HOLM SECURITY

Schwachstellenmanagement in kritischer Infrastruktur – praktische Erfahrung aus der Tanklagerindustrie

Risiken zu beherrschen setzt voraus, dass man seine Angriffsfläche kennt. Holm Security hat Alkion Terminals, einem niederländischen Betreiber von Tanklagern, auf Basis von Holm Security VMP, eine Lösung für Schwachstellenmanagement geliefert, die es Alkion erlaubt Schwachstellen sowohl im Bereich der IT- als auch der OT-Infrastruktur zu erkennen und gezielt zu beheben. Als Betreiber von Tanklagerterminals und den damit verbundenen Risiken, ist Alkion naturgemäß ein sehr sicherheitsbewusstes Unternehmen.

"We care for the safety and health of our employees, customers, suppliers, contractors, neighbors, for the environment, for the security of our assets and have the firm belief that all incidents are preventable."[1]

Hinzukommt die Tatsache, dass Alkions insgesamt 10 Terminals über 5 Länder Europas verteilt sind. Aus einer solch verteilten Infrastruktur ergibt sich aus Sicht der IT-/OT-Infrastruktur automatisch eine größere potentielle Angriffsfläche für externe Angreifer. Die Devise lautet also die Angriffsfläche zu jeder Zeit im Blick zu haben und sie durch konsequente Schwachstellenmanagementprozesse proaktiv zu minimieren.

Heterogene Infrastruktur mit unbekannter Angriffsfläche

Alkion Terminals betreibt eine heterogene, dezentrale sowie organisch gewachsene Infrastruktur, die seit der Gründung im Jahre 2017 sehr vergrößert worden ist. Die Infrastruktur beinhaltet u.a.:

- 10 Tanklagerterminals in 5 Ländern Europas,
- eine Vielzahl von IP-Adressen und eigener Webapplikationen, sowie
- Steuerungsinfrastruktur (OT).

1 Auszug aus „SAFETY, SECURITY, HEALTH, ENVIRONMENTAL, COMPLIANCE and QUALITY POLICY" von Alkion Terminals (https://www.alkion.com/policies/)

Vor dem Einsatz der VMP Schwachstellenmanagementlösung von Holm Security, stellte diese heterogene IT-/OT-Infrastruktur für Alkion ein erhebliches Risiko dar:

- Es gab keine technische Infrastruktur, um gezielt Schwachstellen ausfindig zu machen
- Es existierte kein fortlaufender Schwachstellenmanagementprozess, um Schwachstellen einer Risikobewertung zu unterziehen, zu beseitigen und konsequent nachzuverfolgen

Aufgrund des mit einem Tanklager in Verbindung stehenden Schadenpotentials, war es für das IT-Team der Alkion unverzichtbar eine Lösung zu implementieren, die eine umfassende Kenntnis der potentiellen Angriffsfläche der IT- und OT-Infrastruktur ermöglicht.

Es ist insbesondere für Betreiber von angreifbarer kritischer Infrastruktur unabdingbar, ihre Verwundbarkeit genau zu kennen und den identifizierten Schwächen proaktiv zu begegnen.

Konsequenterweise hat das IT-Team der Alkion, ganz im Sinne des im Qualitäts- und Informationssicherheitsmanagement verankerten Prinzips der kontinuierlichen Verbesserung (Plan-Do-Check-Act), sich die Implementierung einer Schwachstellenmanagementlösung zum Ziel gesetzt. Um mehrere Anbieter und Lösungen objektiv miteinander vergleichen zu können, entschied man sich für die Durchführung einer POC (Proof of Concept) Phase.

Proof of Concept Phase

Die Proof of Concept Phase wurde für die Dauer von **6 Wochen** angesetzt und umfasste:

- die gesamte Büro-IT, inkl. aller Client-/Serversysteme (Windows und Linux)
- ausgewählte Teile der Steuerungs-/OT-Infrastruktur

Da man ein gewisses Risiko in der Durchführung von Schwachstellenscans in der Steuerungsebene sah und keine unbeabsichtigten Ausfälle von speicherprogrammierbaren Steuerungen (SPS) verursachen wollte, hat man die Durchführung der Schwachstellenscans auf eine dedizierte Testumgebung beschränkt.

Holm Security VMP – die leistungsfähigste Plattform

Nach Durchführung des POC fiel die Wahl von Alkion auf die leistungsfähigste Lösung: **Holm Security VMP.**
Die wesentlichen Gründe für die Entscheidung des Alkion IT-Teams:

- Hohe Schwachstellenerkennungsrate
- Überzeugende Abdeckung von IT- und OT-Infrastruktur
- Reibungslose Implementierung in der Alkion-Infrastruktur
- Problemlose Einrichtung der Scan-Konfiguration
- Keine eigenen Hardware-Appliances erforderlich
- Unverzügliche Umsetzung dank Cloud-basierter Bereitstellung aus Holm Security RZ in Schweden
- Qualität des technischen Supports im Zuge der POC-Durchführung

HOLM SECURITY

Auf Basis der erfolgreich absolvierten POC-Phase, ging die in der POC-Phase vollzogene Implementierung nahtlos in den regulären Produktionsbetrieb über.

Übergang in kontinuierlichen Schwachstellenmanagementprozess

Der fortlaufende Betrieb des Schwachstellenmanagements umfasst seit der erfolgreichen Durchführung des POC:

- 10 Tanklagerstandorte in 5 Ländern Europas
- eine Vielzahl von IP-Adressen und eigener Webapplikationen
- Steuerungsinfrastruktur (OT) – ca. 10% der insgesamt gescannten Infrastruktur

Die Durchführung der Schwachstellstenscans wird zentral von der IT der Alkion am Hauptsitz in Amsterdam orchestriert. Dazu zählt ebenfalls die Durchführung des mit dem eigentlichen Schwachstellenscan eng verzahnten Schwachstellenmanagementprozesses, bestehend aus Bewertung, Behebung und Nachverfolgung der erkannten Schwachstellen.

Selbst betreiben oder als Dienstleistung?

Anfänglich wurde das IT-Team der Alkion noch tatkräftig unterstützt, insbesondere bezüglich:

- der Einrichtung der Scan-Konfigurationen,
- des Deployments der virtuellen Scan-Appliances in Infrastrukturbereichen, die von außen nicht
- erreichbar sind, und
- der umfangreichen Schulung der für den fortlaufenden Betrieb verantwortlichen Mitarbeiter.

Mittlerweile betreibt Alkion die Schwachstellenmanagementplattform selbst.

Aber, es gibt auch Alternativen. Unsere Kunden entscheiden sich oftmals Schwachstellenmanagement als Dienstleistung von unseren Partnern einzukaufen, mitsamt Infrastruktur und der dazugehörigen personellen Kapazität. Diese Vorgehensweise hat einige ganz offensichtliche Vorteile, insbesondere für Unternehmen, die keine dedizierten Ressourcen für IT-Sicherheit haben:

- Schnellstmögliche Einsatzfähigkeit
- Kein langwieriger Aufbau zusätzlicher personeller Ressourcen
- Zugriff auf entsprechende technische Fachkenntnisse
- Durch Verantwortungsübernahme für Großteile des gesamten Schwachstellenmanagementprozesses, wird die zusätzliche Belastung des internen IT-Teams minimiert