Digitalizace ve vzdělávání
Národní pedagogický institut ČR

#Kyberšanon

Co dělat, když nastane krize

Autoři:
Jaromír Světlík
kolektiv projektu AIDIG

Editace:
Lucie Gregůrková

Financováno Evropskou unií
NextGenerationEU

NÁRODNÍ PLÁN OBNOVY

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

digitalizace.rvp.cz

Pokud jsou v publikaci používány pojmy učitel, rodič aj., rozumí se tím pedagogická kategorie nebo označení skupiny. Přes volbu mužského rodu text respektuje rovnost pohlaví.

ISBN 978-80-7578-166-6

Obsah

Úvod

Digitální technologie jsou dnes neoddělitelnou součástí života škol. Přinášejí mnoho výhod, ale zároveň otevírají dveře novým hrozbám, které mohou narušit provoz školy nebo ohrozit citlivá data žáků a zaměstnanců. Kybernetické útoky se stále častěji zaměřují i na školní prostředí.

Národní pedagogický institut proto připravil pro vedení škol #kyberšanon. Je to jednoduchý a srozumitelný průvodce, který vám poradí, co dělat v případě kybernetického incidentu. Kyberšanon se zaměřuje na nejčastější hrozby, kterým může škola čelit, od ransomwaru až po ztrátu zařízení. Každé téma obsahuje informace, co udělat jako první i jak předejít dalším krizím.

Předpokladem pro úspěšné zvládnutí kybernetického krize je příprava a prevence. Podívejte se proto na vzorový plán reakce na incident (odkaz), sestavte krizový tým a společně si plán projděte a případně ho upravte. Na webové stránce https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost naleznete další materiály a vzory nebo motivační Kyberpříběhy.

Kyberšanon je připravený k tisku, abyste ho mohli mít po ruce v případě, že elektronické systémy vypadnou.

1.

Jak efektivně spolupracovat při kybernetickém incidentu

Při kybernetickém incidentu je klíčová **rychlá, koordinovaná a informovaná spolupráce** všech zúčastněných. Cílem je **minimalizovat škody, obnovit provoz a zabránit dalšímu šíření hrozby**.

Štěstí přeje připraveným

Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a nebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.[1]

Plán reakce na incident (Incident Reponse Plan) je klíčový pro přípravu na případný kybernetický útok. Podívejte se na vzor takového plánu a upravte si jej podle svých potřeb.

Nastala krize

1. Vezměte si k ruce *Plán reakce na incident* a podle něj identifikujte typ útoku. Jak jednotlivé útoky rozpoznat, naleznete níže.
2. Svolejte krizový tým. Vymezte role a odpovědnosti jednotlivých členů – kdo co řeší a s kým komunikuje.
3. Postupujte dle plánu a metodik v #kyberšanonu.
4. Každé rozhodnutí pečlivě zvažte a konzultujte s odborníky.
5. Všechno pečlivě zdokumentujte.
6. Informujte o incidentu uživatele a dejte jim pokyny, co dělat a co nedělat.
7. V případě potřeby informujte i rodiče.
8. Spolupracujte s externími dodavateli služeb.
9. Oznamte incident příslušným institucím (viz jednotlivé metodiky #kyberšanonu).
10. Proveďte vyhodnocení incidentu a nápravná opatření.

Úspěšné zvládnutí kybernetického incidentu závisí na **včasné a efektivní spolupráci všech zúčastněných**. Důležité je mít připravený plán, vědět, koho kontaktovat, jak řídit komunikaci a jak zabránit opakování podobné situace.

Vzor Plánu reakce na incident k úpravě je k dispozici zde:

1 https://www.e-sbirka.cz/sb/2014/181?zalozka=text

2.

Co dělat, když školu napadne ransomware

Ransomware je zákeřná forma útoku, která může během chvíle ochromit celou školní síť a zablokovat přístup k důležitým datům. Je proto důležité umět rychle rozpoznat varovné signály, že počítače nebo servery mohly být napadeny.

Jak poznat ransomware?

Náhlé zašifrování souborů

Soubory mají neznámé přípony

- Dokumenty, obrázky a další soubory mají najednou **divné koncovky** (např. .locked, .crypt, .ransom, .enc).
- Původní soubory **nejde otevřít** ani v běžných programech (např. Word, Excel, PDF prohlížeče).

Chybí některé soubory nebo složky

- Náhlé **zmizení souborů** nebo přejmenované složky.
- Mohou být nahrazeny soubory s výhrůžným textem (např. READ_ME.txt, HOW_TO_RECOVER_FILES.html).

Výkupné a výhrůžné zprávy

Zobrazí se vyskakovací okno nebo textový soubor s instrukcemi

- **Například:**
  „Vaše soubory byly zašifrovány. Chcete je zpět? Pošlete X bitcoinů na tuto adresu: ...“
  „Kontaktujte nás na [e-mail, Telegram, odkaz] pro získání dešifrovacího klíče.“

Zpráva se může zobrazit:

- Jako vyskakovací okno při zapnutí počítače.
- Jako nový soubor na ploše nebo ve složkách (např. DECRYPT_INSTRUCTIONS.txt).
- Přímo ve jménech souborů (VAŠE_SOUBORY_JSOU_ZAŠIFROVÁNY.txt).

Podivné chování počítačů

Nezvykle pomalý výkon oproti normálu

- Počítače jsou **extrémně pomalé oproti běžnému provozu**, protože ransomware šifruje velké množství souborů na pozadí.

Programy a soubory nelze otevřít

- Dokumenty se **neotevřou** nebo se zobrazí chybová hláška „soubor je poškozen“.
- Programy (např. Word, Excel, e-mailový klient) se **zasekávají nebo padají**.
- **Vysoké vytížení procesoru a disku**
- Ve **Správci úloh (Windows) nebo Monitoru aktivity (Mac)** je vysoké vytížení disku nebo CPU neznámým procesem.
- Mohou se objevit procesy se **zvláštními názvy** (např. encryptor.exe, locker.exe).

Podezřelé aktivity na síti

Nezvykle vysoký síťový provoz

- Velké množství **odchozího provozu** na neznámé IP adresy (možná komunikace s útočníkem).
- **Blokovaný přístup k bezpečnostním webům**
- Počítač najednou **nemůže otevřít** weby bezpečnostních firem (např. Avast, ESET, Microsoft).
- Je to známka toho, že ransomware **blokuje možnosti řešení**.

