



Vážení čtenáři,

před rokem jsme v Loginu řešili téma „nejsou lidi“. Letos máme novou výzvu, která zní „lidi jsou doma“. Bez kontextu by se mohlo zdát, že je to zcela opačné téma. A částečně tomu tak je, protože skutečně i v IT, kde je obecně lidí nedostatek, se vlivem epidemie COVID-19 někteří objevili na pracovním trhu.

„Lidi jsou doma“ však směřuje k jinému fenoménu, a to je „hybridní práce“. Jedná se o situaci, kdy někteří lidé pracují z domu a někteří z kanceláře, popř. kdy se tento stav různě v krátkých časových obdobích mění. Hybridní práce tak zákonitě souvisí s dalším tématem, které jsme již loni představovali. Jedná se o „digitální pracoviště“. Zatímco loni platilo „nice to have“, dnes je to prakticky „must have“. O co jde? Digitální pracoviště umožňuje vám a vašim lidem pracovat odkudkoli. Samozřejmě se to nevztahuje zcela na všechny profese, např. soustruh jen tak nezdigitalizujeme, nicméně všechny kancelářské a manažerské činnosti jdou z větší části nebo zcela přesunout do on-line světa.

Digitální práce přináší řadu výhod. Díky přístupu k informacím a aplikacím odkudkoli mohou být lidé efektivní v situacích, ve kterých to doposud nebylo možné. Přináší však také řadu výzev technického i organizačního charakteru, a to zejména z pohledu bezpečnosti, resp. zabezpečení spolehlivého fungování.

A právě na to, jaké nástroje a služby použít, abyste v hybridním světě obstáli v krátkodobém i dlouhodobém horizontu, jsme zaměřili toto vydání Manažerské přílohy. O konzultaci můžete požádat na: k.k-net.cz/konzultaceBHS.

Já i mí kolegové se těšíme na viděnou s vámi!

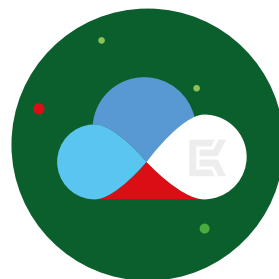


Ing. Jan Knetttig
IT konzultant K-net

BEZPEČNOST V HYBRIDNÍM SVĚTĚ

OBSAH MANAŽERSKÉ PŘÍLOHY:

- Co je hybridní svět z pohledu IT
- Proč být hybridní?
- Výzvy hybridního světa
- Bezpečná práce na dálku



CO JE HYBRIDNÍ SVĚT Z POHLEDU IT

„Hybridní svět“ vnímáme v K-netu jako svět v přechodu z jednoho způsobu fungování do druhého, přičemž tyto dva po nějakou dobu koexistují a doplňují se. O hybridním IT se tradičně posledních několik let mluví v souvislosti s prostředím, které kombinuje prostředky umístěné lokálně (tzv. on-premises) s prostředky umístěnými vzdáleně, tedy v cloudu, popř. více cloudech. Nově se hybridního IT dotýká také hybridní práce, tedy práce z kanceláře i z domu, pro kterou IT musí zajistit spolehlivé, bezpečné a pokud možno pohodlné pracovní prostředí.



PROČ BÝT HYBRIDNÍ?

Ještě nedávno to pro mnoho podniků nebylo téma dne. Řada organizací fungovala „tradičním“ způsobem, kdy hybridní přístup pro ni nedával (takový) smysl. Tradiční způsob je ten, když uživatelé pracují pouze z kanceláře z přiděleného počítače, který nikam nenosí a do firemní sítě se buď vůbec nebo většina z nich vzdáleně nepřipojí, aby byla zajištěna bezpečnost. Zároveň jsou všechny aplikace provozovány na interních serverech a data ukládána na interních úložištích a spravována interními „ajťáky“. Firma, která má vše takto vybudováno, zainvestováno a má zaběhnuté procesy, celkem přirozeně směřuje k tomu tento stav ponechat. Svět ale míří jiným směrem.

