestitionen bereitstellt.
Weitere Informationen: http://intel.ly/1W2vnFx

solutionIT

solutionIT GmbH
Hindenburgstr. 49
D-23843 Bad Oldesloe

Tel.: +49 (0) 45 31 - 66 777-10
Fax: +49 (0) 45 31 - 66 777-39
E-Mail: vertrieb@solutionit.de
www.solutionit.de

Die hier enthaltenen Informationen werden Intel Security-Kunden ausschließlich für Fort- und Weiterbildungszwecke bereitgestellt. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern und werden wie besehen zur Verfügung gestellt, ohne Garantie oder Gewährleistung auf die Richtigkeit oder Anwendbarkeit der Informationen zu einem bestimmten Zweck oder für eine bestimmte Situation. Intel und die Intel- und McAfee-Logos sind Marken der Intel Corporation oder von McAfee, Inc. in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.