Změny v systému a podezřelé účty

Změněné nastavení operačního systému

- **Zmizely nebo nefungují** nástroje pro obnovení systému (např. Windows Recovery).
- **Vypnutý antivir** nebo firewall – ransomware je deaktivoval, aby se snížila šance na odstranění.

Nové neznámé uživatelské účty

- Útočník může vytvořit **skrytý administrátorský nebo uživatelský účet** pro budoucí přístup.
- Zkontrolujte ve **Správě uživatelů (Windows) nebo Nastavení účtů (Mac)**.

Jak rychle ověřit, zda jde o ransomware?

- **Otestujte soubor v izolovaném zařízení** – např. virtuální počítač.
- **Prohledejte systém na neznámé soubory** – hledejte soubory jako README.txt, DECRYPT_INSTRUCTIONS.html.
- **Zkontrolujte Správce úloh** – pokud běží proces s vysokým vytížením CPU/disku a neznámým názvem, může to být ransomware.
- **Použijte online skenery** – například ID Ransomware vám pomůže zjistit, jaký typ ransomwaru vás napadl.

Čím rychleji si ransomwaru všimnete, tím větší je šance, že zachráníte data. Sledujte varovné signály a mějte **dobře nastavenou kybernetickou ochranu**, aby škola nebyla snadným cílem pro útoky.

Okamžitá reakce

Odpojte napadené systémy

- **Ihned odpojte** infikované počítače a servery od školní sítě (tzn. vypněte wi-fi a odpojte síťový kabel), NEodpojujte je však od elektřiny ani NEvypínejte.
- **Odpojte zálohovací zařízení (NAS nebo flashdisk)**, pokud nejsou chráněna, aby se zabránilo zašifrování záloh.

Upozorněte IT specialistu

- Informujte **školního IT správce** nebo externí firmu spravující IT systémy.
- Pokud školní IT tým není dostupný, obraťte se na svého **zřizovatele.**

Nepracujte s infikovanými zařízeními

- Neotevírejte podezřelé soubory ani nespouštějte žádné programy na infikovaných počítačích.
- Nesnažte se **sami odstranit ransomware**, pokud nejste odborník – hrozí zhoršení situace.

Analýza a obnovení

Analýza napadení

- IT tým zjistí, **jaký typ ransomwaru** byl použit a které soubory/systémy byly zašifrovány.
- Ověří, zda existují **nezašifrované (nenapadené) zálohy**.

Obnovení ze zálohy (pokud je k dispozici)

- Pokud máte **offline zálohu**, nejbezpečnější cesta je **obnovit celý systém** ze zálohy.
- Neobnovujte soubory **ze stejného systému**, mohly by být infikovány.

Vyhodnocení možnosti dešifrování

- Některé typy ransomwaru mají **známé dešifrovací klíče** dostupné na bezpečnostních portálech, např. **No More Ransom (nomoreransom.org)**. I dešifrované soubory však mohou nadále obsahovat malware.

Platit, nebo neplatit výkupné?

- **Neplaťte** výkupné – neexistuje záruka, že útočníci data odemknou.

Komunikace

- Ransomware útok naplňuje skutkovou podstatu několika trestných činů, proto je důležité útok nahlásit **Policii ČR**.
- Útok nahlaste i Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).
- Kontaktujte **zřizovatele** a požádejte ho o součinnost.
- Pokud byla kompromitována osobní data (žáků, rodičů, zaměstnanců), je nutné bez zbytečného odkladu informovat i Úřad pro ochranu osobních údajů (ÚOOÚ).

Interní komunikace

- Informujte **zaměstnance o útoku,** aby nepřipojovali svá zařízení do sítě (ani přes VPN) a nevystavili zařízení riziku infekce.
- V případě rozsáhlého útoku rozhodněte, zda a jak informovat **rodiče a žáky**.

Prevence

Aktualizace zabezpečení

- Nainstalujte nejnovější **bezpečnostní aktualizace** pro operační systémy a software.
- Ve spolupráci s odborníky posilte **firewall a antivirovou ochranu**.
- Projděte si **Checklist Kyberbezpečnost ve škole** (odkaz).
- Zaveďte **dvoufaktorové ověřování (2FA)** pro důležité účty.
- Zajistěte proškolení o bezpečném chování na internetu, phishingových útocích a bezpečném používání e-mailů pro zaměstnance i žáky.

Pravidelné zálohování

- **Při zálohování aplikujte pravidlo 3-2-1** – vytvoření nejméně tří kopií dat – uložení kopie na nejméně dva typy médií – udržování alespoň jedné kopie zálohy mimo pracoviště.
- **Testujte obnovu ze záloh**, abyste se ujistili, že data lze obnovit.

Školení zaměstnanců

- Zaměstnanci by měli vědět, kam se obrátit v případě nestandardního chování systému a zařízení.
- Naučte zaměstnance rozpoznávat **phishingové útoky a falešné e-maily**.

Ransomware útok může vážně narušit chod školy. **Rychlá reakce, spolupráce s odborníky a správná prevence** jsou klíčové pro minimalizaci škod a ochranu dat.

Tomuto tématu se věnují i kyberpříběhy (odkaz).

3.

Co dělat, když jsou napadeny webové stránky školy

Napadení školního webu či jeho nedostupnost může způsobit vážné škody, ohrozit citlivá data a narušit důvěru veřejnosti. Proto je důležité vědět, jak rychle reagovat, zjistit příčinu problému a obnovit bezpečný provoz stránek.

Nedostupný web

- Ověřte, zda je web úplně **nefunkční**, přesměrovaný na jinou stránku nebo zda neobsahuje škodlivý obsah (např. phishing, malware, propagandu).
- Vyzkoušejte **přístup z různých zařízení a sítí**, abyste zjistili, zda jde o globální, nebo lokální problém.

Okamžitá reakce

Upozorněte správce nebo webhostingovou službu

- Kontaktujte **webového správce** (interního nebo externího).
- Pokud web hostujete u třetí strany (např. Wedos, Active24, OneBit), **ihned kontaktujte poskytovatele hostingu**.

Dočasné vypnutí webu (pokud je to potřeba)

- Pokud je web **přesměrován na nebezpečný obsah** nebo obsahuje škodlivé soubory, doporučuje se **dočasně ho vypnout**.
- Poskytovatel hostingu může web **zablokovat do vyřešení problému**, aby se zabránilo dalším škodám.
- O zablokování domén/y lze požádat i správce národních domén (CZ.NIC).

Změna přístupových údajů

- Okamžitě změňte **hesla** pro administrátorský účet webu, FTP (vzdálené nahrávání souborů), databázi a hostingový účet.
- Pokud používáte **redakční systém (např. WordPress, Joomla, Drupal)**, změňte hesla i pro všechny administrátory.
- Použijte **silná hesla a dvoufaktorové ověřování (2FA)**, pokud to systém umožňuje.

