Beitrag von SIX, um den Schweizer Finanzplatz sicherer zu machen

Beispiele aus der Praxis
Swiss Banking Services Forum, 22. Mai 2019

Daniel Coray, Head Cyber Defense, SIX Group Services AG

Agenda

- Security Operations Center (SOC)
- Bedrohungslandschaft und Methoden
- Beispiel aus der Praxis
- Zusammenfassung und Ausblick

«Wir bekämpfen die Kriminalität des 21. Jahrhunderts mit einer Organisation de 19. Jahrhunderts.»

Michael Lauber, Bundesanwalt Schweiz

Security Operations Center (SOC)

SIX hat ein SOC der nächsten Generation entwickelt, um die kritische Infrastruktur des Schweizer Finanzplatzes zu schützen

- Auf dem neuesten Stand der Technik, mit Sicherheitsanalysten vor Ort in Zürich – 24 Stunden am Tag, 7 Tage die Woche
- Daten bleiben in der Schweiz
- Kontinuierlicher Betrieb und Verbesserung der Anwendungsfälle und des Betriebshandbuchs für unsere eigene Infrastruktur

Was ist das SIX Security Operations Center (SOC)?

Das SIX Security Operations Center (SOC) ist die Kommandozentrale zur Überwachung der Sicherheit und Reaktion bei Vorfällen:

- SOC überwacht zentral rund um die Uhr bestimmte IT-Ressourcen und Daten, indem nach Indikatoren für Angriffe gesucht und auf Bedrohungen reagiert wird
- SOC ist der Hub zur Erkennung, Analyse und Abwehr von Cyberangriffen
- Entwickelt anhand fallbasierter Bedrohungser-kennung, gebündelt mit verhaltensorientierten Ansätzen und durch kognitive Analyse unterstützt
- SOC kann Angriffe nicht nur reaktiv erkennen, sondern auch präventiv verhindern, bevor sie eindringen

Bedrohungslandschaft und Methoden

Bedrohungssituation

«91% der Cyberkriminalität beginnt mit E-Mails»

«E-Mail ist der beliebteste Träger für Cyberangriffe»

«Phishing-Angriffe haben im letzten Jahr um 65% zugenommen»

«Cyberkriminelle verlassen sich mehr denn je bei Angriffen auf Identitätsbetrug und weniger auf Betrug mit Domänennamen»

Quelle: FireEye Cyber Landscape Report Q1-Q2 2018

Banken sind Cyber-Bedrohungen ausgesetzt

Cyber Threat Intelligence

finma

Mit welchen Cyber-Bedrohungen sind Banken in der Schweiz konfrontiert?

4

APT

Advanced Persistent Threats (Generic) The term "advanced persistent threat" (APT) denotes a type of threat and attack that is technically sophisticated and usually present in…

1

CYBERCRIME

Cybercrime (Generic) The term "cybercrime" denotes a range of criminal acts directed against individuals or enterprises. The specific background to calling a criminal act a "cybercrim…

Phishing

DDOS

Distributed Denial of Service (Generic) The term "denial of service" generally denotes an attack, or series of attacks, on an IT environment, with a view to disrupting or disabling the services p…

INSIDER THREATS

Insider Threat (Generic) An insider threat is defined as the potential of an adverse act or omission from within the organization, i.e., committed by employees or individuals with a spec…

2

MALWARE

Malware (Generic) The term "malware" denotes any malicious software used for the purpose of attacking systems and IT environments. There is a vast number of malware specimens in th…

MOBILE MALWARE

Mobile Malware (Generic) Mobile malware denotes a specific type of malware that affects mobile devices, most notably smartphones. The emergence of mobile malware has b…

RANSOMWARE

Ransomware (Generic) The term "ransomware" denotes the insertion of malware that is designed to extort a ransom in money or money equivalent from the end user. This is usually ach…

3

SOCIAL ENGINEERING

Social Engineering (Generic) The term "social engineering" incorporates any and all human-intelligent interactions that are designed to elicit an involuntary or unconscious respons…

UNPATCHED SYSTEMS

Unpatched Systems (Generic) Unpatched systems are programs for which a patch—software that modifies a system, application or other program—is either unavailable or ha…

