NÚKIB

DOPORUČENÁ BEZPEČNOSTNÍ OPATŘENÍ K VAROVÁNÍ ZE DNE 16. DUBNA 2020

Podpůrný materiál

Verze 1.1, platná ke dni 5. 1. 2023

Obsah

Úvod

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) vydal dne 16. dubna 2020 varování před hrozbou v oblasti kybernetické bezpečnosti, spočívající v realizaci rozsáhlé kampaně závažných kybernetických útoků na informační a komunikační systémy v České republice, zejména pak na systémy zdravotnických zařízení (dále jen „varování“). Realizaci této hrozby lze z informací dostupných NÚKIB očekávat v nejbližších dnech od vydání varování.

Tento podpůrný materiál se zaměřuje na technické a organizační otázky spojené s doporučeními NÚKIB, která jsou ve varování obsažena – konkretizuje doporučené postupy správců informačních a komunikačních systémů spadajících pod zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“) a je určen primárně odborníkům zabývajícím se kybernetickou bezpečností. Nejedná se o vyčerpávající výčet všech opatření, které by bylo možné k ochraně informačních nebo komunikačních systémů spadajících pod zákon o kybernetické bezpečnosti (dále jen „systém“) před hrozbou zavést, ale je zpracován především s ohledem na nutnost rychlého přijetí daných opatření. Veškeré informace uvedené v tomto materiálu jsou pouze doporučením, přijetí relevantních opatření k ochraně před hrozbou je vždy na konkrétním správci systému. Správce systémů také musí zvážit aplikovatelnost opatření, možnosti jejich realizace ve svých systémech a dopady na jejich činnosti, poskytování služeb, stejně jako časový plán zavedení.

Pro ostatní subjekty, které nespadají pod zákon o kybernetické bezpečnosti, může být tento podpůrný materiál doporučeným vodítkem pro zvýšení ochrany jejich systémů.

V případě dotazů k tomuto dokumentu nebo varování se prosím obracejte na sekretariát odboru regulace Národního úřadu pro kybernetickou a informační bezpečnost: e-mail: regulace@nukib.cz.

V případě kybernetického útoku nebo hlášení incidentu se prosím obracejte na e-mail cert.incident@nukib.cz. V případě hlášení incidentu mimo pracovní dobu navíc kontaktujte pracovníka vykonávajícího pohotovost na tel.: +420 725 502 878.

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno. Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

1 Opatření pro zabránění nebo zmírnění dopadů kybernetického bezpečnostního incidentu v souvislosti s obsahem varování

1.1 Základní informace k doporučeným úkonům uvedeným ve varování

1.1.1 Mimořádně upozornit uživatele o hrozbách spear-phishingu a připojit výzvu, aby se uživatelé, kteří v posledních dnech otevřeli podezřelé přílohy, obrátili na správce infrastruktury a dále upozornit uživatele na možnost „maskování“ spustitelných souborů v phishingu, např. „obrazek.png.exe“, „text.txt.exe“, „dokument.pdf.exe“ apod.

Cíl opatření: Minimalizovat riziko průniku útočníka do systému za využití spear-phishingu.

Doporučení:

Varovat uživatele o riziku spear-phishingu, a to alespoň v rozsahu následujících témat:

1. Co je spear-phishing (resp. phishing) a jak jej nejčastěji poznat.
2. Nutnost ověření identity protistrany v případě pochybností o legitimitě odesílatele.
3. Neotevírání příloh a odkazů v e-mailech v případě pochybností o legitimitě odesílatele.
4. Nepovolování maker v souborech typu MS Office.
5. Možnost „maskování“ spustitelných souborů (např. „obrazek.png.exe“, „text.txt.exe“, „dokument.pdf.exe“ apod.).
6. Jak se zachovat a kam se obracet v případě podezření na spear-phishing.

V této věci je možné dále využít metodické materiály publikované na webových stránkách https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/. K dispozici je mj. metodický materiál varující o rizicích phishingu. K těmto informacím je dobré také přidat základní kontaktní údaje na personál zajišťující bezpečnost IT a informovat uživatele o nutnosti bezodkladného hlášení v případě obdržení phishingového e-mailu.

Metodický materiál k phishingu, který je možné rozdat či rozeslat uživatelům, je možné stáhnout zde: https://www.govcert.cz/cs/informacni-servis/doporuceni/2735-doporuceni-pro-chovani-v-pripade-obdrzeni-spear-phishingu/.