Analýza a obnova

Zjistěte, co bylo kompromitováno

Napadení může mít různé formy:

- **Defacement** – změna vzhledu webu (např. politické nebo hackerské vzkazy).
- **Malware** – škodlivý kód vložený do stránek (např. přesměrování na podvodné stránky).
- **Data breach** – únik citlivých dat (např. e-mailových adres, přihlašovacích údajů).

Ověřte soubory a databázi

- Zkontrolujte změny v souborech a databázi (např. neznámé PHP soubory, upravené index.php).
- Použijte **antivirový skener pro weby** (např. Sucuri SiteCheck nebo VirusTotal).

Zjistěte příčinu útoku

- Byl web napaden kvůli **zastaralému softwaru**?
- Mohl být **prolomený administrátorský účet**?
- Byla **kompromitována hostingová služba**?

Obnovení z bezpečné zálohy

- Pokud máte **aktuální zálohu webu a databáze**, obnovte web do stavu z doby před útokem.
- Hostingové společnosti často nabízejí **automatické zálohy**, kontaktujte je.

Odstranění škodlivého kódu

- Pokud není záloha dostupná, je třeba **ručně odstranit škodlivé soubory, opravit napadené soubory** nebo **přeinstalovat** celý systém.
- V případě WordPressu, Joomly apod. **zkontrolujte a znovu nainstalujte** pluginy a šablony.
- Ujistěte se, že v kořenovém adresáři nejsou podezřelé soubory (např. **neznámé .php soubory**).

Komunikace

- V případě cíleného útoku na školu většího rozsahu nahlaste incident Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).
- Pokud došlo k úniku citlivých dat (např. přihlašovacích údajů, e-mailů rodičů), informujte Úřad pro ochranu osobních údajů (ÚOOÚ).
- Pokud web obsahoval škodlivý obsah, můžete požádat **Google o kontrolu a odstranění varování** přes Google Search Console.

Prevence

Zkontrolujte uživatelské účty

- Smažte **neznámé administrátorské účty** a změňte hesla všech uživatelů s oprávněními k úpravě webu.

Aktualizujte software

- Nainstalujte **nejnovější verze** redakčního systému, pluginů, šablon a serverového softwaru.
- Odstraňte **nepoužívané a zastaralé pluginy**, které mohou být zranitelné.

Nastavte lepší ochranu webu

- Aktivujte **dvoufaktorové ověřování (2FA)** pro administrátory.
- Omezte **počet uživatelských účtů** s administrátorskými právy.
- Používejte **silná hesla a bezpečné připojení (protokoly HTTPS, SSH, SFTP místo FTP)**.

Zabezpečení hostingu

- Požádejte poskytovatele hostingu o **lepší bezpečnostní nastavení** (např. Web Application Firewall).
- Zkontrolujte **oprávnění souborů a složek** na serveru – nechte pouze **nutná práva** (např. soubory by neměly mít práva čtení a zápisu pro každého uživatele).

Pravidelné zálohy

- Nastavte **automatické zálohování webu i databáze** na **externí úložiště**.
- Ověřujte, zda je záloha **funkční** a lze ji rychle obnovit.

Monitorování webu

- Používejte **bezpečnostní pluginy** pro redakční systém (např. Wordfence pro WordPress).
- Aktivujte **notifikace o podezřelých aktivitách** (např. pokusy o přihlášení, změny souborů).

Školení zaměstnanců

- Naučte zaměstnance rozpoznávat **phishingové útoky a falešné e-maily**.
- Vysvětlete, proč je důležité používat **unikátní a bezpečná hesla**.

Napadení školního webu může poškodit reputaci školy a ohrozit data žáků i učitelů. **Rychlá reakce, odborná pomoc a důkladné zabezpečení** jsou klíčové k minimalizaci škod a prevenci budoucích útoků.

4.

Co dělat, když se někdo naboural do školní wi-fi nebo se objeví falešná wi-fi

Školní wi-fi síť je klíčová pro výuku i administrativu a její napadení může vést k úniku dat, zpomalení sítě, nebo dokonce i k napadení zařízení žáků a učitelů. Útočníci mohou:

A) **Prolomit heslo školní wi-fi** a připojit se nelegálně.
B) **Vytvořit falešnou wi-fi (Evil Twin Attack)**, která imituje školní síť a krade přihlašovací údaje.

Jak poznat, že školní wi-fi byla napadena?

A) Nabourání do školní wi-fi

Neznámá zařízení připojená k síti

- V administraci routeru nebo v nástrojích IT správce se objeví **neznámé IP adresy a MAC adresy**.
- Náhlé zvýšení **zatížení sítě** bez zjevného důvodu.

Nečekané zpomalení internetu

- Síť je **extrémně pomalá** i při běžném provozu.
- Učitelé a žáci hlásí problémy s připojením.

Neobvyklé změny v nastavení wi-fi, odpojování zařízení

- Změněný **SSID (název sítě)** nebo nefungující připojení.
- **Odpojování některých uživatelů** bez zjevné příčiny.
- Pokud se zařízení často **samo odpojuje**, může útočník provádět útoky typu „deauthentication attack“ (např. pomocí nástroje Wifi Pineapple).

B) Falešná wi-fi (Evil Twin Attack)

Existují dvě stejné wi-fi sítě

- Učitelé a žáci vidí v seznamu dostupných wi-fi **dvě stejné sítě s podobným názvem**.
  Například:
  Skutečná síť: *Skola_WiFi*
  Falešná síť: *Skola_WiFi_Free*

Neobvyklé přesměrování na přihlašovací stránku

- Po připojení k wi-fi se zobrazí **podezřelá přihlašovací stránka**, která se ptá na heslo znovu.
- Může vypadat jako školní portál, ale ve skutečnosti sbírá přihlašovací údaje.

Zvýšený počet phishingových e-mailů a podvodných aktivit

- Pokud učitelé a žáci začnou dostávat podivné e-maily nebo zaznamenají pokusy o reset hesla, může to znamenat, že útočník již získal jejich údaje.

