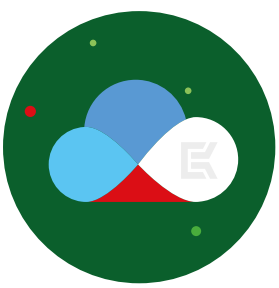
N°02 - 2020
manažerská příloha
K-net Technical International Group

BEZPEČNOST V HYBRIDNÍM SVĚTĚ

OBSAH MANAŽERSKÉ PŘÍLOHY:



Vážení čtenáři,

v minulé manažerské příloze jsme otevřeli téma bezpečnost v hybridním světě. Vysvětlili jsme si, jak se dá na hybridní svět pohlížet, proč se vyplácí být hybridní a jak zajistit bezpečnost při práci na dálku. Dnes v tomto tématu budeme pokračovat. Problematika zabezpečení spolehlivého a efektivního fungování firem v této době je totiž natolik obsáhlá, že si zaslouží druhý díl manažerské přílohy.

V ní se zaměříme na celou řadu praktických otázek. Kdo a kam může přistupovat a jak to kontrolovat? Jak pomoci na dálku kolegům, když si s něčím neví rady, a to nejen na obrazovce počítače? Jak si udělat přehled o tom, zda lidé na dálku vůbec pracují? Jak zajistit spolehlivé spojení mezi vašimi kolegy a jimi používanými aplikacemi a daty?

Jak zajistit, že o data dostupná odevšad nepřijdete? Jak ochránit vaši podnikovou síť v době, kdy data jsou novým platidlem? Jak ochránit vaše weby, webové aplikace a portály, když jsou dnes nejen vaší vizitkou, ale také nástrojem pro práci a skrývají v sobě mnoho citlivých informací? A na závěr nesmíme zapomenout ani na to, jak ochránit samotná zařízení, na kterých uživatelé pracují.

Věříme, že pro vás bude tento přehled klíčových oblastí a nástin možných řešení užitečný. Pro bližší informace jsme k dispozici.

*O konzultaci můžete požádat na **k.k-net.cz/konzultaceBHS**.*

Já i mí kolegové se těšíme na viděnou s vámi!

Ing. Jan Knettig
IT konzultant K-net

PŘÍSTUPY A POLITIKY

Podívejme se nejdříve na nebezpečí zcizování dat. V každé firmě nebo organizaci je naprosto zásadní určit, kdo a kam má přístup. To platí dvojnásob ve chvíli, kdy vaše data zpřístupníte přes internet vzdáleně pracujícím uživatelům. Důležité je mít ve firmě zavedenou doménu, ve které máte všechny uživatele, a nastavujete, k jakým aplikacím, datům a zařízením mají různé uživatelské skupiny a jednotliví uživatelé přístup.

Pro správu domény v prostředí Microsoft se využívá jeho Active Directory. Mnoho interních informatiků tuto službu zná a zvládá ji spravovat. Někdy však potřebují pomoci s pokročilým nastavením, např. v rámci tzv. Software Restriction Policies, kde se detailněji určuje, kdo a jak může s jednotlivými aplikacemi pracovat. Nad rámec běžné správy AD pak zpravidla jdou dnes velmi aktuální funkcionality spojené s prací z domova. Informatikům často chybí nástroje, kterými by dokázali ohlídat např. kdo z uživatelů delegoval práva ke svému účtu kolegovi, kdo přizval do Teamsové komunikace externistu apod.

Problémem této správy často je, že probíhá živelně a po čase v ní vznikne nepořádek a chaos. Prakticky dojde k tomu, že nikdo pořádně neví, kdo přesně a k čemu má přístup. Mnohdy se „zapomíná“, že k citlivým datům může mít přístup kromě konkrétních uživatelů i přímo aplikace – přímá vazba uživatel/data pak vidět není, a přesto prostřednictvím práv aplikace může dojít k bezpečnostnímu či GDPR problému. Správce tak není schopen zaručit požadovaná oprávnění při práci s daty. Ve chvíli, kdy se rozhodnete, že toto chcete zkontrolovat a udělat v tom pořádek, jsou skvělým pomocníkem nástroje Quest. Pro nalezení „kostlivců ve skříni“ ve vašem Active Directory i jinde a pro jejich pravidelnou kontrolu a report bezpečnostních incidentů slouží Quest Enterprise Reporter. Ve chvíli, kdy chcete mít v reálném čase přehled o změnách, které se dějí, a jejich záznam do logu, například, že Franta právě teď upravil dokument na sdíleném úložišti, doporučujeme vám nástroj Change Auditor, rovněž od Questu.
Samozřejmě s posouzením vhodného řešení, s nasazením i správou nástrojů Quest vám můžeme pomoci.

