Digitalizace ve vzdělávání
Národní pedagogický institut ČR

Kyberpříběhy

Motivační příběhy o kybernetické bezpečnosti ve škole

Autoři:
Lucie Gregůrková
Jaroslav Šindler
Veronika Němcová
a kolektiv projektu AIDIG

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 978-80-7578-139-0

Obsah

Úvod

Digitální technologie jsou nedílnou součástí našich životů – ve škole, doma i ve volném čase. Přinášejí nám spoustu příležitostí k učení, zábavě i komunikaci. Ale stejně tak s sebou nesou rizika, která si často ani neuvědomujeme, dokud se nestanou skutečností.

Národní pedagogický institut proto připravil tento soubor deseti kyberpříběhů ze školního prostředí. Jedná se o příběhy smyšlené, avšak inspirované reálnými událostmi. Seznámíte se s různými rizikovými jevy i hrozbami, jako jsou útoky ransomwarem, phishing, kybergrooming, ale i s méně známými fenomény, například s kompromitací školní sítě nebo se sdílením fotografií.

Témata jsme vybírali s ohledem na taxonomii kybernetických incidentů dle organizace ENISA.

Zneužívající obsah (abusive content)

➜ např. spam, nenávistné projevy, dětská pornografie, deepnudes

Škodlivý kód (malicious code)

➜ např. viry, trojany, spyware, ransomware

Shromažďování informací (information gathering)

➜ např. skenování, sniffing, sociální inženýrství

Pokusy o průnik (intrusion attempts)

➜ např. zneužití zranitelností, pokusy o přihlášení

Průniky (intrusions)

➜ úspěšné kompromitace účtů či systémů

Dostupnost (availability)

➜ např. DoS, DDoS, sabotáž, výpadky

Bezpečnost obsahu informací (information content security)

➜ neoprávněný přístup či změna dat

Podvod (fraud)

➜ např. neoprávněné využití zdrojů, phishing, porušování autorských práv

Zranitelné prvky (vulnerable)

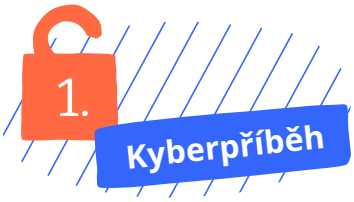
➜ např. otevřené služby, zranitelnosti, lidská chyba, chyba v systému

Zvolili jsme taková témata, se kterými se ve školním prostředí můžete setkat nejčastěji. U každého kyberpříběhu uvádíme, o jaký typ incidentu podle klasifikace ze seznamu na předchozí straně se jedná, a připojujeme také další klíčová slova.

Kyberpříběhy jsme nevytvořili proto, abychom vás vystrašili. Jejich cílem je ukázat, že kybernetická bezpečnost se týká každé školy a že je třeba ji řešit předtím, než nastane nějaká krize. Proto příběhy obsahují vždy i poučení a konkrétní rady, jak podobné situaci předejít, s odkazy na metodickou pomoc.

Kybernetická bezpečnost ve škole je složité téma, Národní pedagogický institut proto vytvořil sérii metodik, kurzů a jiných opor, které vám orientaci v této problematice usnadní. Vše potřebné o kybernetické bezpečnosti naleznete na stránce https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost.

Pojďme se teď společně podívat na to, co všechno se ve škole může stát a jak tomu předcházet.



Ransomware: Lidská chyba

Byl obyčejný školní den. Učitelé se chystali na vyučování, administrativní pracovníci vyřizovali běžnou agendu a žáci během přestávek brouzdali po internetu. Školní sítí proudily desítky citlivých údajů – osobní data žáků i učitelů, známky, docházka.

A pak to přišlo. Na monitorech se náhle objevil textový soubor s hrozivým vzkazem: „Vaše data byla zašifrována. Zaplaťte 2 bitcoiny." Všechna data byla zamčená. Neprostupné šifrování odřízlo školu od informací a paralyzovalo její provoz. Ransomware udeřil naplno.

