Jak se chovat v cyberprostoru

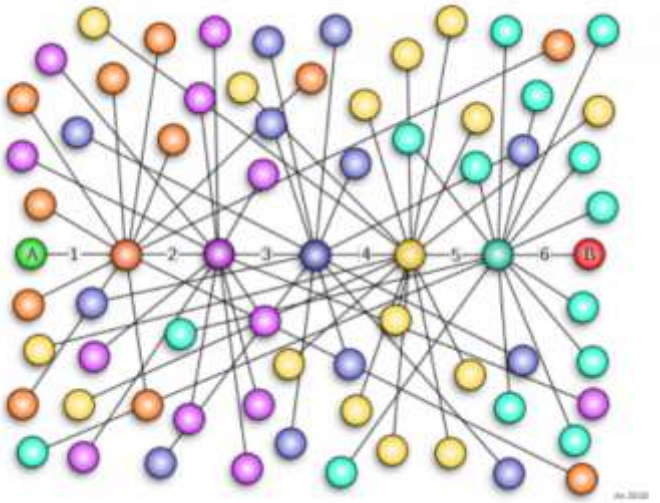
Ing. Pavel Bezpalec, Ph.D.
bezpalec@vosis.cz

- Pojmy Cyber ...
- Virtualizace a cloudy
- Uživatel a jeho data
- Instant messaging
- Osobní vs neosobní komunikace
- Co na sebe prozradíme ...
- Hesla
- Diskuse

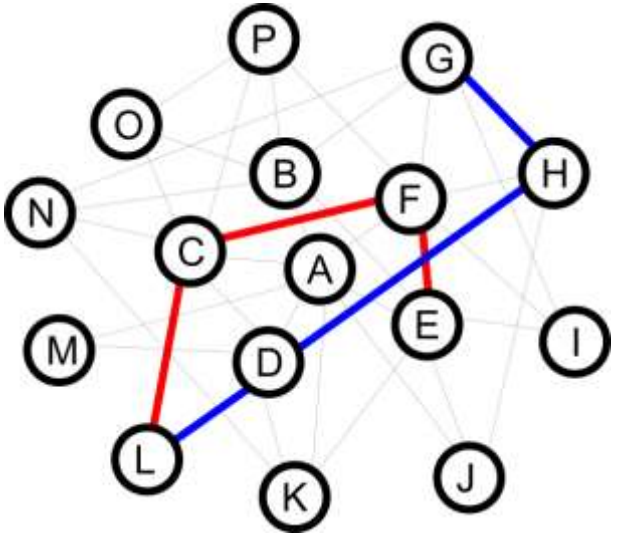
Facebook Friendship Network

Six degrees of separation

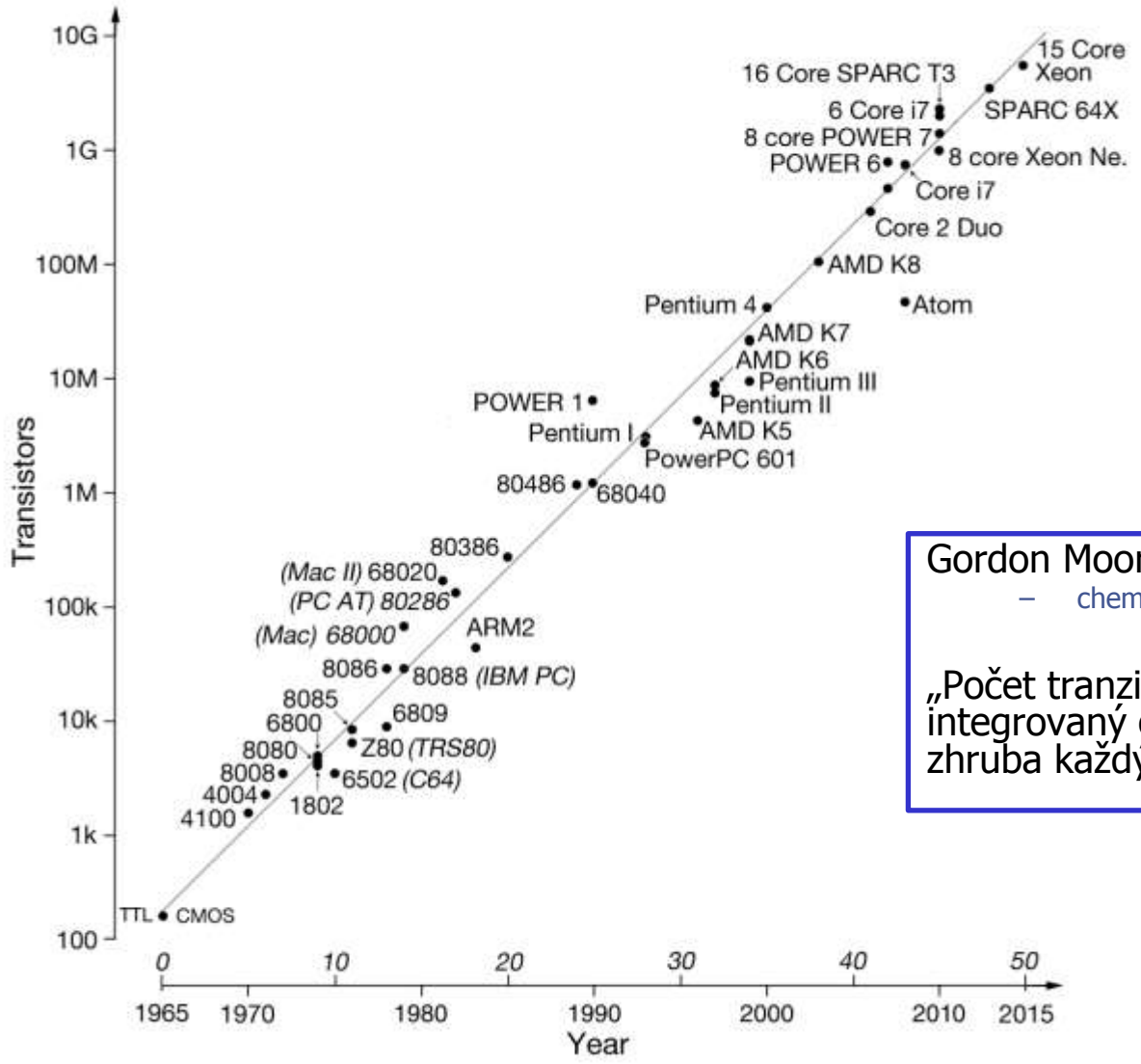
- Šest stupňů odloučení
- 1967 – Stanley Milgram
  - Každý člověk je spojen s každým člověkem prostřednictvím řetězce šesti sobě navzájem známých lidí.



- Facebook
  - 99,6% párů uživatelů jsou spojeni prostřednictvím 5 jiných uživatelů
  - 92% pouze přes 4
- Twitter
  - průměrné číslo odloučení – 4,67



