# Úvod do informačnej bezpečnosti

Letný semester 2015/2016

Michal Rjaško

Slajdy: doc. Daniel Olejár

# Organizačné otázky

- Cieľ kurzu: dať základný prehľad o informačnej bezpečnosti (IB)
- Nestačí na prípravu špecialistov v IB
- Pre podrobnejší prehľad problematiky máme špeciálne prednášky
  - kryptológia,
  - kódovanie,
  - bezpečnosť IT infraštruktúry,
  - IB je aj súčasťou všeobecnejších prednášok (OS, databázy, siete)
- Informačné zdroje:
  - až nadbytok informácií na Internete, množstvo literatúry,
  - prekvapujúco dobrá je Wikipedia,
  - v prednáškach sú odkazy na zdroje

# Organizačné otázky

- Prednášky utorok 14:00
  - Daniel Olejár (Manažment IB),
  - Michal Rjaško (Krypto),
  - Jaroslav Janáček (Bezpečnosť sietí),
  - Peter Košinár (Malware),
  - CSIRT ?
  - …
- Skúška:
  - Test – 30 otázok, aspoň 16 bodov,
    - najlepšia možná známka z testu: D (možno C)
  - Ústna časť pre tých, ktorí chcú lepšiu známku

# Študijná literatúra

- Slajdy
- CD security doc. Daniela Olejára
- Internet

- Stránka kurzu:
  http://dcs.fmph.uniba.sk/~rjasko/

# Obsah prednášky (Kurzu)

- **Čo a prečo je IB, Základné pojmy**
- IB v organizácii
  - Analýza rizík, Bezpečnostný projekt, ...
  - Systém riadenia informačnej bezpečnosti podľa ISO/IEC 27OO2
- IB a štát, resp. IB na globálnej úrovni
  - Legislatíva, normy, koncepcie
- Kryptológia
  - Šifrovacie schémy, hašovacie funkcie, autentizačné kódy, digitálne podpisy
  - Protokoly
- Elektronický podpis a PKI
- Bezpečnosť software
  - Najčastejšie zraniteľnosti a ako sa im brániť
- Bezpečnosť počítačových sietí
- Malware

# Čo je IB a prečo ju potrebujeme?

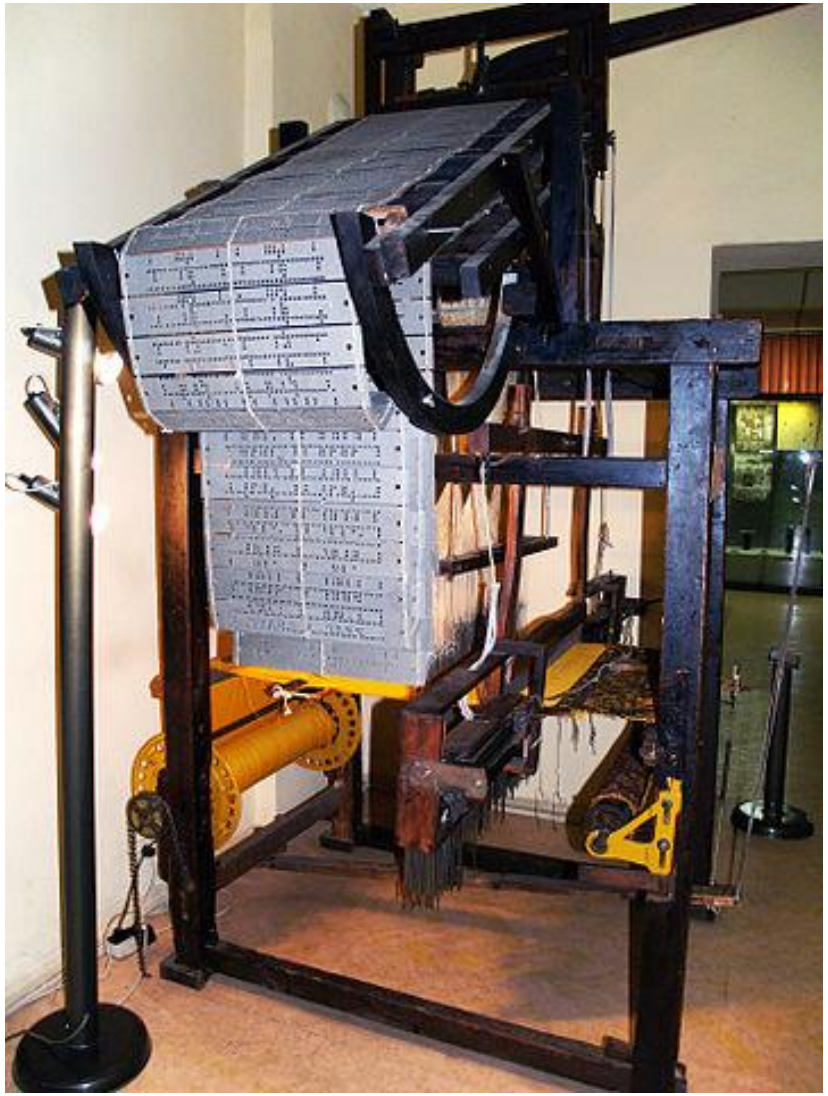
Krátky historický prehľad...