Správce IT spolu s externími odborníky brzy odhalil příčinu útoku. Jeden z učitelů během krátké přestávky **otevřel v chatovací aplikaci odkaz**, který na první pohled vypadal zcela neškodně. Stačil jediný neuvážený klik, a útočníci získali přístup do školní sítě. Lidská chyba v kombinaci s neaktuálním firewallem, chybějícími bezpečnostními opatřeními a nízkým povědomím o kybernetických hrozbách vytvořila ideální podmínky pro útok.

Bohužel se záhy zjistilo, že útočníci nejenže zašifrovali data, ale také stáhli z části databáze **osobní údaje žáků a učitelů.** Tyto informace mohly být dále zneužity nebo zveřejněny na internetu. Škola proto musela splnit zákonnou povinnost a o úniku osobních údajů informovat Úřad pro ochranu osobních údajů.

Vedení školy okamžitě kontaktovalo Policii ČR a rozhodlo se výkupné neplatit. Škody však byly obrovské:

- ztracená data, která už nešla obnovit
- únik osobních údajů s možnými dopady na pověst školy i na bezpečí žáků a učitelů
- výdaje na IT odborníky, bezpečnostní analýzy a nové zabezpečení
- náklady na nové softwarové i hardwarové vybavení
- statisícové finanční ztráty

Škola se stala odstrašujícím příkladem pro ostatní. Ochrana digitální infrastruktury a pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti už nejsou něco, co lze odkládat na později. Stačí jediný neuvážený klik – a škody mohou být nedozírné.

Poučení

1. **I zdánlivě neškodný odkaz v chatu může být pastí.** Kybernetická bezpečnost začíná u lidí a jejich všímavosti.
2. **Pravidelná školení zaměstnanců v oblasti kybernetických hrozeb jsou nezbytná.** Lidská chyba bývá nejslabším článkem obrany.
3. **Síťová ochrana nesmí být zastaralá.** Pravidelné aktualizace firewallů, antivirů a dalších bezpečnostních prvků jsou klíčové.
4. Škola či jiná instituce musí být připravena na to, že v **případě úniku osobních údajů je povinna tento incident oznámit Úřadu pro ochranu osobních údajů.**
5. Úložiště důležitých dat by mělo být zálohováno podle pravidla 3-2-1.
6. **Investice do prevence bývá vždy nižší** než náklady na řešení následků útoku.

Odkazy

Kyberšanon – materiály k výuce kybernetické bezpečnosti (Digitalizace RVP):
Kyberšanon a vzor krizového plánu
https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost

NÚKIB, AFCEA, NAKIT:
Co dělat při ransomware útoku
https://nukib.gov.cz/download/publikace/navody/RANSOMWARE%20-%20Doporuceni%20pro%20mitigaci%20prevenci%20a%20reakci.pdf

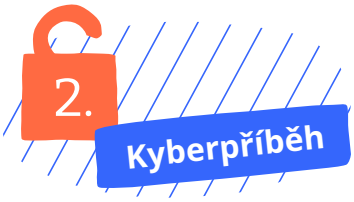
Projekt No More Ransom:
No More Ransom – Pomoc obětem ransomwaru
https://www.nomoreransom.org/cs/index.html

Klasifikace

Zranitelné prvky (vulnerable), škodlivý kód (malicious code)

Klíčová slova

Lidská chyba, ransomware, ztracená data



Ransomware: Víkendový útok

Byl jarní víkend a Martin, učitel informatiky na střední škole, se potřeboval na dálku přihlásit do školního informačního systému. Bohužel se mu to nepodařilo **– systém nešel otevřít**. Pokusil se proto přistoupit i ke svému vzdálenému disku, ale zjistil, že nemůže otevřít ani jeden soubor. Místo toho našel nový textový dokument s názvem „readme_safepay.txt“. Po jeho otevření mu bylo okamžitě jasné, že se **škola stala obětí ransomware útoku.**

Ihned zavolal správci IT, který okamžitě vyrazil do školy. Na místě **odpojil všechny zapnuté počítače** a další zařízení od sítě, aby zabránil šíření malwaru. Brzy zjistil, že všechny školní servery i disky jsou zašifrované. Naštěstí škola uchovává **osobní údaje i další klíčová finanční a personální data v cloudové službě,** takže tyto informace zůstaly v bezpečí.