Jakmile zjistíte potřebu používat novou aplikaci a nechcete ji vyvíjet na zelené louce, často zjistíte, že tato aplikace je dostupná pouze jako cloudová aplikace z vašeho prohlížeče. Pak zjistíte, že vaši uživatelé potřebují posílat větší soubory, než jim umožní e-mail a než se nadějete, vaše data se pohybují po on-line službách, které nabízí úložiště zdarma. A jste v cloudu, ani jste nechtěli. Částečně. Stále máte přece svou robustní místní infrastrukturu a nastavené

procesy. Jste tedy hybridní. V tu chvíli jste ale špatně hybridní.

Vaši uživatelé potřebují pro svou práci nástroje, které jim vaše tradiční IT nechce nebo nemůže dát a oni si najdou své cestičky, jak je získat. To vám může způsobit později značné potíže, protože, na rozdíl od vašich interních informačních technologií, nad těmito nástroji, které si zřídili vaši uživatelé sami, nemá vaše IT oddělení žádnou moc. A to není správně.

Proč tedy být hybridní? Protože vaše interní IT už nemůže samo zajistit úplně všechny služby, které vaše organizace potřebuje. Stále ale na něm leží zodpovědnost za to, že všechny služby dozoruje a spravuje. Také protože bez toho, abyste byli hybridní, pravděpodobně neobstojíte ve scénářích jako dnes, kdy je extrémní situace a vy potřebujete zajistit tzv. business continuity, tedy aby váš podnik jel dál.

Role interního IT se mění. Není již nutné, aby váš ajťák sám provozoval servery v serverovně. Je však potřeba, aby zajistil architekturu a bezpečnost celého hybridního prostředí vaší organizace.



VÝZVY HYBRIDNÍHO SVĚTA

Být hybridní samozřejmě není jen tak. Pracovat na dálku tradičně nelze a je tedy potřeba k tomu použít vhodné nástroje. I v tradičním prostředí je třeba řešit, kdo má kam přístup a v hybridním prostředí je to ještě důležitější. Když vám lidé pracují vzdáleně a vy jim potřebujete nějak poradit, nemůžete za nimi jednoduše přijít.

Je proto potřeba mít nějaký nástroj vzdálené podpory a třeba také dohledu uživatelů. Samozřejmě práci vzdáleně nelze dělat bez kvalitního spojení, které musí být na straně organizace i uživatelů. Vaše data se v tu chvíli pohybují „volně“ po světě a je potřeba je proto zálohovat ještě více než dříve a mít připraveny scénáře pro případy, kdy je potřeba obnovit provoz po havárii. Jelikož počet kybernetických útoků stále stoupá, potřebujete chránit svou interní síť i uživatele pracující vzdáleně. Potřebujete chránit vaše webové aplikace. A potřebujete samozřejmě chránit také koncová zařízení vašich uživatelů, ať jsou kdekoli.

Podrobně nyní představíme jednotlivé naznačené oblasti a možná řešení.



BEZPEČNÁ PRÁCE NA DÁLKU

Když s pandemií COVID-19 přišla potřeba umožnit uživatelům home office, řada organizací umožnila svým zaměstnancům přístup do interní počítačové sítě vzdáleně přes VPN, tedy přes šifrované spojení. Pro organizace, které provozují nějaké aplikace na svých interních serverech nebo sdílí data mezi uživateli přes síťové disky, je to známé řešení, jak přistupovat k těmto prostředkům vzdáleně. Mnoho organizací proto jednoduše dalo tento vzdálený VPN přístup všem zaměstnancům, které chtěly poslat na home office. Problém VPN je, že je velmi náročná na datové přenosy. Když tedy pracujete s nějakou aplikací, která běží na serveru a tam ukládá data, musí se všechna data přenést k vašim uživatelům a pak od nich zase zpět. Pokud chtějí pracovat s dokumentem uloženým na vzdáleném síťovém disku, při jeho otevření čekají, až se jim soubor stáhne. Podobně je tomu i při ukládání. Uživatelsky je to tedy velice nepohodlné. Navíc se v řadě organizací ukázalo, že jejich internetové linky a servery nejsou na takový nápor vzdáleně přistupujících uživatelů vůbec připraveny.