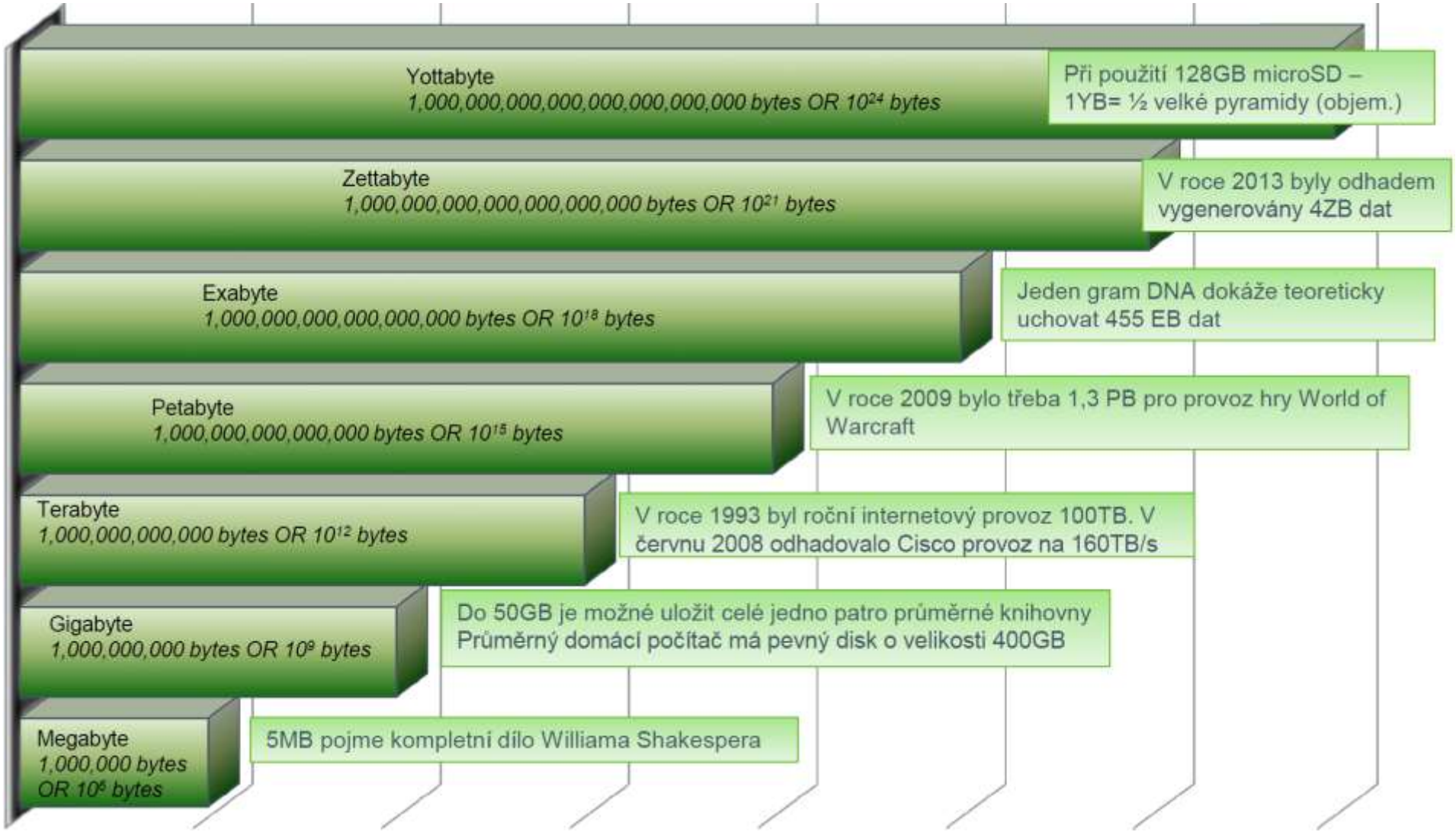
Moorův zákon



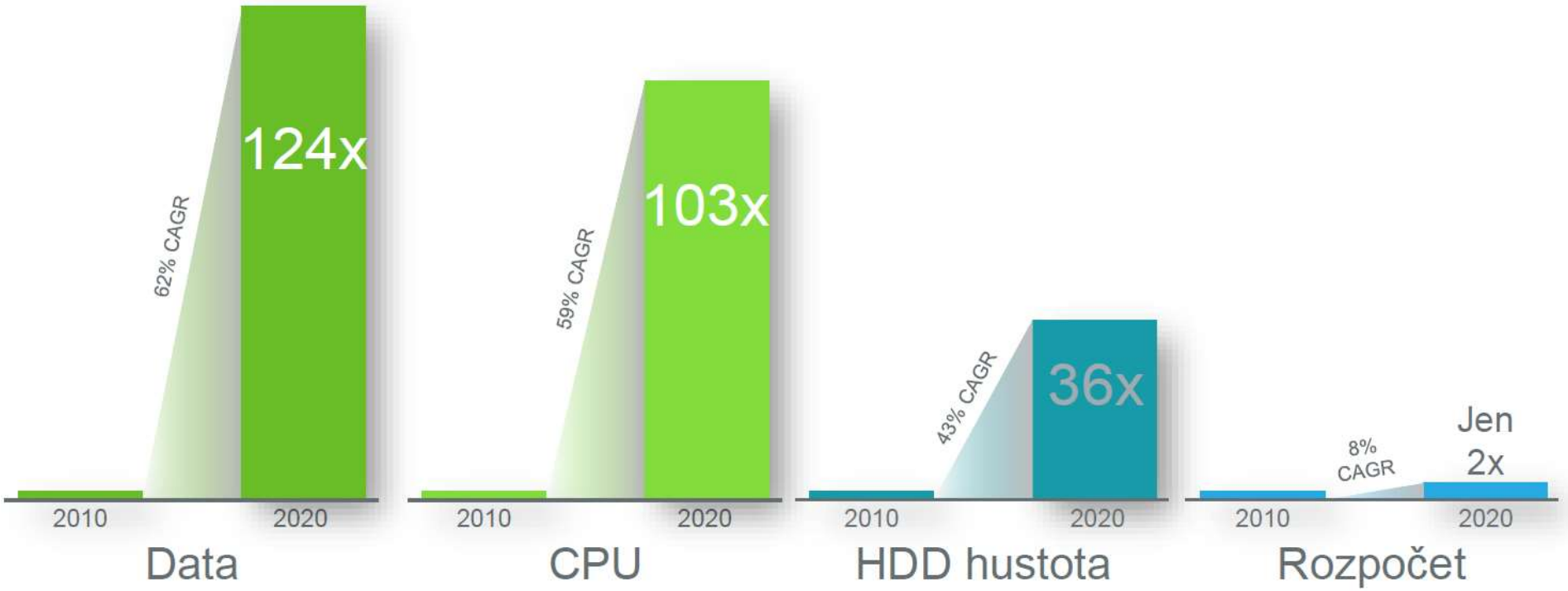
Gordon Moore
- chemik, zakladatel INTEL

„Počet tranzistorů, které mohou být umístěny na integrovaný obvod, se při zachování stejné ceny zhruba každých 18 měsíců zdvojnásobí"

Objem dat ...



Vše roste … až na …



- Stejný rozpočet
- Zvýšená komplexnost
- Nárůst objemu

Virtualizace

Hypervisor - **2001** Dynamic memory - **2001** VMFS - **2001** Vmotion - **2003**

32 logických CPU - **2006** Hot Add vDisk - **2006** Memory Virtualization - **2007**

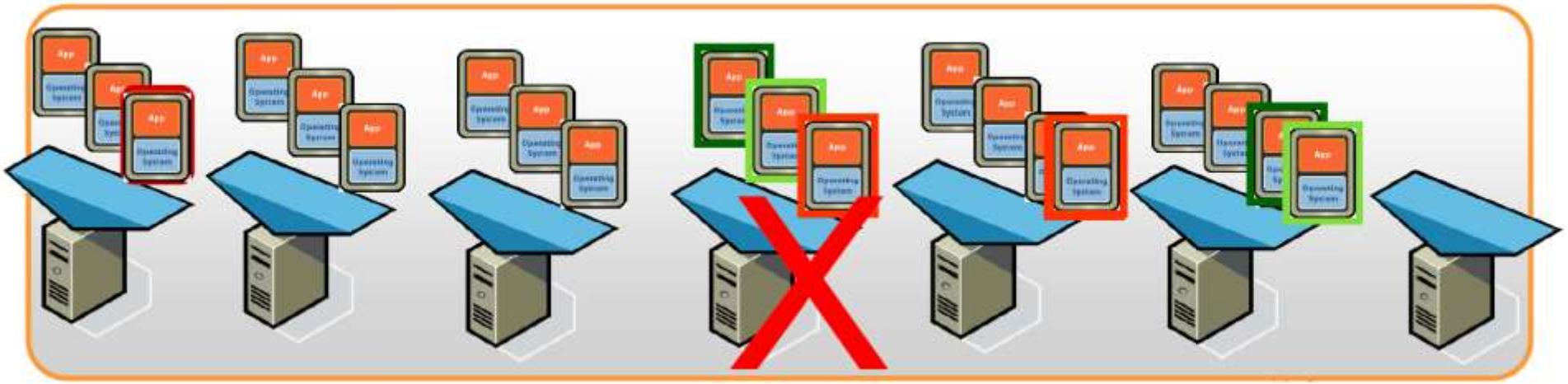
Automated Resource Assurance
- Dynamic Balancing
- Continuous Optimization

