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
Michael Lauber, Federal Prosecutor of Switzerland

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

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