Kybernetická příručka pro lékaře

10+1 kroků k ochraně ordinace

Projekt Národní centrum elektronického zdravotnictví (registrační číslo CZ.31.1.01/MV/22_05/0000005)

Verze: 1.0
Platnost nové verze od: 06/2023

Ministerstvo zdravotnictví České republiky, Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

Obsah

1 Úvod

1.1 Co představuje příručka?

Kybernetické útoky a kybernetické hrozby jsou významným rizikem dnešních dní. Na tento stav se Ministerstvo zdravotnictví rozhodlo reagovat vytvořením kybernetické příručky pro lékaře aneb „10+1 kroků k ochraně ordinace“.

Tento doporučující dokument má za cíl poskytnout praktickým lékařům a malým ambulancím do 5 lidí ucelený pohled na problematiku kybernetické ochrany v ordinaci praktického lékaře a nabídnout účinná opatření, která může lékař aplikovat pro zajištění kybernetické ochrany svého informačního systému proti ztrátě informací a ochraně informací a osobních údajů o pacientech.

1.2 Výchozí stav

Dnešní doba je z pohledu ochrany informací a osobních údajů velmi dynamická. Díky zavádění nových technologií a zvyšující se znalosti jejich zneužití vzrůstají rizika napadení počítačových systémů za účelem zneužití informací, která obsahují. Podoby zneužití informací jsou různé, od prostého smazání, s cílem oběť útoku poškodit, zkopírování informací za účelem jejich prodeje až po jejich zašifrování (zamezení přístupu k informacím) s cílem získat „výkupné“ za jejich opětovné zpřístupnění.

Zdravotnické údaje jsou obecně pro hackery nejvíce žádanou a finančně oceňovanou komoditou ze všech informací, kdy často dochází k jejich prodeji.

Úroveň zajištění kybernetické bezpečnosti v ordinacích praktických lékařů a malých ambulancí do 5 lidí je různá, obecně však můžeme konstatovat, že je většinově nedostatečná. Příčina tohoto stavu je dána jednak povědomím o kybernetických hrozbách a jejich předcházení a jednak i rostoucím nákladům na protiopatření.

1.3 Struktura příručky

Oblast ochrany proti kybernetickým hrozbám je rozsáhlá. Účelem dokumentu není popsat všechny její aspekty, ale zaměřit se pouze na zásadní hrozby a rizika, kterým praktičtí lékaři čelí.

Dokument je rozdělen na 10+1 oblastí, přičemž praktický lékař, resp. malá ambulance do 5 lidí, by měli věnovat svou pozornost každé z těchto základních oblastí ochrany proti kybernetickým hrozbám.

1.4 K čemu je a pro koho je příručka určena?

Je určena pro praktické lékaře a další malé poskytovatele zdravotních služeb typicky do 5 zaměstnanců. Cílem příručky je poskytnout lékaři praktické informace, které pomohou lépe pochopit rizika a hrozby kybernetického prostoru a nabídnou účinná bezpečnostní opatření

s cílem tato rizika a hrozby snížit tak, aby nedošlo ke kybernetickému útoku, tj. zejména ke ztrátě informací o pacientech a výpadku informačního systému.

1.5 Je příručka závazná?

Příručka má charakter doporučení. Nicméně výrazně doporučujeme aplikaci zde uvedených bezpečnostních opatření.

1.6 Další zdroje informací

V příručce jsou dále uvedeny odkazy na další doporučující dokumenty, které rozšiřují a doplňují danou oblast nebo bezpečnostní opatření.

Doporučujeme seznámit se a využít podpůrné metodický materiály kybernetické bezpečnosti vytvořené Ministerstvem zdravotnictví České republiky.[1]

Pro zavedení bezpečnostních opatření uvedených v této příručce doporučujeme využít „Minimální bezpečnostní standard“ vytvořený Národním úřadem pro kybernetickou a informační bezpečnost.[2]

2 10+1 kroků k ochraně ordinace

Počet kybernetických útoků na sektor zdravotnictví celosvětově významně roste. Mění se jednak sofistikovanost útoků a díky dostupnosti vyspělých technologií i účinnost těchto útoků. Od útoků vedené tzv. brutální silou vedoucí k destrukci, zcizení či zamezení přístupu k datům až po sofistikované útoky s cílem zcizení či kontinuálního zcizování informací tak, aby oběť kybernetického útoku neměla o jeho průběhu ponětí.

Proto je naprosto zásadní průběžně zvyšovat povědomí o kybernetické bezpečnosti personálu ordinace praktického lékaře a personálu malých ambulancí a přijímat vhodná bezpečnostní opatření eliminaci nebo alespoň ke snížení kybernetických hrozeb.

Možností, jak zabezpečit ordinaci je mnoho, nicméně v rámci této příručky poskytujeme základní a nezbytná bezpečnostní opatření. Cílem je poskytnout vyvážený přístup mezi funkčností, bezpečností a náklady na zabezpečení.

2.1 Konkrétně k 10+1 krokům

Rizik spojených s nedostatečnou ochranou informačních systémů a informací o pacientech je mnoho a dotýkají se každé další oblasti uvedené v této příručce.

[1] Metodické materiály kybernetické bezpečnosti dostupné na oficiálních stránkách Národního centra elektronizace zdravotnictví https://ncez.mzcr.cz/cs/kyberneticka-bezpecnost/metodika-kyberneticke-bezpecnosti

[2] Minimální bezpečnostní standard vytvořený Národním úřadem pro kybernetickou a informační bezpečnost dostupný na https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

Níže je uvedeno celkem 10+1 kroků, po ucelených oblastech, prostřednictvím kterým dojde k výraznému zabezpečení ordinace praktického lékaře nebo malé ambulance před kybernetickými hrozbami.

Bezpečnostní opatření proti kybernetickým hrozbám jsou rozdělena do těchto oblastí:

- Školení a vzdělávání (1 z 10+1)
- Aplikace a systémy (2 z 10+1)
- Stacionární počítače (3 z 10+1)
- Notebooky (4 z 10+1)
- Mobilní telefon (5 z 10+1)
- Síťová ochrana (6 z 10+1)
- Fyzická bezpečnost (7 z 10+1)
- Zálohování (8 z 10+1)
- Zaměstnanci a dodavatelé (9 z 10+1)
- Hesla a přihlašování (10 z 10+1)
- Co dělat, když se něco stane? (11 z 10+1)

Příručka je strukturována tak, aby intuitivním způsobem předala podstatné informace o hrozbách a odpovídajících bezpečnostních opatřeních ke každé uvedené oblasti:

- Stručné uvedení oblasti, čeho se týká, co pokrývá?
- Co by se mohlo stát, hrozby, rizika?
- Co dělat, aby se to nestalo, konkrétní bezpečnostní opatření?

U každého bezpečnostního opatření je vždy uvedeno doporučení, jestli by měl dané opatření zajišťovat praktický lékař nebo dodavatel. Dodavatelem jsou typicky myšleni správci IT. Je potřeba mít na vědomí, že se jedná pouze o doporučení, a proto při zavádění bezpečnostního opatření musí vždy lékař určit, jestli dané opatření zvládne zajistit sám nebo potřebuje pomoc.

