SUCCESS STORY

ERFOLGE DER TECHNOLOGIE-PARTNERSCHAFT
MIT DER OPTIMA PACKAGING GROUP GMBH

sure[secure]

OPTIMA

WEBSITE

https://www.optima-packaging.com/

REGION

Schwäbisch Hall, Baden-Württemberg

BRANCHE

weltweiter Technologieführer für Verpackungsmaschinen
und Abfüllanlagen

MITARBEITER

Rund 2.650

01 DIE AUSGANGSSITUATION

Im Bereich der IT-Sicherheit gab es folgende Voraussetzungen:

Email Security As a service Lösung aus der Cloud

Firewall: „Checkpoint“ Firewall im Einsatz – war nicht voll Lizensiert – UTM (Unified threat management war nicht vorhanden)

AV Lösung Trend Micro Officescan

02 DER VORFALL

Sonntag, 20.09.2020

01

9:15 Uhr

Erste Auffälligkeiten treten auf

02

10:00 Uhr

Erste Maßnahmen zur Isolierung infizierter Bereiche

Ein Erpresserschreiben wird platziert.

03

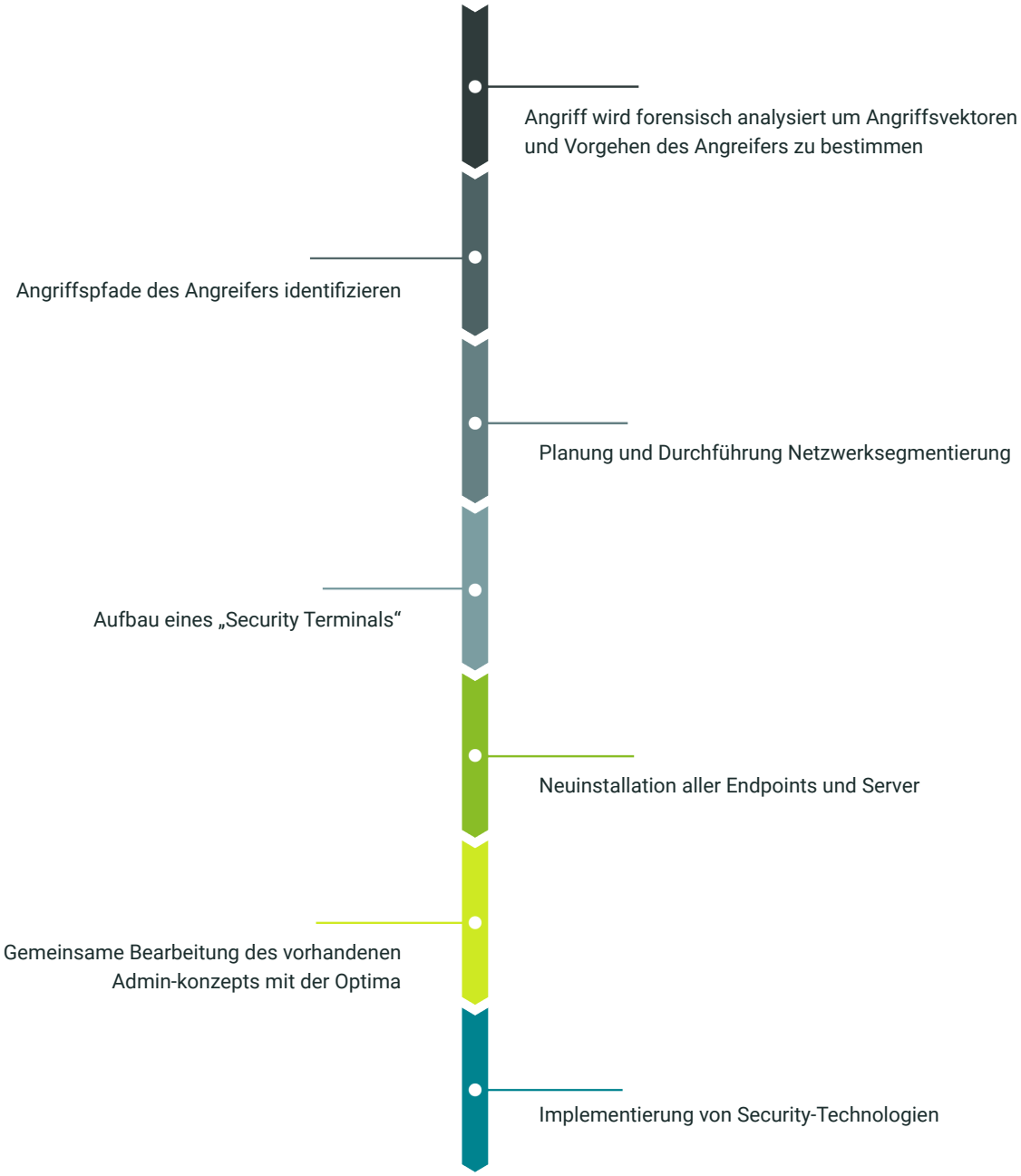
19:00 Uhr

Erstes Statusmeeting mit der suresecure GmbH

Den Sicherheitsvorfall bei der OPTIMA packaging group GmbH klassifizieren wir klar als Major Incident existenzbedrohenden Ausmaßes. Während des Vorfalls sind alle kritischen Geschäftsprozesse zum Erliegen gekommen. Als vermutlicher Point-of-Entry wurden maliziöse Excel-Dateien identifiziert, welche Mitarbeitern per E-Mail zugestellt wurden.

Die Analyse zeigt, dass hier die Malware eGregor verwendet wurde. Der Angreifer hat augenscheinlich das Ziel verfolgt, größtmöglichen Schaden anzurichten, um im Anschluss mittels einer Erpressung wirtschaftliche Vorteile zu erlangen.

03 INCIDENT RESPONSE PHASE



Einrichtung eines SOC as a Service für die 24x7 Überwachung aller securityrelevanten Events im Unternehmen.

04 DIE LÖSUNG

Zunächst wurde ein sicherer Netzbereich aufgebaut. Zentrale Datenbanken, Datenbestände und Server wurden nach umfangreicher forensischer Überprüfung in die Netzbereiche migriert. Server und Clients aus verdächtigen Netzbereichen wurden neu aufgesetzt.

