ZÁKLADNÍ BEZPEČNOSTNÍ DOPORUČENÍ PRO ŠKOLY

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

AFCEA

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

Verze 1.0, platná ke dni 11. května 2021

Obsah

Upozornění:

Tento dokument je primárně určen pro základní a střední školy a může být volně šířen.

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

1 Úvod

Tento dokument představuje základní principy, postupy a doporučení v oblasti kybernetické bezpečnosti **pro školy, případně další organizace, které nespadají pod regulaci zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále též „ZKB“)**. V dokumentu použitý přístup staví na řízení námi předpokládaných rizik, na jejichž základě jsou navržena přiměřená bezpečnostní opatření. Cílem těchto opatření je chránit informační aktiva škol a poskytnout námi předjímanou odpovídající míru bezpečnosti.

Tento dokument je primárně určen pro ICT administrátory, ICT koordinátory a vedení škol.

Doporučení jsou rozdělena do dvou skupin. První skupina doporučení je označená jako **Základní opatření**, druhá skupina je označována jako **Rozšiřující opatření**. Základní opatření by podle nás měla být implementována všemi subjekty. Při volbě základních opatření byly zohledněny požadavky na snadnou implementaci a nízké náklady (reflektujeme omezené finanční a personální kapacity škol). Rozšiřující opatření navrhujeme jako nepovinná, přičemž byla vybrána ta opatření, která mají velký efekt a rozumné náklady na implementaci. Doporučení jsou vhodná zejména tam, kde se s nastavováním zabezpečení začíná.

U škol (a dalších subjektů) **doporučujeme aplikovat** Minimální bezpečnostní standard, který v roce 2020 vydal Národní úřad pro kybernetickou a informační bezpečnost ve spolupráci s Národní agenturou pro komunikační a informační technologie, s. p., (NAKIT) a Ministerstvem vnitra ČR.[1]

1.1 Další zdroje z oblasti kybernetické bezpečnosti

V případě potřeby zavedení komplexního systému řízení bezpečnosti informací nebo jako zdroj inspirace lze využít vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VKB“).

Webové stránky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) mohou rovněž sloužit jako zdroj informací o problematice kybernetické bezpečnosti. Lze je nalézt pod tímto odkazem: https://www.nukib.cz.

NÚKIB dle potřeby vydává další podpůrné materiály, které lze využít v rámci řešení jednotlivých oblastí kybernetické bezpečnosti. Tyto materiály jsou dostupné zde: www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/. Dalším zdrojem jsou také informace o aktuálních hrozbách, které lze nalézt zde: www.nukib.cz/cs/infoservis/hrozby/, nebo doporučení, která se nacházejí zde: www.nukib.cz/cs/infoservis/doporuceni/.

Při zabezpečování informací a osobních údajů musí být rovněž zohledněno nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti

[1] dostupné zde: https://nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

se zpracováním osobních údajů a o volném pohybu těchto údajů a k tomu vydané metodické pokyny MŠMT. Více zde: https://www.msmt.cz/dokumenty-3/gdpr-na-skolach.

V dokumentu jsou použity některé termíny a zkratky typické pro oblast ICT a kybernetické bezpečnosti. Použité zkratky jsou vysvětleny v kapitole 5. Pro výklad terminologie z oblasti ICT a kybernetické bezpečnosti odkazujeme na Výkladový slovník kybernetické bezpečnosti (více v kapitole 4).

2 Základní bezpečnostní opatření

Základní bezpečnostní opatření jsou koncipována jako opatření, která by měla mít každá škola implementována.

Jako nástroje pro implementaci dále uvedených bezpečnostních opatření obecně **doporučujeme zvažovat open source řešení**, ovšem při zajištění jeho odpovídajícího návrhu, implementace, správy a podpory.

2.1 Zabezpečení sítě

Nepřetržité připojení organizace k internetu má za následek její vystavení nehostinnému prostředí a rychle se vyvíjejícím hrozbám. Zaměstnanci mohou navíc svými činy, ať už úmyslně nebo neúmyslně, interní síť ohrozit. Proto je její zabezpečení jednou z klíčových činností k ochraně dat organizace.

Zabezpečení sítě má obecně tři základní cíle:

- Ochránit samostatnou síť.
- Snížit náchylnost koncových zařízení a aplikací vůči hrozbám ze sítě.
- Chránit data během přenosu.