2.1.1 Školení a vzdělávání 1 z 10+1

Lidé jsou obecně považování za nejslabší článek řetězce v oblasti kybernetické bezpečnosti. Nejsnazším způsobem, jak úspěšné vést kybernetický útok je prostřednictvím neproškolených nebo informaticky málo zdatných uživatelů. Hlavními důvody jsou zejména postoje k počítačům a celkově k výpočetní technice, které jsou pro ně na první pohled moc složité a vzdálené. Zároveň jsou však uživatelé velmi rezistentní vůči změnám, a proto tak dochází k tomu, že např. jedno heslo využívají u všech účtů a nechtějí si ho změnit.

Tato oblast se týká jak lékaře, tak i zdravotní sestry. Obě tyto skupiny, a případně další osoby, které pracují s výpočetní technikou v ordinaci, musí být průběžně školeni v oblasti kybernetické bezpečnosti. Cílem je získávání informací o způsobech vedení kybernetických útoků a ochraně proti nim.

Co by se mohlo stát?

Rizik spojených s pochybením ze strany uživatelů je mnoho a dotýkají se každé další oblasti uvedené v této příručce. Patří sem určitě používání stejného přihlašovacího hesla (např. k soukromému e-mailovému účtu, do internetového obchodu, do provozované aplikace, na sociálních sítích apod.) na mnoha místech. Pokud tedy útočník získá toto heslo, může se dostat ke kompletnímu e-mailovému účtu a veškeré historii komunikace. Získá tak přístup jak k soukromé, tak i pracovní korespondenci. Dalším rizikem je důvěra v každý obdržený e-mail,

kdy se kyberútočník snaží získat buď přihlašovací údaje (heslo) nebo další informace, typicky informace o platební kartě, přístupových právech. Velkým nešvarem je také využívání pracovního e-mailu pro soukromé potřeby, a nebo přístupy z pracovních prostředků do soukromého e-mailu.

Základní techniky kybernetických útočníků, o kterých by měl mít uživatel povědomí jsou:

- Plošně zaslaný e-mail tzv. phishingový e-mail s cílem donutit uživatele kliknout na přiložený soubor nebo internetových odkaz obsahující škodlivý počítačový program, který zaviruje počítač.[3]
- Podvržený plošný e-mail – e-mail, který vypadá jako odeslaný od známe instituce (banka, pošta apod.).
- Cílený e-mailový útok – e-mail tvářící se jako od kolegy nebo nadřízeného, většinou nutí uživatele k nějaké akci, například proplatit fakturu.
- Zneužití hesla – ordinace praktického lékaře nebo malé ambulance často nemají pravidla pro tvorbu hesel, často i sdílí jedno heslo napříč ordinací a zároveň stejné heslo používají v internetových aplikacích, například účet Google, učet v e-shopu apod. V případě, kdy bude napaden například e-shop a útočník získá přihlašovací údaje uživatelů, které jsou použity i v jiných službách nebo interních počítačových systémech, může dojít k jejich zneužití.

Co dělat, aby se to nestalo?

1) V první řadě je nezbytné se seznámit s touto příručkou a řídit se jí. Toto seznámení zajistit u zdravotní sestry a dalšího personálu ordinace.
    - *Doporučujeme zajištění ze strany lékaře.*
2) Absolvovat kurz kybernetické bezpečnosti, doporučujeme bezplatný online kurz vydaný Národním úřadem pro kybernetickou a informační bezpečnost s názvem „Dávej kyber – Základy kybernetické bezpečnosti“[4], případně požádat o bezpečnostní proškolení Vašeho IT specialistu.
    - *Doporučujeme zajištění ze strany lékaře.*
3) Opakovat školení každoročně. Vhodné je měnit vzdělávací kurzy.
    - *Doporučujeme zajištění ze strany lékaře.*

2.1.2 Aplikace a systémy (2 z 10+1)

Tato oblast se týká samotného výběru a nastavení využívaných aplikací a systémů. Mezi aplikace a systémy řadíme ty, které jsou nezbytné pro poskytování zdravotní péče. Nicméně zde uvedená bezpečnostní doporučení se týkají obecně všech aplikací a systémů.

Typickými aplikacemi a systémy jsou:

- Ambulantní informační systém (informační systém, kde jsou uloženy klinické události a informace o pacientech)
- Microsoft Office (Word, Excel, Outlook, Powerpoint, Microsoft Teams)
- Operační systém (operační systém počítače, notebooku a mobilního telefonu, Windows, macOS, iOS, Android)

[3] Více informací o nebezpečnosti těchto phishingových e-mailů je uvedeno v Informačním bulletinu 6/02-2023 https://ncez.mzcr.cz/sites/default/files/media-documents/Informacni_Bulletin_6-2023.pdf

[4] Oficiální stránky Národního úřadu pro kybernetickou a informační bezpečnost obsahující vzdělávací kurz Dávej kyber – Základy kybernetické bezpečnosti dostupný na https://osveta.nukib.cz/

- E-mailová komunikace (informační systém pro odesílání a příjem e-mailů Outlook, O365)
- Webový prohlížeč (Google Chrome, Edge, Safari)
- Datová schránka
- Webové stránky ordinace
- Rezervační systém
- eZprava

Co by se mohlo stát?

Nejdůležitějším informačním systémem je jednoznačně ambulantní informační systém, který obsahuje kompletní informace o pacientech. V případě, že by kyberútočník získal přístup do tohoto systému, mohl by provést stažení všech informací a následně by Vás mohl vydírat s žádostí o výkupné před zveřejněním těchto informací. Tato informace by se určitě dostala i do médií a následně k pacientům. Nicméně v případě nevhodně nastavených přístupových oprávnění se k těmto informacím mohou dostat i další osoby, např. zdravotní sestra nebo uklízečka apod.

Komunikace s pacienty, kolegy, laboratořemi a dalšími třetími stranami čím dál více probíhá prostřednictvím e-mailové komunikace. Pokud by se tohoto e-mailu zmocnil kyberútočník, mohl by si přečíst kompletní korespondenci a také za Vás komunikovat.

Co dělat, aby se to nestalo?

1) Zajistit vhodné nastavení přístupů a oprávnění do informačních systémů a aplikací.[5]
    - *Doporučujeme zajištění ze strany dodavatele.*
2) Zajistit přihlašování prostřednictvím silného hesla a druhého faktoru (2FA) všude, kde je to možné.[6]
    - *Doporučujeme zajištění ze strany dodavatele.*
3) Zajistit zálohování ambulantního informačního systému a dalších kritických systémů.[7]
    - *Doporučujeme zajištění ze strany dodavatele.*
4) Zakázat spouštění maker v Microsoft Office dokumentech.
    - *Doporučujeme zajištění ze strany dodavatele.*
5) Nastavit co nejvčasnější aktualizaci informačních systémů, aplikací a operačních systémů.[8]
    - *Doporučujeme zajištění ze strany dodavatele.*
6) Zajistit bezpečnou konfiguraci webové stránky ordinace.[9]
    - *Doporučujeme zajištění ze strany dodavatele.*
7) Využívat pouze oficiální operační systémy.
    - *Doporučujeme zajištění ze strany dodavatele.*

[5] Pro oblast řízení přístupů je možné využít kap. 10 Řízení přístupů od strany č. 19 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[6] Pro oblast vícefaktorového přihlašování je možné využít kap. 10.3 Politika hesel pro uživatelské účty strana č. 21 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[7] Pro oblast zálohování je možné využít kap. 15.3 Zálohování strana č. 31 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[8] Pro oblast aktualizací je možné využít kap. 10 Řízení přístupů od strany č. 19 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[9] Pro oblast ochrany webové aplikace a stránky je možné využít kap. 17.2 Ochrana informačního nebo komunikačního systému typu webové aplikace na straně č. 36 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

8) Využívat webový prohlížeč pouze pro pracovní účely a nenavštěvovat nebezpečné stránky.
    - *Doporučujeme zajištění ze strany lékaře.*

2.1.3 Pracovní stanice – klasické počítače (3 z 10+1)

Počítač nebo notebook je základním administrativním nástrojem pro práci lékaře a sestry. Proto je potřeba u nich myslet kromě funkčnosti i na kybernetickou bezpečnost.

