Swiss Cyber Storm 4
June 13, 2013

APT live – An in-depth example of an professional inside-out attack

Oliver Münchow - Security Consultant/Penetration Tester
Manuel Krucker - Security Consultant/Penetration Tester

Agenda

- Introduction
- APT live – An in-depth example of an professional inside-out attack
- Measures
- Summary
- Q & A Session

Overview Hacking

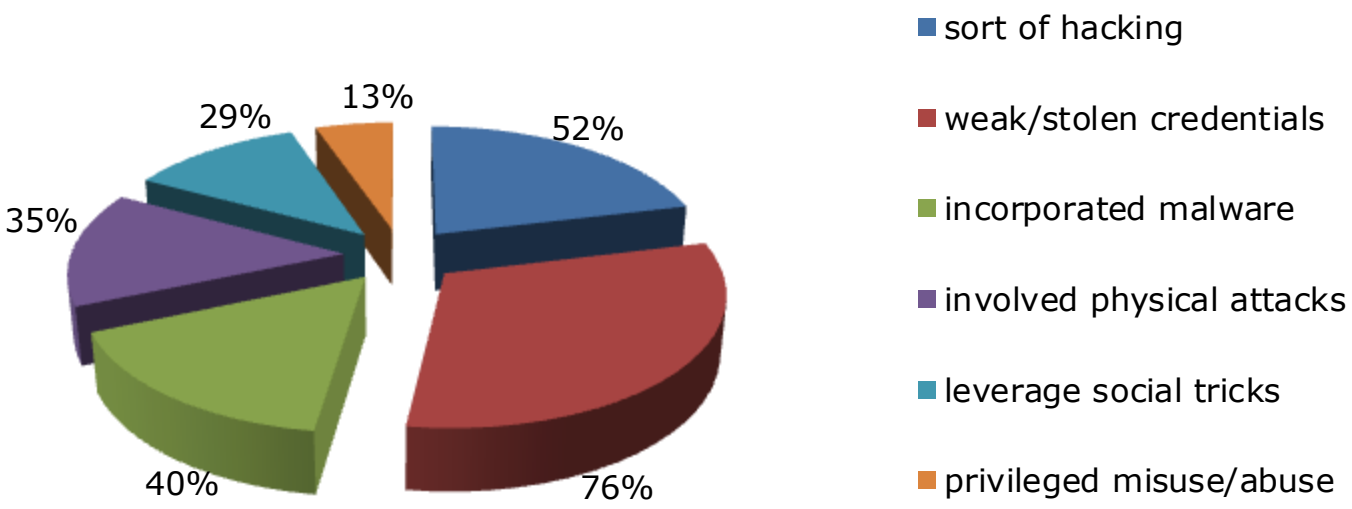
Taxonomy of Hacking

2013 Data Breach Investigation Report - Verizon

- Report for the year 2012
- 47’000 security incidents analysed by Verizon
- Verizon is a large telecommunication company
- The reports covers all possible sectors of industries

Most Important Statistics

(1) How do breaches occur?



(2) 92% of the breaches are perpetrated by outsiders

Scope of our Talk

Attacking targets from an external and anonymous perspective using:

Difference between Hacking & Malware

Sort of Hacking

Attacking a running service from the internet

"Active" Channels

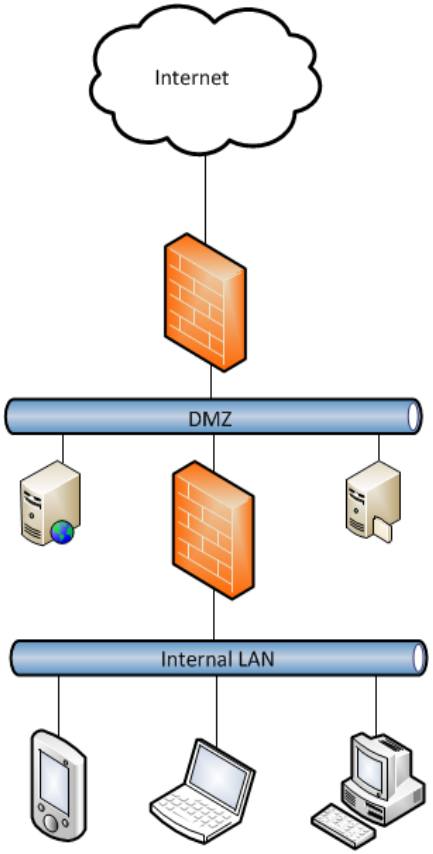
Service is accessible for anonymous attacker

