IOprotect Security Event 2015

Erfahrungsberichte aus erster Hand

Der kürzlich erfolgte Angriff auf Unternehmen weltweit (Fall Carbanak) ist ein weiterer Weckruf für Unternehmen, sich mit dem Thema gezielte Angriffe auseinanderzusetzen. Der zweite IOprotect Security Event steht ganz im Zeichen des Erfahrungsaustausches.

Experten aus unterschiedlichen Firmen und Tätigkeitsgebieten berichten von ihren Erfahrungen bei der Implementation von Massnahmen zur Verhinderung oder Detektierung gezielter Angriffe. Zielpublikum sind Security- und IT-Verantwortliche, Risk-Manager, Incident Responder und weitere an der Thematik interessierte Kreise.

Programm

13:00 - 13:30 **Eintreffen Gäste**

13:30 - 13:45 **Begrüssung und Einleitung**

13:45 - 14:25 **Splunk: Achtung, fertig, los! - Geht es wirklich so schnell?**
Andre Kocher & Mathias Herzog (PostFinance AG) - Splunk Team
Welches sind die Do's und Dont's, was die Herausforderungen um Splunk im Enterpriseumfeld effizient einsetzen zu können? Die in einem schweizerischen Finanzinstitut gemachten Erfahrungen werden erläutert und es werden Antworten zur Architektur und Betrieb geliefert.

14:25 - 15:05 **Security Monitoring mit Splunk. Erkenntnisse aus dem SOC der Bank Julius Bär**
Stefan Meier (Bank Julius Bär & Co. AG) - Senior IT Security Consultant
Julius Bär hat sich vor dreieinhalb Jahren entschieden, ein zentrales Security Monitoring basierend auf Splunk aufzubauen. Die Security Monitoring Umgebung verfügt heute über Module zur Korrelation von Events, Alerting mittels Ticketingsystem sowie Schnittstellen um Threat Feeds und Assets automatisiert einzubinden. In der letzten Ausbaustufe wurden so die Grundlagen geschaffen, um ein flexibles Konzept zur Malwareerkennung umsetzen zu können.

15:05 - 15:25 **Kurze Erfrischungspause**

15:25 - 16:05 **Lessons Learned aus Forensik-Fällen**
Adrian Leuenberger (IOprotect GmbH) - Partner
Seit der Gründung unterstützt IOprotect Strafverfolger und Unternehmen in der Aufklärung von Sicherheitsvorfällen mittels forensischer Methoden. Beispiele aus diesem Erfahrungsschatz geben Aufschluss über optimale Abläufe und Stolpersteine, welche besser vorgängig aus dem Weg geräumt werden.

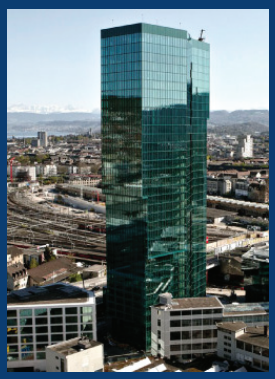
16:05 - 16:45 **Microsoft EMET in der Praxis**
Tom Ueltschi (Die Schweizerische Post) - Operative Informatiksicherheit
Renato Ettisberger (IOprotect GmbH) - Partner
Das "Enhanced Mitigation Experience Toolkit" von Microsoft bietet effektive Möglichkeiten zur Bekämpfung von fortgeschrittenen Angriffen. Neben Details zur Funktionalitäten wird vor allem aufgezeigt, wie sich die Umsetzung im Unternehmen praktisch auswirkt, welcher Nutzen gewonnen wird und wo mögliche Hürden liegen.

16:45 - 17:00 **Wrap-Up durch IOprotect**

17:00 - 18:00 **Apéro**

Datum
7. Mai 2015
13:30 – ca. 17:00, mit anschliessendem Apéro

Lokation
Clouds (34.Stock)
Maagplatz 5
Zürich
www.clouds.ch



Anmeldung
Sichern Sie sich einen der limitierten Anzahl Plätze und melden Sie sich noch heute an via info@ioprotect.ch oder telefonisch auf 044 533 00 05. Die Teilnahme ist kostenlos, die Anmeldung verbindlich.

Anmeldeschluss:
17. April 2015

IOprotect GmbH
Huobstrasse 14
8808 Pfäffikon SZ

+41 (0)44 533 00 05

info@ioprotect.ch
www.ioprotect.ch