Co by se mohlo stát?

Stacionární pracovní stanice představuje počítač lékaře i sestry, kde probíhá zaznamenávání veškerých informací. Na tomto počítači je naistalován ambulantní informační systém (mnohdy je počítač využívána jako server) a tento počítač je využíván pro komunikaci s pacienty, laboratořemi, kolegy z oboru a dalšími subjekty.

Situací, které by mohly způsobit problémy, je mnoho. Jedním z nejvíce rizikových je zanesení škodlivého kódu. Tento škodlivý kód může způsobit kompletní ztrátu všech informací uložených na počítači a ambulantním informačním systému. Uživatel tak může přijít o všechny informace o pacientech. Prostřednictvím tohoto škodlivého kódu však může dojít i k odposlechu komunikace na počítači. Dalším rizikem je situace, kdy útočník získá informace z počítače a následně je zveřejní na internetu.

Je však potřeba dbát i na fyzickou bezpečnosti počítačů, může se totiž stát, že v případě, že se počítač nachází na zemi, je možné do něho kopnout nebo na něj omylem vylít vodu.

Co dělat, aby se to nestalo?

1) Zajistit přihlašování prostřednictvím silného hesla do počítače.[10]
    - *Doporučujeme zajištění ze strany dodavatele.*
2) Zajistit vypínání počítačů, odhlášení uživatele nebo uzamknutí monitoru a klávesnice v případě nepřítomnosti.
    - *Doporučujeme zajištění ze strany lékaře.*
3) Zajistit zálohování informací počítače.[11]
    - *Doporučujeme zajištění ze strany dodavatele.*
4) Zajistit nastavení antivirové a antispamové ochrany.[12]
    - *Doporučujeme zajištění ze strany dodavatele.*
5) Zajistit nastavení firewallu.[13]
    - *Doporučujeme zajištění ze strany dodavatele.*
6) Zajistit nastavení šifrování disku.[14]

[10] Pro oblast hesel je možné využít kap. 10.3 Politika hesel pro uživatelské účty na straně č. 21 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[11] Pro oblast zálohování je možné využít kap. 15.3 Zálohování na straně č. 31 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[12] Pro oblast antivirové a antispamové ochrany je možné využít kap. 11 Požadavky v oblasti ochrany před škodlivým kódem na straně č. 22 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[13] Pro oblast firewallové ochrany je možné využít kap. 11 Požadavky v oblasti ochrany před škodlivým kódem na straně č. 22 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[14] Pro oblast šifrování disků a externích USB disků je možné využít kap. 14 Kryptografické prostředky na straně č. 28 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

- *Doporučujeme zajištění ze strany dodavatele.*

7) Zajistit bezpečné fyzické umístění počítače.
   - *Doporučujeme zajištění ze strany lékaře.*
8) Zajistit pravidelnou fyzickou údržbu počítače před zanesením prachem.
   - *Doporučujeme zajištění ze strany dodavatele.*
9) Zajistit pravidelnou aktualizaci operačního systému.[15]
   - *Doporučujeme zajištění ze strany dodavatele.*

2.1.4 Notebooky (4 z 10+1)

Notebooky jsou využívány zejména mimo ordinaci, tedy mimo bezpečný prostor. Tomu musí odpovídat i zvýšená bezpečnost těchto přenosných zařízení. Notebooky nemusí být nutnou součástí práce každého lékaře, nicméně představují významná kybernetická rizika, a proto je nezbytné je vhodně chránit.

Co by se mohlo stát?

U notebooků hrozí stejná rizika jako u počítačů. Nicméně stacionární počítače jsou neustále fyzicky zamknuté v bezpečí ordinace. To u notebooků nemusí platit, a proto se tak může stát, že je notebook zcizen a útočník se tak může lehce dostat k veškerým informacím na něm uložených. Speciálně v případě, kdy uživatel nevyužívá heslo pro přihlášení a ve webovém prohlížeči má nastaveno automatické vyplňování hesla k různým službám. Dalším rizikem práce na notebooku je, že když na něm pracujete, kdokoliv se Vám může dívat přes rameno a případně si vyfotit obsah Vaší komunikace a dalších zobrazovaných informací. Kromě toho, pokud se prostřednictvím notebooku připojujete k počítači v ordinaci, je možné prostřednictvím tohoto kanálu zanést do počítače škodlivý kód.

Co dělat, aby se to nestalo?

1) Zajistit přihlašování prostřednictvím silného hesla k notebooku.[16]
   - *Doporučujeme zajištění ze strany lékaře.*
2) Zajistit vypínání obrazovky a notebooku v případě nepřítomnosti. Popř. je možné doplnit notebook filtrem, který omezuje úhel čtení dat z obrazovky (nevhodné pro dotykové obrazovky).
   - *Doporučujeme zajištění ze strany lékaře.*
3) Zajistit zálohování informací notebooku.[17]
   - *Doporučujeme zajištění ze strany dodavatele.*
4) Zajistit nastavení antivirové a antispamové ochrany.[18]
   - *Doporučujeme zajištění ze strany dodavatele.*

[15] Pro oblast aktualizací je možné využít kap. 10 Řízení přístupů od strany č. 19 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[16] Pro oblast hesel je možné využít kap. 10.3 Politika hesel pro uživatelské účty na straně č. 21 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[17] Pro oblast zálohování je možné využít kap. 15.3 Zálohování na straně č. 31 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[18] Pro oblast antivirové a antispamové ochrany je možné využít kap. 11 Požadavky v oblasti ochrany před škodlivým kódem na straně č. 22 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

5) Zajistit nastavení firewallu.[19]
    - *Doporučujeme zajištění ze strany dodavatele.*
6) Zajistit nastavení šifrování disku.[20]
    - *Doporučujeme zajištění ze strany dodavatele.*
7) Zajistit bezpečné fyzické nakládání s notebookem.
    - *Doporučujeme zajištění ze strany lékaře.*
8) Zajistit pravidelnou fyzickou údržbu notebooku před zanesením prachem.
    - *Doporučujeme zajištění ze strany dodavatele.*
9) Zajistit pravidelnou aktualizaci operačního systému.[21]
    - *Doporučujeme zajištění ze strany lékaře.*

2.1.5 Mobilní telefon (5 z 10+1)

Mobilní telefony se staly nedílnou součástí našich běžných životů, kdy kromě telefonátů využíváme mobilní telefony i pro vyřizování e-mailové pošty a vyhledávání na internetu.

Co by se mohlo stát?

Stejně jak je pro nás mobilní telefon důležitý, stejně tak je důležité jeho vhodné zabezpečení. V případě, kdyby uživatel neměl nastavený zámek obrazovky, mohl by jeho telefon kdokoliv otevřít. Mobilní telefon však plní i roli bezpečnostního opatření např. při využívání druhého faktoru (např. Google Authenticator, Smart banking, moje ID atd.), což při získání mobilního telefonu útočníkem významně napomůže zneužití informací. Rizika mobilních telefonů jsou dále stejná jako u notebooků, jelikož se také jedná o přenosná zařízení.

