

Technologie v sociálních službách - díl 3

Kudy vede cesta k asistivním technologiím? – Po bezpečné počítačové síti.

Na začátku si připomeňme paní Zvídavou, klientku domova pro seniory z budoucnosti. Paní Zvídavá totiž těží z toho, že je její domov vybavený asistivními technologiemi a sama je taky umí používat. Technologie, které jsou vidět, jsou ale jen pověstnou špičkou ledovce. Dneska se tedy podíváme na jednu důležitou složku, která je zanořena hluboko pod hladinou a paní Zvídavou vlastně nezajímá. Na dobře vyřešenou počítačovou síť.

Tento článek není určený ani napsaný pro „ajťáky“. Je pro nás, kdo technologie používáme, nemusíte se tedy bát, že by byl prošpikovaný odbornou, nesrozumitelnou terminologií. A pokud se přece jenom nějaké to cizí slovo někde vyskytne, nebojte se podívat se do přiloženého slovníčku. Ajťákům naopak posílám varování, že čtení dalšího textu může ohrozit jejich potřebu naprosté přesnosti a dokonalosti v pojmosloví a že další čtení je na jejich vlastní nebezpečí.

Co potřebujeme o počítačové síti vědět my ostatní? Proč je tak důležitá a k čemu slouží? Proč ji někteří odborníci, kteří se věnují vývoji asistivních technologií, označují za kritickou infrastrukturu, což zní docela hrozivě a možná nevíme, co to znamená? Pojďme si to zkusit trochu rozmotat. Musí to jít, vždyť jsou to vlastně dráty.

Počítačová síť slouží jako označení pro soubor technických prostředků, které jsou spojeny tak, aby umožňovaly spojení a bezpečnou výměnu informací mezi počítači. Informace se tak mohou podle nastavených pravidel propojovat a ukládat a my s nimi můžeme pracovat.

Dobře vyřešená počítačová síť musí nám uživatelům dát jistotu, že budou všechna připojená zařízení, všechny asistivní technologie, správně fungovat.

Pojďme si zase pomoci přirovnáním. Tentokrát si představte dětské telefonky. Takové, jaké snadno seženete v každém hračkářství. Dva růžové telefonní přístroje spojené drátem, kterými si mezi sebou mohou telefonovat holčičky. Je to jednoduché. Holčičky ovládají svá telefonní sluchátka a informace v podobě zvuku se předává z jednoho koncového zařízení – tedy z jednoho telefonu do druhého. Když se v jednom z telefonů vybijí baterky, systém přestane fungovat a dokud tatínek nevymění baterky, holčičky se neuslyší. Když už maminka ztratí trpělivost s jejich brebentěním a odpojí drát, stane se totéž – systém přestane fungovat. Když se zvuk přenese, tak prostě zmizí, nikam se neukládá a není tedy potřeba se o něj starat.

A teď si představte počítačovou síť. Desítky, možná i stovky komunikujících koncových zařízení (tedy pomyslných telefonků). Počítače, tiskárny, skenery, tablety, kamery, čidla. Tady už si s jednoduchým drátem asi nevystačíme, tady už to chce pořádné přemýšlení. Není důvod se děsit – chytré aťácké hlavy si po technické stránce budou vědět rady, na nás je ale to, abychom jim dali zadání a tedy si dokázali dobře pojmenovat, co vlastně od své sítě počítačové potřebujeme.

Hodí se určitě mít:

- 1) Přehled o tom, jaká koncová zařízení se k naší síti připojují a jak v ní fungují
- 2) Povědomí o tom, jak informace v síti kolují a co se s nimi děje.
- 3) Jistotu, že vše funguje a nic se nepokazilo nebo neodpojilo
- 4) Znalosti o tom, kudy procházejí a kam se ukládají informace
- 5) Klid daný tím, že víme, že z uložených informací se vytvářejí zálohy a nehrozí nám ztráta
- 6) Zabezpečení sítě tak, aby do ní snadno nepronikl žádný nepřítel z vnějšího světa.