# Spracovanie informácie

## a rozvoj ľudskej spoločnosti

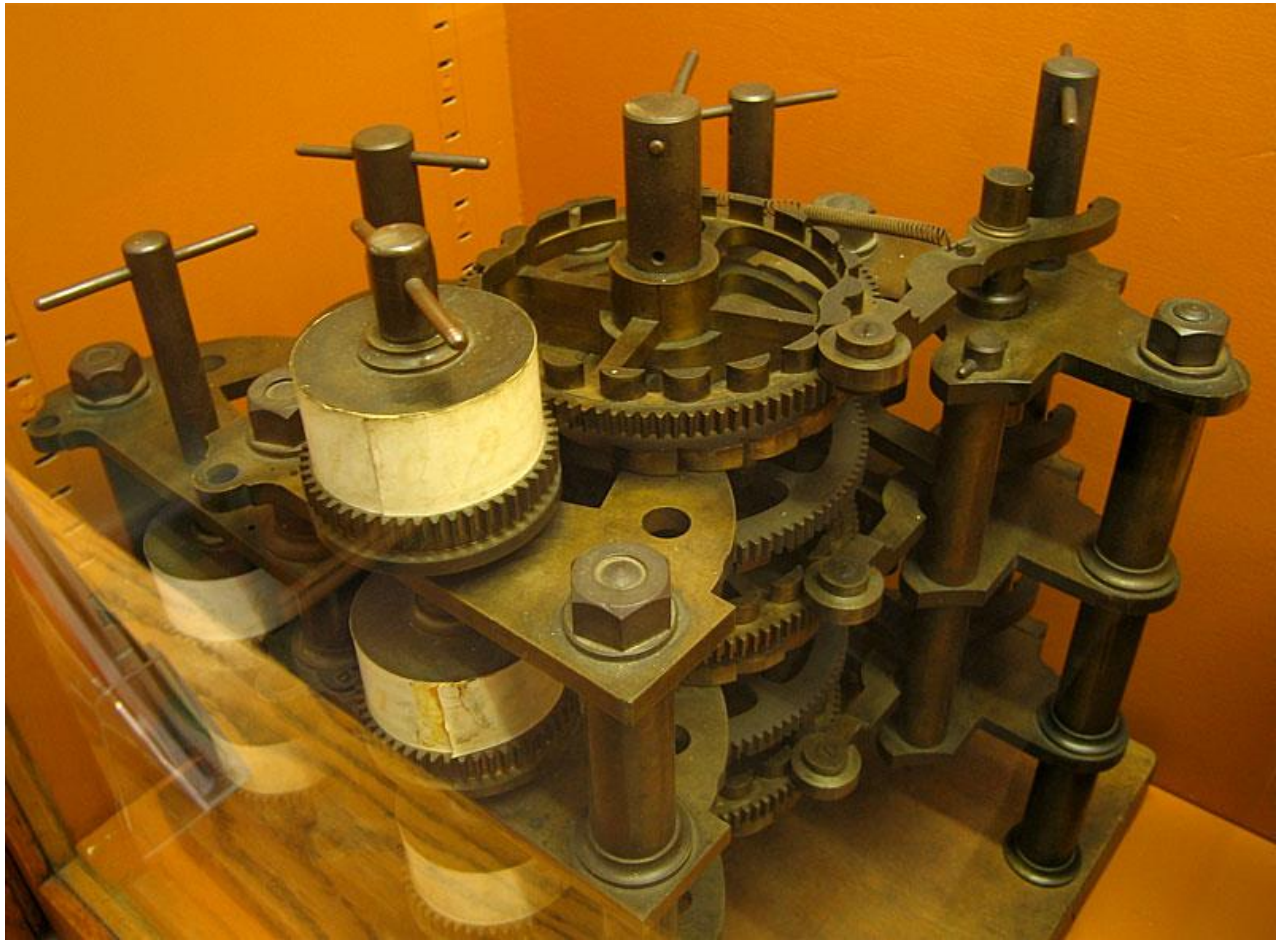
- Spoločnosť pre svoju existenciu a rozvoj potrebuje spracovávať a využívať informácie
  - v širokom zmysle (zber, prenos, vlastné spracovanie, uchovávanie, archivovanie a ničenie)
- Prostriedky na spracovanie informácií = informačné technológie
  - Klasické informačné technológie – kľúčový prvok je človek
- Rozvoj spoločnosti – zvyšovanie jej informačných potrieb
- Nestačia klasické IT, nové technológie
  - najprv komunikácia, distribúcia, uchovávanie, neskôr aj vlastné spracovanie
- Koniec 19. storočia automatizácia vlastného spracovania informácie (diernoštítkové stroje)

# Jacquardove krosná



Austrian hand-driven Jacquard loom, end of 19th century, now in the National Museum of Textile Industry, Sliven, Bulgaria

# Part of Charles Babbage's Difference Engine



Photograph © Andrew Dunn, 5 November 2004

A difference engine is an automatic mechanical calculator designed to tabulate polynomial functions.

On 14 June 1822, Charles Babbage proposed the use of such a machine in a paper to the Royal Astronomical Society, entitled "Note on the application of machinery to the computation of astronomical and mathematical tables".
This machine used the decimal number system and was powered by cranking a handle.

