IT Security - Lecture Agenda

Introduction and Motivation

- *Introduction of Lecturer and participants*
- *Examples of real IT security incidents*
- *How an obvious IT attack looks like*
- *EU Regulation about Personal data protection*
- *Participant's own experience*

IT Security - Theory

Practical tips

Privacy and data protection

Interesting resources

IT Security & privacy

Targets:

- understand basics of IT Security & privacy
- to understand basic threats and how to minimize them
- practical tips to your every day’s life working with IT

Martin Horacek

About author

Education:

- 1992-97 Technical University Brno, physics Engineering
- 2013-16 Master of Science in Economy and Management

Microsoft certified professional
SAP certified Basis Administrator

Work Experience:

- 1997-99 University Hospital Brno, *IT administrator*
- 1999-01 Manesmann Rexroth spol.s r.o., *IT Manager*
- 2001-… Bosch Rexroth AG, *main SAP BC Administrator*

TASK Nr. 1: Where do you see yourself in 5 years ?

- pls. prepare for the discussion:

Do you want to stay away from IT, max. as just as Enduser ?

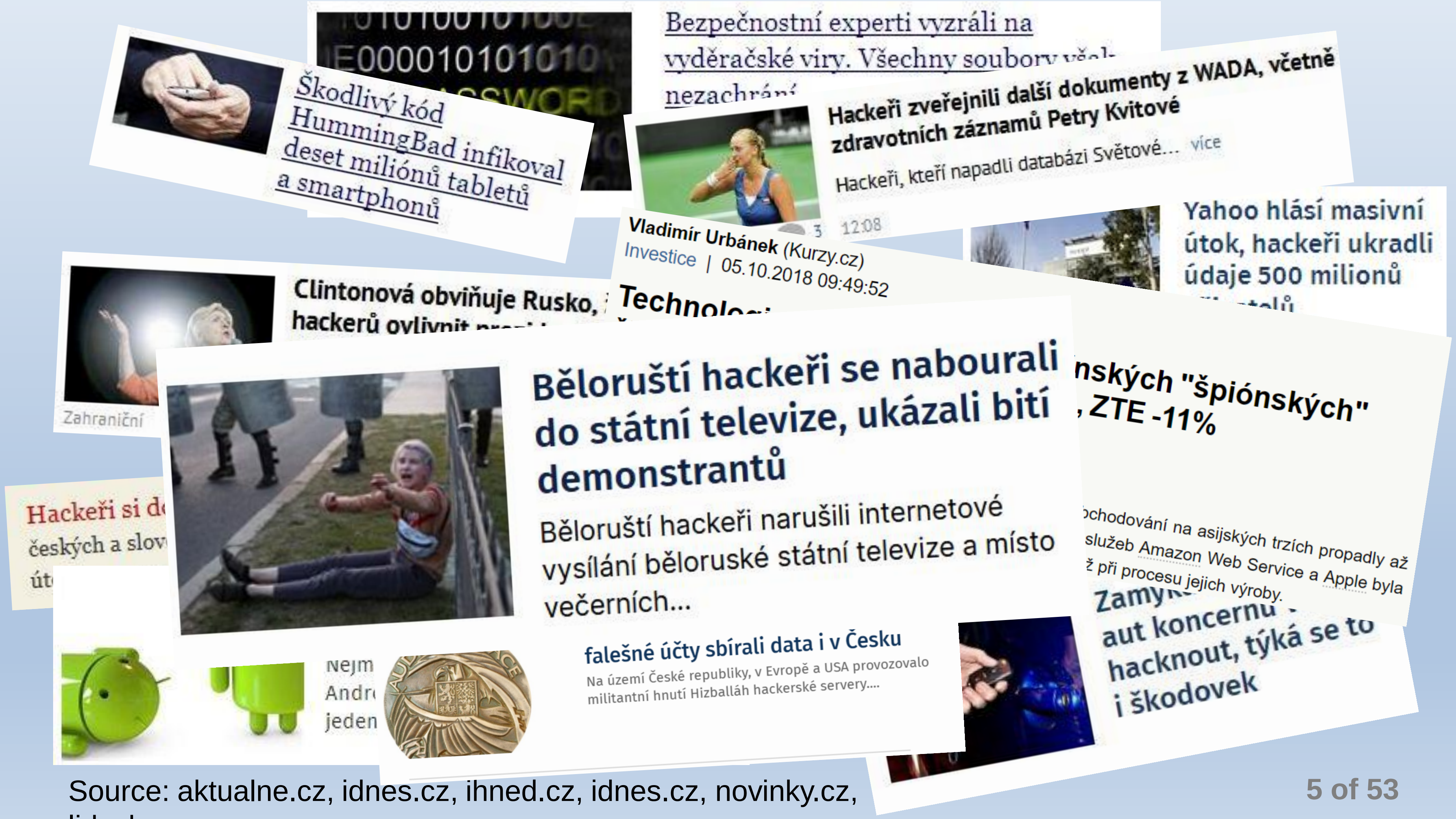
Do you want to be an IT professional ?

- IT manager ?
- IT developer ?
- IT administrator ?

Motivation

Security leaks and problems are everyday's life

- see e.g. Czech news as seen in last 3 years :



Bezpečnostní experti vyzráli na vyděračské viry. Všechny soubory v

nezachrání

Škodlivý kód HummingBad infikoval deset miliónů tabletů a smartphonů

Hackeři zveřejnili další dokumenty z WADA, včetně zdravotních záznamů Petry Kvitové

Hackeři, kteří napadli databázi Světové... více

3 12:08

Yahoo hlásí masivní útok, hackeři ukradli údaje 500 milionů

Vladimír Urbánek (Kurzy.cz)

Investice | 05.10.2018 09:49:52

Technolo

nských "špiónských"

, ZTE -11%

obchodování na asijských trzích propadly až

služeb Amazon Web Service a Apple byla

ž při procesu jejich výroby.

Clintonová obviňuje Rusko,

hackerů ovlivnit

Zahraniční

Běloruští hackeři se nabourali do státní televize, ukázali bití demonstrantů

Běloruští hackeři narušili internetové vysílání běloruské státní televize a místo večerních...

Hackeři si d

českých a slov

út

Nejm

Andr

jeden

falešné účty sbírali data i v Česku

Na území České republiky, v Evropě a USA provozovalo militantní hnutí Hizballáh hackerské servery....

