Počítačová bezpečnost

Počítačová bezpečnost je obor informatiky zabývající se zabezpečením dat v počítačích a jiných úložištích.

Je to důležitá součást péče o pacienta. Bezpečnost dat se týká spousty institucí a nejinak je tomu ve zdravotnictví. Úložiště dat v ambulancích a nemocnicích obsahují spousty citlivých údajů, které jiné instituce nemohou mít, a navíc pokrývají obrovskou část populace. Důležitá je zejména také v rámci telemedicíny (např. teledermatologie, telekardiologie, atd.)

Důvěryhodnost, integrita a dostupnost dat

Bezpečnost dat ve zdravotnictví je nutné zajistit hned v několika ohledech.

Jednak by mělo být zaručeno **soukromí pacienta**, stejně jako ve fyzické podobě, ani v té počítačové by se k datům pacienta neměla dostat žádná nepovolaná osoba (tedy ani číst, ani měnit, ani zapisovat). Měla by tedy být zajištěna **důvěryhodnost**.

S daty by také neměl nikdo manipulovat a měnit je, tzn. je nutné zabezpečit **integritu dat**. Pokud útočník pozmění laboratorní výsledky, informace o alergiích nebo třeba krevní skupinu pacienta, může to mít dalekosáhlé následky.

Dostupnost dat je klíčová pro poskytování bezpečné zdravotní péče. Pokud nastane výpadek informačních systémů a zdravotnický personál se k uloženým datům nedostane, může to způsobit problémy v celém řetězci péče – a to od recepce přes laboratorní výsledky, dokumentaci pacienta, plánování operací atd.

Útoky na data ve zdravotnictví

Zatímco papírová dokumentace je chráněna fyzicky (zámky, omezený přístup do archivu), elektronická dokumentace musí být chráněna i elektronicky (tj. lze ji zcizit na dálku). Elektronická dokumentace je tak v podstatě zranitelnější, protože k papírové kartotéce se útočník musí dopravit až na místo, což jej geograficky omezuje. Útok na elektronickou dokumentaci lze teoreticky spáchat na libovolnou dálku přes síť.

Rychlý technologický pokrok v medicíně i ve zdravotnické technice a IT způsobil, že se přístroje staly mnohem komplikovanější, získaly vlastní procesory a úložiště dat a napojily se do počítačových sítí ambulancí a nemocnic. Bezpečnost těchto zařízení však dlouho zůstávala poněkud stranou zájmu a vývoj zabezpečení nebyl zdaleka tak překotný. Technologie používané ve zdravotnictví bývají nastavené pokud možno co nejjednodušeji a jednotně, aby umožnily snadnou správu. Například administrátorské účty a hesla k zdravotnickým přístrojům (rentgeny, CT, infuzní pumpy, dávkovače, anesteziologické přístroje, apod.) bývaly mnohdy nastaveny ve firmware „natvrdo“, aby umožnily okamžitý přístup servisním pracovníkům.

V posledním desetiletí jsme svědky podobného trendu i u mnohem menších zařízení, která má mnohdy pacient dlouhá léta přímo u sebe. Jedná se o kardiostimulátory, implantabilní defibrilátory, inzulinové pumpy u diabetiků, neurostimulátory a podobně. Donedávna bylo možno tato zařízení připojit buď fyzicky (kabelem), nebo bezdrátově pouze na bezprostřední vzdálenost speciální přikládací „čtečkou“ (elektromagnetické záření, rádiový signál). Nyní se i u těchto zařízení začínají používat další komunikační možnosti, aby umožnily pohodlnou správu jejich funkcí. Jedná se například o bluetooth, webové rozhraní administrace a podobně. To samozřejmě může při nesprávném zabezpečení zpřístupnit zařízení i nevítaným „správcům“, kteří pak mohou zařízení ovládat, například vypnout defibrilátor.

Nejviditelnějším problémem jsou zřejmě úniky citlivých dat ve zdravotnictví. Podle výzkumu Ponemon institutu [1] se v USA s únikem dat potkalo 90 % poskytovatelů zdravotních služeb, navíc 40 % dokonce více než pětkrát v posledních dvou letech. Dle studie jde nejčastěji o ukradená či ztracená zařízení, phishing a malware, až poté následují minoritnější útoky typu spyware, DDoS, clickjacking, rootkity a další.