Co dělat, aby se to nestalo?

1) Zajistit přihlašování prostřednictvím biometrického údaje, pokud je to možné.
    - *Doporučujeme zajištění ze strany lékaře.*
2) Zajistit nastavení antivirové a antispamové ochrany.[22]
    - *Doporučujeme zajištění ze strany dodavatele.*
3) Zajistit nastavení zálohování mobilního telefonu.[23]
    - *Doporučujeme zajištění ze strany dodavatele.*
4) Zajistit bezpečné fyzické nakládání s mobilním telefonem a vyhnutí se jeho ztrátě.
    - *Doporučujeme zajištění ze strany lékaře.*
5) Zajistit pravidelnou aktualizaci operačního systému.[24]
    - *Doporučujeme zajištění ze strany lékaře.*

[19] Pro oblast firewallové ochrany je možné využít kap. 11 Požadavky v oblasti ochrany před škodlivým kódem na straně č. 22 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[20] Pro oblast šifrování disků a externích USB disků je možné využít kap. 14 Kryptografické prostředky na straně č. 28 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[21] Pro oblast aktualizací je možné využít kap. 10 Řízení přístupů od strany č. 19 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[22] Pro oblast antivirové a antispamové ochrany je možné využít kap. 11 Požadavky v oblasti ochrany před škodlivým kódem na straně č. 22 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[23] Pro oblast zálohování je možné využít kap. 15.3 Zálohování na straně č. 31 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[24] Pro oblast aktualizací je možné využít kap. 10 Řízení přístupů od strany č. 19 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

6) Zajistit stahování aplikací pouze z ověřených zdrojů.
    - *Doporučujeme zajištění ze strany lékaře.*
7) Zajistit nastavení hlídání polohy zařízení.
    - *Doporučujeme zajištění ze strany lékaře.*
8) Zajistit nastavení vzdáleného výmazu zařízení.
    - *Doporučujeme zajištění ze strany lékaře.*

2.1.6 Síťová ochrana (6 z 10+1)

Oblast síťové ochrany se týká bezpečného připojení k internetu a také dostupných Wi-Fi sítí jak pro zdravotnický personál, tak pro pacienty. Nastavení sítě a její ochrana bude vždy záviset na fyzickém umístění ordinace, tedy jestli je ordinace součástí většího zdravotnického zařízení (např. nemocnice, poliklinika), administrativní budovy nebo jestli je ordinace součástí vlastního nebo pronajímaného domu. Pokud je ordinace součástí jiného komplexu, bude Vaši síť zřejmě zajišťovat dodavatel daného komplexu. V případě vlastního nebo pronajatého domu bude zajištění na Vás nebo na dodavateli.

Co by se mohlo stát?

Bez připojení k internetu se neobejdeme. Nicméně množství kybernetických útoků je vedeno právě cestou internetu, kdy se do Vašeho prostředí a následně na Vaše servery a počítače může dostat škodlivý kód, který může ukrást informace o pacientech nebo počítače zašifruje prostřednictvím tzv. ransomwaru tak, že s nimi dále nemůžete pracovat. Útočník následně vyžaduje výkupné za odblokování. Nezřídka se stává, že je odblokována pouze část disku a následuje další výkupné, což se může několikrát opakovat.

Dalším rizikem jsou Wi-Fi sítě, ke kterým přistupuje lékař, ale i pacienti ze svých soukromých zařízení společně. Již tento stav představuje významné riziko, jelikož prostřednictvím takovéhoto soukromého zařízení se může dostat škodlivý kód do sítě ordinace. Cílem útočníků totiž nejsou povětšinou pacienti, ale počítače a servery lékaře, kde najdou cenné (citlivé) informace prostřednictvím kterých Vás mohou vydírat. V případě, že se útočník dostane na Váš Wi-Fi router, získá přístup k jeho nastavení a např. k DNS serveru, který má na starosti předklad webových jmenných adres na IP adresy. V takovém případě, pokud do internetového prohlížeče zadáte např. www.mojebanka.cz, Vám útočník podvrhne adresu a přesměruje ji na svou vlastní tak, aby mohl ukrást Vaše přihlašovací údaje, až se budete přihlašovat do svého internetového bankovnictví.

Co dělat, aby se to nestalo?

1) Zajistit neustále aktuální operační systém u prvků síťové ochrany (routery, switche).[25]
    - *Doporučujeme zajištění ze strany dodavatele.*
2) Využívat silné heslo k Wi-Fi.[26]
    - *Doporučujeme zajištění ze strany dodavatele.*
3) Oddělit provozní a pacientskou datovou a Wi-Fi síť.
    - *Doporučujeme zajištění ze strany dodavatele.*
4) Změnit přístupové heslo do administrace prvků síťové ochrany.

[25] Pro oblast aktualizací je možné využít kap. 10 Řízení přístupů od strany č. 19 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[26] Pro oblast hesel je možné využít kap. 10.2 Politika hesel pro privilegované účty na straně č. 20 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

- *Doporučujeme zajištění ze strany dodavatele.*

5) Zajistit firewallovou ochranu sítě.[27]
    - *Doporučujeme zajištění ze strany dodavatele.*

2.1.7 Fyzická bezpečnost (7 z 10+1)

Fyzická bezpečnost pokrývá v první řadě ochranu fyzických dokumentů pacientů (chorobopis v listinné formě), ale i informace o pacientech uložených na nosičích v elektronické podobě. Tím jsou myšleny počítače, přenosná mobilní zařízení (mobilní telefony, notebooky), ale i média (USB flash disk, CD/DVD disk). Proto se fyzická bezpečnost týká jak ochrany ordinace před vstupem neoprávněné osoby, tak i ochrany mobilních zařízení a médií.

Fyzická bezpečnost v sobě zahrnuje i zajištění dostupnosti výpočetní techniky (počítače, serverů a síťových prvků) v případě výpadku elektrické energie.

Co by se mohlo stát?

Mohlo by dojít ke ztrátě fyzických dokumentů o pacientech, stejně jako ztrátě těchto informací z notebooku nebo USB flash disku (CD/DVD disku), což by jistě mělo negativní dopad na dobré jméno lékaře a ordinace. Jistě by to také vzbudilo zájem dozorového orgánu pro ochranu osobních údajů a negativní mediální publicitu.

K získání informací však nemusí dojít jen ze strany útočníka, ale například i ze strany dalších osob, které mají přístup do ordinace. Typickým příkladem jsou úklidové služby, které často mají vlastní přístup do ordinace mimo ordinační hodiny. Mnohdy je taková činnost i nevědomá.

Ke zcizení zařízení (mobilní telefon, notebook) často dochází v místech jako jsou restaurace, prostředky hromadné dopravy nebo při volném ponechání zařízení bez dozoru.

V případě, že dlouhodobě nedochází k údržbě hardwaru, může dojít k jeho znečištění, což může způsobit požár a zničení daného zařízení a informací v něm uložených.

Důležité je i všechna média, na která jste ukládali data o pacientech, ale i jiné citlivé nebo důležité informace, pokud je již nebudete používat, skartovat nebo upravit tak, aby z nich informace nebyly již čitelné. Zde je potřeba uvést, že např. z flashdisku nestačí jen data jednoduše smazat, ale je potřeba je smazat specializovaným programem, který zabrání jejich obnovení. Je třeba mít na paměti, že i vyřazované počítače a notebooky mohou obsahovat paměťová média (pevné a SSD disky).

Co dělat, aby se to nestalo?

