Technologie v sociálních službách

Kudy vede cesta k asistivním technologiím? – Postarejme se o bezpečnost informací

Naše první společně zamýšlení nad technologiemi v sociálních službách se pokusilo otevřít téma asistivních technologií. Je to nový pojem, na který si všichni zvykáme a který už-už klepe na dveře všech typů služeb. V některých zařízeních už mu odvážně otvírají, jinde se opatrně vyčkává zkušenosti průkopníků. Vývoj se ale zastavit nedá. Technologie dobývají svět a pronikají do všech oborů. Sociální služby nejsou výjimkou.

Dobrá zpráva je, že máme výhodu v tom, že se můžeme porozhlédnout, poučit, využít zkušenosti odborníků a dobře se připravit. Čekáte teď na špatnou zprávu? Tak se pohodlně usaďte, protože budete čekat dlouho. Špatné zprávy se totiž v této sérii článků nedočkáte. Jen si ten neviditelný technický svět pomaloučku a polehoučku rozmotáme.

V roce 2028

Pojďme se na začátku zasnít a přenést do domova pro seniory v roce 2028. V domově bydlí paní Zvídavá. Je neděle ráno a vypadá to na slunečný den. Pečovatelka, která právě přišla do služby, se právě u paní Zvídavé zastavila, aby jí nabídla dopolední procházku. Může si to dovolit – má na klienty čas. Informační systémy jsou vyladěné tak, že u počítače tráví minimum času. Ráno po každém pokoji „rozhlédl senzor a změřil teplotu. Naměřené hodnoty se automaticky přepsaly do zdravotnické části informačního systému. Pokud se teplota některého z klientů odlišila od normální hodnoty, zpráva přišla zdravotní sestřičce přímo do ruky, aby mohla hned situaci řešit. Senzor změřil taky teplotu v místnosti a pokud to bylo vhodné, zreguloval ji. U klientů, které trápí demence se ráno vypnula elektronická signalizace opuštění pokoje a komunikační zařízení jim právě napovídá, že se mohou jít obléci a připravit k snídani. Paní Zvídavá a další klienti si právě na svých tabletech prohlížejí nové jídelníčky a objednávají jídlo na další týden. Seznam snídaní, obědů a večeří se bez dalšího zásahu lidské ruky shromažďuje v kuchyni. Postele automaticky mění tvrdost matrací tak, aby měli málo pohybliví klienti pohodlí. Když je potřeba, upozorní personál na nebezpečí pádu. Pouhým dotekem prstu si klienti sami mění polohu postele tak, aby se cítili příjemně.

Protože se všechno povedlo dobře propojit a nastavit, staly se technologie velkou pomocí a „pravou rukou“ personálu. Převzaly rutinní práci a pečovatelé se tak mohou více věnovat přímo klientům.

Háček je v tom, že za popisovanou situací roku 2028 je spousta neviditelné práce předchozích let. Práce, kterou není možné ošidit. Není možné se jí vyhnout a doufat, že když-to-není-vidět-tak-to-nebude-vadit.

Ochrana informací – péče o kybernetickou bezpečnost

Důvodů, proč každé ošizení vadí je víc, pojďme si tedy vybrat jeden z nich. Můžeme si posvítit třeba na bezpečnou práci s informacemi. Zůstaňme tedy ještě chvíli v nedělním ránu 2028. Bez zásahu lidské ruky se počítači příslušného domova prohání velké množství nových informací. Jsou to informace čistě digitální a my se o ně musíme naučit správně starat.

Jestli jste se teď rozhodli, že v klidu přeskočíte na další stránku, protože tenhle článek je pro „ajťáky“, ještě počkejte. Doba, kdy počítače patřily technikům je totiž definitivně pryč. Už dávno je z nich běžný pracovní nástroj, který používá každý z nás. A taky za něj každý z nás svým dílem zodpovídá.

