Informačná bezpečnosť

Ing. Eva Oláhová. PhD.
CIT FEM SPU

- Úvodné slovo - informačná bezpečnosť a informácie
- Informácie a ich charakteristiky
- Definície pojmu informačná bezpečnosť
- Informačná bezpečnosť z pohľadu podniku
- Digitálna identita a digitálna bezpečnosť

1. Prečo sa tým zaoberať ?
2. Čo a prečo treba chrániť?
3. Aké sú hrozby a ako im čeliť?
4. Zaujíma/dotýka sa ma to vôbec ?

Odpoveď na otázku prečo - príklady

1. Rok 2006: Hackeri o NBÚ: heslo nbusr123 stále funguje
2. Rok 2018: Hackeri zo zahraničia opakovane napadli shmu.sk a aj Slovensko.sk
3. Roky 2019-2021: Portál NZCI, etický hackeri (viac na: URL1 URL2)

Spoločnosť NETHEMBA

<NCZI>
Národné centrum zdravotníckych informácií

- 2019 - únik OÚ občanov
- 9/2020 - prístup k PCR/AG testom a OÚ informácie všetkých testovaných občanov
- 8/2021 - prístup k údajom e-hranica/Covid-pas

chyby v systéme umožňovali napr. kohokoľvek poslať do domácej karantény na 14 dní alebo získať digitálny Covid preukaz EÚ ľubovoľnej osoby,

RODNÉ ČÍSLO

4. Rok 2022: Séria útokov na inštitúcie v Českej republike
5. Rok 2022 a súčasnosť: AI a deepfake, príklad: AI brings Mona Lisa to life

Informačná bezpečnosť a informácie
(alebo čo a prečo treba chrániť ...)

- Internet – virtuálny priestor - informácie
  - Spoločnosť IDC: do roku 2025 sa celosvetové údaje zvýšia o 61% na 175 zettabyte v cloude.
  - Forbes: každý deň sa vytvára 2,5 bilióna údajov, tempo sa zrýchľuje s rastom IoT.

Informačná bezpečnosť a informácie
(alebo čo a prečo treba chrániť ...)

- Internet – virtuálny priestor
- Organizácie/podniky/firmy:
  - Virtuálna identita

    Plusy: ľahká dostupnosť, bez geografických obmedzení, potenciálni zákazníci, klienti, partneri

    Mínusy: strata dobrého mena, zákazníkov, narušenie činnosti
  - Záver: bezplynulý chod organizácie v režime 24/7 vyžaduje spoľahlivé fungovanie vybudovanej informačnej a komunikačnej infraštruktúry.
- Jednotlivec:
  - Virtuálna identita

    Plusy: nové možnosti komunikácie, nadväzovania kontaktov. vzdelávania, spolupráce

    Mínusy: strata priamej sociálnej komunikácie (F2F), pseudoidentita, kyberšikana, možnosť zneužitia identity a strata súkromia
  - Záver: koexistencia reálneho a virtuálneho života jednotlivca vyžaduje osvojenie si základných princípov a postupov ochrany jeho komplexnej identity

Digitálna éra a jej riziká

Charakteristiky

- ❑ Ubiquitous connectivity
- ❑ Globálna počítačová sieť, globálne mobilné siete
  - rôznorodosť poskytovaných služieb,
  - rôznorodosť technologických riešení,
  - rôznorodosť používaných zariadení,
  - neustály vývoj nových služieb – cloud, IoT, virtuálna realita, AI,...
- ❑ Fyzická a virtuálna identita – kde je hranica
- ❑ Otázky bezproblémovej adaptácie a zvládnutia nových služieb/riešení a rozhraní

Pravidlo 1:

Bezpečnosť uložených informácií každého počítača je podmienená úrovňou bezpečnosti iného počítača, ku ktorému sú pripojené.

Pravidlo 2:

Čokoľvek, kdekoľvek, kedykoľvek a kýmkoľvek nahrané, prenesené, vložené do kyberpriestoru v kyberpriestore zostane navždy.