VZDÁLENÁ **PODPORA** A **MONITORING** ZAMĚSTNANCŮ

Jsou-li vaši uživatelé doma a mají technický problém, nemůžete za nimi prostě přijít. Potřebujete nějaký nástroj, díky kterému se můžete podívat, co uživateli nefunguje a na dálku mu pomoct, aby mohl opět plnohodnotně pracovat. Velmi známým nástrojem pro vzdálenou pomoc je TeamViewer, který lze výborně využít v případech, kdy uživateli něco nefunguje na počítači. Vy se tedy k němu připojíte, vidíte jeho obrazovku, můžete ji vzdáleně ovládat, najít problém a odstranit ho. V případě, kdy problém uživatele není softwarové povahy a týká se něčeho, co tudíž není vidět na obrazovce, může být skvělým pomocníkem nadstavba TeamViewer Pilot. Ta využívá kamery mobilního telefonu ke snímání fyzického prostředí a pomocí umisťování virtuálních objektů do reálného 3D prostoru, které vidí vzdálený uživatel na svém displeji, jej můžete navést k tomu, co je potřeba udělat. Skvěle se to hodí například při servisu strojů, kdy nemůže specialista dojet na místo a musí někoho navádět, co má provést.

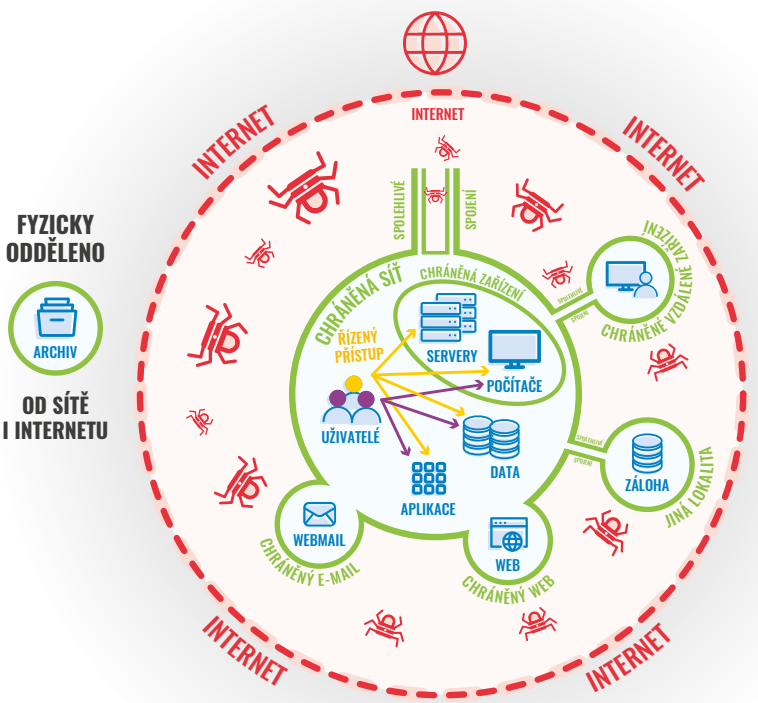
Zajímavou alternativou k produktům TeamViewer jsou produkty NetSupport. Ty kromě vzdáleného ovládání uživatelského počítače umí také spravovat síť místních i vzdálených počítačů a nastavovat určitá pravidla a omezení. Pokud byste měli zájem sledovat, zda lidé na home office skutečně pracují, můžete si nechat zobrazovat miniatury jejich obrazovek v přehledné střídající se matici.

K-net vám umí obě technologie, TeamViewer i NetSupport, dodat a pomoci s jejich nasazením. Zároveň můžete využít naší služby Vzdálená podpora uživatelů, kdy v rámci rodiny služeb Organizační podpora pro vaše uživatele poskytujeme vzdálenou IT podporu a naši technici za pomoci zmíněných nástrojů zajišťují, že vaši uživatelé mohou pracovat.

organizační Podpora

NetSupport

TeamViewer



SPOLEHLIVÉ **SPOJENÍ**

citrix

net Dispatcher ADC

Qnet

Práce na dálku není efektivní bez kvalitního připojení. Jak jsem zmiňoval v minulé manažerské příloze, připojení přes VPN mohou být velmi náročná na množství přenášených dat, čímž je zapotřebí mít velmi rychlé spojení, aby se data přenášela svižně, zvláště je-li vzdáleně připojeno hodně uživatelů. Rychlé připojení musí být jak na straně organizace, aby zvládalo velké množství požadavků od uživatelů, tak na straně uživatelů, kteří se mají přes internet spojovat.

