Security Considerations for German-Japanese Business Collaborations

Best Practice for Servers and Infrastructure

Version 0.2 - Revision 241

Christian Külker

DJW - IT working group

2013-09-06

1. Motivation

2. Communication

3. Security Concepts

4. Best Practice for Server and Infrastructure

Why do we need secure communication?

We have nothing to hide - do we?

All business has something to hide - especially honest ones!

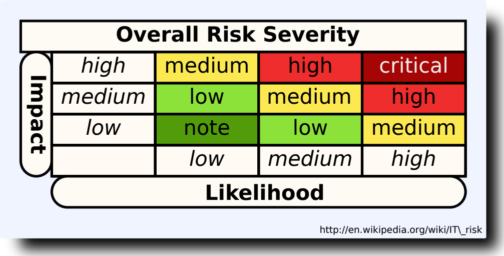
- Competitors
- Information that is now harmless can be harmful in the future
- German and Japan have different culture of secrecy
- Economic Espionage can not be excluded

http://www.thoughtcrime.org/blog/we-should-all-have-something-to-hide/
http://www.heise.de/ct/artikel/Warum-die-NSA-Affaere-auch-Tante-Grete-betrifft-die-gar-nicht-auf-Facebook-ist-1939834.html

A German company has the duty to protect data

Data protection: confidentiality, integrity, availability
Which data: technology, production processes, research, finance, calculations, offers, tenders, personal data see: ix, Sep 2013, page 82

IT (Security) Risk Assessment



Overall Risk Severity

Impact	*high*	medium	high	critical
	medium	low	medium	high
	low	note	low	medium
		low	*medium*	*high*
		Likelihood		

http://en.wikipedia.org/wiki/IT_risk

$$Risk = Likelihood * Impact$$

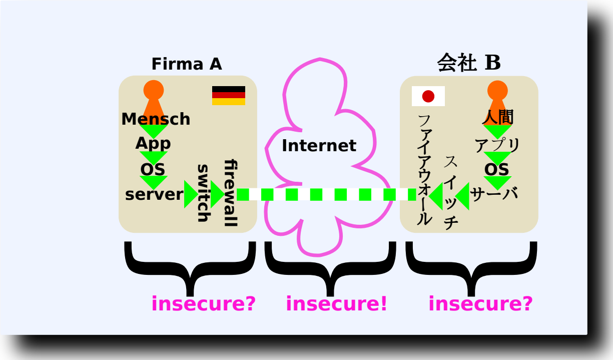
$$Risk_{IT} = Threat * Vulnerability * Asset$$ [1]

$$Risk_{IT} = ((Vulnerability * Threat)/CounterMeasure) * AssetValue$$ [2]

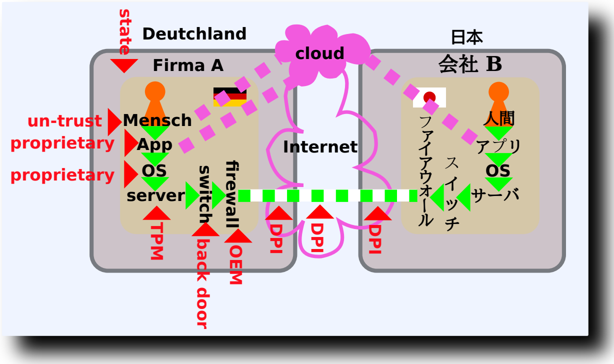
[1] IT Risk: Caballero, Albert. (2009). "14". Computer and Information Security Handbook. Morgan Kaufmann Publications. Elsevier Inc. p. 232. ISBN 978-0-12-374354-1

[2] TIK framework: http://it-risk-management.com/

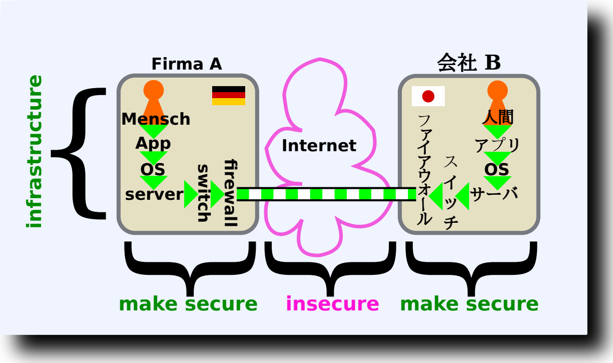
Communication Path insecure?



Communication Path Threads



Make Communication Path secure



Risk of Service Components

in case you use 3rd party infrastructure

Service	Risk
Social Networks	public, sw error exposes ”private” content, 3d party can read DB without notice
mail, mailing lists	if 3rd party has access to file system, all mails can be copied, all intermediate computers can record the traffic
web	3rd party can read file system, CGI/ formulas can be hacked remotely
RTC (VOIP)	3rd party can record, if access to server, transmitted encryption not sufficient, weak clients
Cloud, Cloud HDD	3rd party can breach in if access to hardware

http://www.heise.de/newsticker/meldung/Microsoft-zu-PRISM-Wir-bieten-der-NSA-keinen-allgemeinen-Zugriff-auf-Skype-Co-1919133.html

Risk of Service Components

in case you use 3rd party infrastructure

Service	Risk
Social Networks	public, sw error exposes "private" content, 3d party can read DB without notice
mail, mailing lists	if 3rd party has access to file system, all mails can be copied, all intermediate computers can record the traffic
web	3rd party can read file system, CGI/ formulas can be hacked remotely
RTC (VOIP)	3rd party can record, if access to server, transmitted encryption not sufficient, weak clients
Cloud, Cloud HDD	3rd party can breach in if access to hardware

http://www.heise.de/newsticker/meldung/Microsoft-zu-PRISM-Wir-bieten-der-NSA-keinen-allgemeinen-Zugriff-auf-Skype-Co-1919133.html

Solution: Self-hosting! (and secure protocols)

Do it yourself - or - trusted partners only

* Islands of safe law (German, Japan)
* Trust your employees
* Trust only partners you can trust
* Make a difference between IT partners and others
* Do not trust anybody else
* Make a list
* Exchange public keys between trusted partners in an absolute open way
* Do not be naive!
* Do you have enough money for security?

