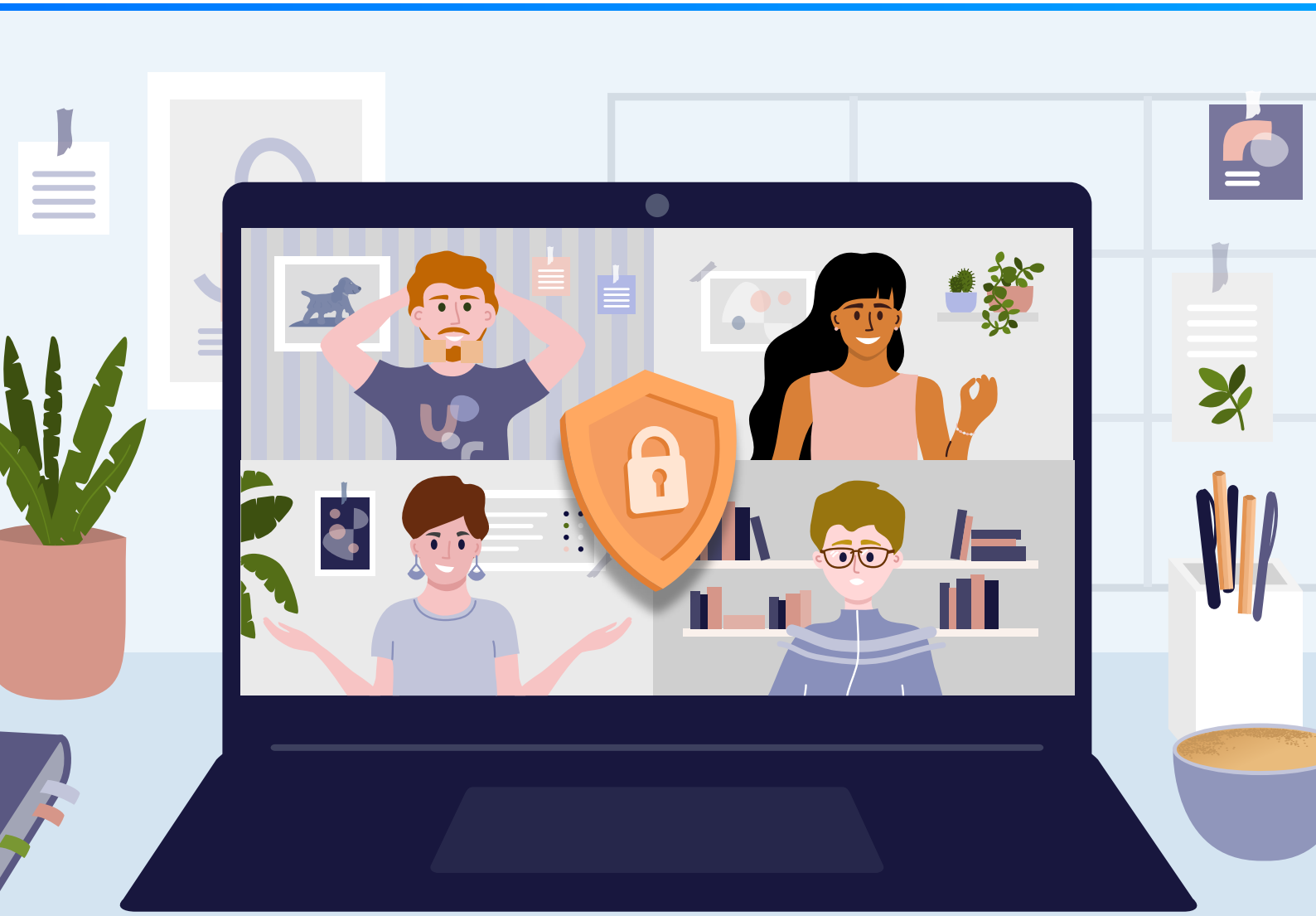
TECHNICKÝ DOKUMENT

Jak zabezpečit vzdálenou pracovní sílu



GFI™

Aurea SMB Solutions

Obsah


Úvod 3

Problémy se zabezpečením, které musí správci IT vzít v úvahu při práci na dálku


Z načný nárůst komunikace on-line 4


Skenování a oprava vzdálených zařízení 5


Zabezpečení domácí sítě 7


Zálohování všech data pomocí šifrovaných záloh 9


Jak obtížné je zabezpečit vzdálenou pracovní sílu? 11


Chraňte svou firmu pomocí **Unlimited | Network Security** 12

Úvod

Vaše malá firma se změnila způsobem, jaký jste nikdy nečekali. A i když nepůsobíte v místech, kde je nařízena práce z domu, je vaším zájmem udržovat své zaměstnance v bezpečí. V důsledku toho se vaše firma mohla částečně nebo úplně přesunout on-line.