Incorporated Malware

Attacking a company form within the network

"Passive" Channels

Attacker requires an action of the user

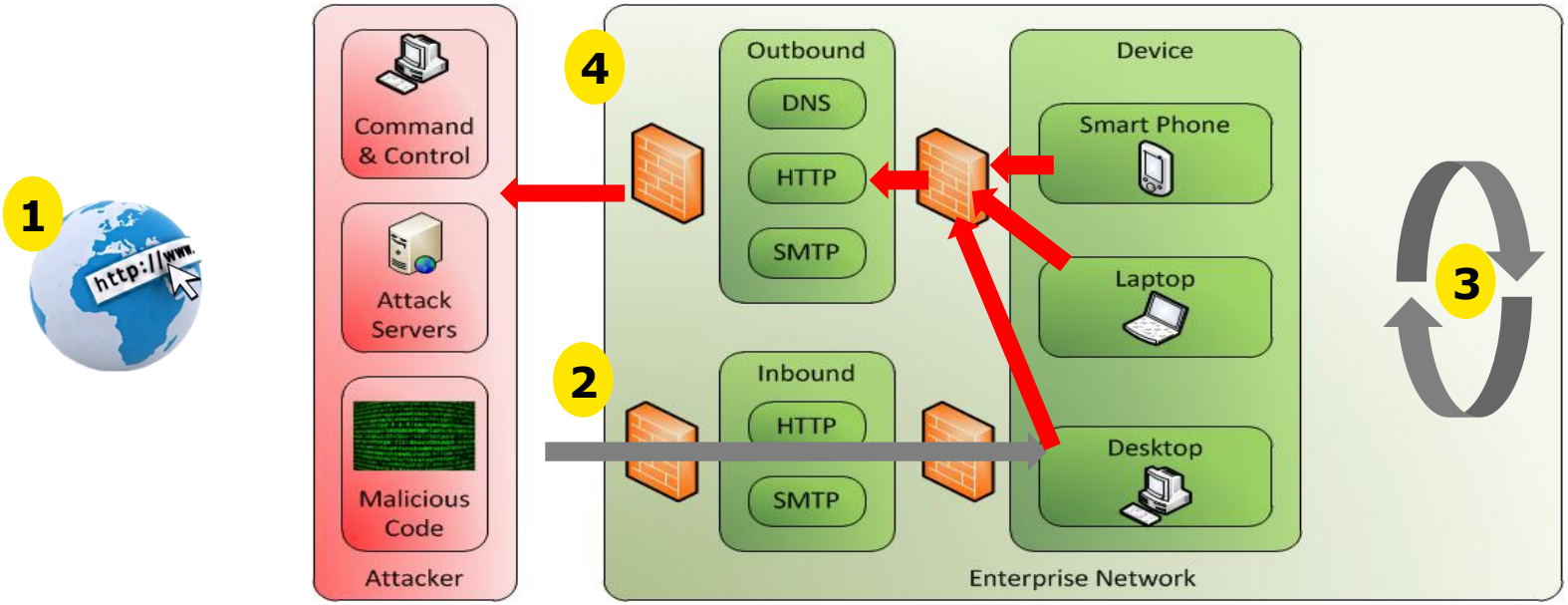


Question to Audience

- Which channels (people, protocols etc.) can i use to infiltrate company with malware?
- What tools/techniques/concepts could stop a malware from being executed within a company?
- Which protocols/applications can i use to send data out of a company?

Life-cycle of Malware Attack

1. Information Gathering
2. Malware Delivery
3. Malware Execution
4. Malware Output Delivery

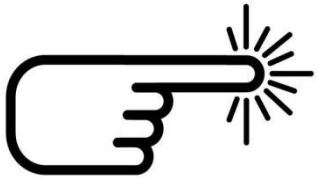


(1) Information Gathering

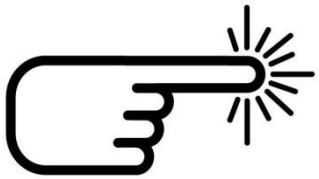
- DNS information
- Hosts
- Services
- UserIDs
- Phone numbers
- Email addresses
- Email headers
- Etc.

Email addresses of victims

APT-Live: Information Gathering



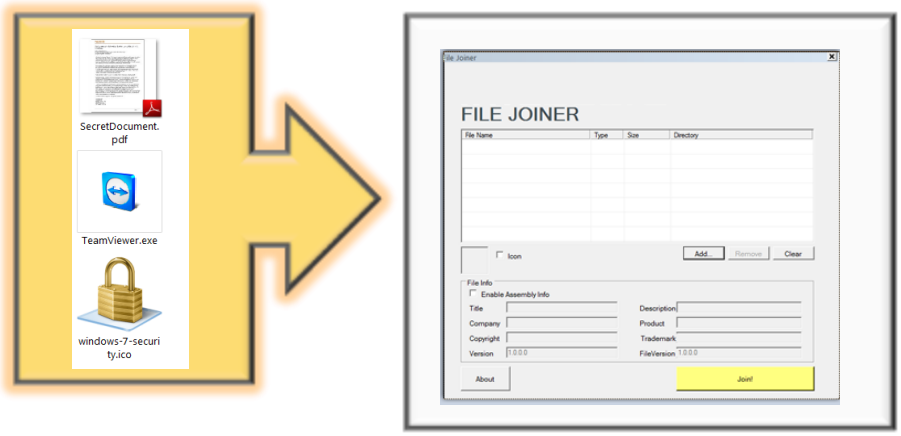
Information Gathering



SMTP

Example: Download latest files from remote PC (PostFilesIE.exe)