Stávame sa informáciou

Informácie verzus údaje

- Informácie → výsledok spracovania údajov → sú:
  - presné a aktuálne,
  - špecifické a usporiadané na určitý účel,
  - prezentované v kontexte, ktorý im dáva význam a relevantnosť,
  - môžu viesť k zvýšeniu porozumenia a zníženiu neistoty.
- Údaje (dáta)
  - spracovaním sa transformujú na informácie → majú hodnotu →nutnosť chrániť ich

Údaje	Informácie
	
• neorganizované, nespracované fakty, bez spracovania sú pre ľudí zdanlivo náhodné a neužitočné	• spracované, usporiadané údaje, prezentované v určitom kontexte a sú užitočné pre ľudí
• „raw“ dáta, nemajú osobitný význam.	• skupina údajov, majú logický význam.
• údaje nezávisia od informácií	• Informácie závisia od údajov
• získavajú sa na základe záznamov a pozorovaní	• získavajú sa na základe analýzy, spracovania
• nie sú ničím špecifické (prispôsobené konkrétnym potrebám)	• sú špecifické pre danú tému, spracovaním sa odstránia irelevantné údaje.
Záver: údaje sú neorganizované popisy a fakty, z ktorých možno informácie získať.	

Informačná bezpečnosť

Definícia: *Ochrana informácií pred hrozbami s cieľom zabezpečiť ich **dôvernosť, integritu a dostupnosť** koncovému používateľovi.*

Triáda CIA

Z pohľadu podniku: *... s cieľom zabezpečiť kontinuitu podnikania, minimalizovať obchodné riziko a maximalizovať návratnosť investícií a obchodných príležitostí.*

Confidentiality (dôvernosť)

- informácie nie sú dostupné/prístupné neoprávneným osobám/systémom,
- prístup len pre používateľov s pridelenými oprávneniami.

Príklady porušenia:

- likvidácia papierovej dokumentácie bez skartovania,
- prienik hackera do internej databázy webu, e-shopu a krádež citlivých informácií o klientoch (mená, adresy, čísla kreditných kariet),
- inštalácia neoverených aplikácií do mobilu.

Integrity (integrita)

- informácie sú v pôvodnej forme a stave počas celého ich životného cyklu,
- informácie sú úplné a bez narušenia (neboli zmenené, zmanipulované alebo poškoden[á]

Príklady porušenia:

- zapísanie nesprávnych údajov do IS zamestnancom,
- poškodenie súboru vírusom/červom pri ukladaní alebo pri prenose sieťou (šum na sieti).

Availability (dostupnosť)

- mať informácie k dispozícii keď sú potrebné,
- prijímanie informácii v požadovanom formáte a čase,
- prístup pre autorizovaných používateľov bez prekážok.

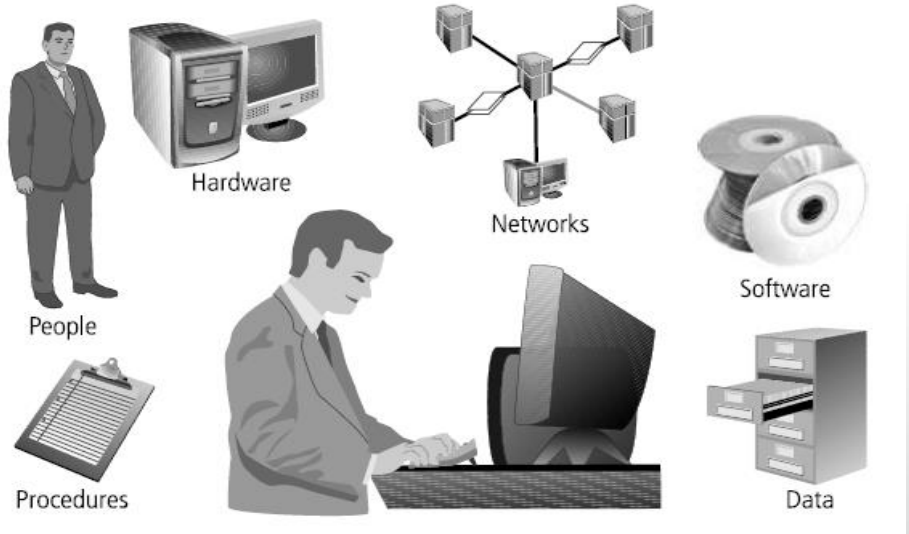
Príklady porušenia:

- výpadok UIS v dôsledku poruchy hardvéru
- ľudská chyba: zamestnanec omylom zmaže kritické súbory.

Informačná bezpečnosť z pohľadu organizácie - proces spracovania informácií

Informačný systém

- ucelený systém pre spracovanie informácií,
- integrované zloženie súboru ľudí, procedúr a postupov, technických prostriedkov (hardvér, softvér, siete) a dát, ktoré zabezpečujú požadovanú funkčnosť a poskytujú informácie pre definovaný účel/cieľ.

