HOW TO PROTECT AIR TRAFFIC MANAGEMENT AGAINST CYBER ATTACKS?
WHY A CO-PRESENTATION REGARDING THE ATM CYBERTHREATS?

• Turnover: 3,1bn €
• +20 Countries
• 35 000 People

• Cyber Security
  • 600 Experts
  • 360° Services
  • Innovation

In order to protect Aircraft Traffic Management against cyberthreats
→ Combine strengths of ATM actors – ATM Products – Cybersecurity services

• 215.7 Mio €
• +120 Countries
• 1.250 People

• Cyber Safety
  • 100+ Experts
  • Safety Process according SAM
INTRODUCTION

• Aircraft Traffic Management
  • Is there a real threat?
  • Mature approach to safety – but what about Cyber-security?
  • What about ATM Digital transformation impact?

• Frequentis market vision
  • Identified cyberthreat - a serious game!
  • Cybersecurity embedded into Frequentis solution
  • Why set-up a partnership with a global cyber-security provider?

• Sopra Steria cyber-security responses
  • Threats and Darkmarket overview
  • Cyber-attack evolution overview
  • Sopra Steria Cybersecurity industrial approach

• Next Steps ...
Strong connection of System Safety & System Security regarding the **availability** of functions for **authorized** parties
Non-physical security events in cyberspace may have real implications

Example:

- Denial of Service (non-physical)
- Disruption of safety-related ATM procedures (reality)

We enable safe innovation

FREQUENTIS is a key partner for ATM Cyber Safety in the future

- ATM-grade end-to-end IP communication solution provider
  - Certified components for secure/non-secure voice communication (CC EAL4+)
  - Proven by software safety assurance (e.g. ED-153)

- Next generation 4k screen & VoIP recording solution „at the glass“
  - Secured encrypted export of ATM data
  - Central authorization control for remote systems

- Safety & Security is the basis for all our solutions
  - Fail-safe and highly redundant systems
  - Security by Design
  - Software Safety Assurance
For a safe and secure world

Prepared for the future
- FREQUENTIS Computer Security Incident Response Team (CSIRT)
- Security Notification & Event Response
- Security Policy, Guidelines & Assessments
- Awareness & Trainings

Urgency in ATM for
- Trusted Partnerships between Industry & ANSPs and Authorities
- Establishment of Cyber Security Operation Centers
- Extended Monitoring & Logging
- Cyber Security Culture & Awareness

Cyber Safety & Security Risk Assessments
- FREQUENTIS combines Safety & Security activities and trusted partnerships to assess the overall risk of threats and hazards within ATM infrastructure
- Partnership on Cyber-security with Sopra Steria on European projects
The Right Balance

Business Focused

Your Information - Protected

Your Reputation – Preserved
APT PRESENTATION
CYBERSECURITY IN THE NEWS

Threats progression and acceleration since three years ...

2012 – EADS Airbus
- Cyber-attack
- 30,000 laptops including 2,000 servers destroyed in one day

2013 – APT1 report
- Penetration delay: 356 days in average (4 years and 10 months for the longest one)
- A data theft estimated to 6.5 terabits of data gathered for one company, in 10 months

2010 – STUXNET
- First APT known
- Massive information theft against US organisations, including the army, during 3 years

2013 – FBI Aviation APT Alert

2015 – SONY

(U//FOUO) APT Actors Increased Interest in the Aviation Industry

(U) General Observations

(U//FOUO) Since June 2013, the FBI has observed advanced persistent threat (APT) actors’ increased interest in the aviation industry. APT actors have sent spear-phishing e-mails targeting individuals associated with the air travel industry. Some of the spear-phishing e-mails originated from a spoofed sender in an attempt to make the e-mail appear more legitimate. E-mail recipients should be aware of suspicious and potentially malicious e-mail attachments or links.

(U) Impact of APT Activity

(U//FOUO) Every organization is at risk of being the target of an APT attack. APT actors, who are semi-sophisticated and difficult to detect while on network systems, have already cost US entities hundreds of millions of dollars over the past decade as a result of harvesting enormous amounts of critical information including proprietary data, source code, negotiation tactics, and strategic operational plans. These actors have also breached networks containing sensitive national security information. Going forward, advanced persistent threat actors differ from common hackers or cyber criminals by conducting targeted, rather than opportunistic, attacks that seek precise information rather than monetary gain, more closely resembling espionage. While the activity cannot often be definitively linked to any particular nation state, the sophistication, resources, and types of information sought suggests governmental support.
DARKNET INTRODUCTION
Threats Overview

- Beginner hacking
- Script kiddies
- Intermediate hacking
- Advanced hacking
- Isolated Cyber-terrorism
- APT Group
- Advanced Cyber-terrorism
- Data leakage
- Ransomware
- Data Destruction
**ADVANCED PERSISTENT THREAT**

**APT IS THE MOST DANGEROUS CYBER-THREAT**

- **Sophisticated and targeted attack** affecting companies and governments
- **Organized Cybercriminals** have the ability to *evade detection and the capability to gain and maintain access* to well protected networks in order to *ex-filtrate* sensitive company information

**APT impact:** Data leakage & Massive data destruction

---

**APT Process**

1. **Phishing and Zero day attack**
   - A handful of users are targeted by two phishing attacks; one user opens a zero day payload (CVE-02011-0609)

2. **Back door**
   - The user machine is accessed remotely by Poison Ivy tool

3. **Lateral movement**
   - Attacker elevates access to important user, service and admin accounts, and specific systems

4. **Data gathering**
   - Data is acquired from target servers and staged for exfiltration

5. **Exfiltrate**
   - Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider

**Reconnaissance**

- Maintain persistence

**Intrusion**

- Data Exfiltration

**Establish Backdoor**

- Install utilities
- Obtain credentials
Ideal matured market … … which is operational now!