Pokud vaše současná konektivita není dostatečná, máte v zásadě dvě možnosti. První je logicky navýšit rychlost a kvalitu internetového připojení vaší organizace. V Brně vám s tímto můžeme pomoci i přes naši vlastní síť Qnet, mimo Brno vám rádi pomůžeme vybrat vhodného poskytovatele.

Druhou možností je přesunout vaše aplikace do cloudu, např. k nám do K-net Cloud, kde je zajištěna nejvyšší možná konektivita díky napojení na páteřní síť internetu v České republice.

Další věc, kterou byste měli řešit, chcete-li zajistit spolehlivost spojení, je jeho duplikace, tzn. mít tedy ještě druhé připojení, na které se přesune váš datový provoz v případě výpadku primárního spojení. To stejné platí o serverech, na kterých aplikace provozujete. Pokud server selže, uživatelé nemohou pracovat, a je proto potřeba mít rychle k dispozici druhý server, kde aplikace mohou dál fungovat. Krom přesunu provozu na jiné spojení či server je možné také využívat obou připojení a serverů naráz pro obsloužení velkého množství požadavků uživatelů.

O směřování těchto požadavků, o vhodné rozdělení zátěže mezi dostupná připojení a servery i o akceleraci samotného spojení se stará zařízení typu ADC, neboli Application Delivery Controller. Vhodným zařízením tohoto typu je Citrix ADC. V případě, že vaše aplikace přesunete do cloudu, jako je K-net Cloud, zdvojené připojení i napájení je zajištěno a můžete mít zdvojené i vaše servery, a to dokonce ve více geograficky oddělených lokacích. Zařízení Citrix ADC vám umíme nasadit a je také součástí K-net Cloud, kde je ho možné využít jako službu jak pro vaše aplikace v K-net Cloud, tak pro aplikace ve vašem datovém centru díky naší službě netDispatcher ADC.

ZÁLOHOVÁNÍ

Microsoft 365

VEEAM

IBM

Nezálohujete? Asi jste ještě nepřišli o data. Zálohujete? Dobře. Není však záloha jako záloha. Možná znáte IT vtípek, kde se říká: „Zálohovat dovede každý. Ale jen ti nejlepší z nás zálohu i obnoví, když je potřeba.“ ☺ V kontextu dnešní doby bych ještě dodal, že ne každý ji obnoví nezašifrovanou kryptovirem.

Zálohování se spíše než uživatelů na home office týká dnešního hybridního IT prostředí, tedy kombinace prostředků u vás a v různých cloudech. Data, která jsou umístěna u vás, je vhodné zálohovat pravidelně a automatizovaně, minimálně na jiném zařízení, než na kterém jsou pořizována. Nejlepší je zvolit k tomu určená zálohovací zařízení v oddělených a bezpečných prostorách, tedy např. mimo možnost zaplavení. Pro menší organizace bývá typické využití tzv. NAS neboli síťových úložišť, větší organizace pak používají zálohovací disková pole a pro archivaci dodnes i páskové knihovny. Z hlediska ochrany před nežádoucím zašifrováním doporučujeme mít určitě nějakou zálohu, která je odpojena od vaší sítě a kryptovir se tak k ní nedostane.

Kromě zálohy u vás můžete svá data zálohovat také do cloudu. Pokud jde o vaše serverová data, ať už aplikační, databázová či uživatelská na sdílených discích, můžete využít garantované služby zálohy do cloudu, jako je náš netBackup. To je velice vhodné, jelikož tím máte zálohu v jiné lokalitě než ve vaší vlastní. Zároveň máte jistotu, že se vám o ni stará specializovaný tým, který vám za data smluvně ručí, pravidelně kontroluje funkčnost záloh a je schopen a ochoten vám obnovit váš ztracený soubor. Pokud jde o data z uživatelských zařízení, tak nejjednodušším způsobem zálohování je nastavit jejich synchronizaci do online úložiště, které přichází např. s Microsoft 365, popsaným v minulé manažerské příloze. Data tak má uživatel minimálně na dvou místech – ve svém počítači a v cloudu. Ale pozor! Microsoft za data v rámci této služby neručí. Je vhodné tedy data ze služeb Microsoft zálohovat ještě někam dál, buď k vám nebo do jiného cloudu, např. opět K-net Cloud. Pro tyto scénáře využíváme technologie Veeam a IBM, které vám rádi pomůžeme nasadit nebo poskytneme jako službu společně s garantovaným úložištěm v K-net Cloud.

