Prieskum kybernetickej bezpečnosti v ambulanciách

Varga Roman - CISO – ITAPA 2024

https://www.linkedin.com/in/roman-varga-55815539/

DÔVERA ZDRAVOTNÁ POISŤOVŇA

Sektor zdravotníctva - aktuálny stav

Kybernetická bezpečnosť v ambulanciách

- Kritický sektor
- Záujem heckerov
- Údaje o zdraví
- Ambulancie
- Pacient
- Legislatíva

Prieskum kybernetickej bezpe čnosti v ambulanciách

LEKÁR, a.s. / vzdelávacie centrum SLK - DÔVERA Zdravotná poisťovna a.s. - ESET, spol. s r.o.

- Prvý celoštátny prieskum ku KB a GDPR
- Odpovedalo viac ako 400 lekárov

Top kybernetické rizika a ich konkrétne riešenia

Nedostatočné vzdelávanie v oblasti IT bezpečnosti
Až 78 % respondentov uviedlo, že sa nestretli s iným spôsobom vzdelávania v oblasti IT bezpečnosti, ako je platforma Lekarnet.

Riešenie: Zaviesť pravidelné praktické školenia. Tie sa majú zamerať na aktuálne hrozby, techniky útočníkov a efektívnu ochranu v oblasti IT bezpečnosti a ochranu osobných údajov.

Nedostatočné zálohovanie a obnova dát nás môže stáť stratu dát a ich obnovu
Až 15 % respondentov nevykonáva pravidelné zálohy svojich dát o pacientoch, len 34 % vie obnoviť prevádzku po tzv. ransomwarovom útoku.

Riešenie: Zaviesť bezpečné automatizované zálohovacie systémy a pravidelne testovať obnovu dát. Mať kľúčové dáta zálohované tak, aby ich prípadný úspešný ransomware útok nepoškodil a vedieť s nimi pracovať aj po ich obnove.

Neschopnosť identifikovať bezpečnostné incidenty a hrozby
Až 58 % respondentov nevie identifikovať bezpečnostný incident alebo zraniteľnosť, čo môže viesť k strate dát, pozmeneniu ich obsahu a znefunkčneniu prevádzky. Reálny hackersky útok, ktorý museli v ambulancii riešiť, zažili **2 % respondentov**.

Riešenie: Implementovať s pomocou overených IT špecialistov ochranu na detekciu, reakciu a monitoring kybernetických incidentov hrozieb. Samotný antivírus už nestačí.

Používanie súkromných e-mailov na pracovné účely je alarmujúce. Nevieme oddeliť pracovný a súkromný svet
Až 63 % respondentov používa svoj súkromný e-mail aj na pracovné účely. Sú to otvorené dvere pre tzv. phishingové útoky. Takéto útoky cez e-mail sú najzávažnejšou hrozbou a mieria na našu (ne)pozornosť. **Stačí jeden nesprávny klik** a útočníci môžu dáta ukradnúť a zašifrovať. Tým to len začína, končí vydieraním a nefunkčnosťou prevádzky ambulancie.
Až 27 % respondentov zdieľa pracovný e-mail (aj s heslom do tohto e-mailu) aj s inými kolegami alebo zamestnancami.

Riešenie: Zaviesť politiku používania výhradne pracovných e-mailov a implementovať dvojfaktorovú autentifikáciu. Nezdieľať s nikým svoj e-mail a ani prístupy do informačných systémov, notebookov a pod.

Prínosy pre zdravotníctvo

- Desatoro kyber bezpečnosti
- Záznamy z webinárov
- sú zverejnené na www.lekarnet.sk
- Vzdelávanie – webináre,školenia
- Výmena praktických skúsenosti

Rozšírené informácie

Kybernetická bezpečnosť v ambulanciách

V rámci vzdelávacích podujatí, realizovaných spoločnosťou LEKÁR, a.s., sme v roku 2023 a 2024 (vždy v aprílovom termíne) zaradili aj tému „Kybernetická bezpečnosť“. Záznamy z webinárov sú zverejnené na www.lekarnet.sk.

V nemocničných zariadeniach je na zabezpečenie kybernetickej bezpečnosti vždy poverený a zodpovedný konkrétny človek, resp. tím, zložený z viacerých ľudí, ktorí sa touto problematike venujú. V ambulantných zariadeniach, ktoré sú vo veľkej väčšine zložené len z lekára (ktorý je súčasne aj majiteľom zariadenia) a zdravotnej sestry, je problematika kybernetickej bezpečnosti za plecami lekára. LEKÁR, a.s., ako vzdelávacie centrum SLK, preto uvítala možnosť venovať sa aj problematike vzdelávania v kybernetickej bezpečnosti. Na túto náročnú úlohu sa podujali zodpovední pracovníci z DÔVERA zdravotnej poisťovne, a. s., a naše pozvanie zapojiť sa do projektu prijala aj spoločnosť ESET, spol. s r.o.

Okrem klasického vzdelávania formou webinára malo každé z podujatí určitý bonus.

V roku 2023 to bolo DESTATORO KYBERNETICKEJ BEZPEČNOSTI, ktoré dostali všetci účastníci webinára nasledne mailom a ktoré je zverejnené na www.lekarnet.sk pod videonahrávkou z webinára zo dňa 26. 4. 2024. K tohtoročnému vzdelávaniu vypracovali v DÔVERA zdravotnej poisťovni, a. s., Dotazník, ktorý je historicky prvým celoštátnym prieskumom v radoch lekárov ku KB a GDPR. No a my, v LEKÁR, a. s., v snahe spestrenia celého projektu a zabezpečenia vyššej účasti v prieskume, sme pripravili pre účastníkov prieskumu žrebovanie o ceny. Do pomyselného mačica okrem nami poskytnutých cien prispela cenami aj DÔVERA zdravotná poisťovňa, a. s., a spoločnosť ESET, spol. s r.o. Žrebovanie sa uskutočnilo 21. augusta 2024 v sídle LEKÁR, a.s.

