TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop 2011

München, 30.06./01.07.2011

Dr. Bernd Grobauer
Siemens AG

A Scenario-based Outlook on (Corporate) IT-Security

SIEMENS

Corporate Technology

A Scenario-based Outlook on (Corporate) IT-Security

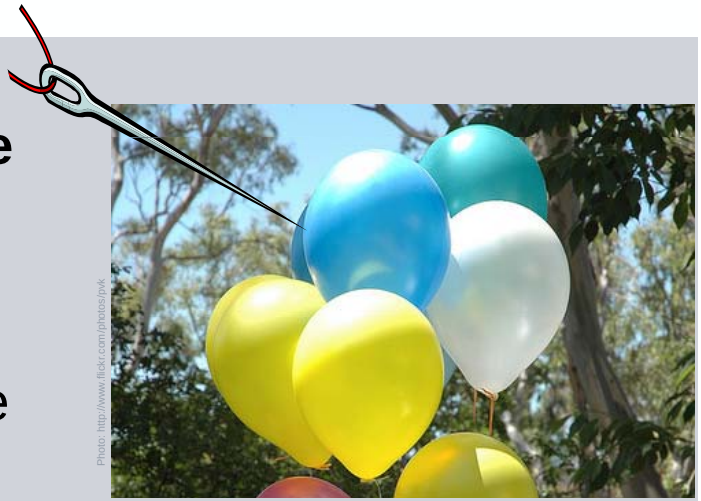
TeleTrusT-interner Workshop 2011, München, 30.06./01.07.2011

Dr. John Fichtner, CT T SSS CER – Siemens CERT
Dr. Bernd Grobauer
Dr. Jan Göbel

There are indicators for two worrying “mega” trends in IT security

SIEMENS

- **A significant increase of the attack surface**
  - more and more aspects of daily life (personal & corporate) become digital
  - there are more and more IT devices … and they are constantly connected to the Internet



- **Attacker’s capabilities consistently exceed defense capabilities**
  - New attitudes create new attackers
  - Money continues to motivate attackers
  - Nation states entering the arena
  - Attacks against cornerstones of IT and Internet security

SIEMENS

Lives become truly digital

Present

Emerging

Not too distant future

eBanking

- Arrange your financial tasks online, stock exchange, money transfers

Social Networks

- Meet your “friends” online, expose your life, pleaserobme.com, …

eGovernment

- Digitalize citizens services
- Online tax declaration, residence registration, …

eHealth

- Your medical history, medication plan, exercise data, etc., is all online

eIdentity

- Your complete identity is in the Internet, your name, your address, your work & life, …

eEverything

- You interact with everything around (car, house, shops you pass on your way, … via the Internet)

SIEMENS

Corporate data processing using interlinked cloud services

- A few examples of how the cloud transforms corporate IT:
  - With SuccessFactors, Salesforce, etc., central topics such as HR and CRM are moving to the cloud
  - Moving to web-based Office tools is a possibility that some corporations are seriously considering
- If you found a new company now, how much “own” IT are you likely to build up? Probably very little!
- There are offerings with a functional USP, for which no “on-site” product is offered: if you want offering service, you have to go into the cloud!
- The “cloud” may finally make true the vision of “service-oriented architectures”, making applications built upon interlinking services the norm

SuccessFactors
People Performance

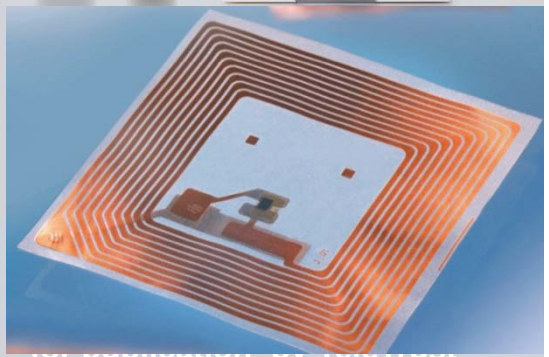
amazon web services™

Google Docs

SIEMENS

IP Connectivity for a multitude of devices

- Networking for Supervisory Control and Data Acquisition (SCADA), building control systems, smart metering, etc.
  - Devices become controllable via the Internet that were never designed to be accessible from the outside world
  - Proprietary protocols and operating systems are increasingly replaced with Internet standards and commercial off-the-shelf (COTS) products that are well known
- Increasing miniaturization and practically infinite address space of IPv6 enable „Internet of Things“, where truly everything is connected