1 Create malicious payload (execute with temp IE cache, get recent docs from authenticated user, send Base64 via POST) & then hide payload within trusted file (f.ex. AV product)



4 Access Files selected for Download from our command center

Webserver

3 Victim downloads «security software» & we start downloading from victim

Internet

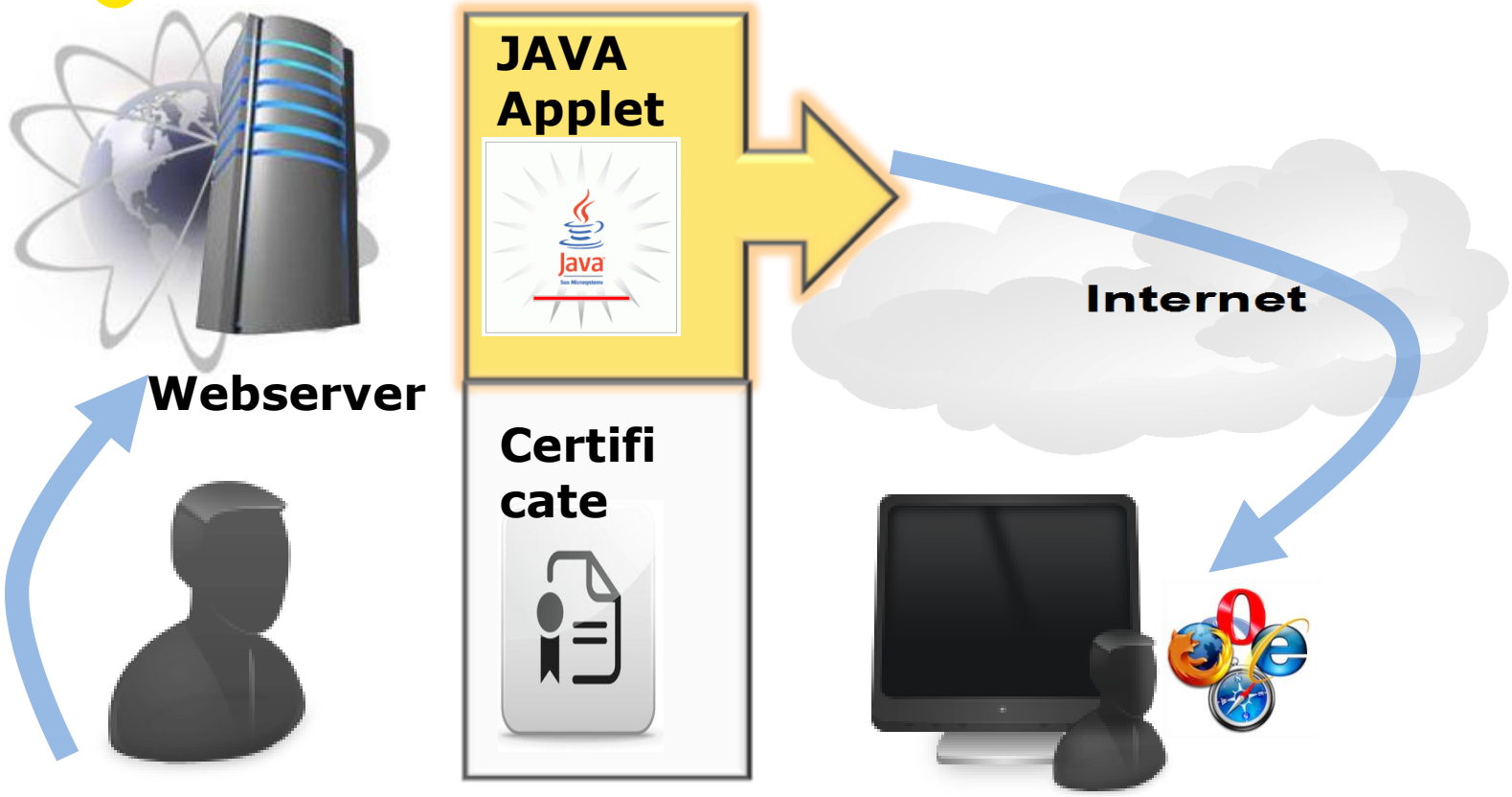
Target (victim)

2 Create domains, sites & upload code

For the lazy one SET

Example: Applet does the same trick (PostFilesIE via applet)