Zamyk

aut koncernu

hacknout, týká se to i škodovek

Source: aktualne.cz, idnes.cz, ihned.cz, idnes.cz, novinky.cz, lidovky.cz

TASK Nr. 2: About your motivation…

- pls. prepare for the discussion:

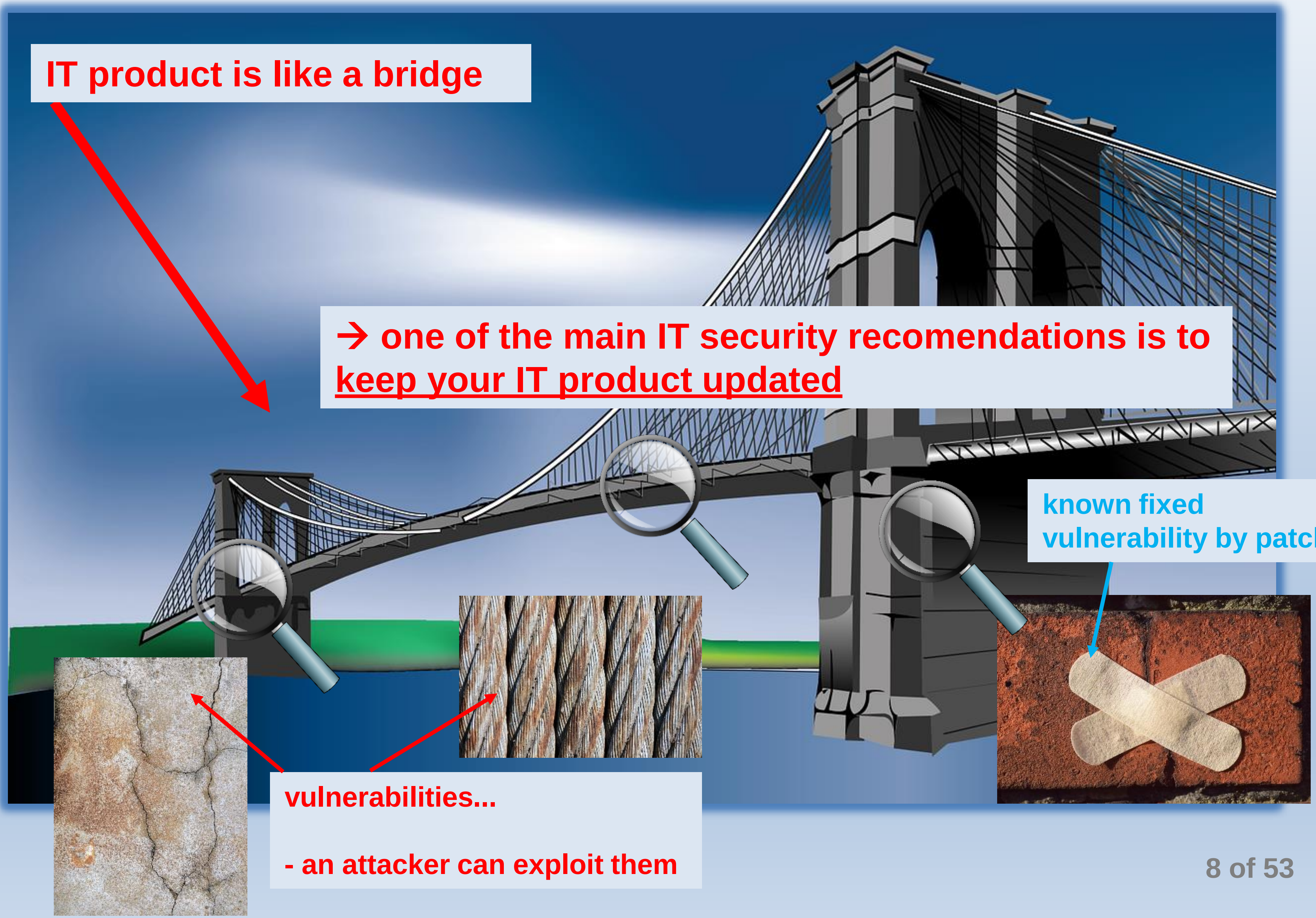
What is your experience with IT Security problems ? Have you ever lost any Data Files ? (lost photos, hdd ecrypted by malicious program...)

What happened to you in your private or business life ?

IT Security - Lecture Agenda

Introduction and Motivation
IT Security - Theory
Practical tips
Privacy and data protection
Interesting resources

IT Security of a Product - Main picture



IT product is like a bridge

→ one of the main IT security recomendations is to keep your IT product updated

known fixed vulnerability by patch

vulnerabilities...

- an attacker can exploit them

Where the vulnerabilities come from ?

Why is our world so unsafe ?

- **Human mistakes of a developer** *(when did you make an error last time ?)*

- **Missing knowledge by the developer** *(IT evolving quickly, non-stop learning whole life is required)*

- **Not enough time/ressources** *(e.g. Deadline calls etc.)*

- intentionally build-in vulnerabilities *(e.g. Developer wants to harm an employer, pushed so by the countrie s goverment interest)*

IT vulnerabilities start by developer

basic principles on secure development:

- **Input validation** *(directory traversal attacks; user can enter text vs. select from pre-selected responses)*

- **Secure error handling** *(if an error leads to a memory dump with visible variables content, an attacker can profit out of it. Or an application enters an unhandled state.)*

- **Defense in depth** *(several security layers – if one layer is compromised, other will keep)*

- **3rd party libraries** *(an application is as secure as its weakest component – could this weakness be a 3rd party library?)*

- **know basics of Cryptography** *(use strong standards like AES, SHA-2 instead of own crypto-development or older cryptographic procedures)*

- **secure DB accesses** *(SQL injection attacks)*

…

TASK Nr. 3: Find out an example of an attack or failure of an IT system

- pls. prepare for the discussion:

Search on the Internet to find an example of breached IT security.

What and when happened ?

Who and how suffered ?

Who was the attacker and what whas his/her motivation ?

An Example for those who could not find anything else: Read about **Ashley Madison data breach** on: https://en.wikipedia.org/wiki/Ashley_Madison_data_breach

Now bit of IT security theory…

security triad:

Confidentiality
- What would happen if other people would read the information?