2.1.1 Segmentace sítě

Rozdělení počítačové sítě do logických celků (segmentů) přispívá k lepší orientaci a snadnější správě samotné počítačové sítě. Následně je nutné efektivně definovat pravidla pro komunikaci do daného segmentu. Tato komunikace by měla být omezena na nezbytné minimum. Pokud dojde k napadení takto segmentované sítě škodlivým kódem, nedochází k rozšíření škodlivého kódu po celé síti, ale jen v daném segmentu napadení. Tím eliminujeme výsledné škody.

Samostatné segmenty by měly být vytvořeny minimálně pro následující kategorie systémů, pokud takové systémy škola provozuje:

- Servery poskytující služby do sítě internet (DMZ)
- Servery poskytující služby do interní sítě školy
- Uživatelské stanice zaměstnanců školy (počítače učitelů, administrativních zaměstnanců apod.)

- Stanice užívané v rámci výuky na učebnách
- Soukromá zařízení žáků a návštěvníků připojujících se na Wi-Fi školy

2.1.2 Ochrana perimetru

Jak bylo již uvedeno v úvodu, připojení organizace k internetu znamená být připojen k prostředí, ve kterém se kybernetické hrozby dynamicky vyvíjí. Je tedy v zájmu organizace zabezpečit perimetr počítačové sítě:

- Povolit pouze nezbytný provoz mezi segmenty a sítí internet (např. povolení komunikace ze stanic v učebnách do internetu pouze na porty TCP 80 a 443 apod.).
- Povolit přístup k systémům školy ze sítě internet výhradně na stroje umístěné v samostatném segmentu DMZ.

2.1.3 Bezpečnost bezdrátových sítí

Přestože možnost bezdrátového připojení do sítě přineslo řadu výhod v podobě zvýšení mobility a produktivity zaměstnanců, ruku v ruce představilo také řadu hrozeb a výzev. V mnoha případech může dojít ke krádežím duševního vlastnictví či citlivých informací právě skrze bezdrátové sítě, a to z důvodu obcházení tradičních sítí segmentovaných a chráněných na perimetru pomocí firewallu či IDS.

Pro zajištění bezpečnosti by měla být dodržena následující opatření:

- Veškerý provoz u organizací spravovaných zařízení musí být zabezpečen minimálně AES šifrováním a standardem WPA2-Enterprise. Zabezpečení WPA2-PSK technologií se ve větších organizacích nedoporučuje; **zabezpečení WEP technologií je silně nedostačující!**
- Pro nespravovaná zařízení je vyhrazena síť pro hosty, skrze kterou není možné přistupovat k interním systémům či aplikacím kromě těch, jež jsou dostupné z internetu.

2.1.4 Soukromá zařízení (trend BYOD)

Jde o koncept, který v poslední době neustále nabývá na popularitě a umožňuje zaměstnancům přinést si svá vlastní zařízení do prostředí organizace. Zatímco toto řešení přináší z uživatelského hlediska řadu výhod, z pohledu bezpečnosti se sebou nese několik rizik, která je nutné uvážit:

- Ztráta zařízení společně s daty organizace.
- Zaměstnanci mohou, třebaže nezáměrně, nainstalovat celou řadu aplikací, mezi nimiž může být i malware.
- Integrace rozličných zařízení s různými OS do prostředí organizace.

Předtím, než se rozhodne o povolení užívání vlastních zařízení v organizaci, by mělo dojít k provedení analýzy rizik, na jejímž základě by bylo možné rozhodnou, zda organizace dokáže řídit související rizika. Pokud se organizace rozhodne pro zavedení BYOD, pak je nezbytné zavést sérii protiopatření ke zmírnění rizik. Souhrn takových protiopatření je dobré přetvořit v interní politiku/směrnici, která by měla obsahovat:

- Upřesnit, na koho se politika vztahuje (zaměstnanci, dodavatelé aj.).
- Zařízení, která mohou být použita (notebooky, telefony aj.).
- Služby a informace, které jsou zpřístupněny takovým zařízením (e-mail, sdílená úložiště aj.).
- Odpovědnosti zaměstnavatele a zaměstnanců (včetně odpovědnosti za bezpečnostní opatření, která je nutné přijmout a implementovat).
- Sankce za nedodržování politiky/směrnice

2.1.5 Vzdálený přístup

V dnešní době existuje celá řada technologií, prostřednictvím kterých je možné zprostředkovat vzdálený přístup do interní sítě. Nicméně stejně jako v případě bezdrátových technologií i zde je důležitá kontinuální správa, aby nedošlo k neautorizovanému přístupu k interním službám.