Vedení školy okamžitě kontaktovalo svého **zřizovatele –** kraj, který bez prodlení poskytl IT pomoc a uvolnil finance na řešení situace. Zároveň byla informována Policie ČR a podáno trestní oznámení.

Od té chvíle byl **provoz školy zcela ochromen –** nikdo nemohl používat žádnou digitální techniku. Aby bylo možné zajistit alespoň základní chod vedení školy, bylo nutné urychleně pořídit nové notebooky pro ředitele, ekonoma a zástupkyni ředitele a také nový router pro krizové zajištění internetového připojení.

V následujících dnech se ukázalo, že bude nutné **vybudovat celou digitální infrastrukturu školy znovu.** Zřizovatel poskytl své odborníky a doporučil škole novou IT firmu, která se ihned pustila do práce. **Obnova provozu** digitálních zařízení a systémů probíhala postupně a trvala celkem **tři měsíce,** než se vše podařilo zprovoznit bez omezení. Celá situace přinesla i nemalé finanční náklady, které se vyšplhaly do desetitisíců korun.

Při pátrání po příčině útoku se ukázalo, že pravděpodobným slabým místem nebyl lidský faktor, ale **neaktualizovaný síťový prvek –** router nebo switch. Přesný okamžik ani místo, kudy útočníci do sítě pronikli, se však nepodařilo zjistit. Jisté ale je, že po průniku začali vytvářet falešné uživatelské účty, kterými postupně skrytě infikovali další počítače.

Po konzultaci s externí firmou přijala škola následující opatření:

- **Správu sítě předala do rukou externí firmy.** Před útokem se o tuto oblast starali učitelé informatiky.
- **Školní informační systém** a další systémy (například docházka) byly přesunuty do **cloudové služby.**

- **Učitelé jsou motivováni využívat sdílené cloudové úložiště**, zatímco používání USB zařízení je postupně omezováno.
- **Externí firma zavedla důkladnější segmentaci sítě –** oddělila učitelskou, administrativní, žákovskou síť a síť pro síťové prvky. Pokud dojde k nákaze v jedné části, neovlivní to ostatní.
- **Byl vylepšen systém zálohování podle pravidla 3-2-1.**

Kybernetické útoky nejsou způsobeny pouze lidskými chybami. Obětí se může stát i škola, která je přesvědčena, že kybernetickou bezpečnost řeší svědomitě.

Poučení

1. **Kybernetické útoky se mohou stát kdykoliv –** i o svátcích nebo o víkendu, kdy je provoz školy omezený a hrozby si nikdo nemusí hned všimnout.
2. **I škola,** která se domnívá, že dbá na kybernetickou bezpečnost, **může být cílem útoku,** pokud podcení pravidelné aktualizace všech zařízení, včetně síťových prvků, jako jsou routery nebo switche.
3. **Správa školní sítě vyžaduje odborné znalosti a kapacity,** které často přesahují možnosti učitelů. Externí odborníci mohou výrazně zvýšit úroveň zabezpečení.
4. **Ukládání důležitých dat do zabezpečeného cloudu** pomáhá ochránit klíčové informace i v případě útoku.
5. **Důležitá je síťová segmentace –** pokud je síť rozdělena na oddělené části, útok v jedné části nemusí paralyzovat celou instituci.
6. **Pravidelné zálohování podle pravidla 3-2-1** (tři kopie dat, na dvou různých médiích, jedna mimo lokalitu) je zásadní pro rychlé obnovení provozu po útoku.
7. **Kybernetická bezpečnost není jednorázová akce, ale nepřetržitý proces.**