Vaše počítačová síť tedy musí být řízená, monitorovaná, bezpečná a data v ní musí být zálohovaná. Tahle věta jen shrnuje předchozích šest bodů do jedné věty, ale současně už může být dobrou otázkou pro ajťáky s nimiž ve svých službách spolupracujete.

CO ZNAMENÁ ŘÍZENÁ POČÍTAČOVÁ SÍŤ?

Řízení, to je vlastně taková maminka z našeho příkladu o telefoncích. Maminka odpojila drát a zařízení přestalo fungovat. Maminka připojila drát a zase všechno šlapalo. Je vám asi jasné, že řízená síť nejspíš nebude mít žádnou opravdovou maminku, že o se o všechno to spojování a nespojování stará nějaké technické udělátko. Tím je zpravidla server nebo spíše servery. Server je řídicí počítač, takový „centrální mozek“ vaší sítě, který může plnit mnoho různých úkolů. Mimo jiné hlídá, jak a kdo se snaží k síti připojit a umožní mu to jen tehdy, pokud splňuje podmínky, které má uložené ve svém nastavení. .

Jednoduše řečeno – každé zařízení, které pracuje ve vaší počítačové síti musí získat povolení serveru, že se může připojit. Že ho server zná a smí mu umožnit práci v síti, pokud se správně přihlásí. Analogii s maminkou ještě nebudeme opouštět. I tady totiž musí být na samém začátku člověk, který řekne, která zařízení se k síti mohou připojovat a jak to bude vypadat. V případě pracovních sítí plní roli maminky vždycky a bez výjimky šéf organizace – tedy ředitel nebo vedoucí. Ten stanoví pravidla, která pak odborníci – ajťáci převedou do řeči, která bude pro server srozumitelná a bude je moci po uživateli vyžadovat. V řeči technické se používá přílehlivé slovo „vynucovat“. Znamená přesně to, co si pod ním představujeme. Server nás a náš počítač umí přimět, abychom udělali i to, co se nám nechce. Umí například vynutit změnu našeho hesla. Prostě nás nepustí dovnitř sítě, dokud si ho nezměníme. Pro nás, lidi, je to sice trochu nepříjemné, ale server nedělá nic jiného než to, že prostřednictvím nastavených pravidel (říká se jim politiky) bdí nad tím, aby v naší síti pracovaly jen ty počítače, zařízení a uživatelé, kteří ji neohrožují.

CO ZNAMENÁ MONITOROVANÁ SÍŤ?

Že se v dnešní době dá sledovat mnohé, to všichni víme. Stejně je to i v počítačové síti. Dá se sledovat, co se v ní děje, kudy „běhají“ data a jestli je to tak obvyklé, dá se sledovat také to, jestli všechny její součásti dobře fungují a jsou aktivní. Pokud se zase vrátíme k našim růžovým telefonkům, pak můžeme sledovat, jestli jsou oba telefonky aktivní a dá se z nich volat. V případě, že v jednom dojdou třeba baterie, dozvíme se to jednoduše. Hlášení podá některá z telefonujících holčiček. Dovedete si to představit? Vidím to přímo živě: „Tatííí, zas mi to nefunguje, vidíš to?“ Tatínek vymění baterky a katastrofa je zažehnaná.

Hlídat stejným způsobem počítačovou síť je samozřejmě nemožné, ta se musí umět hlídat automatizovaně. Není to úplně jednoduché a stojí za to se dobře poradit s odborníky. Není totiž nijak výjimečné, že docela hezky vymyšlená počítačová síť nesleduje svůj provoz dostatečně. Nebo ho dokonce nesleduje vůbec. Nemůže tak zjistit, že některá její součást, některé koncové zařízení, se vypnulo nebo pokazilo. A to by mohl být pro asistivní technologie v sociálních službách kardinální problém.

