Technologie ve SLUŽBÁCH

Kybernetická bezpečnost pro manažery v sociálních službách.

Kybernetická bezpečnost je téma, jehož význam stoupá rovnoměrně s tím, jak se zvyšuje množství informačních systémů, které jsou v sociálních službách využívány a jak stoupá množství dat, které do nich zaměstnanci ukládají. Stačí se ohlédnout o pár let zpátky a uvědomit si, jak rychle se záznamy z papírových sešitů a složek přesunuly do jednoduchých dokumentů na lokálních discích počítačů a jak se teď téměř překotně přesouvají do informačních systémů, které jsou schopny propojovat více zaměstnanců v organizaci.

Na zaměstnance i management kladou tyhle změny poměrně vysoké nároky. Možná si také pojďme nalít čistého vína – studijní a vzdělávací obory, které do sociální práce směřují si vybírají humanitně orientovaní lidé, kteří chtějí mírnit lidské starosti a trápení a technologie často stojí na okraji jejich zájmu.

Je nejvyšší čas si přiznat, že informační technologie, internet a digitalizace dat nutně mění naše pracovní postupy. Tento trend je velmi intenzivní a nevyhne se žádné oblasti, tedy ani sociálním službám (a to ani tehdy, když si to budeme usilovně přát 😊.)

O digitalizaci se dá diskutovat z mnoha úhlů pohledů, dnešní článek si z nich vybírá právě problematiku kybernetické bezpečnosti.

Jak si představit kybernetickou bezpečnost?

Při práci s informačními technologiemi se prostřednictvím technických zařízení pohybujeme v digitálních světech o jejichž vlastnostech a umístění mají běžní uživatelé často jen málo informací a přiznejme si, že se ani příliš nezajímají o to, jestli se v prostředí „divokého internetu“ pohybují alespoň s jistou opatrností. Zdá se to totiž nepodstatné, protože práci s informacemi lidský mozek jednoduše nehodnotí jako nebezpečnou. Zdánlivě nás při ní totiž nemůže nikdo ohrozit, okrást nebo zranit. Tenhle klamný pocit může vést k řadě negativních důsledků, které mohou velmi nepříjemně dopadnout na soukromý život každého jedince a pracovní prostor kterékoliv organizace.

To, že se v běžném životě chováme bezpečně, si skoro neuvědomujeme. K majetku a cenným věcem se téměř automaticky chováme ochranitelsky. Zamykáme domy i auta, schováváme si dobře klíče, cennosti ukládáme do trezorů nebo alespoň pod matraci. Případnému zcizení nebo poškození majetku tak bráníme prostřednictvím fyzických opatření.

Samozřejmostí je také to, že se chováme rozumně. Když přenášíme něco cenného, vybíráme si osvětlené cesty. Tím, že máme v peněžence větší částku peněz se rozhodně příliš nechlubíme, ani nikomu nesdělujeme, kam se s penězi chystáme jít. Jsme obezřetní a používáme k tomu vlastní rozum a opatrnost, tedy „měkká opatření“.

Kybernetická bezpečnost staví na stejných principech. Velmi zjednodušeně řečeno kombinuje fyzické zabezpečení informačních systémů a celých počítačových sítí s „měkkými“

opatřeními, k nimž nepochybně patří dobré znalosti lidí, kteří se systémy pracují a soubor respektovaných, všemi uživateli dodržovaných pravidel.

Co může pomoci při zlepšování kybernetické bezpečnosti?

Je zřejmé, že před zařízeními sociálních služeb nestojí ve frontě experti na ICT, aby manažerům pomohli v procesu zlepšování kybernetické bezpečnosti. Možná to ani v první chvíli není to nejzásadnější, protože tou nejdůležitější informací je, že za bezpečnost informací v organizaci vždycky zodpovídá management. A věřte, že informace, zejména ty osobní, můžeme bez obav označit za velmi cenné.

Pokud jste tedy součástí managementu, je na vás, jak nastavíte cestu k bezpečnosti vašich systémů, zařízení a informací v nich uložených. Samozřejmě bude velmi užitečné přibrat ke spolupráci experty, kteří zajistí, aby odborná část procesu běžela jako na drátkách, je ale důležité, aby celý proces zůstal pod manažerskou kontrolou. Přizvěte tedy ke spolupráci interního IT zaměstnance, který tématu bezpečnosti rozumí, případně hledejte cestu společně třeba se svým zřizovatelem nebo vlastníkem. Můžete také objednat a přizvat externí experty.

Jak si tedy celý postup nastavit? Nebojte se využít doporučení, která vydává Národní úřad pro kybernetickou bezpečnost (NÚKIB), který je pro ČR tou nejpovolanější autoritou. Na jeho webových stránkách najdete dokument „Minimální bezpečnostní standard“, který je určen právě pro organizace, které do tajů cybersecurity začínají pronikat a nevztahují se na ně podmínky dané zákonem o kybernetické bezpečnosti. Dokument je prakticky rozdělen na část manažerskou a technickou a je psán poměrně vlídnou směsí ajťáčtiny a běžné češtiny, takže se v něm neztratíte.

