EVERY REGARD s.r.o.
Zámostní 1155/27
Ostrava-Slezská Ostrava, 710 00
IČO: 05460034 – společnost není plátcem DPH

GDPR a bezpečnost na internetu

Jak všichni přechází na práci z domova, řeší se VPN přístupy do firemní sítě. A s ohledem na fakt, že mnoho zaměstnanců pro výkon své práce používalo stolní PC, je pro mnoho zaměstnavatelů nereálné za dané situace vybavit své zaměstnance firemními notebooky. A tak mnohým nezbývá, než pro výkon své práce použít svůj domácí počítač nebo notebook a zaměstnavatelům nezbývá než to přijmout jako fakt, pokud potřebuje, aby jeho zaměstnanci pracovali.

Vidím spoustu rad o rouškách, pracovně právním aspektu homeofficů, mnoho rad, jak ustát nastalou situaci psychicky. Jak doma vidím práci svého IT administrátora, uvědomuji si, jak nízké je povědomí o tom, jak se chránit v online světě a co já sám jako uživatel mohu a měl bych dělat pro bezpečí své, svých osobních údajů a sekundárně pro bezpečí dat a informací svého zaměstnavatele.

Shrnula jsem pár základních věcí, které byste měli mít na zřeteli, pokud začínáte pracovat online. A upřímně jsou to věci, které byste vlastně měli mít na zřeteli vždycky.

Připojení k internetu

Drtivá většina obyvatel ČR využívá připojení od operátorů nebo jiných poskytovatelů internetu. Nutno podotknout, že je to zejména stabilita, až potom rychlost, připojení, která má vliv na to, jak se nám bude pracovat.

> **Jste zaměstnanec:**
> Vaše domácí připojení je pomalé a nestabilní (tím myslím takové to, že vám to pořád kolísá alias laguje) -> VPN spojení bude neustále vypadávat.

Tady je také důležité uvědomit si, že na tom domácím internetu jsou všechny vaše mobily, všechny PC a notebooky a pokud máte moderní domácnost, tak i lednice, kamery, zabezpečovačka a internetová TV. Pokud máte starší nebo prostě nekvalitní router, bude vám to dělat problémy. Na běžnou domácnost, jakou jsem zde popsala, by vám měl stačit běžný 50 Mb/s internet. Pokud ovšem ze svého internetu chcete dostat maximální výkon, potřebujete k tomu i výkonný router. To je ta krabička, které všichni říkají “modem”.
Výkon této krabičky je dost často příčinou toho, že váš internet “laguje” (jsou to drobné vteřinové až několikavteřinové výpadky) a je to takové to, když vy pak naštvaně voláte operátorovi, že už vám to hodinu nejde a operátor vám tvrdí, že žádný výpadek neeviduje a má pravdu. Na kvalitě routeru prostě záleží.
Drtivá většina uživatelů si koupí “modem”, zapojí ho do zásuvky a tím to hasne. K přihlášení do WIFI sítě potom do skonání věků používá přednastavené jméno a heslo, které je na té krabičce někde napsané. Je to tzv. defaultní nastavení – nebo také tovární nastavení.
Takto (ne)nastavený router je základním a často největším bezpečnostním rizikem pro vaši domácnost, protože skrze tuto skříňku je velice snadné dostat se do vaší sítě a cokoliv si z ní stáhnout. Včetně přihlašovacích údajů do vaší banky. Možná si řeknete “kdo by chtěl hacknout zrovna mě”. Musíte si ale uvědomit, ale že hackeři

vymýšlí plošně fungující mechanismy, které to "prostě zkouší" a rozhodně nechcete, aby někdo prostě jenom mapoval, co ve své domácí síti děláte.

TIP:
Většina routerů má postup, jak si nastavení změnit v přiloženém návodu. Minimálně ty přístupové údaje – název WIFI a její heslo. Cena slušných routerů na trhu nejde pod tisícovku. U těch levnějších už se začínáme bavit o mnoha technických kompromisech, které prostě pocítíte.
Chcete si změnit nastavení svého routeru sami? Zadejte do vyhledávače "model routeru změna nastavení" a určitě najdete postup, který pochopí úplně každý. Hezky krok po kroku.
Pokud máte modem od operátora, vyguglila jsem nastavení za vás nejčastější model routeru o T-Mobile, nejčastější model u O2 a nejčastější model u UPC.
To samé platí pro jakékoliv zařízení, které se připojuje k internetu. Váš telefon, bezpečnostní kamery, chytré spotřebiče. Pokud si netroufnete na nastavení sami, využijte buď servisu od značky (každá větší značka má lokální technickou podporu) nebo investujte pár korun (řádově stovky) do toho, že vám s nastavením pomůže odborník.