SIEMENS

There are indicators for two worrying trends

- **A significant increase of the attack surface**
  - more and more aspects of daily life (personal & corporate) become digital
  - there are more and more IT devices … and they are constantly connected to the Internet

Photo: http://www.flickr.com/photos/pvk

- **Attacker's capabilities consistently exceed defense capabilities**
  - New attitudes create new attackers
  - Money continues to motivate attackers
  - Nation states entering the arena
  - Attacks against cornerstones of IT and Internet security

Photo: http://www.flickr.com/photos/fceefoto

New Attitudes create new attackers: Whistleblowing & Hacktivism

SIEMENS

- Whistleblowing
  - The “Wikileaks” attitude: it is OK or even laudable to leak data
  - State governments buy CDs with stolen banking data

- Hacktivism
  - Defense of Wikileaks by “Anonymous”
    - DDoS attack against City Bank, Sony (not so effective)
    - Take-Down of “Enemy” HBGary (**very** effective)
      - Relatively simple attack
        - SQL injection
        - Social engineering
        - Shared passwords
      - ⇨ attacker owns everything
        - Steal & publish vast amounts of sensitive data
        - Sabotage systems and destroy backups
        - Compromise Twitter, LinkedIn etc. accounts of C-level executives

Photo: http://www.flickr.com/photos/el_bobo_es/espanio

SIEMENS

Attackers go where the money is

- Crooks go where the money is and where it is easy to get
- Internet Fraud: SPAM, „Scareware“, ...

- Thriving underground economy
  - Selling and buying of stolen data
  - Attack tools „as a service“
- Organized crime & criminal affiliate networks
- Money is the key that powers the more and more sophisticated attack machinery.

SIEMENS

Nation states entering the game of cyber attacks

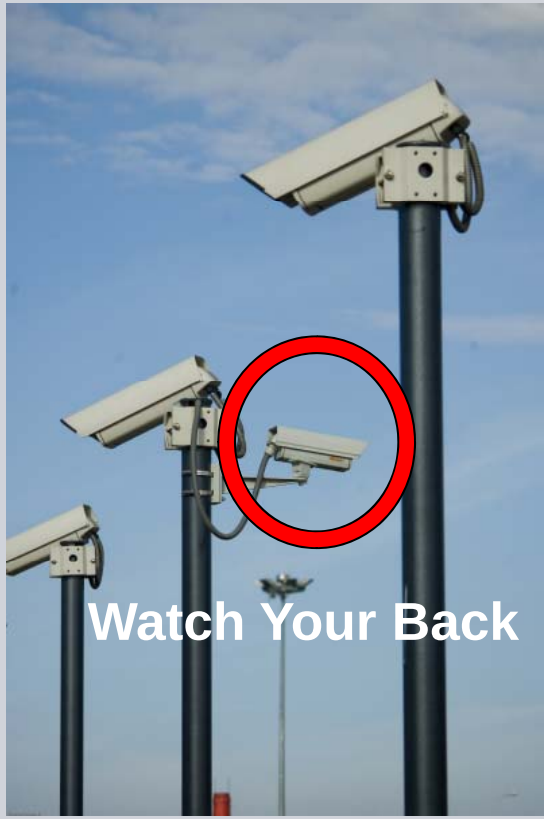
- State-sponsored/approved hacktivism
  - In May 2007, Estonia's IT infrastructure was hit by a massive DDoS attack from Russia after decision to relocate a Red Army soldier statue
  - The 21-year-old Iranian who claimed that he carried out the "Comodo certificate hack" for patriotic reasons … and is unlikely to be prosecuted in Iran for his activities

- Stuxnet Worm may be a first example of new "make malware, not bombs" approach to international conflicts
  - Unusual complexity for current malware (4 zero-days), uses signed drivers
  - Many people are now aware of what can be done in the arena of SCADA systems
  - Digital non-proliferation seems very tricky

