

protection against cyber-risk

policies / real-life attacks
a healthy dialectic

I. Rossenbach

[slightly modified presentation to
remove any restricted information]

Buenos Aires, November 2017

agenda

- Introduction
- Offense guides defense
- Dialectic:
 - security policies --> real-life attacks
 - real-life attacks --> security policies
- Conclusion

Introduction

Security, securing?

Handle and manage risks, adverse events / attacks

Avoid, transfer, accept, mitigate, exploit

How to act / behave? Security policies...

Definition of security policies

“A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources”

(RFC 2828)

Synonyms: guidance, guidelines, best practices, information security standard, cybersecurity framework, information security standards

Samples of security policies

CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures

<http://www.bis.org/cpmi/publ/d146.pdf>

SWIFT Customer Security Programme

<https://www.swift.com/myswift/customer-security-programme-csp>

PCI-DSS (Payment Card Industry Data Security Standard)

<https://www.pcisecuritystandards.org/>

NIST Cybersecurity Framework

<https://www.nist.gov/cyberframework>

CIS-CSC - Center for Internet Security – Critical Security Controls
(ex SANS Top 20 Critical Security Controls)

<https://www.cisecurity.org/controls/>

ISO 27000 series

https://en.wikipedia.org/wiki/ISO/IEC_27000-series

CC - Common Criteria for Information Technology Security Evaluation

<https://www.commoncriteriaportal.org/>

Local and specific policies

N/A

Offense guides defense (1/2)

- > Target data breach – December 2013
- > Drug traffic in the port of Antwerp - 2013
- > “Le Monde” Twitter’s account hacked – January 2015
- > Deloitte’s email system hacked – September 2017

Offense guides defense (2/2)

- > Equifax data breach - August 2017
- > Bank of Bangladesh cyber robbery – February 2015
- > Dyn DDoS attack - October 2016
- > Shipwreck of the oil tanker Erika - December 1999

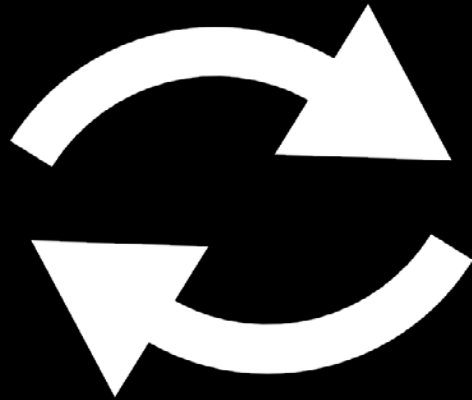
security policies --> real-life attacks (1/2)

- > Target data breach Network segregation
- > Drug traffic in the port of Antwerp Requirement for regular penetration tests
- > “Le Monde” Twitter’s account hacked 2-factor authentication
- > Deloitte’s email system hacked 2-factor authentication

security policies --> real-life attacks (2/2)

- > Equifax data breach Vulnerability and Patch Management policy
- > Bank of Bangladesh cyber robbery Hardening, VPM, 2FA, operational process (missed alarms)
- > Dyn DDoS attack Security assessment methodology (Risk acceptance?)
- > Shipwreck of the oil tanker Erika Regulations and certifications

Dialectic?



What can we learn from attacks
regarding... security policies ?

real-life attacks --> security policies (1/4)

- > *Target data breach*: were compliant to PCI-DSS... **Compliance to a policy is never enough...** one must test (independently from the policy guidance). Furthermore, the attack began at a third party side: **how to enforce security policies by 3rd parties? Shadow IT?**
- > *Drug traffic in the port of Antwerp*: IT systems are often **not industrialized, but artisanal**. Poorly standardized. Policies should be **tailored**.

real-life attacks --> security policies (2/4)

- > *“Le Monde” Twitter’s account hacked / Deloitte’s email system hacked: Same factor... few history. We are not used to learn lessons.*
- > *Equifax data breach: they had a VPM policy... but was not enforced. Regular controls have to be implemented.*

real-life attacks --> security policies (3/4)

- > *Deloitte's email system hacked*: they were ISO certified... but did probably not implement **real processes and controls** (a piece of paper never stopped a bad guy). **Prioritise, focus on essentials** avoid endless documentation

Remember Parkinson's Law of Triviality: organisations give disproportionate weight to trivial issues (it is much more easy to spend a lot of time on policies than in implementing real controls)

real-life attacks --> security policies (4/4)

- > *Bank of Bangladesh cyber robbery*: began with a LinkedIn approach: not enough **awareness, security testing and training**
- > *Dyn DDoS attack*: policies and regulations often rely on **non-regulated fields and industries**
- > *Shipwreck of the oil tanker Erika*: **certification process should not rely on third parties paid by the entity being certified**

Conclusions

- > Policies have to be adapted, tailored
- > Learn lessons from past events
- > Do not only rely on paper, implement real controls
- > Prioritise, focus on essentials
- > Avoid endless documents and discussion around
- > Enforce policies, control their application
- > Test, train and raise awareness
- > Identify and take into account non-regulated domains
- > Ensure that certification & audits are independent

i thank you for your attention !

¿ questions ?

iro@cryptosec.org
Twitter @secucrypt