Okamžitá reakce

A) Pokud někdo pronikl do školní wi-fi

Okamžitě změňte heslo wi-fi

- V administraci routeru změňte heslo pro **všechny sítě (učitelskou, žákovskou, pro hosty aj.)**
- Použijte **silnější heslo** (např. alespoň 16 znaků, kombinace velkých/malých písmen, číslic a speciálních znaků).
- **Zvyšte úroveň šifrování** přístupu k wi-fi (viz část *Jak předcházet útokům* níže)

Odpojte neznámá zařízení

- V routeru zablokujte neznámé **MAC adresy**.
- Pokud se útočník připojil přes známé zařízení (např. žák nebo zaměstnanec), **resetujte jeho přístupové údaje**.

Zkontrolujte logy a zjistěte, odkud útok přišel

- V administraci routeru nebo školního firewallu zkontrolujte **neobvyklý síťový provoz**.
- Pokud vidíte připojení z podezřelých IP adres, **blokujte je v nastavení firewallu**.

Aktualizujte firmware routeru

- Zastaralý firmware může obsahovat bezpečnostní chyby, které útočník zneužil.
- Ujistěte se, že routery mají **nejnovější bezpečnostní aktualizace**.

Nastavte oddělené sítě pro různé uživatele

- **Oddělte síť pro učitele a žáky** (např. VLAN).
- Nastavte **samostatnou wi-fi pro hosty**, která má omezený přístup.

B) Pokud existuje falešná wi-fi

Ověřte dostupné wi-fi sítě

- Zkontrolujte **všechny vysílané SSID** ve škole pomocí **wi-fi skeneru** (např. Wireshark, Acrylic WiFi).

Informujte zaměstnance a žáky

- Upozorněte je, že se objevila falešná wi-fi a že by se neměli připojovat k žádné síti, která není **oficiálně schválena školou**.

Zablokujte falešnou wi-fi

- **Zablokujte MAC adresu útočníka** v nastavení školní sítě (pokud je to možné).
- Pokud útočník používá hotspot na mobilu, může být obtížné falešnou wi-fi vypnout, ale lze ji **rušit silnějším šifrováním** a správným nastavením.

Komunikace

- V případě cíleného útoku na školu většího rozsahu nahlaste incident Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).
- V případě, že došlo k vydírání, útočník požaduje výkupné nebo existuje podezření na trestný čin, se obraťte na **Policii ČR**.
- Pokud došlo k úniku citlivých dat (např. přihlašovacích údajů, e-mailů rodičů), informujte Úřad pro ochranu osobních údajů (ÚOOÚ).

Prevence

Používejte silné šifrování wi-fi

- **Nikdy nepoužívejte otevřenou síť** (např. „Skola_Guest“) bez hesla.
- Nastavte zabezpečení **WPA3,** nebo alespoň **WPA2-Enterprise** (s RADIUS serverem pro autentizaci).

Skryjte SSID školní wi-fi

- Pokud je to možné, nastavte, aby **učitelská wi-fi nebyla veřejně viditelná**.
- Žáci se připojí pouze tehdy, pokud znají **název sítě a heslo**.

Používejte oddělené sítě (VLAN)

- Wi-fi sítě pro učitele, žáky a hosty jsou oddělené.
- Síťová zařízení a prostředky (switche, routery, AP, servery) oddělte od běžných sítí žáků a učitelů.

Monitorujte síťový provoz

- Nastavte **detekční systémy**, které upozorní na neobvyklý provoz.
- Používejte bezpečnostní nástroje pro monitoring a ochranu sítě.

Školení zaměstnanců

- **Vysvětlete rizika falešných wi-fi sítí** a phishingových útoků.
- Doporučte **nepřipojovat se k neznámým wi-fi sítím** a používat **VPN** při připojení k veřejným wi-fi.

Napadení školní wi-fi může ohrozit data školy, učitelů i žáků. **Pravidelné monitorování, silné zabezpečení a informovanost uživatelů** jsou klíčové k tomu, aby škola nebyla snadným cílem útoků.

5.

Co dělat, když dojde ke kompromitaci školního účtu

Kompromitace školního účtu (e-mailu, účtu do školního informačního systému, Microsoftu 365, Google Workspace atd.) může vést k úniku citlivých dat, zneužití identity nebo šíření podvodných zpráv.

Jak poznat, že školní účet byl kompromitován?

Neobvyklé aktivity na účtu

- Přihlášení z **neznámých IP adres nebo zařízení** (např. přihlášení z jiné země).
- **Změna hesla**, kterou uživatel neprovedl.
- **Podezřelé e-maily o resetu hesla** nebo dvoufaktorovém ověřování.

Odesílání podvodných e-mailů z účtu

- Zaměstnanci, žáci nebo rodiče dostávají **podezřelé zprávy**, které vypadají, jako by je poslal napadený účet.
- E-maily mohou obsahovat **phishingové odkazy, falešné faktury nebo žádosti o peníze**.

Neznámé změny v dokumentech a souborech

- **Smazané nebo změněné soubory** v cloudovém úložišti nebo školním serveru.
- Vytvoření **neznámých dokumentů** s podezřelým obsahem.

Ztráta přístupu k účtu

- Uživateli **přestane fungovat heslo**, přestože ho nezměnil.
- Útočník mohl **změnit obnovovací e-mail nebo telefonní číslo**.

Aktivita ve školním systému, kterou uživatel neprovedl

- Změny známek, neznámé komentáře ve školním informačním systému.
- Neznámé **úpravy v databázích nebo školních aplikacích**.

Okamžitá reakce

Okamžitě změňte heslo

- Použijte **silné, unikátní heslo** (tj. takové, které nepoužíváte v jiných systémech).

Odhlaste účet ze všech zařízení

- Pokud je účet napaden, útočník může být stále přihlášen.
- V nastavení účtu vyhledejte možnost **„Odhlásit ze všech zařízení“**.

Zkontrolujte aktivitu účtu

- V Google účtu: **myaccount.google.com/security** → **Vaše zařízení** a **Bezpečnostní události**.
- V Microsoft účtu: **account.microsoft.com/security** → **Historie přihlášení**.

Zapněte dvoufaktorové ověřování (2FA)

- Pokud už není aktivní, nastavte **dvoufázové ověřování** přes autentifikační aplikaci.
- Útočníkovi bude přístup ztížen i v případě úniku hesla.

Analýza

Zkontrolujte nastavení účtu

- Ověřte, zda **nebyly změněny údaje pro obnovení hesla** (e-mail, telefonní číslo).
- Podívejte se, zda útočník nenastavil **automatické přeposílání e-mailů** na jinou adresu.

Zkontrolujte logy přihlášení

- **IT správce může zkontrolovat logy přihlášení** a zjistit, zda došlo k dalším kompromitacím, nebo účet **dočasně zablokovat.**

Zjistěte příčinu kompromitace

- Bylo heslo prolomeno kvůli slabému zabezpečení?
- Byl uživatel obětí phishingu?
- Byl školní systém napaden?