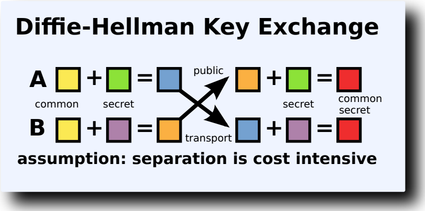
http://www.heise.de/newsticker/meldung/PRISM-koennte-US-Cloud-Anbietern-schaden-1925126.html

Use Strong Encryption!

And PFS!

* There is weak and strong encryption, symmetric and asymmetric keys
* Session initiation according to **perfect forward security**/ Diffie-Hellman:
  SSH, OTR, *IPsec*, *SSLv3*, OpenSSL with elliptic curve Diffie–Hellman
* Never transmit passwords/secrets for session initiation
* Do only sign GPG/PGP keys of people you met IRL (ID card)

http://en.wikipedia.org/wiki/Perfect_forward_secrecy http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange


Diffie-Hellman Key Exchange
A
B
common
secret
public
transport
secret
common secret
assumption: separation is cost intensive

How to Deal With Important Information?

* Do not use social media for internal or external business communication. Never post something for which you can not take responsibility for the next 40 years. (Remember the fall of the Berlin wall was 24 years ago)

How to Deal With Important Information?

* Do not use social media for internal or external business communication. Never post something for which you can not take responsibility for the next 40 years. (Remember the fall of the Berlin wall was 24 years ago)
* Do not store any information in the cloud, virtual hosting, dedicated servers hosted by others (without personal access control)

How to Deal With Important Information?

* Do not use social media for internal or external business communication. Never post something for which you can not take responsibility for the next 40 years. (Remember the fall of the Berlin wall was 24 years ago)
* Do not store any information in the cloud, virtual hosting, dedicated servers hosted by others (without personal access control)
* Do not use 'free' services like cloud hard-disks

How to Deal With Important Information?

* Do not use social media for internal or external business communication. Never post something for which you can not take responsibility for the next 40 years. (Remember the fall of the Berlin wall was 24 years ago)
* Do not store any information in the cloud, virtual hosting, dedicated servers hosted by others (without personal access control)
* Do not use 'free' services like cloud hard-disks
* Use strong encryption. Current strong encryption is considered to be safe the next 30 years

How to Deal With Important Information?

* Do not use social media for internal or external business communication. Never post something for which you can not take responsibility for the next 40 years. (Remember the fall of the Berlin wall was 24 years ago)
* Do not store any information in the cloud, virtual hosting, dedicated servers hosted by others (without personal access control)
* Do not use 'free' services like cloud hard-disks
* Use strong encryption. Current strong encryption is considered to be safe the next 30 years
* Use paper

How to Deal With Important Information?

* Do not use social media for internal or external business communication. Never post something for which you can not take responsibility for the next 40 years. (Remember the fall of the Berlin wall was 24 years ago)
* Do not store any information in the cloud, virtual hosting, dedicated servers hosted by others (without personal access control)
* Do not use 'free' services like cloud hard-disks
* Use strong encryption. Current strong encryption is considered to be safe the next 30 years
* Use paper
* Do not store

How to Deal With Important Information?

* Do not use social media for internal or external business communication. Never post something for which you can not take responsibility for the next 40 years. (Remember the fall of the Berlin wall was 24 years ago)
* Do not store any information in the cloud, virtual hosting, dedicated servers hosted by others (without personal access control)
* Do not use 'free' services like cloud hard-disks
* Use strong encryption. Current strong encryption is considered to be safe the next 30 years
* Use paper
* Do not store
* Speak (and agree) with your German/ Japanese partner

http://www.heise.de/newsticker/meldung/Cloud-Dienst-als-Malware-Einfallstor-1945606.html

Best Practice for Servers and Infrastructure

Server and other Hardware

* Buy servers from local companies
* Use Signed Free Open Source Software
* Do not use commercial software without Source
* Be careful to use or not to use TPM 1.1 or 2.0
* Check your hardware components. Any hidden SOC?
* When buying new hardware check and record all firmware versions
* Remove all unnecessary hardware

http://www.echomountain.com/pdfs/CiscoBestPractices.pdf

Best Practice for Servers and Infrastructure

Infrastructure

* Build your data center at the right spot/ use the right room
* Get a decent redundant Internet Connection
* Redundant utilities: electricity and water
* Wall security: kevlar, ... Avoid windows, fire doors exit only
* Limit entry points, entry protocols, cameras
* Make sure nothing can hide in walls or in the ceiling
* 2 factor authentication, physical security layers
* Monitor 3rd party works
* Use VPN, dedicated gateways, DMZ, ...
* Office: run 2 networks without interconnect: 1 for Internet, 2 for work
* Data center: separate networks: sensors, admins, local users, inter-server

http://www.echomountain.com/pdfs/CiscoBestPractices.pdf
http://www.csoonline.com/article/220665/19-ways-to-build-physical-security-into-a-data-center

The famous last page

Security Is Everyone's Business!

Thank you for listening

Christian Külker

HPC Project Manager
Partnership Program Coordinator
Eurotech - ETH Lab - Business Unit HPC

c.kuelker@ethlab.com

http://www.ethlab.com/

http://christian.kuelker.info/speech/