+

Increased Availability
- Automated
- Across Applications

+

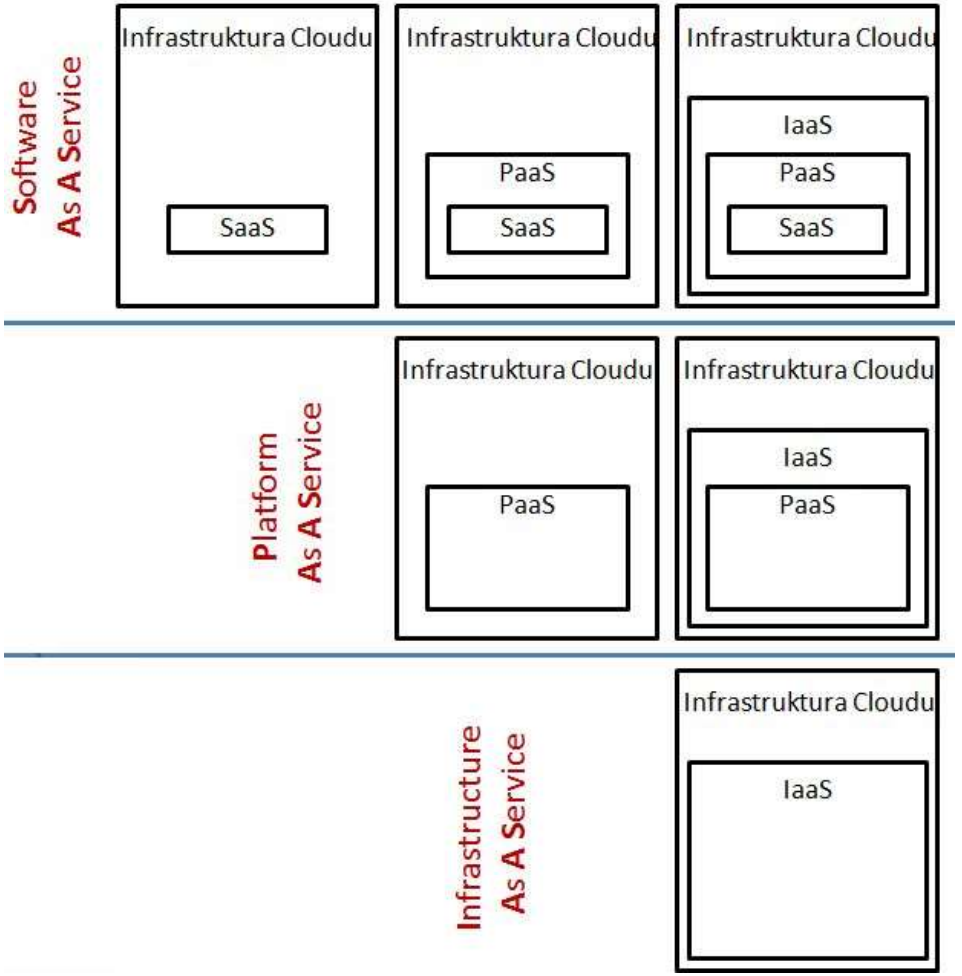
On Demand Capacity
- Non-disruptive Scaling
- Flexible, Reconfigurable




DEFINICE
CLOUD COMPUTING
poskytování sdílených výpočetních prostředků
a jejich využívání formou služby

Cloud – servisní modely

- SaaS (Software as a Service)
  - webmail, kancelářské nástroje, hry
    - Google Apps, Office365
- PaaS (Platform as a Service)
  - běhové prostředí, webservery, DB
    - WinAzure, GoogleApp Engine
- IaaS (Infrastructure as a Service)
  - virtuální stroje, servery, úložiště, síť
    - Amazon EC2, VMWare, GoogleCloudStorage



Cyber-

- Kybernetický prostor
  - Kyberprostor (*cyberspace*)
    - „Konsenzuální datová halucinace, vizualizovaná v podobě imaginárního prostoru, tvořeného počítačově zpracovanými daty a přístupná pouze vědomí uživatelů"
  - virtuální svět informací vzniklý propojením ICT (internet …)

- Kybernetická bezpečnost
  - *cybersecurity*
  - odvětví výpočetní techniky zabývající se ochranou informací a majetku před zneužitím za předpokladu zachování přístupnosti pro jeho uživatele

- Kyberkriminalita, kyberterorismus, kyberzločin, kyberválka, kyberarmáda …
- Kybernetický útok
  - *cyberattack*
  - promyšlené škodlivé jednání útočníků zaměřené proti komunikačním a informačním technologiím s cílem způsobit škody

Kybernetická bezpečnost (*cybersecurity*)

- Definice
  - Souhrn prostředků a postupů na zabezpečení důvěrnosti, integrity a dostupnosti informací, na zabezpečení autentizace uživatelů a zdrojů, účtovatelnosti operací, jakož i zabezpečení ochrany proti neautorizované manipulaci, modifikaci nebo zničení, resp. poškození informací v informačním systému.

- IS – informační systém
  - celek, na který se vztahuje kybernetická bezpečnost

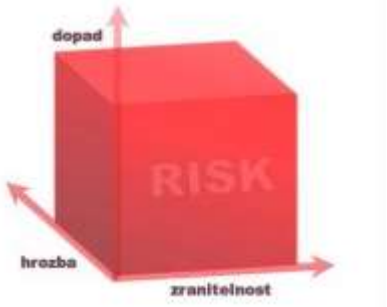
- Důvěrnost (*confidentiality*)
  - přístup k informacím a poskytnutí pouze oprávněným osobám
- Integrita (*integrity*)
  - úplnost a přesnost zpracované, resp. přenášené informace
- Dostupnost (*availability*)
  - dostupnost informací pro oprávněné uživatele v okamžiku potřeby

Ochrana informací, IS

- ISO/IEC 27001 – *Information Security Management Systems (ISMS)*
  - systém řízení bezpečnosti informací
  - nejrozšířenější a celosvětově uznávaný standard
  - bezpečnost informací musí být řízena nezávisle na velikosti firmy
  - zahrnuje management, politiku, organizaci i pravidelné přezkoumávání
  - certifikace systému managementu bezpečnosti informací podle normy ČSN ISO/IEC 27001:2013
- GDPR – Obecné nařízení na ochranu osobních údajů

Rizika IS

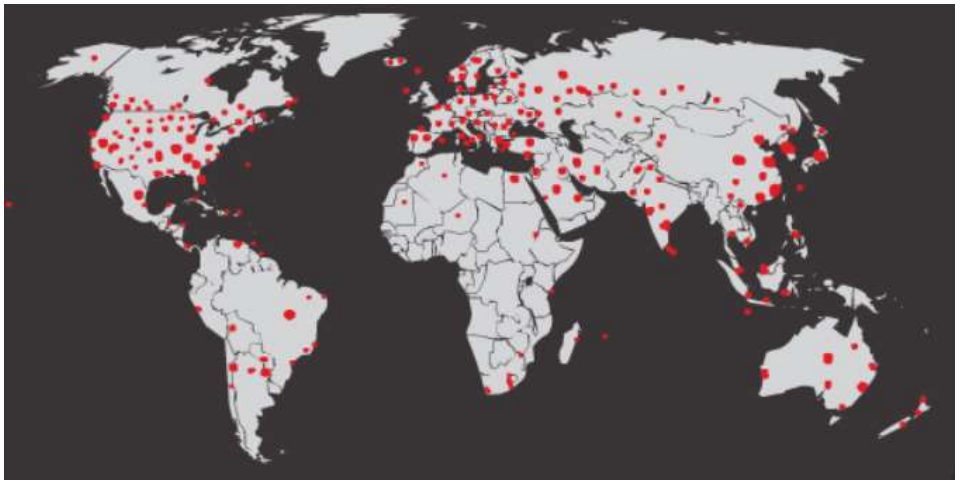
- Zranitelnost (*vulnerability*)
  - slabé místo IS
  - nezpůsobuje přímé škody nebo ztráty, ale vytváří pro to podmínky
  - nízká, střední, vysoká
- Dopad (*impact*)
  - výsledek bezpečnostního incidentu
  - přímý
    - narušení důvěrnosti a integrity dat nebo ztrátou dostupnosti dat
  - nepřímý
    - finanční ztráta, ztráta konkurenceschopnosti
- Hrozba (*threat*)
  - úmyslná
    - odposlech, modifikace informace, neautorizovaný přístup
  - neúmyslná
    - chyby způsobené nesprávnou obsluhou IS

