Úvod do informačnej bezpečnosti (1)

Obsah a organizácia prednášky

Agenda

- Predmet informačnej bezpečnosti
- Cieľ, organizácia a obsah prednášky
- Informačné zdroje a skúška
- Pokračovanie – samoštúdium, ďalšie relevantné prednášky a iné formy vzdelávania

Predmet informačnej bezpečnosti

- Podrobnejšie rozoberieme za chvíľu, teraz stačí, že
- Potrebujeme zabezpečiť, aby IKT, ktoré sú kritickou infraštruktúrou spoločnosti spoľahlivo fungovali
- Úloha na minimálne troch úrovniach:
  - Globálnej
  - Organizácie
  - Jednotlivca
- Viacero špeciálnych profesií v informačnej bezpečnosti
- Ale špecialisti nestačia (IKT sú všade)
- potrebujeme, aby všetci (laici, informatici, vedúci pracovníci, politici, špecialisti na IB) vedeli, čo majú na svojej úrovni robiť na zaistenie IB

Cieľ, obsah a organizácia prednášky

- Poslucháči sú informatici, tí pri zaisťovaní IB majú dôležitú úlohu
  - Programátori: vývoj systémov s minimom bezpečnostných dier
  - Správcovia systémov: implementácia bezpečnostných opatrení, konfigurácia systémov (poriadna starostlivosť o zverený systém výrazne zvýši úroveň jeho IB)
  - Bezpečnostní manažéri na čiastočný úväzok – nie sú ľudia a informatici sú schopní si doplniť potrebné znalosti z netechnickej IB
- Cieľ: poskytnúť prehľad informačnej bezpečnosti
- Obsah:
  - Zatiaľ tri hlavné zamerania: technický, manažérsky a právny; my – technický pohľad, ale aj základy manažmentu a práva
  - prejdeme cez najdôležitejšie oblasti IB
  - CBK, EBK a ISO 27002

Cieľ, obsah a organizácia prednášky

- Viac prednášateľov, úvodné prednášky do najdôležitejších oblastí IB
  - Základné pojmy
  - manažment IB v organizácii: bezpečnostný projekt, analýza rizík, bezpečnostná politika, správa rizík
  - Štátna politika IB
  - Legislatíva a štandardy
  - Kryptológia
  - Zabezpečenie systémov (operačné systémy, siete)
  - Riešenie bezpečnostných incidentov
  - Malvér
  - Elektronický podpis a PKI
  - audit
- Veľa materiálov zväčša verejne dostupných v elektronickej forme
- Elektronická učebnica – bude k dispozícii na webovej stránke

Skúška

- 13 rokov sme organizovali skúšky ISACA
- Podobný test, len 30 otázok namiesto 200
- Väčšina – písomný test, časť – aj ústna skúška

Bloomova taxonómia

Úroveň podľa Bloomovej taxonómie 1-2 (text aj nasledujúci obrázok, Copyright © 2018 ACM CCECC)

- Before we can understand a concept we have to remember it;
- Before we can apply the concept we must understand it;
- Before we analyze it we must be able to apply it;
- Before we can evaluate its impact we must have analyzed it; and
- Before we can create, we must have remembered, understood, applied, analyzed and evaluated

Assessment Verbs by Bloom's Level

Lower Order Thinking Skills — Higher Order Thinking Skills

Remembering	Understanding	Applying	Analyzing	Evaluating	Creating
Define	Classify	Apply	Analyze	Appraise	Assemble
Duplicate	Convert	Calculate	Attribute	Argue	Construct
Find	Demonstrate	Carry out	Categorize	Assess	Create
Identify	Describe	Edit	Compare	Choose	Design
Label	Differentiate	Diagram	Contrast	Critique	Develop
List	Discuss	Execute	Decompose	Debate	Devise
Locate	Exemplify	Illustrate	Deconstruct	Defend	Formulate
Memorize	Explain	Implement	Deduce	Estimate	Hypothesize
Name	Infer	Investigate	Discriminate	Evaluate	Invent
Recall	Interpret	Manipulate	Distinguish	Judge	Make
Recogonize	Paraphrase	Modify	Examine	Justify	Plan
Retrieve	Report	Operate	Integrate	Support	
Select	Summarize	Perform	Organize	Test	
State	Translate	Produce	Outline	Value	
		Solve	Structure	Verify	
		Use			
		Write			

