canacoon Case Study

Umsetzung Malwareschutzkonzept Windows Server

Bewertung und Zitate des Auftraggebers:

„Wir wurden seit 2015 sehr gut durch das Team der canacoon in unseren IT Sicherheitsthemen begleitet und nehmen die Experten der canacoon auch weiterhin gerne in Anspruch - Empfehlung ohne Einschränkung!“

”

Der Kunde in Stichpunkten

- deutsche Finanzgesellschaft eines Automobilherstellers, die 1949 gegründet wurde
- weltweit mehrere Landesgesellschaften
- 130,1 Milliarden Euro Umsatz weltweit
- verwaltet die Finanz-, Leasing- und Mietgeschäfte des Automobilherstellers und seiner Marken

Das Unternehmen unterliegt einer Vielzahl von Regularien und Bankaufsichtsbehörden, unter anderem PCI-DSS, BaFin, EZB, MaRisk und BAIT sowie der Datenschutzverordnung (GDPR).

Die Aufgabenstellung

Unser Kunde hatte bereits ein Projekt zur Umsetzung eines ganzheitlichen und mehrstufigen Malwareschutzkonzepts gestartet. Das Projekt umfasste sowohl Produktmigrationen als auch organisatorische und prozessuale Veränderungen zur Verbesserung des Malwareschutzes insgesamt.

Es wurden bereits mehrere klassische Antiviruslösungen für die ca. 4.200 Windows Server evaluiert. Aufgrund hoher Performance Anforderungen der Online Banking Systeme hatte sich der Kunde für ein Antivirusprodukt entschieden, bei dem die Malwareprüfung in den Rechenzentren in Deutschland auf dedizierte Remote-Scan-Server ausgelagert wird. Für ca. 1.200 Windows Server in Rechenzentren im pazifischen Raum sowie in den weltweit verteilten kleinen Standorten entschied sich der Kunde (aufgrund der Bandbreiten) für ein Full-Scan-Client Antivirus Produkt desselben Herstellers, welches mit derselben Infrastruktur betrieben wird.

Für das Monitoring und Reporting sollten die beiden Lösungen an das zentrale Compliance DWH sowie zu definierende Events an das Security Information and Eventmanagement System (SIEM) angebunden werden.

Zur adäquaten Reaktion auf Events sollten zudem Reaktionspläne für beide Antivirus Lösungen definiert und implementiert werden.

Die Lösung

Die canacoon wurde mit der Planung und Koordination der Migration der Malwareschutzlösung für Windows Server beauftragt. In einem ersten Schritt wurde ein umfassendes Infrastruktur-Architektur-Konzept erstellt, das sowohl die gewachsenen Netzwerkumgebungen als auch die in einem Netzwerkzonenkonzept neu definierten Netzbereiche berücksichtigt. Danach wurde die Infrastruktur für die Malwareschutzlösungen vorbereitet und aufgebaut.

Anschließend wurden die Konfiguration und die Regelwerke des abzulösenden Produkts geprüft und in die neuen Antiviruslösungen übertragen. Die auf die Windows Server zu verteilenden Agenten wurden konfiguriert, exportiert und zur Paketierung und Verteilung mittels SCCM vorbereitet. Aufgrund der verteilten Infrastruktur mussten unterschiedliche Agenten konfiguriert und die Netzwerk-Routen zu den jeweiligen Infrastrukturkomponenten berücksichtigt werden.

Die größte Herausforderung lag darin, den Rollout so vorzubereiten, das die Zeiträume, in denen die Server aufgrund des Produktwechsels ungeschützt sind, minimal bleiben. Notwendige Firewall-, Netzwerk- und Deployment-Changes wurden vorbereitet und gut getaktet umgesetzt, damit alle Endpunkte ihre Pakete erhalten und die jeweiligen dezentral implementierten Management- sowie Remote-Scan-Server erreichen.

Zur Analyse von Events sowie einer angemessenen Reaktion auf Vorfälle wurde der ursprüngliche Auftrag zur Etablierung von Reaktionsplänen ausgeweitet und ein übergreifendes AVERT (Antivirus Emergency Response Team) eingerichtet, das alle Verantwortlichen für sämtliche Malwareschutzlösungen (Client, Server, Gateways, Exchange-Mailboxes) umfasste. Alle Antiviruslösungen wurden zudem an ein zentrales Compliance DWH angebunden, um das Monitoring und Reporting organisatorisch zu bündeln.

Im Rahmen von Vorfall Simulationen wurden im Anschluss an die SIEM-Anbindung die erstellten Reaktionspläne vom AVERT getestet. Mit diesen Tests wurde die adäquate prozessuale und organisatorische Verankerung der Antiviruslösungen überprüft.

Nach der Migration auf die neuen Lösungen und einer erfolgreichen Testphase wurde die Verantwortung an die unterschiedlichen organisatorischen Einheiten des IT-Betriebs des Kunden übergeben.