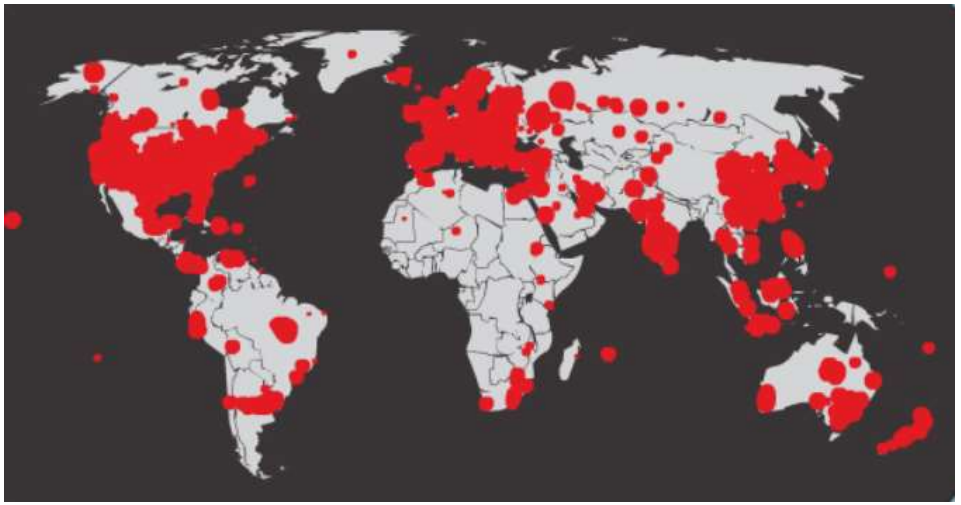


Malware

- škodlivý, zákeřný software

- Virus
  - šíří se sám bez vědomí uživatele
  - vkládá se do jiných spustitelných souborů či dokumentů
- Worm
  - po infikaci systému, převezme nad ním kontrolu a
  - rozesílá kopie sebe sama na jiné počítače
- Trojský kůň
  - uživateli skrytá část programu s funkcí, se kterou uživatel nesouhlasí





červ SQL Slammer po 30 minutách činnosti

Malware

- Ransomware
  - blokuje počítačový systém nebo šifruje data v něm zapsaná
  - pak požaduje výkupné za obnovení přístupu
- Spyware
  - odesílá data bez vědomí uživatele
- Adware
  - reklamní software znepříjemňující práci
- Crimeware
  - podílí se na páchání počítačové trestné činnosti

- Phishing
  - podvodné získávání citlivých údajů
- Rootkit
  - utajení nekalé činnosti modifikací napadeného systému

Útoky na bezpečnost IS

Útoky na bezpečnost IS

- Pasivní útoky
    - získání informací z IS, systémové prostředky nejsou ovlivněny
  - sledování (odposlech) nebo monitorování provozu
    - odkrývaní obsahu zpráv
    - analýza toku dat
- Aktivní útoky
    - pokus o aktivní ovlivnění systémových prostředků
  - předstírání identity
  - opakování
  - modifikace zpráv
  - odmítnutí služby (DOS – Denial of Service)
    - aktivní útok zabraňující standardnímu využití služby
    - rozpad sítě, zamezení přístupu do sítě, zahlcení sítě zprávami s cílem degradace její výkonnosti
  - distribuované odmítnutí služby (DDOS – Distributed Denial of Service)

PRVNÍ ...

- První SPAM
  - 9.5.1978 v 14:00
  - prezentace firmy Digital
- První DoS útok
  - únor 2000
  - Kanadský teenager „Mafiaboy"
    - pravé jméno nebylo zveřejněno
  - 8 měsíců + 1 roční podmínka
  - pokuta USD250
- První virus šířený e-mailem
  - 1999 – Melissa
  - David Smith, New Jersey
  - 20 měsíců nepodmíněn, 5.000$ pokuta
- První červ
  - 1988
  - Rober Morris
  - nakaženo odhadem 6000 počítačů - 10% všech připojených k Internetu
  - 400 hodin veřejně prospěšných prací
  - 3 roky podmínka + pokuta USD10000

Útoky

- Podle motivace útočníka
  - cílené útoky
    - konkurence (průmyslová špionáž)
    - vyhození zaměstnanci
  - necílené – „tohle mi dal Franta a teď jsem H4CK3R"
- Podle místa původu útoku
  - z vnějšku
  - zevnitř
- Podle typu činnosti
  - průzkumné
  - získání přístupu
  - DoS (Denial of Service), DDoS
  - červi, viry, trójští koně

Útočníci

- Vnitřní útočník (Insider)
  - legitimní uživatel, který získal neautorizovaný přístup, nebo zneužívající svých práv
- Vnější útočník (Outsider)
  - subjekt, který nemá autorizovaný přístup do interní počítačové sítě a chce proniknout do této sítě využívajíc jejích zranitelných míst a bezpečnostních děr.
- Amatéři
  - provádí méně nebezpečné útoky
  - adekvátní jejich nízké úrovni vzdělání a vybavení
- Profesionálové
  - špičkoví počítačoví odborníci se špičkovým vybavením
  - schopni generovat velmi nebezpečné útoky s vážnými důsledky

Útočníci

- Scriptkiddies
  - nízká úroveň znalostí
  - útoky náhodné s využitím skriptů obsahujících kód využívající zranitelnost počítačového systému
  - bez hlubší analýzy aplikují takový kód v počítačovém systému
  - značné škodlivé následky
  - nebezpeční

- Hacker
  - osoba s dobrými až výbornými znalostmi z oblasti výpočetní techniky
  - podílí se na výzkumných SW projektech
  - pomoc při hledání zranitelných míst a bezpečnostní děr
  - prospěšný a užitečný
  - hackerský kodex

- Cracker
  - schopný obcházet protipirátské ochrany
  - využívá své vědomosti neeticky

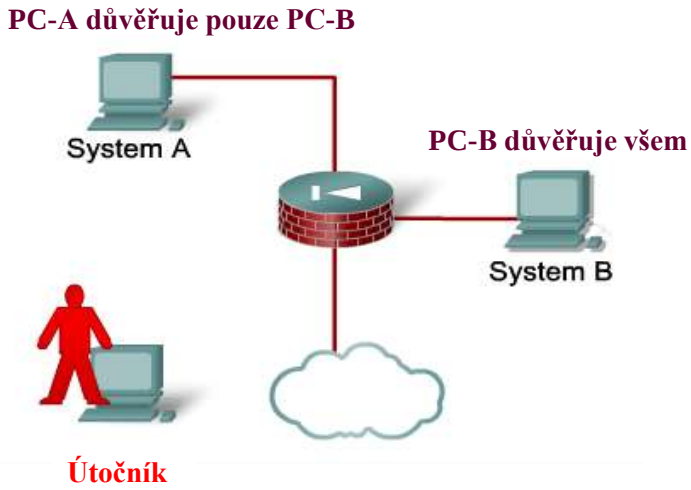
Průzkumné útoky

- Cíl: zjistit informace o topologii sítě, adresaci, aktivních službách, verzích OS a serverových služeb
  - využití i pro správce sítě
  - nemusí se jednat vždy o útok, ale může být jejich součástí
- Techniky:
  - port-scan,
  - odposlouchávání provozu (sniffing),
  - oťukávání (ping sweep)
- Jak na to: http://nmap.org/

Přístupové útoky

- Cíl: získat přístup k chráněným informacím

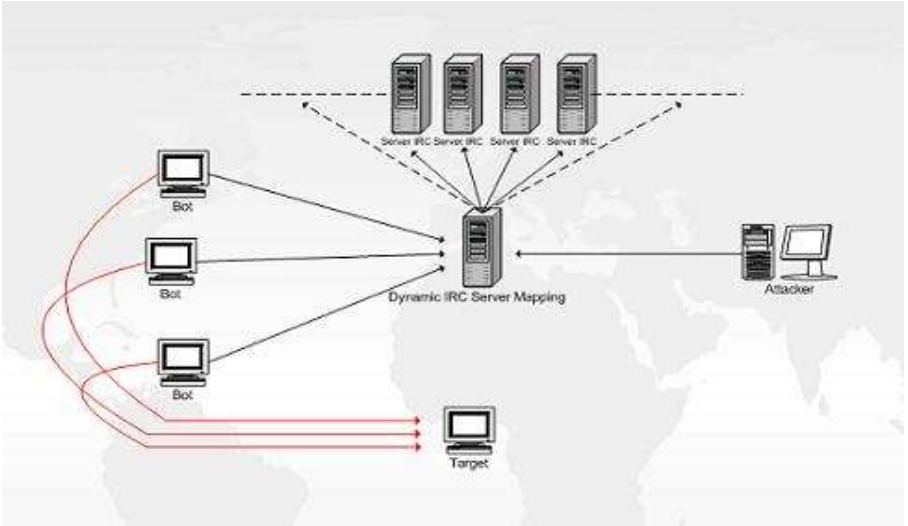
- Patří sem:
  - útoky na hesla
    - zneužití důvěry
  - social engineering
  - přesměrování provozu
  - man-in-the-middle
  - buffer-overflow