1) Zajistit fyzickou bezpečnost a optimálně uzamykání fyzických dokumentů o pacientech. Následně neponechávat klíč k této kartotéce volně dostupný.[28]
    - *Doporučujeme zajištění ze strany lékaře.*
2) Zajistit fyzickou bezpečnost mobilních zařízení a médií.
    - *Doporučujeme zajištění ze strany lékaře.*

[27] Pro oblast firewallové ochrany je možné využít kap. 11 Požadavky v oblasti ochrany před škodlivým kódem na straně č. 22 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[28] Pro oblast fyzické bezpečnosti je možné využít kap. 9 Fyzická bezpečnost na straně č. 18 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

3) Zajistit kontrolu fyzického přístupu do ordinace tak, aby se tam nedostala neoprávněná osoba.
    - *Doporučujeme zajištění ze strany lékaře.*
4) Zajistit záložní zdroj elektrické energie UPS.[29]
    - *Doporučujeme zajištění ze strany dodavatele.*
5) Zajistit pravidelnou péči o hardware a profylaxi.
    - *Doporučujeme zajištění ze strany dodavatele.*
6) Zajistit prázdný stůl a vypnutý počítač při odchodu z ordinace.
    - *Doporučujeme zajištění ze strany lékaře.*
7) Zajistit skartaci nebo neobnovitelné smazání dat z médií, která již nebudete používat
    - *Doporučujeme zajištění ze strany lékaře.*

2.1.8 Zálohování (8 z 10+1)

Jednou z největších obav lékaře je rozsáhlá ztráta informací o pacientech. Z tohoto důvodu je nezbytné provádět pravidelné a bezpečné zálohování informací. Pokud by došlo k zašifrování nebo ztrátě informací, tyto mohou být jednoduše obnoveny ze zálohy.

Co by se mohlo stát?

Škodlivé kódy (malware) se do počítačů často dostávají prostřednictvím stažených Microsoft Office dokumentů (především Word, Excel) a v případě, že je uživatel stáhne a spustí, může to znamenat kompletní nefunkčnost počítače a ztrátu všech informací. Stejně tak může být počítač napaden škodlivým šifrovacím kódem (ransomware), který počítač zašifruje a útočník následně vyžaduje výkupné za jeho obnovení.

Co dělat, aby se to nestalo?

1) Zajistit pravidelné a bezpečné zálohování informací, o které nechcete přijít (včetně měsíčních záloh uchovávaných nejméně po dobu 6 měsíců zpětně).[30]
    - *Doporučujeme zajištění ze strany dodavatele.*
2) Zajistit, že zálohy máte uložené fyzicky mimo ordinaci pro případ krádeže, požáru, zašifrování prostřednictvím ransomware nebo obdobné situace.
    - *Doporučujeme zajištění ze strany lékaře.*
3) Zajistit pravidelné zálohování nastavení systémů a zařízení.
    - *Doporučujeme zajištění ze strany dodavatele.*

2.1.9 Zaměstnanci a dodavatelé (9 z 10+1)

Zaměstnanci jsou dlouhodobě považováni za největší hrozbu v oblasti kybernetické bezpečnosti. Obsluhují počítače, zdravotnické prostředky a další zařízení v ordinaci, která jsou řízena pomocí software, a tento software může být napaden. Zaměstnanci jsou myšleni zejména zdravotní sestry a další lékaři, kteří sdílí ordinaci. Rizika však představují i dodavatelé, kteří zajišťují správu a nastavení IT prostředků a komunikačních sítí a jsou kontaktem, kam se lékař obrací v případě IT problémů. Je však potřeba myslet i na další dodavatele, kteří poskytují služby lékaři. Mezi tyto typicky patří dodavatelé zajišťující bezpečnostní služby,

[29] Pro oblast fyzické bezpečnosti je možné využít kap. 9 Fyzická bezpečnost na straně č. 18 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[30] Pro oblast zálohování je možné využít kap. 15.3 Zálohování na straně č. 31 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

úklidové služby a dodavatelé zdravotnických prostředků. Dodavatelé jsou však i poskytovatelé Ambulantního informačního systému.

Co by se mohlo stát?

Rizik, které představují zaměstnanci a dodavatelé, je mnoho. Zaměstnanci mají přístup k informacím jako lékař a mohou tak nahlédnout do zdravotnické dokumentace pacientů. Může tak dojít k úniku těchto citlivých osobních údajů. Stejně tak může ze strany zaměstnance dojít k zanesení škodlivého kódu do počítače. V případě sporů a ukončení zaměstnaneckého poměru se zaměstnancem může také dojít k takovému jednání zaměstnance, který se bude snažit uškodit zaměstnavateli.

Obdobně jako v případě zaměstnanců je potřeba si při výběru prověřovat i dodavatele. Zejména jaká je jejich spolehlivost, důvěrnost, jestli není zadlužený apod. V případě výběru nespolehlivého dodavatele, např. dodavatele internetu nebo správce interní sítě, tak může dojít k výpadku internetu a dodavatel zahájí opravu až po týdnu. Stejně tak může ze strany dodavatele dojít k úniku citlivých informací (např. při zálohování dat).

Co dělat, aby se to nestalo?

1) Zajistit sběr informací o zaměstnanci před jeho náborem, zejména s ohledem na hrozby, které může představovat.
    - *Doporučujeme zajištění ze strany lékaře.*
2) Zajistit, aby součástí pracovní smlouvy se zaměstnanci byla dohoda o mlčenlivosti a také, aby byl zaměstnanec povinen dodržovat bezpečnostní opatření v oblasti kybernetické bezpečnosti.
    - *Doporučujeme zajištění ze strany lékaře.*
3) Zajistit pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti.[31]
    - *Doporučujeme zajištění ze strany lékaře.*
4) Zajistit sběr informací o dodavateli před uzavřením smlouvy, zejména s ohledem na hrozby, které může představovat.[32]
    - *Doporučujeme zajištění ze strany lékaře.*
5) Zajistit, aby součástí smlouvy s dodavatelem byla dohoda o mlčenlivosti a také, aby byl dodavatel povinen dodržovat bezpečnostní opatření v oblasti kybernetické bezpečnosti.
    - *Doporučujeme zajištění ze strany lékaře.*
6) Zajistit, že při ukončení smluvního vztahu se zaměstnancem dojde k navrácení všech prostředků a také že dojde k odebrání všech přístupů do informačních systémů.
    - *Doporučujeme zajištění ze strany lékaře.*
7) Zajistit, že při ukončení smluvního vtahu s dodavatelem dojde k odebrání všech přístupů do informačních systémů.
    - *Doporučujeme zajištění ze strany lékaře.*

[31] Pro oblast vzdělávání bezpečnostního povědomí zaměstnanců je možné využít metodický materiál Plán rozvoje bezpečnostního povědomí, který je dostupný na https://ncez.mzcr.cz/cs/kyberneticka-bezpecnost/metodika-kyberneticke-bezpecnosti

[32] Pro oblast řízení dodavatelů je možné využít metodický materiál Metodiku řízení dodavatelů dostupnou na https://ncez.mzcr.cz/cs/kyberneticka-bezpecnost/metodika-kyberneticke-bezpecnosti

2.1.10 Hesla a přihlašování (10 z 10+1)

Přihlašování do počítače, mobilních zařízení a informačních systémů je dlouhodobým a přetrvávajícím problémem všech uživatelů. Důležité je při přihlašování využívat silná hesla, která budou splňovat požadavky na bezpečné heslo – minimálně 12 znaků v kombinaci malých písmen, velkých písmen, číslic a speciálních znaků. Heslo by nemělo obsahovat lehce zjistitelné údaje, např. jméno manželky, jméno psa, datum narození apod. Vhodné je využívání kromě přihlašování heslem i použití druhého faktoru (např. prostřednictvím SMS, Google Authenticator apod.) v závislosti na možnostech přihlašování do zařízení informačního systému. Častým problémem je zapamatování si silných hesel.