Odkazy

Kyberšanon – materiály k výuce kybernetické bezpečnosti (Digitalizace RVP):
Kyberšanon a vzor krizového plánu
https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost

NÚKIB, AFCEA, NAKIT:
Co dělat při ransomware útoku
https://nukib.gov.cz/download/publikace/navody/RANSOMWARE%20-%20Doporuceni%20pro%20mitigaci%20prevenci%20a%20reakci.pdf

Projekt No More Ransom:
No More Ransom – Pomoc obětem ransomwaru
https://www.nomoreransom.org/cs/index.html

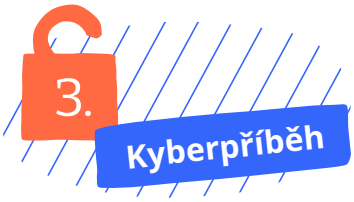
Video – Jak na kybernetickou bezpečnost nejen u vás ve škole
https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost

Klasifikace

Škodlivý kód (malicious code)

Klíčová slova

Zranitelný systém, neaktualizovaný systém



Phishing: Nečekaný e-mail

Paní Hlaváčková, matka Adama, který navštěvoval 2. ročník českobudějovického gymnázia, si zapnula počítač, aby zkontrolovala Adamovu docházku a známky ve školním informačním systému. Tentokrát ji ale **překvapil e-mail,** který jí přišel **z adresy školní účetní.** Stálo v něm, že Adam má **neuhrazených 125 korun za stravování.**

Paní Hlaváčková se zarazila. Věděla, že všechno platí včas, a navíc ji překvapilo, že informace o školním stravování jí **chodí ze školního stravovacího systému, a nikoliv od školní účetní.** Přesto nechtěla nic riskovat, a tak **klikla na přiložený odkaz.** Otevřela se stránka, která vypadala stejně jako informační systém, kde běžně obědy objednává a platí. Místo běžného přihlášení ji však systém požádal o **zadání čísla platební karty.**

V tu chvíli si uvědomila, že něco není v pořádku. Místo aby zadala údaje, **zavolala na infolinku** stravovacího systému, kde jí sdělili, že žádný nedoplatek u Adama neevidují. Když jim paní Hlaváčková sdělila další informace a to, že po ní systém chtěl, aby zadala číslo karty, bylo jasné, že jde o podvod. **Školní jídelna následně všem poslala informační e-mail o podvodu** a začala situaci dále řešit.

Jak se ukázalo, útočníkům se pravděpodobně **podařilo získat e-mailové adresy uživatelů.** Získaný seznam e-mailů následně využili pro šíření odkazu s falešnou stránkou stravovacího systému.

Poučení

1. **Podvody jsou díky nástrojům umělé inteligence mnohem přesvědčivější než dříve.** Nestačí jen hledat překlepy nebo špatný jazyk. Vždy si informace ověřujte, například telefonicky, než zadáte jakékoli osobní či platební údaje. Kritické myšlení je základ.
2. **Chraňte e-mailové adresy žáků i rodičů.** Při rozesílání hromadných e-mailů používejte funkce jako „skrytá kopie“ (BCC) nebo nástroje pro hromadnou korespondenci, aby nedošlo k úniku adres.
3. **Zabezpečte databáze s e-mailovými adresami.** Údaje ukládejte šifrovaně a zajistěte, aby k nim měli přístup jen oprávnění zaměstnanci.
4. **Pravidelně školte zaměstnance.**

5. Zaměstnanci by měli umět rozpoznat phishingové útoky, techniky sociálního inženýrství a vědět, na co si dát pozor při práci s e-maily i online systémy.
6. **Informujte rodiče, jakým způsobem škola posílá důležité zprávy.** Například prostřednictvím oficiálního informačního systému, e-mailu s elektronickým podpisem nebo jiné ověřené komunikace.

