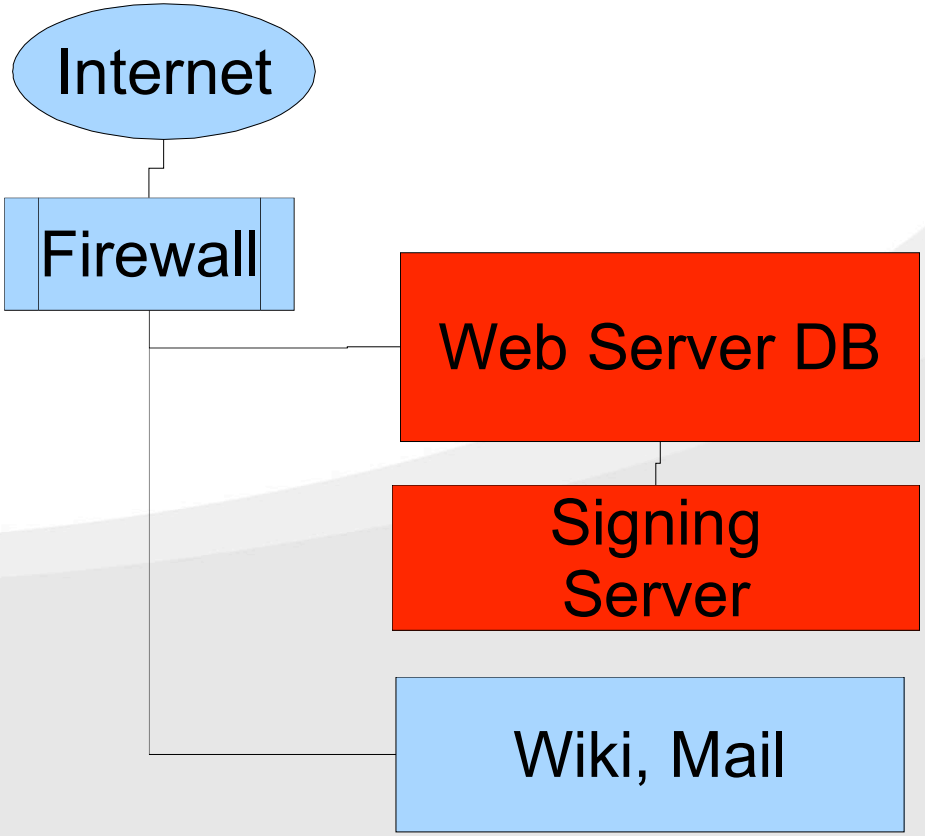
CAcert Day 4 - Systems

Philipp Gühring

History of the Systems

- **Network-Concept that was used in Australia:**
- **Security mechanisms:**
- **SSH filtered on source IP**
- **RS232 link to Signing Server**
- **No network access to Signing Server**



Architecture

- 1 Main datacenter (Web, Signing, ...)
- 1 Hot-Standby Datacenter (off-country)
- 10 servers for high-availability services (CRL, OCSP, Stamp) distributed worldwide on high-bandwidth locations
- 5 servers worldwide for high-security services (ITTC) on high-security locations
- Independent cluster of >= 3 DNS servers

Progress of migration

- **We had do a quick move of all the core-systems from AU to AT in late 2006 due to unavailability of hosting solutions.**
  - The CommModule had to be rewritten from scratch, all other parts were transferred 1:1
- **The initial setup of the datacenter in NL happened in March 2007**
  - We did the installation of the security mechanisms and the security check of the datacenter during April and May.
  - Since June we are transferring service after service from AT to NL. Some services are transferred 1:1, some services are rebuilt or improved during the move.
  - Currently successfully transferred:
    - OCSP
    - Backup
    - Subversion
    - IRC

Security

The audit demands a Security Manual.

At first we tried to outsource the creation of the security manual, to avoid insider-blindness. But that didn´t worked, since the people that tried it weren´t experienced enough in writing security manuals.

Then we searched for people that are experienced in security-manual-writing, and found a SO of a bank that helps us.

Then we learnt that a security manual is normally the result of a threat- and risk-analysis, not a document that can be written from scratch itself.

So we started with listing assets, objectives, values, and threats, and we will continue by evaluating the threats, qualifying them, listing possible measurements, and finally writing guidelines that will result in the Security Manual.

Assets+Objectives -> Threat Model -> Risk Analysis -> Security Manual

SecurityManual/ThreadModel.odt

SecurityManual/SecurityManual.odt

Assets

Vienna data center

3 Servers are provided by local people

Domains and DNS

cacert.org, cacert.com, ... are owned by CAcert Inc.