1 Use signed applet that streams content and executes it (self signed)

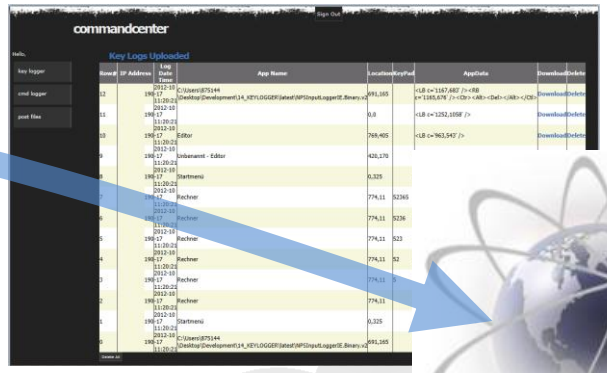


2 Code gets downloaded and executed automatically

Is this new stuff???? (Example CCC: 1997)

Example: work with shell from remote (CmdIE.Exe)

Operator



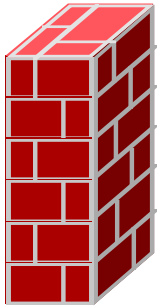
HTTP (80/443)

Internet

IIS7

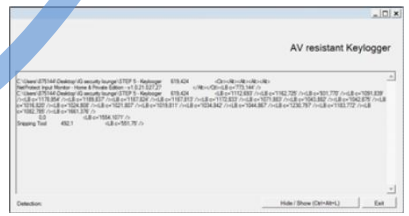
2 Remote Shell Access via Webconsole (start working interactively)

1 Victims browser connects to our webserver after executing our payload

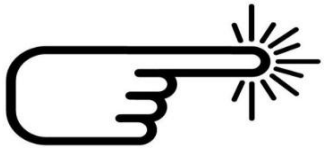


Zielrechner

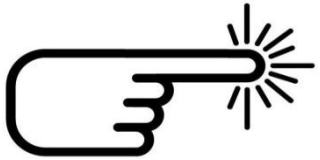
3 More apps can be downloaded and executed (also encoded)



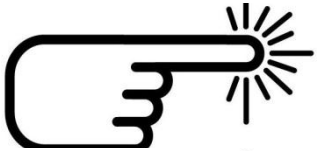
SMALL DEMO



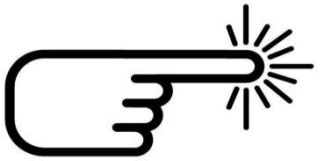
Create Malicious File (Post Docs & CommandIE)



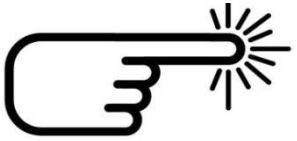
Merge into other Exe (FileJoiner)



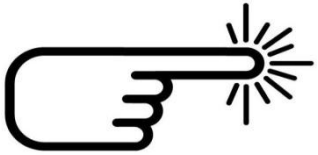
Download Software (DriveBy Attack)



Monitor with Sniffer

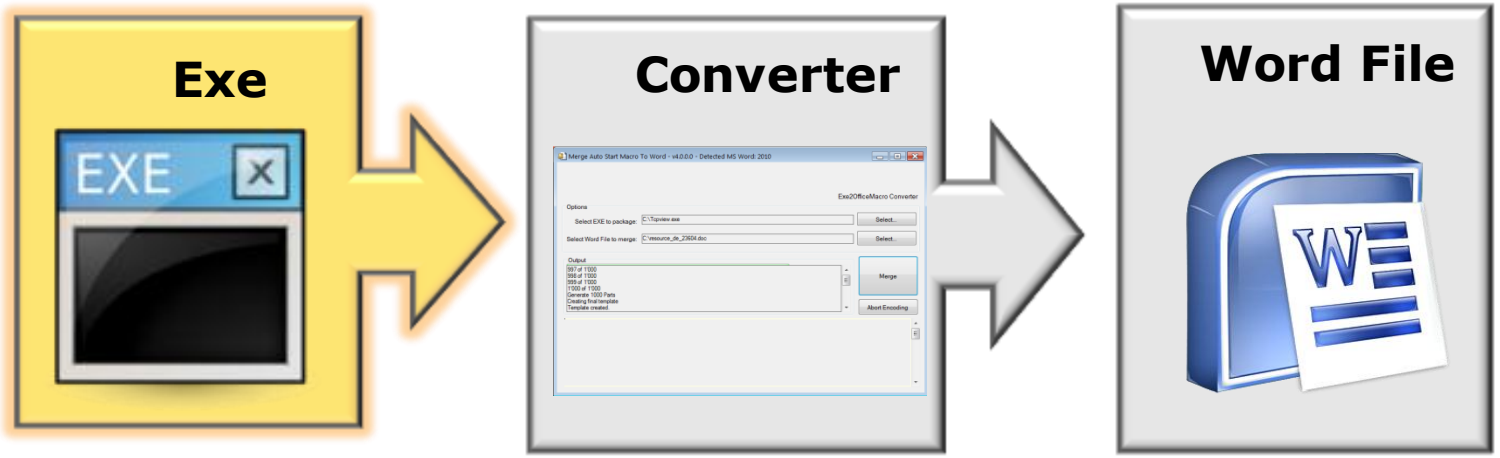


Execute Software & connect to command center
(View Posted Files & Start Commands)