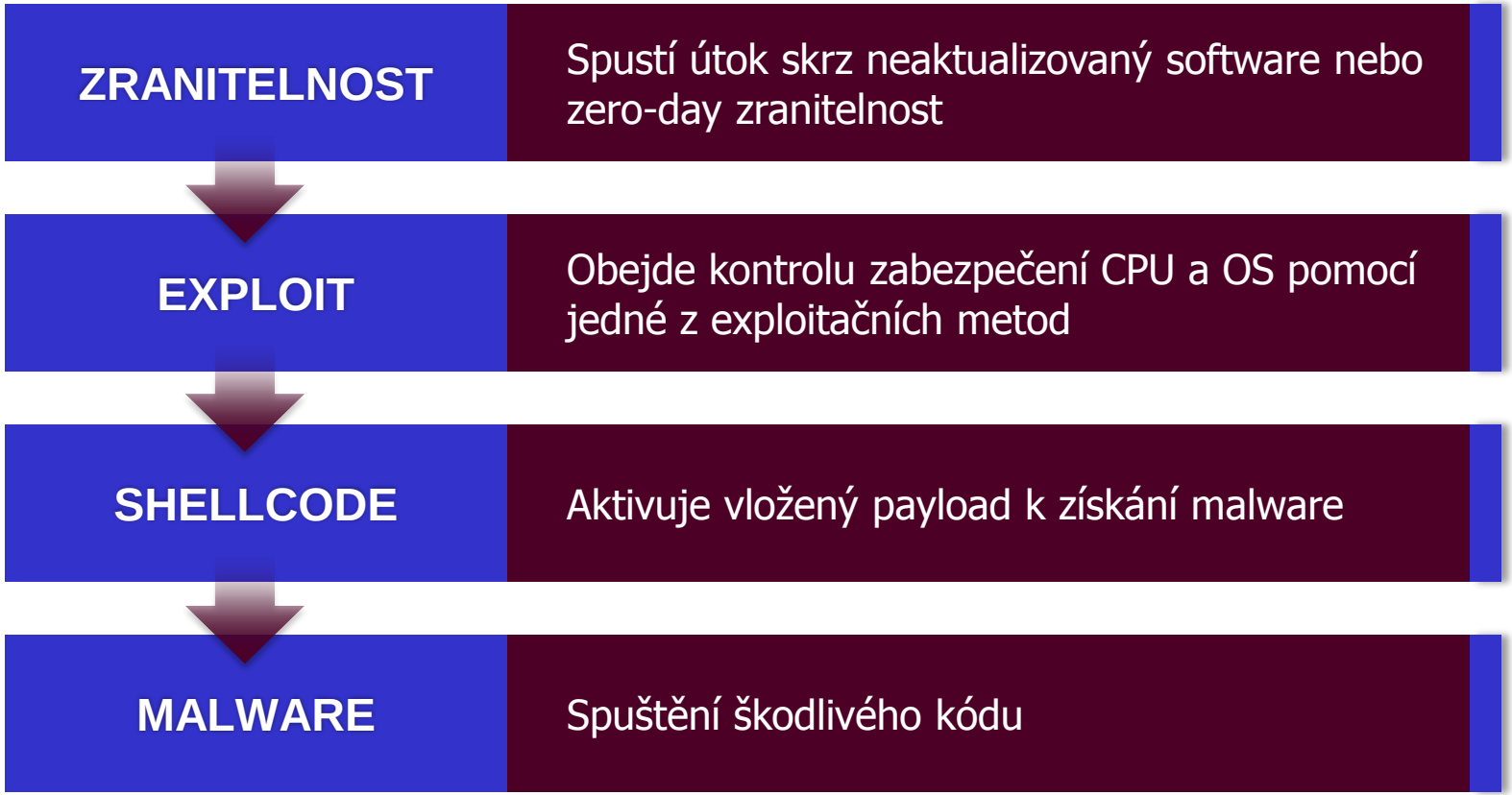
DoS – Denial of Service

- cílem útočníka je vyčerpání systémových prostředků (paměť, CPU, šířka pásma) síťového prvku nebo serveru a jeho zhroucení nebo změna požadovaného chování

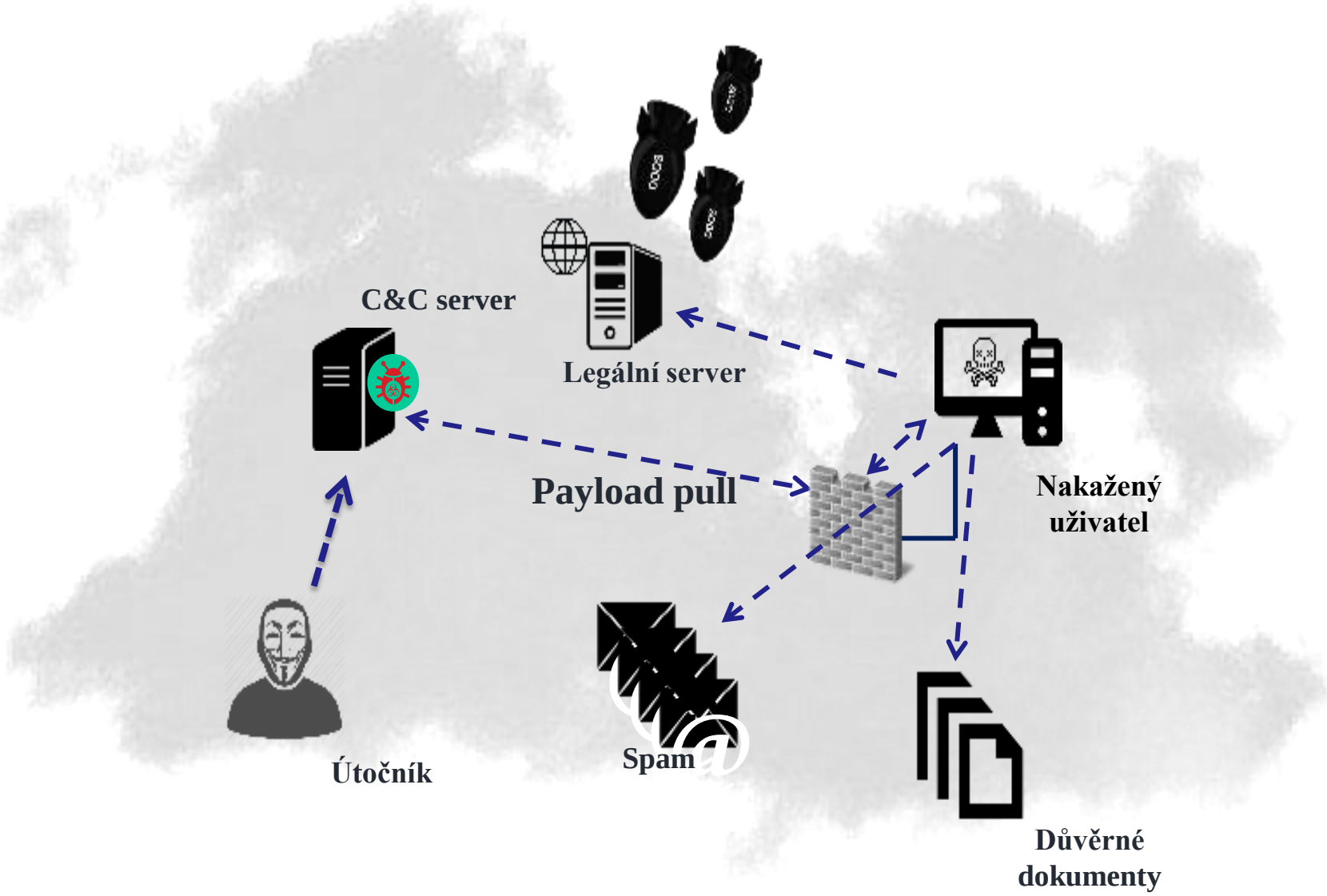
- DDoS – zombie / botnet
  - až desetitisíce PC
  - Botnet Srizbi – 6*1010 SPAMů denně
  - dobrovolné botnety
- Příklady:
  - Ping of Death
  - ICMP Flood
    - Smurf – directed broadcast se zfalšovanou SA
  - SYN Flood