> **Jste zaměstnavatel:**
> Pamatujete si, jak vám dodavatel vysvětloval, že mít ve firmě kvalitní konektivitu a slušné linky je k nezaplacení. Protože ve chvíli, kdy se vám na server přes VPN snaží dostat 40 zaměstnanců, zjistíte, že stejně nic neudělají, protože k tomu prostě nemají podmínky. No a že byste měli mít taky slušné servery a jiné věci, to je zas na jinou diskusi. Pokud si vaši zaměstnanci stěžují, že jim blbne VPNka a furt jim padá, pravděpodobně bude na vině právě špatná konektivita.

WIFI a nastavení viditelnosti zařízení v síti

Každý z nás jsme zvyklí se s mobilem i s PC připojovat na WIFI takřka kdekoliv, kde to jde. A pokaždé, když to uděláme, vyskočí na nás taková rádoby otravná hláška, kterou drtivá většina z nás prostě přejde.

Ačkoliv nám to tam Windows píše jak pro blbce, nikdo to nečte. Z praxe vím, že drtivá většina z vás klikne na možnost "domácí" a to je strašně špatně. Takže pokud se příště budete v kavárně připojovat na veřejnou WIFI, vyberte možnost Veřejná síť. Odborník na security by vás samozřejmě zasypal jinými doporučeními. Já tento krok vnímám stejně jako mytí rukou po návštěvě veřejné toalety. Navštívila jsem místo plné bacilů, ale když si ty ruce umyji, riziko nějakého nechtěného pozůstatku rozhodně minimalizuji.

TeamViewer

To není sprosté slovo. To je něco, co když si stáhnete do svého PC a budete to mít připravené ve chvíli, kdy se chystáte volat své IT podpoře, budete za mnohem větší frajery, než když se budete machrovat, že už jste to třikrát restartovali a stejně to furt nefunguje…
Ale prosím vás – VŽDYCKY A JEDINĚ A NIKDY JINAK stahujte pouze z oficiální stránky výrobce software. Tady to udělátko je věc, díky které má IT administrátor přístup do vašeho PC a vidí všechno skoro tak jako vy. A vy zase vidíte, co dělá, protože jeho počínání vidíte na monitoru. Vidíte, kam kliká, co kam píše. Nejedná se o žádné hacknutí. Je to účinný nástroj, díky kterému vám "ajťák" pomůže s řešením vašeho PC problému vzdáleně.

Pokud se nacházíte v situaci, že pracujete z domu a váš IT musí váš domácí PC přidat do firemní sítě, usnadněte sobě i jemu život tím, že si TeamViewer nainstalujete. Oni ti ajtý lidi fakt nemají potřebu hrabat se ve vašem domácím pornu. Mají svoje vlastní. Oni jenom chtějí mít jistotu, že když si vás do té své udržované zabezpečené sítě pustí, že jim tam ten váš domácí PC neudělá totální paseku a oni nebudou naráz řešit problém pro dalších XY vašich kolegů a nedej bože ztrátu dat.

Aktualizace operačního systému

Objeví se vždycky, když nejvíc spěcháte, a proto je pořád odkládáte. A někdo je dokonce rovnou zakáže. To je, přátelé, cesta do pekla. Moderní hacking už vám nezamyká klávesnici a nemaže soubory. Moderní hacking vás sleduje. Sleduje vaše chování. Kopíruje si všechno, co v PC máte. Nebo si prostě jenom půjčí výkon vašeho počítače pro své účely, kterými může být páchání jiné trestné činnosti. O ničem z toho se vy jako běžný uživatel nikdy nedozvíte. Většinou se jedná o nějaké přídavné programy, které se vám do PC stáhnou s filmem z torrentů nebo jsou jako součást nějakého dokumentu a jeho otevřením se spustí. Nebo kliknete na odkaz a už stahujete.