Pro získání dalších informací je rovněž dostupná obsáhlejší analýza o metodách spear-phishingu a možnostech ochrany zde: https://www.govcert.cz/cs/informacni-servis/doporuceni/2748-spear-phishing-a-jak-se-pred-nim-chranit/.

1.1.2 Zabránit pomocí centrálního nastavení spouštění aktivního obsahu a maker, zejména v .doc a .docx dokumentech

Cíl opatření: Zamezení možnosti kompromitace systému pomocí maker MS Office.

Doporučení:

Makra v dokumentech Microsoft Office jsou velmi často používána jako způsob distribuce malware. Pro minimalizaci tohoto rizika a s ohledem na nutnost rychlosti provedení doporučujeme postupovat následovně, pokud je to pro potřeby organizace vhodné:

1. Zakázat použití maker pro všechny uživatele.
2. Povolit použití maker individuálním uživatelům na základě žádosti.

Postup, jak nastavit příslušnou politiku, naleznete v dokumentaci na stránkách společnosti Microsoft.[1]

1.1.3 Okamžitě zablokovat vzdálené přístupy do infrastruktury a zablokovat otevřené služby do veřejné sítě, vyjma těch nezbytně nutných (veřejné IP rozsahy lze zkontrolovat v dostupných vyhledávačích zařízení připojených do sítě a zjistit tak i historicky otevřené či zapomenuté porty, nebo služby dostupné z veřejné sítě)

Cíl opatření: Minimalizovat riziko průniku útočníka do systému za využití zranitelností v systému nebo útoku hrubou silou.

Doporučení:

Ověřit služby, které jsou publikovány do internetu. Ponechat otevřené pouze takové služby, které jsou nezbytné pro fungování organizace. Mezi tyto služby patří především komunikace:

1. nezbytná pro fungování systémem podporovaných služeb,
2. nezbytná pro bezpečnost systému (vzdálený monitoring, bezpečnostní aktualizace systémů apod.),
3. nezbytná pro informování veřejnosti (e-mailové komunikace, webové prezentace apod.),

[1] https://docs.microsoft.com/en-us/DeployOffice/security/plan-security-settings-for-vba-macros-in-office?redirectedfrom=MSDN#changedefault

4. nezbytná pro podpůrné infrastrukturní komunikace (protokoly DNS, BGP, kontrola platnosti certifikátů apod.) a proxy servery.

Primárně se jedná o omezení přístupu služeb z internetu (jako např. přístup přes protokoly typu VPN, RDP, SSH, SMB, databázové přístupy, administrace systémů), pokud jsou propojeny na důležité systémy a pokud nesplňují jednu z výše uvedených podmínek.

Pokud není možné některé přístupy zablokovat, je vhodné povolit přístup pouze přes VPN nebo pro vymezené IP adresy.

1.1.4 Okamžitě vytvořit offline zálohy a postupovat v zálohování dle důležitosti dat v organizaci

Cíl opatření: Zajistit dostupnost záloh i v případě kybernetického bezpečnostního incidentu.

Doporučení:

Pro bezpečné uchování záloh je nutné tyto zálohy zkopírovat i na offline datové médium (flash disk, hard disk nebo jiné) a tato nahraná data verifikovat. To lze provést v ideálním případě obnovením zálohy z tohoto nově vytvořeného média. Toto lze samozřejmě provádět pouze mimo produkční prostředí. Pokud to ale nebude z technických důvodů možné, lze ověřit alespoň hashe souborů offline zálohy vůči hashům online zálohy. Tato procedura je nutná pro to, aby v případě kompromitace (nebo zašifrování) zálohovacího serveru či virtualizační platformy nedošlo ke ztrátě záloh.

1.1.5 Zkontrolovat konzistenci již vytvořených záloh

Cíl opatření: Zajistit funkčnost záloh i v případě kybernetického bezpečnostního incidentu.

Doporučení:

Prověřit, zda jsou aktuální zálohy funkční a to tím způsobem, že se provede testovací obnova serverů a stanic. Toto lze samozřejmě provádět pouze mimo produkční prostředí. V případě, že je zjištěna nefunkčnost jedné nebo více záloh, je třeba okamžitě provést novou zálohu systému. V rámci těchto úkonů je nutné postupovat od nejkritičtějších systémů. Při prověřování záloh nelze opomenout ani vzájemné závislosti. Příkladem může být databázový server nebo celý databázový cluster, který je nasazen jinde. Při kontrole je pak potřeba provést i test těchto systémů.

1.1.6 Aktualizovat antivirové řešení v infrastruktuře

Cíl opatření: Zajistit elementární ochranu zařízení před škodlivým kódem.

