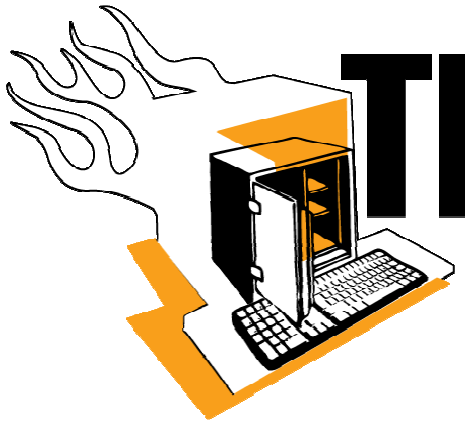

TROOPERS10

IT-Security Conference & Workshops

How to fail an (ISO27001) audit –
Wie man durch ein Audit fällt

secunomic GmbH
www.secunomic.com

Martin Freiss
mf@secunomic.com

But seriously….

- A not so serious talk on a very serious topic.

Why this talk?

- We do all kinds of audits – ISO27001, best practice, vuln scans, as preparation for SOx, PCI-DSS, ….
- We have 2 accredited (by DQS) ISO27001-Auditors and qualified auditors for 20000 (ITIL), 27001, PCI-DSS, …
- And the life of an auditor is a lot less boring than you would think.

What I want to talk about…

- The Hitchhiker´s Guide to ISO27001 – an intro for those who wonder why one does audits
- Before the Audit
- During the Audit
- After the Audit
- After the Audit is before the Audit

A word on 27001 and audits

- **Vulns and hacking and firewalls are exciting stuff, but only one part of the picture.**
- **`If you think technology can solve your security problems then you don't understand the problems and you don't understand the technology.` (Bruce Schneier)**
- **So what is missing?**

secunomic
security meets business

Global views – local impacts

What is missing?

- Some help in making the right decisions about security
- „In Zweifelsfällen entscheide man sich für das Richtige“ – Karl Kraus (1874-1936)
- Not really helpful, is it?
- So, we need something that can serve as a basis for decisions…

What is 27001 about?

- It‘s about understanding what you do, and where the risks are.
- It‘s about management and control (and the German translation for this is not „Kontrolle“!).
- It’s about defined processes, documentation, known corrective and preventive actions, and management review – and the technology to support this.
- Almost sounds like – eek – ISO9000… ☺

A word on 27001 and audits: securitymanagement

… and it is! Knowing what good security (or a good job) is about…

Very trivial questions:

- What is the difference between good and bad security? (Strategy / Plan)
- How do you implement security and ensure you have good security? (Assurance / Do)
- How do you measure security? (Quality / Check)
- How do you (re-) act? (Act)

A word on 27001 and audits: What do we really need?

- This needs an understanding of the business requirements
- It does not necessarily need tools. A fool with a tool…

A word on 27001 and audits

- … but it needs audits – internal and external.
- You probably thought we'd never come to that.
- Audits give valuable input, a different perspective…
- … because the risks are usually not where you think they are.

Bombs are harmful – in unexpected ways.

A word on 27001 and audits

- … that was a nice example of what an auditor would probably have seen coming.
- Besides 3rd party input …
- Audits are necessary for a security certification, (i.e. marketing reasons, customer pressure, or an enlightened view of what security is about…)
- … in which case they are more like examinations, which is the German view of what audits are all about anyway.

Finally

- So, what can you do wrong in audits?

Oh god, what have we done?

- Audits are done because the customer wants to be audited (and have a certification).
- That‘s what the auditor thinks.
- In real life, immediately after ordering an audit, companies go into panic mode and view the auditor as… THE ENEMY

Before the Audit

- **Haggle!**
  - **With the certification body**
    - **Which is often bound by rules it cannot change (e.g. ISO27006)**
  - **With the Auditor**
    - **Who is usually at the end of the food chain and can do nothing about the price anyway.**
- **Always take the cheapest!**
  - **Why pay money for being tortured?**

Examples of cheap audits…

- Now what?