K zajištění bezpečného vzdáleného přístupu je dobré dodržet následující body:

- Vytvořte zásady vzdáleného přístupu a seznamte s nimi zaměstnance, aby se jimi řídili.
- Vzdálený přístup by měl být poskytován pouze pomocí zabezpečených technologií VPN. Vyvarujte se vytváření přímého přístupu k systémům pomocí dostupných SSH a RDP služeb z internetu. Případně omezte přístup pouze na konkrétní IP adresu a nastavte přístup min. prostřednictvím certifikátu s heslem.
- Služba VPN by měla být nakonfigurovaná tak, aby nebylo povolen tzv. *split tunnelling*.
- Monitorujte a logujte všechna spojení vzdáleného přístupu.
- Vynuťte více faktorovou autentizaci pro všechna spojení.

2.2 Řízení uživatelských oprávnění

Není vhodné, aby zaměstnanci školy a žáci měli plná, tzv. administrátorská práva na počítači. Uživatel s administrátorskými právy může měnit nastavení operačního systému, instalovat nelegální software nebo spouštět nebezpečné soubory. Uživatel s neomezenými právy může kompromitovat počítač a ohrozit ostatní počítače v síti.

Výjimku pak může tvořit výuka v oblastech, pro něž je používání účtů s vysokými oprávněními nezbytné (např. výuka administrace OS), přičemž tato výjimka musí být podmíněna segmentací a/nebo restrikcemi vůči zbytku sítě.

Optimální cestou je centrální řízení účtů s využitím adresářových služeb, které umožňují správci sítě z jednoho místa spravovat uživatelské účty, definovat politiku hesel a nastavit práva pro přihlášení na jednotlivé počítače.

Pokud není možné využít centrální řízení účtů, je možné vytvářet jednotlivé účty na konkrétních počítačích, což je ale časové náročnější a zvyšuje se riziko kompromitace jednotlivých počítačů z důvodu sdílení uživatelských účtů nebo opomenutí nastavení bezpečnostních politik na některém z počítačů.

- Nenastavujte běžným uživatelům administrátorská práva.
- Využívejte centrální správu uživatelských účtů s využitím adresářových služeb.
- Definujte centrální politiku hesel.
- Omezte práva uživatelů pro přihlášení na jednotlivé počítače.
- Zakažte výchozí administrátorský účet v operačním systému.
- Nepřidávejte lokální účty na jednotlivé počítače, pokud to není nutné.

2.3 Zálohování aktiv školy

Při určování adekvátní úrovně ochrany aktiv je vhodné definovat si jejich hodnotu na základě vyhodnocení požadavků na jejich důvěrnost, integritu a dostupnost. Tyto požadavky je třeba zohlednit v havarijním plánu a plánu obnovy a záloh tak, aby byla zajištěna kontinuita a bezpečnost činností u nezbytných systému/dat (zpravidla „interní“ servery a systémy – například ty, které obsahují účetnictví školy, informace o klasifikaci žáků apod.) a zároveň nebyly vynakládány neúměrné prostředky na ochranu tam, kde to není účelné.

Zálohy mohou být ukládány lokálně (například na diskové pole připojené k interní síti), nebo do prostředí cloudu. U cloudu je ale vždy třeba vyhodnotit vhodnost tohoto řešení s ohledem na požadavky na ochranu důvěrnosti dat. Doporučuje se aplikovat pravidlo 3 – 2 – 1 (Vytvoření nejméně tří kopií dat – Uložení kopie na nejméně dva typy médií – Udržování alespoň jedné kopie zálohy mimo pracoviště).

Bez ohledu na použitý mechanismus zálohování musí být přístup k zálohám, ve smyslu jejich čtení, modifikace nebo mazání, umožněn pouze k tomuto účelu specificky určené množině technických/administrátorských účtů.

Škola by měla pravidelně ověřovat nejen čitelnost, ale především obnovitelnost zálohovaných dat.