OCHRANA SÍTĚ

Forcepoint

Kybernetických útoků neustále přibývá a vaše servery a další síťové prvky je potřeba chránit od nepříznivých vlivů z internetu. Pro odrážení útoků na vaši počítačovou síť slouží zařízení typu Firewall. Těm nejmodernějším, které umí odrazit nejsofistikovanější nové útoky, se říká Next Generation Firewall. A co vlastně dělá? Poskytuje například ochranu před vstupem viru do firemní sítě, může filtrovat nebezpečné či jinak nežádoucí aplikace a weby nebo zamezovat komunikaci z nežádoucích lokalit, jako jsou Rusko nebo Čína, z jejichž serverů plyne velká část kybernetických útoků. Oproti standardním firewallům dokážou síťovou komunikaci prozkoumat daleko důkladněji a rozlišovat větší detail, díky čemuž odhalí nežádoucí jevy, které standardní firewall nemůže objevit.

Námi doporučované firewally nové generace jsou Forcepoint NGFW, které poradenská společnost Gartner pravidelné hodnotí jako vizionářské a my s nimi máme velmi dobré zkušenosti u zákazníků i v našem Cloudu. V tomto čísle Loginu si můžete přečíst referenci z nasazení na Moravskoslezském kraji. Zvládneme je tedy nasadit i u vás nebo můžete mít ochranu pomocí Forcepoint jako službu u nás v K-net Cloud pod názvem netDispatcher NGFW. Umíme takto chránit jak vaše servery u nás v cloudu, tak celou vaši lokální síť přes její propojení k nám do Cloudu.

OCHRANA WEBŮ

citrix

acunetix

Také vaše weby jsou otevřeny nástrahám internetu. Web není pouze vaše webová stránka nebo e-shop, ale také informační systém či e-mail dostupný z prohlížeče, provozovaný na vašich serverech. Umístit váš web či webovou aplikaci do internetu bez jakékoli ochrany bude pravděpodobně znamenat její brzké nabourání ze strany hackerů. Vzhledem k tomu, že na webu dnes často sbíráte osobní údaje, na e-shopech v rámci objednávek rovněž (a o důvěrnosti dat v e-mailech či informačních systémech se asi vůbec nemusíme bavit), je jistě velmi nežádoucí, aby k nim někdo nepovolaný získal přístup.

Pro ochranu webů existují specializované technologie WAF, neboli Webový Aplikační Firewall. Pomocí něj můžete např. chránit přihlášení do systému a vytváří zkrátka nárazník mezi vaším webem a útočníky. Typickým útokem je DoS, neboli Denial of Service, tedy útok, kdy útočník vytvoří takové množství dotazů na vaši webovou aplikaci, že ji přehltí, a ta v důsledku toho zkolabuje. Cílem může být vaše prosté ochromení, popř. to, aby nastalého chaosu využil k jinému útoku, kterého si v důsledku toho nevšimnete. WAF dokáže takové a další méně známé útoky rozpoznat a včas zastavit, aby nemohly vaše weby ohrozit.

Mezi výrobci těchto zařízení a software za nás opět boduje Citrix WAF, který vám rádi nasadíme nebo jej opět můžete využít jako naši cloudovou službu, netDispatcher WAF, pro vaše weby a aplikace umístěné u nás i u vás.

Další technologií, která vám pomůže udržet váš web bezpečný, je Acunetix. Web oskenuje a najde všechny bezpečnostní problémy, které váš web má. Je-li bezpečnost vašeho webu opravdu velmi důležitá, můžete si tuto technologii pořídit a nechat si tímto softwarem skenovat váš web pravidelně a vyhodnocovat, jak se vám daří bezpečnost vašeho webu zlepšovat. Technologie je provázaná s Citrix WAF a zjištěné problémy můžete rovnou pomocí WAF řešit úpravou jeho konfigurace. Pokud máte zájem spíše o jednorázovou analýzu jednou za čas, může být vhodnější využít naší služby Penetrační testování.

