Interview mit Florian Oelmaier

Leiter IT-Sicherheit & Computerkriminalität, IT-Krisenmanagement bei Corporate Trust

Herr Oelmaier, die Corporate Trust ist Dienstleister im Bereich Unternehmenssicherheit. Zu Ihrem Spezialgebiet gehört auch das Thema Cybersicherheit. Wie stufen Sie die aktuelle Sicherheitslage ein und was empfehlen Sie den Unternehmen?
Die IT-Sicherheitslage hat sich radikal verändert. Dieser Wandel hat nicht im Bereich der IT-Sicherheitslücken stattgefunden – diese sind im Wesentlichen gleich geblieben: alte wurden geschlossen, neue gefunden. Die IT-Sicherheitsanstrengungen wurden intensiviert, dafür sind Vernetzung und Komplexität gestiegen. Der signifikante Wandel hat im Bereich der Täter und deren Motivation stattgefunden. Noch vor 10 Jahren waren die Täter Skriptkiddies und IT-Nerds, motiviert durch Geltungsbedürfnis und Selbstverwirklichung. Heute dominieren organisierte Kriminalität, Geheimdienste, Cyber-Söldner und wohl bald auch Terroristen das Geschehen. Unsere Empfehlung: Machen Sie sich bereit, auch signifikante Änderungen in Ihren Verteidigungsstrategien in Betracht zu ziehen.

Sie stellen fest, dass nicht mehr alle Bereiche eines Unternehmens gleichermaßen abgesichert werden können. Was meinen Sie damit?
Die meisten Unternehmen denken in drei Sicherheitszonen: Internet, DMZ und Intranet. Das reicht nicht mehr aus. Ein durchschnittliches Unternehmen braucht heute 6 bis 8 Zonen mit unterschiedlichem Sicherheitsniveau. Die Frage, welche Daten welchen Schutzbedarf haben, muss dabei das Business beantworten. In einer solchen Struktur werden dann auch komplexere Sicherheitslösungen wie SIEM, IDP und ein 100%-Log für die höchste Schutzzone handhab- und bezahlbar.

Wo sehen Sie die Schnittstelle zur ACP?
Die Corporate Trust – Business Risk & Crisis Management GmbH versteht sich als Berater und Partner in Krisen- und Notfallsituationen. Eine solche Krisensituation ist ein laufender Cyberangriff bzw. die Entdeckung eines bereits abgeschlossenen Informationsabflusses. In solchen Fällen ergänzen wir mit unserem Know-how rund um Angriffsaufklärung, Täterverfolgung, IT-Forensik und Krisenmanagement die ACP-Experten beim Kunden vor Ort.

TERMINE 30

30. Juli 2015
München: Workshop ACP Safebox

23. September 2015
Hauzenberg: Microsoft-Lizenzierung

24. September 2015
Regensburg: Microsoft-Lizenzierung

21. Oktober 2015
Hauzenberg: 3. Security Forum

22. Oktober 2015
Regensburg: 3. Security Forum

IHR REGIONALER ACP-KONTAKT IN DEUTSCHLAND

Bad Tölz
Tel.: 08041-799988-0
E-Mail: bad-toelz@acp.de

Frankfurt
Tel.: 06109-69691-0
E-Mail: frankfurt@acp.de

Hannover
Tel.: 0511-35777-0
E-Mail: hannover@acp.de

Hauzenberg (SWS Computersysteme AG)
Tel.: 08586-9604-0
E-Mail: info@swsnet.de

Kolbermoor
Tel.: 08061-9089-0
E-Mail: kolbermoor@acp.de

Köln
Tel.: 0221-66992-0
E-Mail: koeln@acp.de

Markdorf
Tel.: 07544-50399-0
E-Mail: markdorf@acp.de

München
Tel.: 089-358980-0
E-Mail: muenchen@acp.de

Regensburg (SWS Computersysteme AG)
Tel.: 0941-20605-0
E-Mail: info@swsnet.de

Stuttgart
Tel.: 0711-23917-0
E-Mail: stuttgart@acp.de

Sulzbach/Taunus
Tel.: 06196-56142-0
E-Mail: sulzbach@acp.de

Ulm
Tel.: 0731-141151-0
E-Mail: info.ulm@acp.de

UNSERE PARTNER (Auszug):

Cisco, Citrix, DataCore Software, Dell, DeskCenter Management Suite, EMC² where information lives, IBM, Fortinet, Fujitsu, hp, Kaspersky, KEMP Technologies, lenovo, Microsoft, NetApp, Samsung, Sophos, Trend Micro, Veeam, vmware

HERAUSGEBER:
ACP Holding Deutschland GmbH
Stuttgarter Straße 3-5
80807 München
E-Mail: inside_acp@acp.de