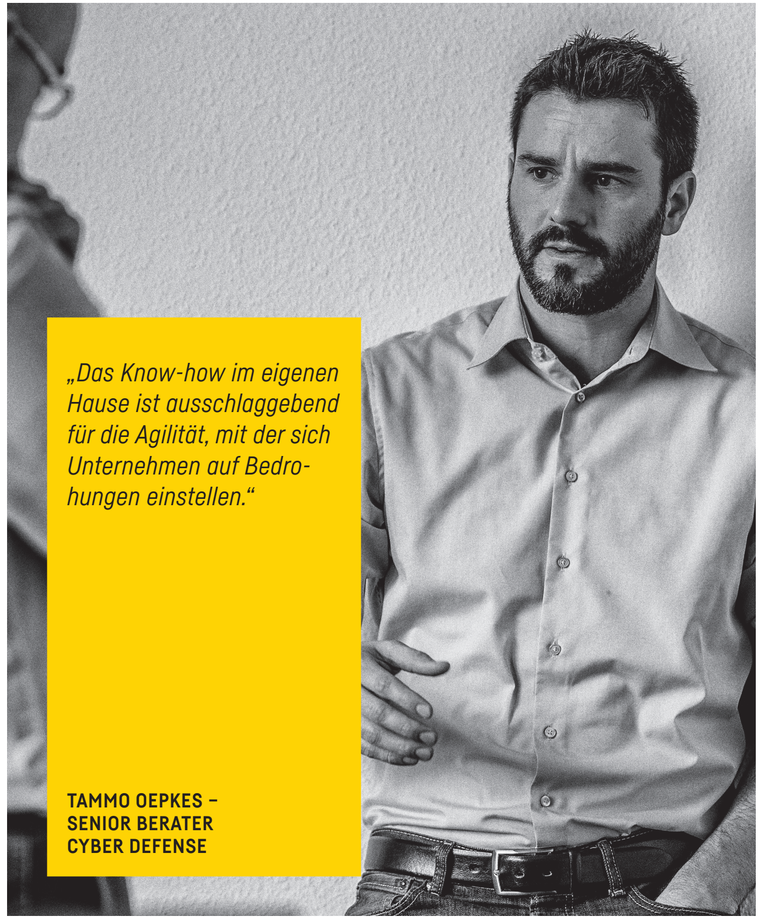
Aufbau des Cyber Defense Centers bei HP in Palo Alto



„Das Know-how im eigenen Hause ist ausschlaggebend für die Agilität, mit der sich Unternehmen auf Bedrohungen einstellen.“

TAMMO OEPKES –
SENIOR BERATER
CYBER DEFENSE

ConSecur
[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de

CS_REFERENZBERICHT

Pionierarbeit für Hewlett-Packard

ConSecur begleitet HP beim Aufbau seines Cyber Defense Centers in Palo Alto.

ConSecur
[security and consulting]

Know-how der ConSecur GmbH

Hewlett Packard setzt neue Standards in der Cyber-Abwehr. Der IT-Konzern sichert seine weltweite IT-Infrastruktur mit einem hochmodernen Cyber Defense Center (CDC) in Palo Alto vor externen und internen Cyber-Angriffen. Das CDC ist gleichzeitig als Think Tank aufgebaut, der fortlaufend Innovationen für eine sicherere digitale Welt hervorbringen wird. Für die Einrichtung des Cyber Defense Centers setzte HP auf das Know-how der ConSecur GmbH, die in einem 15 Monate andauernden Projekt auch Standards für die Auswahl und das Training der IT-Security-Analysten entwickelt hat.

Die HP-Zentrale in Palo Alto Kalifornien/USA.

Legitime Vorgänge von Cyber-Attacken unterscheiden

Die Analysten im Cyber Defense Center haben die Aufgabe, aus dieser Masse an Informationen legitime Vorgänge von Cyber-Attacken zu unterscheiden, die das gesamte weltweite HP-Netzwerk gefährden können. Im Cyber Defense Center werden deshalb sämtliche Systeme und Vorgänge erfasst und analysiert: Mit der HP eigenen „Security Information and Event Management (SIEM)"-Lösung HP ArcSight ESM identifizieren die IT-Security-Analysten Anomalien, indem sie relevante Daten korrelieren und analysieren.