Zkusme se od drátku spojujícího dva růžové telefony v myšlenkách přesunout ke složitě strukturované kabelu v domově pro seniory roku 2028. Pamatujete si ho? To je ten, kde žije paní Zvídavá. Jejími koncovými zařízeními nejsou jen počítače, ale také desítky, či spíše stovky senzorů, které sledují, jestli jsou klienti v bezpečí. Jeden z nich je připojený v koupelně paní Zvídavé. Po většinu času je nečinný, ale kdyby paní Zvídavá upadla a zůstala ležet na zemi, vyhlásil by poplach. Ten by mohl vypadat třeba tak, že by se v telefonu v kapse pečovatelky zobrazilo hlášení o pádu a ona by mohla hned zasáhnout. Pokud by se čidlo pokazilo, počítačová síť to prostě musí poznat, vyvolat poplach a zvednou ze židle technika, který ho opraví nebo vymění.

Na začátku tohoto článku jste si možná všimli zmínky o tom, že počítačovou síť lze z pohledu používání asistivních technologií považovat za kritickou část infrastruktury. A tady máme důvod. Síť musí být tak dobře řízená a monitorovaná, aby dokázala informovat o tom, že některá její součást neplní svoji funkci. Je to velmi, velmi důležitá věc.

Možná se teď trochu usmíváte, protože teď žádná čidla téměř nikde nejsou, pečovatelé klienty kontrolují, sledují a dělají pro jejich bezpečí maximum. Přiznejme si ale, že každý z nich může být najednou jen na jednom místě a k tomu musí reagovat na klienty a jejich potřeby, o kterých se aktuálně dozví.

V tom jsou čidla samozřejmě lepší a mohla by být hodně nápomocna. Jsou totiž schopna sledovat situaci na mnoha místech najednou a neúnavně. 24 hodin každého dne, 7 dní v týdnu. Síť ale musí umět sledovat, jestli jsou v pořádku a fungují. Nesmíme totiž zapomínat na to, že senzory v budoucnu hodně ovlivní způsob práce, ale i přemýšlení pečovatelů. Ti se na ně, po překonání počáteční fáze nedůvěry, začnou spoléhat a budou očekávat, že když se jejich klient ocitne v nouzi, mobil s naléhavostí rozvibruje jejich kapsu. Věřím, že už je teď jasnější, proč je potřeba mít počítačovou síť dobře sledovanou.

CO ZNAMENÁ BEZPEČNÁ SÍŤ?

Po tomto tématu se zlehka svezeme po povrchu jako sáňky na sněhu. Tomu, co mohou uživatelé udělat pro bezpečný provoz sítě jsme se totiž věnovali v minulém článku. Zbývá dodat, že téměř každá síť má brány do neprobádaného vnějšího světa, který ji prostřednictvím internetu propojuje s dalšími sítěmi a systémy. Takových propojení by mělo být co nejméně a je nezbytné pečlivě ochránit každé z nich.

Pokud naši pomyslnou počítačovou síť už teď dokážeme vnímat jako neviditelnou pevnost, pak k ní bude neodmyslitelně patřit rytíř, který neohroženě stráží její bezpečí a do roztrhání brnění dodržuje příkazy tak, aby dovnitř i ven pustil jen ty, které může. Počítačová terminologie je v tomto případě skoro poetická a pro strážce používá termín firewall, tedy řečeno hezky česky – hořící zeď. Firewall v počítačové síti povoluje nebo blokuje navazované komunikace s „vnějším světem“ a chrání ji tak před různými typy útoků včetně těch, které by mohly způsobit, že útočník nad sítí přebere částečnou nebo úplnou kontrolu. Jako u všeho, i tady platí, že musí být dobře nastavený a velmi bedlivě monitorovaný tak, aby upozornil na každou podezřelou situaci. Samozřejmostí v oblasti bezpečnosti už určitě je aktualizovaný a monitorovaný antivir, ale ten už dneska určitě používá každé zařízení sociálních služeb. Pro jistotu si to raději můžete zkontrolovat, to nikdy neuškodí.