Integrity
- May I rely that data I am working with are true and not modified by 3rd parties?

Availability
- Will I get a response of a server?
- Can I access my work email from home?

Root cause for IT problems

Human errors

System failures

Natural phenomena

Malicious actions

Third party failures

Source: Enisa 2015, ***Technical Guideline on Threats and Assets***

3 additional IT security pillars

Authentification
- ability to confirm an identity

Nonrepudiation
- sender cannot deny he sent the information

Audibility
- log and trace all actions

What is authentication ?

- a process how to identify authorized person:

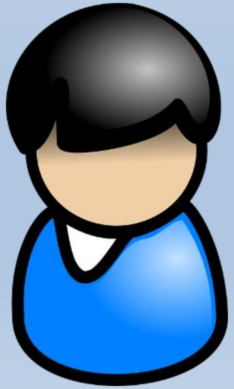
Real life examples: you want to withdraw a money from your bank account.
- You can go to desk, show your identity card with picture and if clerks recognizes you on the picture, you can then withdraw a money.
- You own a bank card associated with PIN. Having the card and knowing the PIN authenticates you.

- a person is identified by:

- by something he/she **knows**, (Password, PIN, username …)
- by something he/she **has**, (Personal ID card, mobile phone, SecureID card…)
- by something he/she **is**, (Biometrical data)

Secured authentication combines 2 of above

– e.g. User/Password+code sent to mobile phone…
- fixed password and changing part on Secure ID token,
- username and biometrical information



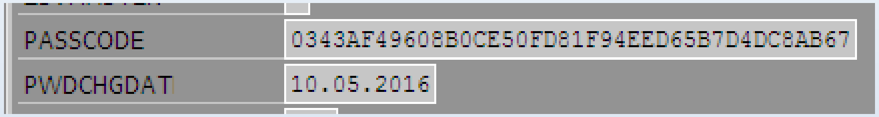
TASK4: Password strength

find out your own PW, that would take more than 1 bilion years to crack on:
https://howsecureismypassword.net/
(do not give exactly your one, they might build up a dictionary of used PWs… :-)

PW = 1234	→ can be cracked instantly
PW = pass1234	→ can be cracked instantly
PW = Jakub	→ 10 milliseconds to crack
PW = Jakub1234	→ 4 days to crack
PW = Jakub-1234	→ 6 years to crack
PW = blkT,npz,pznu,zjpr.	→ 118 quadrilion years to crack

běžela liška k Táboru,
nesla pytel zázvoru,
pejsek za ní utíká,
že jí pytel rozpíchá → **blkT,npz,pznu,zjpr.**

Dangers to a strong Password



PASSCODE	0343AF49608B0CE50FD81F94EED65B7D4DC8AB67
PWDCHGDAT	10.05.2016

not every system stores user PW encrypted → **use different Passwords for different systems**

every system can be still hacked exploiting new unknown vulnerability → **change your strong Passwords regularly**

do not write down PINs or PWs to a paper or let an application (e.g. internet browser /apple Wallet …) to remember it for you → **use rather local PW Store application based on open source that stores the PW DB encrypted locally only**

KeePass Password Safe

Version 2.28

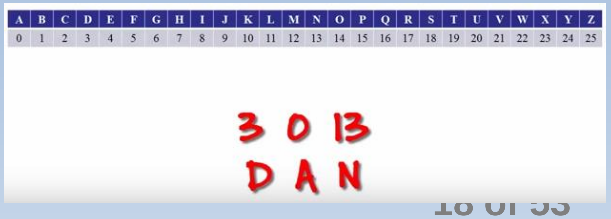
Basics of Cryptography

Caesar cipher
(ABC → DEF , knowledge of reading was a filter already)

Public key = certain page of a book
(spies using publicly available book as key to encrypt text)

IT Systems:
- keyless cryptography,
- symmetric key (one key for encryption and decryption)
- asymetric key (one key to lock, another to unlock)

Advanced Encryption Standard (AES)
- length of key 256 bit + 14 enc.rounds



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

3 0 13
D A N

Typology of attackers

opportunistic amateurs *(my colleague did not logged out and not locked his PC…, I found my chef's password – will it work? And in other systems as well ? In his home banking?... On internet I found a way how to attack our ERP system. Will it work?...)* → ***90 % of all IT attacks***

hackers = non-malicious *(yes, I can) Want a cheap IT penetration test ? - start an open competition and give a prize for winner…*

crackers = malicious

- career criminals,
- organized crime syndicates,
- cyber terrorists (ideological / political agenda)
- state supported spies and information warriors

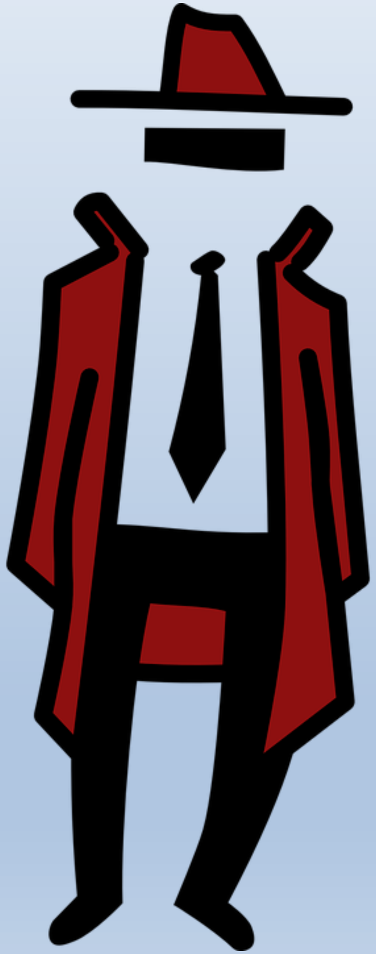
Basic harmful acts

Interception
(unauthorized party gained an access to a system)

Interruption
(as a result system is unusable, lost or unavailable)

Modification
(unwanted change in database, program)

Fabrication
(added new data, transactions, users in DB)



Interesting targets for attackers

network hardware *(attacker wants to listen unencrypted communication)*
servers *(attacker wants to access data stored on it)*
…

power users

- IT administrators,
- Top managers,
- all others who posses access rights to company’s critical resources

→ See how everyone plays own role:
https://www.youtube.com/watch?v=2sh4BIaF6gg from 02:10

Methods of defense

prevent attack
(block attack, e.g. by closing known vulnerabilities)

deter attack
(make attack more difficult, e.g. using non-standard process)

deflect attack
(provide target that looks more attractive)

detect attack
(watching attacker you can learn about typical weaknesses)

recover from attack
(restore systems from backups)

Every attacker needs MOM !

all 3 must exist at the same time:

Method
(skill, knowledge)

Opportunity
(time and access to attempt an attack)

Motive
(a reason for attack)

The attacker needs your help !

