Security Night 2022
20. Oktober 2022

// HEIDI – Das Chalet am Wiener Ring // Opernring 11 // 1010 Wien

16:00 Uhr // Registrierung & Empfang

16:30 Uhr // Unerwartetes Ereignis im neuen Jahr: Pumpstationen stehen in Flammen!

Böses Erwachen für die OPFA-Chemiewerke Raffinerien: Das Unternehmen ist offline! Aufgrund einer fehlgeschlagenen Verhandlung mit einer unbekannten Gruppe ist das Unternehmen nicht mehr in der Lage die Cloud-basierten Dienste anzubieten. Die lokale Pumpinfrastruktur gilt als unwiderruflich zerstört. Die Wiederherstellungsarbeiten werden auf mehrere Monate geschätzt. Der Energiepreis schießt laut Experten durch die Decke.

Patrick Pongratz // Raphael Szabo // Philipp Allmer
// K-Businesscom

17:20 Uhr // Was wäre gewesen, wenn ... Teil 1

Die Cyber Security Spezialisten klären auf.

Lückenlose Überwachung zum Schutz vor (un)bekannten Bedrohungen – Palo Alto Cortex XDR

Cortex XDR stellt branchenführende Funktionen zur Abwehr von Malware und Ransomware sowie exploitbasierten und dateilosen Angriffen bereit, die mittels lückenloser Überwachung auf Clients erkannt und proaktiv unterbunden werden. Der ressourcenschonende Agent der Lösung nimmt nur ein Minimum der Rechen- und Speicherkapazität des Endpunkts in Anspruch, während er erkannte Bedrohungen stoppt und zugleich Ereignisdaten für die Auswertung sammelt.

Manuel Lecher-Peham // K-Businesscom
Roman Anger // Palo Alto Networks

K-Businesscom AG

Stop dem Angriff auf Ihre Cloud Dienste – Check Point Harmony und CloudGuard

Egal ob Ihre Benutzer über SaaS Services wie Microsoft M365 und Teams ausgetrickst werden oder versucht wird Ihr Datacenter zu übernehmen, mit Check Point Cloud Guard und Harmony werden Modifikationen und Hacks erkannt und proaktiv verhindert. Ein Rundum-sorglos-Schutz gegen Zero Phishing, Zero Day Malware, Konfigurationsfehler in Cloud Accounts und OWASP Top 10 Schwachstellen.
Kevin Mühlböck // K-Businesscom
Patrik Fetter // Check Point

18:10 Uhr // Pause

18:20 Uhr // Was wäre gewesen, wenn ... Teil 2

Verdächtige OT-Aktivitäten verhindern – Cisco Cyber Vision

Cisco Cyber Vision bietet umfassende Transparenz im ICS, einschließlich dynamischer Bestandsaufnahme, Echtzeitüberwachung von Kontrollnetzwerken und Prozessdaten sowie umfassender Threat Intelligence. So können sichere Infrastrukturen aufgebaut und Sicherheitsrichtlinien zur Risikokontrolle durchgesetzt werden. Durch Cyber Vision und SecureX ist somit der Worst Case für das Unternehmen abgewandt worden.
Thomas Lampalzer // K-Businesscom
Andreas Hack // Cisco Systems

Schutz der lokalen Netze – Fortinet OT-Segmentierung

Mit einer strikten Segmentierung und der entsprechenden Technologie hätte der Angriff erkannt und die Verbindungen proaktiv auf mehreren Ebenen blockiert werden können. Die Verteidigung kann mit Details angereicherten Incident Reports auf den Vorfall reagieren und weitere unmittelbare und zukünftige Maßnahmen einleiten.
Tobias Gasior // K-Businesscom
Teemu Schaabl // Fortinet

Ab 19:10 Uhr // Expert:innen-Community & Food & Drinks