FAKULTNÍ NEMOCNICE BRNO

Digitalizace a kybernetická bezpečnost ve zdravotnictví

Prezentuje:

Ing. Tomáš Iránek, MBA

Náměstek pro informatiku FN Brno

Datum: 9. 12. 2024

Kybernetická bezpečnost ve zdravotnictví

Nemocnice čelí kybernetickým útokům. Zastaralé systémy je nedokážou chránit

Reklama

13. listopadu 2023

Kyberútoky mohou i zabíjet. Za úspěchy hackerů bývají velké ego či neznalost

9. října 2024 12:21

Pacient kvůli vyšetření nebo léčbě přišel do nemocnice na radioterapii, jenže dostal mnohonásobně vyšší [illegible] nebo dokonce smrt. Lékař přitom udělal v[illegible] ečnost, která se stala, když byl v 80. l[illegible] dioterapii Therac-25.

Root.cz » Bezpečnost » Zranitelné infuzní pumpy firmy B. Braun umožňovaly skrytě předávkovat pacienta

Zranitelné infuzní pumpy firmy B. Braun umožňovaly skrytě [illegible]

PŘIDEJTE NÁZOR

ZDRAVOTNICTVÍ

AKTUÁLNÍ INFORMACE ZE ZDRAVOTNICTVÍ A SOCIÁLNÍ PÉČE

ZPRÁVY INTERVIEW REPORTÁŽE ZDRAVÍ

Hrozba. Přibývá kybernetick[illegible] útoků na nemocnice

Redakce · 11. 1. 2021 · Zprávy

Brněnská nemocnice čelí kybernetickému útoku, neoperuje a převáží pacienty

aktualizováno 13. března 2020

Fakultní nemocnice v Brně Bohunicích, která prověřuje testy na koronavirus, čelí kybernetickému...

FAKULTNÍ NEMOCNICE BRNO

Co je kyberne

Kybernetická bezpečnost je sou ochraně počítačových systémů, sítí, dat a uživatelů před neopr nebo krádeží. Cílem je zajištění **důvěrnosti** (**C**onfidentiality), **in** tálním prostředí.

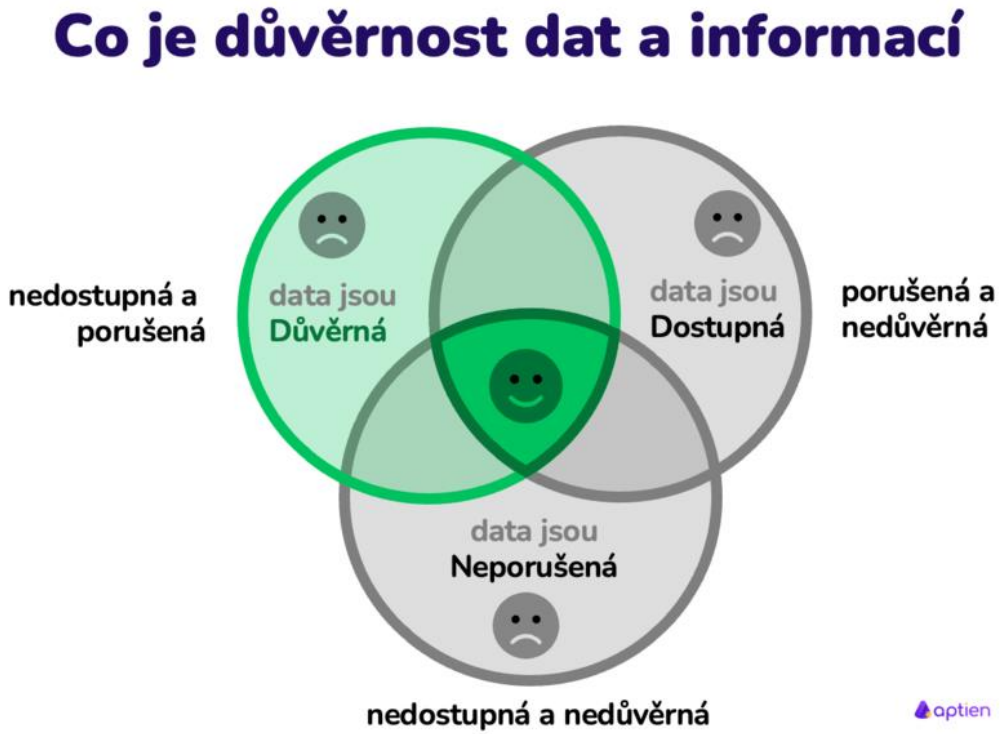
Hlavní oblasti kyb

- **Ochrana dat -** Zajištění, aby osobám.
- **Ochrana infrastruktury -** Za útoky nebo pokusy o průnik do sy
- **Prevence před malwarem -** sou viry, trojské koně nebo ransomw
- **Bezpečnost aplikací** - Zame
- **Bezpečnostní audity a správ** k jakým datům a systémům.
- **Školení uživatelů** , jak rozpoznat hrozby