Doporučení:

Nástroj pro ochranu před škodlivým kódem (antivirus, antimalware) by měl být nasazen na všech možných systémech, vč. serverových operačních systémů. Primárně se jedná o operační systém Windows, neboť je ve většině případů cíleno právě na něj. V případě virtualizovaných systémů není možné považovat ochranu pomocí agentless řešení za dostatečnou.

Pokud není v organizaci použit žádný nástroj pro ochranu před škodlivým kódem, je nutné alespoň aktivovat zabudovanou ochranu systému, pokud takovou systém obsahuje.

1.2 Další doporučení, která lze provést pro zabránění nebo zmírnění dopadů kybernetického bezpečnostního incidentu

Níže uvedená doporučení jsou seřazena podle priority, která by jim měla být přiřazena.

1.2.1 V rámci systémů provést změnu hesel u privilegovaných účtů. Překontrolovat a popřípadě nastavit vhodnou politiku pro využití privilegovaných účtů.

Cíl opatření: Zamezit případnému útočníku vyskytujícímu se v systému v další činnosti.

Doporučení:

Opatření spočívá ve vynucení změny hesel všech privilegovaných účtů způsobem stanoveným pro povinné subjekty dle platné vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, tedy minimálně 17 znaků s nutností jejich obnovy alespoň každých 18 měsíců. Pro ostatní subjekty, které nespadají pod zákon o kybernetické bezpečnosti, je tato politika doporučená. Nutné je také provést audit privilegovaných účtů a zablokovat ty, které již nejsou využívané, případně odebrat oprávnění těm účtům, které daná oprávnění nepotřebují.

Pro nastavení politiky hesel doporučujeme použít *Fine Grained Password Policies*[2], což umožní nastavit politiky hesel pro různé skupiny uživatelů. Pro nastavení vhodné politiky pro využití privilegovaných účtů také doporučujeme použít *Active Directory administrative tier model*.[3]

Je také nutné zamezit doménovým administrátorům, aby se přihlašovali na jakékoliv stanice a servery s výjimkou doménového řadiče. Důvodem je zamezit útočníkovi získání

[2] Dokumentace Microsoftu k dané problematice dostupná na https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770394(v=ws.10)?redirectedfrom=MSDN
[3] Dokumentace Microsoftu k dané problematice dostupná na https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

privilegovaného účtu. Tím, že hash administrátora zůstane zaznamenán v cache stanice, může útočník získat oprávnění doménového správce při kompromitaci stanice.

1.2.2 Ověřit a zajistit, že systém záloh je od ostatních systémů oddělen tak, že ani získání nejvyššího oprávnění k systému, který je zálohován, nemůže umožnit smazání záloh.

Cíl opatření: Zamezit útočníkovi možnost smazání záloh v případě získání oprávnění doménového administrátora.

Doporučení:

Zabezpečit systém záloh tak, aby v případě kompromitace privilegovaného účtu, např. Domain/Enterprise Administratora, nedošlo zároveň ke kompromitaci zálohovacího systému a následně ke smazání či poškození záloh.

Pokud je totiž možné zálohovací systém spravovat přes sdílený privilegovaný účet (např. Domain/Enterprise Administratora), útočník může zálohy smazat, poškodit či zašifrovat.

V prostředí Microsoft Windows je možné toto vyřešit odpojením fyzických i virtuálních strojů zajišťujících službu zálohování z domény a pro přihlášení používat lokální účty, případně vytvořit speciální účet pro tuto činnost. Je však potřeba zhodnotit dopad na další služby a funkcionality systému.

1.2.3 Zamezit přístup a propojení mezi systémy důležitými pro zajištění fungování organizace a systémy nebo sítěmi, které nejsou důležité pro poskytování služeb nebo bezpečnost systému.

Cíl opatření: Zamezit propojování systémů mezi sebou (vyjma nezbytných případů) a tím omezit možnost šíření malware.

Doporučení:

Jedná se o omezení komunikace na systémy, které jsou nezbytné pro fungování organizace (zejména pro poskytování služeb). Pokud tedy existuje přístup z jiné sítě (např. z internetu, ze sítě jiné organizace či z jiné sítě organizace) do sítě, která je nezbytná pro zajištění fungování organizace, musí být zváženo, zda je tento propoj důležitý pro poskytování služeb nebo bezpečnost systému.

Omezit komunikaci mezi pracovními stanicemi tam, kde je to možné.

1.2.4 Zkontrolovat segmentaci sítě a řízení provozu mezi segmenty, situaci vyhodnotit a přijmout nezbytná opatření k zajištění alespoň elementární segmentace.

