Cloud Security Fails & How the SDLC could (not?) have prevented them

CSA CEE Summit 2015, Ljubjana

By Christopher Scheuring, ERNW Germany

/whoami

- Christopher Scheuring
- Security Analyst @ ERNW
- Since 2010 IT Security Architect and Analyst
- Before: 8 years software development
- Email: cscheuring@ernw.de

ERNW GmbH

- ERNW provides vendor independent security services to support our customers' business.

- Established 2001
- 35 employees
- Customers predominantly large/very large enterprises
- Vendor Independent
- We understand corporate
- Deep technical knowledge
- Structured (assessment) approach
- Business reasonable recommendations

Agenda

- Cloud – From a security point of view
- Typical Cloud Security Fails
- SDLC & Cloud and Information Security

Attackers – Not Today

- We will ignore Attackers for this talk :-)
- We will talk about cloud security fails and how SDLC could (not) prevent them.

SDLC

Secure Development Life Cycle

- Is the inclusion of IT security aspects into the (software) Development Live Cycle.
- Focus is checking:
  - Company policies
  - Legal requirements
  - Technical IT-Security requirements
  - Efficacy of security measures

How does the *Security Landscape* change?

In The Cloud…

- …you don't own the hardware/computing engine/RAM.
  - → you **can not** *control* it.
  - → did you get that? You **can not**!
- … you don't own the network.
  - → you **can not** *control* it.
- … you don't own the facilities.
  - → you **can not** *control* it.
  - → You don't even know where they are.
- … you don't employ the administrators.
- … you don't own the processes.
- Yadda-yadda-yadda

The Threats, Assets and the Fails

Remember Your Assets

- Data
- User Identities
- Service Availability
- Cloud Service Availability

The Threats (1)

- Policy & Organizational
  - Loss of governance
  - Compliance challenges
  - Cloud service termination or failure
  - Loss of business reputation due to co-tenant activities
  - Supply chain failure

The Threats (2)

- Technical
  - Resource exhaustion (under or over provisioning)
  - Loss of encryption keys and data
  - Data leakage on up/download
  - Distributed denial of service (DDoS)
  - Typical web application attacks
  - Unauthorized data access to (disposed) media

The Threats (3)

- Legal
  - Subpoena like Patriot Act
  - e-discovery
  - Risk from changes of jurisdiction
  - Data protection risks
  - Licensing risks

...some of the Fails

we found in several security analysis.

SDLC & SaaS

- Most customer using SDLC for their traditional software projects.
- And a lot of them also using SDLC for Cloud projects (SaaS).
- But often they don't dig deep enough.
- Or the project scope changes - but not the SaaS like to need.

SDLC
The Cloud API (1)

- SaaS with business user synchronization.
- Authentication by federation service.
- Compliance requirement:
  - 2 factor authentication for administrative tasks.
- Previous business and security analysis done – everything's fine.

SDLC
The Cloud API (2)

- The Evaluation:
- For using the federation service synchronization of the user IDs is necessary.
- At evaluation everything was fine:
  - 2 factor authentication for the administrative login using the web GUI works as expected.
  - Synchronizing user IDs over the web GUI by file upload.

SDLC
The Cloud API (3)

Compliance 

Technical 

Legal

The Fail

- An automated process is needed to keep the synchronization of the business user IDs between the company and the cloud service up to date.
- Using the API for administrative task couldn't provide 2 factor authentication.
  - Just uses username and password!
- SaaS provider is currently not able to solve this problem…

SDLC
Data Encryption (1)

- SaaS “sales application” of a CSP.
- Customer needs to store BDSG (German data privacy law) relevant data – so the data needs to be encrypted.
- Project management checked the features of the SaaS:
  - Encryption is available for data.

SDLC
Data Encryption (2)

- During the project setup a lot of compliance checks were performed.
- They talked about data security and encryption.
- They asked the CSP about data encryption for special data fields.
  - CSP: Yes, of course – we are PCI compliant and use HSM.
  - Customer: Cool – everything is fine.

SDLC
Data Encryption (3)

Compliance

Technical 

Legal 

The Fail

- The customer never asked what PCI implies and if it's suitable for his needs.
- During security approval we asked how they become BDSG compliant.
  - The CSP could only provides encryption for PCI relevant data and not for the used data fields.
- The customer now needs to change requirements of the stored data…

SDLC
Data Encryption 2nd (1)

- SaaS “sales application” of another CSP.
- Customer needs to store confidential data encrypted inside the cloud application.
- The CSP provides transparent encryption of the data.
  - The encryption keys where stored at customer site.
- Everything seems to be perfect.

SDLC
Data Encryption 2nd (2)

- While the project is running scope change:
  - They want to use the CRM functionality of the SaaS.
  - No Problem – feature is available as part of the SaaS.
- As usual the project scope is changed another time:
  - They even want to use the CRM functionality of the SaaS of encrypted data fields.

SDLC
Data Encryption 2nd (3)

Compliance 

Technical

Legal

The Fail

- The CRM functionality for encrypted fields is possible.
- But only if the encryption key is stored inside the SaaS application.
- The company compliance prohibits the storage of encryption keys outside the company environment.
- Project needs the check how they could keep going on.

Some other fails – on the SaaS side

Not only the SaaS costumer have problems ;-)

War Story
Pentest HR SaaS (1)

- Evaluation of a SaaS CSP
  - Some "HR management software"
- They agreed to perform a pentest on behalf of the potential customer.
  - Which is not necessarily the case!
- Target of evaluation:
  - HR web application
  - Management interfaces, deployment mechanisms, isolation.

