Malé a střední firmy jsou snadným cílem kybernetických útoků

7.6.2023 - | České Radiokomunikace

Kybernetické útoky na malé a střední firmy a organizace neustále narůstají. Ze statistik vyplývá, že každá druhá firma o velikosti mezi 50 až 250 zaměstnanci se již potkala s nějakou formou kybernetických útoků. Mnoho z těchto útoků firmám způsobilo i značné finanční škody. Ti dobře připravení se ubránili. Naše zkušenost říká, že útočník si raději vybírá snazší cíle, tj. subjekty, které nemají poslední aktualizace na počítačích a komunikačních systémech, mají na většině počítačů účty s administrátorskými právy, nemají dobře definované bezpečnostní politiky, používají slabá hesla bez vícefaktorového ověřování nebo nemají řádně vyškolené uživatele.

Zde je několik základních pravidel a doporučení, které by malé a střední firmy, podniky a organizace měly dodržovat, aby se vyhnuly kybernetickým hrozbám:

1. Zálohování dat

Zamyslete se nad tím, jak moc spoléháte na svá kritická data. Mohou to být údaje o zákaznících, nabídky, objednávky, CRM/ERP systém, finanční ukazatele nebo data pro řízení výroby. Nyní si ale položte otázku – jak dlouho byste byli schopni fungovat bez nich? Všechny firmy a organizace, a to bez ohledu na velikost, by měly pravidelně zálohovat svá důležitá data a současně se ujistit, že jsou tyto zálohy aktuální a lze je obnovit. Tím zajistíte, že vaše firma bude fungovat i v případě nějaké živelní katastrofy. Například po úderu blesku, povodni, požáru, fyzickém poškození nebo krádeži. Navíc, pokud máte zálohy dat, které můžete rychle obnovit, nemůžete být vydíráni pomocí ransomware. Držte se toho jednoduchého návodu:

- určete si, jaká data potřebujete zálohovat a v jakých intervalech;
- zálohujte pravidelně a klíčové zálohy mějte oddělené od své sítě nebo od jednotlivých počítačů (zálohujte nejen na síťové disky nebo cloud, ale i externí disky);
- používejte cloud a cloudové služby pro ukládání a sdílení dokumentů, spolupráci týmů a uchovávání verzí během úprav;
- cloudové služby si dobře zabezpečte a jejich data na šifrujte.

2. Ochrana proti malware

- základem je kvalitní moderní antivirový software s rozšířenou detekcí malware na všech kancelářských zařízeních včetně mobilních telefonů a tabletů;
- zamezte zaměstnancům stahování a instalaci pochybných a nebezpečných aplikací na firemní

počítače a mobilní telefony;

- zaměstnanecké účty by měly mít pouze takový přístup, který je nezbytný pro výkon jejich role. Další oprávnění (např. pro správce) by měla být přidělena pouze těm, kteří je potřebují;
- udržujte všechny operační systémy, firemní programy a komunikační zařízení aktuální. Instalujte poslední verze a aktualizace softwaru ihned po jejich vydání;
- pokud můžete, tak zakažte používání USB portů na všech počítačích. Data sdílejte v cloudu nebo přes bezpečná firemní úložiště a vždy sdílené soubory kontrolujte antivirem;
-

3. Mobilní zařízení

Mobilní technologie jsou dnes nezbytnou součástí moderního podnikání, stále více firemních dat je uloženo v tabletech a chytrých telefonech. Navíc jsou tato zařízení často stejně výkonná jako tradiční počítače, tak je používáme i na cestách pro běžnou práci. Z tohoto důvodu doporučujeme:

- zapněte na telefonech a tabletech zámek a použijte složitější PIN kód (6 znaků). Pokud to telefon umožňuje, aktivujte biometrické ověření (otisk prstu nebo identifikace tváře);
- mobilní zařízení automaticky zálohujte;
- zapněte funkce „najít zařízení“ s možností vzdáleného smazání obsahu v případě ztráty;
- udržujte všechna mobilní zařízení aktuální, instalujte důsledně všechny aktualizace operačních systémů a aplikací;
- v kavárnách, na letištích nebo na veřejných místech (free hotspot) se nepřipojujte k neznámým wifi sítím bez použití VPN.

4. Používání hesel

Firemní notebooky, počítače, tablety a chytré telefony obsahují spoustu důležitých obchodních dat, osobních údajů, dat zákazníků a také podrobnosti o online účtech, ke kterým přistupujete. Je důležité, abyste tato data měli k dispozici, ale aby nebyla dostupná neoprávněným uživatelům. A proto je potřeba používat silná hesla, která jen tak útočník neuhodne. Dnes se pro „lámání“ hesel používají výkonné počítače a sofistikované metody. V tomto případě jsou naše doporučení takováto:

- nastavte si zámky obrazovek a silné heslo do každého zařízení, kam přistupujete;
-
- silné heslo má mít minimálně 16 znaků, malá/velká písmena, speciální znaky a číslice;

- stejná hesla nikdy nepoužívejte pro více účtů;
- pro ukládání hesel používejte heslové manažery;
- při instalaci nového zařízení vždy nejdříve změňte tovární nastavení účtu administrátora.

5. Vyhněte se phishing útokům

Phishing útoky je stále obtížnější odhalit a potkává se s nimi dnes prakticky každá firma. Při typickém phishing útoku podvodníci rozesílají tisícům lidí falešné e-maily, ve kterých jsou obsaženy infikované soubory (doc, xls nebo pdf), a snaží se tak šířit malware nebo uživatele přesměrovat na podvodné webové stránky, aby získali přihlašovací údaje. Například do internetového bankovnictví, přístupy k webovým a cloudovým službám a podobně. Zde je pár dobrých tipů, jak se útokům vyhnout:

- jako ochranu proti phising útokům je důležité správně nastavit oprávnění účtů zaměstnanců (pouze nejnutnější práva pro výkon funkce) a pro klíčové systémy vyžadovat vícefaktorové ověření;
- pravidelné školení zaměstnanců je dnes už nutnost, naučte je, jak rozpoznat phishing emaily a jak na ně reagovat;
- trvejte na dodržování firemních postupů zejména při práci s penězi (placení faktur a podobně). Dobře je popište, seznamte s nimi všechny zaměstnance, a hlavně nedělejte výjimky. Je to nejúčinnější ochrana pro cíleným phishing útokům (sparephishing nebo bossscam);
- důležité je také začlenit pokyny k obraně proti phishing útokům do běžné činnosti. Snažte se je zahrnout do firemní komunikace (uvádění do zaměstnaní/nástupu, bezpečnostní školení, komunikační kampaně, školení pro management, výzvy/bannery v e-mailu, na chodbách a podobně);

na webových stránkách NUKIB (Národní úřad pro kybernetickou a informační bezpečnost) sledujte aktuální hrozby a způsoby, jak se jim bránit.

Pokud se chcete dozvědět více o tom, jak se bránit hrozbám a rizikům, kterým vy nebo vaše firma čelíte, zdarma se přihlaste na jeden z připravovaných webinářů: **Kybernetická bezpečnost pro každého od CRA** určený pro začátečníky nebo **Digitalizujte svou bezpečnou budoucnost s CRA**, který je určen již pro pokročilejší uživatelé.

https://www.cra.cz/male-a-stredni-firmy-jsou-snadnym-cilem-kybernetickych-utoku