Current Security Issues in Corporate IT Environments

Dr Wojciech Swiatek

Director, EMEA Motorola Security Services

What this presentation is about

- No technical aspects (well, almost...)

(... some time left for people to evacuate ...)

- Picture of the security in large scale organizations
- Usually not applicable to SOHO environments
- Based on real assessments worldwide (sources follow)

Sources

- Environment
  - Large companies
  - Government organizations
  - Telecom operators
- Scope
  - Overall connectivity (wired, wireless, specific)
  - Network, host security
  - Policies
  - Organization, budget, investement strategy
  - Physical security

Buzz vs. Real World

- Security assessment is a trendy activity
  - Consulting companies
  - Technology companies
  - Round-the-corner companies
- Two kind of security approaches
  - Standard-based
  - Best practices
- Implementation must be carefully weighted
  - Risk, risk and risk
  - And risk

RISK

The world of security

I almost broke into NASA yesterday

SOME security management

The circle of friends

I have my ways to do security

You make a ping sweep, yah know, and then you you ACK-scan, ya know...

We are here to solve your problems

And the winners are...

(in no particular order)

Patching strategy

- The most typical IT issue
- Patching startegies:
  - No patching
  - Ad-hoc patching (usually users)
  - Enterprise patching (which works or not)
- Type of attacks
  - Zero-day: trendy, for bleeding edge techies
  - Reality strikes back
  - Many 2003-2006 patches missing
  - Good hackers do not try to exploit a rumor, they wait for the patch

Reactivity

- An issue arises and then what?
- From an AV alert to a global disaster
- IDS/IPS are good but one needs to analyze, correlate, react
- Outsourcing to a SOC?

People ...

- ... make mistakes
  - „clickers”
  - `# rm -fr * .o`
  - historical data
- ... are emotional
  - rage
  - vengeance
  - politics
- ... are atavistic
  - they like to talk
  - they are lazy
  - they do not like to be in the same room as a decision
- Over 60% of the cases were detected by people outside IT security staffs, 35% of them by **customers**.

Lack of policies

- **Policies document a process. They are not an art display.**
- They must:
  - make sense!
  - be implemented
  - be enforced
  - be reviewed
- Generic vs. tailored
  - look outside your day to day environment
  - ensure an exception process
  - create plug-ins for exceptions
- Legal aspects
  - ethics
  - licensing
  - SOX, Basel II, ...

Communication devices

- Your employees use:
  - Laptops running Vista this, Vista that, MS Windows XP, 2000, SP1, SP2, SP3, SP4, SP5, SP6
  - Desktops running Vista this, Vista that, MS Windows XP, 2000, SP1, SP2, SP3, SP4, SP5, SP6
  - Laptops from Dell, Toshiba, HP, Acer, California Computing, Sony, IBM
  - Desktops form Dell, HP, IBM, Optiplex, Gateway, home made
  - Laptops running ubuntu, gentoo, kubuntu, fedora, RH, Linware, LinuxFromScratch
  - Desktops running linuxes with 2.4.x to 2.6.x kernels
  - Blackberries
  - Treos
  - PocketPCs
  - Smartphones
  - External disks
  - Flash drives
  - SUN, IBM, HP boxes
  - mp3, mp4 players
- One common aspect: They all store data you do not want to leak out

What to protect?

- Today, we protect:
  - networks
  - devices
  - operating systems
- Incidentally, the valuable stuff is:
  - data
  - Information
- And finally we protect everything the same way (DRM anyone?)

Network topology

- Everything accessible form everywhere
- Usually an effect of the growth
- Very dangerous when you have a varied landscape
  - office space
  - supply chain
  - manufacturing
  - research labs
- Wireless networks extend beyond your walls
- DSL lines are cheap and easy to order

Applications

- Several layers of data processing
  - the network (TCP/IP, IPX, ...)
  - the operating system (Win, Unix, MacOS, ...)
  - the backend service (Oracle, clearcase, ...)
  - the backend engine (Java, tomcat, AJAX, ...)
  - the application (finance, portal, ...)
- The deeper you go:
  - the less tested
  - the worse support
  - the more tailored

Spam

- User driven
  - education
  - usually does not help
- Phishing
  - education
  - usually does not help
- Blackmail
  - a virus encrypts data and a decryption key is made available after treansferring money

DRP/BCP/CM

- Tough area:
  - costs to create, test and maintain are high
  - no obvious ROI
  - usually created in house with limited experience
- Too often an IT problem
- Different pieces do not come together
  - DRP: IT
  - BCP: Operations
  - CM: management
- No involvement of finance, HR
- Way too technical
- Spectacular failures (New Orleans, 9/11, wars)

Conclusions

- **Look for experienced assessors**
  - been there, done that
  - experience of scale
- Your common sense is your friend
- Best practices are an average
  - Works for some, not for others
  - Usually easier to implement than standards
  - The ultimate filter is common sense
- Assess risk and invest accordingly

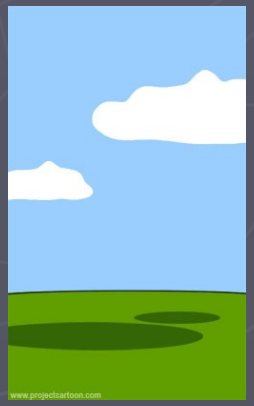
The Security Project Lifecycle

Sales talk to management

Management orders the service

IT tries to get the right thing

Then comes the invoice



Followup by the consultants