Prevence

Nastavte pravidla pro hesla

- Používejte silná a unikátní hesla (tj. nepoužívají se v jiných systémech ani osobních účtech).
- Hesla nikomu nesdělujte ani nikam nezapisujte.
- Nepovolujte prohlížeči zapamatovat si heslo.
- Doporučte uživatelům používat aplikace pro správu hesel.
- Hesla by měla být **pravidelně měněna**, například jednou ročně.

Aktivujte dvoufaktorové ověřování (2FA) pro všechny důležité účty

- Používejte vícefaktorové ověřování všude, kde je to možné. Minimálně u administrátorských účtů, ideálně i u zaměstnaneckých účtů.
- Pokud to externí služby umožňují, využívejte jednotného přihlašování školním účtem (SSO).

Monitorujte přihlášení a podezřelou aktivitu

- IT správce by měl pravidelně kontrolovat **logy přihlášení, podezřelé aktivity a bezpečnostní výstrahy.**

Omezte oprávnění uživatelů

- Uživatelé by měli mít jen **nezbytná oprávnění** k systémům a souborům.
- Administrátorské účty by měly být **oddělené a chráněné** silnějšími pravidly.

Komunikace

- Pokud došlo k úniku citlivých dat (např. přihlašovacích údajů, e-mailů rodičů), informujte Úřad pro ochranu osobních údajů (ÚOOÚ).
- Pokud útočník rozeslal podvodné e-maily z napadeného účtu, upozorněte příjemce, aby na odkazy neklikali a nestahovali žádné soubory.
- Pokud došlo ke kompromitaci školního informačního systému, informujte učitele, aby zkontrolovali zadané údaje.

Školení zaměstnanců

- Uživatelé by měli vědět, **jak rozpoznat phishing** a **jak chránit svůj účet**.
- Uživatelé by měli vědět, jak nahlásit podezřelé chování systému.
- Vysvětlete zaměstnancům důležitost vícefaktorového ověřování a silných hesel (viz kurzy NPI).

Kompromitace školního účtu může vést k vážným bezpečnostním incidentům. **Rychlá reakce, změna hesla, aktivace 2FA a vyškolení uživatelů** jsou klíčové pro ochranu dat a prevenci proti dalším útokům.

6.

Co dělat, když dojde ke kompromitaci DNS záznamů

Kompromitace **DNS (Domain Name Service) záznamů** znamená, že útočník změnil záznamy na DNS serveru školy. To může vést k:

- **Přesměrování školních webů na falešné stránky** (např. phishingové kopie).
- **Blokování přístupu k e-mailům, školním systémům a cloudovým službám**.
- **Úniku dat** – útočník může zachytávat přihlašovací údaje nebo citlivé informace.

Jak poznat, že došlo ke kompromitaci DNS záznamů?

Školní web se přesměrovává na jinou stránku

- Místo školního webu se načítá **neznámá nebo podvodná stránka**.
- Stránka může **vypadat stejně, ale být pod kontrolou útočníka** (phishing).

E-maily nefungují nebo končí ve spamu

- Školní e-maily nejsou doručovány nebo se vracejí jako **nedoručitelné**.
- Příjemci hlásí, že **dostávají podezřelé e-maily ze školní domény**.

Problémy s připojením ke školním službám

- Učitelé a žáci se **nemohou přihlásit** ke školnímu informačnímu systému nebo cloudovým službám.
- Objevují se náhlé výpadky školního informačního systému nebo cloudových služeb.

Neznámé změny v DNS záznamech

- **Kontrola DNS záznamů** ukáže neznámé IP adresy, které nesedí s původním serverem, nebo podezřelé MX (mailové) záznamy.

Okamžitá reakce

Přihlaste se do DNS správy

- Přihlaste se ke svému **DNS poskytovateli** (Wedos, Active24 apod.).
- Zkontrolujte všechny **DNS záznamy (A, MX, CNAME, TXT, NS)**.

Ověřte a opravte DNS záznamy

- Obnovte správné IP adresy pro **web, e-mail, školní systémy**.
- **Smažte neznámé DNS záznamy**, které přidal útočník.

Změňte heslo k účtu u DNS registrátora (zpravidla externí poskytovatel)

- Použijte **silné heslo a dvoufaktorové ověřování (2FA)**.
- Pokud byl napaden i účet administrátora, kontaktujte **technickou podporu registrátora**.

Analýza a obnova

Zkontrolujte a obnovte bezpečnostní nastavení

- Pokud to DNS služba umožňuje, aktivujte **DNSSEC** (ochrana proti podvržení DNS).
- Ověřte, zda **nedošlo ke změně přístupových práv** – útočník mohl přidat svůj e-mail jako administrátora.

Otestujte e-mailové záznamy (SPF, DKIM, DMARC)

- Použijte nástroje jako **MXToolbox** k ověření, zda e-maily nejsou přesměrovány jinam.
- Pokud byl změněn MX záznam, mohl útočník **zachytávat školní e-maily**.

Kontaktujte poskytovatele hostingu nebo registrátora domény

- Pokud nemáte přístup k DNS správě, **registrátor vám může pomoci obnovit záznamy**.
- Požádejte o **audit přihlášení k účtu**, abyste zjistili, kdo provedl změny.

Komunikace

- Pokud došlo k přesměrování na phishingovou stránku, informujte **učitele, žáky a rodiče**, aby **nezadávali přihlašovací údaje ani jiné informace**.
- Pokud byla e-mailová komunikace kompromitována, upozorněte na možnost podvodných zpráv.
- V případě cíleného útoku většího rozsahu na školu nahlaste incident Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

- Pokud došlo k úniku citlivých dat (např. přihlašovacích údajů, e-mailů rodičů), informujte Úřad pro ochranu osobních údajů (ÚOOÚ).
- V případě, že došlo k vydírání, útočník požaduje výkupné či máte podezření na spáchání jiného trestného činu, se obraťte na **Policii ČR**.

Prevence

Používejte silná hesla a dvoufaktorové ověřování (2FA)

- Administrátorský účet u DNS registrátora **musí být chráněn 2FA**.
- Omezte **počet lidí, kteří mají přístup k DNS správě**.

Aktivujte DNSSEC

- **DNSSEC (Domain Name System Security Extensions)** chrání doménu před podvrženými DNS záznamy.
- Většina DNS registrátorů tuto funkci podporuje.