2.4 Ochrana proti škodlivému kódu

V dnešní době se uživatelé setkávají s různými nástrahami prakticky na denní bázi. Většina útočníků se zaměřuje ve svých útocích přímo na uživatele a snaží se využít jejich chybných reakcí na vzniklou situaci. Abychom minimalizovali možnost úspěšného provedení takového útoku, musíme uživatelům nastavit prostředí tak, abychom jim dali šanci se těmto útokům bránit nebo je alespoň odhalit.

Z toho důvodu je potřeba se držet následujících doporučení:

- Mít na stanicích a serverech nainstalovanou a pravidelně aktualizovanou antivirovou ochranu s nastaveným reportingem na správce.
- Zapnutý a správně nastavený lokální firewall (povolit pouze ta pravidla/protokoly, které uživatel potřebuje pro svoji práci).
- Nepoužívat zastaralé a zranitelné verze protokolů (např. Samba v. 1 a 2).

- Omezeno spouštění spustitelných souborů (např. s příponou .EXE, .BAT aj.).
- Běžnou práci provádět pouze pod uživatelským účtem, nikoliv pod privilegovaným.
- Zakázat uživatelům spouštění maker, případně politikou omezit na makra podepsána organizací.
- Pravidelně zálohovat (ochrana proti ransomware).
- Pravidelně aktualizovat operační systém a provozované aplikace.

2.5 Řízení aktualizací (Patch management)

S rostoucím počtem koncových zařízení a aplikací je spojena i jejich různorodost. Což způsobuje, že správa těchto systémů a softwaru nadměrně zatěžuje IT správce. Neprovedená nebo opomenutá včasná aktualizace může navíc způsobit narušení zabezpečení sítě, incident a finanční škody. Proto je potřeba tuto problematiku správně řešit.

Co je potřeba splnit pro správné nastavení správy aktualizací:

- Centralizované aktualizace – urychlí a zpřehlední proces aktualizace. Správce nebude muset obcházet jednotlivá zařízení a spouštět na nich aktualizace OS a nainstalovaných aplikací. Současně bude mít přehled, kde aktualizace proběhly a kde ne.
- Nepoužívat nepodporované verze OS a aplikací – zabraňuje zneužití známých zranitelností. Pokud je to vyžadováno např. z důvodu provozu nějakého staršího zařízení nebo aplikace, je nutné přijmout jiná bezpečnostní opatření, např. umístit zařízení přesunout do izolované VLANy s minimálními prostupy.
- Provádět pravidelné aktualizace OS a používaných aplikací – zabraňuje zneužití známých zranitelností.
- Kritické aktualizace doporučujeme provádět v co nejkratším možném čase, aby se předešlo zneužití známých zranitelností. Ostatní aktualizace je možné provádět ve větším časovém rozmezí.
- Aktualizace provádíme vždy na určitém vzorku zařízení, abychom předešli situaci, kdy nám aktualizace způsobní nefunkčnost zařízení. Pokud je možné zranitelnost opravit jiným způsobem než aktualizací, doporučujeme tuto možnost zvážit.
- V souvislosti aktualizacemi je vhodné co nejvíce sjednotit používané typy OS a aplikací.
- Pro aktualizace je vhodné zvolit čas mimo pracovní dobu, aby se předešlo nedostupnosti služby, případně jiným problémům.

Všechny aplikace i operační systém musí být aktuální. Staré verze s neopravenými zranitelnostmi často bývají terčem útočníků. Zároveň se ujistěte, že vaše zařízení jsou správně nakonfigurována a bezpečnostní funkce zapnuty.

Opravný SW musí být implementován neprodleně po jeho zveřejnění. Kontrola existence záplat a aktualizací aplikací a SW komponent musí probíhat periodicky u všech aktiv, minimálně 1x do měsíce.

2.6 Ukládání auditních záznamů (logování)

Ve chvíli, kdy dojde na stanici či serveru k problémům (konfiguračním, napadení stanice škodlivým kódem) se logy stávají jediným vodítkem ke zjištění, k jakým změnám na stanici došlo. Cílem je zaznamenávat jednotlivé události tak, aby zapsaly posloupnost činností (auditní stopu), ze které by bylo možné pochopit aktuální chování systému a diagnostikovat případný problém. Zároveň je vhodné tyto logy zabezpečit proti manipulaci či smazání.