Durch die eingesetzten Schutzmaßnahmen und die schnelle und direkte Reaktion der IT-Abteilung konnte das Ausmaß des Schadens deutlich reduziert werden. Aufgrund der Kombination aus der schnellen Reaktion und den vollständigen Backups kam es zu keinem relevanten Datenverlust.

Dass die Reaktion so zeitnah erfolgte, war auf den Umstand zurückzuführen, dass die Server- und Ressourcenüberwachung ausfallende Dienste und auffällige Ressourcenauslastung meldete. Durch diese Überwachung konnte die Verschlüsselung kurzfristig entdeckt und betroffene Systeme gestoppt werden.

04 DAS FAZIT

Der Vorfall bei der OPTIMA packaging group GmbH wurde vermutlich als Testobjekt für eine darauffolgende groß angelegte Kampagne der Gruppe FIN6 genutzt.

Die Analyse genutzter Angriffsobjekte und Überprüfung in übergreifenden Datenbanken zeigten in den Wochen nach dem Angriff, dass weitere Organisationen von dem Angriff betroffen waren. Außerdem wurde in den Tagen nach dem Incident weitere prominente Vorfälle u.a. bei international agierenden Unternehmen bekannt.

Die Reaktion im Incident erfolgte sehr zeitnah und in richtigem Maß. Viele der empfohlenen Maßnahmen konnten schnell umgesetzt werden, da diese sich bereits im Vorfeld des Incidents in Planung oder Konzeptionierung befanden. Teilweise wurden die Prozesse zur Umsetzung der Maßnahmen in den vergangenen Monaten bereits begonnen.

So gelang es dem Angreifer nicht die vorhandenen Backups zu löschen oder unbrauchbar zu machen. Darüber hinaus wurde die bestehende Segmentierung des Netzwerks weiterentwickelt und fortlaufend umgesetzt. Bereits segmentierte Netzbereiche, wie bspw. eine DMZ zum Internet oder die Produktionsnetze, waren von dem Angriff nach heutigem Kenntnisstand nicht betroffen.

05 UNSERE PARTNERSCHAFT

Nach diesem Incident ist die Optima packaging Group GmbH ein dauerhafter Partner geworden. Folgende Services wurden anschließend implementiert:

- Ein SOC as a Service
- Managed Security Service Standard (IT-Betriebsunterstützung) auf monatlicher Basis

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de