V manažerské části si ujasníte, že:

1. Podpora ze strany managementu je v každé organizaci tím základním předpokladem, které umožní systematický přístup a zlepšování.
    - Rolí managementu je nastavení celého procesu změny k němuž patří posouzení současné situace při níž doporučujeme na chvilku odložit růžové brýle a uvědomit si reálný stav ICT v organizaci a naplánovat postup krok za krokem společně s odborníky.
    - Je zásadní zajistit nastavení pravidel a zachytit je v písemné dokumentaci (politice).
    - Neusnout na vavřínech, když jsou politiky schváleny, ale v dohodnutých intervalech sledovat dodržování postupů dohodnutých v dokumentaci a podporovat další zlepšování.

2. Byste měli krok za krokem zdolat následující úkoly:
    - Uzavření smluv o mlčenlivosti (setkáte se s ní také jako s „NDA“ - non disclosure agreement) se všemi administrátory a osobami, které ve vaší kyberbezpečnosti zastávají nějaké role
    - Vytvoření přiměřených opatření, která je nutno dodržovat v organizaci. Tato opatření pak promítnout do dokumentu - politiky, který bude schválen

podobně jako ostatní dokumenty, které ovlivňují interní chod organizace tak, aby byla pro všechny (včetně vás samotných) závazná.

- Plánování – nejlépe vytvoření „plánu zavádění bezpečnostních opatření“. Pokud do něj připojíte harmonogram, pomůže vám sledovat, jestli se vám daří řešit to, co jste si předsevzali. Plánujte tak, abyste zvyšovali nároky, postupně a v souladu s tím, jak stoupají znalosti, dovednosti a technické možnosti organizace. Není potřeba chtít vše najednou. Zkuste to pěkně postupně.
- Třídění informací v organizaci je důležitým úkolem a umožní správně postupovat v souladu s citlivostí informací. Téměř jistě se setkáte s informacemi veřejnými, které v zásadě žádné zvláštní zacházení nevyžadují, ale také s informacemi interními a citlivými/důvěrnými, kdy už je žádoucí určit, kteří zaměstnanci s nimi mohou pracovat a za jakých podmínek. Toto třídění vám také umožní stanovit pravidla vnitřního provozu a určit ty informace, které jsou pro organizaci klíčové a citlivé, protože právě ty je potřeba zvláště dobře zabezpečit.
- Řiďte práci svých dodavatelů. Zařaďte do smluv ustanovení o bezpečnosti a mlčenlivosti, ale také stanovte, jak váš dodavatel může nakládat s daty a jaké jsou jeho povinnosti. Pamatujte si, že ve váš prospěch bude nastavena jen taková smlouva, jejíž přípravu budete mít sami pod kontrolou.

3. Rozvíjejte gramotnost a vzdělanost zaměstnanců organizace, aby se mohli naučit „být kyber“.
   - Školte, školte, školte. Podpořte zaměstnance, aby měli k dispozici dostatek vysvětlujících informací, pořádejte školení, diskuse, zaveďte třeba online vzdělávání
   - Seznamte zaměstnance s dokumenty/politikami a vyžadujte jejich dodržování. Buďte si jisti, že všemu rozumí
   - Naučte zaměstnance hlásit podezřelé situace – incidenty. Pokud rozeznají nebezpečnou situaci (např. kliknou na neověřený odkaz v e-mailu), musí vědět, že je bezpečné, když takový incident nahlásí a že je potřeba to udělat neprodleně.
   - Připravte soubor školení pro nové zaměstnance a potřebné informace jim předejte co nejdříve
   - Pečujte o průběžné vzdělávání administrátorů, „ajťáků“ a zaměstnanců, kteří v rámci kyberbezpečnosti zastávají speciální role.
   - Pokud se ve vaší organizaci, ale i v okolí, objeví nebezpečná situace, která ohrozila/ohrožuje bezpečnost informací, uspořádejte mimořádné školení a předejte informace.
   - Přečtěte si, co o vzdělávání v kyberbezpečnosti tvrdí třeba výše uvedený NÚKIB. Určitě se v mnohém zorientujete.

4. Nezapomeňte řídit změny a postupovat kontinuálně tak, aby znalosti a opatření v organizaci postupovala rovnoměrně a plynule

5. Nechte nezávislé odborníky, aby se podívali, jak na tom jste. Můžete třeba objednat audit, nebo si najít experta, který vás celým procesem doprovodí, postará se o vstupní analýzu a naleje vám pro začátek „čistého vína“.