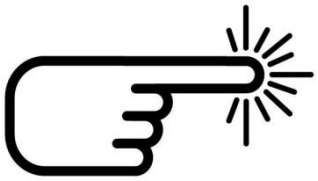


Example: Config Applet

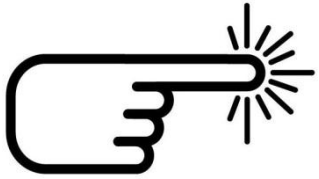
Example 6: Hide Payload in Office Document



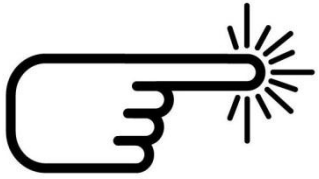
APT-Live: More Attacks



Demo: put EXE in Word



Demo: Run NP_Logger



Demo: Run Keylogger via Outlook

Measures Entry Point Mail

- Avoid email address enumeration
  - Use a unpredictable naming schema
  - Configure SMTP gateway properly (no VRFY, “secure” Non Delivery Reports)
  - Do not publish personal email addresses
- Gateway software – filter executable files

  Executable files, archives, archives cont. executables, archives cont. malware, etc. → Dozens of test cases
- Use real-time blacklists for known phishing web sites
- Use mail client security features
  - Clients can be configured to detect phishy links
- Use email trust building techniques
  - Validate from and to fields for impede the success of phishing attacks
  - Use SPF entries of sender address
- Awareness of Users

Measures Entry Point Web

- Software on the Gateway – Filter Executables
  - Filter incoming code by the web proxy
  - Use whitelists for allowed URLs
- Software on the Gateway – Analyse Code on Behaviour

  Software product that filters malicious code based on rules rather than signatures

  Example: Trustwave Secure Web Gateway
- Internet Access DMZ

  Use an area in the internal network which is isolated from the clients

  Example: Citrix Access Gateway,
- Browser Virtualisation

  This technique creates an area on the client (e.g. USB stick) that is isolated from the rest of the system

Measures Unauthorized Execution of Code

- Behaviour Based Scanners

  There are more sophisticated products that can trigger root kits and unknown malware on the client side.

  Examples: Mamutu, WildFire, Malwarbytes, etc.

- Restrict Execution of Code
  - MS AppLocker
    Restrict the execution of code by using white list approach
  - GPOs
    Start hardening the end client (e.g. limit write access to dirs or fine-tuning existing security products).
  - 3rd Party Software
    Lock down executables by using 3rd party software.
    Examples: Bit9 Parity Suite, CoreTrace Bounce, …
- Last but not least: Awareness of users

  Aware users is the best protection mechanism. Especially knowledge of the SSL protocol is important

Measures Unauthorized Access of Data

- Control Access to documents by using cryptography

  Windows Rights Management Service

  If the ACL's are moved from the network to the data itself a stolen document would have no use for an attacker. This might be achieved by using RMS.

Measures Exit Point Web

- Web Proxy

  Use a web proxy which filters outgoing web content. However, filtering encoded GET and POST parameter not feasible due to operational aspects

- 3rd Party Software

  Use a 3rd party software – well known as Data Leakage Prevention system

- Additional Authentication Layer

  The user could be forced to authenticate himself again with a specific username/password whenever he wants to access the internet. This manual authentication layer would prevent automated calls to the build in browser.

Problem

- Defending against data leakage through outgoing HTTP traffic is almost impossible
- Measures must be applied in earlier phases of the attack

Measures Exit Point DNS

- Indirect DNS resolution

  Clients should not be able to resolve external DNS request. This should be done by a proxy.
- Implement payload analysis detection mechanism

  Detect DNS tunneling by using signatures based on attributes of individual DNS payloads such as the FQDN

  contents.
- Implement traffic analysis detection mechanism

  Detect DNS tunneling by monitoring the count of unique FQDNs for a give root domain.

Measures Exit Point Mail

- Operation systems should only allow sending emails for foreground processes – use enforcement rather then warnings
- Gateway Software
  - Filter internal documents sent as attachments
  - Filter encrypted or encode message bodies
- Use a whitelist for email receivers
- Periodically control email receivers

Measures Mobile Device

- Mobile Device Management
  - Whitelist of applications
  - Only allow applications from trusted manufacturer or do an individual review (runtime and/or source code analysis) of every application

General Measures for Detecting Fraud

- Log, analyze and review security relevant events
  - Logins
  - Failed login attempts
  - Access to critical data
- Define, collect and analyze incident data
  - login at night
  - Huge transactions of data
  - Etc.
- Use One Time Pad (OTP) whenever possible, also for internal systems
- Use session time-outs
- Restrict access for unauthorized employees
- Limit software which allows execution of code

➔ These activities requires man power, but are very effective

Initial Questions – Are they answered?