Mnoho oblastí spojených se zajištěním práce na dálku řeší populární cloudové služby v čele s Microsoft 365. Pokud jde o sdílení dokumentů, v dnešní době je daleko pohodlnějším

řešením než sdílený disk přes VPN využít jejich služeb on-line úložišť. Každý uživatel získává svůj osobní on-line disk o velikosti 1 TB v rámci služby OneDrive a dále máte k dispozici 1 TB prostoru na organizaci + 10 GB na každého uživatele na sdíleném disku v rámci služby Sharepoint. Kromě toho uživatelé mohou spolupracovat nad dokumenty Office ve stejný čas bez toho, aby si museli dokumenty posílat e-mailem nebo ukládat nové verze, čímž se významně šetří místo. Jedná se o on-line úložiště, přístupné je tedy z jakéhokoli zařízení včetně mobilních telefonů. Z pohledu bezpečnosti je velice příjemná funkce, kdy při sdílení dokumentu ze sdíleného disku (Sharepoint) se standardně vytváří odkaz, který mohou otevřít pouze lidé z dané organizace. Ostatním se dokumenty nezobrazí. V tomto ohledu se dají nastavit různá bezpečnostní pravidla. Dokumenty navíc mohou být synchronizovány na lokální disk zařízení uživatele, což funguje daleko lépe než offline složky z běžného sdíleného disku na Windows serveru. Kdo svá data nechce dávat mimo firmu, ale chce mít cloudové úložiště podobné tomu od Microsoftu, může využít naši službu netSpace postavené na technologii Citrix ShareFile, kdy jsou dokumenty na jeho serverech, nebo na serverech K-netu, dle preference zákazníka.

Zmínil jsem e-mail. Ten je v rámci Microsoft 365 rovněž obsažen jako služba Exchange Online. Samozřejmě je možné se k e-mailům dostat z jakéhokoli zařízení a e-mailového klienta (např. oblíbeného Outlooku, který je od určité verze Microsoft 365 rovněž součástí) a každý uživatel má v základu k dispozici 50GB schránku.

Mnoho lidí ke své práci potřebuje kromě e-mailu převážně pouze aplikace Office, jako je Word, Excel a Powepoint. Ty jsou v balíčku Microsoft 365 samozřejmě rovněž obsaženy. V nejnižší verzi jsou pouze on-line v prohlížeči, ve středním plánu Microsoft 365 Business Standard jsou již součástí i klasické desktopové aplikace, které si uživatelé navíc mohou nainstalovat v rámci jedné licence i na své domácí počítače, tablety či telefony a být tak produktivní odkudkoli.

Poslední oblastí, která se nyní pomocí Microsoft 365 standardně a velmi kvalitně řeší, jsou on-line schůzky a vedení týmu a projektů. V aplikaci Teams můžete vytvořit týmy napříč organizací a realizovat on-line schůzky až s 300 uživateli naráz, což většině podniků bohatě postačí. Dá se však přes ně realizovat i on-line konference až pro 10 000 účastníků. Při vedení týmu a projektů vám zase může

dobře pomoci nástroj Planner, díky kterému lze přehledně plánovat i rozdělovat práci a sledovat, jak se plní. Mnoho manažerů nedá dopustit také na OneNote, což je zpracovaný digitální poznámkový blok, který umožňuje poznámky dobře kategorizovat a kombinovat psané na klávesnici s ručně psanými. Skvěle se hodí např. na zápisky z porad a jiné sdílené projektové dokumenty.