Tím se komplikuje nutnost udržovat všechny soubory a komunikaci v bezpečí. Počítače, které jsou hnacím motorem vašeho podnikání, již nemusí být umístěny pouze ve vašich kancelářích.

Co s tím? Váš rozpočet je napjatý. Ve svém týmu nemáte odborníky na vzdálené IT. Váš podnikatelský plán pravděpodobně nepočítal s nutností udržovat věci v bezpečí v případě katastrofické události, při které musí všichni zaměstnanci zůstat doma.

Mnoho firem začalo před pandemií COVID-19 přecházet na vzdálené zaměstnance. Pro ostatní to znamená, že existují zavedené osvědčené postupy a cenově výhodný software, které vám usnadní život a zabezpečí vaši společnost.

Problémy se zabezpečením, které musí správci IT vzít v úvahu při práci na dálku

Značný nárůst komunikace on-line

Nyní, když tolik interakcí a komunikace přešlo na on-line, musíte zajistit, abyste měli silné zabezpečení e-mailu a komunikace.

Zatímco pro zabezpečení videohovorů obecně stačí najít software, který zajistí co nejlepší ochranu soukromí pro vaše potřeby, opatření v případě e-mailů jsou komplikovanější. E-mail je třeba chránit před mnoha hrozbami, včetně neoprávněného přístupu nebo ztráty.

E-mailovými útoky mohou být phishingové útoky, spam nebo malware s klamným předmětem, obsahem, přílohami nebo odkazy, které lákají uživatele. Potřebujete komplexní antispamovou službu společně s poučením zaměstnanců o tom, jak tyto útoky fungují a jak vypadají.

Cílené phishingové útoky na pracovníky z domova se pravděpodobně zvýší, protože záškodníci vědí, že v této nové a potenciálně méně chráněné pozici bude více lidí.

Existuje řada útoků typu „práce z domu“ a jiných, které by mohly lidi stát peníze, riskovat životně důležité informace a otevřít vaši společnost dalším útokům. Potenciální pokusy o hackerství lze rozpoznat, pokud lidé vědí, čeho si všímat. Nabídněte opakovací kurz pro zaměstnance, aby si byli vědomi aktuálních e-mailových podvodů a phishingových útoků.

Záškodníci mohou stále používat nezabezpečený e-mail jako přístupový bod pro vstup do vaší sítě. Chcete-li tomu zabránit, ujistěte se, že má každý silné heslo a zapnuto MFA (vícefaktorové ověřování).

Jako osvědčený postup by vaše společnost měla také zvážit řešení automatického šifrování e-mailů, které analyzuje odchozí e-mailový provoz, rozpoznává citlivý materiál a šifruje e-maily považované za citlivé.

Pokud používáte velký e-mailový klient na bázi prohlížeče, jako je Gmail, každý e-mail již šifrujete pomocí protokolu Transport Layer Security (TLS). Tento typ šifrování není tak bezpečný jako šifrování typu end-to-end, takže pro citlivá data byste měli stále používat jinou službu. Pokud všichni ve vaší společnosti dodržují výše uvedená doporučení, aby udržovali své účty v bezpečí, vyhýbali se malwarovým odkazům a poznali pokusy o phishing, měla by být vaše komunikace pro vzdálenou práci zabezpečená.

Nástroje, které potřebujete pro tento problém se zabezpečením

- Antivirový program s integrovaným skenováním e-mailů
- Nástroje pro internetové zabezpečení a ochranu před phishingem (obvykle integrované do vašeho prohlížeče)

Osvědčené postupy

- Poučte své zaměstnance o všech běžných phishingových a spamových útocích
- Věnujte velkou pozornost všem odkazům a přílohám zasílaným prostřednictvím e-mailu, zejména od neznámých odesílatelů
- Zaveďte zásady pro vhodná hesla
- Zaveďte dvoufaktorové ověřování
- Kodesílání citlivých dat používejte bezpečnější a šifrované metody typu end-to-end

Skenování a oprava vzdálených zařízení

Za normálních okolností váš tým IT postupuje podle harmonogramu a firemního provozu, vydává důležité opravy okamžitě a podle harmonogramů zavádí méně důležité opravy přes noc nebo mimo pracovní dobu, aby omezil rušení personálu. Nyní vaše síť zahrnuje počítače, které již nejsou jen v kanceláři.

Aby byli všichni zabezpečení i při práci z domova, potřebujete software, který skenuje a opravuje všechna vzdálená zařízení. **Každé třetí narušení** je způsobeno neopravenými chybami zabezpečení. Těmto narušením zabezpečení lze zabránit jednoduchým ověřováním, zda jsou vaše počítače plně opravené.