Jak je to ale s těmi informacemi, které si vesele víří v infosystémech našeho ukázkového domova? Kdo za ně vlastně zodpovídá a na co bychom měli myslet dřív, než do pokojů klientů umístíme první čidla a než nakoupíme první chytré postele? Na co je tedy potřeba se připravovat už dnes?

Možná je vám to jasné a další odstavce tohoto článku pro vás budou opakováním jednodušším než malá násobilka. Ale možná patříte do skupiny lidí, pro které je bezpečnost digitálních dat zatím spíš pověstnou španělskou vesnicí. Jestli to tak je, vůbec se netrapte – zkusíme ti to postupně vysvětlit. Dobrá zpráva totiž je, že pokud se odhodláte zamyslet se nad tématem kybernetické bezpečnosti, stoupne nejen vaše odbornost v práci, ale lépe se budete umět postarat také o své osobní a rodinné záležitosti. Dneska se už zloději zas tak moc neobtěžují vykrást vám dům. Proč by to taky dělali, když je pro ně jednodušší vloupat se do vašeho bankovního účtu? Je určitě nejvyšší čas naučit se nepouštět hackery – novodobé lupiče do svého pracovního ani soukromého světa.

Proč se musíme o svá digitální data starat? Jejich hodnota je vysoká.

Zjednodušeně řečeno, zajištění bezpečnosti dat je neoddělitelnou součástí péče o klienty v sociálních službách. Je to důležitá, velmi významná a citlivá součást jejich životů. Občas přemýšlím, jestli nějaký jiný typ organizace nebo instituce shromažďuje na jednom místě tolik důležitých informací o lidech a přiznávám, že jsem prozatím nikoho jiného nenašla. Služby „ví“ o každém klientovi mnohé. Znají jeho zdravotní stav, zaznamenávají péči, kterou mu věnují, znají jeho plány a představy vtělené do individuálního plánování, často do detailu zachycují jeho ekonomickou situaci a dotýkají se i rodinných a sociálních vazeb.

Konkrétnější představu si můžeme udělat třeba na příkladu paní Zvídavé. Systém ví, že měla k snídani rohlík se šunkou a sladký čaj a že si odhlásila oběd, což může znamenat, že půjde ven. Ví, kdy si s kým telefonovala i to, že v noci neklidně spala a hodinu nebyla v posteli. Zná všechny její osobní údaje, zdravotní stav za celý dlouhý život. Zná její dětí. Ví také, jak má vysoký důchod a kolik peněz jí z něj každý měsíc zbývá. Paní Zvídavá má vlastní bankovní účet, takže domov nemá celkovou informaci o jejím majetku. Co ale mít může, jsou záznamy o jejích přáních. O tom, že ráda čte a poslouchá vážnou hudbu, o tom, že by ještě chtěla zažít koncert v pražském Obecním domě. A možná by se mohl najít i záznam o tom, jak by si přála prožít své poslední dny a že pokud to půjde, chce zemřít v domově obklopená svou rodinou. Každý z čtenářů si určitě dovede představit spoustu dalších informací, které jsem tady ani nezmínila, a to se zabýváme jen oblastí informací o klientech.

K asistivním technologiím to sice už tolik nepatří, ale pro úplnost je potřeba doplnit, že Informačním ekosystémem kolují také velmi přesné informace o zaměstnancích a o celém provozu organizace. Je zde zachycena náplň každé minuty času a využití každé koruny z rozpočtu.

Co nám hrozí? Únik informací

Je důležité se o shromážděné informační bohatství dobře starat. Jinak by totiž z hranic naší organizace mohlo uniknout a takový únik dat, to může být setsakramensky nepříjemná věc, která celé organizaci pořádně zkomplikuje práci na dlouhé měsíce a roky. Může to být nejen nepříjemné, ale také docela časově náročné a opravdu hodně drahé. O ztrátě dobré pověsti celé organizace se snad ani zmiňovat nemusím.