Často se bohužel stává, že přestože má uživatel silné přihlašovací heslo, toto heslo má volně dostupné (např. dostupné na lístečku na monitoru, uložené v peněžence apod.) Z tohoto důvodu je vhodné využívat správce hesel pro bezpečné uchování hesel a také pro neustálou dostupnost těchto hesel. U správce hesel stačí uživateli znát pouze jedno silné heslo a má přístup ke všem heslům uložených v této aplikaci.

Důležité je také používání rozdílných hesel pro pracovní a soukromé účely. V případě vyzrazení např. hesla do aplikace Facebook by se mohl útočník lehce dostat do pracovního e-mailu a obráceně.

Co by se mohlo stát?

Pokud dojde k využívání slabého hesla, je pro současné kybernetické útočníky jednoduché jejich odhalení a pokud není využíván i druhý faktor, útočník tak může získat přístup do informačního systému nebo k e-mailové schránce lékaře. Stejně tak při ztrátě notebooku, mobilního telefonu nebo USB flash disku bez požadavku na přihlášení pomocí zabezpečení (hesla, biometrického údaje) se tak útočník nebo nálezce dostane ke všem informacím uložených na těchto zařízeních.

Co dělat, aby se to nestalo?

1) Zajistit, aby přihlašování do všech využívaných zařízení a informačních systémů bylo podmíněno bezpečným heslem nebo v případě možnosti biometrickými údaji.[33]
    - *Doporučujeme zajištění ze strany lékaře.*
2) Zajistit tam, kde je to možné, aby byl k přihlašování využíván i druhý faktor.[34]
    - *Doporučujeme zajištění ze strany lékaře.*
3) Zajistit, že jedno heslo není využíváno pro přihlašování k více službám, zařízením a systémům s důrazem na rozdílnost pro pracovní a soukromé účty.
    - *Doporučujeme zajištění ze strany lékaře.*
4) Zajistit vhodnou bezpečnost hesel využíváním správce hesel (nepoužívat správce hesel v prohlížeči).
    - *Doporučujeme zajištění ze strany lékaře.*

[33] Pro oblast hesel je možné využít kap. 10.3 Politika hesel pro uživatelské účty na straně č. 21 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

[34] Pro oblast vícefaktorového přihlašování je možné využít kap. 10.3 Politika hesel pro uživatelské účty strana č. 21 Minimálního bezpečnostního standardu https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

2.1.11 Co dělat, když se něco stane? (11 z 10+1)

Může se stát, že přes dodržování všech bezpečnostních opatření uvedených v tomto dokumentu dojde k situaci, kdy se lékař stane obětí kybernetického útoku, kdy může dojít k zašifrování počítače, ztrátě zdravotnických dokumentů v listinné nebo elektronické podobě nebo ke ztrátě přihlašovacích údajů. Dále se může stát, že dojde k selhání počítače, serveru nebo dalších využívaných zařízení v důsledku požáru, nebo zaplavení místnosti nebo daného zařízení.

Pro všechny tyto případy je nezbytné mít nastavený scénář, co dělat a na koho se obrátit, aby nedošlo k dlouhodobému výpadku fungování ordinace v závislosti na nedostupnosti jednotlivých zařízení, internetu nebo informačního systému, případně byly způsobené škody co nejmenší.

Co by se mohlo stát?

V případě, že dojde k úniku informací nebo nedostupnosti zařízení, internetu nebo informačního systému, může být významně ovlivněno normální fungování ordinace. V takovém případě je lékař závislý na dodavateli, který by měl přispěchat s pomocí co nejdříve tak, aby se ordinace a lékař mohli co nejrychleji vrátit k běžné praxi.

Co dělat, aby se to nestalo?

1) Vytvořit si plán co dělat, kam volat, na koho se obrátit v případě problémů spojených se zařízeními, informačními systémy apod.[35]
    - *Doporučujeme zajištění ze strany lékaře.*
2) Jednou za rok si vyzkoušet daný plán na nečisto, ověřit si, že telefonní čísla fungují a že je dodavatel dostupný.
    - *Doporučujeme zajištění ze strany lékaře*

[35] Vzor takového plánu je možné najít v Minimálním bezpečnostním standardu v na straně č. 40 https://www.nukib.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

2.2 Oblasti kybernetické bezpečnosti – shrnutí

Oblast kybernetické ochrany	Činnost	Zajišťuje lékař	Zajišťuje dodavatel
Školení a vzdělávání	Seznámit se s tímto dokumentem a řídit se jím. Toto seznámení zajistit u zdravotní sestry a dalšího personálu ordinace	X	
	Pravidelně absolvovat školení v oblasti kybernetické bezpečnosti	X	
Aplikace a systémy	Nastavit oprávnění a přístupy k informačním systémům a aplikacím		X
	Přihlašovat se prostřednictvím silného hesla a druhého faktoru (2FA) všude, kde je to možné		X
	Zálohovat ambulantní informační systém a další kritické systémy		X
	Zakázat spuštění makra v Microsoft Office dokumentech		X
	Nastavit co nejvčasnější aktualizaci informačních systémů, aplikací a operačních systémů		X
	Zajistit bezpečnou konfiguraci webové stránky ordinace		X
	Využívat pouze oficiální operační systémy		X
	Využívat webový prohlížeč pouze pro pracovní účely a nenavštěvovat nebezpečné stránky	X	
Počítače	Zajistit přihlašování prostřednictvím silného hesla do počítačů		X
	Zajistit vypínání počítačů, odhlášení uživatele nebo uzamknutí monitoru a klávesnice v případě nepřítomnosti.	X	

Oblast kybernetické ochrany	Činnost	Zajišťuje lékař	Zajišťuje dodavatel
	Zajistit zálohování informací notebooku		X
	Zajistit nastavení antivirové a antispamové ochrany		X
	Zajistit nastavení firewallu		X
	Zajistit nastavení šifrování disku		X
	Zajistit bezpečné fyzické umístění notebooku	X	
	Zajistit pravidelnou fyzickou údržbu notebooku před zanesením prachem		X
	Zajistit pravidelnou aktualizaci operačního systému		X
Notebooky	Zajistit přihlašování prostřednictvím silného hesla k notebooku	X	
	Zajistit vypínání obrazovky a notebooku v případě nepřítomnosti	X	
	Zajistit zálohování informací notebooku		X
	Zajistit nastavení antivirové a antispamové ochrany		X
	Zajistit nastavení firewallu		X
	Zajistit nastavení šifrování disku		X
	Zajistit bezpečné fyzické nakládání s notebookem	X	
	Zajistit pravidelnou fyzickou údržbu notebooku před zanesením prachem		X

