SIX's Contribution to Making the Swiss Financial Center More Secure

Real-life Examples

Swiss Banking Services Forum, 22 May 2019

Daniel Coray, Head Cyber Defense, SIX Group Services Ltd

Agenda

- Security Operation Center (SOC)
- Threat Landscape & Methods
- Everyday life example
- Summary & Outlook

“We are fighting 21st century crime with a 19th century organization.“

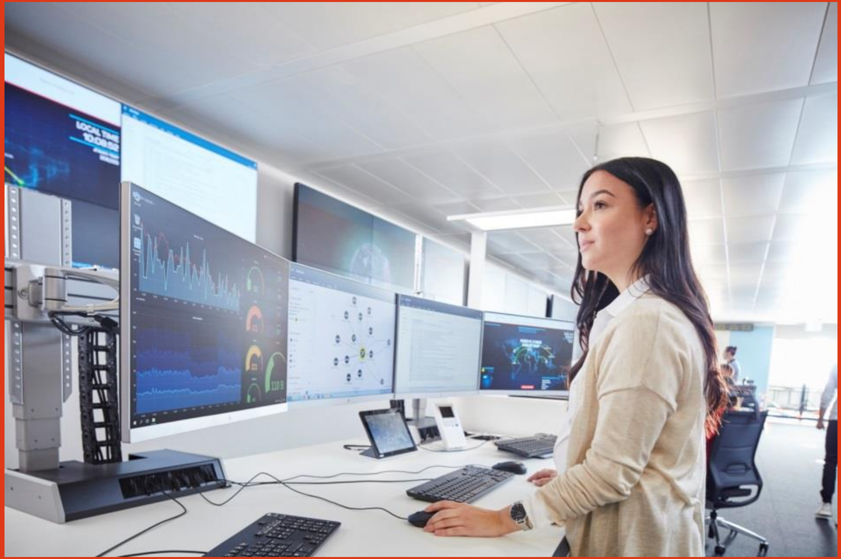
Michael Lauber, Federal Prosecutor of Switzerland

Security Operations Center (SOC)

SIX Has Built a Next Generation SOC to Protect the Critical Infrastructure of the Swiss Financial Center

- State of the Art, with Security Analysts on site in Zürich, 24 hours a day, 7 days a week
- Data remains within Switzerland
- Continuously operate and improve use cases & runbooks for our own infrastructure

What Is the SIX Security Operations Center (SOC)



The Security Operations Center (SOC) is the command center for Security Monitoring & Response:

- The SOC centrally monitors 24x7 specific IT resources and data through searches of attack indicators and responds to threats
- The SOC is the hub of detection, analysis and defense against cyber attacks
- Derived from use-case based detection bundled with behavioural approaches and supported by cognitive analysis
- The SOC can not only reactively detect but can also prevent attacks from being successful

Threat Landscape & Methods

Threat Situation

“91% of cyber crime starts with e-mail”

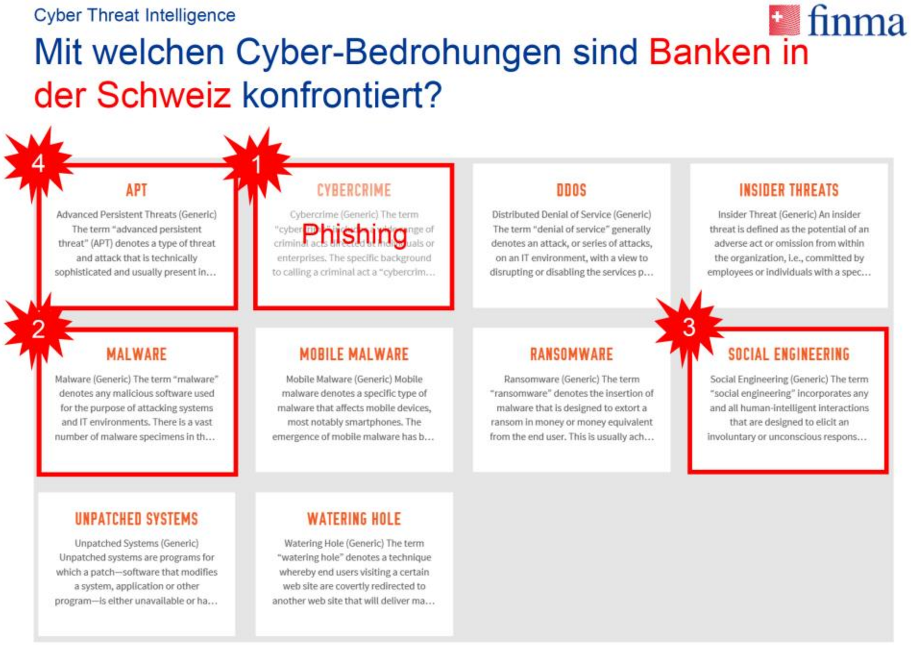
“email is the most popular vectors for cyber attacks”

“phishing attempts grew 65% in the last year”

“Cyber-criminals are relying more on friendly name impersonation over domain name fraud for attacks“