Pokračovanie

- Úvod do IB samozrejme nestačí na špecializáciu v IB
- Základný prehľad
- Ambícia – IB ako samostatný študijný program
- Zatiaľ špecializácia v rámci informatiky
- Manažment, právo skôr na postgraduálne štúdium (sú potrebné skúsenosti z praxe)
- Samozrejme celoživotné štúdium
- Ponúkame prednášky, semináre z
  - Kryptológie
  - Kódovania
  - Operačných systémov a sietí
  - Bezpečnosti IT
  - Manažmentu IB
  - Reverzného inžinierstva
  - Špeciálneho programovania (ESET)
  - Forenzná analýza (CSIRT)
- Projekty, bakalárske, diplomové práce, doktorandské štúdium

Pokračovanie

- Záujem o spoluprácu rastie:
- Spolupráca s CSIRT, ESET, rokujeme s MO SR a ÚV SR
- Stáže vo firmách, aj v zahraničí
- Podmienky:
  - Charakter
  - Znalosti
  - Pracovitosť
  - spoľahlivosť

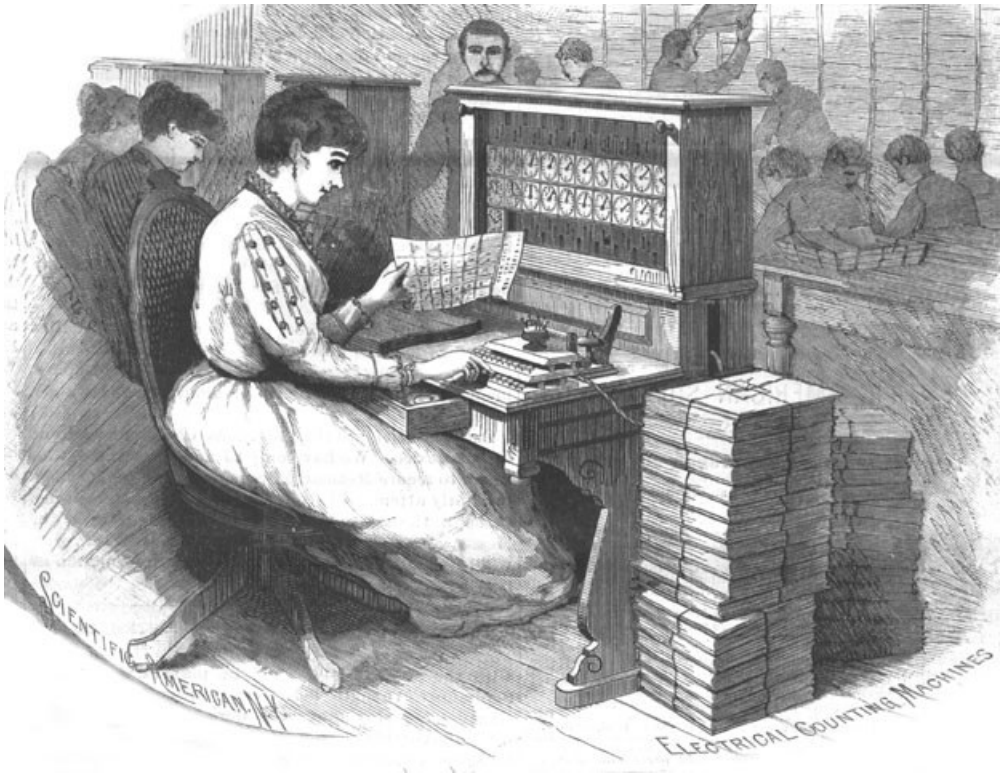
Úvod do informačnej bezpečnosti (2)

Základné pojmy

Informačné a komunikačné technológie, IKT

- Komunikácia a učenie – základ ľudskej spoločnosti
- Informačné a komunikačné technológie – nie sú vynálezom 20. storočia
- Ale 20. storočie, resp. koniec 19 storočia- nový problém: spoločnosť potrebovala na svoju existenciu viac informácií, ako stihla spracovať manuálne
- USA, census v roku 1890 – diernoštítkové stroje
- Telegraf, rozhlas, televízia
- 2. svetová vojna, počítače (riadenie protilietadlovej paľby, kryptoanalýza, vylodenie v Normandii)
- Koniec 20. storočia – syntéza: masovokomunikačné prostriedky + telekomunikačné siete + počítače = digitálne IKT

US 1890 census & Hollerithov stroj



ešte aj pár desaťročí neskôr...