FAKULTNÍ NEMOCNICE BRNO

Klíčové prvky KB - CIA triáda

CIA triáda je základní model kybernetické bezpečnosti, který slouží k ochraně informací. Zkratka **CIA** v tomto kontextu znamená **Confidentiality (důvěrnost), Integrity (integrita) a Availability (dostupnost)**. Tyto tři prvky představují klíčové cíle bezpečnosti dat, které jsou nezbytné k zajištění ochrany informací před hrozbami.



FAKULTNÍ NEMOCNICE BRNO

Důvěrnost (Confidentiality)

Důvěrnost znamená ochranu citlivých zdravotních informací před neoprávněným přístupem.

Příklady:

- **Šifrování zdravotních záznamů**: Elektronické zdravotr
  šifrovány, aby byly chráněny před neoprávněným čter
- **Kontrola přístupu**: Pouze autorizovaní zdravotníci, jak
  k citlivým údajům o pacientech. Například systém ner
  pacientů jen zaměstnancům, kteří mají platný důvod
- **Ochrana osobních údajů**: Data o zdravotním stavu, di
  sdílena s neoprávněnými osobami ani veřejností bez s
  nařízení GDPR v Evropě).

Úroveň		Popis
1	Nízká	Aktiva **jsou veřejně přístupná** nebo byla určena ke zveřejnění (např. na základě zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy FN Brno.
2	Střední	Aktiva **nejsou veřejně přístupná** a tvoří know-how FN Brno, či je nutné je chránit z pohledu zajištění bezpečností informací FN Brno. Ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.
3	Vysoká	Aktiva **nejsou veřejně přístupná** a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 110/2019 Sb., o zpracování osobních údajů, Nařízení evropského parlamentu a rady (EU) 2016/679 (GDPR) s výjimkou zvláštní kategorie osobních údajů).
4	Kritická	Aktiva **nejsou veřejně přístupná** a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. zvláštní kategorie osobních údajů, data chráněná podle zvláštních předpisů vztahujících se k ochraně utajovaných informací apod.).

FAKULTNÍ NEMOCNICE BRNO

Integrita (Integrity)

Integrita zajišťuje, že data jsou přesná, úplná a nebyla neoprávněně změněna.

Příklady:

- **Ochrana před neoprávněnými úpravami**: Zdravotní systémy mají zabudované mechanismy, které zabraňují neoprávněným změnám ve zdravotních záznamech pacienta. Jakékoli změny musí být schváleny a zaznamenány, aby bylo možné sledovat, kdo změny provedl.

- **Digitální podpisy**: Použití digitálních podpisů u elektronických lékařských dokumentů a předpisů zajišťuje, že dokument nebyl pozměn zdroje.

- **Verifikace lékařských údajů**: Automatizované s pacienta (např. léky, alergie) a zabránit chybám jiným zdravotním komplikacím.

Úroveň		Popis
1	Nízká	Aktivum **nevyžaduje** ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy FN Brno.
2	Střední	Aktivum **může vyžadovat ochranu** z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů FN Brno a může se projevit méně závažnými dopady na primární aktiva.
3	Vysoká	Aktivum **vyžaduje ochranu z hlediska integrity**. Narušení integrity aktiva vede k poškození oprávněných zájmů FN Brno s podstatnými dopady na primární aktiva.
4	Kritická	Aktivum **vyžaduje ochranu z hlediska integrity**. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů FN Brno s přímými a velmi vážnými dopady na primární aktiva.

FAKULTNÍ NEMOCNICE BRNO

Dostupnost (Availability)

Dostupnost se týká toho, aby informace a systémy byly dostupné pro oprávněné uživatele, když je potřebují.