Pravidelně kontrolujte DNS záznamy a zálohujte

- Nastavte **monitoring DNS změn** u poskytovatele DNS.
- Pravidelně ověřujte, zda **IP adresy, MX a CNAME záznamy odpovídají skutečným hodnotám**.
- **Pravidelně DNS** záznamy **zálohujte.**

Omezte změny DNS na schválené IP adresy

- Pokud to váš registrátor umožňuje, **omezte přístup k DNS správě jen na školní IP adresy**.
- Používejte **firewallová pravidla pro přístup k administraci**.

Využijte ochranu před DDoS útoky

- Zvažte ochranu i proti DDoS útokům. Tento útok je využíván pro zahlcení DNS serverů a znepřístupnění služeb.

Školení zaměstnanců

Vysvětlete zaměstnancům důležitost vícefaktorového ověřování a silných hesel (odkaz na vzdělávání NPI).

Kompromitace DNS může mít vážné důsledky, včetně ztráty kontroly nad školním webem a e-maily. **Rychlá reakce, oprava DNS záznamů, zabezpečení účtu a prevence** jsou klíčové k ochraně školních digitálních služeb.

7.

Co dělat, když se ztratí školní zařízení

Ztráta školního zařízení (notebooku, tabletu, telefonu, USB disku apod.) může vést k **úniku citlivých dat**, **zneužití školních účtů** a k dalším **bezpečnostním hrozbám**.

Jaký je typ ztraceného zařízení?

Nejdříve zjistěte, o jaké zařízení se jedná a jaká data obsahovalo:

Notebook / stolní počítač

- Obsahuje školní systémy, přístup k e-mailu, citlivé dokumenty?
- Má šifrovaný disk, nebo je volně přístupný?

Tablet / mobilní telefon

- Je zařízení chráněno heslem, PINem nebo biometrikou?
- Je zařízení lokalizovatelné na dálku (např. Google Find My Device, Apple Find My iPhone, Intune)?

USB disk / externí disk

- Obsahoval osobní údaje studentů, učitelů nebo citlivé dokumenty?
- Byla data **zašifrována,** nebo šlo o otevřené soubory?

Školní přístupové údaje (hesla, čipové karty apod.)

- Obsahovalo zařízení **uložené heslo k e-mailu, školnímu informačnímu systému, cloudovým službám**?

Okamžitá reakce

Pokud je zařízení připojené k internetu, pokuste se ho lokalizovat

- **Google Find My Device** (android.com/find)
- **Apple Find My iPhone** (icloud.com/find)
- **Microsoft Intune**

Okamžitě změňte hesla k důležitým účtům

- Změňte hesla ke školnímu e-mailu, cloudové službě i školnímu informačnímu systému.
- **Aktivujte dvoufaktorové ověřování (2FA)**, pokud ještě nebylo zapnuto.

Odhlaste účet ze zařízení na dálku

- **Google účet**: myaccount.google.com/security → „Vaše zařízení“ → Odhlásit
- **Microsoft účet**: account.microsoft.com → „Zařízení“ → Odstranit
- **Apple iCloud**: icloud.com → „Najít iPhone“ → Vymazat zařízení

Informujte IT správce

- IT správce může **odpojit zařízení od školní sítě**, zablokovat přístup a monitorovat podezřelé aktivity.

Prevence

Všechna zařízení by měla mít šifrování disku

- **Windows**: Aktivovat **BitLocker**
- **Mac**: Aktivovat **FileVault**
- **Android a iOS**: Většina zařízení má šifrování aktivní automaticky

Používejte správu zařízení (MDM – Mobile Device Management)

- Umožní **centrální správu školních notebooků, tabletů a telefonů**.
- Škola může vzdáleně **vymazat data, blokovat zařízení, resetovat hesla**.

Pravidelně zálohujte školní data

- Při zálohování aplikujte pravidlo 3-2-1. (vytvoření nejméně tří kopií dat – uložení kopie na nejméně dva typy médií – udržování alespoň jedné kopie zálohy mimo pracoviště)

Používejte bezpečné přihlašování

- **Dvoufaktorové ověřování (2FA)** na všech důležitých účtech.
- **Silná hesla** a možnost **automatického odhlášení po nečinnosti**.

Označte školní zařízení

- Každé zařízení by mělo mít **unikátní inventární číslo** a kontakt na školu.
- Tipy, jak evidovat školní IT techniku, naleznete zde:

Komunikace

- Ztrátu zařízení je třeba nahlásit zodpovědné osobě ve škole.
- Pokud zařízení obsahovalo citlivá data zaměstnanců, žáků nebo rodičů, kontaktujte Úřad pro ochranu osobních údajů (ÚOOÚ).
- Při **krádeži** zvažte informování **Policie ČR.**

Školení zaměstnanců

- Uživatelé by měli vědět, jak bezpečně zacházet s IT technikou a jak ji chránit silným heslem a vícefaktorovým ověřováním.
- Uživatelé by měli vědět, kam nahlásit ztrátu zařízení a jak bezprostředně reagovat.

Ztráta školního zařízení může znamenat **bezpečnostní riziko i finanční ztrátu**. Rychlá reakce, změna hesel, vzdálená správa a prevence do budoucna jsou klíčem k minimalizaci škod.

8.

Co dělat, když dojde k DDoS útoku na školu

DDoS (**Distributed Denial of Service**) útok znamená, že útočník **zahlcuje školní servery, web nebo síť** obrovským množstvím požadavků. To může vést k **výpadkům internetu, nedostupnosti cloudových služeb nebo školního webu**.

Jak poznat, že škola čelí DDoS útoku?

Selhávání online služeb

- Učitelé a žáci hlásí, že **wi-fi je pomalá** nebo že **internet vůbec nefunguje**.
- Nelze se připojit ke cloudovým službám nebo školnímu informačnímu systému.
- Web školy se **načítá velmi pomalu nebo vůbec**.
- **E-mailová komunikace nefunguje**, odesílání a přijímání zpráv je extrémně pomalé.
- **Náhlé odpojování od online výuky**.

Neobvyklý provoz ve školní síti

- Velký **počet připojení z neznámých IP adres**.
- Dramatický nárůst požadavků na web, server nebo firewall.
- **Extrémní zátěž serveru**.

Okamžitá reakce

Informujte IT správce

- IT správce může **analyzovat provoz, blokovat škodlivé IP adresy a zavést protiopatření**.

Kontaktujte poskytovatele internetu

- **Poskytovatel internetu může dočasně blokovat útok** na své úrovni.
- Větší poskytovatelé internetu mívají **DDoS ochranu**, kterou mohou aktivovat.