1st & 2nd Market

1btc=272€

1st & 2nd Market

http://rentahacker暗网平台

http://2amhostniinuylg.onions/02/2am

Small Job like Email, Facebook etc hacking
200 EUR = 0.733 $

Medium-Large Job, running people, espionage, website hacking etc
500 EUR = 1.832 $

Zero day Exploit services

Insurance

ATM 2015 - Sopra Steria & Frequentis - ATM Cyber-threats 13
NEW GENERATION OF CYBER-SECURITY SERVICES

- New Generation of Cyber-security Centers
- Industrialization
- 360° services
SOPRA STERIA CYBERSECURITY KNOW-HOW
A GLOBAL SERVICE OFFERING

DETECTION & REACTION
Cyber monitoring
- SIEM / SOC
- APT Détection
- NGIPS / HIPS
- Security Watch/ CERT
- Forensic
- Crisis management

PREVENTION
Strategy, Risks & Governance
Audits & compliance

Strategy, Risks & Governance
- Strategy/ ISMS
- Risks Analysis
- IS Security policy
- CISO support
- IT Business continuity plan

Audits & Compliance
- Regulatory Compliance
- IS Compliance
- Organizational audits
- Penetration testing
- Vulnerabilities management

PROTECTION
Digital ID
Data Security

Data Security
- Classification
- Encryption
- DLP

Digital identities
- IAM / PKI
- Electronic signature
- Access management and privilege
- CMS / Biometric / eID

GLOBAL CYBERSECURITY CAPABILITIES FOR
A DIGITAL TRANSFORMATION IN CONFIDENCE
“CYBER THREATS WILL ALWAYS GET AHEAD OF DEFENCES, WHICH IS WHY ORGANISATIONS NEED A STRATEGIC APPROACH” (GARTNER)
RIGHTSECURITY SERVICES OFFER

THE RSS OFFERING : A SEAMLESS SERVICE MODEL

A right delivery model, flexible and scalable, combining proximity and industrialisation
- Adapted to clients’ demands and maturity
- Supporting our model’s clients transformation

Our Cyber Security Centers
- 24/7 Coverage
- Comprehensive approach based on a specific methodology from management by the risks: IPPCoR
- « As a service » security

A continuous innovative approach
- An Innovation Lab
- Box@PME
- An R&D partnership with CEA Tech
FRONT OFFICE/BACK OFFICE MODEL

STRATEGIC WORLDWIDE CYBERCENTRE EXPANSION

FO activated

• PKI solution (Microsoft)
• Security technology center
• Security products

Short term FO

• Data classification
• Security infrastructure
• Defence projects
• Biometry/access control
• Secure messaging

Middle term FO

• Governance/consulting
• Architecture/operation
• Crisis management
• Audit

Long term FO

• PKI
• Crisis management
• Electronic ID

Strong focus on business development UK & SG cyber anticipation

1

• SAP security audit /SSO
• Dematerialisation and secure storage

2
A Centre with Experts proud of the best Certifications:

- ISO 27005 Risk Manager,
- ISO 27001 Lead Implementer and Lead auditor,
- McAfee EPO and VirusScan, MCSE Windows, CCISP, EBIOS V2, ITIL, CISA, CISM...
- CERT referencement since 2014, ANSSI certification in progress

Our CyberSecurity Centres in a few figures over 2014:

- 2000 security catalogue requests handled
- IT devices under management by our team/services:
  - 150 000 work stations (laptops, desktops..)
  - 20 000 servers, 6 000 applications, 2 500 databases
  - 400 000 user accounts
- 12 Tb (tera) of SIEM log live (before archiving)
- 12 newsletters edited and delivered/ more than 2000 security incident treated

Our Toulouse CyberSecurity Centre features:

- Some 140 security professionals, including:
  - 30 consultants
  - 73 experts, specialists or architects
  - 30 solutions experts or administrators
- 7 Non IT profiles: legal experts, mathematician, statisticians
ATM CYBERTHREAT ARE REAL AND HAVE TO BE ADDRESSED

ATM IS A KEY SECTOR WITH HUGE IMPACT
A pragmatic Approach to protect the ATM Environment

• Three service levels:

1. Access and enable cyber-security services
   • Governance
   • Security product
   • SOC Compliance

2. Develop an innovative ATM Cyber-security Program
   • Develop innovation program
   • Create Dedicated ATM Cybersecurity Program
   • Frequentis/Sopra Steria

3. Cybersecurity General Auditing
   • CxO/Senior Management
   • Cyber-threats analysis including Risks, Logs audit, Pen-test
   • 5 months of analysis
   • Executive + Technical report
THANK YOU!

GET TOGETHER – MARCH 11, 2015, 5PM
BOOTH N° 488

Join us at our booth right after our conference to discuss with our experts tomorrow’s ATM Cyber-security
QUESTIONS