Příklady:

- **Záložní systémy a zálohování dat**: Nemocnice pravidelně zálohují všechny zdravotní záznamy, aby je bylo možné rychle obnovit v případě selhání systému nebo kybernetického útoku (např. ransomware útok).
- **Vysoce dostupné IT systémy**: Zdravotnické systém 24/7. To znamená, že například lékaři na pohotov záznamům pacientů, což je kritické při poskytován
- **Disaster Recovery Plan (Plán obnovy po katastrof** obnovení systémů po výpadcích nebo útocích, aby pacienty.

Úroveň		Popis
1	Nízká	Narušení dostupnosti aktiva **není důležité** a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2	Střední	Narušení dostupnosti aktiva **by nemělo překročit** dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů FN Brno.
3	Vysoká	Narušení dostupnosti aktiva **by nemělo překročit** dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů FN Brno. Aktiva jsou definována jako velmi důležitá.
4	Kritická	Narušení dostupnosti aktiva **není přípustné**, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů FN Brno. Tato aktiva jsou považována za kritická.

FAKULTNÍ NEMOCNICE BRNO

Zranitelnosti a hrozby

Zranitelnost je slabé místo v systému, softwaru, síťové infrastruktuře nebo organizaci, které může být zneužito k provedení útoku.

- Nezáplatovaný software, který obsahuje známé bezpečnostní chyby.
- Slabé nebo snadno prolomitelné heslo u uživatelského účtu.

Hrozba je potenciální nebezpečí nebo entita, která může využít *zranitelnost* k provedení útoku. Hrozba může být cokoli, co ohrožuje integritu, dostupnost nebo důvěrnost systému či dat.

- Hacker, který se pokouší proniknout do systému za účelem krádeže dat.
- Ransomware, který infikuje síť a šifruje data výměnou za výkupné.
- Zaměstnanec, který neoprávněně zpřístupní citlivé informace.

FAKULTNÍ NEMOCNICE BRNO

Uživatel - zranitelnost nebo hrozba

V kontextu kybernetické bezpečnosti může být **uživatel** považován za **zranitelnost** i za **hrozbu**, v závislosti na jeho chování a úmyslech:

• **Uživatel jako zranitelnost**: Když uživatel jedná nedbale nebo neinformovaně, může vytvořit slabinu, kterou útočník zneužije.

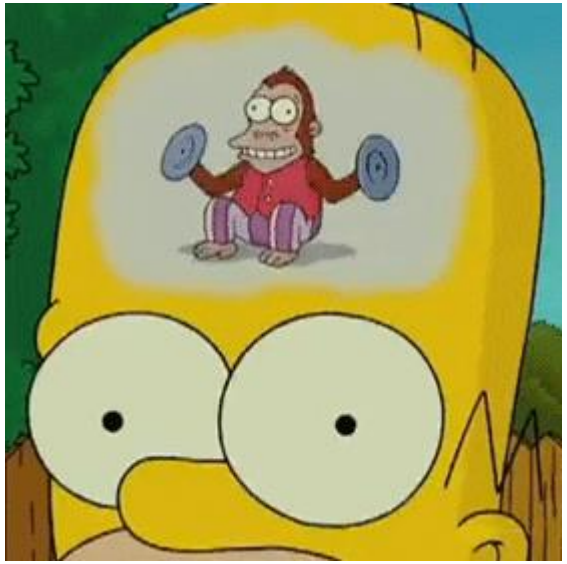
- Nevědomé sdílení citlivých informací.
- Kliknutí na škodlivé odkazy nebo stažení infikovaných souborů.
- Používání nezabezpečených sítí nebo zařízení.
- Stejná nebo snadno uhodnutelná hesla

• **Uživatel jako hrozba**: Když uživatel jedná úmyslně, aby způsobil škodu nebo ohrozil bezpečnost organizace, stává se aktivní hrozbou.

- Úmyslné sdílení citlivých dat se třetí stranou.
- Sabotáž vnitřních systémů.
- Ignorování bezpečnostních protokolů navzdory varování.

FAKULTNÍ NEMOCNICE BRNO

Je to o lidech – BFU a školení KB



Uživatel se školí kybernetickou bezpečnost

Uživatel používá poznatky ze školení v praxi

Výsledek uživatelova snažení

FAKULTNÍ NEMOCNICE BRNO

Má to smysl ?

<u>IT nikdy nic nedělá</u> – když všechno funguje, IT nic nedělá (funguje to samo) a když to nefunguje, IT zase nic nedělá (proto to nefunguje).

