Konzeption eines Schwachstellenmanagements

Change Driver

Der Sicherheitsbeauftragte eines Handels- und Logistikunternehmens setzt sich, basierend auf dem bereits vorhandenen Information Security Management System (ISMS), konzeptionell mit dem Thema Sicherheit auseinander.

Zum einen fordern Compliance-Richtlinien eine kontinuierliche Überwachung, Risikobewertung und gegebenenfalls Aktualisierung von Systemen und Anwendungen.

Zum anderen zeigt ein Blick in aktuelle Verwundbarkeitsdatenbanken eine Zunahme von Schwachstellen in Systemen und Anwendungen. Bekannte Schwachstellen können gezielt ausgenutzt werden, bspw. mit umfangreichen Exploits (vorgefertigte Angriffsprogramme) und damit dann auch schon von Nutzern mit geringen Grundlagen-kenntnissen.

Daher ist der Sicherheitsbeauftrage auf den Aspekt der Risikominimierung fokussiert und muss das Schwachstellen- und Patch-management im Rahmen der Cyberhygiene adäquat berücksichtigen. Da diese Themen von ihm jedoch nicht vollumfänglich und zeitgerecht geleistet werden können, benötigt er Unterstützung von einem externen Dienstleister.

Damovo Approach

Damovo hat im Rahmen eines Beratungsauftrages ein Schwachstellenmanagement konzipiert, das weit über ein einfaches Patchmanagement hinausgeht.

Grundlagen sind ein konzeptioneller Ansatz, kontinuierliche Prozesse und Automatisierungen. Nur so kann der Wettlauf gegen Angreifer gewonnen werden.

Zudem werden Schwachstellen und Risikomanagement verknüpft, sodass das schwächste Glied der Sicherheitskette priorisiert angegangen werden kann. Erfolgreiche Angriffe können somit von Anfang an präventiv verhindert werden.

Basierend auf diesem konzeptionellen Ansatz kommt das Vulnerability Management (VM) von Damovo zum Einsatz, das ein Lösungsbaustein des Security Operation Center (SOC) von Damovo ist.

Customer Value

DAMOVO

So profitiert der **Sicherheitsbeauftragte**

Durch die Einführung der Vulnerability Management Lösung von Damovo wurden, im Vergleich zur bisherigen manuellen Lösung, personelle Ressourcen für andere Aufgaben freigesetzt.

Das Spannungsverhältnis zum IT-Leiter, der eine zeitnahe Beseitigung vorhandener Verwundbarkeiten fordert, konnte ebenfalls entschärft werden.

So profitiert das **Unternehmen**

Mit der Vulnerability Management Lösung wird die Widerstands-fähigkeit des Unternehmens gegen Angriffe erhöht und somit das Cyberrisiko reduziert.

Zudem lassen sich durch den Einsatz der Lösung die Anforderung von ISO/IEC 27001 und PCI DSS in diesem Bereich vollumfänglich erfüllen.