- Which channels (people, protocols etc.) can i use to infiltrate company with malware?
- What tools/techniques/concepts could stop a malware from being executed within a company?
- Which protocols/applications can i use to send data out of a company?

DBIR – Measures?

- Eliminate unnecessary data; keep tabs on what's left.
- Ensure essential controls are met; regularly check that they remain so.
- Collect, analyze and share incident data to create a rich data source that can drive security program effectiveness.
- Collect, analyze, and share tactical threat intelligence, especially Indicators of Compromise (IOCs), that can greatly aid defense and detection.
- Without deemphasizing prevention, focus on better and faster detection through a blend of people, processes, and technology.
- Regularly measure things like "number of compromised systems" and "mean time to detection" in networks. Use them to drive security practices.
- Evaluate the threat landscape to prioritize a treatment strategy. Don't buy into a "one-size fits all" approach to security.
- If you're a target of espionage, don't underestimate the tenacity of your adversary. Nor should you underestimate the intelligence and tools at your disposal.

Summary – Good news at the End

- Reducing risks form internet access is a challenging task – even for non 0-day attacks
- Measures are required on technical as well as on organisational level
- Many of the presented measures are heavy-weight solutions or almost infeasible due to the enormous configuration overhead (e.g. whitelisting of applications)
- There is no one-measure-fits-all solution
- Security conflicts with operational aspects

Recommendation of InfoGuard:

- Assign a project for managing the risks resulting form internet access
- Make a detailed analysis every incoming channel (mainly web and mail) ➔ Which business use cases are essential and really required for the company (e.g. nobody requires macros from external sources)
- Try to eliminate business cases with high risks
- Implement measures for the risks of the required business cases

Temporary Workaround: Filter all executable code at the perimeter

Q & A

Contact

Manuel Krucker
Senior Security Consultant
Master of Computer Science ETH

Telefon: +41 41 749 19 68 / +41 79 377 28 28
E-Mail: manuel.krucker@infoguard.ch

Oliver Münchow
Senior Security Consultant

Telefon: +41 41 749 77 22 / +41 79 695 95 10
E-Mail: oliver.muenchow@infoguard.ch

InfoGuard AG
Lindenstrasse 10 · 6340 Baar/Schweiz
Telefon +41 41 749 19 00 · Fax +41 41 749 19 10
www.infoguard.ch · info@infoguard.ch
Baar | London | Frankfurt | Dubai