Cíl opatření: Zamezit šíření malware, nebo pohybu útočníka.

Doporučení:

Segmentace sítě a řízení provozu mezi segmenty (prostupy mezi segmenty, omezení povolených služeb) může značně snížit dopady případného kybernetického bezpečnostního incidentu. Proveďte kontrolu nastavení vašich síťových prvků s cílem identifikovat slabá místa a příliš benevolentní pravidla. Kontrolu proveďte také mezi vnější a vnitřní sítí. Restriktivní pravidla mohou ztížit práci útočníkům a poskytnou organizaci čas pro reakci.

Omezit komunikaci mezi pracovními stanicemi tam, kde je to možné.

1.2.5 Zvážit aktualizaci všech používaných systémů, za podmínky, že bude taková aktualizace otestovaná. Pokud je aktualizace otestovaná a funkční, tak ji provést.

Cíl opatření: Zajistit aktuálnost používaných systémů a tím zvýšit jejich bezpečnost a odolnost před kybernetickými bezpečnostními incidenty.

Doporučení:

Neaktualizované systémy často obsahují známé chyby, které útočníci využívají ke kompromitaci systému. Proto je nutné v rámci možností zajistit aktuálnost používaných systémů. Pokud tomu brání závažný důvod (například aktualizací by byla porušena záruka, mohlo by dojít k rozpadu systému, nefunkčnosti nebo k jiným neakceptovatelným dopadům) není nezbytné aktualizaci provést. Je však potřeba zajistit náhradní bezpečnostní opatření.

Především je nutno mít na paměti, že aktualizace nemá být provedena, pokud by toto způsobilo větší škodu než případný kybernetický bezpečnostní incident nebo by provedení takového úkonu mělo negativní dopad na poskytování služeb.

Aktualizace musí být v každém případě předem otestována, jak je uvedeno výše, a to mimo produkční systémy.

1.2.6 Prověřit platné plány kontinuity činnosti a havarijní plány související s provozováním systémů s cílem ověřit jejich platnost, účinnost a použitelnost zejména s ohledem na možnou nedostupnost těchto systémů.

Cíl opatření: Ověření, že existují plány kontinuity činností a havarijní plány a že jsou aktuální a použitelné za účelem jejich použití v případě nutnosti.

Doporučení:

Prověřit, zda jsou plány kontinuity činnosti a havarijní plány aktuální a platné, případně zda některé nechybí. Primárně je nezbytné se zaměřit zejména na ověření následujících bodů:

- plány rozlišují důležitost systémů a počítají s prioritní obnovou kritických systémů,
    - v rámci prioritizace obnovy systémů je zohledněna vzájemná závislost systémů a služeb,
- plány obsahují seznamy osob zodpovědných za jednotlivé prvky systémů a jsou k dispozici aktuální kontakty na odpovědné osoby,
- existuje aktuální seznam dodavatelů a kontaktních osob za dodavatele včetně kontaktů (mobilní telefony, e-maily); je třeba prověřit nastavení spolupráce s dodavateli v případě mimořádné události, dohodnuté reakční doby apod. (v případě nedostatků či absence dohody doporučujeme dohodnout se s dodavateli na pravidlech spolupráce v případě mimořádné události).

1.2.7 Zajistit uchování plánů kontinuity činností a havarijních plánů souvisejících s provozováním systémů odděleně od systémů, pro které jsou tyto plány zpracovány (např. na odděleném paměťovém médiu, v tištěné podobě, apod.).

Cíl opatření: Zajistit dostupnost plánů v případě incidentu za účelem jejich použití v případě nutnosti.

Doporučení:

Ze zkušenosti s ransomware útoky vyplývá, že plány kontinuity činnosti, havarijní plány a další obdobná dokumentace jsou často uloženy na úložištích, která útočník zašifruje či vymaže, případně jsou v rámci ochrany ostatních systémů tato úložiště vypnuta. Následně nejsou tyto plány v kritických okamžicích dostupné. Z uvedených důvodů je nutné tyto plány uložit mimo systémy, např. na výměnné médium, které bude chráněno proti neautorizovanému zápisu (pro případ nutnosti připojení úložiště do potenciálně napadeného počítače), či je mít v tištěné podobně.

1.2.8 Pokud plány kontinuity činností a havarijní plány související s provozováním systémů nejsou aktuální či nebyly zpracovány, zpracovat tyto plány alespoň pro nekritičtější systémy důležité pro poskytování služeb.

Cíl opatření: Disponovat aktuálními a použitelnými plány kontinuity a havarijními plány, aby byla organizace schopna fungovat i v případě kybernetického bezpečnostního incidentu.