Je to složitější, když využíváte vzdálené pracovníky, ale není to nemožné. Přesně k tomuto účelu jsou vytvořena určitá softwarová řešení. Váš tým IT může s mírnými úpravami dodržovat svůj zavedený plán zabezpečení. Počítače vašich zaměstnanců mohou zůstat aktuální a zabezpečené, i když jsou vzdálené.

Nástroje, které potřebujete pro tento problém se zabezpečením

- Monitor sítě
- Software pro vzdálenou správu

Osvědčené postupy

- Vyhodnoťte svou síť a proveďte kompletní inventarizaci. Pravidelně kontrolujte, zda v síti nechybí opravy
- Ujistěte se, že jsou pokryty všechny operační systémy ve vaší síti (něco, čeho byste se nemuseli bát, kdybyste nepracovali na dálku, když by každý počítač ve vaší kanceláři používal například pouze Windows)
- Naplánujte si čas na zaslání oprav a přitom si uvědomte důležité aktualizace, které je nutné odeslat okamžitě
- Po nasazení je otestujte a buďte připraveni na vrácení oprav, které způsobují problémy, dokud nenajdete řešení nebo nevydáte novou opravu
- Identifikujte všechny chyby zabezpečení pomocí vzdálených skenování, a to i těch, které nejsou způsobeny chybějícími opravami

Zabezpečení domácí sítě

Dalším důležitým krokem k zabezpečení vzdálených pracovníků je zajistit, aby byl jejich systém zabezpečení domácí sítě připravený a robustní.

Šifrování dat při přenosu

Při práci z domova je důležité, aby vaši zaměstnanci šifrovali svá data. Aby se zachovalo soukromí materiálů, měl by každý ve vaší společnosti používat doma při přístupu k citlivým informacím VPN.

VPN poskytuje šifrovaný tunel, který chrání váš webový provoz a odváže vás od vaší konkrétní adresy IP. Vaše společnost a zaměstnanci tak získají více soukromí.

V závislosti na vaší VPN mohou zaměstnanci vnést do vaší sítě větší riziko prostřednictvím připojení k potenciálně nezabezpečeným zařízením. Zajistěte, aby si zaměstnanci byli vědomi tohoto rizika, a VPN používejte pouze při přístupu k pracovním datům.

Šifrovaná síť Wi-Fi

I když je vzácné, že dojde k ohrožení osobní sítě Wi-Fi, může útočník zachytit vše, co posíláte nebo zadáváte on-line: bankovní údaje, e-mailové účty, firemní přihlašovací údaje a další.

Ujistěte se, že je vaše síť správně nakonfigurována a připojení šifrujete. Za nejlepší volbu pro šifrování Wi-Fi je obvykle považováno WPA2 nebo nyní WPA3 a vaše heslo k Wi-Fi musí být silné.

Změny routeru

Měli byste změnit přihlašovací jméno a heslo routeru. Ty mohou být nastaveny z výroby (například „admin“) a mohou být slabé nebo snadno uhodnutelné. Záškodníci toho využívají k podchycení routeru, jeho přeměně na bot, nebo umožnění útočníkům vás špehovat při odesílání on-line informací prostřednictvím routeru. Zajistěte, aby se aktualizace firmwaru instalovaly automaticky, aby se odstranily chyby zabezpečení.

V závislosti na úrovni zabezpečení, kterou vaše firma vyžaduje, můžete také provést další kroky, například aby zaměstnanci omezili příchozí a odchozí síťový provoz, zvolili nejvyšší úroveň šifrování nabízenou v nastavení routeru a vypnuli WPS. Tyto kroky nejsou uživatelsky přívětivé, proto je uplatněte pouze v nezbytných případech.

Úpravy brány firewall

Znovu zkontrolujte nastavení brány firewall, abyste posílili zabezpečení domácí sítě. Brány firewall vytvářejí bariéru, aby zabránily hrozbám dostat se do vašeho systému. Pomáhají dvěma způsoby: zabráněním vstupu škodlivých programů do vaší sítě a zabráněním úniku dat z domácích zařízení.

Brány firewall jsou obvykle ve vašich zařízeních již integrovány; ujistěte se, že jsou ve vašem nastavení povoleny. Pro posílení brány firewall mohou malé firmy potřebovat komplexnější plán zabezpečení od třetího dodavatele.

Zaveďte antivirovou ochranu pro osobní zařízení

Zatímco počítače, které máte v kanceláři, již mohou mít zavedenou antivirovou ochranu, mnoho zaměstnanců nyní používá osobní zařízení, která ji možná nemají. I když budou dodržovat ostatní uvedené rady, špatně zabezpečená zařízení představují významné bezpečnostní riziko.