Jakmile budete mít jasno v tom, co organizace používá a jaká jsou rizika s ohledem na kybernetickou bezpečnosti, bude ten pravý čas pro vytvoření zadání pro řešení technických témat. Abychom si to pro začátek zjednodušili, je pro vás připraveno **desatero kroků** ke kybernetické bezpečnosti pro začátečníky a mírně pokročilé

1. Staráme se o **fyzickou bezpečnost** své počítačové sítě: vše, co používáme skutečně zabezpečíme. Do množiny opatření patří např. zamykání kanceláří a dalších prostor, zajištění kamerami, ale také třeba klimatizace k serverům a zhášecí systémy, které nedopustí, aby došlo k požáru.
2. **Řídíme, kdo do naší počítačové sítě vstupuje z vnějšího světa**. K tomu je užitečné používat tzv. firewall. Ne nadarmo se tohle zařízení v překladu nazývá „ohnivá zeď“. Slouží totiž jako ochranka, která umožní vstoupit do počítačové sítě jen takovým službám a uživatelům, kterým to výslovně povolíte. Firewall může prostřednictvím svého nastavení také zakazovat přístup interních uživatelů k nebezpečným aplikacím. Slouží tedy jako užitečný, stále bdělý vrátný.
3. **Řízení přístupů**, tedy zajištění toho, aby se ke konkrétním prvkům počítačové sítě a do informačních systémů a jejich částí dostali pouze ty osoby, které mají oprávnění a důvod s nimi pracovat. Jednoduše řečeno – aby každý viděl jen to, co vidět má.
4. Nezapomeňte si definovat **pravidla pro mobilní zařízení**, která se připojují do vaší interní sítě. Dejte si pozor např. na „univerzální“ telefony – tedy takové, které vaši zaměstnanci používají v soukromí a současně pro svoji práci.
5. Vytvořte pravidla pro tvorbu přístupů. Vyřešte, kteří zaměstnanci mají mít přístup do konkrétních systémů, kdo bude jejich účty zakládat, měnit v případě potřeby, ale také rušit.
6. Věnujte se heslům – určete pravidla pro přihlašování a práci s hesly. Nastavte délku hesel a jejich složení, vysvětlete zaměstnancům, že svá hesla musí chránit a nesdělovat je. Přístupy do systémů, kde zaměstnanci používají společné jméno a heslo nahraďte individuálními přístupy.
7. Mějte rozdělenou (segmentovanou) počítačovou síť tak, aby byly oddělené její části tam, kde to je rozumné. Např. lze oddělit síť pro klienty, zaměstnance, ekonomické úseky, zdravotnictví. Případně síť pro připojování zařízení rodin klientů nebo pro dobrovolníky.
8. Mějte zálohy – postarejte se, aby vaše systémy ukládaly zálohy nejméně na 2 na sobě nezávislých místech. V případě selhání nebo napadení některého systému z nich bude možné systém obnovit.
9. U citlivých dat používejte šifrování. Nezapomeňte šifrovat přenosné nosiče, jako jsou flash disky.
10. Nebojte se cloudových služeb – umístění systémů a dat mimo vaši organizaci v dobře vybavených centrech je trendem doby a může řadu otázek z pokročilejší kyberbezpečnosti dobře vyřešit v rámci poskytované služby.

Pár slov o NIS 2

V roce 2024 můžeme očekávat v ČR řadu změn a nová opatření, která budou posilovat úroveň kybernetické bezpečnosti. Evropská Unie se tomuto tématu věnuje ve směrnici „o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii“, která je také označována jako směrnice NIS2. V ČR budou změny promítnuty do nového zákona o kybernetické bezpečnosti, který by se měl celé naší společnosti dotknout právě v roce 2024.

Za důležité lze považovat to, že se změny nově dotknou velkého množství organizací, které doposud žádné povinnosti plnit nemusely a v budoucnu se budou muset kybernetické bezpečnosti aktivně věnovat. Jak tedy nové podmínky ovlivní práci v segmentu sociálních služeb? Přílohy směrnice definují 60 služeb, které budou v blízké budoucnosti kybernetickou bezpečnosti aktivně řídit a plnit podmínky vyplývající ze směrnice.

Ačkoliv mezi nimi sociální služby taxativně vyjmenovány nejsou, rozhodně by měly vývoj pozorně sledovat všechny, ale zejména ty organizace, které kromě sociálních poskytují také služby zdravotní. Na zdravotnictví se totiž směrnice vztahuje. Pokud tedy organizace poskytuje kromě sociálních také zdravotní služby a současně má více než 50 zaměstnanců, nelze doporučit nic menšího, než situaci pozorně sledovat a případně se na ni zvolna začít připravovat třeba právě implementací Minimálního bezpečnostním standardu NUKIB o který se celý tento článek snaží opírat.

Závěrem

Digitalizace tady je už s námi zůstane. Přináší mnoho zajímavých užitků, ale také nové výzvy. K těm rozhodně patří péče o kybernetickou bezpečnost. Jestli je potřeba mít z této změny obavy? Neřekla bych. Daleko lepší bude se do ochrany dat organizace pustit a krok za krokem se v této práci zlepšovat a u toho neustále myslet na to, že během své práce získávají organizace řadu informací o svých klientech. A ty (ale nejen ty) je potřebné účinně chránit.

Přečtěte si:

1. Minimální bezpečnostní standard NUKIB - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/
2. Informace o směrnici NIS2 - https://osveta.nukib.cz/course/view.php?id=145
3. Kurz Základy kybernetické bezpečností – Dávej kyber - https://osveta.nukib.cz/course/view.php?id=123
4. Kurz Senior proti internetovým padouchům - https://osveta.nukib.cz/course/view.php?id=140
5.