Nesmíme zapomenout ani na to, že v dnešní době plné pohybu, se čas od času potřebujeme k počítačové síti připojit odněkud z vnějšího světa. Jedinou vhodnou metodou je v takovém případě použití šifrovaných spojení, která dokážou komunikaci se sítí skrýt a nedovolí tak nikomu v internetu, aby ji sledoval. Používá se pro ně zkratka VPN (pro snaživé čtenáře dodávám, že je to virtuální soukromá síť). Pokud se potřebujete ke své pracovní síti připojit třeba z domu, dělejte to jedinečně prostřednictvím VPN. Způsobů zabezpečení je samozřejmě daleko víc a často jsou velmi vychytané. Dá se okukovat třeba to, jak zajišťují bezpečnost svých dat banky. Ale nalejme si čistého vína – tak daleko sociální služby v České republice zatím nejsou.

CO JE TO CLOUD?

Na závěr si ještě připojíme kapitolku o tom, že ne všechna data, která vlastníme, ne všechny systémy, které se v sociálních službách používají, „bydlí“ uvnitř vlastní počítačové sítě. Ptáte se, co je to zase za komplikovanost? Nebojte se, zas tak složité to není.

Některé programy a aplikace jsou nastěhované neboli nainstalované, přímo na počítačích uvnitř sítě. Organizace si je jednoduše koupí jako každý jiný majetek. Druhou možností je využít tzv. „cloudové řešení“. Cloud je anglický výraz pro mrak a počítačové řešení se používá jako metafora pro soubor vysoce výkonných počítačů, které jsou umístěny někde na světě. Podotýkám, že abychom byli v souladu s legislativou musí být všechna naše data na území Evropské Unie.

Je tak docela možné, že v práci běžně používáte program, který je umístěný někde v cloudu. Téměř jistě tak fungují významnější programy, které se pro sociální služby používají. Způsob zabezpečení je tady na provozovatelských cloudových úložištích nebo datového centra, na nás pak je, abychom se bezpečně přihlašovali a nenechávali své přihlašovací údaje nikde volně ležet. Jsou totiž nehmotným klíčem k velkému množství informací.

V současné době se jeví, že cloudová řešení budou využívána stále víc. Pro sociální služby je to nejspíš docela inspirativní zpráva. Brzy totiž bude nejspíš stačit dobře si vybrat užitečnou službu v bezpečném cloudu a pronajmout si ji. O to, aby byl systém zajištěný, aktuální a informace v bezpečí se pak na základě smluvního vztahu už nebudeme muset až tolik starat a zůstane tedy čas na ty očekávané asistivní technologie a jejich testování.

Co připomenout na závěr? Nebojme se počítačových sítí. Dávno je známe, tvoří důležitou základnu pro práci sociálních službách už dneska. V budoucnu jejich význam ještě vzroste. Problematika je to opravdu složitá a je docela pochopitelné, že se nám nad ní nechce přemýšlet. Na druhou stranu je tak moc důležitá, že pokud jste ještě nezačali, bude nejlepší se na to vrhnout hned. Nebo aspoň zítra ráno. Řešení existují a někdo z odborníků vám určitě rád pomůže. Doporučuji konzultovat s takovými externisty, kteří vám dokážou doložit, že se o podobně velké sítě starají i u jiných klientů. IT už je dneska oborem s řadou vnitřních specializací, vyberte si tedy tu, kterou potřebujete. Tady může být improvizace neúčinná, ba přímo škodlivá.

Už proto, aby si paní Zvídavá mohla být jista, že kdyby kdekoliv ve svém pokoji upadla, čidlo hned upozorní personál a ten jí pomůže zpátky na nohy. Až to bude takto fungovat, bude to velká věc. My se ale mezitím, než dobudujeme počítačové sítě a dořešíme bezpečnost dat, můžeme nad asistivními technologiemi zasnít a promyslet si, v čem mohou být nápomocny. Nechat si na to můžeme celý příští článek.