War Story
Pentest HR SaaS (2)

Compliance

Technical 

Legal

The Fail

- Basic result: After one day, we had to stop the test.
  - We already had more severe findings than in some other 20 man day tests ;-)
- *HTTP PUT* to the web root was possible!
- Seriously, when did you see something like that the last time?

War Story
Isolation Failure (1)

- Initial setting: Security assessment of an IaaS cloud environment
- Question set: Can customer A access data of customer B?

War Story
Isolation Failure (2)

Compliance

Technical 

Legal

The Fail

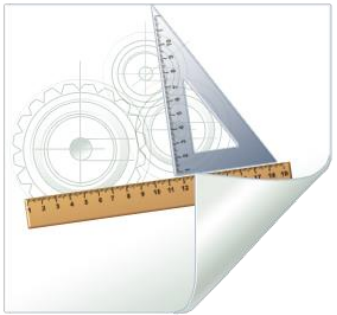
- During the analysis of methods for the hopping between customer networks, we suddenly were able to access systems of customer C
  - Which was not a test customer…
- This resulted from the accidental re-use of customer C's VLAN ID.
- Typical operational error – caused by incomplete SDLC.

SDLC & Cloud and Information Security

SDLC & SaaS (1)

- SDLC for SaaS projects become more important than most project managers think.
- IT-Security is a very important part.
- The responsible need to dig deep into the offered features of SaaS **and** if they are suitable for their needs.
- Applying security is not possible or very expensive!

SDLC & SaaS (2)



- Security should be taken into consideration in each phase of application/system development.
- Existing SSDLC methodologies focus on Governance, Construction, Verification and Deployment business functions and their relevant security activities.

SDLC & SaaS (3)

- Use Software Assurance Maturity Models e.g.
  - OpenSAMM [http://www.opensamm.org]
  - BSIMM (Building Security In Maturity Model) [www.bsimm.com]
- These methodologies can help to improve security of cloud hosted applications (SaaS).

SDLC & SaaS – some SAMM examples (1)

- **In Governance**, they require to consider "Compliance and Policy" issues. One should check if the provided cloud solution/platform is compliant especially with the technical policy requirements (e.g. confidential data must be stored in encrypted form, two-factor authentication is supported or not, etc.)
- **In Construction**, they require to consider best-practices for "Secure Architecture". One should check if the provided cloud solution/platform follow these best practices for its architecture, like VLAN separation of different customers, N-Tier architecture within a single VLAN, least privilege, fail securely, deployment of security components (e.g. WAF, XML Firewall etc.).

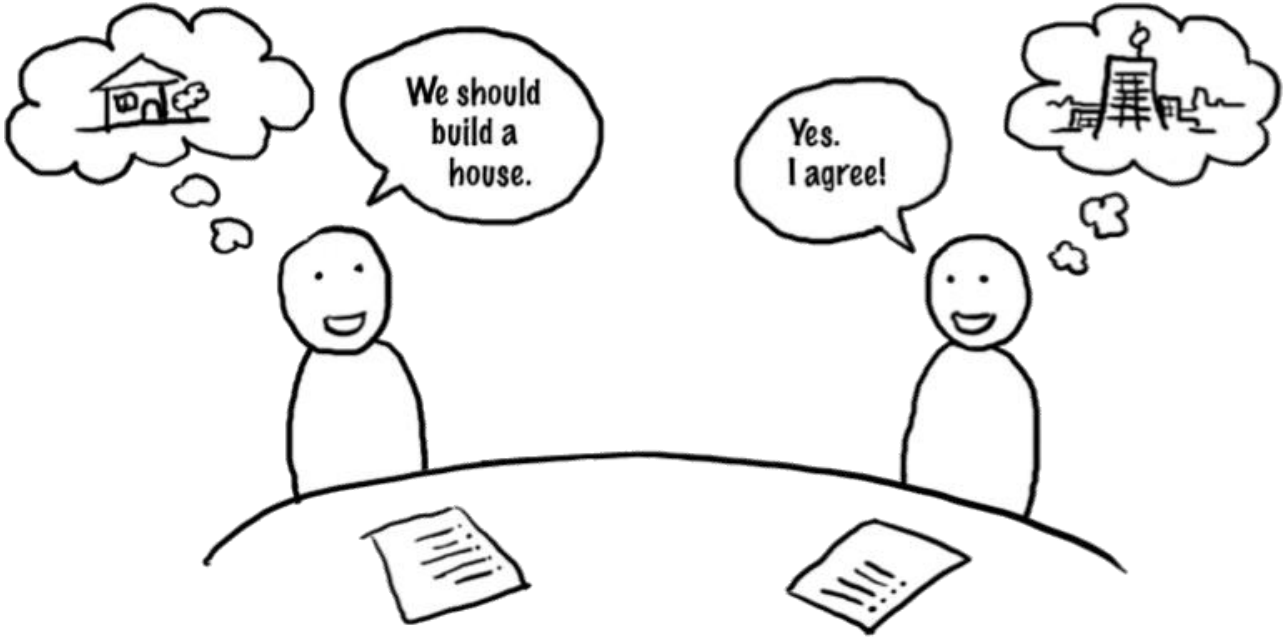
SDLC & SaaS – some SAMM examples (2)

- **In Verification**, they require to consider security testing and penetration testing. One should check if the provided cloud solution/platform performs regular penetration tests both for network and application services.
- **In Deployment**, they require to consider patch management, secure configuration and vulnerability management. One should check if the provided cloud solution/platform has an in-time patch management process and environment hardening is performed and regularly checked.

Conclusion

- Using cloud services spreads our data – we need to know this.
- Because of changing our way of work, data ownership becomes more important:
  - BYOD
  - Mobile devices
  - Working with the private devices at home
- The Big Question: How will data security policies have to be implemented in the future?

Thanks a lot for your attention :-)



Questions

www.TROOPERS.de