Zapněte ochranu na firewallu a routeru

IT správce může na úrovni firewallu:

- **Blokovat útočné IP adresy** (zejména z jiných zemí).
- **Omezit počet připojení na jedno zařízení**.
- **Zapnout filtrování provozu** (např. pouze pro určité porty a služby).

Přesměrujte provoz přes DDoS ochranu

- Pokud je napaden **web školy**, **služba CDN (Content Delivery Network)** může pomoci zmírnit útok.

Odpojte klíčové služby od veřejného internetu

- Pokud útok míří na konkrétní servery školy, IT správce může **dočasně odpojit interní systémy**, aby se nepoškodily.

Prevence

Používejte DDoS ochranu na úrovni poskytovatele internetu

- Zjistěte, zda váš poskytovatel internetu **nabízí DDoS ochranu,** a aktivujte ji.

Posilte firewall a síťová pravidla

- Omezte **maximální počet připojení na IP adresu**.
- Povolte **pouze školní IP adresy pro administraci serverů**.

Používejte CDN (Content Delivery Network) pro školní web

- **Služba CDN** může pomoci absorbovat DDoS útoky na web školy.

Pravidelně monitorujte síťový provoz

- IT správce by měl **sledovat logy firewallu** a hledat podezřelé vzory v provozu.

Komunikace

- Pokud útok ovlivňuje výuku, je dobré zaměstnancům, žákům, příp. rodičům **rozeslat informaci** o technických problémech.
- Informujte uživatele, aby **neklikali na podezřelé odkazy nebo e-maily** – některé DDoS útoky jsou doprovázeny phishingem.
- V případě cíleného útoku na školu většího rozsahu nahlaste incident Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).
- Pokud došlo k úniku citlivých dat (např. přihlašovacích údajů, e-mailů rodičů), informujte Úřad pro ochranu osobních údajů (ÚOOÚ).
- V případě, že došlo k vydírání, útočník požaduje výkupné či máte podezření na spáchání jiného trestného činu, se obraťte na **Policii ČR**.

Školení zaměstnanců

- Uživatelé by měli vědět, jak **nahlásit podezřelou aktivitu (např. online formulářem)**.

DDoS útok může **zablokovat školní systémy**, ale správná reakce a preventivní opatření pomohou minimalizovat dopady. **Rychlá komunikace s poskytovatelem internetu, firewallová pravidla a DDoS ochrana** jsou klíčem k udržení školní infrastruktury v bezpečí.

Tomuto tématu se věnují i kyberpříběhy (odkaz).

9.

Co dělat, když dojde k phishingovému útoku

Phishingový útok je pokus **vylákat z obětí citlivé údaje**, například hesla, e-maily nebo přístup k systémům školy. Útočník se často **vydává za známou osobu nebo organizaci**, např. vedení školy, IT správce nebo poskytovatele e-mailu.

Jak poznat phishingový útok?

Podezřelý e-mail nebo zpráva

- Odesílatel má **překvapivě důvěryhodné jméno**, ale neznámou nebo pozměněnou e-mailovou adresu (např. reditel@skolaa.cz místo reditel@skola.cz). V případě sofistikovaných útoků umí útočníci zaslat e-mail i z oficiální adresy.
- Zpráva obsahuje **naléhavou výzvu** – např. „Změňte si heslo“, „Klikněte zde pro aktualizaci“, „Ověřte svůj účet“.

Podezřelé odkazy nebo přílohy

- Odkaz nevede na oficiální doménu (např. skola-log.in místo skola.cz).
- Příloha je **.exe, .zip, .js nebo makro ve Word/Excel souboru**.

Útočníci se díky AI zdokonalují, spoléhejte na kritické myšlení

- Dnes už nelze identifikovat phishing podle špatné gramatiky. Díky využívání AI nástrojů dokážou útočníci generovat velmi přesvědčivý podvodný obsah s detailními informacemi nejen o naší organizaci, ale i o nás samotných.

Tento obrázek byl vygenerován pomocí umělé inteligence.

Zaměření na konkrétní osoby (spear phishing)

- Útočník si vybere konkrétní osobu, **oslovuje ji jménem a zná některé detaily z jejího života nebo organizace.**
- Cílený útok na administrátora/IT správce není výjimkou.

Okamžitá reakce

Neotvírejte neověřené přílohy a neklikejte na podezřelé odkazy

- Uživatelé by měli **okamžitě nahlásit podezřelé zprávy IT správci nebo vedení školy**.

Zablokujte podezřelý e-mail v e-mailovém systému

- IT správce může e-mail **označit jako phishing a zablokovat doménu odesílatele**.
- V cloudových službách lze nakonfigurovat **antiphishingová pravidla**.

Analýza

Zjistěte, zda někdo kliknul na odkaz nebo zadal údaje

- Pokud ano, **okamžitě změňte heslo** a aktivujte **dvoufaktorové ověřování (2FA)**.
- Zkontrolujte účet na známky kompromitace – např. neobvyklé přihlášení, změny nastavení.

Zkontrolujte, zda útočník nezískal přístup do systémů školy

IT správce by měl prověřit:

- Přihlášení z neobvyklých IP adres.
- Neautorizované změny v nastavení systémů.
- Nové nebo upravené uživatelské účty.

Kontaktujte technickou podporu platformy

- Poskytovatel služby by měl pomoci s vyšetřením útoku a zabezpečením účtů.

Prevence

Používejte dvoufaktorové ověřování (2FA)

- Zaveďte 2FA minimálně pro zaměstnance.

Nastavte antiphishingovou ochranu v e-mailovém systému

- Zapněte a spravujte SPF, DKIM a DMARC záznamy.
- Aktivujte filtrování neznámých domén, podezřelých příloh a přesměrování.

Používejte školní e-maily výhradně pro školní komunikaci

- Uživatelé by pro soukromé účely neměli používat pracovní účty a ani naopak.

Komunikace

Rozešlete uživatelům upozornění:

- Popis phishingového e-mailu.
- Co dělat, pokud uživatel kliknul, kam neměl, nebo zadal údaje.
- Kam hlásit další podezřelé zprávy.
- V případě cíleného útoku na školu velkého rozsahu nahlaste incident Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).
- Pokud došlo k úniku citlivých dat (např. přihlašovacích údajů, e-mailů rodičů), informujte Úřad pro ochranu osobních údajů (ÚOOÚ).
- V případě, že došlo k vydírání, útočník požaduje výkupné či máte podezření na spáchání jiného trestného činu, se obraťte na **Policii ČR**.