InfoGuard

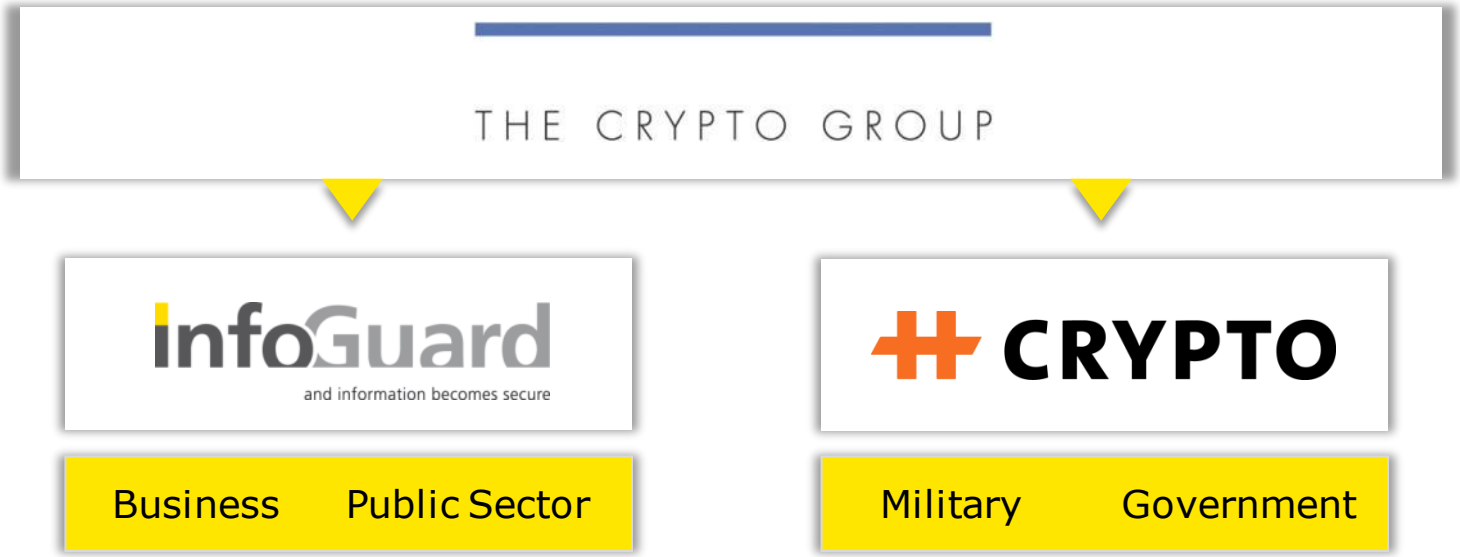
and information becomes secure

IS YOUR INFORMATION SECURE?

Secure and reliable ICT.

Your benefit. Our experience.

A Member of The Crypto Group - Competence since 1952

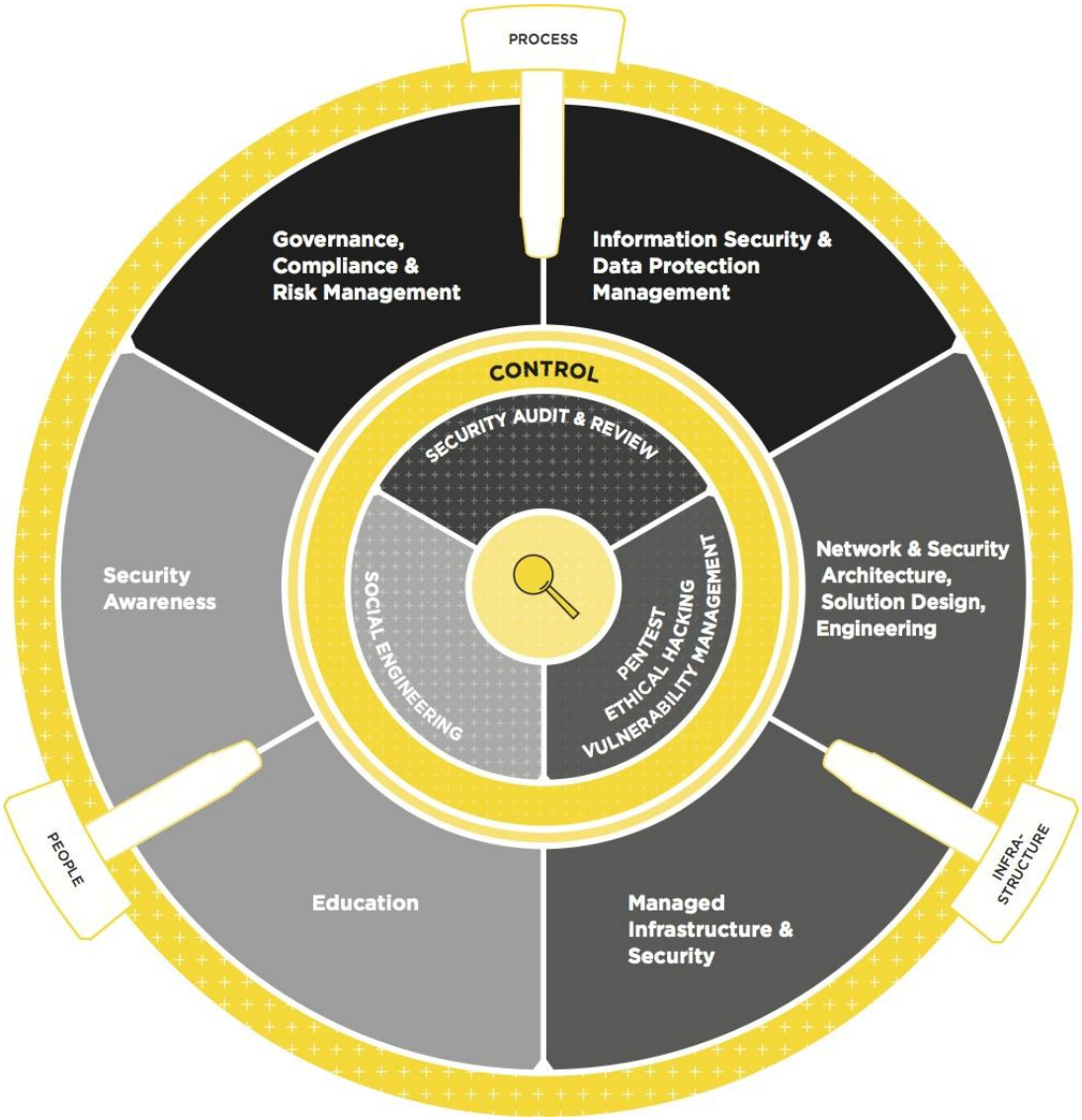


- **Swiss companies** offering Swiss made ICT security solutions
- Many years of **experience and continuity**
- Customers in over **130 countries worldwide**
- More than **300 employees** (largest Swiss Security Specialist and Top in Europe)
- Research, development and production **in house**
- **Partnerships** with selected suppliers