OCHRANA ZAŘÍZENÍ

Vaše síť je chráněna firewallem před útoky. Pokud máte Next Generation Firewall, tak je chráněna i před viry. Stále však je nutné chránit i samotná zařízení, ať už se jedná o počítače či servery. Potřebujete tedy antivirus. Ten je zvláště důležitý na zařízeních, která si berou uživatelé domů, kdy nemusí být vždy připojeni vzdáleně ve vaší bezpečné firemní síti, a tak jsou zranitelnější. Přitom se pak připojují zpět do vaší interní sítě a virus by tam mohli zanést.

Kromě antiviru je zajímavým rozšířením také sandboxing, což je služba, kdy se stažený soubor při otevření nejdříve odešle do cloudové „zkušebny" výrobce antiviru, kde se pomocí simulace zjistí, jak by se soubor choval nyní, a také, zda by se jeho chování nezměnilo v čase. Některé viry jsou totiž latentní, i několik měsíců jsou zcela neškodné a čekají na vhodnou příležitost, kdy začnou dělat problémy. Třeba 24. prosince večer, kdy jsou všichni doma a virus tak může nerušeně konat svou práci. Sandbox tedy toto chování pomocí zrychlené simulace prozkoumá na měsíce dopředu během pár sekund a soubor buď povolí nebo zamítne k otevření. Jako antiviry doporučujeme a nasazujeme Bitdefender a Eset.

Ochránit zařízení a vaši síť můžete i tím, že uživatelům poskytnete tzv. bezpečný prohlížeč. Jedná se tedy o prohlížeč, který je jim poskytován jako chráněná aplikace z vašeho datového centra nebo z cloudu. Kromě toho, že je dobře chráněn výše zmíněnými technologiemi, tak tím, že reálně neběží na uživatelově zařízení, ale někde na serveru, a má zakázáno stahovat data na lokální disk, jakékoli zavirování by se dotklo pouze tohoto vzdáleného prohlížeče, který správce může jednoduše přemazat a uživatelův počítač to nijak neovlivní. Takový prohlížeč můžete poskytovat z vašeho datového centra pomocí technologií Citrix nebo jej můžete mít jako službu netApps Secure Browser v K-net Cloud.

ZÁVĚR

Doufám, že jste v manažerské příloze našli uchopitelný a ucelený přehled o tom, co vše může či je vhodné řešit, chcete-li zajistit funkční a bezpečné IT, které bude spolehlivě podporovat vaše podnikání či jinou činnost v dnešní hybridní době. Vše se samozřejmě odvíjí od velikosti, typu a specifických potřeb každé organizace. Jsme tu pro vás a pro vaše individuální požadavky. Rádi s vámi prodiskutujeme, jaký přístup nejlépe podpoří bezpečný provoz vaší organizace.

Tématům bezpečnosti dat i zajištění kontinuálního provozu vlastní serverovny, cloudu či hybridního řešení jsme se věnovali v rámci našeho 16. Zákaznického dne. Zhlédněte záznamy z webinářů a získejte tak i vy cenné informace, jak zabezpečit vaši organizaci v dnešním hybridním světě.

Zhlédněte webináře na **k.k-net.cz/16-zakaznicky-den.**

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

En | *IT Security is an important and wide topic today. It's a good idea to have a quality management of who can access what. When working distantly, it's crucial to provide a quality remote support to employees. It's impossible to be productive both on-site and remotely when there is not a reliable and secure connection. Nothing is better for securing against different threats including cryptoviruses than a quality backup. For network security nowadays a Next Generation Firewall is a must have. Both websites and web-based information systems need to be secured from attacks using Web Application Firewalls. Lastly, we shall not forget about endpoint security both using Antivirus as well as secure systems by design which can be made with the use of Citrix technologies, such as Secure Browser.*

K-net Technical International Group, s.r.o.
Olomoucká 170
627 00 Brno – Černovice
tel.: 548 220 150
GSM: 734 686 001
Pobočka: Rovečínská 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

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

Manažerská příloha časopisu LOGIN 2/2020, ročník č. 15 | *Jan Knettig, Blažena Kamasová, Věra Staňková, Jana Hejtmánková, Petr Nepustil*
Vydala společnost K-net | Neprodejné | Uzávěrka čísla: 1. 12. 2020