IOprotect Security Event 2017

Security Community als Antwort auf Bedrohungslage

WannaCry, Petya und der SWIFT-Vorfall haben eines gezeigt: Alleine kann ein Unternehmen die Herausforderungen im Bereich der Cyber Angriffe kaum stemmen. Es braucht mehr als ein trendiges Security-Endprodukt oder irgendwelche IoC-Feeds, denn Angriffsparameter wechseln viel zu schnell. Der dritte IOprotect Security Event zeigt auf, wieso der stetige Austausch in einer Security Community essentiell ist, um die Bereiche der Prävention, Detektion und Reaktion gezielt und nachhaltig zu stärken.

Programm

11:30 - 12:30 **Eintreffen Gäste / Steh-Lunch**

12:30 - 12:45 **Begrüssung und Einleitung**

12:45 - 13:30 **Cyber Security Map: Darstellung eines komplexen IT-Sicherheitsdispositivs**
Walter Kunz (Post CH AG) - Stv. CISO
Wie zeigt man dem Top Management auf, wie das Unternehmen im Bereich Cyber Security aufgestellt ist? Diese Präsentation stellt den von der Schweizerischen Post gewählten Ansatz vor, bei dem die Komplexität soweit möglich verborgen bleibt, jedoch die Struktur und Terminologie allgemein anerkannt ist.

13:30 - 14:10 **Effektivere Detektion: Modus Operandi der Angreifer verstehen**
Renato Ettisberger (IOprotect GmbH) - Partner
Indicator of Compromise (IoC) sind hilfreich bei konkreten Vorfällen, jedoch wenig nachhaltig für ein effektives Security Monitoring. Viel entscheidender ist es, den Modus Operandi der Angreifer zu verstehen und dieses Wissen für die Detektion zu nutzen. Anhand aktueller Angriffstrends wird aufgezeigt, wie man daraus effektive Monitoring Use Cases ableiten kann.

14:10 - 14:30 **Erfrischungspause**

14:30 - 15:15 **Wo ist der Perimeter geblieben - Endpoint Security im Fokus**
Andreas Schneider (SRG SSR) - CISO Generaldirektion, CIO ad interim
Mit wenigen technischen Massnahmen am Perimeter konnte in der Vergangenheit ein adäquater IT-Schutz gewährleistet werden. Der Wandel bei den Endgeräten und der Wunsch nach BYOD und Cloud Lösungen stellen jedoch zusätzliche Anforderungen an den IT-Schutz. Diese Präsentation gibt einen Einblick, wie diese Herausforderungen bei der SRG SSR angegangen werden.

15:15 - 15:50 **Vorteile eines Community-basierten Malware Analyse Services**
Peter Wälti (IOprotect GmbH) - Information Security Advisor
Seit Oktober 2016 bietet IOprotect eine automatisierte Malware Analyse innerhalb des Security Community Services (SCS) an. Damit können unterschiedlichste Dateitypen in einer Sandbox auf Schadinhalte hin untersucht werden. Es wird aufgezeigt, wie der Dienst aufgebaut ist, welche Schlüsse aus den Reports gezogen werden können und worin der Mehrwert für die Community liegt.

15:50 - 16:00 **Wrap-Up durch IOprotect, anschliessend Apéro**

Datum
1. September 2017
11:30 - 12:30 Steh-Lunch
12:30 - 16:00 Event mit anschliessendem Apéro

Lokation
Hotel Marriot
Neumühlequai 42
Zürich

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:
18. August 2017

IOprotect GmbH
Dürstelenstrasse 136
8335 Hittnau

+41 (0)44 533 00 05

info@ioprotect.ch
www.ioprotect.ch