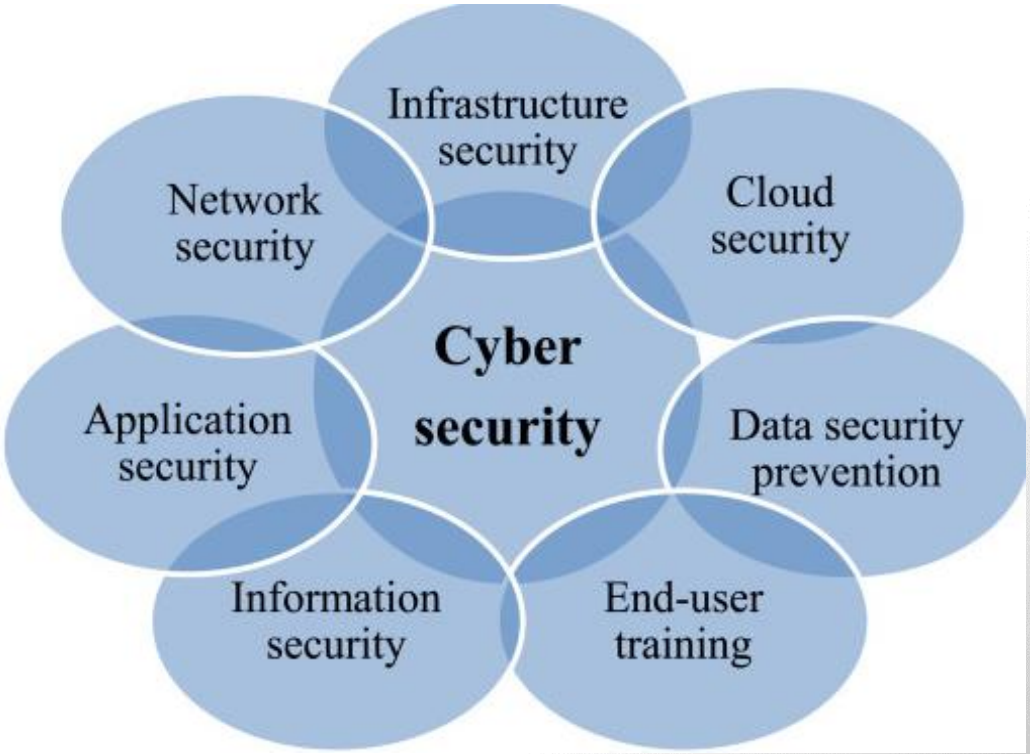


Organizácia →digitálna identita → existencia v kyberpriestore

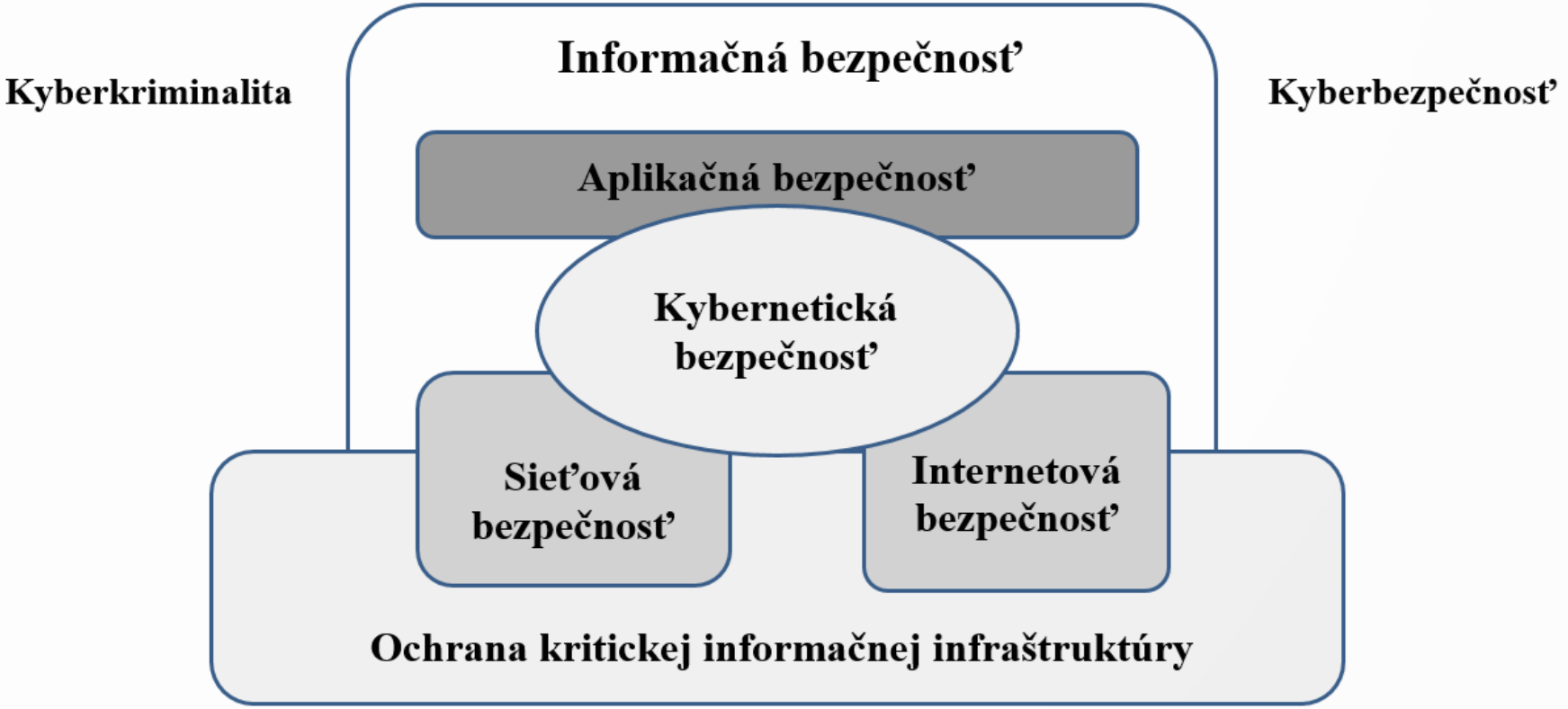
Aké sú východiská pre definovanie IB organizácie:

- špecifiká lokalizácie informačných aktív/údajov: intranet - internet - extranet
- špecifiká poskytovaných služieb: typy služieb a previazanosť s inf. zdrojmi
- špecifiká end-users: inside/outside; anonymizovaní/overení

určujú ČO je obsahom IB



Informačná a kybernetická bezpečnosť



Kybernetické hrozby - PS/WS/MS

Počítačové siete

- Malvér
- Spam
- Sociálne inžinierstvo
- DoS/DDoS
- Phising
- Pharming
- .... ďalšie

WiFi siete:

- Malvér
- DoS
- Sniffing
- Spoofing
- Rouge Access Point
- Wifi Hijacking
- Break WEP/WPA

.... ďalšie

Mobilné siete

- Malvér
- Útok „keeps on going“
- Madware (mobile adw)
- Phishing
- Smishing (SMS phishing)
- Sociálne inžinierstvo
- Únos SIM karty (SIMjacking)
- Fakturačné podvody (billing fraud)
- Cryptojacking
- Jailbreaking/Root