The most popular methods of attacks needs your help, otherwise attack would fail…

- You have installed a very special sw or cracked sw that was infected.

- On the Internet page you followed an advertisement (e.g. measure IQ for free, to see nude pict. of person ABC).

- You have received a phishing email and followed the unknown link in it.

→ *Even visiting a dangerous www site can be dangerous !!!*

Attacks by internal employees

Do you remember MOM?
Do you remember Amateur attackers ? …

E.g. does your accountant have access to accounts payable (in SAP Tcode F110) and can also modify the vendor’s bank account Nr. (XK02)?

→ *Opportunity is something you should minimize. Define and check by 4/6 eyes critical activities and their combinations.*

→ *Grant access based on minimal principle (=minimum rights to be able to work). Mind traceability = one employee, one username forever.*

→ *Introduce periodic controls of randomly selected critical activities.*

Social attacks

*as IT systems in big companies tend to be secure, attackers are misusing the most **weak part – employees**…*

They need their „help“ by e.g. clicking a link in a phishing email...

- watch these 2 examples of hacker s attacks:
https://www.youtube.com/watch?v=fHhNWAKw0bY

IT Security - Lecture Agenda

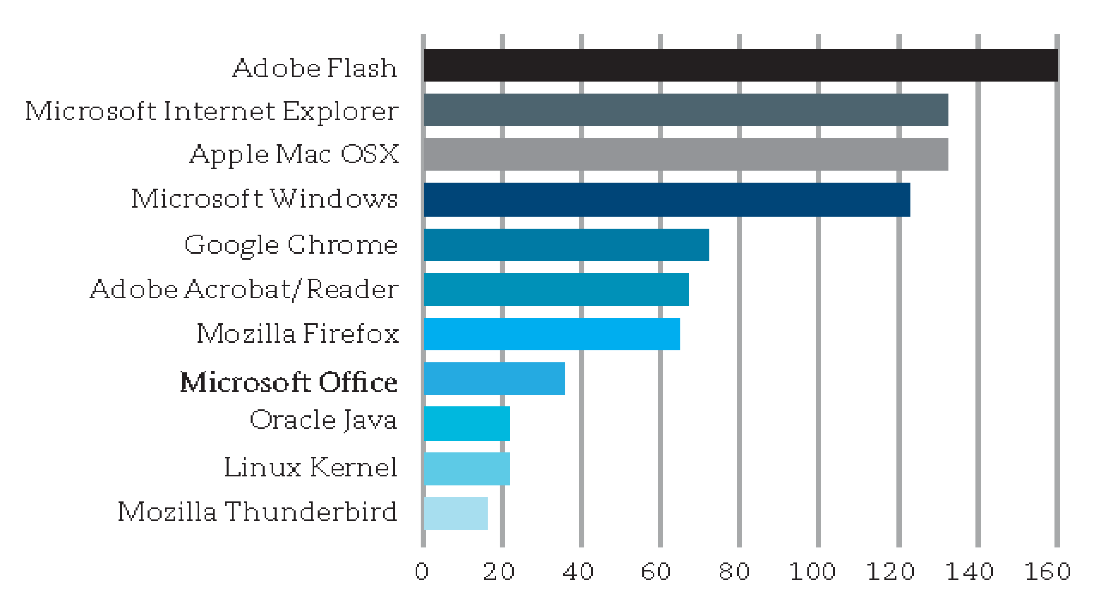
Introduction and Motivation
IT Security - Theory
Practical tips – for the IT managers and administrators
Privacy and data protection
Interesting resources

Count on coming IT problems

no system can be 100% secure

- we can only minimize the risks by prevention
- security is not a product, it is a behavior, an ongoing process …

- e.g. Nr of vulnerabilities found in year 2015 in different SW:



Source: [Die Lage der IT-Sicherheit in Deutschland 2015, BSI]

Make inventory of your systems

act effectively …

categorize all your data / systems according:

0 … no protection need
1 … low protection need
2 … medium protection need
3 … high protection need

For example:

Type of data / system	Confidentiality	Integrity	Availability
Business contacts	1	2	3
Accounting system	2	3	2
HR system	3	3	1
Intranet Canteen info	0	0	0
Product manuals on web pages	0	3	2

Create threat catalogue to IT systems

Threats from nature

- heavy snow and ice,
- heavy wind,
- flood,
- earthquake,
- wild fire,

…

Threats from criminals

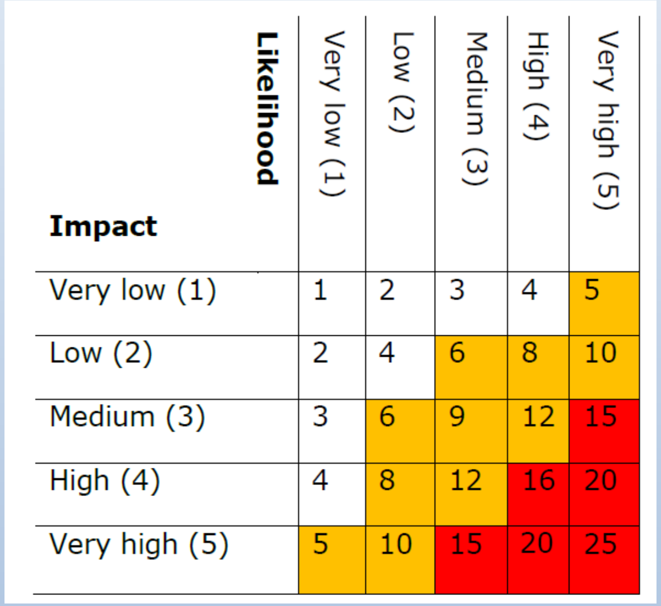
- arson *(a fire started intentionally),*
- electromagnetic interference gun,
- denial of service attack,
- network traffic hijack,
- malware and viruses,
- advanced persistent threats,
- hardware theft,
- power or network cable cut,