Odkazy

Kyberšanon – materiály k výuce kybernetické bezpečnosti:
Co dělat, když dojde k phishingovému útoku
https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost (ČR):
https://nukib.gov.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/

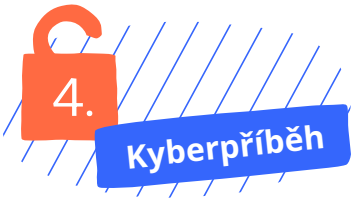
KOPECKÝ, Kamil. Jak podvodníci zneužívají popularitu umělé inteligence k šíření malwaru a phishingu. E-Bezpečí, roč. 9 (2024), č. 2, s. 4–5. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=4179

Klasifikace

Podvod (fraud)

Klíčová slova

Phishing, falešná stránka, ochrana e-mailů



Phishing zaměřený na admina

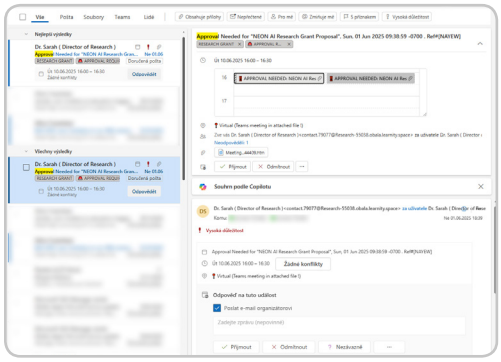
Jarda, správce ICT na jedné brněnské střední škole, **si v posledních týdnech začal všímat znepokojivých událostí.** Na jeho administrátorský e-mailový účet začala přicházet vlna podezřelých zpráv – **zprávy byly určeny výhradně jemu,** nikdo jiný ze školy je neobdržel. Všechny obsahovaly odkazy k prokliku, často maskované za **legitimně vypadající výzvy,** např. ke kontrole nastavení nebo k potvrzení údajné faktury.

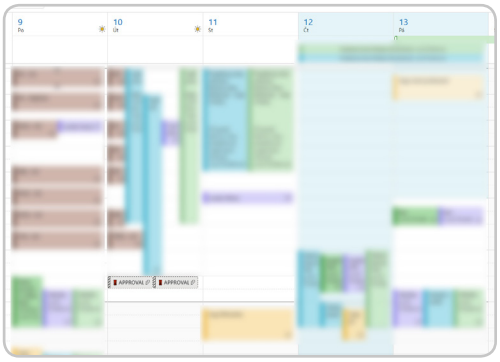
Situace se postupně zhoršovala. Do jeho kalendáře začaly samovolně **přibývat události s žádostí o potvrzení účasti** – i ty obsahovaly podezřelé odkazy. Zároveň systém správy IT infrastruktury hlásil neobvyklé aktivity, například **pokusy o přesměrování e-mailové komunikace běžných uživatelů na cizí adresy.**

Jardovi bylo jasné, že nejde o běžný spam. Jednalo se o **sofistikovaný phishingový útok,** který velmi pravděpodobně využíval nástroje umělé inteligence k personalizaci a maskování škodlivého obsahu. Útočníci se zjevně zaměřili na něj jako správce systému s rozšířenými oprávněními – **cílem bylo získat přístup k celé infrastruktuře školy.**

Naštěstí i škola sama využívá správce systému s podporou umělé inteligence, která dokáže analyzovat podezřelé vzory chování a navrhovat bezpečnostní opatření. Jarda tedy v rámci administračního rozhraní detailně popsal celou situaci: uvedl, jaké typy e-mailů a událostí dostával, jaká přesměrování byla zaznamenána, a upozornil, že by mohlo jít o cílený útok na školní síť.

