axivia

:: Workshop Informationssicherheit ::

Antimalware 2.0
Mobile Security 2.0
SSL/TLS Everywhere
Datacenter Security
Cloud Security

:: Live Demos, Live Hacking ::

zu Gast: Check Point - F5 - IMPERVA

AGENDA

9:00 Uhr: Empfang und Registrierung
9:15 Uhr: Begrüßung und Einführung

AntiMalware 2.0: Konzepte gegen Locky & Co.

:: Zero Day Malware Protection – Szenarien - Lösungen ::

- Anatomie aktueller Angriffe - Analyse der Problematik
- klassische Konzepte AV, IPS, FW an Client und Gateway
- Analyse aktueller Technik – Sandboxing = Sandboxing?
- Das SSL-Problem: Lücken, Performance, Bind Spots
- Mobile Device Security
- Forensic und Monitoring: Maßnahmen im Ernstfall

R. Klug, R. Kempf axivia GmbH

Schützen Sie ihre "Kronjuwelen" im Unternehmen:

- IMPERVA Cloud WAF & DDoS Protection
- SecureSphere: die beherrschbare Web App Firewall
- Database & File Activity Monitoring

Skyfence: wie managen Sie "Bring-your-own-Cloud“

- **Visibility & Control:** Skyfence Cloud Gateway
- **Kontrollierte Apps** wie Salesforce, Dropbox, Office365

Live Demos und Hacking, M. Dombrowski IMPERVA

10:45 Uhr: Pause

Check Point Update

:: R80 das neue Major Release – Einblicke ::

- **Management, Gateway, SmartEvent**

:: NEU: Check Point Appliances ::

- **High Performance für Threat Prevention und SSL**

12:00 Uhr: FAQ Diskussion – Ende Teil1

12:15 Uhr: Mittagessen

13:30 Uhr: Update - Was ist neu bei Check Point

NEU: Malware: Zero-Day Protection & Forensic:

- CPU Level Sandboxing Cloud – on Prem – Hybrid Architektur, Technik, Demo
  - Testen Sie Sandblast noch heute
  - Deployment im Ernstfall
- Im Ernstfall: Forensic, Loganalyse + Reaktion in Echtzeit
- Endpoint: Sandblast & Forensic Agent

Malware& Smartphones: Mobile Threat Prevention

- Situation Malware für iOS, Android, Windows Mobile
- MDM/EMM: die Grenzen von MDM und Containerization
  - SIDESTEPPER (iOS)
  - Certifigate (Android)
- Mobile Endpoint Security: Analyse & Kontrolle von
  - Apps, MITM, Endgerät

vSEC für VMware NSX:

:: nahtlose Sicherheit im Software-Defined Data Center ::

- vSEC Sicherheit gepaart mit der Micro-Segmentierung von NSX für „Ost-West“ Datenverkehr im Data Center
- umfassende Threat Prevention
- Auto-Detection, Quarantäne und Behandlung von infizierten Virtual Machines

Architektur - Arbeitsweise - Skalierung in der Demo GUI

14:30 Uhr: Pause

F5 Networks – Mobile Access – SSL - Portalsicherheit

- Übersicht F5 Portfolio
- SSL Everywhere – TLS/SSL-Verschlüsselungsprobleme zentral beherrschen
- Mobile Access, SSO: Use-Cases für den Access-Policy-Manager
- **Hacking und Demo:** Web Application Firewall
- Demo Websafe – Application Layer Encryption und Generic Malware/Web-Injection-Detection

Architektur - Arbeitsweise – „Hacking“ in der Demo GUI

Seehotel Niedernberg

Mittwoch, 08.06.2016

Beginn: 9:15 Uhr Ende: ca. 16:30 Uhr

FAX-Anmeldung: 06022 - 50872 20

Anmeldung zum axivia

Workshop Informationssicherheit

am Mittwoch 08.06.2016

Seehotel Niedernberg

Die Teilnahme ist **kostenlos**.
Jeder Teilnehmer erhält Informationsmaterial.

Name / Vorname

Firma / Position

Telefon / Telefax

E-Mail

Datum / Unterschrift

axivia GmbH - Industriering 7 - 63868 Großwallstadt 06022/50872 0 – info@axivia.de

Adresse:

Seehotel Niedernberg
Leerweg
63843 Niedernberg
Tel. +49 6028 999-0
www.seehotel-niedernberg.de

Anfahrt: