Kybernetická bezpečnost v oblasti biomedicíny

Ing. Pavel Blažek, Ph.D.

Obsah

- Vymezení pojmů
- Oblasti kybernetické bezpečnosti
- Fyzická bezpečnost
- Datové sítě a komunikace
- IS a aplikace
- Uživatelé
- Legislativa
- Vzdělávání v oblasti kybernetické bezpečnosti

- Diskuze, příklady z praxe

Kybernetický prostor

Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.

- Vymezení hranic
- Neznamená jen virt. prostředí

Kybernetická hrozba

Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.

- Vychází z vlastností subjektu
- Specifické typy útoků
- Různé vrstvy/cíle

Kybernetické hrozby

Kompromitace dat

- Výkupné (jednorázová akce – ransomware)
- Vydírání (pravidelný příjem)
- Zneužití informací
- Prodej informací třetí straně
- Konkurenční boj

Zneužití zařízení

- Kompromitace zařízení pro další útok

Poškození systémů

- Destrukce dat (smazání lékařských a logistických záznamů)
- Destrukce HW (poškození/rekonfigurace přístroje udržujícího životní funkce pacienta, komunikačního HW)
- Politické cíle

Bezpečnostní incident

- Porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie.

- Neoprávněný vstup do budovy nebo systému
- Ochromení poskytovaných služeb
- Smazání nebo odcizení dat

Kybernetická bezpečnost

Kybernetická bezpečnost představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem

- Úrovně nebezpečnosti útoků a zabezpečení

Útočníci – dle motivace

- **Black hat**
  - Typický hacker bez skrupulí, finanční motivace
- **White hat**
  - Etičtí hackeři – odhalování slabin dříve než Black hat
- **Grey hat**
  - Hacking pro zábavu, neškodí, baví se
- Blue hat
  - Nevšední agrese motivovaná vendetou
- Red hat
  - Bojovníci proti Black hat komunitě, necílí na uživatele
- Green hat
  - začátečníci sbírající zkušenosti
- *Script kiddie*
  - *působí chaos a narušují fungování služeb bez finanční motivace*

Cíle útoků

- Firmy, organizace (konkurenční, ideologický boj)
- Finanční instituce (zisk)
- Státní správa a služby (ochromení funkcí)

- Osoby
- Infrastruktura
- Služby
- Data

Rozmanitost útoků

Závislost na schopnosti útočníka a jeho cílech

Jednoduché/krátkodobé

- Krádež identity spojená s rychlou akcí – jednorázová akce
- Útok na služby - DDoS

Komplexní

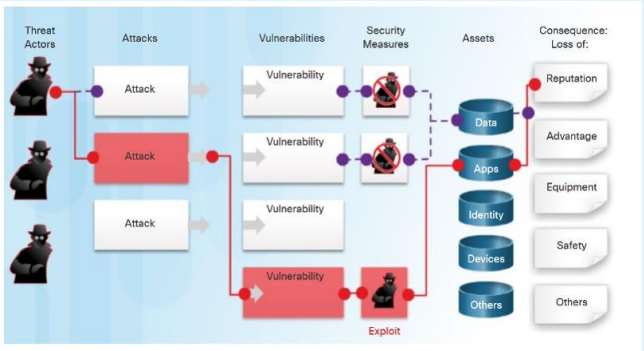
- Plánovaný
- Sofistikované nástroje a metody
- Obvykle dlouhodobý proces (měsíce)

Prostředky útoků

- Sociální inženýrství
- Infikované webové stránky
- Fyzické napojení do sítí přes nezabezpečené vstupy
- Phishing - scareware
- Trojské koně
- backdoory
- Keyloggery

Určení rizika

- Pomoci s určením rizika mohou následující otázky:
- Kdo jsou útočníci, kteří chtějí daný systém napadnout?
- Jaké slabiny může útočník v systému zneužít?
- Jaké dopady by měl úspěšný útok na systém/na organizaci?
- Jaká je pravděpodobnost, že dojde k různým útokům?
- Co může organizace udělat ke snížení rizika?



Zranitelnosti podle OWASP
(Open Web Application Security Project)

Síťové služby a zařízení

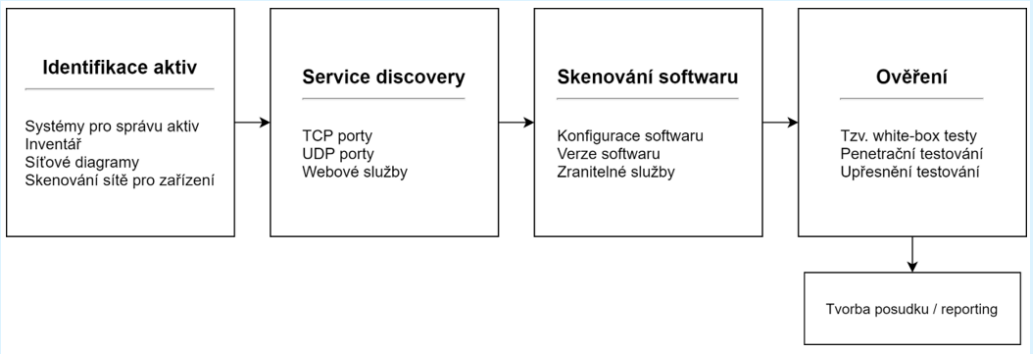
- Zveřejnění citlivých informací
- Injekce malware
- Znepřístupnění služby (DoS, DDoS)
- Nezašifrované služby
- Chybně nebo slabě implementované šifrování
- Testovací/Vývojářské služby
- Nedostatečné ověřování zatížení sítě
- Nedostatečné ověřování integrity zpráv

Síťový provoz

- Provoz v síti LAN
- Provoz ze sítě LAN do internetu
- Nestandardizované protokoly
- Bezdrátová komunikace
- Manipulace s pakety

Posouzení zranitelností

- Identifikace zranitelností, které mohou být útočníkem potenciálně zneužity
- Rutinní, pravidelný proces pro celý systém nebo jeho vybranou část



Příklady útoků

Nemocnice Benešov

- 11.12. 2019 2:50 “Dobrý večer, nejde nám aplikace“
- Vypnutí serverové infrastruktury (přechod na papírovou agendu)
- Analýza logů
- 16.12. 2019 Instalace a obnova dat (ne celých serverů – infikované zálohy) servisních serverů, provozovaných IS a koncových stanic
- Resumé k 31.12.2019 – stále není zcela hotovo

Universitätsklinikum Düsseldorf (Ransomware)

- 10. září 2020 došlo k výpadků IT infrastruktury nemocnice
- Zasaženo 30 serverů
- útok vedený přes nezáplatovanou zranitelnost softwaru Citrix Systems (objevena 17. prosince 2019, oprava v update 1/2020)
- Aktualizace proběhla krátce po vydání
- => útočníci se do nemocniční sítě pravděpodobně dostali ještě před provedením aktualizace, vrátit se do ní mohli díky infikovanému systému (Backdoor)
- Použitý nástroj pro paralýzu organizace Ransomware DoppelPaymer
- 24.9. stále není navozen normální provoz (!)
- Útočníci údajně cílili na univerzitu ne na nemocnici. Po zjištění poskytli klíč pro odšifrování a „zmizeli“.

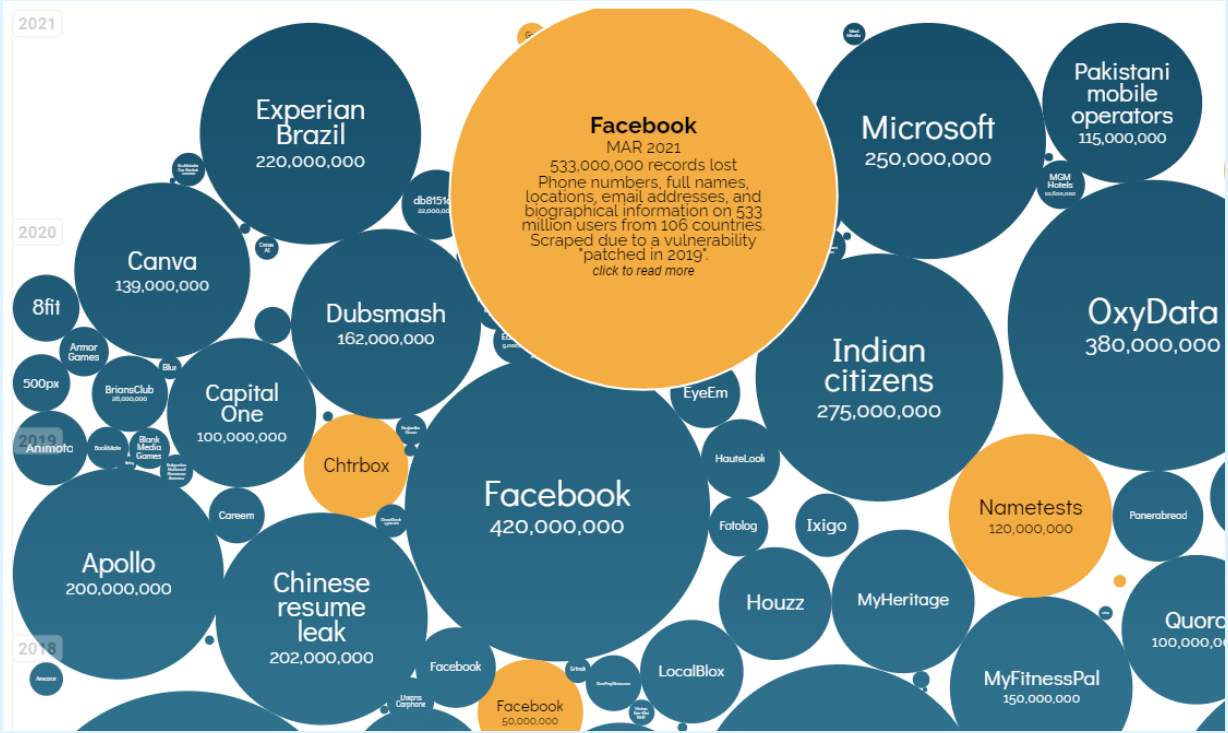
Únik dat ze PACS/DICOM

HIPPA Journal (13.7.21)

- Únik nezabezpečených dat pacientů z databáze Northeast Radiology a Alliance HealthCare
- Upozornění od bezpečnostních výzkumníků 12/2019 – bez reakce
- V březnu 2020 vydán report
- duben 2019 - leden 2020 – hackeři nasbírali 61 milionů popsaných snímků(!) 298 532 osob

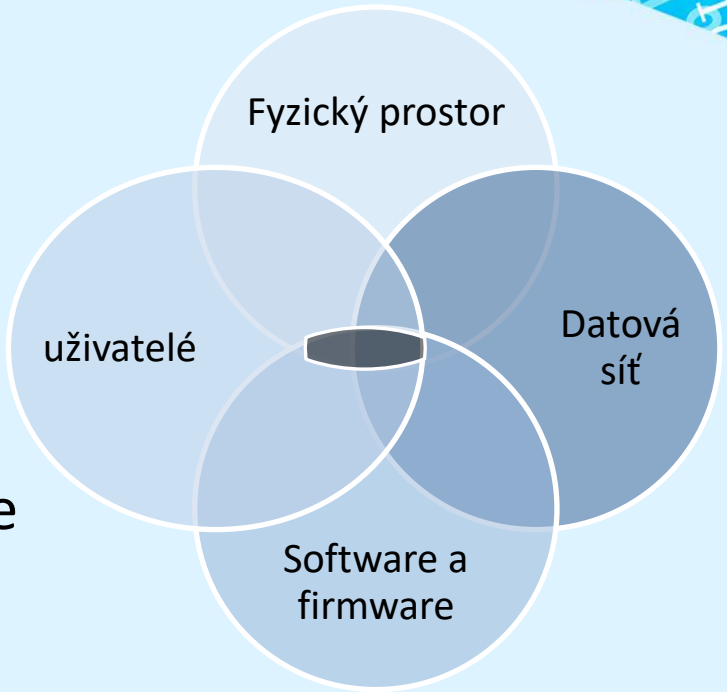
Únik dat z databází společností

(https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks)



Segmentace
cyber prostoru dle útoků

- Fyzický prostor
- Datová síť a HW
- Software a firmware
- Uživatelé



Fyzický prostor

Fyzická bezpečnost

Adekvátní zabezpečení fyzických prostor objektů

- Elektronické systémy kontroly vstupu (EKV)
- Prvky a kombinace:
  - Čipové přístupové karty - RFID
  - Biometrická identifikace – otisk prstu, otisk oční rohovky, hlas, krevní řečiště
  - Kamerové systémy – rozpoznání tváře

Kritická místa fyzického zabezpečení

Plný přístup

- Krádež PC z ordinace lékaře
  přes sádrokartonovou příčku z čekárny

- Krádež aktivního síťového prvku
  z rozvaděče na WC

Částečný přístup

- Jističe datových rozvodů a klimatizace (manag. UPS, monitoring)
- Datové zásuvky a strukturovaná kabeláž
  - Odposlech provozu
  - Modifikace provozu

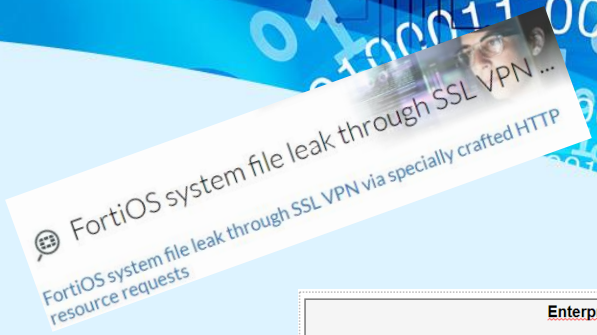
Zabezpečení datové sítě

Komunikace

- Infrastrukturní prvky
  - access level / … /backbone - zabezpečení
- Služby sítě LAN
  - DHCP, DNS,…
- Perimetr
  - NGFW, IDS/IPS, sondy…
- Hybridní prostředí a inter-konektivita
  - Pobočky / cloud, VPN, IP tunely, WIFI / BYOD
  - IoT

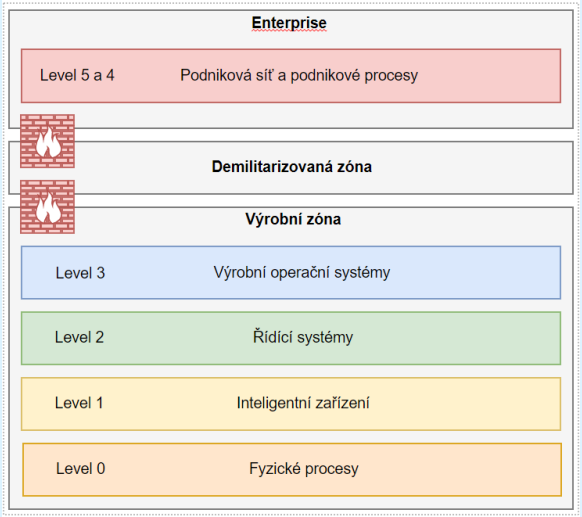
= mnoho bezpečnostních výzev

Komunikace



Doporučení

- Ochrana perimetru NGFW
- IDS/IPS
- Monitoring a logování
- Segmentace sítě
- Zabezpečené VPN
- Aktualizace firmware aktivních prvků



Útoky na HW

Všeobecně

- IP kamery (DDoS) a routery (přesměrování provozu)

(Kaspersky - mapa DDoS útoků @https://cybermap.kaspersky.com)

- Aktualizace firmware
- Podpora výrobce služby UPnP na routerech Cisco – ne, vypnout
- Hesla – výchozí a slabá
- Nejnebezpečnější vyhledávač (nezabezpečená zařízení) https://www.shodan.io/ … „nemocnice“

Medicínská zařízení

Medjack – útok vedený na zdrav. přístroje zapojené do datové sítě

- analyzátor krevních plynů
- Rentgen (PACS)

Software

Aplikace a informační systémy

- Lifecycle provozovaných aplikací
- Lokální aplikace vs cloudové služby
  - B2B
  - NIS
  - Hybridní cloudy
  - Certifikace poskytovatelů
  - Místa uložení dat (právní vymahatelnost k přístupu)
- Kryptografie (šifrování)
  - Provozu (SSL/TLS)
  - Uložených dat (provozní, zálohy, archiv)

Aplikace a informační systémy

- Komerční
  - Vím za co platím
  - Podpora aplikační
  - Vývoj a aktualizace
- Open source
  - Zdarma(?)
  - Komunitní záležitost
  - Vývoj a podpora nezávislá na provozovateli
  - Customizace
- Zákaznické
  - Custom řešení
  - Platím sám za celý životní cyklus
  - Integrace do aplikačního prostředí?
  - Testování?
  - Aktualizace?
- Zranitelnosti: https://cve.mitre.org/cve/search_cve_list.html

Uživatelé

Scénář zvědavého uživatele I

Jak zavirovat firemní síť

- Firma využívá dvě datové galvanicky oddělené sítě
  - Internet
  - Intranet
- Do schránky paní sekretářky dorazil mail s obrázkem v příloze
- Aktualizovaný antivirový program nedovolil otevření přílohy, kopírovat na výměnné medium soubor šlo.
- Antivir na PC v Intranetu je aktualizovaný se zpožděním
- Otevřením přílohy došlo během 30 minut k zavirování desítek serverů a jejich odstavení (DC, DNS, MAIL,…)
- Návrat k normálnímu provozu (reinstalace a obnovy) po 7 dnech

…

Scénář zvědavého uživatele I

Jak ztratit kontrolu nad PC

- Načtení infikované webové stránky, (odkaz v mailu, infikovaná stránka důvěryhodné organizace)
- Načtení exploitu a následné stažení škodlivého kódu z jiného serveru/webu již bez přičinění uživatele (trojský kůň)
- Otevření „Zadních vrátek“ (backdoor) následované..
  - Implementace kódu pro vzdálené ovládání = zombie v botnetu (zdroj DDoS útoků)
  - Kompromitace lokálních dat (krádež, zašifrování)
  - Finanční ztráty (kompromitace el. bankovnictví)
  - Součást těžby kryptoměn

Sociální inženýrství (stalo se v české kotlině)

Telefonát z údajného centra Microsoft, který uživatele:

- informuje o monitorování a bezpeč.problémech jeho systému a žádá o spolupráci při nápravě stavu – vzdálený přístup
- Následně žádost o přístup do mobilního telefonu

Útok:

- Pro překonání zabezpečení využitý vzdálený přístup
- Uživatel přihlášený jako administrátor
- Přepsání aktualizované knihovny integrované služby za původní, u níž byla dříve známa zranitelnost

Využití PC

- Zpracování privátních o pracovních dokumentů
- RDP přístup do firemní sítě s uloženým heslem(!)
- Bankovnictví (autorizace přes mobilní telefon)

Reakce

- Kontaktováno IT oddělení firmy – změna hesla
- Kontaktována banka
- Analýza logů a souborového systému externím systémem

Problémy uživatele

- Autentizace
  - Hesla (délka, složitost, tvorba, doporučení)
  - Vícefaktorová autentizace
  - Biometrika (omezení v podmínkách biomed.provozů)
  - Ukládání hesel do prohlížečů, xls,.. (!)
- Phishing + scareware (Uhraďte fakturu, nebo…)
- Sociální inženýrství (striktní dodržování postupů,..)
- Sociální sítě a aktivita na Internetu (digitální identita, digitální stopa)
- Kvalifikovaný elektronický podpis (čip, flash disk)
  - Datová schránka – vyšší míra důvěryhodnosti (heslo + dvoufaktorová autentizace) … jen 2% Čechů

Vyškolený uživatel osobní zodpovědnost

- Selský rozum
- Školení - směrnice
  - Dostupné funkce IS
  - Nebezpečí
  - Postupy prevence
  - Postupy odvrácení škod
  - Práva a povinnosti
- Přezkoušení (elektronické testy, ext.firmy)
- Penetrační testy (imitace phishingu)
- Motivace

Quo vadis?

Mobilní platforma

- Tablety IZS, klinická pracoviště (projekt VŠB: VIZITA)
- Mobilní telefony a mobilní klienti v nich – přístup do interních systémů, emaily… vs ztráta mobilu BEZ zabezpečení (PIN, gesto, otisk, obličej,..)
- Oddělení pracovních a soukromých prostorů
- Funkce vzdáleného uvedení do továrního nastavení
- Data na interním nosiči mobilu, tabletu či notebooku
- Ukládání hesel do prohlížečů (!)

(Mobilní) aplikace

- Odhaduje se, že až 35 % z nabízených aplikací má významné bezpečností nedostatky. **V roce 2017 například Google Play odstranil asi 700 000 aplikací, které sice předtím prošly vstupní kontrolou, ale přesto byly nějakým způsobem závadné nebo podvodné**

- **služby a aplikace, které naopak na bezpečnost dlouhodobě dbají.** Doplňky webových prohlížečů, vyhledávače, messengery, platební aplikace a další. To vše přehledně poskytuje: www.privacytools.io

- BYOD
  - firemní prostředí
  - zabezpečení

Internet of (Medical) Things

- Svět IoT, OT, IIoT, IoMT,..
- Souhrn uvedených hrozeb pro „velké“ IT ve specifické podobě
- Počet případů zneužití IoT zařízení neustále roste
- Hrozba v podobě teplotních čidel, elektronických zámků, kamer,…
- Absence zabezpečení kritických částí = velká škála různých útoků

Oblasti nasazení IoT prvků

- SMART implantovaná elektronika (kardiostimulátory)
- Wearables (TERKA), swallowable healthcare (kapsle)
- Interface pro integraci staršího technického vybavení (LIMS, OT2IoT)
- SMART skladovací skříně (LIMS)

Legislativa v oblasti kybernetické bezpečnosti

- Legislativa ČR
- Evropská legislativa
- Mezinárodní normy
- Národní a mezinárodní organizace zabývající se kybernetickou bezpečností
- Legislativa pro systémy ve zdravotnictví

Legislativa ČR

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

…

- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (zákon č. 365/2000 Sb.), přináší soubor bezpečnostních požadavků rozdělených do bezpečnostních úrovní, které musí poskytovatelé cloud computingu naplnit, aby mohli být spolu se svými nabízenými službami zapsáni v katalogu cloud computingu.
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (na základě zmocnění, zákon č. 181/2014 Sb.), kritéria pro ohodnocení významnosti informačního nebo komunikačního systému

Evropská legislativa

- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)

- Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií

Mezinárodní normy

Systém řízení bezpečnosti informací podle ČSN ISO/IEC 27001 Systémy managementu bezpečnosti informací

- Systém řízení informační bezpečnosti - **ISMS** (Information Security Management System)
  - systém stanovující základní požadavky na bezpečnost všech forem reprezentace informací podle ISO27001

- Penetrační testy a testy zranitelnosti (Monitorování, analýza, zlepšování)
- Bezpečnostní incidenty (Monitorování, analýza, zlepšování)
- Výcvik pracovníků v oblasti bezpečnosti informací (Zvyšování kvalifikace pracovníků)
- Trvalé zlepšování ISMS (Preventivní opatření)
- Interní audity ISMS (Provedení interního auditu)
- Testování záloh dat (Monitorování, Zálohování dat)
- Plány zvládání rizik (Analýza rizik)

Soubor postupů pro management bezpečnosti informací ČSN ISO/IEC 27002

- soubor nejlepších praktik z oblasti bezpečnosti.
- definuje 114 dílčích opatření rozdělených do 14 oblastí pro zvýšení bezpečnosti informací v rámci ISMS

FDA-2015-D-5105: Postmarket Management of Cybersecurity in Medical Devices (Final Guidance)

- Poskytuje doporučení pro strukturovanou a komplexní správu zranitelností kybernetické bezpečnosti postmarketových produktů prodávaných a distribuovaných zdravotnických prostředků v celém životním cyklu produktu.

FDA-2020-D-0957: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software

- Metody aplikace předpisů na proces kybernetické údržby

NUKIB

Gestor kybernetické bezpečnosti ČR

- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany

NCKO
Národní centrum kybernetické obrany

- Organizace zřízená Vojenskou zpravodajskou službou.
- Účinný systém obrany v kybernetickém prostoru tak, aby Česká republika byla schopna zastavit a případně odvrátit kybernetické útoky, a tím zabezpečit ochranu civilního obyvatelstva a infrastruktury.

Vzdělávání

- Advis Consulting s.r.o (http://www.kyberskoleni.cz/)
- Gopas a.s. (https://www.gopas.cz/)
- ALEF (https://www.alef.com/)
- KEY Trainings (https://www.skoleni.cz/)
- OK systems (https://www.okskoleni.cz/)
- CISCO (www.netacad.com)
- NUKIB (https://osveta.nukib.cz/)

…a mnoho dalších

Shrnutí

- Selský rozum
- Lidský faktor
  - Pravidelná školení a přezkoušení pracovníků
- Poddimenzování IT oddělení
  - Zabezpečení služeb
- Investice do IT
  - Služby (průběžně)
  - Technologie (životní cyklus)
- Segmentace sítí
- Aktualizace SW i firmware
- Autentizace, autorizace, accounting
- Dokumentace
  - Sítě
  - Služby
  - Logování
  - papírová podoba kritických informací
- Zálohování a archivace
- Disaster recovery
  - Plány
  - Testy
- Penetrační testy
  - Infrastruktury
  - Pracovníků

Dotazy…?