Ako sa zabezpečiť ambulanciu pre kybernetickým útokom?

DÔVERA
ZDRAVOTNÁ POISŤOVŇA

Vyhlásenie o konflikte záujmov autora

☒ **Nemám potenciálny konflikt záujmov**

☐ Deklarujem nasledujúci konflikt záujmov

Forma finančného prepojenia	Spoločnosť
Participácia na klinických štúdiách/firemnom grante	
Nepeňažné plnenie (v zmysle zákona)	
Prednášajúci	
Akcionár	
Konzultant/odborný poradca	
Ostatné príjmy (špecifikovať)	

Informácia o podpore

Prednáška bola vytvorená v podmienkach ***spoločnosti Dôvera zdravotná poisťovňa.***

Čo je to kybernetický priestor?

Existuje niekto v našom okolí, ktorého by neovplyvňovali informačné – digitálne technológie? **Existuje nedigitálny človek?**

Na Slovensku používa internet cez 90% obyvateľstva (2022).

Každého koho sa týkajú informačné technológie tak sa aj týka kybernetický (virtuálny) priestor a jeho ochrana – hovoríme teda o kybernetickej ochrane.

S kybernetickým priestorom sú spojené aj IT nástroje, ktoré nám umožňujú zaznamenávať dáta, komunikovať a ktoré si zaslúžia našu pozornosť.

Najradšej využívame e-mailovú komunikáciu.

- Počas pandémie si veľa z nás musela zvyknúť na nový štýl komunikácie, ktorý prebiehal v prevažnej miere virtuálnymi kanálmi. Po uvoľnení proti pandemických opatrení virtuálne aktivity síce poklesli, niektoré však ostali v obľúbenosti aj naďalej.

Email je pre útočníkov top!

Kde máme zamerať našu pozornosť?

Viete čo je to **phishing, vishing, smishing, smurfing či rooting**? A mali by ste to vôbec viedieť?

Máme vôbec šancu držať krok so stále pribúdajúcimi kybernetickými hrozbami a technikami s ktorými prichádzajú útočníci (heckeri)?

Nemáme na to čas, záujem o štúdium predmetnej problematiky je minimálny. Fakt je ten, že školstvo v oblasti vzdelávania a ani štát nie je adekvátne pripravený na mohutný rozvoj **kybernetickej kriminality.**

Ak sú útočníci úspešný tak je škoda obrovská. Platí to aj pre náš sektor, kde nehovoríme len o hodnote výkupného ale aj o mo**žných fatálnych dopadoch.**

Ochrana vášho podnikania pred kybernetickými hrozbami: definujte si **“korunovačné klenoty – informačné aktíva”**

Ako prebieha kybernetický útok v ambulancii?

- **Kybernetický útok** v ambulancii môže prebiehať rôznymi spôsobmi a môže sa líšiť v závislosti od konkrétnej situácie.
- Všeobecne platí, že **útočníci sa snažia získať prístup k dôležitým informáciám** alebo zablokovať prístup k nim pomocou ransomware.
- **Ransomware** je typ škodlivého softvéru, ktorý blokuje počítačový systém alebo šifruje dáta v ňom zapísané a potom požaduje od obete výkupné za obnovenie prístup.
- **Ransomware** môže byť šírený rôznymi spôsobmi, napríklad prostredníctvom **phishingu** alebo cez neaktualizovaný softvér či **USB.** Ak sa ransomware dostane do počítača, môže zašifrovať dáta a požadovať výkupné za ich obnovenie.

Ako zistím, že som bol napadnutý heckermi?

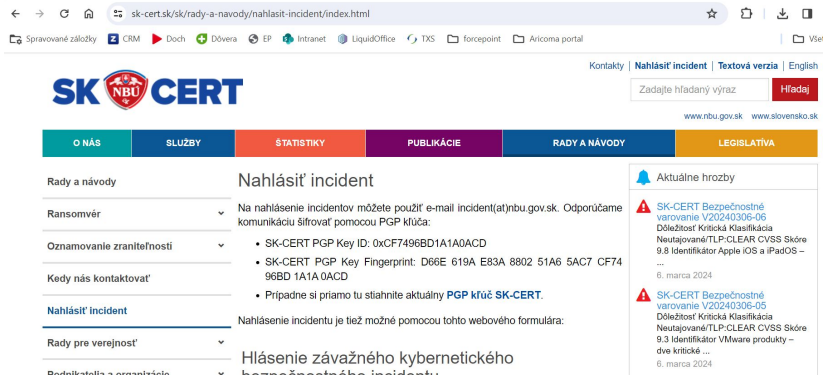
Ak máte podozrenie, že vašu ambulanciu napadli hackery, môžete sa pozrieť na niektoré z nasledujúcich príznakov:

- **Zvýšená aktivita na vašom počítači alebo sieti**
- **Zmeny v nastaveniach počítača alebo siete**
- **Neznáme programy alebo súbory na vašom počítači alebo sieti**
- **Zmeny v zálohách dát alebo ich zmazanie**
- **Zvýšená aktivita na vašom účte alebo neznáme transakcie**
- **Príde vám emailom vzorka vaších dát, ktoré už má útočník u seba a začal fázu vydierania.**

Ak máte podozrenie, že vašu ambulanciu napadli hackery, odporúčame vám kontaktovať odborníka na kybernetickú bezpečnosť.

Čo mám robiť ak som bol napadnutý heckermi? Ako sa chrániť?

- **Nepanikárte**
- **Nahlásenie incidentu:** kontaktovať odborníka na kybernetickú bezpečnosť, nahlásiť incident miestnemu policajnému oddeleniu, alebo emailom na SK CERT / Národný bezpečnostný úrad.



DÔVERA ZDRAVOTNÁ POISŤOVŇA

Phishing test / odkúpenie starého HW

Odkúpenie starého hardwaru

PO Personálne oddelenie <hr@dovera.digital>
To Katarína Galanská

Reply | Reply All | Forward

Milí zamestnanci!

radi by sme Vám oznámili, že sme sa rozhodli Vám ponúknuť možnosť odkúpiť si starý hardvér, ktorý ste používali pri svojej práci. Týka sa to zariadení ako notebooky, monitory, mobilné telefóny a dokovacie stanice.

Tento program odkupu bol zavedený, aby sme Vám umožnili získať dobrú cenu za zariadenia, ktoré už nepotrebujete. Ak ste sa rozhodli, že by ste chceli nejaké zo svojich starších zariadení odkúpiť, prosím, nájdite ich v Excel tabuľke na nasledujúcom odkaze, kde sú uvedené všetky dostupné položky.

Ak máte záujem o odkúpenie, napíšte nám e-mail na adresu personalne@dovera.sk a uveďte názov, model zariadenia SN/Harware Tag zariadenia, ktoré by ste si radi odkúpili. Potom Vám radi poskytneme ďalšie informácie a koordinujeme celý proces.

Dúfame, že tento program Vám bude prínosom a pomôže Vám získať finančné prostriedky za zariadenia, ktoré už nepoužívate.

S pozdravom,
Personálne oddelenie, Dôvera

DÔVERA ZDRAVOTNÁ POISŤOVŇA

https://dovera.digital?rid=ql3r8ts
Click or tap to follow link.

DÔVERA

Staršie zariadenia k odkúpeniu nájdete v nasledujúcom súbore:

	A	B
1	Hardware	SN/Hardware tag
2	FUJITSU CELSIUS H760	D51B003405
3		
4	Dell Latitude 5511	2H5FDJ
5		
6	~~FUJITSU CELSIUS H760~~	~~D54B004745~~
7	HP Probook 440 G8	BJTM2N2
8		
9	HP Elitebook 840 G5	AKBJYBD3
10	LCD Dell U2414H	FJTDJ52
11		
12	JP Probook 440 G8	F1SI5G2
13	LCD DELL U2419H	CC6KS2
14		
15	HP HP EliteBook 850 G6	5CG582DF7K
16		
17	FUJITSU CELSIUS H730	F1E55G2
18		
19	HP ZBook Studio G4	CND75215ZV
20	DELL Latitude 5511	5XBK6D3
21	LCD Dell U2415	BXDSVK2

Pre zobrazenie zdieľaného dokumentu odkup_harwaru_2023.xlsx kliknite na náhľad vyššie.

DÔVERA

DÔVERA ZDRAVOTNÁ POISŤOVŇA

Príklady kybernetických útokov – Vishing

Typ podvodnej aktivity, ktorá sa uskutočňuje pomocou hlasového telefonického hovoru. Podvodník sa predstavuje ako dôveryhodná osoba, ako napríklad vedúci pracovník, pracovník banky alebo iného dôležitého inštitútu a snaží sa získať cenné informácie od obete. Často sa jedná o prihlasovacie údaje, čísla kreditných kariet alebo iné citlivé informácie.