Doporučení:

V případě, že plány kontinuity činnosti a havarijní plány chybí, je potřeba provést jejich vypracování alespoň v takové míře, aby podle nich bylo možné opět zajistit dostupnost důležitých systémů. Prioritně by měly být řešeny tyto body:

- Stanovit práva a povinnosti administrátorů a osob podílejících se na zajištění chodu organizace. Kdo, kdy, a co má v průběhu mimořádné situace dělat. Např. eskalační postupy atd.
- Pomocí hodnocení rizik a analýzy dopadů vyhodnotit a posoudit možná rizika související s ohrožením kontinuity činností. Je nutné sestavit možné elementární scénáře toho, co se stane v případě narušení důvěrnosti, dostupnosti a integrity dat v systémech a co to bude znamenat pro poskytování dané služby.
- Na základě výstupů hodnocení rizik a analýzy dopadů stanovit cíle řízení kontinuity činností formou určení
    - minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu systému,
    - doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb systému, a
    - bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.
- Vytvořit postupy, které budou obsahovat naplnění cílů podle předchozího bodu. Tzn., jakým způsobem organizace dosáhne toho, aby udržela určitou úroveň služeb, aby byla schopna obnovit data atd.

1.2.9 Nemazat jakákoliv data o kybernetickém bezpečnostním incidentu bez svolení Policie ČR nebo NÚKIB, a poučit o této povinnosti všechny administrátory a všechny relevantní bezpečnostní a IT (provozní) role.

Cíl opatření: Zajistit možnost vyšetření kybernetického bezpečnostního incidentu.

Doporučení:

Všechna data (obrazy serverů, bezpečnostní záznamy, záznamy ze síťového monitoringu, a další) jsou důležitá pro vyšetření kybernetického bezpečnostního incidentu, zejm. aby bylo možné určit zdroj a způsob šíření malware v rámci sítě a identifikovat, která zařízení mohla být infikována. Taktéž u některých typů ransomware existuje možnost data následně dešifrovat. Proto je důležité tato data nemazat bez povolení Policie ČR nebo NÚKIB.

Je nutno zdůraznit, že i neopatrná manipulace s daty může vést ke ztrátě metadat důležitých pro šetření incidentu. To může zkomplikovat i následnou pomoc. Povinné osoby podle zákona o kybernetické bezpečnosti musí kybernetický bezpečnostní incident hlásit bezodkladně po jeho detekci. Všem ostatním doporučujeme taktéž okamžitě kontaktovat Úřad a incident nahlásit. Pro hlášení incidentů lze použít e-mailovou adresu cert.incident@nukib.cz, v mimopracovní době nejprve kontaktujte pohotovostní číslo +420 725 502 878.

1.2.10 Pouze pro poskytovatele zdravotních služeb: Vyčlenit komunikační síť lékařských přístrojů – modality (např.: CT, rentgeny), od zbytku sítě.

Cíl opatření: Oddělit lékařské přístroje od zbytku sítě a tím omezit šíření malware v síti.

Doporučení:

Aby bylo možné zajistit požadované služby i po případném kybernetickém bezpečnostním incidentu, je nutné oddělit síť lékařských přístrojů od ostatních systémů tak, aby tyto přístroje dokázaly fungovat i při odpojení od zbytku sítě. Prostupy mezi sítěmi jsou možné, ale musí být řízeny formou whitelistingu povolených komunikací. Provedení daných opatření je nezbytné pro zachování bezpečnosti daných systémů, neboť tyto specializované systémy mnohdy běží na unikátních a zastaralých operačních systémech a další metody zabezpečení těchto systémů nelze vždy aplikovat.

1.2.11 Obecná doporučení NÚKIB pro administrátory

Vedle všech výše uvedených doporučení zaměřených přímo na varováním danou hrozbu, považuje NÚKIB za vhodné zmínit také dokument „Bezpečnostní doporučení pro administrátory“. Tato doporučení jsou určena jak manažerům kybernetické bezpečnosti, tak vedoucím pracovníkům IT oddělení a obecně všem, kdo se zajímají o kybernetickou bezpečnost v praktické, pracovní rovině. Dokument je možné stáhnout zde: https://www.govcert.cz/cs/informacni-servis/doporuceni/2736-doporuceni-nukib-pro-administratory-verze-4-0/

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
17. 4. 2020	1.0	Odb. regulace Odb. Vládní CERT	Vytvoření dokumentu
5. 1. 2023	1.1	Odb. regulace	Změna kontaktních údajů