The British government was interested, since producing tables was time-consuming and expensive and they hoped the difference engine would make the task more economical

This is a file from the Wikimedia Commons

# Rozvoj IKT

- Klesajúca cena, rastúca výkonnosť
- Programové vybavenie umožňuje, aby ich používali laici
- Narastajúci počet aplikácií
- Mobilné zariadenia
- IKT (pôvodne nástroj) ovplyvňujú spoločnosť (kde všade by sa IKT dali použiť)
- Informatizácia spoločnosti – redesign tradičných procesov, aby sa dali využívať IKT
- Dôvod: rýchlejšie, lacnejšie, pohodlnejšie
  - súčasné informačné potreby spoločnosti sa nedajú zabezpečiť pomocou tradičných (ručných) metód spracovania informácie
- Dôsledok: spoločnosť je závislá od fungovania svojich IKT

# Prečo potrebujeme informačnú bezpečnosť?

- Spoločnosť potrebuje presné, pravdivé a dostupné informácie
  - Tie získava prostredníctvom IKT
  - Keby došlo k narušeniu IKT, nemôžeme sa z kapacitných dôvodov vrátiť k ručnému spracovaniu informácie
- IKT majú globálny charakter (dominový efekt)
- Riadia technologické systémy bežiace v reálnom čase
- IKT = kritická infraštruktúra spoločnosti
- Z existenčných dôvodov si nemôžeme dovoliť narušenie spoľahlivého fungovania IKT (sú pre nás príliš dôležité)

# Informačná bezpečnosť (IB)

- Trojaký význam pojmu IB
  - Ideálny stav IKT a/alebo informačných a komunikačných systémov organizácie (úroveň IB v organizácii)
  - Činnosť zameraná na dosiahnutie ideálneho stavu (Systém manažmentu informačnej bezpečnosti)
  - Medziodborová disciplína, ktorá skúma hrozby voči IKT a hľadá riešenia, ako IKT chrániť (štúdium, kurzy IB)
- IB nevznikla až s príchodom IKT
  - Má minimálne 4000 ročnú históriu (šifrovanie)
  - So vznikom IKT IB získava nový obsah
- Oslabenie väzby informácie/údajov na materiálny nosič
  - výhoda z hľadiska spracovania,
  - nevýhoda z hľadiska bezpečnosti

# História informačnej bezpečnosti (1)

- Samostatná kapitola informačnej bezpečnosti je kryptológia a komunikačná bezpečnosť
  - Kahn D., The Codebreakers, Scribner, New York 1996
- 2. svetová vojna (Enigma, Purple)
- Po 2. svetovej vojne rozvoj telekomunikácií (nelegálne telefonovanie)
- Počítače a elektronické IKT nová kapitola IB
  - (obdobie 1950-1975) počítačové sály najmä fyzická a režimová bezpečnosť
  - Terminály, lokálne siete, fyzická ochrana nepostačuje
  - 80-te roky – prepojenie cez modemy a telefónne linky
  - Koniec 80-tych rokov PC a Internet

# História informačnej bezpečnosti (2)

- Prvý červ (Morris 1988) http://en.wikipedia.org/wiki/Morris_worm
- Hackeri
- Vírusy a iná háveď
- Nedávna minulosť a súčasnosť
  - Elektronický obchod
  - Profesionalizácia útočníkov
  - Ekonomické motívy
  - Kriminálne živly a teroristi
  - Špionáž
  - Vojna v cyberspace

# História informačnej bezpečnosti (3)

**Aktuálne problémy (podľa BSI)**

- Poruchy systémov a infraštruktúry
- Bezpečnostné diery
- Zlomyseľný softvér
- DoS útoky
- Nevyžiadaná pošta
- Bot-nets
- Phishing a krádeže identity
- Vlastní zamestnanci, chyby a nedbalosť
- Outsourcing

**Dodávame**

- Terorizmus
- Sociálne siete
- Špionáž a sabotáže
- Štátom organizované/podporované útoky

# História informačnej bezpečnosti (4)

- Politický dosah
  - USA (podrobnejšie pri legislatíve a štandardoch)
  - EÚ – informatizácia spoločnosti (e-Europe, i-Initiative), pripravovaná Direktíva o IB
- Echelon a UKUSA
- Čo z toho vyplýva:
  - IKT = Kritická infraštruktúra spoločnosti
  - Ochrana digitálneho priestoru si vyžaduje komplexný a koordinovaný prístup
- Naviac spoločenské aspekty
  - Ochrana duševného vlastníctva
  - Ochrana súkromia
  - Právo na informácie
  - Sloboda prejavu

# The Big Brother

## Odvrátená tvár informačnej bezpečnosti

November 1999, WASHINGTON (NWS)

The U.S. Navy is supporting new speech recognition research for its potential benefits to Navy sonar. Biomedical engineers at the University of Southern California have created the world's first machine system that can recognize spoken words better than humans can. In benchmark testing, USC's speech recognition system bested all existing computer systems and outperformed the keenest human ears.