Source: FireEye Cyber Landscape Report Q1-Q2 2018

Cyber Threats Banks Are Exposed



Cyber Threat Intelligence

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

Phishing

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

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…

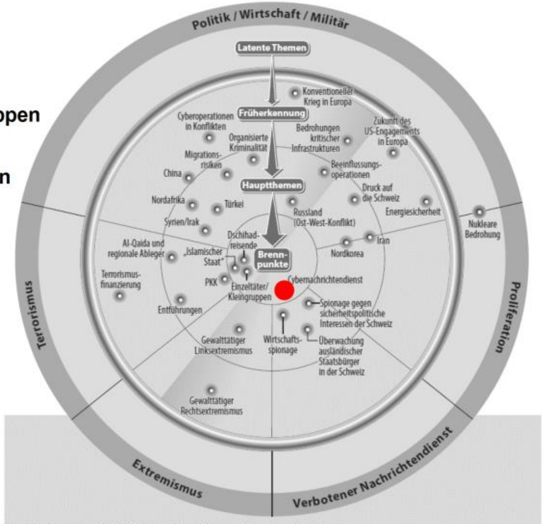
WATERING HOLE

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

Bedrohungslage – Wer sind die Cyber-Akteure?

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



Politik / Wirtschaft / Militär
Latente Themen
Früherkennung
Hauptthemen
Brenn-punkte
Konventioneller Krieg in Europa
Cyberoperationen in Konflikten
Organisierte Kriminalität
Bedrohungen kritischer Infrastrukturen
Zukunft des US-Engagements in Europa
Migrationsrisiken
China
Beeinflussungsoperationen
Druck auf die Schweiz
Energiesicherheit
Nordafrika
Türkei
Russland (Ost-West-Konflikt)
Nukleare Bedrohung
Syrien/Irak
Dschihadreisende
Iran
Al-Qaida und regionale Ableger
„Islamischer Staat"
Nordkorea
Terrorismusfinanzierung
PKK
Einzeltäter/ Kleingruppen
Cybernachrichtendienst
Entführungen
Spionage gegen sicherheitspolitische Interessen der Schweiz
Gewalttätiger Linksextremismus
Wirtschaftsspionage
Überwachung ausländischer Staatsbürger in der Schweiz
Gewalttätiger Rechtsextremismus
Terrorismus
Proliferation
Extremismus
Verbotener Nachrichtendienst

Quelle: Lagebericht 2018 des Nachrichtendienstes des Bundes

Source:
- FINMA's self-assessment of Cyber Threat Intelligence
- Switzerland's Security 2018 - Situation Report 2018 of the Federal Intelligence Service FIS

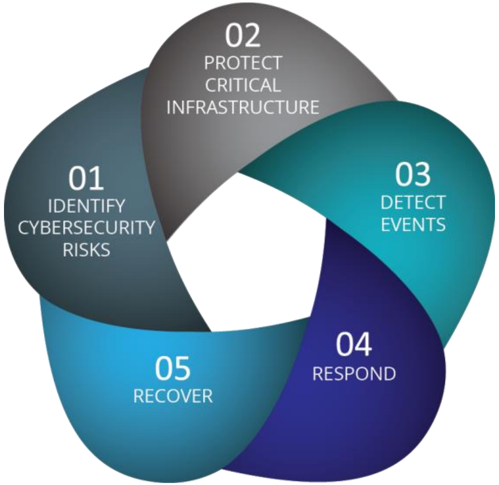
Insight to Daily Challenges

- Password Cracker
- Identity Theft
- Skimming
- Virus
- Trojan
- Spyware
- Social Engineering
- Insider Threat
- Nation State
- Cyber Vandal
- Theft of Credentials
- Hacktivist
- Fraud / Unauthorized Payments
- Impacting Bank Accounts with Banking Trojans
- Worms
- Spear-phishing
- Jailbreak
- Scareware
- Session-Hijacking
- Zero-day Exploit
- Spoofing
- Pharming
- Ransomware
- Data Breach / Data Leakage
- Organized Crime
- Man-in-the-Middle
- Distributed Denial-of-Service (DDoS)
- Rootkit
- SQL Injection
- Vulnerabilities
- Blackmail Trojans
- Backdoor
- Bot / Botnet
- Coin mining
- Hacker
- Keylogger
- Metasploit
- Malware
- Phishing
- Remote Access Trojans

Summary & Outlook

Cyber Risk Mitigations / SIX's Contribution to Making the Swiss Financial Center More Secure

- 7x24h **Security Operations Center** on premise (incl. SIEM)
- Dedicated **CSIRT* team** for fast response to any emerging threats
- **Active member** in several security communities
- Forest and **shares threat-intelligence** with selected Swiss and international trusted partners
- Base hygiene factors as **Red-Team** assessments, **penetration tests** of systems and proactive **vulnerability management**
- Educate employees through regular trainings and **awareness sessions**
- Use of information from the **Darknet**
- **Building cyber resilience**
- **Cyber risk insurance**



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

‘We do not expect that the SOC makes SIX invulnerable to any cyber attack…

…but it provides a continuous increase of capabilities over time to deal with today’s and future cyber threats.’

Interested in a Further Dialogue?
Please Reach Out to Us…

for SIX Cyber Defense

Daniel Coray
Head Cyber Defense

daniel.coray@six-group.com

for SIX Managed Security Services

Michael Boppel
Head Managed Security Services

michael.boppel@six-group.com

Visit us, SIX on Cyber Security

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