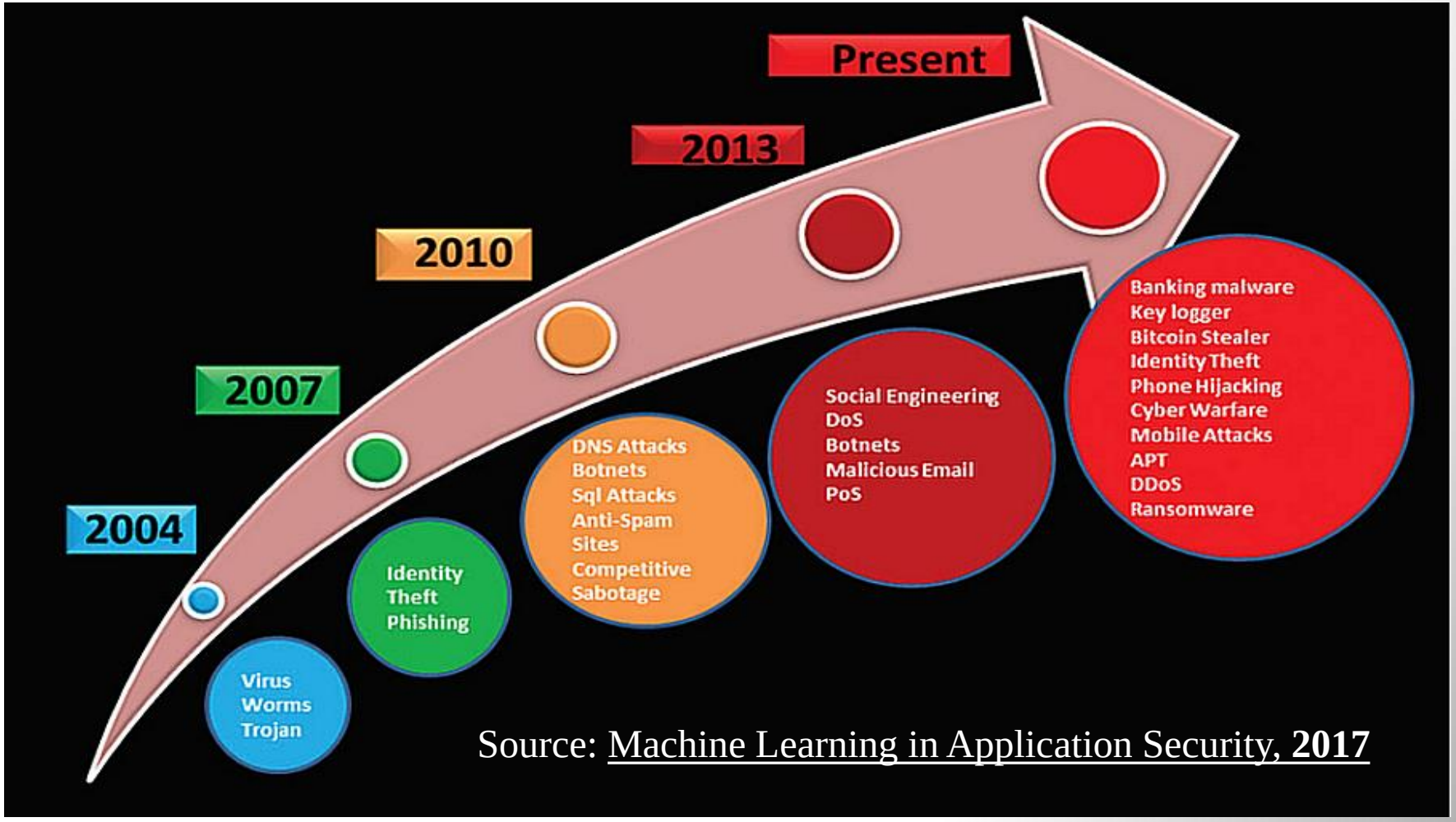
... a ďalšie??

- IoT
- AI
- VR/AR

And not-so-smart end user :-)

Hrozba - akákoľvek okolnosť alebo udalosť s možným nepriaznivým dopadom na prevádzku organizácie alebo jednotlivcov.

Útoky - vývoj v čase podľa technológií/služieb



Útok - cieľavedomý pokus o získanie, zmenu, zničenie, odstránenie informácií bez autorizovaného prístupu alebo povolenia.

Informačná bezpečnosť – jednotlivec

Incidenty, hrozby <=> riziká, dôsledky
Vzdelávanie + Legislatíva

- Týka sa to aj mňa?
- Prečo sa tým zaoberať ?
- Ako predchádzať ohrozeniu a ako sa brániť ?
- Ako vyvodzovať dôsledky ?

Otázka: Týka sa to aj mňa?

Anonymita používateľa na Internete

Pardoxy

- Aplikácie, webové služby, sociálne siete zhromažďujú o používateľoch informácie.
- Majoritne nie sú potrebné k ich priamej funkčnosti.

- Informácie → osobné údaje → akékoľvek údaje k identifikácii jednotlivca
  - osobné (meno, priezvisko, e-mailová adresa, telefónne číslo, bydlisko)
  - citlivé (využívaný OS, verzie aplikácií, súbory cookies a i.)
  - lokalizačné údaje (súradnice GPS, informácie o WiFi, GPRS)
- Poskytnutím (nedobrovoľným či nevedomým) údajov umožňuje používateľ danej služby získať dôležité informácie o svojom živote – ***sám sa stáva informáciou, s ktorou môže niekto obchodovať.***
- Smernica GDPR – ochrana osobných údajov, máj 2018

Digitálna stopa

- Digitálna stopa neovplyvniteľná
  - Informácie z počítačového systému
  - Pripojenie k počítačovým sieťam a Internetu
  - Používanie poskytovaných služieb

- Digitálna stopa ovplyvniteľná
  - vedome využitie služieb,
  - dobrovoľne zverejnenie informácie (blogy, fóra, sociálne siete, e-mail, dátové úložiská, cloud).