The system may eventually advance voice control of computers and other machines, help the deaf, aid air traffic controllers and others who must understand speech in noisy environments, and instantly produce clean transcripts of conversations, with each speaker correctly identified.

# The Big Brother

a ekonomika ...

- Some examples of the misuse of economic information intercepted by global networks such as ECHELON:
  - We can actually quote the contract which was spirited away from France in January 1994. It involved an arms supply contract worth 30 million francs with Saudi Arabia. The contract ended up with McDonnell-Douglas, the rival of the Airbus consortium, because the former was privy to the financial terms offered by Airbus thanks to the electronic interception system.
  - that ECHELON has been used to benefit American companies involved in arms contracts and to strengthen Washington´s hand in major negotiations with Europe in the World Trade Organisation in relation to disputes with Japan concerning the export of motor vehicle spare parts.
  - the French electronics giant, Thomson, had lost a contract worth 1.4 million dollars for the supply of a surveillance system to Brazil because the Americans had intercepted details of the negotiations and passed them on to the US Raytheon Corporation, which subsequently won the contract.

# Terorizmus

- Potenciál veľký, hrozba zatiaľ veľmi nenaplnená
- Estónsko, NIMDA
- Útok Severnej Kórei na Sony
- Aktraktívny
  - Anonymita
  - Potenciál spôsobiť veľké škody
  - Psychologický dopad
  - Príťažlivá téma pre médiá
- Cyberterrorism spája dve obavy
  - Možnosť stať sa náhodnou obeťou
  - Strach z počítačových technológií
- Médiá preháňajú (Dan Brown Digital Fortress)
- Kritické informačné systémy sú chránené (aj air gap), ale nie dostatočne Stuxnet – SCADA (2010)

# Estónsko

- V apríli 2007 chceli v Talline premiestniť sochu a hrob neznámeho vojaka
- Protesty ruskej minority
- Denial od service attack na vládne systémy, banky, noviny, telekomunikačných operátorov
- Na webe premiéra Andrusa Ansipa – zverejnený falošný ospravedlňujúci list
- Predpoklad – Rusi, sa nedokázal
- Pôvodca nebol odhalený, neskôr obvinili jediného človeka (Dmitri Galushkevich) za účasť na útoku, dostal pokutu asi 1600 USD
- http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
- Estonia has urged its allies in the European Union and NATO to take firm action against a new mode of warfare

# ACTA, TRIPS, IPR a ľudské práva

- V digitálnom priestore sa podniká
- Nedajú sa doň mechanicky preniesť pravidlá z fyzického sveta
- Vzťahy vo virtuálnom svete sa len vyvíjajú a ťažko sa regulujú
- Zločinci objavili možnosť podnikať v digitálnom priestore (krádeže identity, pirátstvo, krádeže údajov, špionáž a pod.)
- Pokusy zaviesť pravidlá na postihnutie zločincov sa stále objavujú, ale
  - sú jednostranné (preferujú záujmy držiteľov IPR – intellectual property rights)
  - zasahujú neprimerane do práv obyčajných ľudí
  - a sú neúčinné
- O ACTA, TRIPS, EU direktívach na ochranu intelektuálneho vlastníctva budeme možno hovoriť

# Mŕtva ACTA, pripravovaná CETA

**Zamietnutá 92% väčšinou v EP jún 2012**

"Whereas intellectual property is important to society and must be

protected, it should not be placed above individuals' fundamental

rights to privacy and data protection [and other rights such as

presumption of innocence, effective judicial protection and freedom of

expression]. A right balance ... should be ensured."

European Data Protection Supervisor, Peter Hustinx

(Press release of 22 February 2010, accompanying the EDPS Opinion on the then available text of ACTA.

The words in square brackets have been added; they are taken from para. 83 of the Opinion)

- ACTA vzbudila nebývalú pozornosť verejnosti aj politikov

# Cyberwars

- Potenciál už koncom 80-tych rokov
- Príprava odborníkov na útok aj obranu
- Podmorské káble
- NIMDA 2001
- Stuxnet 2010
- Obama Presidential Policy Directive 20 Október 2012
- Čo obsahujú Windows a iné masovo rozšírené programy?

# CRITIS (kritická informačná infraštruktúra)

- IKT – zasahujú všetky sektory kritickej infraštruktúry
  - Riadenie technologických systémov (SCADA)
  - Obchodovanie
  - Finančné transakcie
  - Doprava (riadenie letovej prevádzky) a spoje
  - Zdravotníctvo
  - Verejná správa
  - Armáda a bezpečnosť
- Sprostredkovane aj samé o sebe (komunikácia, informačné zdroje) IKT = kritická infraštruktúra
- Rozsiahle, rôznorodé, zložité, dôležité, obsluhujú ich často nedostatočne kvalifikovaní ľudia, pracujú s nimi laici – možnosť technickej poruchy, omylu alebo cieľavedomého útoku
- Globálny charakter – dominový efekt

# Čo chrániť?

- **Informácie –** bez nich IKT nemajú zmysel
- **Technológie** – lebo ich narušenie môže spôsobiť poškodenie alebo zneprístupnenie informácií
- **Podpornú infraštruktúru** – lebo jej narušenie môže vyradiť IKT
- **Ľudí** – lebo IKT nebude mať kto obsluhovať, resp. s nimi pracovať
- **Know-how** – lebo nekvalifikovaní ľudia nebudú vedieť správne narábať s IKT
- …