SIEMENS

Attacks against cornerstones of IT and Internet security

- RSA Security Hacked
  - Successful advanced persistent threat attack
    - „2011 Recruitment plan.xls“ contained zero-day Flash exploit
    - Has compromised the security of the authentication product SecurID
- Comodo Certificate Hack
  - Compromise of world’s largest webmail providers certificates to secure email communication: Google Gmail, Microsoft Hotmail, and Yahoo Mail
    - Attack was possible due to insecure account password and hardcoded credentials in certificate request scripts
    - 21-year-old Iranian claims responsibility



From trends towards scenarios
Dealing with uncertainty

SIEMENS

- As stated previously, these are two very broad/abstract trends, and we cannot know at the moment, how far things are going to go

- But we can draw them as an axis and get some better understanding of their meaning by thinking of extremes.
- Let us look at the example of an individual person first, what would be the minimum, i.e. the best case, and what could be the maximum, the very extreme with regards to IT security in the future

From trends towards scenarios
Extremes of Trend „Increasing attack surface“

SIEMENS

Maximum:

- Pretty much **every aspect of daily life is digitally** shared using social networks
- People are **always online all the time**, juggling content between several devices that synchronized via cloud services.
- The government has pushed **eGovernment to the maximum**; everything from registering your car to marriage and divorce is subject to eGovernment

Minimum:

In some aspects (e.g., use of Internet services) more minimal than today (most likely driven by serious privacy/security issues)

From trends towards scenarios
Extremes of Trend „Attacker's capabilities consistently exceed defense capabilities“

SIEMENS

Minimum:

- **compromised home PCs become the exception** rather than the norm
- **Internet fraud is down**, because people have learned to recognize it
- **ID theft is also down**, because reliable ways of providing identity have become common place.
- **Attackers are deterred** by improvements in digital forensics and international co-operation on law enforcement: there is a real chance of being caught now!

Maximum:

- **Information cannot be trusted anymore**: falsification is common place
- The **private information** is regularly disclosed
- **Internet fraud and identity theft are rampant**: not having been victimized is pure luck
- **Attackers run virtually no risk**, because hardly anyone is every caught.

SIEMENS

The Combination of the two trends results in 4 scenarios

The Combination of two trends results in 4 scenarios Resulting Questions

SIEMENS

With this chart in mind, four questions come to mind:

- A: What will **not** change in IT security?
- B: What **has** to change in IT security?
- C: How do we know which direction things are moving?
- D: What is our strategy in “sailing” on this chart?

Not changed, but challenged: Basic "truths" of IT-Security

SIEMENS

Defend against basic attacks first

“The employee is key”

Know where your crown jewels are and protect them

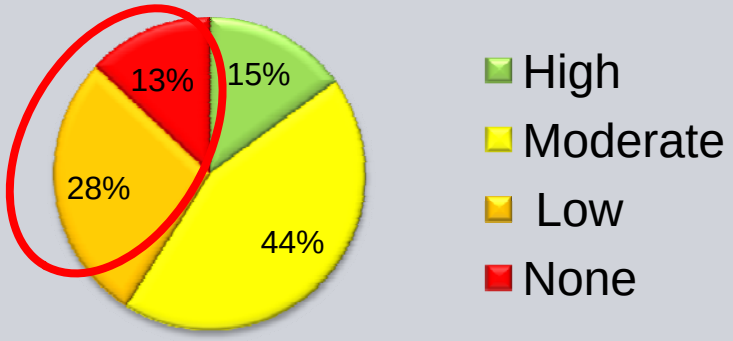
Be able to detect when something goes wrong

Know how to react when things go wrong

SIEMENS

Defend against basic attacks first

- We need to define an appropriate level of base-line security and get that level right
- With the exception of Stuxnet, none of the attacks we talked about before, were very sophisticated
- Challenges:
  - Also capable attackers try easy stuff first
  - Will rising attacker capabilities force us to adapt a higher level of base-line security?
  - How to assure base line security in open IT infrastructures?
    - Cloud service providers
    - User-owned/managed devices