Mächtige globale IT-Infrastruktur

Die globale IT-Infrastruktur von Hewlett-Packard ist mächtig. Weltweit unterhält das Unternehmen Standorte in 170 Ländern; 330.000 Mitarbeiter und Systeme kommunizieren täglich auf verschiedenen Wegen untereinander sowie mit Kunden und externen Partnern. Die Menge der Vorgänge, die täglich innerhalb der weltweiten HP-IT-Infrastruktur erzeugt wird, ist immens.

Vorzeigeprojekt Cyber Defense Center

Das Cyber Defense Center besitzt für HP über die Erkennung und Reaktion auf Cyber-Attacken hinaus auch eine strategische Bedeutung. Als Anbieter von Security Services und Produkten ist das CDC zugleich der technologische Showroom für moderne Informationssicherheit made by Hewlett Packard. HP stellt Kunden und Besuchern im Corporate Headquarter in Palo Alto vor, wie hauseigene Produkte und Lösungen zusammenwirken, um ein Höchstmaß an Informationssicherheit zu gewährleisten.

„Durch das sehr gute Trainingsangebot von ConSecur arbeiten unsere Analysten auf einem gleichmäßig hohen Qualitäts-Niveau. In der Zusammenarbeit haben wir innerhalb kürzester Zeit die Ziele erreicht, die wir uns vorgenommen haben."

MARCEL HOFFMANN, SR. MANAGER, CYBER DEFENSE CENTER, HEWLETT-PACKARD COMPANY


ENRICO HARTEMA – SENIOR BERATER CYBER DEFENSE


GUIDO STEENTJES – SENIOR BERATER CYBER DEFENSE


TAMMO OEPKES – SENIOR BERATER CYBER DEFENSE


STEPHAN ILIC – SENIOR BERATER CYBER DEFENSE

Köpfe für das Cyber Defense Center gewinnen

Im Cyber Defense Center waren innerhalb kürzester Zeit 16 Stellen mit Analysten zu besetzen. Deshalb hatte die Rekrutierung geeigneter Köpfe höchste Priorität. Da es einen klassischen Ausbildungsweg zum IT-Security-Analysten nicht gab, entwickelte ConSecur ein Verfahren zur Identifizierung geeigneter Bewerber, das Einstellungskriterien für Security-Analysten umfasst sowie ein objektives Bewertungsschema definiert.

Die ConSecur-Berater Enrico Hartema, Guido Steentjes, Stephan Ilic und Tammo Oepkes, die in Zweierteams in Palo Alto gewesen sind, haben damit eine valide Entscheidungsgrundlage für die Einstellung geeigneter Mitarbeiter geschaffen und bei der Mitarbeiterqualifizierung Pionierarbeit geleistet.

Wer bei HP im Cyber Defense Centers arbeitet, besitzt Schlüsselkompetenzen wie ausgeprägtes analytisches Denkvermögen und hohe Problemlösungskompetenz. „Ein IT-Background ist kein Einstellungskriterium", erklärt Tammo Oepkes. Heute beschäftigt HP in seinem Cyber Defense Center unter anderem einen gelernten Meeresbiologen und einen früheren Verkäufer von Apple-Produkten. „Beide bringen die Eigenschaften mit, die einen IT-Security-Analysten auszeichnen", sagt Stephan Ilic.

Ausbildungsinhalte für IT-Security-Analysten entwickelt

ConSecur entwickelte für die Qualifizierung der eingestellten IT-Security-Analysten Ausbildungsinhalte, die sie auf ihre tägliche Arbeit im Cyber Defense Center vorbereiteten. Dieses mehrmonatige ConSecur-Training umfasste Basisarbeit wie technische Grundlagen, Kommunikationsschulungen und „Hacking-Events", bei denen die Analysten die Position des Angreifers eingenommen haben.

Methodik und Analytik bildeten den zweiten Schwerpunkt der Ausbildung, in dem ConSecur die IT-Security-Analysten auch in der Threat Intelligence unterwiesen hat. Bei diesem analytischen Vorgehen werden Informationen und Daten außerhalb der eigenen Unternehmung ausgewertet, zum Beispiel aus einschlägigen Cybercrime-Foren oder publizierten Analysen von Angriffen auf andere Organisationen.

Threat Intelligence ist eine Grundlage dafür, zukünftige Bedrohungen zu identifizieren und nach Möglichkeit im Vorfeld abzuwehren.