Inteligentní systém okamžitě zareagoval. Doporučil posílení bezpečnostních opatření, jako je zavedení vícefázového ověřování, kontrola e-mailových filtrů, audit uživatelských účtů a revize oprávnění. Dále navrhnul zpřesnění mechanismů pro hlášení podezřelé aktivity napříč školou, včetně edukace zaměstnanců o možných hrozbách. **Díky včasné reakci se podařilo útok zastavit dřív, než způsobil reálné škody.**





Poučení

1. **Administrátorské účty chraňte vícefázovým ověřováním (MFA)** – jsou primárním cílem útočníků a jejich kompromitace může ohrozit celý systém.
2. **Ignorujte odkazy v nevyžádaných e-mailech nebo kalendářových pozvánkách a neklikejte na ně.** I když vypadají věrohodně, často jde o phishing.
3. **Využívejte nástroje s prvky umělé inteligence i pro obranu** – dokážou analyzovat vzory útoků a pomoci s rychlým zajištěním systému.
4. **Zaveďte mechanismy pro snadné hlášení podezřelých aktivit všemi uživateli, nejen administrátorem** – prevence začíná u včasného upozornění.
5. **Pravidelně školte zaměstnance v oblasti kybernetické bezpečnosti**, včetně aktuálních hrozeb, jako je phishing generovaný AI.

Odkazy

Kyberšanon – materiály k výuce kybernetické bezpečnosti:
Co dělat, když dojde k phishingovému útoku
https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost (ČR):
https://nukib.gov.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/

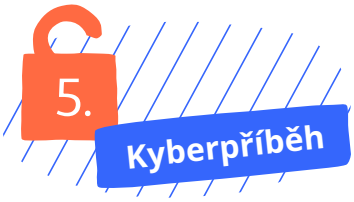
KOPECKÝ, Kamil. Jak podvodníci zneužívají popularitu umělé inteligence k šíření malwaru a phishingu. E-Bezpečí, roč. 9 (2024), č. 2, s. 4–5. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=4179

Klasifikace

Podvod (fraud)

Klíčová slova

Phishing, admin, falešná událost, umělá inteligence



Narušení internetové sítě na střední škole

Byl květen a na jedné střední škole v malém okresním městě právě **skončily maturitní zkoušky.** Vše bylo připraveno k odeslání maturitních výsledků, když došlo k náhlému výpadku školního systému. **Webové stránky školy, další webové služby i školní informační systém se staly nedostupnými.**

Správce sítě se nejprve domníval, že jde o technickou závadu na straně poskytovatele internetového připojení. Vedení školy předpokládalo, že se jedná o přetížení systému kvůli zvýšenému provozu. Po prvotním šetření však bylo odhaleno, že v síti došlo k neobvyklé aktivitě, která vedla k **přetížení školního serveru.**

Po konzultaci s externím IT specialistou se ukázalo, že škola se stala cílem **DDoS útoku (distributed denial of service)** – tedy útoku, při kterém je server zahlcen tisíci falešnými požadavky s cílem ho vyřadit z provozu. Zároveň byl v systému detekován **malware,** který útočníkovi umožnil vzdálený přístup do sítě. Tento škodlivý kód se pravděpodobně dostal do systému prostřednictvím přílohy v e-mailu, kterou jeden z uživatelů otevřel.

Podrobná analýza incidentu odhalila závažné **nedostatky v zabezpečení vnitřní sítě školy:**

- neprobíhaly pravidelné aktualizace systémů,
- většina zařízení používala zastaralý antivirový software,
- nebyla nastavena síťová segmentace, což umožnilo volné šíření škodlivého kódu napříč celou infrastrukturou,
- ani zaměstnanci, ani administrátoři nepoužívali dvoufaktorové ověřování (2FA).

Díky rychlé reakci se podařilo situaci stabilizovat a maturitní výsledky byly odeslány s pouze dvoudenním zpožděním. Následně proběhla důkladná analýza incidentu a škola ve spolupráci s odborníky přijala řadu bezpečnostních opatření.

Tento incident se stal pro školu cennou lekcí a impulsem k výraznému posílení její kybernetické bezpečnosti.