Proto si nejčastější útoky probereme podrobněji.

- **phishing** – podvodná webová stránka (napodobující přihlašovací stránku do e-mailu, internetového bankovnictví nebo nemocničního systému) používaná k získání citlivých nebo přihlašovacích údajů
- **virus** – škodlivý program, který se dokáže šířit a působit bez vědomí uživatele
- **spyware** – virus odesílající data z napadeného počítače bez vědomí uživatele
- **ransomware** – virus způsobující zašifrování koncového zařízení, pro odšifrování chtějí útočníci vysoké výkupné v anonymní měně (např. bitcoin)
- **DDoS** (*Distributed Denial of Service*) – DDoS je útok způsobující přehlcení a odstavení služby, například útok mnoha požadavků na webový server, které tento server zahltí a zastaví
- **spam** – nevyžádané obchodní sdělení (nejčastěji e-mailem)
- **hoax** – klamavá informace

Ransomware

Vážné útoky byly dosud hlášeny především ze zahraničí. Nicméně již máme první výskyty i u nás a následky jsou varovné. Při ransomwarovém útoku na nemocnici v Benešově na konci roku 2019, byly zašifrovány síťové disky všech zařízení v síti a nemocnice byla vyřazena z chodu na více než 3 týdny.

- https://www.itsec-nn.com/jak-se-nenechat-vydirat-ransomwarem/

Elektronický podpis

Elektronický podpis by měl určitým způsobem zaručovat důvěryhodnost dokumentu. Tato důveryhodnost může mít několik stupňů, což definuje Nařízení Evropského parlamentu a rady EU č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu [2].

- Prostý **elektronický podpis** jsou data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která podepisující osoba používá k podepsání. Může jít třeba o podpis v mailu nebo naskenovaný podpis v dokumentu.
- **Zaručeným elektronickým podpisem** je elektronický podpis již s vyšším stupněm ověření (certifikátem).
- **Kvalifikovaným elektronickým podpisem** je zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy. Zde je již nutné ověření podpisu např. USB tokenem nebo čipovou kartou.

Jednoduchá doporučení pro bezpečnou práci s počítačem

Existuje spousta doporučení a pokynů, jak bezpečně pracovat s počítačem a s citlivými daty pacienta. V reálném provozu ale mnohdy lékaři tápou a vystavují se zbytečnému riziku, že způsobí únik citlivých dat svých pacientů. V zahraničí je již zvykem o osobní údaje a zdravotní záznamy pečovat a nevystavovat je rizikům, u nás je však ještě praxe takříkajíc v plenkách. V následujícím článku bych tedy rád shrnul pár základních bodů, jak se správně chovat u počítače.

1. Používejte přiměřeně silné heslo

Vaše heslo do ambulantního či nemocničního systému by nemělo znít „heslo“, „1234“, „nemocnice“, „spital“ či jinak. Heslo by měla být co nejdelší těžko odhadnutelná sekvence znaků či slov, obsahujících nejlépe malá a velká písmena a číslice, rozhodně by neměla obsahovat např. jméno vašeho psa nebo rok narození v libovolné kombinaci. Nedoporučuje se používat písmena s diakritikou a atypická interpunkční znaménka, protože pokud chodíte po nemocnici a používáte více počítačů, mohlo by se stát, že na klávesnici na jiném oddělení nenajdete správný znak do svého hesla.

Rozhodně nepoužívejte stejné heslo, které máte kdekoliv jinde – v mailu, v mobilu nebo na sociálních sítích. Heslo také nevystavujte na papírku přilepeném k monitoru.