Správné nastavení logování zaznamenává následující události:

- Úspěšné/neúspěšné přihlášení
- Odhlášení
- Přihlášení privilegovaného uživatele
- Auditování příkazové řádky
- Manipulace s účty
- Manipulace se skupinami
- Změna politiky autentizace
- Spuštěné procesy

2.7 Vzdělávání zúčastněných osob

Pro snížení rizik spojených s využíváním informačních technologií je potřeba udržovat osoby, které využívají informační systémy organizace, řádně proškolené. V případě, kdy nejsou jednotlivé osoby v oblasti kybernetické a informační bezpečnosti řádně vzdělány, hrozí kompromitace informačních technologií v organizaci.

Cílem vzdělávání v oblasti informační a kybernetické bezpečnosti je naučit žáky, pedagogy a další zaměstnance školy dodržovat bezpečnostní zásady využívání moderních technologií.

V rámci vzdělávání uživatelů je důležité se zaměřit především na žáky a pedagogy, kteří by měli mít povědomí o základech informační a kybernetické bezpečnosti. Pro danou vzdělávací činnost je možné využít online kurzy, které zdarma poskytuje NÚKIB (více na https://osveta.nukib.cz/local/dashboard) nebo MŠMT (více na https://ema.rvp.cz/).

Samostatnou skupinou jsou správci ICT ve školách, kteří musí procházet periodickým školením o hrozbách, proškolením principů ISMS a tvorby bezpečnostní architektury.

3 Rozšiřující bezpečnostní opatření

Rozšiřující bezpečnostní opatření jsou koncipována jako opatření, která rozšiřují Základní opatření a nabízí školám vyšší úroveň kybernetické bezpečnosti, a proto **doporučujeme** všem školám, aby je rovněž aplikovala.

3.1 Content security

Jak bylo již zmíněno v bodě 2.4, velká část útoků cílí přímo na uživatele s pomocí podvodných mailů, škodlivých příloh nebo odkazů na podvodné stránky. Tyto techniky útoku se do jisté míry dají eliminovat s pomocí níže uvedených technologií, spadajících pod pojem content security.

V případě, že škola používá vlastní e-mailový server, je vhodné zajistit i spamový a antivirový filtr, který je určen pro filtraci škodlivých zpráv a příloh. Doporučujeme pro zvýšení účinnosti filtrování zpráv nakonfigurovat protokoly SPF, DKIM a DMARC. Pokud škola využívá externího subjektu pro provoz e-mailového serveru, může přenést tuto povinnost na poskytovatele služeb.

Škola by měla zajistit filtrování přístupu k potenciálně škodlivému obsahu v internetu (domény a stránky spojené se škodlivým kódem apod.) z interní sítě. Filtraci je možné provádět například s pomocí odpovídajících mechanismů na webových proxy serverech nebo s využitím služeb specializovaných bezpečných DNS služeb.

Za minimální funkční řešení lze považovat nasměrování interních DNS serverů na službu bezpečných DNS překladů a zablokování přístupu k jiným DNS serverům z těch segmentů sítě, v nichž jsou umístěny uživatelské stanice.

3.2 Centrální řízení účtů

Důvodem pro zavedení centrální správy účtů v organizace je snaha zvýšit bezpečnost, produktivitu a zároveň snížit náklady a opakující se úkony při správě stejných účtů v rozličných aplikacích napříč organizací. Každému uživateli v síti je umožněno přihlásit se pomocí jeho unikátního loginu a hesla na jakoukoliv jemu povolenou stanici či do aplikaci.

Centrální řízení účtů umožňuje:

- Jednotnou správu účtů uživatelů a správců s možností nastavení konkrétních oprávnění pro přístup k systémům či jen k datům v rámci sdílených úložišť apod.
- Rozdělovat účty do skupin s různými oprávněními přístupu (např. ke službám).
- Nastavit a vynutit více faktorovou autentizaci pro určitou skupinu účtů.