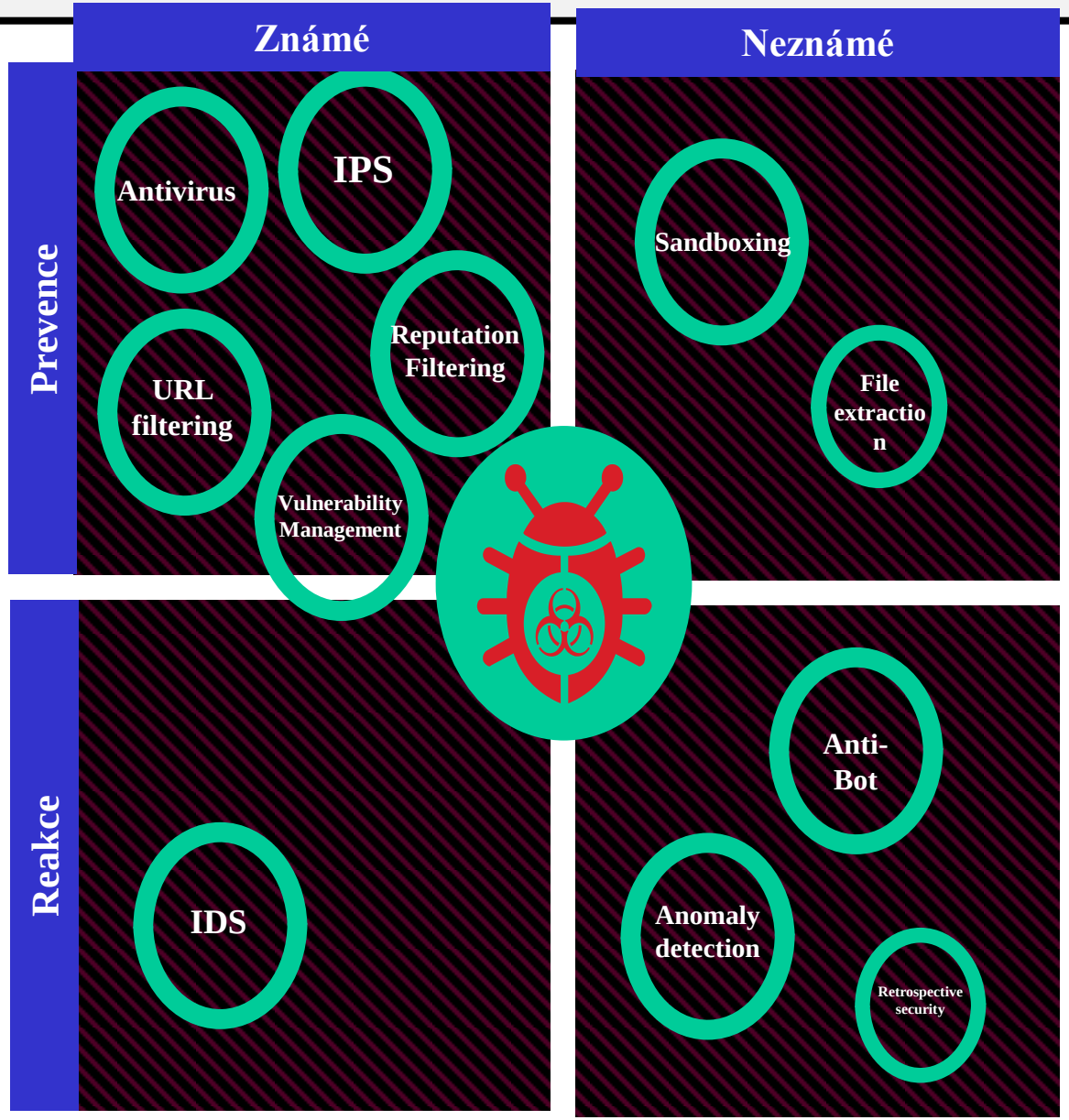
Průběh útoku



A potom?



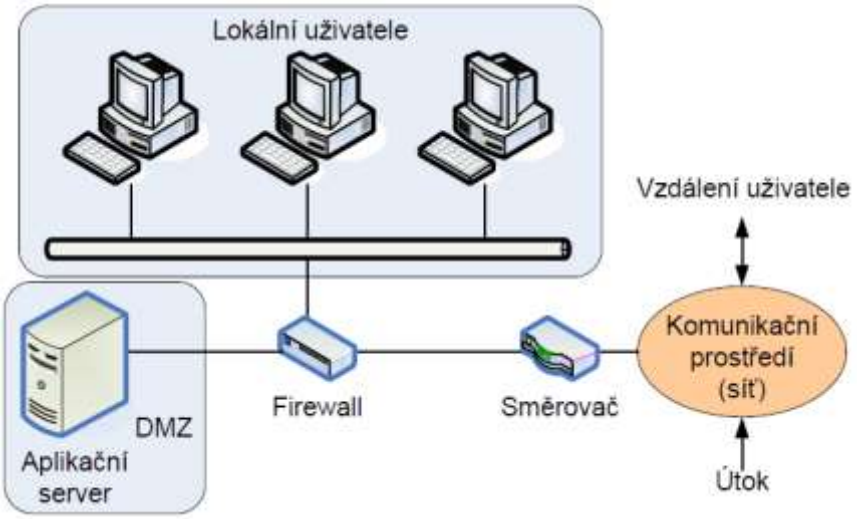
Jak se aktivně bránit ?



Jak se bránit

- Firewall
  - samostatný
  - osobní
  - jednoduchý síťový filtr
    - komunikační pravidla
  - stavový filtr
    - stav rozhraní
  - FW na aplikační vrstvě
    - proxy server
- Aktualizace a záplatování
  - a nejenom Windows …
- Bezpečnostní politiky
- Ochrana citlivých informací
- Anti-[virus | spam | malware | rootkit] programy

- DMZ
  - speciální síť
  - externí služby
  - interní služby
  - oddělení FW



Bezpečnost v praxi

Služby bezpečnosti

- Autentizace (*authentication*)
  - zaručení autenticity komunikace, uživatelů, zdrojů dat
- Řízení přístupu (*access control*)
  - řízený přístup k datům na základě přístupových práva
- Zabezpečení důvěrnosti dat (*data confidentiality*)
  - ochranu informačního obsahu dat
  - spojově nebo nespojově orientovaná komunikace
  - ochrana dat proti analýze
- Zabezpečení intergrity dat (*data integrity*)
  - ochrana proti neautorizované modifikaci
- Ochrana proti odmítnutí původu zprávy (*nonrepudiation*)
  - důkaz o původu dat