…

Threats from products

- hardware failure,
- faulty upgrade/change,
- software bug,
- design error

…



Impact \ Likelihood	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very low (1)	1	2	3	4	5
Low (2)	2	4	6	8	10
Medium (3)	3	6	9	12	15
High (4)	4	8	12	16	20
Very high (5)	5	10	15	20	25

Threats from own organization

- wrong decision,
- lack of procedure,
- no knowledge how to react

…

Source: Enisa 2015, ***Technical Guideline on Threats and Assets***

Backup strategy (=recover after attack)

be ready to recover from attack or failure…

1. backup your data

(always have copies of your documents, contacts, data …)

Full backups, Incremental, Offline, Online backups…

→ ***3-2-1 principle***

- always have 3 copies,

- on 2 different media types,

- out of it 1 outside of location where main data are

2. backup your whole system

(without sw deployment tool also re-installing OS and sw can be a long-lasting process)

→ ***use device image backup*** *(e.g. CloneZilla, Ghost, Acronis...)*

When have you last time tested by recovery if you really backup all you need ??

TASK Nr. 5: Think a while – imagine your PC/smartphone got stolen ...

- pls. prepare for the discussion:

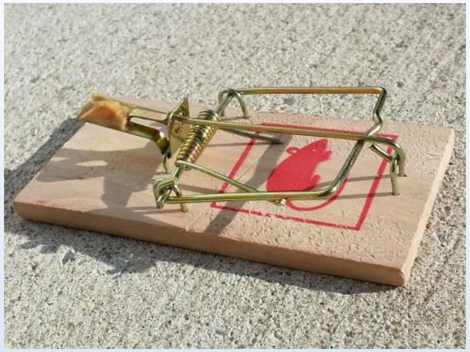
Let us imagine your PC/smartphone got stolen – what would be more painful to loose ? Hw or data ? (e.g. contacts/photos)

Have you got backup of your data? And how old ?

Consider – having physical backup at your home – what if it would be flooded or burn up together with your phone ?

Consider – if backup exists in the cloud – how safe is the backup on that cloud ? See: https://www.techlicious.com/tip/can-iphones-be-hacked/#:~:text=If%20your%20iCloud%20account%20is,to%20hack%20your%20other%20accounts.

Typical security relevant pitfalls by IT organizations



Are the responsibilities and processes clearly set ?

Do you have a „constitution rules“ for a situations out of a described processes ? *(e.g. 4 eyes principle | test on QAS first then 1:1 same on PROD)*

Are the IT systems and interfaces documented ? What about interfaces ? Is a product lifecycle on place?

Is the company culture supporting transparency, truth and right to be errorneous human ?

Are the employees motivated for life-time learning ?

Building / Location defense

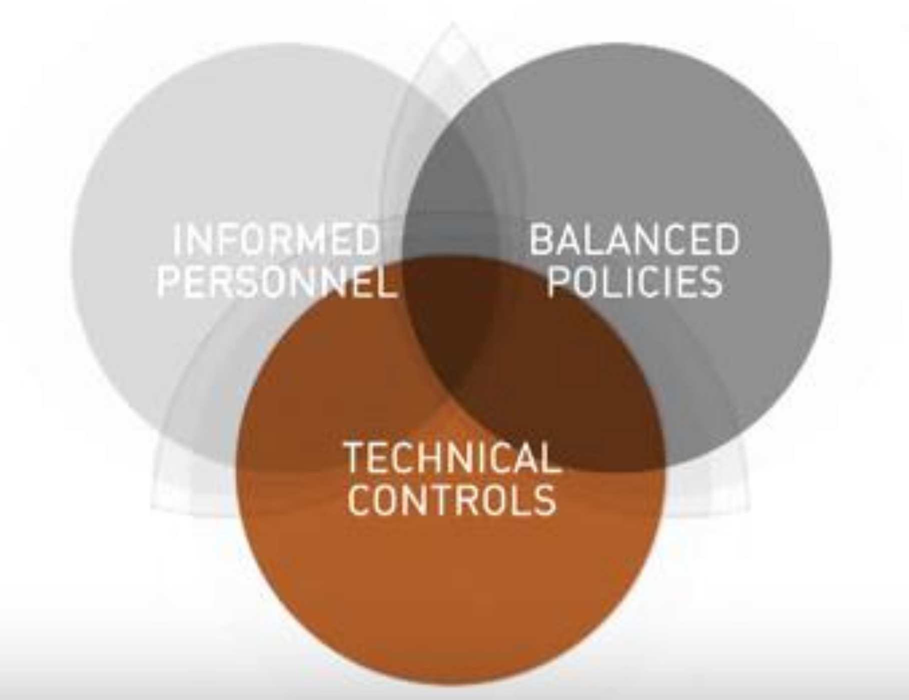
Is there building access control available ?
(can attacker freely use network socket or company’s WiFi)

Is there restricted access to a server room?
(have you considered overheating, smoke & fire alarm…)

Is company’s WiFi reachable beyond building access ?
(attacker can try bruce force e.g. from parked car)

How would your employees react on stranger in offices?
(would they question stranger or inform security service…)

Tips for organizations



ISO 27001

IT governance

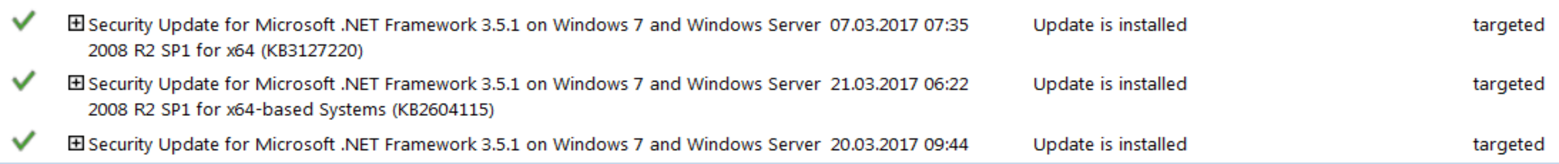
- ISO 38500

COBIT

- plan, build, run, monitor
- ITIL (..., change management, ...)