2. Nikomu nesdělujte své přihlašovací údaje

Nikdy! Pokud někdo (kolega lékař, zdravotní sestra, kdokoliv jiný) potřebuje vaše přihlašovací údaje, pak je to zřejmě z důvodu, že se nedostane k nějaké potřebné funkci informačního systému nebo v systému nevidí některou ambulanci či oddělení, které pro svou práci potřebuje vidět. V tom případě je namístě kontaktovat svého vedoucího pracovníka a pracovníka IT, aby práva nastavil správně. Řešením není dávat komukoliv své přihlašovací údaje – nikdy! Buďte si jisti, že budou zneužity k jiným účelům, než ke kterým jste je někomu v dobré víře prozradili. A vinu nesete vždycky vy. Takže ještě jednou: nikdy neprozrazujte své přihlašovací údaje!

3. Při odchodu od počítače se odhlaste ze systému

Vždycky se odhlašujte! Nikdy nevíte, jak dlouho se zdržíte od počítače, může se něco zkomplikovat a necháte počítač přístupný kolegům, jiným pracovníkům či dokonce pacientům. Vyhledávat v dokumentaci a nahlížet do cizích údajů je hračka a v každém systému zůstane záznam, že jste se tam dívali vy. Nedejbože tam někdo vaším jménem nějaká data změní a poškodí pacienta.

4. Nikdy nenahlížejte do dokumentace pacienta, o kterého nepečujete

Každé otevření, zavření a změna dokumentace je ze zákona zaznamenána v systému. Pokud pacient bude chtít jmenný seznam všech, kteří nahlíželi v počítači do jeho dokumentace, může se divit. A může si také stěžovat. V zahraničí jsou pokuty za nahlédnutí do dokumentace velmi vysoké a mohou šplhat od několika stovek dolarů až k miliónům dolarů. Únik citlivého údaje o pacientovi je např. v USA vyčíslen v průměru částkou přes 200 dolarů.

5. Používejte firemní (nemocniční) e-mailovou schránku

Pro komunikaci týkající se vašeho zaměstnání používejte výhradně firemní e-mailovou schránku. Jednak je firemný e-mailová adresa důvěryhodnější v elektronické korespondenci a jednak je často dobře zabezpečena oproti freemailovém službám typu Seznam, Centrum, Gmail a podobně. Ne proto, že by snad velké firmy neuměly zabezpečit svůj e-mailový server lépe než vaše nemocnice. Ale svůj osobní e-mail používáte k více účelům, jistě jste registrováni v sociálních sítích nebo na různých e-shopech. A člověk nikdy neví, kam jeho přihlašovací údaje mohou uniknout. Navíc vůči velkým firmám existuje mnohem více útoků. Příkladem může být skandál okolo soukromé e-mailové schránky Hillary Clinton či nabourání schránky šéfa CIA. Samozřejmostí je neotevírat nevyžádané e-mailové zprávy a už vůbec ne jejich podivné přílohy.

6. Nekopírujte. Anebo kopírujte s rozmyslem

Často se stane, že na počítači potřebujete vložit část dokumentace pacienta do nějaké jeho zprávy. Většina systémů na tuto činnost obsahuje vestavěný nástroj. Pokud však z důvodu pohodlí používáte prosté Ctrl+C a Ctrl+V, myslete na to, že až se odhlásíte ze systému, údaje ve schránce budou stále k dispozici. Není nic snazšího, než otevřít Word na počítači, kde seděl někdo z lékařů, a vložit si do dokumentu pomocí Ctrl+V obsah kopírovací

schránky. Ve většině případů schránka obsahuje velmi citlivé údaje, které by se takto neměly vůbec dostat ven. Takže buď používejte vestavěnou funkci systémů (poradí vám váš IT pracovník) nebo při kopírování dbejte na to, abyste schránku „přemazali“ nějakým neškodným textem.

7. Neukládejte citlivé údaje pacientů na plochu počítače. Ani nikam jinam

Pokud potřebujete část pacientovy zprávy překopírovat jinak či přenést do jiného zařízení, existují oficiální cesty, spousta nemocnic a poliklinik má vlastní šifrované interní úložiště sdílené ve vnitřní síti. Případně si data s velkou opatrností lze s přimhouřením oka nahrát na flash disk v šifrované formě nebo např. v zaheslovaném archivu. Nezapomeňte, že valná většina úniků dat je způsobena krádeží zařízení (nešifrovaný počítač, CD, flash disk, apod.). A zapomenutý soubor s citlivými údaji pacientů přímo na ploše počítače je už úplně neomluvitelný prohřešek, který může vyústit ve velký problém.