Pomocí Microsoft 365 tedy můžete vyřešit moderní vzdálený přístup prakticky ke všemu, co se týká Microsoftu. Co však s vašimi podnikovými aplikacemi typu účetní systém, ERP či aplikace vyvinuté vám na míru, pokud jsme řekli, že VPN není optimální řešení?

Zde se nabízí využití technologií Citrix. Díky nim je možné jakoukoli aplikaci poskytnout virtuálně tak, aby byla on-line přístupná z jakéhokoli zařízení. Váš tradiční informační systém tak budou moci vaši uživatelé ovládat klidně i z tabletu. Zásadní výhodou oproti VPN pak je velké snížení přenášovaných dat. Nepřenáší se totiž samotná data, ale pouze obraz toho, co se reálně děje na serveru u vás nebo někde v cloudu. Toto řešení navíc významně zvyšuje bezpečnost, jelikož se data nestahují na zařízení zaměstnanců. Kromě toho je možné je nechat přistupovat i k webovým aplikacím pouze z chráněného bezpečného prohlížeče poskytovaného z Citrix prostředí a chránit tak vaši interní síť i data.

Nejvyšší formou zajištění pohodlné a bezpečné práce odkudkoli je pak využití platformy Citrix Workspace. V rámci ní mohou uživatelé přistupovat ke všem podnikovým aplikacím, datům a dokumentům z jednoho prostředí. Je úplně jedno, zda je daná aplikace na serverech vaší organi-

zace či v cloudu. Pro uživatele je to pouze ikonka na ploše, vůbec nepozná, kde a jak je aplikace provozována. Vám jako organizaci pak může být prakticky jedno, jak je jejich zařízení moderní a bezpečné, jelikož práce se odehrává v chráněném prostředí Citrix. Pro uživatele je zajištěna vysoká míra pohodlí a přehlednosti i díky tomu, že do jednotlivých aplikací se nemusí hlásit, přihlásí se pouze do prostředí Workspace, které další přihlášení již zajistí za uživatele.

K-net je Citrix partner, a proto vám můžeme pomoci toto řešení nasadit nebo můžete využít naší služby netApps, v rámci které budeme provozovat vaše aplikace v prostředí Citrix v našem K-net Cloud. Pokud by vám nevyhovovalo dát vaše data k Microsoftu, kterého jsme rovněž partnerem, upře-

dnostňujete vše u české firmy a chcete vědět, kde vaše data fyzicky jsou, díky technologiím Citrix jsme vám schopni zajistit i provoz aplikací Office a on-line bezpečného sdíleného úložiště v K-net Cloud. S rozhodnutím vám každopádně umíme pomoci, stejně tak jako s tím, že vás i vaše uživatele naučíme ovládat veškeré technologie.



V příští Manažerské příloze se budeme věnovat správnému nastavení přístupů, vzdálené podpoře a sledování zaměstnanců, zajištění spolehlivého spojení, zálohování, ochraně sítě, webů a zařízení.

+







Konzultaci si domluvme na
k.k-net.cz/konzultaceBHS

K-net Technical International Group, s.r.o.
Olomoucká 170
627 00 Brno – Černovice
tel.: 548 220 150
GSM: 734 686 001
Pobočka: Rovečinská 16
679 74 Olešnice
tel.: 511 447 055

K-net Team Praha, s.r.o.
Sazečská 560/8
108 00 Praha 10 – Malešice
tel.: 734 686 014

K-net Team Ostrava, s.r.o.
Smetanovo náměstí 328/1
702 00 Ostrava
tel.: 734 686 012

-  facebook.k-net.cz
-  linkedin.k-net.cz
-  youtube.k-net.cz
-  info@k-net.cz

www.k-net.cz



Vysvětlění podtržených výrazů z Loginu a Manažerské přílohy najdete v glosáři IT pojmů na k.k-net.cz/glosar.