Ty dokola se opakující aktualizace nejsou ničím jiným než souborem oprav slabých míst ve vašem PC. Když svůj PC udržujete aktuální, snižujete riziko, že se vám do něj dostane nějaký brajgl. Víte je to stejné, jako když si postavíte dům. Když zanedbáte údržbu svého domu, tak dřív nebo později vám do něj začne zatékat střechou, profukovat pod okny a budou vám plesnivět zdi od vlhkosti.

Pro bezpečí svých dat je naprosto nezbytné aktualizovat. Ne za týden, ne za den. Ihned. Protože aktualizovaný počítač nebo telefon je pro vás tím samým, co nový nátěr na okna nebo ošetření střechy. A vy přeci nechcete, aby vám teklo do baráku.

Antivirové programy

Tady platí že co je zadarmo, není dobré. Existuje mnoho antivirových programů, které jsou v Home edici zdarma. Ale tyto verze jsou spíš zdrojem dat pro vývojáře těch software a jejich uživatelé jsou něco jako testeři. Výrobci si těmito verzemi zdarma testují, kde ještě mají jakou díru v obraně a co všechno ještě přes ten “antivir” prošlo. Doufám, že za svá předchozí slova předejdu žalobě od výrobců, když dodám investujte do koupě legálního antivirového programu.
Uvědomte si, že i na svých domácích počítačích máte mnoho citlivých informací, které když si někdo stáhne, může de facto cokoliv. Skeny rodných listů, bankovní certifikát a přihlašovací údaje od emailu po banku ke všemu.
Velice častý argument – kdo by chtěl hacknout zrovna mě “Pepu Vopršálka”. Co by si ten hacker na mě vzal. Chcete riskovat, že fotky vašich dětí, jak se koupou hambatý v bazénu na zahradě, někdo zařadí do databáze dětského porna na dark netu? Jak se vám líbí představa, že nad fotkami vaší 6leté dcery masturbuje nějaký perverzní hovado? Proto věnujte bezpečnosti svých dat pozornost a naučte se, že to holt stojí prachy.
U nás doma se oblíbenosti těší ESET. Další, které bych dokázala doporučit s klidným svědomím je Avira, BitDefender a se zavřeným jedním okem Norton a Kaspersky. Se zavřenýma oběma očima Avast a AVG.
Pokud máte Windows 10 jako operační systém, máte obrovské štěstí. Protože si opravdu vystačíte s Windows Defenderem, který se v této verzi Windows nebývale povedl a byl vyhlášen nejlepším antivirovým systémem roku 2019. To je program, který ve svém počítači už máte. Nemusíte jej instalovat. Prostě ho mějte zapnutý, moc se v něm nehrabte a pokud vám začne něco hlásit, tak si hodně dobře přečtěte, co po vás chce. A pokud tomu

nerozumíte, udělejte si screen, sdílejte ho třeba na Linkedin, on už se najde někdo schopný, kdo vám opravdu odborně poradí.
A pamatujte si, v případě antivirových programů platí naprostá věrnost a monogamie. JEDEN je akorát. V poslední době jsem na soukromých PC viděla i situace, že uživatel měl na svém PC aktivní Windows Defender a k tomu měl aktivní tři další antivirové programy.
Za prvé vám takové řešení obrovským způsobem ubírá kapacitu a výkon vašeho PC. Za druhé antiviry dost často pracují proti sobě.
Když vám antivirus A prochází složku, kterou chce projít i antivirus B, dostanou se do takové blbé situace. Jeden druhého přesvědčuje, kdo ten soubor zkontroluje, a nakonec se to nepodaří ani jednomu z nich. Kontrola neproběhne korektně. Takže nakonec může nastat situace, že když se dva perou, třetí se směje a tím třetím bude samozřejmě nějaký škodík ve vašem PC.