Experience and Competence– Our Clients

Security Services

Efficient security process made to measure



Our partners

InfoGuard SECURITY OPERATION CENTER

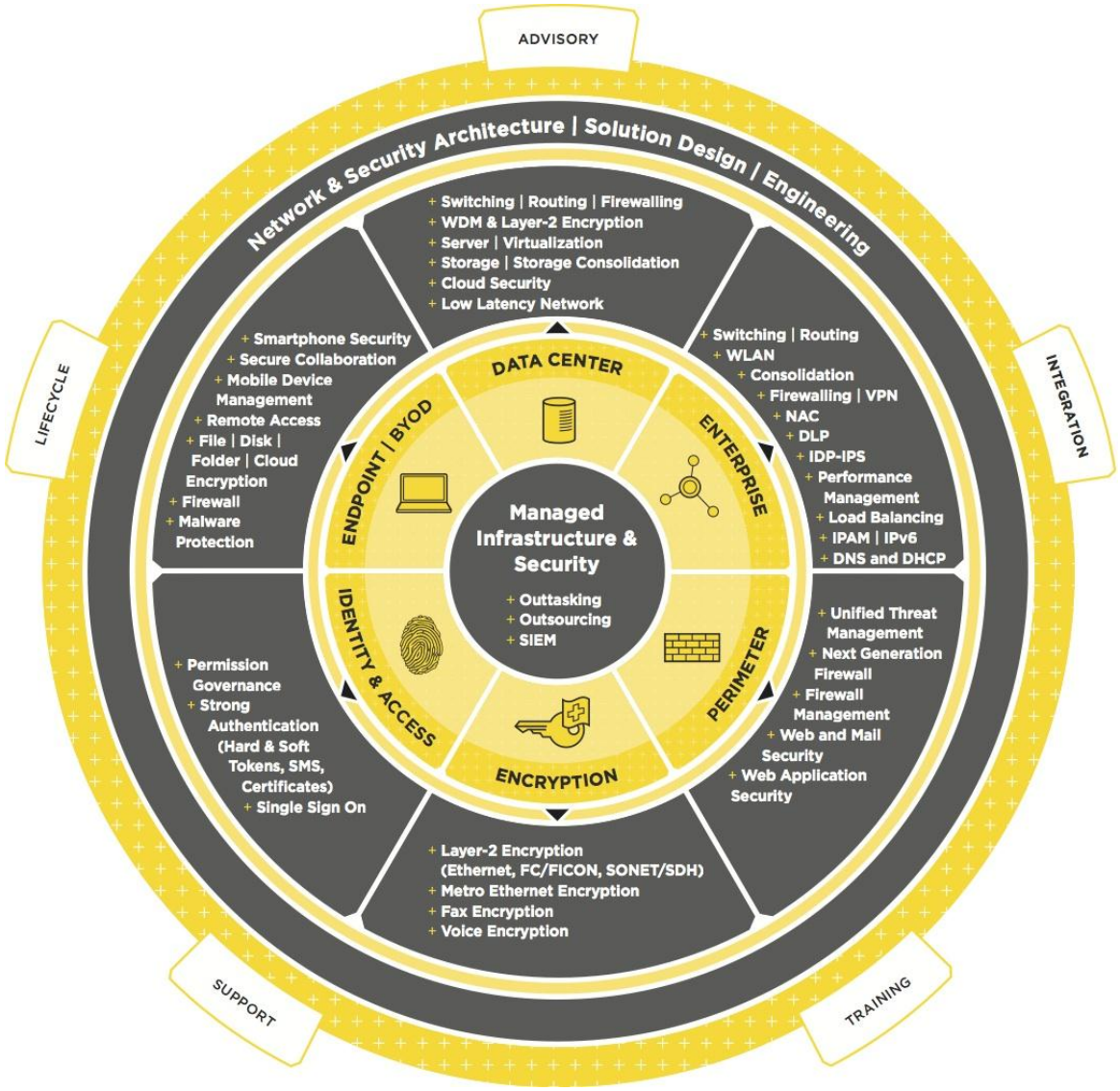
First Security Technology

E-SEC

ISAT-X

Network & Security Solutions

Reliable solutions for any requirement



Our partners

Secure:

Network:

Store:

Compute:

InfoGuard – Swiss Expert for Network- and Information Security Solutions

Awaiting your Challenges!

- Questions
- Customer Requirements
- Further Steps

InfoGuard AG
Lindenstrasse 10 · 6340 Baar/Schweiz
Telefon +41 41 749 19 00 · Fax +41 41 749 19 10
www.infoguard.ch · info@infoguard.ch
Baar | London | Frankfurt | Dubai