enisa

AGENTURA EVROPSKÉ UNIE PRO KYBERNETICKOU BEZPEČNOST

Příručka kybernetické bezpečnosti pro malé a střední podniky

12 KROKŮ

K ZABEZPEČENÍ VAŠEHO PODNIKÁNÍ

Krize COVID-19 zdůraznila důležitost internetu a počítačů obecně pro malé a střední podniky. S cílem zajistit rozvoj podnikání během pandemie muselo mnoho malých a středních podniků přijmout opatření k zajištění kontinuity provozu, jako je využití cloudových služeb, zlepšení internetových služeb, modernizace webových stránek a umožnění zaměstnancům pracovat na dálku.

Tento leták poskytuje malým a středním podnikům 12 obecných praktických kroků s cílem lépe zabezpečit systémy a podnikání. Je to doprovodná publikace k podrobnější zprávě agentury ENISA s názvem **„Cybersecurity for SMES – Challenges and Recommendations“** (Kybernetická bezpečnost pro malé a střední podniky – výzvy a doporučení).

1 VYTVOŘTE KULTURU DOBRÉ KYBERNETICKÉ BEZPEČNOSTI

PŘIŘAĎTE ODPOVĚDNOST VEDENÍ

Dobrá kybernetická bezpečnost je u malých a středních podniků klíčovým prvkem trvalého úspěchu. Odpovědnost za tuto zásadní funkci by měla být svěřena určité osobě v rámci organizace, která by měla zajistit, že se pro kybernetickou bezpečnost vyhradí odpovídající zdroje, například čas pracovníků, nákup softwaru, služeb a hardwaru, odborná příprava pro zaměstnance a vypracování účinných zásad.

ZÍSKEJTE AKTIVNÍ ZAPOJENÍ ZAMĚSTNANCŮ

Získejte zapojení zaměstnanců díky účinné komunikaci o kybernetické bezpečnosti a otevřené podpoře iniciativ v oblasti kybernetické bezpečnosti ze strany vedení a díky vhodné odborné přípravě a jednoznačným a konkrétním pravidlům popsaným v zásadách kybernetické bezpečnosti pro zaměstnance.

VYDÁVEJTE ZÁSADY KYBENERTICKÉ BEZPEČNOSTI

V zásadách kybernetické bezpečnosti pro zaměstnance by měla být uvedena jasná a konkrétní pravidla týkající se očekávaného chování, pokud používají podnikové prostředí, vybavení a služby IKT. V těchto zásadách by se také měly zdůraznit důsledky, kterým by zaměstnanec mohl čelit, pokud by je nedodržoval. Zásady je třeba pravidelně revidovat a aktualizovat.

PROVÁDĚJTE AUDITY KYBERNETICKÉ BEZPEČNOSTI

Osoby s příslušnými znalostmi, dovednostmi a zkušenostmi by měly provádět pravidelné audity. Auditoři by měli mít nezávislé postavení, ať už se jedná o externího dodavatele nebo interního dodavatele malých a středních podniků, a měli by být nezávislí na každodenním provozu IT.

NEZAPOMÍNEJTE NA OCHRANU ÚDAJŮ

Podle obecného nařízení EU o ochraně osobních údajů[1] musí všechny malé a střední podniky, které zpracovávají nebo uchovávají osobní údaje obyvatel EU/EHP, zajistit, aby byla zavedena vhodná bezpečnostní opatření s cílem chránit tyto údaje. V souvislosti s tím je nutné zajistit, aby všechny třetí strany pracující jménem malého nebo středního podniku zavedly vhodná bezpečnostní opatření.

1 Obecné nařízení o ochraně osobních údajů https://ec.europa.eu/info/law/law-topic/data-protection_cs.

2

POSKYTUJTE VHODNOU ODBORNOU PŘÍPRAVU

Poskytujte pravidelnou odbornou přípravu ke zvyšování povědomí o kybernetické bezpečnosti pro všechny zaměstnance s cílem zajistit, že dokážou rozpoznat různé kybernetické hrozby a vypořádat se s nimi. Tato odborná příprava by měla být přizpůsobena malým a středním podnikům a měla by se zaměřit na situace z reálného života.