Ujistěte se, že počítače, které vaši zaměstnanci používají doma, využívají silnou antivirovou ochranu. Vzhledem k okolnostem to může znamenat nákup důvěryhodného antivirového řešení pro zařízení vašich zaměstnanců, přinejmenším v době, kdy jsou povinni mít v nich soukromé firemní údaje.

Je zásadně důležité chránit všechny informace týkající se vaší firmy, což zahrnuje zabezpečení osobních zařízení a zajištění včasných aktualizací těchto řešení.

Nástroje, které potřebujete pro tento problém se zabezpečením

- VPN
- Správa šířky pásma
- Vylepšené nástroje brány firewall
- Řešení antivirové ochrany

Osvědčené postupy

- Při práci v nedůvěryhodných sítích vždy používejte VPN
- Mějte na paměti možnosti šířky pásma ze vzdálené firemní VPN
- Vzdálenou síť VPN své společnosti stahujte pouze na zařízení, která používáte k práci
- Ujistěte se, že metoda ověřování a šifrování VPN jsou nejsilnější možné
- Neustále monitorujte příchozí a odchozí síťovou komunikaci na podezřelou aktivitu
- Mějte pro svou bezdrátovou síť nastaveno silné heslo
- Používejte router, který osobně vlastníte, místo routeru, který vám poskytl váš ISP, a změňte tovární uživatelské jméno a heslo
- Využívejte nejsilnější dostupné funkce brány firewall, které vám stále umožňují přístup k internetu podle potřeby
- Implementujte WPA2 nebo WPA3 ve své bezdrátové síti
- Udržujte svůj router aktuální
- Udržujte své řešení antivirové ochrany aktuální

Zálohujte všechna data s použitím šifrovaných záloh

Data nejsou správně zabezpečena bez pravidelných šifrovaných záloh. To platí bez ohledu na to, zda vaši zaměstnanci pracují z domova či nikoli, ale u vzdálených pracovníků je to ještě důležitější.

Máte méně kontroly nad zařízeními vzdálených pracovníků, a proto si nikdy nemůžete být tak jisti, že je vše plně funkční a zabezpečené. Dokonce i tak obyčejná událost, jako je rozlití kávy na zařízení, může znamenat ztrátu práce nebo dat, pokud nejsou správně zálohovány.

Dobře zabezpečený systém zajišťuje, že všechna firemní data lze zašifrovat, nahrát a zálohovat na centralizovaný zdroj (často v cloudu, ale nemusí to být tam), takže se nemusíte obávat ztráty důležitých informací vinou lidské chyby nebo škodlivých akcí.

Nástroje, které potřebujete pro tento problém se zabezpečením

- Bezpečné úložiště podporující šifrování

Osvědčené postupy

- Často a pravidelně zálohujte
- Data během ukládání šifrujte
- Rozhodněte se, jak dlouho je nutné uchovávat zálohu v závislosti na vaší firmě a jejích zásadách o shodě s předpisy
- Zvažte uložení nejdůležitějších dat na více než jednom místě (zajistěte, aby byla stále šifrována a správně chráněna)

Jak obtížné je zabezpečit vzdálenou pracovní sílu?

Mnoho z těchto navrhovaných kroků vyžaduje jen malé úpravy postupů, které již máte zavedeny nebo jste je prováděli, jako je služba automatizované správy oprav nebo pravidelné zálohy vašich dat.

Na některé změny si možná budete muset zpočátku zvykat, ale existuje mnoho produktů na podporu firem přecházejících na zaměstnance pracující částečně nebo zcela z domova. Dodržováním několika jednoduchých osvědčených postupů a přidáním několika nezbytných nástrojů bude vaše firma a zaměstnanci schopni pracovat vzdáleně a zabezpečeně a zůstat v bezpečí.

Chraňte svou firmu pomocí sady bezpečnostních řešení od GFI

Unlimited | Network Security

Vícevrstvé zabezpečení pro prevenci, detekci a řešení hrozeb pro vaši síť

Zabezpečená síť díky **bráně firewall a prevenci vniknutí**

Zabezpečený síťový provoz díky **webovému a e-mailovému antiviru**

Zabezpečené koncové body díky **monitorování a opravám zranitelností**

Zjistit více

GFI™
Aurea SMB Solutions

ZEBRA SYSTEMS

Zebra Systems s.r.o.
Opavská 6230/29A
708 00 Ostrava
Czech Republic

Tel: +420 596 912 961
Fax: +420 596 912 963
info@zebra.cz
www.zebra.cz