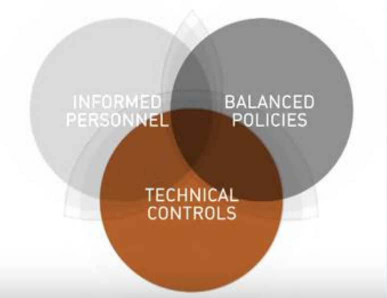
TOP5 IT topics to focus at:

- data backup management
- IT standardization
- central sw distribution and patch management
- education of personnel
- strategy what to do when under attack ? *(first reaction, whom to notify, whether to publish, document)*



✓	⊞ Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64 (KB3127220)	07.03.2017 07:35	Update is installed	targeted
✓	⊞ Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server 2008 R2 SP1 for x64-based Systems (KB2604115)	21.03.2017 06:22	Update is installed	targeted
✓	⊞ Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows Server	20.03.2017 09:44	Update is installed	targeted

Example: Balanced policies



ensure traceability to critical processes

(make sure each activity or decision is documented)

mitigate critical activities

(verify by an independent team a randomly selected transactions)

use minimal principle for granting system rights

(grant only rights which are inevitable for the process to be working)

introduce 4/6 eyes principles for critical processes

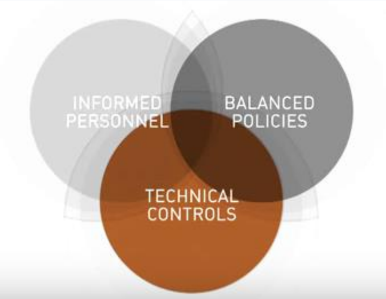
(do not concentrate too much power into hands of individual users – have always 2-3 different persons to be needed on critical process – e.g. one entering incoming invoices, second agrees on what should be payed, third can perform physically the payment in the system)

have emergency strategy

(Emergency user, emergency paper workflow when IT system is down…)

→ make sure all these policies are not too strict to harm your organization; have concepts for fallbacks / deputees

Example: Technical controls



segment your networks
(use firewalls, NATs)

separate physically access to server rooms
(minimize Nr. of people with this access)

have systems detecting an unusual activity
(e.g. detection of running port scanners etc.)

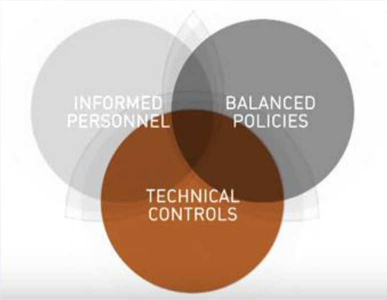
decommission your old unneeded devices properly
(delete is not enough)

unify and minimize sw/hw used
(unification can save your costs and efforts on IT security too)

lock USB ports on PCs
(infection via USB ports are very common)

authenification policy
(minimal length of PW, special chars in PW, dual authentification – e.g. PW + RSA token)

Example: Informed personnel



inform and train personnel
(to increase knowledge about possible risks)

establish an organization of well informed key users
(this can help to have a local person avail)

regularly keep up personnel‘s sensibility about IT risks
(to keep personnel sensible to recognize security topics in everyday‘s life)

test and audit awarness of personnel
(organize a situation alike social attack or phishing attack to see personnel would act properly)

IT Security - Lecture Agenda

Introduction and Motivation
IT Security - Theory
Practical tips – for the standard users of an IT devices
Privacy and data protection
Interesting resources

Every user - tips how to defend 1/3

use Kensingston lock for your Laptop
(advantage for attacker having Laptop physically)

LCD Foil
(when travelling your neighbors would not look)

HDD storage encryption
(lost Laptop = lost data, make sure no one can access them)

Lock USB ports, SD cards…
(most viruses now spread via USB Sticks)

Separate your activities
(have a business PC / OS and another one for private activities)

use Screensaver with Password

Every user - tips how to defend 2/3

Use only safe, pre-tested sw , regular upgrades
(consider Trojan, interferences)

update your software regulary, use Antivirus sw.
(fresh today’s virus cannot be recognized by yesterday’s Antivirus sw...)

Use an own user without Admin rights
(an unwanted sw installation can be so avoided)

Store data on trustworthy servers

Have backups available
(images of your PC setup,
backup your data on 3-2-1 principle:

have always 3 copies
on 2 different media (tape, hdd, DVDs)
an 1 of them off-site

Every user - tips how to defend 3/3

Change standard passwords / PINs

(non-trivial password, different pass per system, no easy-to-guess security questions in case of forgotten password, do not accept sw to remember pass for you…)

Store and communicate the sensitive data encrypted

(use HTTPS, disk/file encryption)

Visit only safe Internet sites, be aware of Phishing

do not follow any unknown URL links

Connect only to trustworthy WiFi providers

(consider the free WiFi as suspicious, see why: https://www.youtube.com/watch?v=CV39QzFpJx4)

Consider your activities in Internet create footprints

(check what Google, Facebook etc. knows about you already…)