Digitálne informačné a komunikačné technológie, IKT

- Oproti klasickým IKT:
  - Digitálne kódovanie informácie
  - Tie isté prenosové kanály
  - Automatizované spracovanie informácie
- Internet, web (DARPA, CERN)
- Rozvoj informačnej spoločnosti
  - Masové rozšírenie počítačov a ich prepojenie do sietí,
  - zabudované špecializované počítače do elektronických zariadení
  - Informačný obsah na Internete
  - Najrôznejšie aplikácie
  - Sociálne siete
  - Virtuálna/virtualizovaná realita
- https://en.wikipedia.org/wiki/Zettabyte

Prečo potrebujeme informačnú bezpečnosť?

- Každá organizácia má nejaký zmysel existencie (poslanie)
- Na jeho naplnenie vyvíja nejakú činnosť
- Na túto činnosť potrebuje zdroje
- Informácie sú kľúčovým zdrojom
- Aby sa dalo spracovávať potrebné množstvo informácií, používajú sa IKT
- Narušenie IKT a informácií môže organizácii spôsobiť problémy
- Bez IKT sa informácie v požadovanom množstve a čase nedajú spracovávať
- IKT a informácie potrebujeme chrániť ► dostatočná úroveň IB je nutnou podmienkou fungovania organizácie

Čo je informačná bezpečnosť (IB)?

- Často sa vyskytujúci dôležitý pojem, ale nie je poriadne definovaný a používa sa v rozličných významoch (=zdroj nedorozumení) [presne vieme, čo znamená, až kým sa nás na to niekto neopýta. sv. Augustín]
  - Želaný stav IKT (všetko funguje v súlade s požiadavkami a potrebami organizácie) [úroveň IB v organizácii]
  - Činnosť smerujúca k dosiahnutiu ideálneho stavu [Systém manažmentu informačnej bezpečnosti]
  - Medziodborová vedná disciplína zaoberajúca sa vývojom metód ochrany informácie a IKT
- Pojem IB budeme používať vo všetkých troch významoch, najmä však v druhom

Ciele informačnej bezpečnosti

- Všeobecný cieľ je jasný (mať vždy včas k dispozícii informácie, na ktoré sa môžeme spoľahnúť), ale treba ho konkretizovať, aby bolo možné na jeho dosiahnutie niečo spraviť
- Informácie sú zaznamenané v podobe údajov (údaj = **forma**, informácia = **obsah**), ak to nebude podstatné, budeme pojmy údaj a informácia chápať ako synonymá
- Informácie spracovávanie - spracovanie informácií znamená vytváranie, získavanie, prenos, uchovávanie, vlastné spracovávanie, využívanie, archivovanie, ničenie informácií
- Čo potrebujeme chrániť: informáciu od vytvorenia až po zničenie

  Konkrétne chrániť = zaistiť dôvernosť, integritu, dostupnosť údajov

Základné bezpečnostné požiadavky

- ***Dôvernosť údajov (confidentiality)*** – k informácii, ktorú údaje obsahujú nemajú prístup nepovolané osoby
- ***Integrita údajov (data integrity)*** – údaje nemôžu byť modifikované bez toho, aby si to oprávnená osoba všimla
- ***Dostupnosť údajov (data availability)*** – oprávnená osoba má údaje k dispozícii kedykoľvek, keď o to požiada
- **CIA** = základné bezpečnostné atribúty údajov/informácie alebo základné bezpečnostné požiadavky na ochranu údajov

Poznámky

- Okrem CIA existujú aj iné bezpečnostné požiadavky na ochranu údajov
- Rozdiel medzi prístupom k údajom a prístupom k ich obsahu
- Spôsob zabezpečenia dôvernosti (ochrana prístupu a šifrovanie)
- Dôvernosť – všeobecný pojem a dôverné = druhý stupeň klasifikačnej schémy utajovaných skutočností
- Integrita: absolútna požiadavka – nemennosť údajov – je nerealistická
- Zaistenie integrity – ochrana prístupu, logy a kryptografické prostriedky
- Dostupnosť – prípustné omeškanie, alebo max. % nedostupnosti

Čo chrániť?

- Informácia počas celého životného cyklu – rôzne formy, v rozličných systémoch, prístup k nej majú rozliční ľudia,
- Rôzne informácie môžu mať rôzne požiadavky na ochranu
- Miera podrobnosti pri špecifikácii informácie/údajov/systémov (väčšia podrobnosť, presnejšie požiadavky, väčšia zložitosť)
- Vnesieme do ochrany informácií systém/poriadok:
- ***Aktívum (asset)*** – čokoľvek, čo má pre organizáciu hodnotu a vyžaduje si ochranu (príklady: pracovné procesy, činnosti a služby organizácie, dobré meno, informácie, hw, sw, sieť, personál, sídlo, organizačná štruktúra,...)

Základné pojmy IB (1)

- ***Hrozba*** - objektívne existujúca možnosť, ktorej naplnenie môže poškodiť niektoré aktívum (prírodné javy, technické poruchy, chyby, omyly, ľudia)
- Hrozba má ***nositeľa*** (hrozba záplavy, nositeľ rieka, kanalizačné potrubie)
- ***Zraniteľnosť*** : chyba, nedostatok, spôsob použitia aktíva, ktoré spôsobujú, že sa hrozba voči aktívu môže uplatniť (príklad: hrozba krádeže, zraniteľnosť – umiestnenie počítača v nezabezpečenej miestnosti)

Základné pojmy IB (2)

- Existujú rozsiahle katalógy hrozieb aj zraniteľností
- Naplnenie hrozby, v širšom zmysle akákoľvek odchýlka od stanovených pravidiel, ktorá môže viesť k narušeniu bezpečnosti – ***bezpečnostný incident***
- ***Útok*** – cieľavedomý pokus o narušenie informačnej bezpečnosti
- Pôvodca útoku: ***útočník***
- ***Útočný potenciál:***
  - Motivácia
  - Znalosti
  - Príležitosť
- Príklad: krádež PC a krádež údajov z databázy organizácie

Základné pojmy IB (3)

- ***Dopad*** – negatívne dôsledky toho, že sa naplnila hrozba voči aktívu (ukradnutý počítač, prezradené heslo)
- ***Riziko*** = veličina umožňujúca merať prakticky závažnosť hrozieb: stredná hodnota dopadu hrozby (dopad x pravdepodobnosť toho, že hrozba nastane)
- Príklad: organizácia má 100 PC, pravdepodobnosť poruchy 15%, cena opravy 200 Euro, riziko poruchy je 100 x 0.15 x 200 = 3000 Euro

Základné pojmy IB (4)

- ***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)

Základné pojmy IB (5)

- ***Informačné a komunikačné technológie*** (IKT, anglicky ICT)
- ***Informačný systém*** – ucelený systém, ktorý slúži na spracovanie informácie (A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. NIST SP 800-53)
- Zaujímajú nás IS postavené na IKT
- ***Systém a jeho okolie*** (hranica systému)
- ***Bezpečnostné prostredie/okolie systému*** – všetko, čo má vplyv na bezpečnosť systému

Základné pojmy IB (6)

- *His master voice*, (Ilustračný obr. Wikimedia Commons) alebo ako zistiť, kto je kto vo virtuálnom priestore?

Vo virtuálnom priestore absentuje fyzický kontakt

Ako zistiť s kým komunikujeme?

Ale potrebujeme overovať aj autentickosť dokumentov, správ a neživých/nehmotných objektov

Základné pojmy (7)
Identifikácia a autentizácia

- Entita (osoba vec, správa, myšlienka, ...) čokoľvek, čo je totožné len so samým sebou a dá sa odlíšiť od iných objektov (entít) toho istého typu
- Atribúty entity (vlastnosti, charakteristiky)
- Identita = množina atribútov postačujúca na odlíšenie entity od iných entít toho istého typu
- Absolútna identita
- Stačí aj podmnožina absolútnej identity
- Oblasť použiteľnosti identity
- Identifikátor = špecifická identita, môže pozostávať z jediného umelého atribútu, ktorý je entite priradený a ktorý je jedinečný (rodné číslo)

Základné pojmy (8)

- Identifikácia = deklarácia identity (meno)
- Autentizácia = potvrdenie deklarovanej identity (heslo)
- Spôsoby autentizácie
  - To čo viem (heslo, PIN)
  - To čo mám (autentizačný token, napr. preukaz, pas)
  - To čo som (biometrické údaje)

Základné pojmy IB (9)

- V IB je veľa pojmov s predponou cyber-
- Nemá to logiku, lebo
- Kybernetika = veda o riadení v živých organizáciách a strojoch (Wiener, Ashby, Ampér)

- *William Gibbson Neuromancer* 1984 Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.

Základné pojmy IB (10)

- William Gibson o cyberspace

All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page.

Základné pojmy IB (11)

- V súčasnosti cyberspace označuje
  - informačnú a komunikačnú infraštruktúru
  - Sociálne vzťahy budované na základe a udržiavané prostredníctvom Internetu, sociálnych sietí a pod.
- V SR digitálny priestor donedávna
  - Národná informačná a komunikačná infraštruktúra a
  - jej okolie
- Kybernetický priestor
  - Podpriestor digitálneho priestoru, v ktorom sa spracovávajú utajované skutočnosti
- Cybercrime: kybernetický zločin
  - Trestné činy, pri ktorých sa počítače používajú ako nástroje
  - Trestné činy zamerané na IKT

Základné pojmy IB (10)

- Ďalšie pojmy zavedieme v texte
- V učebnici krátky výkladový slovník pojmov IB (250 pojmov)
- veľký výkladový slovník IB MF SR (1800 pojmov)

Legislatíva a odborná terminológia

- V poslednom čase boli prijaté tri zákony relevantné z hľadiska informačnej bezpečnosti
- Uvedieme na ukážku definície základných pojmov
- **Zákon o ochrane osobných údajov**

Osobnými údajmi sú údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje,) alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu.

Zákon o kybernetickej bezpečnosti

Na účely tohto zákona sa rozumie

a) **sieťou a informačným systémom** elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,

b) **kybernetickým priestorom** globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi týmito entitami,

c) **kontinuitou** strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,

Zákon o kybernetickej bezpečnosti

d) **dôvernosťou** záruka, že informácia nie je prezradená neoprávneným subjektom alebo procesom,

e) **dostupnosťou** záruka, že údaje alebo informácie sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je informácia potrebná a požadovaná,

f) **integritou** záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,

g) **kybernetickou bezpečnosťou** stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,

h) **rizikom** miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,

Zákon o kybernetickej bezpečnosti

i) **hrozbou** každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,

j) **kybernetickým bezpečnostným incidentom** akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je

1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
4. ohrozenie bezpečnosti informácií,

Zákon o kybernetickej bezpečnosti

k) **základnou službou** služba, ktorá je zaradená v zozname základných služieb a

1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,

2. je informačným systémom verejnej správy, alebo

3. je prvkom kritickej infraštruktúry,

l) **prevádzkovateľom základnej služby** orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k),