Znaky:

- Nátlak od na prvý pohľad dôveryhodnej osoby alebo nadriadeného. (Vydávanie sa za autoritu)
- Hovor zo skrytého čísla či zo zahraničia. (Napodobňovanie telefónnych čísel)
- Vzbudzovanie strachu. (Napadnutý počítač)

Ako sa brániť :

- Nikdy neposkytujte telefonicky osobné, autorizačné alebo finančné informácie neznámym osobám vydávajúcim sa za zamestnancov, dodávateľov...

Ak si myslíte, že ide o podvodný telefonát, nahláste ho telco operátorovi. Neoverujte si volajúceho na telefónnom čísle, ktoré vám uviedol, môže sa jednať o falošné číslo.

Desatoro pre kybernetickú bezpečnosť v ambulancii

1. **Zabezpečím ambulanciu a kartotéku pred neoprávneným prístupom k údajom.** A to tak, že zamedzím vstup nepovolaným osobám (bezpečnostný zámok, alarm), uzamknem kartotéku, dodržiavam pravidlo čistého stola, chránim monitor pred odpozeraním. Zachovávam dôvernosť pri poskytovaní zdravotnej starostlivosti a informácií pacientom.

2. **Používam silné heslo** (aspoň 15 znakov a špeciálne znaky napr. @, *, _) a pravidelne (aspoň raz za 3 mesiace) si heslo zmením. Nepoužívam rovnaké heslo do rôznych systémov. **Pre prihlasovanie do systémov využívam druhý faktor**, t.j. napríklad overenie prostredníctvom SMS.

3. **Heslo neprezrádzam ani s nikým nezdieľam** (ani so sestričkou a kolegami). Heslo nenechávam nalepené na klávesnici, v kalendári ani na nástenke.

4. **Pri používaní mobilu alebo tabletu** kde sa nachádzajú citlivé údaje, sa správam rovnako, akoby išlo o počítač. Platí to najmä ak poskytujem zdravotnú starostlivosť cez telefón (napr. telemedicínske úkony).

5. **Žiadosť dotknutej osoby** (prístup k osobným údajom, prenos, výmaz, oprava, námietka voči spracovaniu) vybavím najneskôr do 30 dní odo dňa doručenia. Po ukončení účelu spracovania osobné údaje zlikvidujem (zdravotná dokumentácia 20 rokov od posledného poskytnutia zdravotnej starostlivosti, všeobecný lekár 20 rokov od smrti osoby).

Desatoro pre kybernetickú bezpečnosť v ambulancii

6. So zdravotnými poisťovňami **komunikujem prednostne elektronicky**, cez ich zabezpečené portály (napr. prostredníctvom elektronickej pobočky)

7. **U svojho dodávateľa IT služieb** si preverím rozsah zabezpečenia svojho PC a iných zariadení pripojených v sieti, vrátane mobilov (najmä tzv. antivir, firewall, zálohovanie údajov) a v súčinnosti s ním zabezpečím pravidelné aktualizácie softvéru.

8. **Údaje si zálohujem** pravidelne a to na viacerých bezpečných úložiskách (tzv. cloud, šifrovaný externý harddisk – po použití vždy odpojím).

9. **Neotváram podozrivé maily.** Nesťahujem a neotváram prílohy, ktoré prišli z neznámeho zdroja. Neklikám na podozrivé odkazy v e-mailoch ani v SMS-kách. Na podozrivých internetových stránkach nezadávam svoje prihlasovacie údaje ani neplatím za tovar. Pri telefonovaní si vždy preverujem kto je na druhej strane linky (identifikujem volajúceho/volaného).

10. **Vzdelávam seba a svojich zamestnancov** aj v oblasti kybernetickej bezpečnosti a IT technológiách.

Použité zdroje:

Používanie internetu na Slovensku a vo svete - VIRTUÁLNÔ (virtualno.sk)

https://www.sk-cert.sk/sk/rady-a-navody/nahlasit-incident/index.html

https://www.techbyte.sk/2023/01/slovensky-internet-v-roku-2022-tiktok-uz-pouziva-1-milion-slovakov-najradsej-komunikujeme-cez-e-mail/

https://www.sk-cert.sk/sk/rady-a-navody/podnikatelia-a-organizacie/index.html

https://www.eset.com/sk/generator-hesiel/