DNS is provided by SRN5

NL data center

NL datacenter with 6 servers, 2 firewalls, 1 SAN, several switches

are provided by Oophaga

status of Australian servers

The new server is stored by Robert. The 3 old servers are still in Australia

Personal computers of admins

Support

- support@cacert.org is currently handled by Guillaume and Philipp
- support handling is currently running smoothly (no considerable backlog)
- Support only available when Guillaume or Philipp has time for it.
- Support handling takes too much of my time.
- ->We could need more (perhaps 2) trustchecked people with enough time to help with core support.

Software Development

Open Source

I tried to find people to help with making CAcert OpenSource, but I got no replies yet.

It wasn´t clear to me, whether there was an actual board decision, or just an agreement that CAcert will go OpenSource.

Software

- **Projects:**
  - LibreSSL
  - API
  - Education
  - Certificator, AEP
  - ITTC
  - CommModule
  - SecurityDatabase
  - Timestamping
  - mod_ssl
  - OpenSSL
  - OpenXPKI/OpenCA
  - ILO Security
  - Security Logfiles
  - Tverify
    - SignatureCard
  - Random Numbers
  - Miss Venona
  - Timestamping
  - UProve, credlib
  - Vhost-Taskforce
  - Translingo

Issues

Advertising

We had several people that were not happy with the board-approved advertising on the website. The old advertisments are currently expiring (only 2 left at the moment).

We received several requests for additional advertising from different companies recently. So we need to decide upon the advertising strategy.

Expiring the advertising would make our users happier, adding more advertising would give us additional income sources that would provide the necessary sustainability

Team

We are currently lacking 10 Developers, 3 trusted System administrators, 4 trusted Officers, 5 trusted product managers (and 1 licensed Webtrust Auditor)

Issue: TrustCheck

We have currently several roles that require trusted personnell:

- System Administration on core systems with logical access (we´ve got an exception for physical access due to good security mechanisms)
- Core-Support
- Officers in critical areas (Security, Assurance, QC, Policy, DR, Privacy)
- Internal auditors

Areas where trusted personnell is preferred, but it´s not clear, whether it´s a requirement or not:

- Auditors, Advisory team, Board, Developers
- “OrgAdmins” (Orga-Assurers and Core-Support that can authorize Orgas in the system)
- Suppliers, „lethal persons“, ...

TrustCheck Problems

I think we already lost about 10 people due to delays of the trustchecks

We currently have potentially lethal availability issues that can´t be solved due to not enough trusted people.

We currently have a backlog of about 15 unprocessed trustchecks

To be able to improve the TrustCheck programme, we need more experience with it.

Proposal:

Restart the TrustChecks immediately

Assign 2 different people to the TrustCheck Team to solve the backlog and ensure the availability of the programme.

Audit-News

- **Microsoft moves from „WebTrust equivalent“ to WebTrust**
- **Opera moved from 8000 EUR to WebTrust**
- **Microsoft closes open holes**
  - like the SubCA hole (we were told about by PW)
  - **the equivalent audit hole -> DRC is not an option**
  - **the independent auditor hole -> unlicensed auditors are not an option**
  - **old root certificates -> updates every 12 months**

Potential price solutions

- Defining a budget of >= 50.000,- EUR per year
- Asking WK to try to get a WebTrust auditor license
- Getting a Sub-CA cert from a commercial CA (I heard a price of 200,000 EUR, but I guess we might not get one)
- We could ask the Big5, whether we can donate Man-Power (WK) to make it cheaper. Alternatively, we could do a Webtrust criteria based Audit with an external auditor first, and then let that auditor help us doing the Big5 audit, which should make the real audit a little faster and cheaper.
- Get listed by the European governmental root-certificate lists, and included into Microsoft that way
-

Possible Criteria solutions

- Doing lobbying to get DRC approved by Microsoft
- Writing an RFC for CA audit criteria based on DRC, to get DRC/derived criteria adopted as an open standard by IETF
- We should think about switching from DRC to WebTrust criteria now.
- We should negotiate the kind of audit we do with the responsible people at Microsoft, upfront.
- We need more manpower in the audit (and internal) team to be able to react faster
- How should we communicate all that to the public?

Future plan

- Migration
- 3-Layer Architecture
- More and better monitoring
- ITTC
- Secure Database
- Email-TAN
- Airlock

Breakout / Board meeting

- It´s your task now ;-)

Any questions?

Just ask. We are here to answer them!