Data samozřejmě nemusí „jenom“ uniknout, možností jejich napadení je celá řada. Určitě jste zachytili případy, kdy útočníci pronikli dovnitř systému, zašifrovali v něm informace a vyžadovali výkupné. Tihle digitální korzáři jsou často úspěšní, protože dokážou ochromit chod celé firmy nebo organizace. Jestli si teď říkáte, že se sociálních služeb tahle forma zločinnosti netýká, protože se to ještě nestalo, pak vězte, že drobnější incidenty už se objevily. A ty větší mohou přijít každou chvíli.

Kdo zodpovídá za bezpečnost informací? Ředitel

Pokud zastáváte manažerskou pozici, možná si teď říkáte, že celou tu slavnou oblast ochrany osobních údajů máte s dodavateli smluvně ošetřenou, máte své pověřence a za vnitřních chod ICT přece odpovídá váš ajťák. Pokud to tak vnímáte, pak vězte, že jsme společně právě teď narazili na první a velmi častý mýtus. Dovolím si tuto vaši jistotu nahlodat. Za bezpečnost dat v každé firmě a organizaci totiž zodpovídá její vedení. Hotovo, tečka. Velmi pozorní by tedy měli být ředitelé, jednatelé, předsedové správní rad a vůbec všichni lidé na podobných pozicích. Způsob zajištění bezpečnosti je totiž opravdu na nich. Je to podobný typ odpovědnosti jako za bezpečnost fyzickou - zámky na dveřích, revize výtahů, volné únikové cesty a ploty bez děr.

Pokud nejste manažeři, a právě se vám ulevilo, že „za všechno může šéf“, tak vězte, že dobrý šéf se o zodpovědnost rád podělí a prostřednictvím interních směrnic a metodiky ji rozprostře napříč celou organizací. Každý zaměstnanec se v této oblasti musí zapojit a chovat se bezpečně.

Kdo má pro nás doporučení? Národní úřad pro kybernetickou a informační bezpečnost

Jen tak pro pořádek tady doplním, že každodenně narůstající agendu kybernetické bezpečnosti opečovává v ČR Národní úřad pro kybernetickou a informační bezpečnosti. Sídlí v Brně a na jeho webu jsou nejen technické informace, ale také doporučení pro manažery. V poslední době příjemně narůstá také sekce, která se věnuje vzdělávání. Nebojte se vybrat si to, co se vám hodí. Doporučení můžete získat i od zřizovatelů, kteří by se mu měli věnovat průběžně.

Co všechno ovlivňuje bezpečnost informací?

Mohu si odvážně myslet, že už jsme se shodli na tom, že informace kolující počítačovým světem našich organizací si pozornost, péči a ochranu zaslouží?

Celou tu hromadu hádanek, které je potřeba postupně rozlousknout, si pro zjednodušení můžeme rozdělit do čtyř skupin.

- První tvoří dobře vymyšlená počítačová síť, která tvoří pomyslný „plot“, který drží digitální informace uvnitř organizace. Musí být řešena tak, aby byla co nejbezpečnější a současně nebránila lidem v práci. Není to jednoduchý úkol, naštěstí se jím zabývá celá řada odborníků a bezpečná řešení není potřeba vymýšlet – stačí si jen vybrat.
- Druhou skupinou jsou programy, informace a systémy, které najdeme výhradně uvnitř organizace.
- Třetí tvoří informace a systémy, které jsou ukládány mimo organizaci samotnou, nejčastěji v tzv. „cloudech“, což jsou velká, profesionálně chráněná datová centra. K informacím, které u nich mají organizace uloženy, přistupují uživatelé nejčastěji prostřednictvím internetu.
- Poslední skupinou, která je stejně důležitá jako výše jmenované jsme potom my. Lidé, kteří usedají k počítačům a tvoří, přeskupují, shromažďují, využívají, ale také archivují a mažou informace. Uživatelé

Navrhuji, abychom pro témata shrnutá do prvních třech skupin ponechali samostatný článek. Bez dobře a bezpečně fungující počítačové sítě a programového vybavení totiž asistivní technologie do smysluplného provozu prostě rozumně neuvedeme.