Školení zaměstnanců

- Vysvětlete uživatelům, jak poznat phishing, a nacvičte **ověřování odkazu před kliknutím** (najíždění myší, kontrola domény) – viz vzdělávání NPI (odkaz).
- Pravidelně testujte odolnost vůči phishingu (simulované útoky) – existují nástroje (např. Microsoft Attack Simulator, KnowBe4), které umožní simulovat phishingový útok a zjistit, kdo na nebezpečné odkazy kliká.
- Vysvětlete uživatelům důležitost vícefaktorového ověřování a silných hesel – viz vzdělávání NPI (odkaz).
- Uživatelé by měli vědět, jak **nahlásit podezřelou aktivitu (např. online formulářem)**.
- Zdůrazněte: Škola **nikdy nepožaduje změnu hesla e-mailem s odkazem**.

Phishing je jednou z **nejčastějších a nejnebezpečnějších hrozeb**. Důležitá je **rychlá reakce, informovanost zaměstnanců, technické zabezpečení a školení**. Prevence je nejsilnější zbraň proti phishingovým útokům.

Tomuto tématu se věnují i kyberpříběhy (odkaz).

10.

Co dělat, když dojde ke kompromitaci školní sítě

Kompromitace školní sítě může znamenat, že došlo k **neoprávněnému přístupu**, **infikování sítě škodlivým softwarem** (např. spywarem) nebo že se v síti nachází **cizí zařízení**, které sbírá a odesílá data.

Jak poznat, že je školní síť kompromitovaná?

Neznámá zařízení v síti

IT správce zjistí:

- na serveru, firewallu nebo routeru **neidentifikované MAC adresy nebo IP adresy**.
- **nárůst provozu** v síti bez zjevného důvodu. Například v době, kdy ve škole nejsou zaměstnanci ani žáci, se objevuje neobvyklý provoz na síti.

Zpomalení sítě a podezřelý provoz

- Internet náhle zpomaluje nebo dochází k **výpadkům připojení**.
- V síťovém provozu se objevuje **komunikace s neznámými servery nebo porty**.

Detekce škodlivého softwaru (Spyware, RAT, keylogger)

- Antivirový software zachytí podezřelé aplikace nebo procesy.
- **Uživatelé hlásí podivné chování počítačů** (např. otevírání oken, zpomalení, samovolné přesměrování webů).
- Falešné notifikace „systému“ nebo „antiviru“ s urgencí kliknout na nějaký odkaz.

Změny v nastavení sítě nebo zařízení

- **Firewall nebo směrovač má změněné nastavení** (např. DNS, port forwarding).
- **Neoprávněné pokusy o přístup do serverů** nebo cloudových služeb školy.

Okamžitá reakce

Okamžitě izolujte podezřelá zařízení

- Odpojte neznámé nebo infikované zařízení z wi-fi a kabelové sítě.
- Využijte nástroje pro síťový monitoring k identifikaci podezřelého provozu.

Změňte přístupové údaje do sítě

- Změňte hesla k wi-fi, administraci routeru, firewallu a dalším síťovým prvkům.
- Ujistěte se, že nová hesla jsou **silná a unikátní**.

Analýza

Proveďte antivirové a antispyware skenování

- Na všech školních zařízeních spusťte **důkladnou kontrolu pomocí aktualizovaných bezpečnostních nástrojů**.

Zkontrolujte logy a podezřelé aktivity

V protokolech o síťovém provozu hledejte:

- Neobvyklé přihlášení nebo provoz mimo pracovní dobu.
- Komunikaci s IP adresami v zahraničí.
- **Nestandardní přístupy ke školním systémům**.

Zkontrolujte, zda nedošlo k úniku dat

- Pokud máte podezření, že mohlo dojít k úniku dat, kontaktujte experty na forenzní kybernetickou bezpečnost. S tím může pomoci zřizovatel.

Prevence

Segmentace sítě a oddělené VLANy

- Vytvořte **oddělené sítě pro učitele, žáky, systémový provoz, případně hosty nebo administrátory.**
- Umožněte přístup jen k nutným službám a serverům podle uživatelské role.
- Minimálně jednou ročně revidujte uživatelská oprávnění.

Monitorování sítě (IDS/IPS)

- Implementujte systémy pro **detekci a prevenci průniků.**
- Aktivujte **notifikace o podezřelém provozu**.

Zabezpečte přístupová místa

- **Změňte výchozí přihlašovací údaje** u všech síťových zařízení (routery, switche, AP).
- Používejte **dvoufaktorové ověřování minimálně pro administrátory a ideálně i pro zaměstnance**.
- Zajistěte i **fyzické zabezpečení** síťových prvků (zamčená serverovna, routery a kabely jsou mimo dosah).

Pravidelná aktualizace zařízení a softwaru

- Ujistěte se, že **všechna zařízení v síti mají aktuální firmware a bezpečnostní záplaty**.

Povolte pouze známá zařízení (MAC filtering)

- Nastavte síť tak, aby **jen schválená zařízení** mohla přistupovat k interní infrastruktuře.

Komunikace

- V případě potvrzení úniku citlivých a osobních údajů informujte Úřad pro ochranu osobních údajů (ÚOOÚ).
- V případě cíleného útoku na školu většího rozsahu nahlaste incident Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB).
- V případě, že došlo k vydírání, útočník požaduje výkupné či máte podezření na spáchání jiného trestného činu, se obraťte na **Policii ČR**.

Školení zaměstnanců

- Vysvětlete zaměstnancům rizika **neoprávněného připojení zařízení, používání neznámých USB, stahování nelegálního softwaru**.
- Vysvětlete uživatelům důležitost vícefaktorového ověřování a silných hesel – viz vzdělávání NPI (odkaz).
- Uživatelé by měli vědět, jak **nahlásit podezřelou aktivitu (např. online formulářem)**.
- Kompromitace školní sítě může ohrozit **osobní údaje, provoz školy i výuku**. Důležitá je **rychlá reakce, izolace hrozby, analýza škod a posílení zabezpečení sítě**.

Příloha: Vzor Plánu reakce na incident (zde)

Tomuto tématu se věnují i kyberpříběhy (odkaz).

#Kyberšanon
Co dělat, když nastane krize

Autoři:
Jaromír Světlík
kolektiv projektu AIDIG

Editace:
Lucie Gregůrková

1. české vydání

Národní pedagogický institut České republiky, Praha, 2025

Aktuální informace o publikacích Národního pedagogického institutu České republiky najdete na webových stránkách www.npi.cz.

Národní pedagogický institut České republiky
2025
www.npi.cz