3/2014

ISSN 2198-0527

CP CRISIS PREVENTION

Das Fachmagazin für Innere Sicherheit, Bevölkerungsschutz und Katastrophenhilfe

IT-SICHERHEIT

Brandschutz

BOS-Digitalfunk

Krisenmanagement IT

digitalDefense - IT Sicherheitsmonitoring

Kleine Ursache große Wirkung! So lassen sich IT Sicherheitsprobleme meist beschreiben. Bereits kleinste Fehler können für IT Infrastrukturen verheerende Folgen haben. Wir wissen von Cyber-Attacken, Hackerangriffe, Spionage und Viren. Denken wir an gekoppelte Netze in der Sicherheitstechnik in öffentlichen Infrastrukturen. Je größer und komplexer Netze sind, desto größer sind die Herausforderungen, Angriffswege, intelligente Cyber-Attacken, Malware Outbrakes sowie Fehler zeitnah zu erkennen. Stefan Bächer, IT Security Consultant und Geschäftsführer von digitalDefense hat in Verbindung mit der Lösung von Tenable Network Security, dem Pionier des Nessus Scanner folgende Strategie entwickelt:

Strategie Teil 1: Analyse der Schwachstellen

digitalDefense erfasst die Schwachstellen in einer Active/Passive-Analyse. Dabei werden die IP Adressen gescannt und auf Verwundbarkeit und Verhalten analysiert (digitales Profiling). Gleichzeitig werden von vorhandenen IT Sicherheitssystemen Logs erfasst und korreliert. All diese Erkenntnisse gehen in die Bedrohungsanalyse ein. Am Ende des Tages liefert die Lösung aus diesen Ergebnissen eine Bedrohungslandkarte in Verbindung mit der Kritikalität. Die Kritikalität liefert die Idee, mit welchen analysierten Sicherheitsproblemen man sich zuerst beschäftigt (Priorisierung) und wie die kritischen Schwachstellen in der IT Infrastruktur verteilt sind.
Aus den gewonnenen Erkenntnissen lassen sich dann genaue Verfahrensanweisungen ableiten, die sowohl für die organisatorische IT Sicherheit als auch für zuständige Fachabteilungen von größter Bedeutung sind. Somit lassen sich genaue Verfahrensanweisungen delegieren, überwachen und die Strategie für die richtige Gefahrenabwehr in kürzester Zeit entwickeln.

Strategie Teil 2: Die Gefahrenabwehr - Vorbereitung der IT auf Angriffe!

Eine Organisation auf Angriffe vorbereiten unterscheidet sich deutlich von traditionellen Lösungen, die nur Sicherheitsmängel verwalten. Dabei kommt der Kombination aus aktiven und passiven Scannen eine bedeutende Rolle zu: Die Kombination von aktiven und passiven Scannen liefert dafür ein klares Bild und schärft das digitale Profiling der Schwachstelle in besonderer Weise.
Aktive Scanner, wie Nessus, besitzen Eigenschaften wie High-Speed-Schwachstellenerkennung. Weitere Eigenschaften sind Asset Profiling, agentenlose Konfigurationen und Compliance-Audits, Erkennung sensibler Daten und tiefgehende Prüfungen. All das hilft den Betreibern von IT Infrastrukturen, den allgemeinen Security-Status noch besser und vor allem zeitnah (in Echtzeit) zu charakterisieren und zu quantifizieren.
Die Kombination von aktiver und passiver Analyse bietet zudem mehr Sicherheit für Daten in jedem IPv4 oder IPv6 Netzwerk. Die Lösung ist auch in der Lage alle mit der IT Infrastruktur gekoppelten und in Verbindung stehenden mobilen Geräte in die Analyse mit einzubeziehen. Dies ist wichtige, um Querverweise von Sicherheitscheck mit dem Patch-Management-System des Unternehmens herzustellen.

Aufbau der Abwehrbereitschaft

Folgende Strategie liegt der Abwehrbereitschaft zugrunde.

1. Zeitnahes Detektieren von Schwachstellen
2. Anomalieerkennung
3. Korrelation der gefundenen Schwachstellen mit bekannten Exploits
4. Identifizierung von Angriffswegen
5. Konfigurations Auditing
6. Assoziierung der Exploit-Pfade mit den einzelnen Assets der IT Infrastruktur, so dass priorisiert Sicherheitslücken beispielsweise durch Patches, Firewall-Regeln oder Proxies behoben werden können.
7. Risikomanagement: Das in Verbindung bringen von Assets, administrativer und politischen Verantwortlichkeiten in einem Workflow (Prozess)

Montitoring

Um die Erkenntnisse im Blickfeld zu behalten, sorgt ein ausgefeiltes Monitoring für die Darstellung und Alarmierung der detektierten Schwachstellen. Ebenso werden tägliche Veränderungen des Netzes sichtbar. Wie etwa die Kritikalität von Systemen in Form der in CVSS Score Darstellung, Complianceverletzungen oder Anmeldedaten, neue IP Adressen im Netz, ect.
Zudem werden Datenbewegungen erkannt, die wiederum dem DLP (Data Loss Prevention) - Prozess zugeführt werden können. Die dabei entstehenden Reports beantworten neben den Grundfragen und Trends auch individuelle Sicherheitsmomente, die ohne dieser Methodik im „Rauschen" untergehen würden.

Praxis

In der Praxis ziehen sich Audit- und Monitor Projekte in die Länge. Die zugrunde liegende Lösung von Tenable Security Center CV zeigt, dass sich damit in wenigen Tagen eine vollumfassendes IT Security Monitoring auf Basis der Schwachstellenanalyse etablieren lässt. Der Grund für Projektverzögerungen liegen meist darin, dass keine strukturierten Daten über die Infrastruktur in der Planungsphase vorhanden sind. Aus diesem Grund empfiehlt Stefan Bächer von digitalDefense vor Projektbeginn einen eintägigen Workshop, mit dem die Planungsdaten erhoben werden, um Planungsfehler zu vermeiden. Die Lösung ist skalierbar und wächst mit der Infrastruktur. digitalDefense integrierte kürzlich erfolgreich die Korrelation mit HoneyPots (SecXtreme), welche in Behördennetzen gerne zur Angriffserkennung eingesetzt werden.

Fazit

Die Architektur der Lösung unterstützt die Strategie leitende Mitarbeiter und IT-Manager bei ihren täglichen Entscheidungen, im Krisenmanagement und im Betrieb.
Im Krisenfall müssen zeitnahe Bewertungen der Bedrohungslage in Form der Schwachstellenerkennung zu den IT-verantwortlichen Stellen gelangen (Techniker und politisch sowie organisatorisch verantwortliche Stabstellen).
Im Krisenfall ist die zeitnahe Qualität der Daten von größter Bedeutung. Diesem Umstand trägt die von digitalDefense implementierten Tenable SecurityCenter/ Nessus Enterprise Rechnung. Mit über 60.000+ Plugins und täglichen Updates hält die Lösung mit den fortlaufend wachsenden Bedrohungen Schritt.

Kontakt:
digitalDefense
Information Systems GmbH
Zeppelinstr. 71-73, D-81669 München
Tel. +49 (0)89 / 452 119 29
info@digitaldefense.de
www.digitaldefense.de