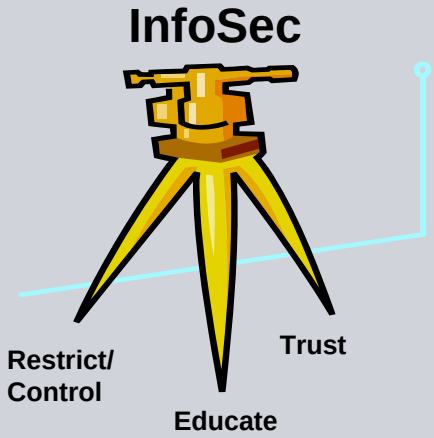
Attack difficulty of cases handled by Verizon in 2009

SIEMENS

The employee is key

- The human remains at the center of all IT security activities: all technical restrictions and controls are only effective if human actions do not counteract or circumvent them

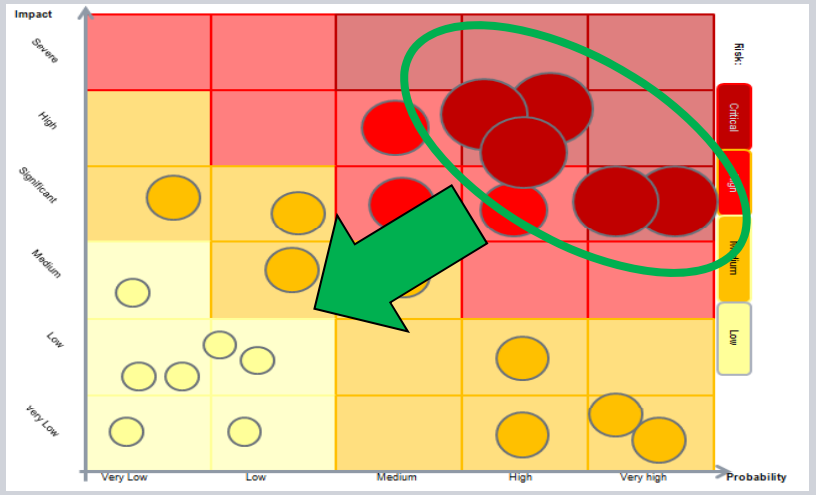
- Corporate IT security requires balance between trust of employees, education of employees and restrictions/controls
- Challenge:
  - Social engineering is likely to become even easier with so much PI “floating” around
  - With more open IT infrastructures, for many scenarios, the balance may have to shift more towards trust and education than we currently feel comfortable with



SIEMENS

Know where your crown jewels are … and protect them

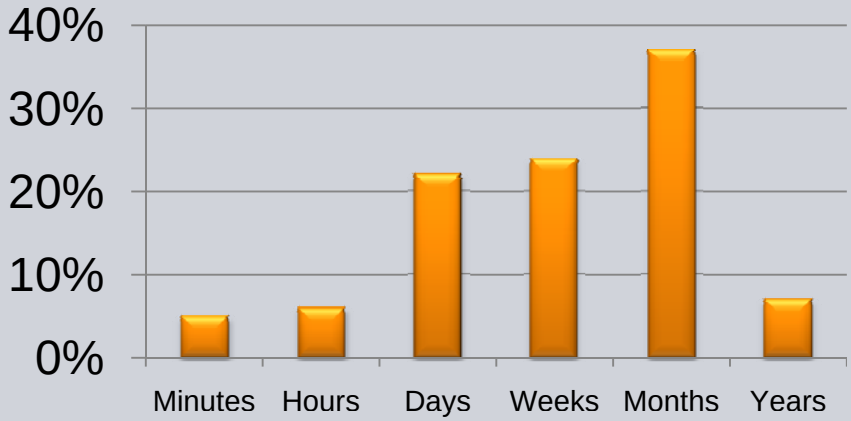
- Risk-based decisions are key: we need adequate protection for our assets
- The first step must be to identify what is really valuable to us … we must know what/where our “crown jewels” are.
- Challenge: It gets increasingly important to get this right:
  - Capable attackers will circle in on high-value targets
  - With an increase of digital data, various locations, service providers and devices, we must focus!