- Zdá sa, že všetko, čo súvisí so spracovaním informácií, ktoré si samé o sebe zasluhujú ochranu
  - To je však veľmi vágne konštatovanie, aby sa z neho dalo vychádzať
- Preto sa konštituuje a rozvíja informačná bezpečnosť

# Odkiaľ začať?

- Kto by mal riešiť IB:
  - Jednotlivci
  - Organizácie/inštitúcie
  - Štát
  - Medzinárodné organizácie
- Podobá sa to síce organizačným úrovniam IB, ale neznamená to, že jednotlivci sa starajú len o individuálne systémy, organizácie výlučne o svoje atď.
- Budeme vychádzať z potreby zaistenia IB v organizácii (rozumný model a najprepracovanejší)
  - Čo, prečo a ako robiť
  - Zovšeobecnenie: čo by sa malo robiť na ostatných úrovniach
  - Čo je na to potrebné

# Základné pojmy v IB

Dôvernosť, integrita, dostupnosť, ...

# Informácia a údaje

- Informácia – zapísaná v podobe údajov (údaje = forma, informácia = obsah)
- Údaje – konečné postupnosti znakov nad konečnou abecedou
- Životný cyklus informácie
  - získavanie
  - prenos
  - spracovanie informácie
  - využívanie
  - uchovávanie
  - archivácia
  - ničenie

# Čo znamená „bezpečnosť“ systému?

- „Bezpečnosť je vlastnosť systému, že sa správa tak, ako sa od neho očakáva“
  - G. Spafford a iní
- Všimnite si, že to nehovorí nič o tom, čo má / nemá systém robiť
  - To znamená, že neexistuje univerzálna definícia alebo test bezpečnosti (prečo?)
  - Ako by sa mal správať bezpečný bankomat?

- Poväčšine pod výrazom „systém sa správa ako očakávame“ myslíme dôvernosť (Confidentiality), integritu (Integrity) a dostupnosť (Availability).
  - CIA = základné bezpečnostné atribúty údajov/informácie alebo základné bezpečnostné požiadavky na ochranu údajov

# Dôvernosť (confidentiality)

- Informácia je zapísaná pomocou údajov
- Dôvernosť: zaistenie toho, aby sa k informácii obsiahnutej v údajoch nemohli dostať nepovolané osoby
- Ako:
  - Ochrana prístupu (bezpečné prenosové kanály, prístup do systému)
  - Šifrovanie
- Poznámka: dva významy pojmu: všeobecný a špeciálny (= 2. klasifikačný stupeň pre utajované skutočnosti)

# Integrita (integrity)

- Ideálne celistvosť/neporušenosť údajov (použiteľné aj pre iné aktíva)
- Reálne nedosiahnuteľná požiadavka
- Realistickejšie: aby oprávnená osoba mohla zistiť/overiť, či údaje neboli zmenené
- Ako:
  - Ochrana prístupu k údajom,
  - Ochrana fyzických zariadení pred nepovolaným prístupom (fyzická)
  - Digitálne odtlačky (hašovacie funkcie – opäť kryptológia)

# Dostupnosť (availability)

- Bez dostupnosti by informáciu nebolo treba chrániť, ale bola by nepoužiteľná
- Definícia: informácia musí byť k dispozícii kedykoľvek (do času t) o to oprávnená osoba požiada
- Použiteľné aj pre zariadenie, službu či iný zdroj systému
- Zaujímavý je čas t
  - Okamžite (t=0)
  - Prípustné je nejaké oneskorenie
- Aj štatistické chápanie dostupnosti: % času, kedy sú informácia alebo iný zdroj použiteľné pre oprávneného používateľa

# Aktívum (asset)

- Čokoľvek, čo má pre organizáciu hodnotu.
  - hmotné (zariadenia, infraštruktúra, personál)
  - nehmotné (informácie, know-how, dobré meno)
- Vyžaduje si ochranu pred zneužitím
  - Čo to znamená?
  - Že dôjde k narušeniu
    - Dôvernosti
    - Integrity
    - Dostupnosti
- vlastník aktíva (systému), zodpovedná osoba a povinná osoba

# Hrozba (threat)

- Čokoľvek, čo je potenciálne schopné priamo alebo nepriamo spôsobiť škodu na aktíve
  - Závislé na kontexte
- Dopad hrozby = negatívne dôsledky uplatnenia hrozby voči aktívu
  - poškodenie, zničenie, vyradenie z činnosti, finančné straty, nedostupnosť
- Pravdepodobnosť nastatia hrozby (pád lietadla)
- Threat model
  - Zoznam hrozieb, ktoré sú relevantné pre daný systém / prostredie
  - Hrozby potrebujeme poznať, aby sme vedeli, pred čím aktíva chrániť
  - Inak povedané, „bezpečnostné požiadavky“ na systém