Nesmíme ani zapomenout, že prosté smazání souboru např. z flashky neznamená, že se k souboru už nikdo nedostane. Existuje software, jak získat smazaný soubor zpět v plné kráse. Ukládání dat pacientů do nešifrovaných souborů by se tudíž vůbec nemělo dít.

8. Používejte vzdálený přístup k informačnímu systému opatrně

Některé nemocnice a ambulance umožňují vzdálený přístup do systému (VPN). Tuto funkci používejte s rozmyslem. Ideálně v soukromí, ze zabezpečeného (služenbího) notebooku. počítače . Při připojení k síti může totiž snadno dojít k úniku dat. Buď vás bude někdo sledovat přes rameno, nebo vás bude sledovat prostřednictvím sítě na nezabezpečené wifi. Takže vzdálené připojení není určeno k použití v internetových kavárnách, v halách supermarketů ani na veřejných prostranstvích.

Navíc mějte na svém počítači vždy aktuální software a aktuální antivirový program – ať už máte jakýkoli operační systém.

Bezpečnostní pravidla pro sociální sítě

Chytré telefony (smartphony) se stávají velmi populárními v současné společnosti. Výjimkou nejsou ani zdravotničtí pracovníci, lékaři a koneckonců i studenti medicíny. Chytrý telefon samozřejmě primárně slouží komunikaci s rodinou, známými a přáteli, ale může se stát i cenným pomocníkem v medicíně. Lze na něm vyhledávat aktuální údaje, kontaktovat kolegy či odborníky a zasílat fotografie či skeny z dokumentace. Jako takový se tím chytrý telefon stává i velmi nebezpečným nástrojem, který může ohrozit bezpečnost dat pacienta.

- **Řiďte se zdravým rozumem.** Nesete odpovědnost za materiál, který zveřejníte na internetu, ať už jde o osobní blog, sociální sítě či jiná média. Nevhodné či ohrožující informace mohou poškodit pověst Vás či Vaší instituce a mohou negativně ovlivnit mezilidské vztahy.
- **Přemýšlejte před zveřejněním**. Vše, co zveřejníte na internetu, může být trvale spojeno s Vaší osobou, může se objevit sdíleno na jiných sítích či může být šířeno prostřednictvím e-mailu či jiných médií. Dbejte zvýšené opatrnosti, než cokoli odešlete na web. Smazání původního zdroje totiž nezaručuje, že si již někdo neudělal kopii.
- **Chraňte soukromí pacientů.** Nikdy nezveřejňujte informace o konkrétních pacientech a nepoužívejte nevhodné fotografie.
- **Chraňte své soukromí.** Snažte se prozkoumat, kde máte svůj profil, jaká ochrana osobních údajů a jaké bezpečnostní prvky daná stránka používá. Nezveřejňujte více, než je vhodné, osobní příspěvky, osobní fotografie a videa ponechejte sdílená jen mezi nejbližšími přáteli nebo je nejlépe nesdílejte vůbec.
- **Identifikujte se.** Pokud na webu komentujete dění okolo Vaší instituce, vždy uveďte, kdo jste a jaký vztah k instituci máte. Za zveřejněné příspěvky nesete plnou zodpovědnost.
- **Respektujte autorská práva.** Nepoužívejte na webu materiály, ke kterým nevlastníte žádná autorská práva a ani nemáte povoleno s materiálem pracovat. Pokud používáte něčí informaci, obrázek či video, ujistěte se, že Vám to licence dovoluje a důkladně ocitujte zdroj, ze kterého jste čerpali.

Lékaři a internetové poradny

V poslední době je velkým trendem vytvářet různá fóra a diskusní weby, kde si pacienti navzájem radí ohledně svých zdravotních problémů. Některé weby jdou ještě dále a určité rubriky spravuje lékař, který pacientům na základě poskytnutých informací radí, jak se zachovat nebo čím se léčit.

Je to problematika velmi ošemetná, nemá v našich zemích moc dlouhou historii. Některé ambulance si již zakládají účty na sociálních sítích, ale půda pro „poradny na internetu“ není příliš příznivá.