SIEMENS

Be able to detect when something goes wrong

- Early detection can dramatically decrease or completely avoid impact
- Statistics show that often weeks/months go by before an incident (series) is detected
- Challenges:
  - With improving attackers, timely detection becomes harder and more important at the same time
  - Open IT infrastructures add a whole new level of complexity

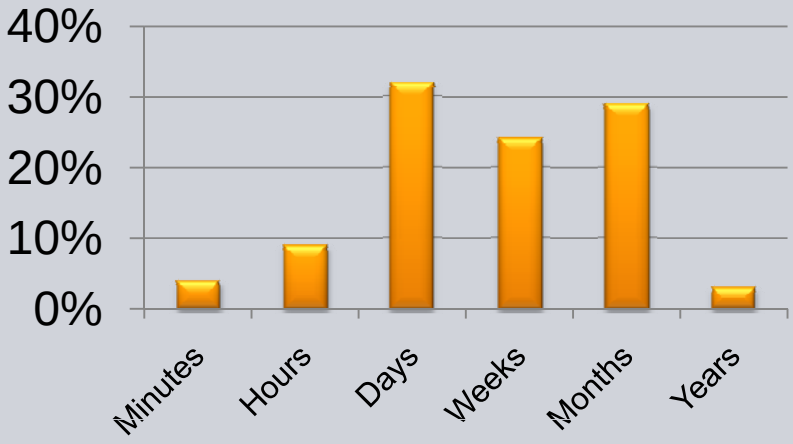


Time from compromise to detection in 2009 Verizon cases

SIEMENS

Know how to react when things go wrong

- Timely detection only helps if we can act upon it to contain the incident
- Statistics show that often weeks/months go by before an incident can be contained
- Challenges:
  - The Comodo and RSA hacks showed: attackers may target corner stones of Internet security: how can we react?
  - In an open IT world, where incidents occur at a cloud service or on a private user-owned device: do we have the ability to react properly?



Time from detection to containment in 2009 Verizon cases

for publication by TeleTrust

The Combination of two trends results in 4 scenarios Resulting Questions

SIEMENS

With this chart in mind, four questions come to mind:

- A: What will **not** change in IT security?
- B: What **has** to change in IT security?
- C: How do we know which direction things are moving?
- D: What is our strategy in "sailing" on this chart?

SIEMENS

How do we know in which direction we are moving?

- The good message: there are plenty of resources on general trends regarding IT security – it is relatively easy to get an idea of where things in general are headed.
- But, what about the specific situation of your corporation? For example: if you are detection relatively few incidents: is that, because there are few attacks or because the attackers are outsmarting us?
- How can you know, where you are on the x-axis of our chart and in which direction you are moving?

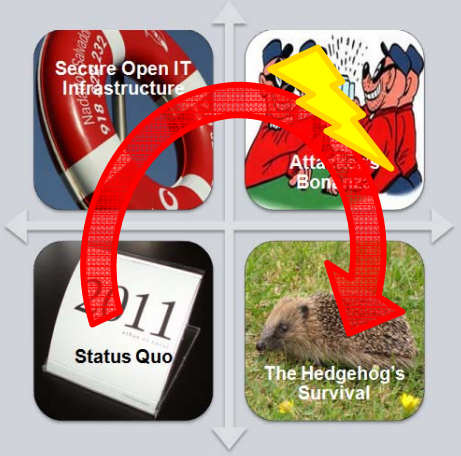
SIEMENS

What is our strategy in “moving” within these trends?

- There is the danger of a round journey
  - from the *status quo*
  - toward more openness
  - into trouble (“attacker’s bonanza”)
  - back to a hedgehog’s strategy as last line of defense for survival

- How fast does your corporation want to make the step from the status quo towards opening up your IT infrastructures?

- In certain cases, being a late adopter does have its advantages!



SIEMENS

Conclusion

- Trends regarding the increasing attack surface and rising attacker capabilities are cause for concern
- The basics of InfoSec continue to serve as compass, but we have to
  - adapt in order to meet the challenges:
    - shore up preventive defenses
    - heavily increase detective and reactive defenses
  - know where we are and where we want to go