# Hrozba (threat)

- Neumyselné ľudské zlyhanie / chyba je jednou (ak nie najväčšou hrozbou)
  - Zamestnanci sú najbližšie k chráneným údajom
  - Väšinou je spôsobené
    - Neskúsenosťou
    - Neznalosťou
    - Nesprávnymi predpokladmi (napr. že môžem dôverovať obsahu emailu, ak je ako odosielateľ uvedený môj šéf / administrátor)
    - Lajdáckosť, časová tieseň / stres, ...
  - Chyba zamestnanca môže spôsobiť:
    - Odhalenie utajovaných údajov
    - Vloženie chybných údajov
    - Neúmyselné zmazanie údajov
    - Uloženie údajov v nechránených zónach
    - Neschopnosť ochrániť informáciu
- Aj voči väčšine ľudských zlyhaní sa dá brániť (resp. minimalizovať ich pravdepodobnosť)

# Útočník (adversary)

= Nositeľ hrozby (záplava, prepätie, útok hackera, malware)

- Útočník je osoba snažiaca sa obísť / prekonať bezpečnostnú infraštruktúru systému
- Môže byť:
  - Zvedaný a inak zväčša neškodný (decko stiahol nejaký skript a skúša...)
  - Nie veľmi nebezpečný, snažiaci sa pochopiť systém
  - Profesionálny hacker s cieľom zarobiť
  - Veľmi sofistikovaná skupina osôb snažiaca sa zarobiť
  - Konkurencia (industriálna špionáž)
  - Štát a vládne agentúry
- Predpoklady úspešného útoku = útočný potenciál

# Zraniteľnosť (vulnerability)

- Vlastnosť, spôsob použitia alebo okolnosť umožňujúce naplnenie nejakej špecifickej hrozby
- „Chyba / nedostatok“ systému umožňujúca útočníkovi naplniť hrozbu
  - Otázka: Dá sa povedať, že zraniteľnosti sú len chyby systému?
- Bez zraniteľnosti sa hrozba nenaplní
- Čo je väčšinou zdrojom zraniteľností?
  - Zle navrhnutý / naprogramovaný software (prípadne hardware)
  - Zlý návrh systému resp. zle koncipované požiadavky na systém
  - Zlý manažment/politika/nastavenie
  - Zneužitie systému na iné účely ako bol pôvodne navrhnutý

# Útok (attack)

- Cieľavedomý pokus o využitie nejakej *zraniteľnosti* systému/aktíva za účelom získania neoprávnených privilégií, alebo poškodenia/zničenia aktíva
- Útok nastáva keď sa niekto (útočník) pokúsi zneužiť zraniteľnosť
- Druhy útokov:
  - Pasívne (napr. odpočúvanie komunikácie)
  - Aktívne (napr. hádanie hesla)
  - Denial of Service (DoS / Distributed DoS)

- Bezpečnostný incident nastane, keď je útok úspešný

# Účastník (Participant)

- Účastníci sú entity, ktoré zasahujú do systému:
  - Počítače, zariadenia, agenti, ľudia, organizácie, ...
  - Každý účastník môže mať iný pohľad
  - Bezpečnosť systému je definovaná vzhľadom na účastníkov

- Dôveryhodná tretia strana
  - Dôverujú jej všetci účastníci systému (v zmysle že dôveryhodne vykoná nejaké akcie)

# Dôvera (Trust)

- Vo všeobecnosti, ak účastník A dôveruje účastníkovi B, znamená, že A predpokladá, že sa B bude správať tak, ako A očakáva.
- Čo môžu účastníci od seba „očakávať“?
  - napr. že nebudú prezrádzať svoje tajné heslá
  - alebo budú postupovať podľa nejakého vopred definovaného protokolu
    - Čo ak to tak nebude?
- Trust model
  - Pre dané prostredie / systém popisuje, komu sa dôveruje a v čom

# Bezpečnostný model

- Kombinácia „trust“ a „threat“ modelov
  - „Bezpečnostné požiadavky“, z ktorých vychádzame pri návrhu systému
  - Veľká chyba z pohľadu bezpečnosti je žiadny alebo zlý bezpečnostný model systému
  - Je **veľmi** ťažké riešiť bezpečnosť systému keď až po jeho návrhu

- Každý návrh systému by mal mať bezpečnostný model
  - Či už LAN sieť alebo globálny informačný systém
  - Jednoduchý Java applet alebo operačný systém

# Ďalšie pojmy (1)

- Spoľahlivosť systému (Reliability) – schopnosť systému správne pracovať počas dlhého obdobia
- Schopnosť prežitia (Survivability) – schopnosť systému udržať svoju funkcionalitu aj za nejakých abnormálnych okolností
- Dôveryhodnosť (Assurance) – stupeň istoty, že systém spĺňa svoje bezpečnostné požiadavky
  - Zvyčajne je dôveryhodnosť systému meraná/určená podľa nejakej metodiky (FIPS 192, Common Criteria)

# Ďalšie pojmy (2)

- Riziko – zohľadňuje dopad aj pravdepodobnosť hrozby na aktívum = stredná hodnota dopadu
- Opatrenie – riešenie (technické, organizačné, personálne, právne, iné), ktoré znižuje riziko (pravdepodobnosť naplnenia a/alebo dopad hrozby)
- Analýza rizík – stanovenie a vyhodnotenie rizík vyplývajúcich z hrozieb relevantných vo vzťahu k aktívam organizácie
- Hranica akceptovateľného rizika – úroveň rizika, ktorú sa organizácia rozhodla znášať (napr. preto, lebo znižovanie rizika pod akceptovateľnú úroveň nie je z ekonomického hľadiska efektívne)