Poskytujte specializovanou odbornou přípravu v oblasti kybernetické bezpečnosti pro osoby odpovědné za řízení kybernetické bezpečnosti v rámci podniku s cílem zajistit, že budou mít dovednosti a kompetence potřebné k výkonu své práce.

3

ZAJISTĚTE EFEKTIVNÍ ŘÍZENÍ TŘETÍCH STRAN

Zajistěte, aby všichni dodavatelé, zejména ti, kteří mají přístup k citlivým údajům a/nebo systémům, byli aktivně řízeni a splňovali dohodnuté úrovně zabezpečení. Měly by být uzavřeny smlouvy, které upraví, jakým způsobem mají dodavatelé tyto bezpečnostní požadavky splňovat.

4

VYTVOŘTE PLÁN REAKCE NA INCIDENTY

Vypracujte formální plán reakce na incidenty, který bude obsahovat výčet jasných pravidel, funkcí a odpovědností s cílem zajistit, že u všech bezpečnostních incidentů bude následovat včasná reakce provedená profesionálně a vhodným způsobem. S cílem rychle reagovat na bezpečnostní hrozby prozkoumejte nástroje, které by mohly monitorovat podezřelé aktivity nebo narušení bezpečnosti a hlásit upozornění, pokud k nim dojde.

5 ZABEZPEČTE PŘÍSTUP K SYSTÉMŮM

Vydejte výzvu, aby všichni používali heslovou frázi, soubor alespoň tří náhodných běžných slov spojených do fráze, která se snadno pamatuje a zároveň je bezpečná. Pokud se rozhodnete používat tradiční heslo:

- vytvářejte dlouhá hesla s malými a velkými písmeny, případně doplňte čísla a speciální znaky,
- vyhněte se snadno odhadnutelným heslům, například „heslo“, posloupností písmen nebo číslic, např. „abc“, číslům jako „123“,
- nepoužívejte osobní údaje, které lze nalézt na internetu,

A ať už používáte heslové fráze nebo hesla:

- nepoužívejte je nikde jinde,
- nesdílejte je s kolegy,
- povolte dvoufaktorové ověřování,
- používejte vyhrazený software pro správu hesel.

6

ZABEZPEČTE ZAŘÍZENÍ

Zabezpečení zařízení, která používají zaměstnanci, ať už jde o jejich stolní počítače, notebooky, tablety nebo chytré telefony, má v oblasti kybernetické bezpečnosti nezastupitelné místo.

ZAJISTĚTE OPRAVY A AKTUALIZACE SOFTWARU

Nejlépe pomocí centralizované platformy pro správu oprav. Malým a středním podnikům důrazně doporučujeme:

- pravidelně aktualizovat veškerý software,
- pokud je to možné, zapnout automatické aktualizace,
- identifikovat software a hardware, který vyžaduje ruční aktualizace,
- zohlednit mobilní zařízení a zařízení internetu věcí.

ANTIVIRUS

Na všech typech zařízení by mělo být zavedeno centrálně spravované antivirové řešení, které je třeba udržovat aktuální, aby byla zajištěna jeho nepřetržitá účinnost. Neinstalujte pirátský software, protože může obsahovat malware.

ZAVEĎTE NÁSTROJE E-MAILOVÉ A WEBOVÉ OCHRANY

Zaveďte řešení na blokování e-mailového spamu, e-mailů s odkazy na škodlivé webové stránky, e-mailů se škodlivými přílohami, například viry, a phishingových e-mailů.