Oblast kybernetické ochrany	Činnost	Zajišťuje lékař	Zajišťuje dodavatel
	Zajistit pravidelnou aktualizaci operačního systému	X	
Mobilní telefon	Zajistit přihlašování prostřednictvím biometrického údaje	X	
	Zajistit nastavení antivirové a antispamové ochrany		X
	Zajistit nastavení zálohování informací mobilního telefonu		X
	Zajistit bezpečné fyzické nakládání s mobilním telefonem a vyhnutí se jeho ztrátě	X	
	Zajistit aktualizaci operačního systému	X	
	Zajistit stahování aplikací pouze z ověřených zdrojů	X	
	Zajistit nastavení hlídání polohy zařízení.	X	
	Zajistit nastavení vzdáleného výmazu zařízení.	X	
Síťová ochrana	Zajistit neustále aktuální operační systém u prvků síťové ochrany (routery, switche)		X
	Využívat silné heslo k Wi-Fi		X
	Oddělit provozní a pacientskou datovou a Wi-Fi síť		X
	Změnit přístupové heslo do administrace prvků síťové ochrany		X
	Zajistit firewallovou ochranu sítě		X
Fyzická bezpečnost	Zajistit fyzickou bezpečnost a optimálně uzamykání fyzických dokumentů o pacientech. Následně neponechávat klíč k této kartotéce volně dostupný.	X	

Oblast kybernetické ochrany	Činnost	Zajišťuje lékař	Zajišťuje dodavatel
	Zajistit fyzickou bezpečnost mobilních zařízení a médií	X	
	Zajistit kontrolu fyzického přístupu do ordinace tak, aby se tam nedostala neoprávněná osoba	X	
	Zajistit záložní zdroj elektrické energie UPS		X
	Zajistit pravidelnou péči o hardware a profylaxi		X
	Zajistit prázdný stůl a vypnutý počítač při odchodu z ordinace	X	
Zálohování	Zajistit pravidelné a bezpečné zálohování informací, o které nechcete přijít (včetně měsíčních záloh uchovávaných nejméně po dobu 6 měsíců zpětně)		X
	Zajistit, že zálohy máte uložené fyzicky mimo ordinaci pro případ krádeže, požáru, zašifrování prostřednictvím ransomware nebo obdobné situace	X	
	Zajistit pravidelné zálohování nastavení systémů a zařízení		X
Zaměstnanci a dodavatelé	Zajistit sběr informací o zaměstnanci před jeho náborem, zejména s ohledem na hrozby, které může představovat	X	
	Zajistit, aby součástí pracovní smlouvy se zaměstnanci byla dohoda o mlčenlivosti a také, aby byl zaměstnanec povinen dodržovat bezpečnostní opatření v oblasti kybernetické bezpečnosti	X	
	Zajistit pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti	X	
	Zajistit sběr informací o dodavateli před uzavřením smlouvy, zejména s ohledem na hrozby, které může představovat	X	

Oblast kybernetické ochrany	Činnost	Zajišťuje lékař	Zajišťuje dodavatel
	Zajistit, aby součástí smlouvy s dodavatelem byla dohoda o mlčenlivosti a také, aby byl dodavatel povinen dodržovat bezpečnostní opatření v oblasti kybernetické bezpečnosti	X	
	Zajistit, že při ukončení smluvního vztahu se zaměstnancem dojde k navrácení všech prostředků a také že dojde k odebrání všech přístupů do informačních systémů	X	
	Zajistit, že při ukončení smluvního vtahu s dodavatelem dojde k odebrání všech přístupů do informačních systémů	X	
Hesla a přihlašování	Zajistit, aby přihlašování do všech využívaných zařízení a informačních systémů bylo podmíněno bezpečným heslem nebo v případě možnosti biometrickými údaji	X	
	Zajistit tam, kde je to možné, aby byl k přihlašování využíván i druhý faktor	X	
	Zajistit, že jedno heslo není využíváno pro přihlašování k více službám, zařízením a systémům s důrazem na rozdílnost pro pracovní a soukromé účty.	X	
	Zajistit vhodnou bezpečnost hesel využíváním správce hesel	X	
Co dělat, když se něco stane?	Vytvořit si plán co dělat, kam volat, na koho se obrátit v případě problémů spojených se zařízeními, informačními systémy apod	X	
	Jednou za rok si vyzkoušet daný plán na nečisto, ověřit si, že telefonní čísla fungují a že je dodavatel dostupný	X	

3 Bezpečnostní jedenáctero (10+1)

Prázdný stůl a vypnutý monitor

Pokud odcházíte od počítače, zamkněte jej (Win+L) a papírové dokumenty bezpečně uložte. Nikdy nenechávejte papírové dokumenty obsahující citlivé informace (zdravotnické) bez dozoru, po vytisknutí je ihned odeberte z prostoru tiskárny.

Podezřelé e-maily

Neklikejte bez rozmyslu na odkazy, obrázky a přílohy v e-mailech. Raději dvakrát zkontrolujte odesílatele e-mailu. Ověřte si, že se jedná o legitimní požadavek odesílatele (např. zpětným zavoláním).

Uchování informací

Dokumenty s informacemi o pacientech uchovávejte pouze uzamykatelných skříních / kartotékách nebo místnostech. Neukládejte pracovní informace na veřejná úložiště, např. uloz.to.

Užívání internetu

Internet užívejte pouze pro pracovní účely, nikoliv k zábavě jako sledování Youtube, hraní her apod. Nestahujte žádné aplikace a další soubory, protože mohou obsahovat škodlivý kód a ochromit tak provoz ordinace. Využívejte oddělené Wi-Fi sítě pro ordinaci a pacienty.

Používání mobilních zařízení

Nenechávejte svá mobilní zařízení (notebook, mobilní telefon) bez dozoru. Pravidelně aktualizujte operační systém a aplikace. Nepřipojujte cizí soukromá zařízení do interní sítě ordinace.

Hesla a přihlašování

Zvolte si silná hesla obsahující alespoň 12 znaků včetně čísla, velkého písmena a zvláštního symbolu např. 4fk8_7hPRuj5+2. S nikým heslo nesdílejte a nepiště si ho na viditelné místo. Nepoužívejte pracovní heslo na více místech např. k soukromým aplikacím. Využívejte pro ukládání hesel správce hesel.

Chování na sociálních sítích

Na veřejném profilu (Facebook, LinkedIn apod.) neuvádějte svůj pracovní e-mail a telefonní číslo. Nesdílejte informace, které by Vás mohly kompromitovat.

Vzdálený přístup

Při práci mimo prostory ordinace dbejte zvýšené pozornosti, nikdy nevíte, kdo se Vám dívá přes rameno. Nevyužívejte veřejně dostupná bezdrátová připojení Wi-Fi, např. v kavárně, na nádraží apod. Využívejte šifrované kanály VPN.

Řešení problémů

Pokud si nejste jisti nebo Vám přijde chování počítače nebo jiného zařízené podezřelé, radši to konzultujte se svým dodavatelem IT.

Dodavatelé

Kybernetickou bezpečnost nelze nastavit bez dodavatelů, kteří se starají o technická nastavení informačních systémů a zařízení. Proto je potřeba najít spolehlivého a bezpečného dodavatele.

Zálohování

Abyste předešli ztrátě informací, je nezbytné pravidelně zálohovat své informace na jiné zařízení a následně ho odpojit. Zálohování je potřeba provádět u počítačů, notebooků, mobilních telefonů, ale zejména u ambulantního informačního systému.

4 Typická aktiva praktického lékaře a malé ambulance

Níže je uveden rozpad typické ordinace praktického lékaře nebo malé ambulance s dekompozicí na jednotlivá aktiva pro potřeby kybernetické bezpečnosti.