Mechanizmy

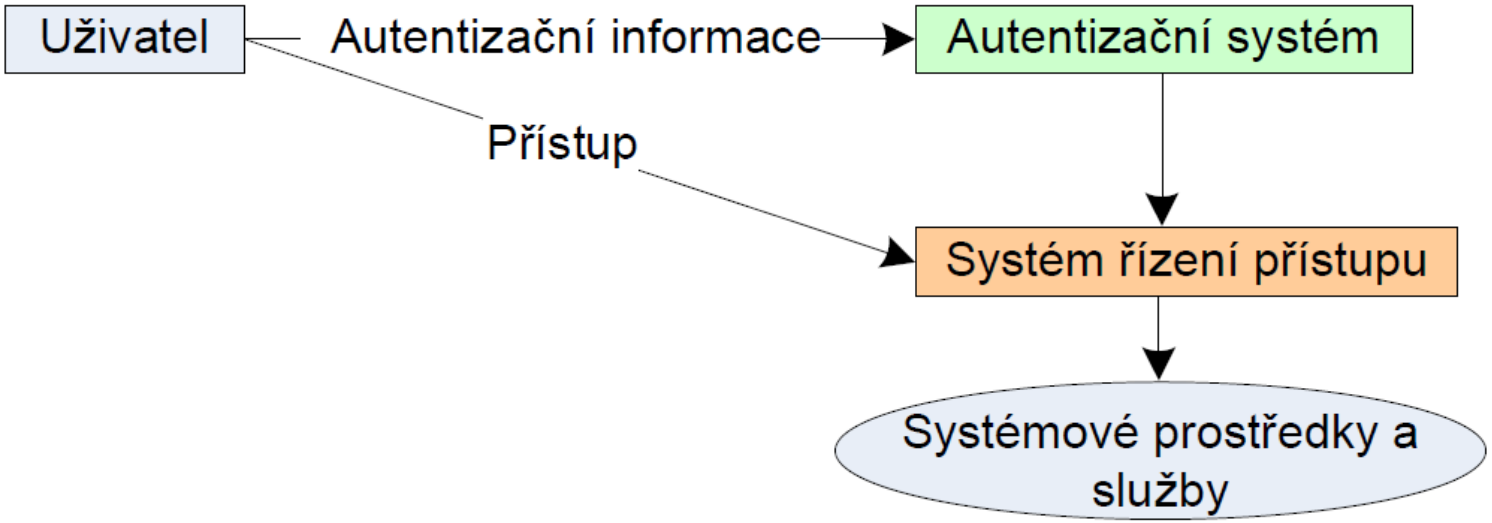
- Šifrování
  - utajení informačního obsahu zprávy
  - kryptografická transformace zprávy do formy nečitelné neautorizovaným subjektem
- Digitální podpis
  - kryptografické transformace pro autentizaci zdroje zprávy a integrity dat
- Řízení přístupu
  - řízení a kontrola přístupových práv k systémovým prostředkům a službám
- Integrita dat
  - kontrola integrity přenášených dat
- Výměna autentizační informace
  - mezi uživatelem a IS
  - ověření identity uživatele
  - ovlivňuje řízení přístupu k systémovým prostředkům a službám
- Vyplňování mezer
  - vkládaní dodatečných bitů do mezer mezi daty
  - znemožnění analýzy toku dat
- Řízení směrování
  - změna směrování toku dat
    - zejména v případech, kdy se očekává narušení bezpečnosti
- Osvědčení třetím (důvěryhodným) subjektem
  - využití třetího subjektu na zabezpečení určitých bezpečnostních aspektů

Přístupová bezpečnost

- Autentizace
  - ověření identity entity
  - rozhodnutí o přístupu k systémovým protředkům

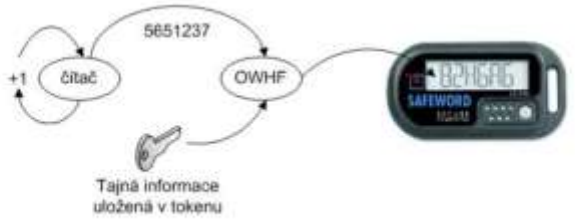
  - registrace ➔ potvrzení totožnosti ➔ udělení/neudělelní přístupu

  - heslo, PIN, čip, USB token, biometrie

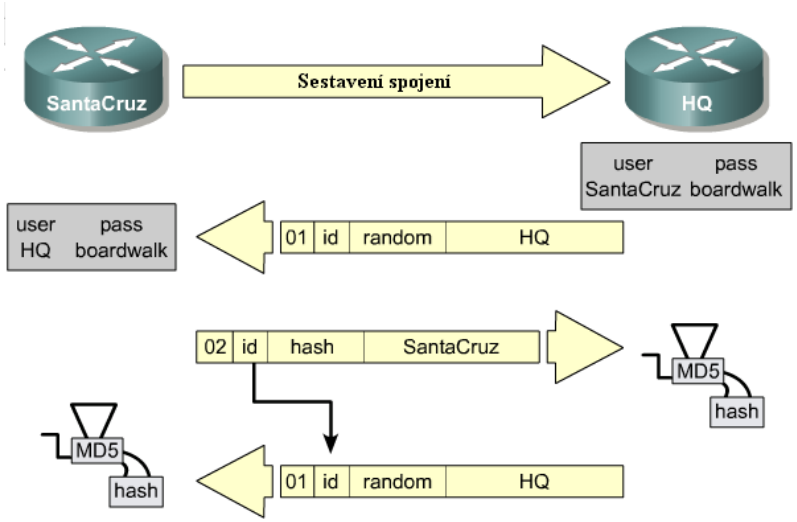


Autentizace

- Token
  - unikátní
  - mag. nebo čipové karty
  - HW i SW



- Dvoufaktorová autentizace



- Heslo
- Hash z hesla
- Výzva-odpověď

HESLA, Hesla, hesla

- Politika hesel
  - změna *defaultního* hesla
- Životní cyklus hesel
  - stáří a obnova
- Tvorba a ochrana hesla
  - papírek na monitoru ?
  - na krabici na kapesníky ?
- Množství hesel
  - intranet, e-mail, banky, škola, obědy, e-obchody, …

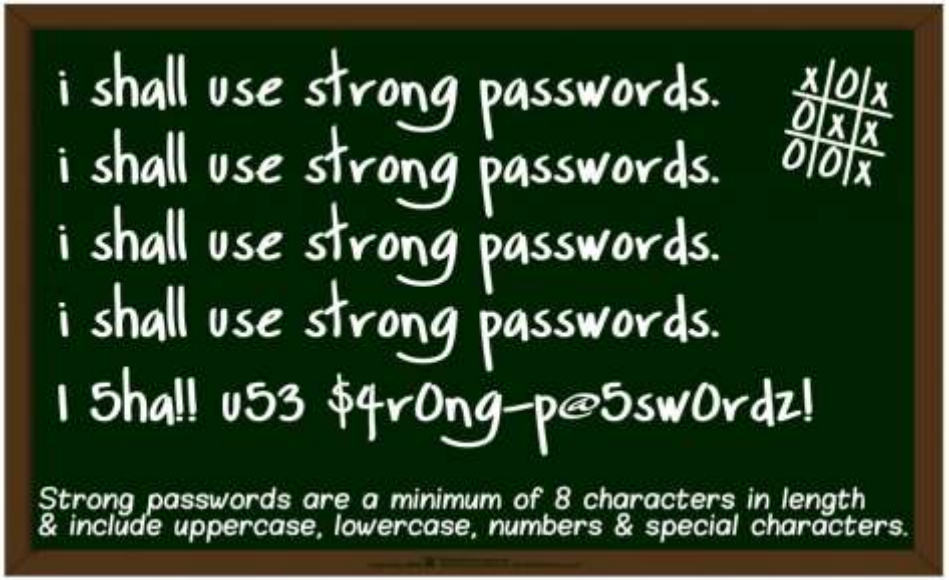
www.howsecureismypassword.net

Dobré heslo

- Nepředpověditelné
- Jedinečné
- Snadno zapamatovatelné pro lidi
  - rozumně dlouhé
    - Dobrojeprisjetitisedaprividnopravputpremaciljupredstavljaustvaripravodlivokrivudanje
  - jednoduše napsatelné
- Nesnadno uhodnutelné pro stroje
    - S0bJK7BYqlmSeQ4QB4rwG8pVgLg5WXOU
- „Často" měněno
- Passphrase
  - dlouhé heslo složené z více slov

Nejhorší hesla roku 2017

- 123456
- password
- 12345
- 12345678
- qwerty
- 123456789
- 1234
- baseball
- dragon
- football
- 1234567
- monkey
- letmein
- abc123
- 111111
- mustang
- access
- shadow
- master
- michael
- superman
- 696969
- 123123
- batman
- trustno1



https://www.securitymagazine.com/articles/88626-the-worst-passwords-of-2017-revealed

Bezpečnost mobilní komunikace

Mobilní zařízení

- Notebook, netbook, tablet, phablet, smartphone …
- Víceúčelová zařízení, která mimo jiné umí i telefonovat
  - náhrada kalendáře, fotoaparátu, diktafonu, zápisníku, kalkulačky, slovníku …
  - mapy, navigace
  - úložiště hesel, přístupových údajů (EZS …)
  - přístup k internetu
  - e-maily, VPN, firemní internet
  - sociální sítě
    - FB, LinkedIn, Instagram, G+, Flicker, Lidé, Spolužáci …
  - NFC technologie ➔ peněženka
  - přístup k bankovním účtům