# Ďalšie pojmy (3)

- Bezpečnostná dokumentácia – bezpečnostný zámer, bezpečnostná politika, bezpečnostné štandardy, bezpečnostné praktiky
- Bezpečnostný projekt – komplexné posúdenie bezpečnostných potrieb/požiadaviek na systém a návrh spôsobu, ako im efektívne vyhovieť. Pozostáva z bezpečnostného zámeru, analýzy rizík a bezpečnostných smerníc / štandardnov
- Personálna, fyzická, prevádzková, komunikačná bezpečnosť
- Monitoring
- Audit
- Certifikácia a akreditácia systémov
- Oprávnenia (povolané osoby/entity)
- Identifikácia, autentizácia
- Prístup (k údajom, do systému)

# Ďalšie bezpečnostné požiadavky (1)

- Autentickosť (authenticity) – vzťahuje sa na nejaký dokument (nie surové údaje)
- Autentickosť (pôvodnosť) – dokument je taký, ako ho autor vytvoril, t.j. dva aspekty: integrita a možnosť určiť autorstvo
  - Riešenie: digitálne/elektronické podpisy
- Súkromnosť (privacy)
  - Relevantná pre údaje, dokumenty obsahujúce informáciu vzťahujúcu sa na nejakú osobu
  - Dotknutá osoba má možnosť určiť, ktoré údaje, komu a za akých okolností a komu (konkrétne osoby alebo okruh osôb) budú poskytnuté
  - Príklad: osobné údaje, zdravotná informácia
- Rozdiel medzi dôvernosťou a súkromnosťou

# Ďalšie bezpečnostné požiadavky (2)

- Nepopretie autorstva/pôvodu (non repudiation of origin)
  - Pri dokumentoch, ktoré majú právny význam
  - Ale aj predpoklad pre presadenie zodpovednosti za činnosť v systéme
  - Ako
    - Na dokumentoch elektronický/digitálny podpis
    - V systémoch identifikácia, silná autentizácia a záznamy o činnosti v systéme
- Nepopretie prijatia (non repudiation of receipt)
  - Pri doručovaní právne relevantných dokumentov
  - Podateľne, osobné schránky – potvrdenie o prijatí s časovou pečiatkou a podpisom
- Len technické riešenia nestačia

# Ďalšie bezpečnostné požiadavky (3)

- Anonymita – nemožnosť určiť pôvodcu nejakej činnosti (napr. platby)
- Pseudonymita – namiesto identity pôvodcu sa používa pseudonym, ktorý pozná len dotknutá osoba a dôveryhodná tretia strana
- Zodpovednosť za činnosť v systéme (vystopovateľnosť, accountability) – možnosť určiť, kto a čo v systéme spravil
  - Čo na to treba: identifikáciu a autentizáciu
  - Záznam auditu o činnostiach v systéme (log)
  - Podobné ako v prípade non repudiation of origin, vzťahujúceho sa na činnosť v systéme
  - Ešte: právna relevantnosť dôkazov
- Určite existujú aj ďalšie bezpečnostné požiadavky

# Na čo sa vzťahuje IB?

## Cyberspace

- Magický pojem: IB = ochrana kybernetického priestoru, cyberspace
- Cyberspace = Kybernetický priestor
  - Term originated by author William Gibson in his novel Neuromancer
  - The word Cyberspace is currently used to describe the whole range of information resources available through computer networks
- Súčasné chápanie cyberspace je technické = elektronická informačná a komunikačná infraštruktúra organizácie, štátu alebo globálna
  - Nemôže fungovať bez programového vybavenia
  - Spracovávajú sa v nej údaje (bez nich nemá zmysel)
  - Závisí od podpornej infraštruktúry
  - Obsluhujú ju ľudia
  - Riadi sa pravidlami (politika, normy, štandardy, legislatíva)
- Zlyhanie, chyba alebo úmyselné narušenie čohokoľvek z vyššie uvedeného môže viesť k narušeniu informácie

# Čo potrebujeme chrániť?

- Už pri všeobecnom pohľade dva prístupy:
  - Lokálny (konkrétny IKT systém)
  - Globálny (celý digitálny priestor)
- Dopĺňajú sa
  - Digitálny priestor tvoria konkrétne systémy a ich obsah
  - Bez ochrany lokálnych systémov sa nedá chrániť ani celok
  - Niektoré problémy sa nedajú riešiť na lokálnej úrovni
- Udržiavanie IB je veľmi ťažké
  - Každý IKT systém využíva ďalšie podsystémy (OS, Hardware, knižnice...)
  - Aj keď bezpečnosti Vášho kódu 100% dôverujete, stále je to len malá časť kódu na ktorom systém beží

  => Nutnosť neprestajne sledovať zraniteľnosti systémov

# Reporting zraniteľností

- Udržiavanie IB je veľmi ťažké
  - Našťastie ľudia spolupracujú ... na sledovaní zraniteľností