Dovolím si malé přirovnání. Trochu kulhá, ale přesto vám ho nabídnu. Pokud bychom zkusili přirovnat asistivní technologie k elektromobilu, v němž chceme převážet klienty, pak je nám všem jasné, že abychom ho mohli používat, nutně potřebujeme komunikace po kterých se dá rozumně jezdit, nabíjecí stanici a vhodné parkovací stání. Podobné je to s technologiemi - v případě nasazení chytrých postelí s čidly musíme nezbytně nutně mít dobrou vnitřní síť po které budou „jezdit“ informace, stejně jako dobře nastavené programy a systémy.

Základy bezpečného chování uživatelů

Zastavme se v závěru tohoto textu u toho, jaký je význam zaměstnanců pro bezpečnost informací v systémech. Je to jednoznačné. Zaměstnanec je nejdůležitějším článkem pro fungování každého systému. Systémy přece nevznikají pro radost ajťákům, ale jsou určeny k tomu, aby usnadnily každodenní rutinní práci nám, uživatelům. Nám, kteří každý den usedáme k počítačům a s digitálními informacemi pracujeme.

Dobré je, že s péčí o bezpečnost dat se nám to už docela daří, pokud pracujeme s tradičními informacemi na papíře. Jsme zvyklí zamykat kanceláře, kartotéky, šuplíky s důležitými dokumenty. Skartujeme, archivujeme, zakládáme podle dohodnutých pravidel a na dohodnutá místa. Děláme ale totéž v případě práce s digitálními informacemi?

Co je základní pro každého uživatele?

Bezpečná hesla

Používat bezpečná hesla a přístupy a dobře se o ně starat. Je to stejné, jako když bez přemýšlení zamykáme své domy bezpečnostními zámky a klíče nikomu nesvěřujeme. Pravidla pro tvorbu hesel by měla mít stanovená každá organizace. Pro běžné uživatele by mělo rozumné heslo mít nejméně 10 znaků a mělo by obsahovat kombinaci nejméně tří ze čtyř typů znaků – tedy malá písmena, velká písmena, číslice, případně nějaký speciální znak. Hesla je potřeba v dohodnutých intervalech měnit. A co je důležité – nechat si ho pro sebe podobně jako ty klíče od domu. Nepsat na nástěnku, na monitor a rozhodně nesdílet s kolegy. Nechcete přece, aby někdo měnil informace v systému „vašim jménem“. Věřte mi, že ve valná většina systémů každý pohyb uživatele sleduje a dokáže přesně určit, kdo je autorem zápisů.

Vícefaktorové přihlašování

Všude, kde je to možné, používat tzv. dvoufaktorové přihlašování. I tohle z reálného světa roky znáte. Nebo se mezi čtenáři tohoto článku najde někdo, kdo doposud neslyšel o tom, že pojišťovny jsou často ochotny pojistit váš majetek pouze tehdy, pokud musí zloděj cestou k němu překonat dva zámky? Dvoufaktorové přihlašování je právě takovým dvojitým zámkem. Většinou se přihlásíte svým jménem a heslem a přihlášení potvrdíte další formou. Může to být třeba kódem přepsaným z sms, nebo přímo aplikací v mobilu. Takový dvoufaktor je docela šikovná věcička, protože váš přístup dokáže ochránit i v případě, že nějak unikne vaše jméno a heslo. A to se hodí nejen v práci, ale také v přístupu k soukromému e-mailu, elektronickému bankovnictví, sociálním sítím a dalším důležitým vymyšlenostem, které používáme v soukromí.