3.3 Řízení dodavatelů

Cílem řízení dodavatelů je dosáhnout jasného vymezení dodávky a odpovědností obou smluvních stran a nastavit jasná a daná pravidla, kterými se budou strany řídit. Pokud jsou dodavatelé řízeni nedostatečně, nastává v případě problému nebo potřeby změny plnění problém a škola se zpravidla ocitne v nevýhodné situaci, které se dalo při uzavírání smlouvy předejít správným řízením dodavatelů. V případě bezpečnostních doporučení jde především o stanovení pravidel

mezi školou a dodavatelem, která se týkají ustanovení o bezpečnosti informací, oprávnění užívat data, možností zákaznického auditu, pravidel řetězení dodavatelů, informování školy dodavatelem o různých potřebných skutečnostech, postupu při ukončení smlouvy apod.

Základem řízení dodavatelů jsou ustanovení ve smlouvě, nicméně proces řízení dodavatelů musí začít již ve fázi plánování nákupu. Je potřeba dbát na výběr vhodného dodavatele pomocí kvalifikačních kritérií, případně neakceptovat ty dodavatele, se kterými má zadavatel špatnou předchozí zkušenost. S dodavatelem je dále potřeba smluvně uzavřít přesnou specifikaci dodávky díla nebo poskytování služeb. Smlouva musí obsahovat všechny obchodní, finanční, sankční, technické, právní, servisní, logistické, bezpečnostní požadavky nebo další závazky. Minimem co do bezpečnostních požadavků by mělo být zahrnutí relevantních oblastí uvedených v příloze č. 7 k VKB. Čím dlouhodobější smlouva je s dodavatelem uzavírána, tím více je potřeba dát si záležet na výběru spolehlivého partnera a na specifikaci podmínek smluvního vztahu. Stejně tak je potřeba vyvarovat se závislosti na jednom dodavateli (tzv. vendor lock-in), tedy nemožnosti změny dodavatele v důsledku nevhodně nastavených smluvních podmínek.

V etapě plánování se zejména hodnotí rizika a stanovují bezpečnostní požadavky, které se odrážejí v akvizici, vývoji a údržbě ICT.

V etapě pořizování se projekt akvizice, vývoje a údržby ICT stává podkladem pro zpracování zadávací dokumentace a pro výběr dodavatele, a to s ohledem na zákon č. 134/2016 Sb., o zadávání veřejných zakázek.

V realizační etapě je hlavní povinností zadavatele pravidelně hodnotit rizika a kontrolovat dodavatelem prováděná bezpečnostní opatření (stejně jako kvalitu plnění celé smlouvy).

V etapě ukončení vztahu je nutné zejména zajistit odebrání nebo změnu přístupových oprávnění osob na straně dodavatele k ICT systémů a do organizace zadavatele a zajistit předání všech dat a informací zpět do rukou zadavatele.

3.4 Vyhodnocení auditních záznamů (Logy)

Toto doporučení rozšiřuje základní požadavek na logování (bod 2.6). Ve chvíli, kdy zajistíme sběr a bezpečné uložení logů, dalším logickým krokem je pravidelné vyhodnocení informací, které nám logy poskytují. Na základě proaktivní analýzy lze odhalit špatné konfigurace, ale i předcházet napadení či kompletnímu převzetí stanice útočníkem.

Primárně se jedná o logy ze serverů, stanic a logy z bezpečnostních nástrojů.

V případě vyšetřování incidentu jsou důležitým zdrojem informací a pomohou odhalit mj. i stupeň rozšíření nákazy. Regulované subjekty mají z VKB definovanou dobu uchováni logů minimálně 12 nebo 18 měsíců dle druhu regulovaného subjektu. Tuto minimální dobu doporučujeme používat všem administrátorům škol.

3.5 Základní bezpečnostní dohled

S ohledem na personální kapacity školy lze uvažovat o spolupráci nad bezpečnostním dohledem s externími subjekty. Tým bezpečnostního dohledu aktivně sleduje probíhající datovou

komunikaci v reálném čase s cílem odhalit škodlivou činnost. V případě pozitivního nálezu dochází k okamžité reakci a následné spolupráci k odstranění nalezené hrozby.

Po dohodě s dalšími subjekty nebo ideálně ve spolupráci se zřizovatelem je vhodné hledat partnera zajištění základních služeb bezpečnostního dohledu. Svou úlohu teoreticky mohou sehrát SOC týmy poskytovatele internetového připojení. Alternativně lze přistoupit k nasazení síťové sondy na perimetr školní sítě a sdílet informace o datové komunikaci s třetí stranou poskytující SOC služby.