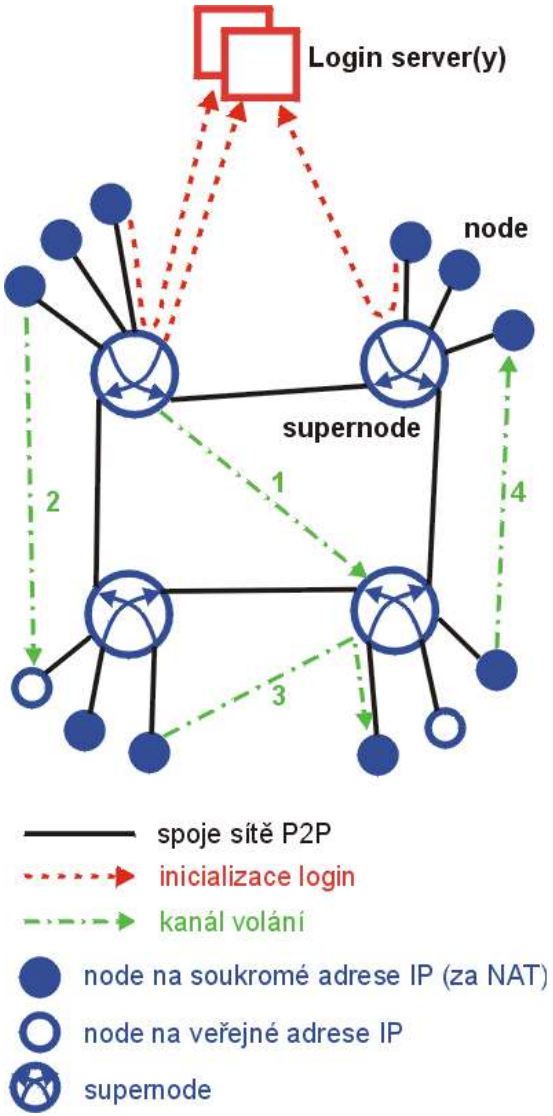
Mobilní uživatel a jeho data

- Vysoké riziko zneužitelnosti dat
  - i přes snahy zabezpečit komunikaci více kanálovým způsobem ➔ data + SMS
    - přístup k bankovním službám
    - EUROGRABBER …
  - sběr info o poloze
    - GPS data, Wifi sítě
      - Google, Microsoft, Nokia, Samsung …
      - levné čínské telefony prodávané v USA
  - instalace app bez autorizace !!!
    - možné trojské koně, viry

Mobilní komunikace

- GSM/3G/LTE
  - není „zdarma“
    - hovor, zprávy (SMS), obrázky (MMS)
- Riziko používání
  - odposlech
  - šifrování hovoru
    - šifrování GSM, 3G, LTE
    - fallback
      - 3G → GSM
      - vynucení vypnutí šifrování
    - dodatečný sw pro šifrování
      - je opravdu kvalitní ?
- Velká obliba IM
  - okamžitá odezva
  - „zdarma“
    - hovor, zprávy, obrázky, soubory
- Nejužívanější IM
  - Skype, WhatsApp, Viber
- Rizika používání IM?
  - P2P sítě
  - neprůhledná topologie
  - nestandardní komunikační protokol

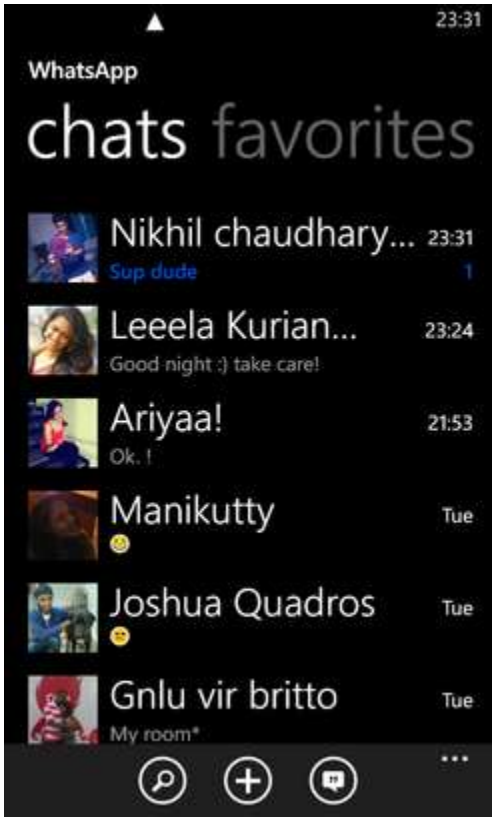
SKYPE



- Neveřejná architektura
  - ? protokoly ? šifrování ?
- Peer-to-peer síť umožňuje
  - (video)hovor
  - přenos souborů a zpráv
- Dříve
  - parazit na PC uživatele
  - node, supernode
- Nyní
    - po převzetí Microsoftem
      - žádná změna

WhatsApp

- nezávislost na platformě
  - Android, iOS, BlackBerry, WinPhone, Symbian …
- 2009 WhatsApp
  - ➔ Facebook
- ID = telefonní číslo
- upload a akualizace telefonního seznamu
- vyhledávání „přátel"
  - kontakty vašich kontaktů



Viber

http://s3.amazonaws.com/staticphotos/eac09a37d51979ccf13e3d9e595ec98520fed44e6f83ac10cf5d8cf628f7f470.jpg

- nezávislost na platformě
  - Android, iOS, BlackBerry, WinPhone, Symbian, Bada …
  - Win, Mac, Linux
- hlavní tahák pro lidi
  - sdílení: textové zprávy, obrázky, čmáranice, GPS pozice, videa
- ID = telefonní číslo
- upload telefonního seznamu
  - cloud Amazon AWS
- vyhledávání „přátel"
  - kontakty vašich kontaktů
- úplná a **skrytá** integrace do systému telefonu
- až do 04/2014 **bez šifrování** dat posílaných do cloudu
  - obrázky, videa

Internet, dobrý sluha zlý pán

SecurityFest 2016, útržky z přednášky

- CZ.NIC
  - správce domény .cz.
  - provozuje
    - národní CSIRT (*Computer Security Incident Response Team*)
    - internet-hotline.cz

- http://internet-hotline.cz
  - Kontaktní centrum pro příjem hlášení týkajícího se nezákonného obsahu na Internetu
    - především dětské pornografie a kyberšikany páchané na dětech
  - Hlavní úkol
    - nezákonný obsah odstranit
    - Spolupráce s PČR

Rodiče, děti a Internet

- Starost rodiče :
  - co z Internetu stahuje jejich syn
  - co na Internet nahrává jejich dcera

- Potomci se mohou obávat toho, co na Internet nahrávají rodiče.
- Rodiče si často pořizují vzpomínky na letní dovádění a ukládají je na různé sociální sítě, či weby určené ke sdílení fotografii

- Vše co se na internet vloží si žije vlastním životem
- Zneužitelnost fotografií, či informací je velice jednoduchá
- Nikdo z rodičů si nepřeje, aby se nad fotkou jejich dítěte rozplýval někdo cizí, někdo jehož úmysly nejsou čisté

Hlášení → odstranění obsahu

- Případ malého chlapce – fotografie vyhledatelná při zadání slova **červenec** do vyhledávače google a kliknutí na obrázky.

- Fotografie vedla na jeden z největších český webů určený ke sdílení fotografií.
- Fotografie byla nahlášena adminům serveru a ti ji ihned odstranili.
- Tím se rozjelo pátrání …

Zobrazení, oblíbenci, fanoušci

- Po chvilce strávené na tomto webu si nejde nevšimnout určitých zvláštností
- Tisíce zobrazení různých alb a uživatelů
- Většinou s názvem:
  - vana
  - koupání
  - bazén
  - pláž
  - dovolená
  - …
- Zařazených v kategorii:
  - děti
  - rodina
  - cestování ...

oblíbená fotka – 126 zobrazení

Soudnost rodičů

20 000 zobrazení

18 000 zobrazení

- U všech alb jsou komentáře
  - „mmmm“, „cute photos“, …
- Komentáře jsou veřejné a zakladatel je vidí.
- Přesto je neodstraní.

17 000 zobrazení

Práva dětí a povinnosti rodičů

- Povinností rodiče je zajištění morálního a hmotného prospěchu dítěte, přičemž rodiče mají při výkonu své rodičovské odpovědnosti mj. dítě chránit, pečovat o jeho zdraví, citový, rozumový a mravní vývoj.
- A brát přitom v potaz, že i dítě je člověk, i když malý, a vztahují se na něj práva na ochranu soukromí.
- Fotka člověka může být rozšiřována pouze s jeho svolením, ovšem za děti dávají tato svolení rodiče.
- A takové svolení by mělo být v souladu se zájmy dítěte.

Děkuji za pozornost, diskuse