Pozor na podvodníky

Nebojte se být trochu opatrní a nevěřte neznámým hlasům v telefonu ani neznámým e-mailům. Podle zkušeností odborníků nejčastěji unikají přístupy do systémů tak, že někdo jednoduše „vytáhne“ jméno a heslo z některého z uživatelů. Je to jednoduché. Někdo zavolá, vy zvednete telefon a jste zdvořile požádáni o přístup do počítače s tím, že je v něm potřeba něco opravit. Nevěřte. Udělejte věc úplně opačnou – dejte ihned informaci o takovém divném telefonátu svému nadřízenému. Není to žádné „žalování“, jen je prostě možné, že někdo z vašich kolegů fintu neprohlédl, heslo sdělil a ve vaší síti už se zvědavě prohání hacker. S e-maily je to podobné. Naučte se neotvírat přílohy mailů neznámých adresátů a při sebemenším podezření si raději jinou cestou ověřte, jestli je e-mail v pořádku. Buďte velmi ostražití, pokud k Vám dorazí nabídka téměř bezpracné výhry nebo jakákoliv žádost o vaše osobní údaje. I tady platí, že každou událost, která se vám nezdá, je opravdu dobré nahlásit.

Učte se

Nebojte se být zvědaví, vybírat si kurzy, učit se, ptát se. Je to užitečné. Stejně dobře, jako firemní data, totiž budete umět ochránit třeba svoje peníze na bankovním účtu.

Taky se vám zdá, že jsme se od těch asistivních technologií dostali úplně někam jinam? Připadá vám, že by bylo lepší psát si o chytré podlaze, která upozorní na to, že se paní Zvídavé rozlil čaj a mohla by uklouznout nebo o robůtkovi, který jí bude trpělivě pouštět alba fotografií na tabletu nebo staré videozáznamy ze

školních besídek jejich dětí? Na dobu, kdy budeme moci s klidem diskutovat o atraktivních robotických pomocnících a propojování dat z různých systém, už se moc těším. Už proto, že to bude znamenat, že naše organizace budou mít bezpečné počítačové sítě, dobré a aktuální programové vybavení, bezpečné informační systémy, vzdělané uživatele a že budou řídit bezpečnost svých dat. Je jasné, že některé organizace jsou tomuto cíli už blízko, jinde práce spíše začíná. Aby nám šla od ruky, můžeme příště probrat záludnosti počítačových sítí.

Vítejte ve světě digitalizace

Na závěr mám pro vás zprávu. Z pohledu zavádění asistivních technologií jsme právě vrátili na začátek. Proč to tak je? Měli byste se totiž vrátit k samotným základům informačních technologií ve vaší službě a podívat se na ni z nového pohledu.

- Ať zastáváte jakoukoliv pozici, měli byste si v klidu promyslet, které technologie by mohly být pro vaši práci v budoucnu užitečné a co potřebujete zlepšit.

- Pokud jste manažer, měli byste se navíc pořádně zamyslet nad tím:
    - Jestli máte svou počítačovou síť a systémy v ní běžící rozumně funkční a řízené a bezpečné.
    - Jestli jsou tvůrci používaných systémů nakloněni předávání dat. Je to k nevíře, ale není to tak obvyklé, jak bychom se mohli domnívat.
    - Jaké možnosti a znalosti mají lidé v organizaci. Mají rozumnou techniku? Nepotřebují v něčem proškolit? Používají své infosystémy dobře?
    - Nakonec nezapomeňte průřezové a třaskavé téma – kybernetickou bezpečnost. O vaše informace se totiž určitě nepostará nikdo jiný než právě vy.

Není málo toho, co bychom si měli před vstupem do světa asistivních technologií ověřit a dát do pořádku. Aby to bylo jednodušší, můžeme se na tomto místě setkávat i v příštích číslech časopisu a trochu víc se zamyslet nad je jednotlivými tématy. Digitalizace a asistivní technologie a pokrok v inovacích totiž do sociálních služeb nezadržitelně míří. Vlastně už přešlapují na prahu. Při udržitelném a dobrém zavedení pomohou ušetřit práci, získat informace o klientech a díky tomu se o ně lépe starat. A to rozhodně není málo.