Pravidlo 3:
Vždy existuje digitálna stopa - kópia dát ako záloha vytvorená samotným používateľom alebo uložená iným používateľom

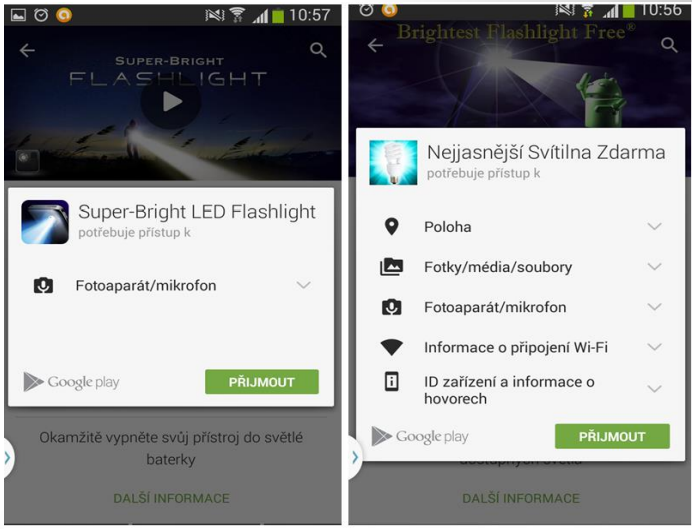
Digitálna stopa – neovplyvniteľná

Patria k nej:

- IP adresa/MAC adresa PC/zariadenia
- E-mail
- Súbory cookies
- Údaje zbierané prostredníctvom smart zariadení

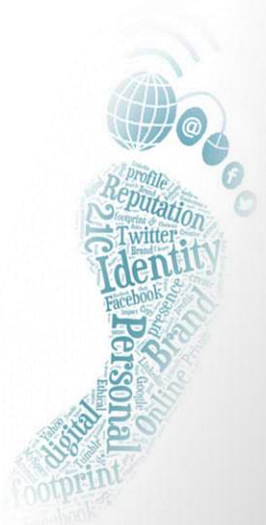
Smart zariadenia – chybné používateľské postupy

- Inštalácia aplikácií používateľom
- Zariadenia nemajú nastavené bezpečnostné mechanizmy, antivír
- Obchod Play umožňuje vývojárovi nastaviť pravidlá „zberu“ informácií
- Obchod Play - aplikácie nie sú overované a testované → možný výskyt aplikácii infikovaných malvérom



Digitálna stopa – ovplyvniteľná

- Informácie dobrovoľne odovzdané/poslané inej osobe (fyzickej či právnickej, ISP).
- Relatívna kontrola používateľom - rozhoduje, čo zverejní.



Činnosti:

- odoslanie e-mailu,
- pridanie príspevku do diskusie, fóra,
- zverejnenie (foto, video, audio) v rámci sociálnych sietí,
- registrácie - sociálne siete, P2P siete, chaty, blogy, webové stránky, cloudové služby, dátové úložiská
- **EULA** podmienky - používanie služieb najväčších ISP (Microsoft, Apple, Google, Facebook a i.) je podmienené odsúhlasením zmluvných podmienok.

Digitálna stopa – ovplyvniteľná

EULA - podmienky

- jednostranne definované práva a povinností zo strany poskytovateľa služby (ISP),
- používateľ má možnosť výberu.

Dilema – problémy a otázky

- **!! malé percento používateľov zmluvné podmienky číta,**
- ? je si vedomý aké zmluvné podmienky odsúhlasil,
- ? kedy sa stávajú záväznými,
- ? aký legálny zásah do jeho základných ľudských práv a slobôd súhlas predstavuje
- ***!! Služba môže ovplyvniť práva a záujmy (alebo bezpečnosť dát) tretích osôb alebo zamestnávateľa, ktorý k službe explicitne nevyjadrilsúhlas.***

Príklad – Google a používateľ

- **Informácie, ktoré používateľ zdieľa sám** (*meno, e-mail adresa, tel. číslo, platobná karta)*
- **Informácie z používania služieb Google**
  - *zariadenie (model hardvéru, verzia OS, telefónne číslo),*
  - *protokol použitej služby (mail, telefón),*
  - *geografická poloha,*
  - *licenčné čísla aplikácií,*
  - *súbory cookies,*