Prinášame vám výsledky vyhodnotenia Dotazníka aj výsledky žrebovania.

Sme radi, že ste s nami. Sme radi, že sa zúčastňujete aj nemedicínskych vzdelávaní (CPD) k problematike, ktorá je nevyhnutná na výkon vašej súkromnej ambulantnej praxe.

Pripravila: MUDr. Zuzana Teremová, LEKÁR, a. s.

Výsledky žrebovania:
1. cena: MUDr. Milan Zemančík
2. cena: MUDr. Lenka Vanyová
3. cena: MUDr. Andrej Miškeje

Historicky prvý celoštátny prieskum

Výzvy a ich riešenia

Kybernetická bezpečnosť v zdravotníckych zariadeniach je kľúčová pre ochranu citlivých dát pacientov a chod ambulancií. Tejto téme sa dlhodobo venuje spoločnosť LEKÁR, a. s., DÔVERA zdravotná poisťovňa, a. s., a ESET, spol. s r.o.

Kybernetická bezpečnosť v zdravotníckych zariadeniach je kľúčová pre ochranu citlivých dát pacientov a chod ambulancií.

Spoločne sme pripravili cielený prieskum, ktorý sa zameral na zistenie stavu kybernetickej bezpečnosti v ambulanciách. Išlo historicky o prvý a jedinečný takýto prieskum. Ambulantných lekárov sme požiadali 28 otázok a dostali sme odpoveď od 412 respondentov. Identifikovali sme niekoľko závažných rizík a navrhli riešenia na ich zmiernenie, z ktorých dnes vyberáme tie najdôležitejšie. V skratke, téme kyber bezpečnosti venujú zdravotníci len okrajovú pozornosť a je len otázkou času, kedy budú úspešne konfrontovaní s útočníkmi. Úspešne pre útočníkov...

V Dôvere si uvedomujeme závažnosť ochrany osobných údajov a kybernetickej bezpečnosti v sektore zdravotníctva. Preto sa jej systematicky venujeme, používame naše ochranné opatrenia a inovujeme naše riešenia. Sme otvorení zdieľaniu našich skúseností a riešení aj takouto formou, či pravidelnými školeniami a konzultáciami.

Pripravili: Ing. Roman Varga, manažér kybernetickej bezpečnosti DÔVERA zdravotná poisťovňa, a.s.

V prieskume sme identifikovali tieto štyri najzávažnejšie riziká:

Nedostatočné vzdelávanie v oblasti IT bezpečnosti
Až 78 % respondentov uviedlo, že sa nestretli s iným spôsobom vzdelávania v oblasti IT bezpečnosti, ako je platforma Lekarnet.

Riešenie: Zaviesť pravidelné praktické školenia. Tie sa majú zamerať na aktuálne hrozby, techniky útočníkov a efektívnu ochranu v oblasti IT bezpečnosti a ochranu osobných údajov.

Nedostatočné zálohovanie a obnova dát nás môže stáť stratu dát a ich obnovu
Až 15 % respondentov nevykonáva pravidelné zálohy svojich dát o pacientoch, len 34 % vie obnoviť prevádzku po tzv. ransomwarovom útoku.

Riešenie: Zaviesť bezpečné automatizované zálohovacie systémy a pravidelne testovať obnovu dát. Mať kľúčové dáta zálohované tak, aby ich prípadný úspešný ransomware útok nepoškodil a vedieť s nimi pracovať aj po ich obnove.

Neschopnosť identifikovať bezpečnostné incidenty a hrozby
Až 58 % respondentov nevie identifikovať bezpečnostný incident alebo zraniteľnosť, čo môže viesť k strate dát, pozmeneniu ich obsahu a znefunkčneniu prevádzky. Reálny hackerský útok, ktorý museli v ambulancii riešiť, zažili **2 % respondentov**

Riešenie: Implementovať s pomocou overených IT špecialistov ochranu na detekciu, reakciu a monitoring kybernetických incidentov hrozieb. Samotný antivírus už nestačí.

Používanie súkromných e-mailov na pracovné účely je alarmujúce. Nevieme oddeliť pracovný a súkromný svet
Až 63 % respondentov používa svoj súkromný e-mail aj na pracovné účely. Sú to otvorené dvere pre tzv. phishingové útoky. Taketo útoky cez e-mail sú najzávažnejšou hrozbou a mierta na našu (ne)pozornosť. **Stačí jeden nesprávny klik** a útočníci môžu dáta ukradnúť a zašifrovať. Tým to len začína, končí vydieraním a nefunkčnosťou prevádzky ambulancie.
Až 27 % respondentov zdieľa pracovný e-mail (aj s hesiom do tohto e-mailu) aj s inými kolegami alebo zamestnancami.

Riešenie: Zaviesť politiku používania výhradne pracovných e-mailov a implementovať dvojfaktorovú autentifikáciu. Nezdieľať s nikým svoj e-mail a ani prístupy do informačných systémov, notebookov a pod.

Desatoro pre kybernetickú bezpe čnosť v ambulancii

https://lekarnet.sk/?online-podujatie=84&t=137

Pri dodržiavaní aspoň nevyhnutného minima uvedeného v tomto desatore môžete ochrániť seba a svoju ambulanciu pred kybernetickým útokom, stratou alebo poškodením osobných údajov (vašich vlastných, svojich zamestnancov aj pacientov), čím sa môžete vyhnúť následným nepríjemnostiam a prípadným sankciám.

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 10 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).
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. antivír, 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.

DÔVERA ZDRAVOTNÁ POISŤOVŇA