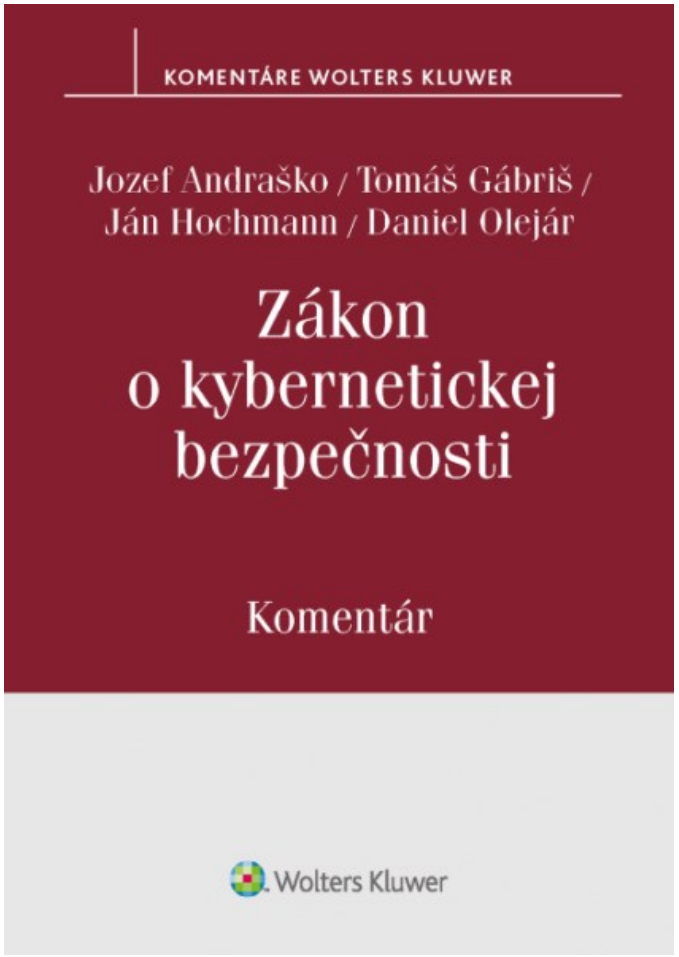
m) **digitálnou službou** služba, ktorej druh je uvedený prílohe č. 2,

n) **poskytovateľom digitálnej služby** právnická osoba alebo fyzická osoba - podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur,

o) **riešením kybernetického bezpečnostného incidentu** všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a jeho následky.

Ďalšie informácie o zákone o kybernetickej bezpečnosti

https://uniba.sk/infosec/



Zákon o IT vo verejnej správe

- Zákon č. 95/2019 Z. z.Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- §§ 18 – 23 Bezpečnosť informačných technológií verejnej správy
  - Základné ustanovenia (vymedzenie voči zákonu o KB)
  - Bezpečnosť IT VS v oblasti plánovania a organizácie
  - Bezpečnosť IT VS v oblasti obstarávania a implementácie
  - Bezpečnosť IT VS v oblasti prevádzky, servisu a podpory
  - Bezpečnosť IT VS v oblasti monitoringu a hodnotenia
  - Osobitné opatrenia na úseku bezpečnosti informačných systémov verejnej správy

Vybrané európske zákony

- Hierarchia:
  - Nariadenie
  - Smernica
  - Odporúčanie
- Nariadenie eIDAS – upravuje služby na zaistenie dôvery v digitálnom priestore
- Na Slovensku – Zákon o e-governmente
- GDPR – ochrana osobných údajov
- Zákon o ochrane osobných údajov
- COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
- Smernica NIS

Úloha štátu v IB

- Legislatíva a štandardy
- Ochrana vlastných systémov
- koordinácia ochrany celého národného virtuálneho/kybernetického priestoru
- CSIRT, varovania a pomoc pri riešení bezpečnostných incidentov
- Budovanie bezpečnostného povedomia a vzdelávanie v IB
- Medzinárodná spolupráca
- Na to potrebuje štát kompetencie a výkonné zložky

Historický vývoj IB

- Stará záležitosť (šifrovanie)
- Kryptológia, steganografia
- Špionáž, kryptoanalýza
- Povojnová konferencia v Paríži
- Enigma, Purple
- Orange Book, NSA
- DES
- Rainbow series

Záver

- Podrobnejšie v prednáške venovanej úlohe štátu v IB
- Nasledujúca prednáška – informačná bezpečnosť v organizácii
- Odporúčané čítanie (na rozšírenie všeobecného rozhľadu)
- Harrari Homo sapiens
- Andrew Hodges Turing: the Enigma