  - Specify It: Open Vulnerability Assessment Language (OVAL)
  - Name It: CVE - Common Vulnerabilities and Exposures
  - Post It: Verejne dostupné databázy CVE
    - cve.mitre.org
    - nvd.nist.gov
  - Check for It: Vo formáte čitateľnom aj pre počítače (XML)
    - Možnosť automatickej kontroly niektorých zrianiteľností
- Najčastejšie typy CVE sa potom kategorizujú do CWE
  - CWE - Common Weakness Enumeration
  - cwe.mitre.org, nvd.nist.gov/cwe.cfm

# Koncepcia informačnej bezpečnosti

- Za IB zodpovedá vedenie organizácie
- Nedá sa kúpiť
- Týka sa všetkých zamestnancov, externých spolupracovníkov a dodávateľov, čiastočne klientov
- Trvalý proces
- Naštartuje ho vedenie organizácie - bezpečnostnou politikou (politika informačnej bezpečnosti) = koncepcia informačnej bezpečnosti v organizácii
- Bezpečnostná politika: povedať každému zamestnancovi organizácie čo môže, čo nesmie, čo musí a za čo je zodpovedný
- Poverenie vhodného človeka (IT manažér, bezpečnostný manažér) zostavením pracovnej skupiny a vypracovaním bezpečnostnej politiky
- BP schvaľuje vedenie a vydáva ako vnútorný predpis

# Bezpečnostná politika

- Stanoví
  - zásady pre monitoring, kontrolu a audit informačných a komunikačných systémov organizácie
  - zásady riešenia bezpečnostných incidentov (vrátane disciplinárneho postupu pre vinníka),
  - stratégiu pre zaistenie kontinuity činnosti IKS organizácie,
  - správu bezpečnostnej politiky (ako často sa budú robiť pravidelné a z akých dôvodov mimoriadne revízie bezpečnostnej politiky).

# Bezpečnostné štandardy

- Bezpečnostná politika nerieši všetko – spravidla vysokoúrovňový dokument **(1. úroveň)**
- Podrobnosti v špecializovaných bezpečnostných politikách alebo bezpečnostných štandardoch **(2. úroveň)**
- Pravidlá na uplatňovanie bezpečnostnej politiky: bezpečnostné praktiky **(3. úroveň)**
- Pojmy Bezpečnostná politika, Bezpečnostný zámer, Bezpečnostný projekt, Bezpečnostný plán a iné sa (ani v legislatíve) nepoužívajú konzistentne

# Analýza rizík

- Bezpečnostná politika = koncepcia, potrebujeme poznať konkrétny stav
- Prostriedok: analýza rizík
- Aké riziká vyplývajú z hrozieb voči aktívam organizácie a ktoré sú také vážne, že ich treba riešiť
- Kto: externí špecialisti a vlastní pracovníci, potom vlastní pracovníci a prizvaní špecialisti
- Analýza rizík je podrobne popísaná
  - V norme ISO/IEC 27005 Information technology — Security techniques — Information security risk management
  - Nemeckom BSI štandarde 100-3 Risk Analysis on the Basis of IT-Grundschutz
  - SP-800-30 Risk Management Guide for Information Technology Systems amerického NIST-u
- Analýza rizík = základ pre správu/manažment rizík

- Viac v ďalších prednáškach

# Po analýze rizík

- Analýzu rizík robia odborní pracovníci, ale návrh na ošetrenie rizík sa týka chodu organizácie (opatrenia) – schvaľuje vedenie (v norme = akceptovanie rizík)
- Informovanie o rizikách (všetky zainteresované strany)
- Implementácia opatrení
- Monitorovanie rizík a revízie odhadu/ohodnotenia rizík (zmeny)
- Celý proces = spravovanie rizík (podstata zaistenia IB v organizácii)
- Metaúroveň: posudzovanie a vylepšovanie samotného systému spravovania rizík

# Zhrnutie

- Informačná bezpečnosť je už v tejto fáze informatizácie spoločnosti nevyhnutnosťou
- Oblasť pôsobnosti IB je veľmi široká
  - Manažment, Krypto, Siete, OS, Hardware ...
  - Našťastie existujú štandardy (ISO 27000, BSI, ...)
- IB si vyžaduje systematický prístup
  - Poznať stav
  - Navrhnúť riešenia problémov
  - Implementovať opatrenia
  - Monitorovať stav a v prípade potreby robiť korekcie
- IB je nikdy nekončiaci proces
- Detaily sú dôležité

# Zhrnutie

- Zaistenie potrebnej úrovne IB v organizácii – trvalý proces
- Opatrenia na zaistenie IB zasahujú do činnosti (procesov) organizácie
  - Potreba súčinnosti všetkých zamestnancov a tretích strán (nedá sa uplatniť uniformný prístup, lebo majú rôzne práva aj povinnosti)
  - IB nie je zadarmo (náklady na IB sa pritom ťažko zdôvodňujú)
- V malých systémoch/organizáciách sa možno dá uplatňovať ad hoc prístup (problém - riešenie), v ostatných je potrebné zaviesť nejaký systém manažmentu IB
- Rozdiel: mať v organizácii systém manažmentu IB a mať certifikovaný systém manažmentu IB v súlade s ISO 27001-2