IT Security - Lecture Agenda

Introduction and Motivation

IT Security - Theory

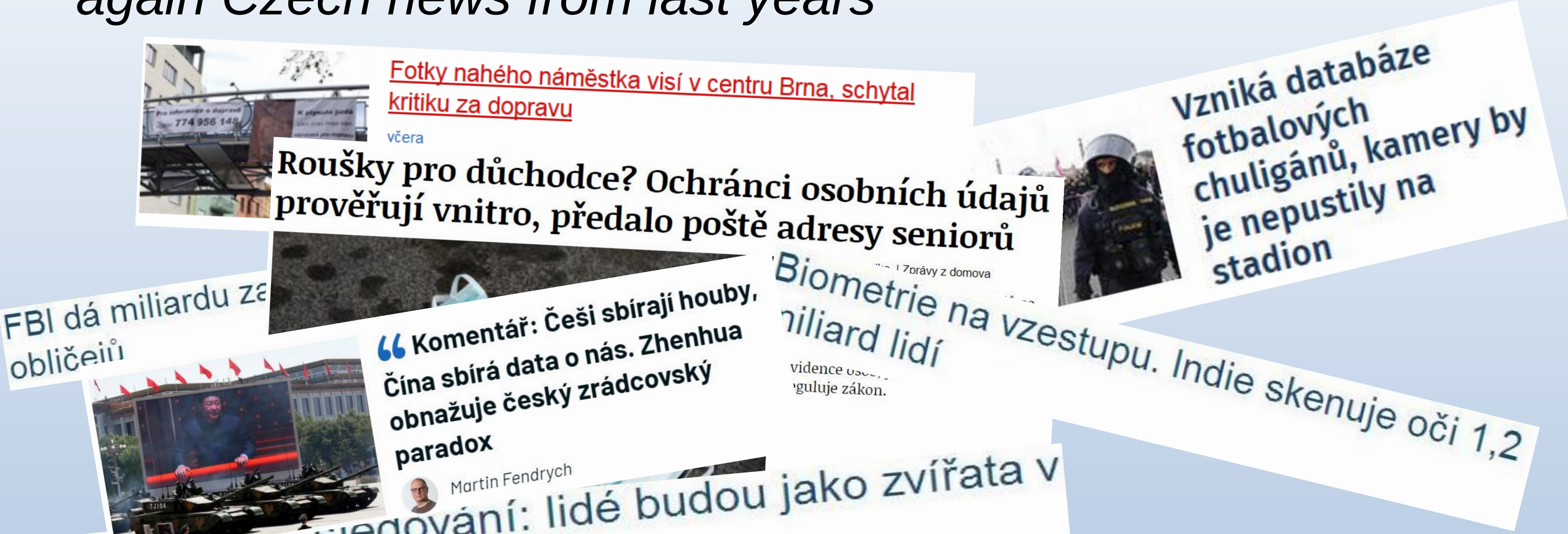
Practical tips

Privacy and data protection

Interesting resources

Privacy issues

again Czech news from last years



Fotky nahého náměstka visí v centru Brna, schytal kritiku za dopravu

včera

Roušky pro důchodce? Ochránci osobních údajů prověřují vnitro, předalo poště adresy seniorů

Zprávy z domova

Vzniká databáze fotbalových chuligánů, kamery by je nepustily na stadion

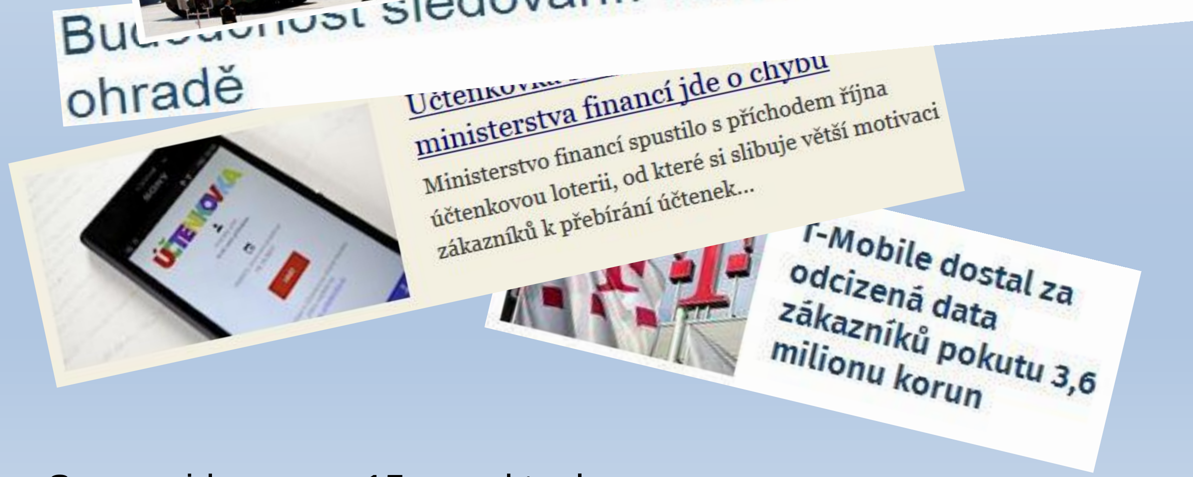
FBI dá miliardu za obličejů

Komentář: Češi sbírají houby, Čína sbírá data o nás. Zhenhua obnažuje český zrádcovský paradox

Martin Fendrych

Biometrie na vzestupu. Indie skenuje oči 1,2 miliard lidí

vidence osob, reguluje zákon.



Budoucnost sledování: lidé budou jako zvířata v ohradě

Účtenkovka ministerstva financí jde o chybu

Ministerstvo financí spustilo s příchodem října účtenkovou loterii, od které si slibuje větší motivaci zákazníků k přebírání účtenek...