Jak je to se zákony?

Samozřejmostí je ochrana osobních údajů podle zákona 101/2000 Sb. o ochraně osobních údajů [3], dále nakládání s údaji a povinnost mlčenlivosti zdravotnických pracovníků upravují paragrafy 51 a 52 zákona 372/2011 o zdravotních službách [4].

Stran poraden je velmi důležitý §2950 nového občanského zákoníku [5] (č. 89/2012), který doslova uvádí:

> *„Kdo se hlásí jako příslušník určitého stavu nebo povolání k odbornému výkonu nebo jinak vystupuje jako odborník, nahradí škodu, způsobí-li ji neúplnou nebo nesprávnou informací nebo škodlivou radou danou za odměnu v záležitosti svého vědění nebo dovednosti.“*

Poradny na internetu

Lékař radící na internetu tedy musí dávat bedlivý pozor, aby nezískával od radychtivého pacienta informace, které sám pacient uvést veřejně nechtěl, a aby neporadil tak, že pacientovi kvůli navrženému postupu vznikne škoda či újma na zdraví.

V tuto chvíli se lékař ocitá v situaci, kdy o pacientovi nic neví a kdy chce vymyslet kloudnou radu na pacientovy obtíže. Kromě bezpečí lékaře se zde samozřejmě jedná zejména o bezpečí pacienta: ten nemusí (a neměl by!) chtít zveřejnit všechny podrobnosti o svém zdravotním stavu, které jsou nutné k zamyšlení nad vhodný postupem. Navíc i vzhledem k bezpečí jeho citlivých údajů není vhodné problematiku probírat veřejně v diskusi a koneckonců i dobře míněná rada může nakonec vést jiného čtenáře-pacienta s poněkud jinou symptomatologií k chybnému úsudku.

Nejvhodnější se tedy jeví do podrobných rad a poraden se nepouštět a ponechat léčbu v poněkud (oboustranně) bezpečnějším prostředí: v osobním kontaktu v ambulancích.

Porada s lékařem přes internet

Často se uvažuje o „soukromé“ konzultaci s lékařem – po telefonu, přes SMS, e-mail a další kanály. Je nutné si uvědomit, že ačkoli v danou chvíli se zdá, že „nikdo neposlouchá“, opak může být pravdou. Telefony, SMS zprávy, e-mail či nedejbože chatovací aplikace – ani jedno není zabezpečeno vůči úniku dat, natož citlivých dat. Možná nyní nejsou k dispozici hackeři, kteří by měli zájem na ranním tlaku pana Vomáčky z Horní Lhoty, ale představte si vždy situaci nějakého VIP klienta… propouštěcí zpráva ministra jistě neputuje z nemocnice do soukromé e-mailové schránky praktického lékaře, každý si totiž dovede představit, jaké dopady by měl únik takovéto zprávy na veřejnost. Stejným způsobem je nezbytné zacházet s citlivými daty všech pacientů bez rozdílu, je to nutnost a vyžaduje to zákon.

Některé ambulantní či nemocniční informační systémy umožňují pacientům objednávat kontroly, odesílat některá data či zeptat se na drobnou radu přes internet. Jsou to ale součásti zabezpečených informačních systémů, komunikace probíhá zabezpečeným kanálem a je šifrována. V žádném případě ale nelze takto komunikovat e-mailem či nezabezpečeným chatem.

Bezpečnost pacientů především

Závěrem lze tedy říci, že nezabezpečená komunikace na internetu by neměla probíhat vůbec, ale lze do jisté míry použít zabezpečených komunikačních kanálů v ambulantních či nemocničních informačních systémech.

Odkazy

- Počítačové sítě

Reference

1. https://www2.idexpertscorp.com/knowledge-center/
2. https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014R0910,
3. https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=49228&nr=101~2F2000&rpp=15#local-content
4. https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=75500&nr=372~2F2011&rpp=15#local-content
5. https://portal.gov.cz/app/zakony/zakonPar.jsp?page=2&idBiblio=74907&recShow=2949&nr=89~2F2012&rpp=15#parCnt