Výsledky testovacích phishingových kampaní ve FN Ostrava

	2020		2021	
Odesláno	1003		1489	
Reakce	357	36%	299	20%
Kompromitace	279	**28%**	203	**14%**

FAKULTNÍ NEMOCNICE BRNO

Ale co to stojí ?

FN Brno od roku 2021 investovala v přímých výdajích na kyberbezpečnost více než 600 mil Kč, z toho cca 400 mil Kč bylo z dotačních titulů

Platíme řádově stovky tisíc Kč měsíčně za služby související s KB (SOC, poradenské služby, analytické služby, testování…)

S novými regulacemi přicházejí nové náklady

Další dotace zatím nejsou

FAKULTNÍ NEMOCNICE BRNO

Něco praktického na závěr

Nejčastější techniky hackerů

- **Útok hrubou silou (Brute Force)**
  - Hacker systematicky zkouší všechny možné kombinace znaků, dokud nenajde správné heslo.
- **Slovníkový útok (Dictionary Attack)**
  - Hacker používá seznam běžně používaných hesel nebo slov (např. „123456“, „password“, „qwerty“).
- **Útok přes sociální inženýrství**
  - Hacker manipuluje uživatele k prozrazení hesla (např. podvodné e-maily, telefonáty, phishingové stránky).
- **Phishing**
  - Hacker vytváří falešnou stránku (např. kopii webové přihlašovací stránky) a přiměje uživatele zadat své přihlašovací údaje.
- **Úniky databází hesel (Útok prostřednictvím opakovaného použití hesla)**
  - Hacker získá přístup k databázím, kde jsou uložena uživatelská hesla (často hashovaná).

Nejčastější techniky hackerů

- **Malware a keyloggery**
  - Hacker nainstaluje na zařízení uživatele škodlivý software, který zaznamenává stisky kláves nebo krade přihlašovací údaje.
- **Man-in-the-Middle (MitM) útoky**
  - Hacker zachytává komunikaci mezi uživatelem a serverem a získává hesla přenášená nešifrovaně.
- **Útoky na zranitelnosti systému**
  - Hackeři využívají chyb nebo zranitelností v systému, které jim umožní obejít autentizaci a získat hesla.

Nejlepší obranou proti většině těchto útoků je **kombinace**:

- **Silných hesel** (dlouhá, složitá, unikátní).
- **Vícefaktorové autentizace** (MFA).
- **Pravidelné změny hesel** u citlivých účtů.
- **Bezpečnostního povědomí** uživatelů.

FAKULTNÍ NEMOCNICE BRNO

Víte jak bezpečné je Vaše heslo?

Studie ukázaly, že 4 % lidí v České republice využívají níže zmíněná hesla:

12345	000000	159753	password	asdfgh	internet	ahojky	nevim
123456	11111	aaaaaa	qwerty	heslo	genius	slunicko	killer
12345678	111111	hesloheslo	qwert	martin	matrix	tomas	lopata
123456789	666666	heslo123	asdasd	michal	hovno	tunning	nasrat
jahoda	lucinka	sparta	monika	lukasek	pavel		

...Je zde i to Vaše?

FAKULTNÍ NEMOCNICE BRNO

Jak snadno lze heslo prolomit

Průměrná doba prolomení při použití útoku hrubou silou, pokud útočník zkouší **1 miliardu hesel za sekundu**

Znaková sada
Pouze čísla (PIN)
Pouze malá písmena
Malá a velká písmena
Písmena a čísla
Rozšířená sada znaků

FAKULTNÍ NEMOCNICE BRNO

Jak vypadá bezpečné heslo?

- Minimální délku hesla zvolte 8 znaků a čísel (********) – čím více, tím lépe
- Heslo změňte (***minimálně*** jednou za 12 měsíců a vždy pokud máte podezření, že došlo k jeho prozrazení).
- Nepoužívejte celé srozumitelné slovo („heslo“).
- **Nikomu** jej **nesdělujte** (ani pracovníkům IT ani nadřízenému).

- Nepoužívejte stejné heslo pro vaše pracovní a soukromé účty.
  - Využijte oblíbené věty nebo hlášky a použijte první písmena

    „Hliník se odstěhoval do Humpolce“ → **HliseodsdoHum**
  - Použijte svoji oblíbenou větu a trochu ji upravte

    „Šla Nanynka do zelí“ → **SlaNanynkaDoZel1.**

FAKULTNÍ NEMOCNICE BRNO

Kontaktní údaje

iranek.tomas@fnbrno.cz

532 232 844