T-Mobile dostal za odcizená data zákazníků pokutu 3,6 milionu korun

Source: idnes.cz, e15.cz , aktualne

On the picture Trifot by David Cerny

EU law - Protection of personal data

applies since 05/2018... Known as GDPR

- everyone has the right to protection of personal data,

- right to be „forgotten“,

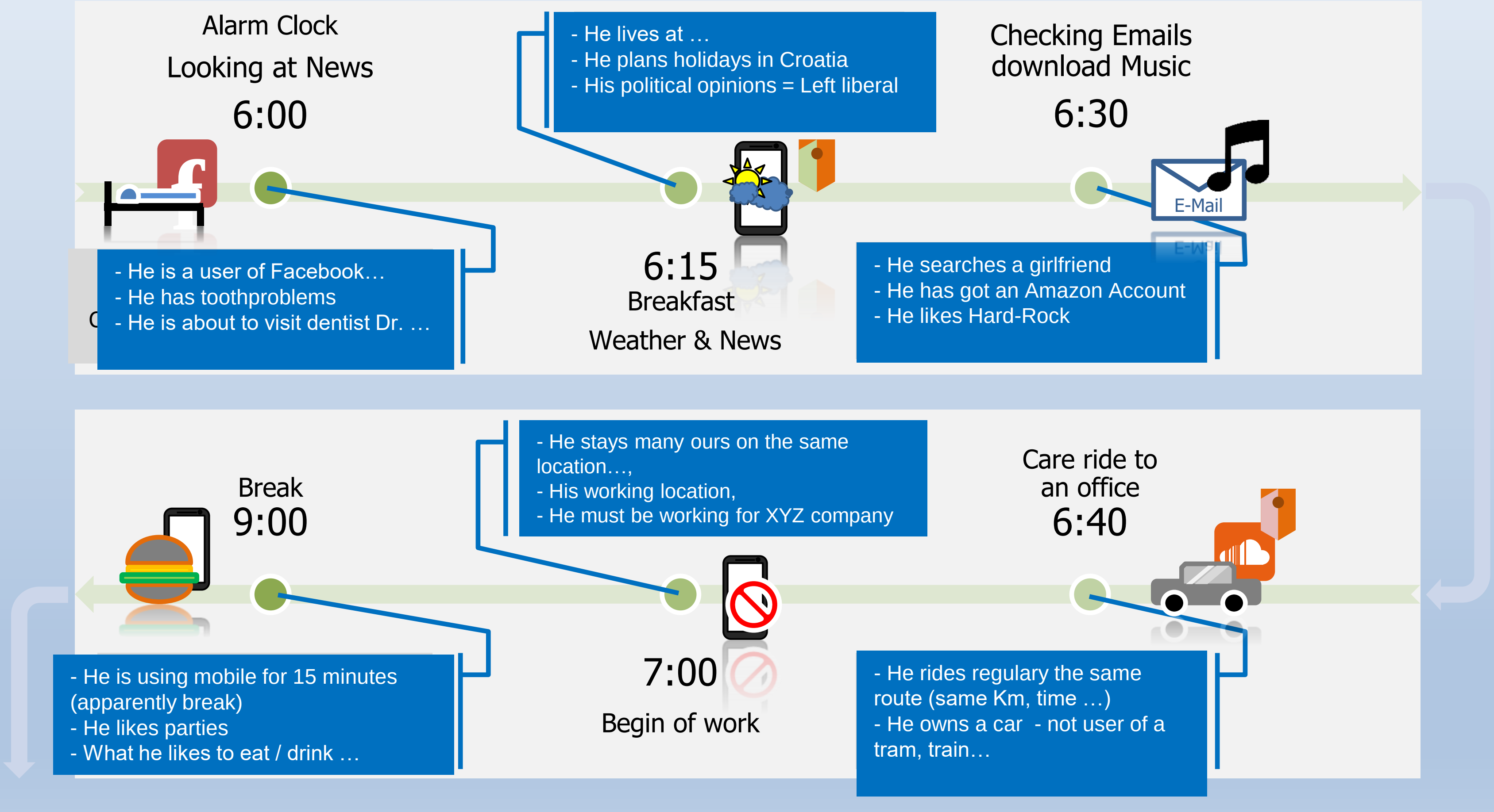
- right to know when one‘s data has been hacked

- data protection by design and default

- stronger enforcement of the rules *(fines up to 4% of global turnover)*

Source: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Smartphone publishes your life



Alarm Clock

Looking at News

6:00

- He is a user of Facebook…
- He has toothproblems
- He is about to visit dentist Dr. …

- He lives at …
- He plans holidays in Croatia
- His political opinions = Left liberal

6:15

Breakfast

Weather & News

Checking Emails
download Music

6:30

- He searches a girlfriend
- He has got an Amazon Account
- He likes Hard-Rock

Care ride to
an office

6:40

- He rides regulary the same route (same Km, time …)
- He owns a car - not user of a tram, train…

- He stays many ours on the same location…,
- His working location,
- He must be working for XYZ company

7:00

Begin of work

Break

9:00

- He is using mobile for 15 minutes (apparently break)
- He likes parties
- What he likes to eat / drink …

…

Who wants data about you?

every day everyone creates by living in 21st century
a lot of data, every year more and more…

… and this data is very interesting for many parties, e.g.

Insurance Are you fan of extreme sports? Has your family any genetic Diseases? Do you drive safely? Do you follow speed limits?	**Thieves, Kidnappers** When will you be out of home for work, holidays etc ? Are there any valueables in your house?	**Political parties** What are your politic opinions, what do you believe in? Can they get you as a new member?
Banking industry What is your lifestyle? What does It mean to your credibility?	**Flat Rental** Do you have a stable income? Do you have pets? Do you invite people for parties? Do you smoke?	**Your Employer …** **Your Boss …** **Your spouse …** ☺

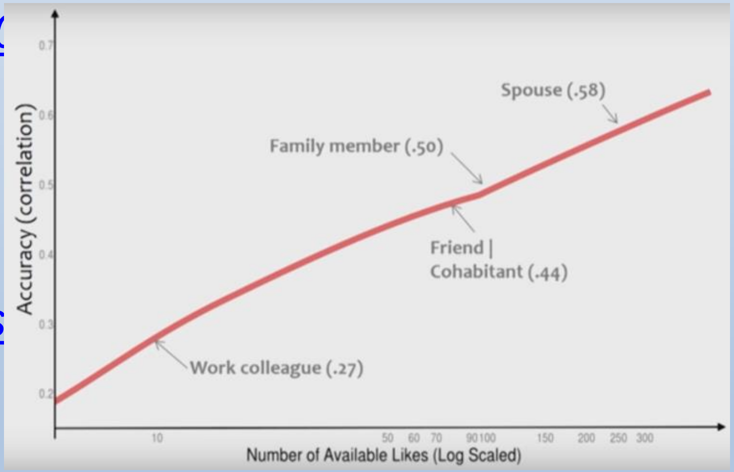
Privacy issues – watch these

Malte Spitz: *Your phone company is watching* – watch this video:
http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching

→ **EU Regulation:** http://ec.europa.eu/justice/data-protection/

Michal Kosinski: *The end of privacy* – watch this video (29mins.):
https://www.youtube.com/watch?v=NesTWiKfpD0

See a trailer for the Film –
The Social Dilemma (Sep-2020) :
https://www.imdb.com/video/vi306953753?playlis



See how algorythm can see your profile based on your digital footprints:
https://applymagicsauce.com/demo

IT Security - Lecture Agenda

Introduction and Motivation

IT Security - Theory

Practical tips

Privacy and data protection

Ineteresting resources

Interesting internet resources

Dr. Daniel Soper‛s IT Security tutorial videos: https://www.youtube.com/watch?v=zBFB34YGK1U

Czech Security Incident Response Team

https://www.csirt.cz/

Czech Cyber Security law

https://www.csirt.cz/files/csirt/zkb-181-2014-sb.pdf

ENISA – European Union Agency for Network and Information Security

https://www.enisa.europa.eu/

German State Office for IT Security: *Repository of IT Threads and defensive recommendations* https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf , https://bsi.bund.de/