3.6 Reakce na kybernetický útok

I s kvalitně nastavenými bezpečnostními opatřeními je stále třeba počítat s rizikem, že může dojít k bezpečnostnímu incidentu. Je tedy vhodné mít pro tyto situace definované plány a procesy, které umožní co nejrychlejší obnovu a sníží potenciální finanční a materiální škody.

Proces zvládání/řešení kybernetických incidentů je vhodné dekomponovat na prevenci a reakci. Dále jsou uvedeny doporučené aktivity, které je doporučeno vykonat v etapě před a v etapě po zjištění kybernetického útoku na vaši organizaci. Seznam aktivit je koncipován jako seznam, kterého se můžete v případě incidentu držet a umožnit tak efektivnější řešení incidentu.

3.6.1 Před útokem

- Mějte připraven seznam klíčových lidí z organizace a decision makerů (manažera kybernetické bezpečnosti, DPO, vedoucí IT, ředitel školy) a stanovte komunikační plán pro případ takového incidentu.
- Vytvořte plán reakce na kybernetický útok (seznam dílčích kroků a posloupností, které bude administrátor provádět v návaznosti na vybrané, nejvíce pravděpodobné, scénáře). Do plánu reakce a obnovy zakomponujte i systémy nezbytné pro vaši činnost, které jsou pod správou třetí strany (např. cloudové služby, server spravovaný dodavatelem), a to dle uzavřených smluv.
- Vytvořte havarijní plány (DRP) a otestujte jejich funkčnost.
- Vytvořte dostatečný rozpočet pro řešení následků incidentů (přesčasy pracovníků, najmutí konzultační firmy, případná potřeba výměny hardware).

3.6.2 Neprodleně po útoku

Tato opatření jsou určena především pro situace, kdy došlo k závažnému incidentu s následkem kompromitace značné části sítě, nebo k jejímu znepřístupnění (např. zašifrování ransomwarem), a je třeba infrastrukturu (nebo její část) odstavit, aby se zabránilo dalším škodám. Nejedná se o univerzální postup a vždy je třeba zvážit konkrétní situaci a možné dopady.

- Odpojte zálohovací server od sítě, popř. od elektřiny.
- Maximálně omezte síťovou komunikaci mezi stroji (např. panic mode na firewallech).
- Pokud nejste zařízení v síti schopni vypojit na síťové úrovni, odpojte je od zdroje elektrické energie.

- Odpojte komunikaci do veřejné sítě.
- Zjistěte rozsah napadení a napadené systémy izolujte, dokumentujte zjištění.
- Pozastavte virtuální stroje, pokud je to možné, jinak pořiďte snapshot a vypněte je.
- Kontaktujte manažera kybernetické bezpečnosti, vedení vaší organizace a osoby zodpovědné za dané systémy.
- Požádejte o logy ze sondy/firewallu/od poskytovatele internetu.

V případě napadení ransomwarem důrazně doporučujeme neplatit výkupné, ani jakkoliv jednat s útočníky bez účasti Policie ČR a dalších orgánů, a to z mnoha důvodů, které se týkají jak ochrany kyberprostoru jako celku, tak ochrany oběti konkrétního útoku:

- Zaplacení utvrdí útočníka v ziskovosti jeho jednání a motivuje jej k dalším útokům.
- Neexistuje záruka, že útočník data skutečně odblokuje.
- Odblokování dat neodstraní samotný ransomware ani další potenciální malware, situace se tak může i přes zaplacení výkupného rychle opakovat.
- Z právního hlediska může představovat zaplacení výkupného porušení zásad péče řádného hospodáře.

Podrobnější postup určený pro řešení následků ransomware útoku lze nalézt například v metodickém materiálu: https://www.nukib.cz/download/publikace/navody/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf.

3.6.3 Před zahájením obnovy

- Stanovte postup obnovy jednotlivých částí systému – v návaznosti na zpracované havarijní plány (DRP).
- Pokud se řešení incidentu na místě účastní více organizací (dodavatelská či konzultační firma, policie), ustanovte si dostupný a bezpečný komunikační kanál. Pro rychlejší a efektivnější komunikaci přímo na místě je doporučeno připravit označení pro každého, kdo se bude účastnit obnovy (např. jednoduše pomocí nalepovacích jmenovek, které obsahují jméno, organizaci, funkci a případně další potřebné informace).
- Zajistěte dostatečně velkou místnost pro analytiky, dodavatele a další zúčastněné, ideálně vybavenou tabulemi (whiteboard, flip chart).