4.1 Personál:

- Lékař
- Zdravotní sestra

4.2 Dodavatel:

- Dodavatel IT (HW/SW) – nastavit antivir, zálohování, firewall, update Windows
- Dodavatel IS (Ambulantní IS, E-mail)
- Správce budovy včetně energií
- Bezpečnostní a úklidová služba

4.3 Hardware:

- Počítač a/nebo notebook (dle velikosti personálu) včetně monitoru, klávesnice a myši
- Chytré zdravotnické prostředky (přenášející informace na koncovou stanici)
- Mobilní telefony
- Notebook
- Pevná linka
- Kovová kartotéka
- Multifunkční tiskárna (včetně skeneru)
- Vyvolávací systém
- Modem (router)
- Zálohovací zařízení

4.4 Informační systém a aplikace:

- Ambulantní informační systém
  - IS eRecept (pokud není napojen na AIS)
  - IS eNeschopenka (pokud není napojen na AIS)
- Elektronická pošta
- Datová schránka
- Webový prohlížeč
- Webové stránky ordinace
- Objednávkový systém (často součástí webových stránek ordinace)
- Kvalifikovaný certifikát

4.5 Komunikační síť:

- Ethernetový kabel
- Wi-Fi

4.6 Objekty

- Čekárna
- Ordinace

5 Praxe

Před zpracováním kybernetické příručky pro lékaře byla provedena analýza využívání technologií u třech praktických lékařů s různou vyspělostí kybernetické bezpečnosti.

Níže jsou uvedeny základní informace o běžné praxi těchto tří praktických lékařů.

5.1 Praktický lékař č. 1 (větší využívání digitálních technologií)

Ordinace více praktických lékařů

Základní informace:

- 3 ordinace ve dvou lokalitách Prahy

Seznam aktiv:

- Celkem 7 koncových stanic, které jsou vzájemně propojeny
- V každé lokalitě je NAS server pro ukládání a sdílení informací
- Server pro SmartMedix v každé lokalitě
- IS Sestraemmy
  - (https://www.sestraemmy.cz/)
  - SAAS pro objednání k lékaři
  - Pacient se registruje (přes RČ)
  - 2FA není vyžadován
- IS SmartMedix
  - (https://www.medax.cz/index.php)
  - 25 tis/rok/licenci
  - SAAS pro vedení zdravotnické dokumentace výkon zdravotnické péče
  - IS je napojen na laboratoře pro sdílení informací
  - Napojení na pojišťovny pro výkaz činností
  - Každý uživatel má vlastní účet
  - Všichni vidí všechny pacienty
  - Celkem 4 zálohy
  - Zdravotnické prostředky jsou síťově napojeny
- IS eZprava
  - (https://ezprava.net/)
  - SAAS pro elektronickou komunikaci mezi zdravotnickými pracovišti
- IS Google Mail

    - SAAS – bezplatná verze pro elektronickou komunikaci
- Správce IT
    - Zajišťuje dodavatel
- VPN
    - Vzdáleně se připojují ke koncové stanici
- Internetová konektivita
    - O2
- Wi-Fi pro pacienty
- Zdravotnické prostředky chytré
    - EKG
- Tiskárny

Způsob práce:

- Všechny fyzické zprávy se skenují do digitální podoby
- Žádanky na vyšetření pouze v tištěné podobě
- Zprávy (rentgen) získávají elektronicky, nepotřebují obraz, stačí textová podoba
- S ostatními praktickými lékaři komunikují přes eZpravu
- Koncové stanice jsou neustále zapnuty (VPN)
- Pacienti se objednávají v 50 % vzdáleně přes SestraEmmy
- Fyzický vstup přes tři dveře a kódovací zámek
- Jednou měsíčně schůzka ordinace – řešení se bezpečnostní požadavky, které jsou součástí zápisu
- USB a CD nevyužívají
- Cca 1800 pacientů na jednoho praktického lékaře

5.2 Praktický lékař č. 2 (využívání digitálních technologií)

Ordinace 1 praktického lékaře

Základní informace:

- 1 ordinace v Praze

Seznam aktiv:

- Celkem 2 koncové stanice (1 doktor, 1 sestra)
- Provádějí zálohy lokálně a na externí USB flash disk
- IS AIS
    - https://aiscz.cz/
    - 8 tisíc/licenci/rok
    - Lokální IS pro vedení zdravotnické dokumentace a výkon zdravotní péče
    - Servis je zajišťován vzdáleně přes dodavatele
- E-mailová komunikace
    - Koupena vlastní doména
- Internetová konektivita
    - Od poskytovatele internetové konektivity
    - Nastavení provádí poskytovatel a doktor sám
- Koncová stanice
    - Podporovaný Windows 10

    - Antivirová ochrana Kaspersky (mj. požadavek na certifikáty)
- USB flash disk pro zálohování
- Datová schránka – pro posílání informací mezi pacienty
- Soukromý notebook a mobilní telefon
- Tiskárny

Způsob práce:

- Přemýšlel o zálohování do cloudu, ale zatím nevyužívá
- Rezervace není běžná, když už tak telefonicky
- Kompletní správu PC si zajišťuje lékař sám
- Wi-Fi pro pacienta není žádoucí
- Žádný zdravotnický prostředek není připojen k AIS
- Zprávy (rentgen) získávají elektronicky, nepotřebují obraz, stačí textová podoba
- Dokumenty v papírové podobě se nekopírují do digitální podoby
- Pacienti přes e-mail zasílají zdravotnickou dokumentaci
- Není potřeba práce z domova
- Klíče od ordinace 3x (doktor, sestra, fyzická ostraha)
- Žádanky na vyšetření pouze v tištěné podobě
- USB a CD nevyužívají
- Cca 1800 pacientů na jednoho praktického lékaře

5.3 Praktický lékař č. 3 (využívání digitálních technologií v rámci nemocnice)

Ordinace praktického lékaře je součástí fakultní nemocnice.

Základní informace:

- 1 ordinace v jedné lokalitě
- NIS Medea
- Podpis na flash disku pro eRecept

Seznam aktiv:

- NIS Medea není propojen s dalšími IS
- Windows 11
- LAN
- Zapnutý firewall + antivir
- Všechno MEDEA, žádný jiný IS nepotřebuje
    - Výsledky se centrálně neposílají
- Tiskárna, skener

Způsob práce:

- Objednávky přes telefon a také e-mailem
- Posílají eNeschopenky a eRecept na mobilní telefon
- Nepotřebují žádné chytré zdravotnické zařízení
- V případě problémů volají normálně na IT support
- 30–50 pacientů denně
- Všechny dokumenty elektronicky + papírově

6 Konkrétní aktiva

6.1 Ambulantní informační systémy

- Medicus
- PC Doktor – CompGroup
- Amicus
- Praktik
- WinMed
- AIS
- Medicalc
- TurboAsistent
- SmartMedix

6.2 Přenos informací mezi praktiky

- eZprava
- Datová schránka
- E-mailová komunikace (z důvodu zabezpečení předávaných informací je nutné přílohy chránit heslem, které bude zasláno jiným kanálem, např. prostřednictvím SMS)

6.3 Přenos informací mezi praktikem a pacientem

- Fyzicky
- E-mailem (z důvodu zabezpečení předávaných informací je nutné přílohy chránit heslem, které bude zasláno jiným kanálem, např. prostřednictvím SMS)

Citace dle ČSN ISO 690:2022:

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY, **Kybernetická příručka pro lékaře,** verze dokumentu 1.0. Praha, 2023. Licencováno pod CC BY 4.0, licenční podmínky dostupné z: http://creativecommons.org/licenses/by/4.0/.