WATERING HOLE

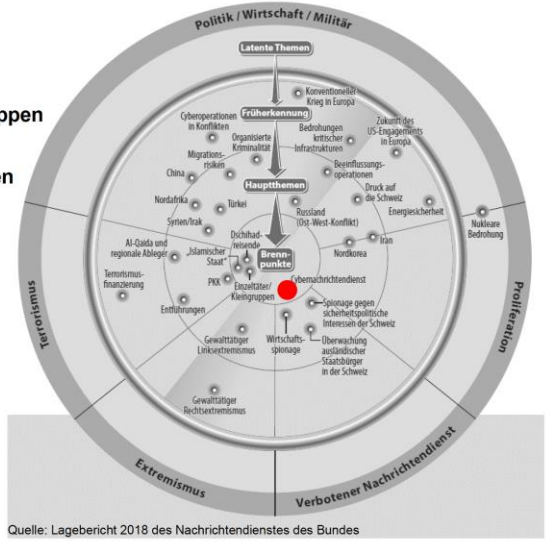
Watering Hole (Generic) The term "watering hole" denotes a technique whereby end users visiting a certain web site are covertly redirected to another web site that will deliver ma…

Cyber Threat Intelligence

finma

Bedrohungslage – Wer sind die Cyber-Akteure?

- Staatlich finanzierte Gruppen
- Kriminelle Organisationen
- Interne Mitarbeiter
- Isolierte Hackers
- Script Kiddies



Quelle: Lagebericht 2018 des Nachrichtendienstes des Bundes

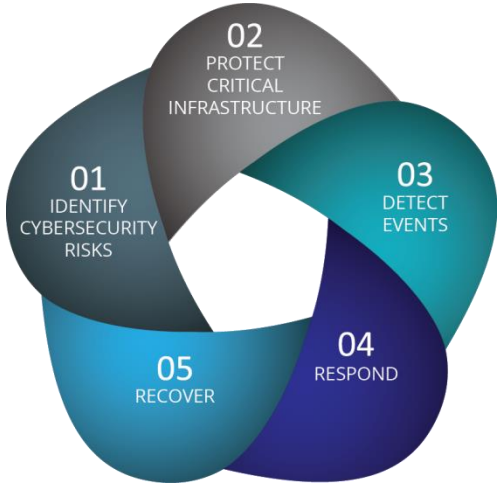
Quelle:
- FINMA Selbsteinschätzung der Cyber-Bedrohungsintelligenz
- Sicherheit Schweiz 2018 - Lagebericht 2018 des Nachrichtendienstes des Bundes

Einblick in die tägliche Bedrohungslage

Zusammenfassung und Ausblick

Minderung des Cyber-Risikos / Beitrag von SIX, um den Schweizer Finanzplatz sicherer zu machen

- 7x24 h betriebenes **Security Operations Center** vor Ort (inkl. SIEM*)
- Eigenes **CSIRT*-Team**, um bei auftretenden Bedrohungen eine schnelle Reaktion zu ermöglichen
- **Aktives Mitglied** in verschiedenen Sicherheitsgemeinschaften
- **Austausch von Bedrohungsinformationen** mit ausgewählten Schweizer und vertrauenswürdigen internationalen Partnern
- Basis-Hygienefaktoren wie **Red-Team** Assessments, **Penetrationstests** bei Systemen und proaktives **Schwachstellenmanagement**
- Weiterbildung der Mitarbeitenden durch regelmässige Schulungen und **Seminare zur Sensibilisierung**
- Verwendung von Informationen aus dem **Darknet**
- **Ausbau der Cyber-Resilienz**
- **Cyber-Risiko-Versicherung**



*Computer Security Incident Response Team
*Security Information and Event Management

«Wir erwarten nicht, dass SIX mithilfe des SOC unverletzbar gegenüber Cyberangriffen wird …

… aber es ermöglicht eine kontinuierliche Steigerung der Fähigkeiten, um mit heutigen und künftigen Cyberbedrohungen fertig zu werden.»

An einem weiteren Dialog interessiert? Bitte wenden Sie sich an uns …

für SIX Cyber Defense

Daniel Coray
Leiter Cyber Defense

daniel.coray@six-group.com

für SIX Managed Security Services

Michael Boppel
Leiter Managed Security Services

michael.boppel@six-group.com

Besuchen Sie SIX on Cyber Security

- www.six-group.com/de/site/cybersecurity.html
- www.six-group.com/de/site/cyber-security/security-operations-center.html