Přípony známých typů souborů

Když cokoliv stahujete z internetu, vždycky byste si měli být jisti, že otevíráte to, co chcete. Není nic jednoduššího, než EXE soubor (soubory s příponou .exe jsou spustitelné programy) přejmenovat na “obrázek.jpg” a pokud máte skryté koncovky souborů, tak nepoznáte, že jste si do svého PC právě stáhli škodlivý program. Toto je něco, čemu byste měli věnovat svou maximální pozornost, protože se jedná o způsob, kterým se zamoří drtivá většina PC. V praxi to vypadá tak, že vy klikáte na něco, co se tváří jako “obrázek”, který nejde otevřít, ale pravdou je, že jste spustili škodlivý program, který skenuje váš PC a stahuje z něj data. A opět…. Fotky vašich dětí v porno databázi nechcete…

Pokud jste si stáhli dokument nebo tabulku či prezentaci a má divnou koncovku, smažte to. Nemilosrdně. Nezkoušejte na to klikat. Nesnažte se to otevřít. Je to stejné, jako když byste chtěli otevřít krabičku plnou vší a čekali jste, že se ani jedna neusadí ve vašich vlasech. Usadí. Tečka.

Instalování programů do počítače

A s tím souvisí i samotná instalace nových programů. I když stahujete software z oficiálních stránek poskytovatelů a vývojářů, neznamená to, že ty stránky oficiálního poskytovatele nemohl někdo hacknout, že. Takový hack vypadá tak, že při stahování instalačního souboru se stáhne i nežádoucí škodík. Zejména nyní, v době, kdy se mnoho z nás vrací k hraní her, je dobré mít se na pozoru. Pokud stahujete různé cracky nebo třeba titulky k filmům, nebo prostě jenom přehrávač hudby – to všechno může být opatřeno nežádoucím škodíkem.

Každý standardní uživatel při instalaci kliká na tlačítko “další” a příliš nesleduje, co se v tom či onom kroku děje. A dít se toho může hodně.

Součástí instalace třeba starších her může být i instalace starších verzí Acrobat Readeru. Pokud máte WIN7 a další, tak váš PC umí PDF soubory zobrazovat v prohlížeči a nepotřebujete si počítač zabordelit zastaralým software, který stejně nikdy nepoužijete. Mimo jiné tím chráníte kapacitu svého SSD disku, a pokud máte starší typ hardware, tak pořád platí – netahejte si domů staré harampádí.

Mnohem horší je, že součástí instalace mohou být různé pluginy a rozšíření pro prohlížeče, které značně zpomalují výkon počítače a jsou spíše otravné než užitečné. To je třeba Seznam lištička a jiné podobné blbiny. Fujtajbl.

A nejhorší situace je, že součástí instalačního balíčku je nějaký jiný nežádoucí škodík, kterého si do PC nainstalujete, aniž byste to věděli a ke všemu odklikáním celého instalátoru z toho uděláte software s jehož instalací a podmínkami jste souhlasili. No a jsme zpátky u fotek vašich dětí v porno databázi….

Proto VŽDYCKY při instalaci vybírejte možnost variantu “rozšířená” nebo “vlastní” instalace. Ještě se mi nestalo, že by tam ta možnost nebyla. Vypadá to nějak tak, jak na obrázku. Zpravidla buď v tom kroku nebo kliknutí na možnost se zobrazí zaškrtávací tlačítka, která vám jasně ukážou, co všechno si skutečně nainstalujete.

Já osobně bych nedopustila, aby v mé firemní síti byl počítač, který nemá nainstalovaný antivirový program a není aktualizovaný. To je prostě základ. Stejně tak, ve chvíli, kdy se pouští do firemní sítě soukromé stroje, ve kterých je spousta nelegálního software, kladla bych si otázku, zda mi to za to stojí.

Nemusíte nic stahovat, abyste zaplakali nad výsledkem

Vážení a milí, zabordelit si počítač můžete pouhým kliknutím na odkaz. Je to sice starý dobrý oldschool, ale stále funkční a rozšířený. Proto byste měli navštěvovat pouze stránky, které znáte a jsou důvěryhodné. A proč chodit na nebezpečné ruské a čínské stránky, když PornHub aktuálně frčí “zadara”. 😉

Zdravý selský rozum

Největším bezpečnostním rizikem je vždycky a všude uživatel. Tedy každý z nás. Nyní jste v režimu homeoffice připojeni k interním datům. Třeba k zákaznickým datům. A měli byste zajistit, že tyto údaje ochráníte i doma. Měli byste umět zajistit, že vaše děti, které jsou na váš počítač zvyklé chodit, omylem něco nesmažou. Všechno se může stát a za všechno nesete odpovědnost.

Autorkou článku je Lucie Zitterbartová a originál článku najdete na Linkedin.