Príklad 2: spracovávané údaje o zákazníkoch e-shopy SR

E-shop Mall.sk (od 2024 Allegro)	E-shop Alza.sk
• ***Identifikácia:*** meno, priezvisko, užívateľské meno a heslo, IČO/DIČ. • ***Kontaktné údaje:*** e-mail, telefónne číslo, adresa doručenia/fakturačná adresa, kontakt na sociálnych sieťach. • ***Nastavenia zákazníka:*** účet zákazníka, odber newsletter, vernostné programy, nákupné zoznamy, sledované produkty, hodnotenia produktov. • ***Objednávky:*** objednaný tovar/služba, spôsob doručenia a platby, číslo účtu, reklamácie. • ***Správanie na webe:*** prehliadaný tovar a služby, klikané odkazy, údaje o zariadení (IP adresa, typ zariadenia a jeho parametre: OS, prehliadač, cookies). • ***Čítanie zasielaných správ:*** čas otvorenia správ, použité zariadenie. • ***Odvodené údaje:*** pohlavie, vek, finančná situácia, nákupné správanie. • ***Call centrum***: záznamy telefónnych hovorov	***Pri prístupe zákazníka cez web stránku:*** • IP adresa, • dátum a čas prístupu na web stránku e-shopu, • informácie o internetovom prehliadači, • informácie o operačnom systéme či nastavení jazyka, • informácie o správaní zákazníka na webových stránkach internetového obchodu, • v prípade návštevy webovej stránky cez telefón alebo tablet - dáta o mobilnom telefóne.

Právo a Internet

- **Základné otázky**
  - Platí právo na Internete?
  - Ak áno, aké právne normy sa použijú?
- **Dilemy**
  - Kyberpriestor
    - Virtuálne prostredie
    - Je otvorený a prístupný všetkým
    - Neplatia tu žiadne zvláštne zákony a je potrebné sa riadiť všeobecne záväznými normami
  - Fenomén Internetu:
    - Je globálny a nepozná hranice
    - Nemá majiteľa
  - Fenomén internetových služieb:
    - Široké spektrum
    - Nespoplatnené – veľké množstvo používateľov – viac rôznych identít
  - Fenomén koncového používateľa:
    - Digitálna gramotnosť
    - Dôverčivosť, naivita, láskavosť, zvedavosť, nedôslednosť,...
    - ?? Váš názor

Právne normy Slovenskej republiky

Základný dokument:

- Ústavný zákon č. 460/1992 Zb. - **Ústava Slovenskej republiky**
- Čl. 19 ods. 3 Ústavy SR

  *Každý má **právo na ochranu pred neoprávneným zasahovaním** do **súkromného a rodinného života**.*

- Čl. 22 Ústavy SR

  ***Listové tajomstvo, tajomstvo dopravovaných správ a iných písomností** a **ochrana osobných údajov** sa zaručujú*.

Právne normy Slovenskej republiky

Základné dokumenty:

- Zákon 40/1964 Občiansky zákonník
- Zákon 513/1991 Obchodný zákonník
- Zákon 311/2001 Zákonník práce
- Zákon 300/2005 Z. z. Trestný zákon
- Zákon 301/2005 Z. z. Trestný poriadok

- Zákon 211/2000 o slobodnom prístupe k informáciám
- Zákon 215/2004 o ochrane utajovaných skutočností
- Zákon 22/2004 o elektronickom obchode
- Zákon 45/2011 o kritickej infraštruktúre
- Zákon 351/2011 o elektronických komunikáciách
- Zákon 185/2015 autorský zákon
- Zákon 214/2008 zmena zákona o elektronickom podpise

- **Zákon 18/2018 o ochrane osobných údajov**
- **Zákon 69/2018 o kybernetickej bezpečnosti**
- **Zákon 95/2019 o informačných technológiách vo verejnej správe**
- **Zákon 236/2021 o nebezpečnom elektronickom obťažovaní (kyberšikana)**

Obsah informačnej bezpečnosti zhrnutie

- Informácie, dáta ==> aktíva spoločnosti, organizácií
- Incidenty, hrozby <==> riziká, dopady
- Dokumenty pre IB <==> legislatíva, právne normy
- Proaktívny prístup <==> vzdelávanie

Be smart end user ...