3.6.4 Postup při obnově dat/sítě

- Zjistěte stav online a off-line záloh.
- Zajistěte alternativní internetové připojení.
- Navrhněte novou architekturu sítě.
- Definujte segmentaci sítě.
- Vytvořte čistou VLAN, ve které se začne budovat nová infrastruktura.

- Proveďte audit administrátorských účtů a reset všech administrátorských hesel v celé infrastruktuře.
- Připravte čisté administrátorské stanice, kterým můžou administrátoři plně důvěřovat.

4 Další informace

AFCEA, Policejní akademie ČR v Praze, 2015, **Výkladový slovník Kybernetické bezpečnosti** https://www.cybersecurity.cz/data/slovnik_v310.pdf nebo https://www.nukib.cz/download/publikace/podpurne_materialy/vykladovy_slovnik_KB_3_vydani.pdf

NÚKIB, 2020, **Minimální bezpečnostní standard**, https://nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

NÚKIB, 2020, **Ransomware: Doporučení pro mitigaci, prevenci a reakci**, https://nukib.cz/download/publikace/podpurne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf

NÚKIB 2020, **Bezpečnostní standard pro videokonference v1.0**, https://nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Standard-pro-VTC_1.0.pdf

NÚKIB, 2020, **Poskytované služby**, https://nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/poskytovane-sluzby/

NÚKIB, 2020, **Analýza hrozby ransomware**, https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf

NÚKIB, 2020, **Spear-phishing a jak se před ním chránit**, https://nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/

NÚKIB, 2019, **Bezpečnostní doporučení NÚKIB pro administrátory 4.0**, https://www.nukib.cz/download/publikace/vzdelavani/Admin%204.0%20brozura.pdf

5 Použité zkratky

Zkratka	Popis
BYOD	Využívání soukromých zařízení zaměstnanců, která jsou přinášena, užívána a připojena na pracovišti do počítačové sítě organizace (Bring Your Own Device)
DMZ	Demilitarizovaná zóna
DPO	Pověřenec pro ochranu osobních údajů (Data Protection Officer)
DRP	Plán obnovy po havárii (Disaster Recovery Plan)
EU	Evropská unie
GDPR	Nařízení Evropské unie pro ochranu osobních data (General Data Protection Regulation)
HTTP	Internetový protokol (Hypertext Transfer Protocol)
HTTPS	Internetový protokol (Hypertext Transfer Protocol Secure)
ICT	Informační a komunikační technologie
IDS	Systémy monitorující síťový provoz nebo aktivity operačního systémů provoz s cílem odhalení podezřelých aktivit (Intrusion Detection System)
IPS	Intrusion Protection Systems
ISMS	Systém řízení bezpečnosti informací (Information Security Management System)
IT	Informační technologie
KB	Kybernetická bezpečnost
LDAP	Protokol pro ukládání a přístupu k datům (Lightweight Directory Access Protocol)
MFA	Více faktorová autentizace (Multi-factor authentification)
MKB	Manažer kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
RDP	Proprietární síťový protokol (Remote Desktop Protocol)
SMTP	Internetový protokol určený pro přenos zpráv elektronické pošty (Simple Mail Transfer Protocol)
SOC	Security Operations Center
SSH	Zabezpečený komunikační protokol (Security Shell)
SW	Software

VKB	Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
VNC	Grafický program pro vzdálené připojení (Virtual Network Computing)
VPN	Virtuální privátní síť (Virtual Private Network)
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

6 Kontakty

GovCERT.cz

- Hlášení incidentů: cert.incident@nukib.cz
- Obecný komunikační kanál: cert@nukib.cz
- Mimo pracovní dobu pohotovostní telefonní číslo +420 725 502 878
- Během pracovní doby telefonní číslo +420 541 110 777

CSIRT.cz

- Hlášení incidentů: abuse@csirt.cz

PČR

- Místně příslušné oddělení Policie ČR
- Postup pro podání trestního oznámení naleznete na https://www.policie.cz/clanek/oznameni-trestneho-cinu.aspx