ŠIFROVÁNÍ

Chraňte data šifrováním. Malé a střední podniky by měly zajistit šifrování dat uložených na mobilních zařízeních, jako jsou notebooky, chytré telefony a tablety. U dat přenášených přes veřejné sítě, jako jsou hotelové nebo letištní bezdrátové místní sítě, zajistěte šifrování dat, a to buď pomocí virtuální privátní sítě (VPN), nebo přístupem na webové stránky prostřednictvím zabezpečeného připojení pomocí protokolu SSL/TLS. Ujistěte se, že jejich vlastní webové stránky využívají při přenosu klientských dat přes internet vhodnou šifrovací technologii k jejich ochraně.

7 ZABEZPEČTE SVOU SÍŤ

ZAVEĎTE SPRÁVU MOBILNÍCH ZAŘÍZENÍ

V rámci zjednodušování práce zaměstnanců na dálku jim mnoho malých a středních podniků umožňuje používat vlastní notebooky, tablety a/nebo chytré telefony. To s sebou nese řadu problémů se zabezpečením citlivých obchodních údajů uložených na těchto zařízeních. Jedním ze způsobů, jak toto riziko zvládnout, je použít řešení MDM (správa mobilních zařízení), které malým a středním podnikům umožňuje:

- řídit, jaká zařízení mají přístup k jejich systémům a službám,
- kontrolovat, zda je v zařízení nainstalován aktuální antivirový software,
- zjistit, zda je zařízení šifrováno,
- ověřit, zda jsou v zařízení nainstalovány aktuální softwarové opravy,
- vynutit, aby bylo zařízení chráněno kódem PIN a/nebo heslem,
- pokud vlastník zařízení nahlásí jeho ztrátu nebo odcizení, nebo pokud má skončit pracovní poměr vlastníka zařízení u malého nebo středního podniku, vzdáleně vymazat ze zařízení všechny údaje malého nebo středního podniku.

ZAVEĎTE BRÁNY FIREWALL

Brány firewall spravují příchozí a odchozí provoz sítě a jsou zásadním nástrojem při ochraně systémů malých a středních podniků. Brány firewall by měly být nasazeny k ochraně všech důležitých systémů, zejména by měla být použita brána firewall k ochraně sítě malých a středních podniků před internetem.

ZKONTROLUJTE ŘEŠENÍ DÁLKOVÉHO PŘÍSTUPU

Malé a střední podniky by měly pravidelně kontrolovat všechny nástroje vzdáleného přístupu s cílem ověřit, že jsou bezpečné, zejména:

- zajistěte, aby měl veškerý software pro vzdálený přístup nainstalovány opravy a aktualizace,
- omezte vzdálený přístup z podezřelých zeměpisných poloh nebo určitých adres IP,
- omezte vzdálený přístup pracovníků pouze na systémy a počítače, které ke své práci potřebují,
- vynuťte silná hesla pro vzdálený přístup a pokud je to možné, povolte dvoufaktorové ověřování,
- zajistěte, aby bylo povoleno monitorování a upozorňování s cílem mít k dispozici varování před podezřelými útoky nebo neobvyklou a podezřelou aktivitou.

8 VYLEPŠTE FYZICKOU BEZPEČNOST

U zařízení, na nichž jsou uloženy důležité informace, by měla být použita vhodná fyzická kontrolní opatření. Například podnikový notebook nebo chytrý telefon byste neměli nechat bez dozoru na zadním sedadle auta. Uživatel by měl před každým odchodem uzamknout svůj počítač. V opačném případě povolte funkci automatického uzamčení na všech zařízeních používaných pro obchodní účely. Také je třeba neustále dohlížet na citlivé tištěné dokumenty a pokud se nepoužívají, bezpečně je uložte.