GG_SA040	ITS-1	The Apache web server running on the remote server is outdated. This version is affected by several security issues including, DOS, buffer overflows, cross site scripting and similar. Following systems are affected: • [redacted] • [redacted]	A		
GG_SA041	ITS-1	The Sylantro Server Status Flash application	A		

- Now you see it…
  now you don‘t

GG_DA013	BACKUP 2.01	**Availability Management** A backup concept for [redacted] exists and defines the relevant aspects. In the section [redacted] it seem that no such backup concept is existing yet but the requirements to the backup/restore infrastructure are defined by the project team already and includes several restore situations with appropriate check lists. Backup and restore procedures from the supplier are available. Based on these requirements the operational group creates the backup concept by end [redacted]	A		
GG_DA014	BACKUP 2.02	**Availability Management** A general backup/restore concept valid for all sections and including all applications does not exist. Different backup/restore solutions and processes	A		

Before the Audit

- **Never take the time to prepare!**
  The Auditor is always happy to come and waste his time:
  - **Interview partners are completely surprised**
  - **Documents are lost and need to be found**
  - **Interviews take place in the casino**
  - **No access to the data center, sorry about that**
- **Never prepare the staff for an audit!**
  - **This creates a nice examination-type atmosphere: You, talk to the auditor and IT‘S ALL YOUR FAULT IF WE FAIL!**

Before the Audit

- And then there was…
- The Auditor from England, who got mugged by drunk women on Weiberfastnacht on Düsseldorf Airport (maybe not such a good time to do an audit in Germany?)
- The Auditor, who had no common language with his interview subjects (surprise, surprise…)

During the Audit – First impressions always win…

- **The cabinet full of empty beer bottles …**
  Kamil I, Consultant
- **The whisky collection in the raised floor**
  Not such a rare occurrence
- **19“ racks are for waste-paper storage, obviously**
  Stefan Z., Operations
- **The underwear we found in the data center**
  The auditor wonders what to put in the report?

During the audit – who is this guy, and why does he talk to me?

- „Why do you ask all those silly questions? It‘s all documented, look in the bloody docs!“
  Dr. S.P., Teamleader Operations

- „Administration processes? Well, we use sudo for all administration that needs root priviledges, and the processes do have root then, but the users can… “
  „????“
  U. D., Operations

During the Audit – the Executive View

- „Management Support? Oh, that means us? I always thought this was network management.“
  A. P., CEO
- „We only have one process: permanent improvement“
  S. W., CIO
- „Erm… Mr Meier, who is the privacy officer again?“
  S. P., Managing Director

During the Audit – why do we do this at all?

- „Restrict access? But we are all colleagues here!“
  S. K., Project Manager
- „Incident Management? We never had any incidents!“
  A.L., CISO
- „We don‘t do preventive measures. We don‘t have enough staff for that.“
  B.V., Department Head for Security

During the Audit – Somebody Else‘s Problem

- „Compliance / conform to laws? We don‘t do that here, the legal dept. does that.“
  A. R., Internal Audit
- „Training of employees is not my responsibility, HR does that.“ (on security awareness)
  F. L., CISO
- „The CEO had other pressing business, like last year.“
  A. B., CISO

During the Audit

- Finally, an opportunity to badmouth the company you work for!

- …and always focus on the things that don‘t work.
- …the more technical detail, the better.
- Is this a German problem?

During the Audit

- **The top 4 ways to waste time:**
  - **Explain the org chart – past, present and future (#1 at big companies)**
  - **Five course lunch at an expensive restaurant far away. Preferably with wine to get the auditor drunk.**
  - **Detail, more detail and even more detail… the speedtalkers at internal audit**
  - **Tours that take forever**

During the Audit – the other side

- **Auditors are not omniscient….**

…and the good ones know that.

During the Audit – the far side

- There are of course the others, who…
  - … check first aid kits for completeness during an 27001-Audit (is that business continuity?)
  - explain to a major data center how virus protection on their PC works and that their favorite personal firewall product should be installed everywhere
  - What does SAP stand for again?
  - Explain to the company under audit how to improve their business strategy
  - Hold long boring talks
  - … and the SAP viruses? How do you protect against the SAP viruses?

After the Audit

If the (expected) audit report is not good:

- **Whine.**
- **Argue with the auditor.**
- **Raise doubts about his qualifaction, or his understanding of the standard**

After the Audit

- **Old saying:**

  To argue with an auditor is like wrestling with a pig in the mud -

After a while you realize that the pig enjoys it!

After the Audit … is before the Audit

- Never do anything about the audit findings and suggested mitigations (we know better, right?)
- … and if you do, do it the night before the re-audit.
- If you hand over documents, make sure they are still warm from the laser printer…
- … and if you need to produce evidence for processes, make sure all the documents have a change date of yesterday (so we all can see they are faked).

After the Audit … is before the Audit

- The end
- Questions?