Hot Topics from a Security Consultant

Lea Viljanen
Ph.Lic, GSNA, CISSP
Lea.Viljanen@lavsecurity.fi
Agenda

• Who am I and what do I do?

• Planning secure.

• Ensuring secure.

• Questions.

LAV Security Oy
http://www.lavsecurity.fi/
Who am I

• Graduated with an MSc in 1995.
• Nixu Oy, from 10 to 100+ people, more and more with security consultant focus.
• Left Nixu, did an interim CISO stint
• Now I have my own one person security consulting company - LAV Security Oy.
  – clients range from small startups to listed companies and government agencies
What are the key questions today?

- How can we be secure as an organisation to prevent data leaks and hacks?
- How can our service/product be secured?
- How can we be assured that our finished product is now secure to be deployed?
I. PLANNING SECURE
THERE IS NO SUCH THING AS ABSOLUTE SECURITY

It is all about **MANAGING RISK** to a reasonable level.
Risk

• Going outside is a risk:
  – slipping on icy pavements, traffic accidents, spree killers...

• Staying home is a risk:
  – electrical fires, falling in the shower, food gone bad...

• Even breathing is a risk.
CRACK

BOOM

WHOA! WE SHOULD GET INSIDE!

IT'S OKAY! LIGHTNING ONLY KILLS ABOUT 45 AMERICANS A YEAR, SO THE CHANCES OF DYING ARE ONLY ONE IN 7,000,000. LET'S GO ON!

THE ANNUAL DEATH RATE AMONG PEOPLE WHO KNOW THAT STATISTIC IS ONE IN SIX.
Risk analysis

• We still do these risky things because it brings us benefits
  – shelter, food, social contacts, education...

• But is the risk likelihood and its impact bigger than the benefits?
  – Every day we evaluate this subconsciously
DARWIN
Naturally selecting for the good of humanity since 1859.

LAV Security Oy
http://www.lavsecurity.fi/
Risk and business

• Similarly, companies have business needs and business goals, which bring in the benefits.

• In today’s agile business environment it means networking with others, opening up previously internal services and APIs, BYOD....

• This contains risks. Security people see the risks, but seldom the benefits.

LAV Security Oy
http://www.lavsecurity.fi/
MORDAC, THE PREVENTER OF INFORMATION SERVICES.

SECURITY IS MORE IMPORTANT THAN USABILITY.

IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.

To complete the log-in procedure, stare directly at the sun.

© Scott Adams, Inc./Dist. by UFS, Inc.
Security people

• The classic view on any security people is that they are the knights that always say **NO**.

• In some organisations, business people have stopped asking because of this and just do...
All aboard the Failboat
Say YES with risk analysis.

1. Identify threats and misuse scenarios.
2. Assess each for likelihood and impact.
3. Select key scenarios which are too risky.
4. Design controls and countermeasures to diminish key risks into tolerable level.
5. Say YES and give the cost of controls.
6. Get approval and implement.

... PROFIT!
Organisation vs. product

• The process is the same regardless of our scope (organisation vs product/service)
• On organisational level threats are a bit more abstract and more hand waving.
• On product level the scenarios can be very specific.
• Implement risk analysis as part of your management or development process!
Benefits of risk analysis

- **Cost effective**: We put our money into controls that are the most important.
- **Trackable**: We can justify each euro by detailing what threats it mitigates.
- **Understandable**: Management understands the concept of risk.
- **Proactive**: Become secure by adopting controls before becoming a victim.

LAV Security Oy
http://www.lavsecurity.fi/
II. ENSURING SECURE
When we have made something

• There is always a question, is this secure enough to be deployed.

• Usually about a week before deployment deadline..

• So we call a security auditor.
Mrs. Vilj... Robinson

Hi, this is your son's school. We're having some computer trouble.

Oh, dear - did he break something? In a way-

Did you really name your son Robert?); DROP TABLE Students;-- ?

Oh, yes. Little Bobby Tables, we call him.

Well, we've lost this year's student records. I hope you're happy.

And I hope you've learned to sanitize your database inputs.

LAV Security Oy
http://www.lavsecurity.fi/
A sad fact

• Every system is somehow breakable given enough time & money & smart people

• Unfortunately audits are limited in scope.
Method choices

• **Approach:**
  – Technical vs. process vs. social engineering

• **Level of knowledge:**
  – Black box vs. white box

• **Methods:**
  – Application vs Network vs Source code vs…

• **Tools:**
  – Automated or manual

LAV Security Oy
http://www.lavsecurity.fi/
Typical findings

• Servers:
  – missing patches

• Web applications:
  – cross-site scripting
  – authorisation failures

• Processes:
  – some short cuts taken
  – not enough audit trail

LAV Security Oy
http://www.lavsecurity.fi/
Benefits to audits

• The obvious security issues will be revealed.
• Pick out the low hanging fruit.
• After a competent technical audit you’re probably safe from a random internet attack.
• But not from a really determined party.
• It’s really best to **build security in**.
Conclusions

• Understand risk and business needs.
• Say YES and give conditions.
• Plan security from the start.
• Revew risks and countermeasures regularly.
• Check the implementation with an audit.

LAV Security Oy
http://www.lavsecurity.fi/
SECURITY
IT GIVES US THAT WARM & FUZZY FEELING
AND USUALLY A DESIRE TO FIND A WAY AROUND IT

motifake.com

LAV Security Oy
http://www.lavsecurity.fi/
Questions?

THANK YOU!

Lea Viljanen
Lea.Viljanen@lavsecurity.fi