9 ZABEZPEČTE ZÁLOHY

Aby bylo možné obnovit klíčové informace, je nutné udržovat zálohy, které představují účinný způsob, jak zajistit obnovu po katastrofách, například útoku ransomwarem. Měla by platit následující pravidla zálohování:

- pokud je to možné, zálohování je pravidelné a automatizované,
- záloha se uchovává odděleně od produkčního prostředí malého nebo středního podniku,
- zálohy jsou šifrovány, zejména pokud se přesouvají z místa na místo,
- testuje se schopnost pravidelně obnovovat data ze záloh. V ideálním případě by se měl provádět pravidelný test úplného obnovení od začátku do konce.

10 PROZKOUMEJTE CLOUD

Přestože cloudová řešení nabízejí mnoho výhod, představují určitá jedinečná rizika, která by malé a střední podniky měly před navázáním spolupráce s poskytovatelem cloudových služeb zvážit. Agentura ENISA zveřejnila příručku s názvem „Cloud Security Guide for SMEs“[2] (Příručka zabezpečení cloudových služeb pro malé a střední podniky), kterou by malé a střední podniky měly při migraci do cloudu používat.

Při výběru poskytovatele cloudových služeb by měl malý nebo střední podnik zajistit, aby neporušoval žádné právní nebo správní předpisy tím, že bude ukládat data, zejména osobní údaje, mimo EU/EHP. Unijní nařízení GDPR například požaduje, aby osobní údaje subjektů údajů sídlících v EU/EHP nebyly uchovávány ani přenášeny mimo EU/EHP, pokud nejsou splněny velmi konkrétní podmínky.

---

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

11 ZABEZPEČTE WEBOVÉ STRÁNKY

Je nezbytné, aby malé a střední podniky zajistily, že jsou jejich on-line webové stránky bezpečně nakonfigurovány a udržovány a aby byly náležitě chráněny všechny osobní nebo finanční údaje, jako jsou údaje o kreditních kartách. To znamená, že je třeba provádět pravidelné bezpečnostní testy na webových stránkách s cílem identifikovat potenciální nedostatky v zabezpečení a pravidelné kontroly k zajištění správné údržby a aktualizace webových stránek.

12 VYHLEDÁVEJTE A SDÍLEJTE INFORMACE

Účinným nástrojem v boji proti počítačové kriminalitě je sdílení informací. Sdílení informací v souvislosti s počítačovou kriminalitou má pro malé a střední podniky zásadní význam a umožňuje jim lépe porozumět rizikům, kterým čelí. Společnosti, které se dozví o výzvách v oblasti kybernetické bezpečnosti a o tom, jak byly tyto výzvy překonány, od svých protějšků, podniknou kroky k zabezpečení svých systémů s větší pravděpodobností, než kdyby podobné informace získaly ze zpráv odvětví nebo z průzkumů kybernetické bezpečnosti.

AGENTURA EVROPSKÉ UNIE PRO KYBERNETICKOU BEZPEČNOST

O AGENTUŘE ENISA

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) je agenturou Unie, která usiluje o dosažení vysoké společné úrovně kybernetické bezpečnosti v celé Evropě. Agentura Evropské unie pro kybernetickou bezpečnost, která byla zřízena v roce 2004 a následně posílena aktem EU o kybernetické bezpečnosti, se podílí na kybernetické politice EU, prostřednictvím systémů certifikace kybernetické bezpečnosti zvyšuje důvěryhodnost produktů, služeb a procesů IKT, spolupracuje s členskými státy a subjekty EU a pomáhá Evropě připravit se na budoucí kybernetické výzvy. Sdílením znalostí, budováním schopností a zvyšováním povědomí usiluje agentura společně s hlavními zúčastněnými stranami o posílení důvěry v propojenou ekonomiku, o podporu odolnosti infrastruktury Unie a především o zajištění digitální bezpečnosti evropské společnosti a občanů. Více informací viz www.enisa.europa.eu.

ENISA
Agentura Evropské unie pro kybernetickou bezpečnost

Kancelář v Aténách
Ethnikis Antistaseos 72 &
Agamemnonos 14, Chalandri
15231, Attiki, Řecko

Kancelář v Heraklionu
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Řecko

enisa.europa.eu