Poučení

1. **Pravidelná školení zaměstnanců v oblasti kybernetických hrozeb jsou nezbytná.** Lidská chyba bývá nejslabším článkem obrany.
2. **Síťová ochrana nesmí být zastaralá.** Pravidelné aktualizace firewallů, antivirů a dalších bezpečnostních prvků jsou klíčové.
3. **Nastavte systém pravidelných aktualizací a kontrol** softwaru a zařízení, aby bylo jisté, že je vše aktuální a zranitelnosti minimalizovány.
4. **Důležitá je síťová segmentace** – pokud je síť rozdělena na oddělené části, útok v jedné části nemusí paralyzovat celou instituci.
5. **Zaveďte dvoufaktorové ověřování** pro všechny klíčové uživatele – minimálně pro administrátory a ideálně i zaměstnance.

Odkazy

Kyberšanon – materiály k výuce kybernetické bezpečnosti:
Co dělat, když dojde k DDoS útoku na školu
https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost

Kyberšanon – materiály k výuce kybernetické bezpečnosti:
Řízení kybernetických rizik ve škole
https://digitalizace.rvp.cz/clanky/rizeni-kybernetickych-rizik-ve-skole

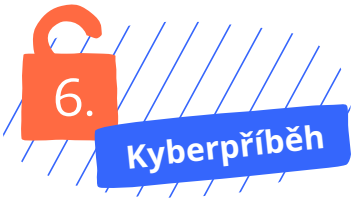
NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost (ČR):
Doporučení pro případ napadení DDoS útokem – jak se zachovat a jak postupovat
https://nukib.gov.cz/cs/infoservis/doporuceni/1452-doporuceni-pro-pripad-napadeni-ddos-utokem-jak-se-zachovat-a-jak-postupovat/

Klasifikace

Dostupnost (availability), škodlivý kód (malicious code)

Klíčová slova

DDoS útok, zranitelnost sítě, segmentace sítě



Neviditelný špeh

Adam z 8. B měl velký zájem o počítače a technologie. Se svým kamarádem Jirkou se často předháněli, kdo toho ví a zvládne víc.

Jednoho dne Adama napadlo, že Jirku „trumfne“ tím, že **zjistí přihlašovací údaje jejich třídního učitele.** Po konzultaci s AI chatbotem zjistil, že existuje program zvaný *keylogger*, který dokáže zaznamenávat stisknuté klávesy – včetně zadávaných hesel. Rozhodl se, že to ve škole vyzkouší.

Nejprve se pokusil takový program vytvořit sám za pomoci AI chatbota. Po zadání jednoduchého požadavku mu chatbot – společně s varováním o neetickém použití – ukázal potřebný kód.

Pak ale musel přijít na to, jak keylogger do školního počítače dostat. **Chatbot mu poradil dvě možnosti:** buď přímou instalací softwaru do počítače, nebo použitím speciálního USB zařízení. Protože školní účty žáků neumožňují instalaci programů, rozhodl se Adam pro druhou variantu – **koupil si USB keylogger.**

Ve škole pak stačilo jen nenápadně vložit USB zařízení mezi klávesnici a počítač. Za čtrnáct dní ho opět nepozorovaně vytáhl – a doma si mohl přečíst vše, co během té doby učitelé na klávesnici napsali. Včetně uživatelských jmen, hesel, známek, poznámek nebo zápisů do třídní knihy. **AI chatbot mu následně pomohl data analyzovat a z přihlášení odhalit hesla všech uživatelů daného počítače.**

Když se Adam s Jirkou nadšeně probírali získanými informacemi u Adama doma, zaslechl jejich rozhovor Adamův tatínek. Byl ohromen tím, co dokázali, ale zároveň jim vysvětlil, že **jejich chování nebylo správné**. Navrhl, aby na bezpečnostní chybu **upozornili školu**.

Společně tedy zašli za školním správcem ICT a vše mu popsali. Ten ocenil, že se chlapci rozhodli jednat správně a získaná data nezneužili. Následně **provedl opatření pro zvýšení zabezpečení školní sítě.**

Poučení

1. **Fyzické zabezpečení je základ.** Pokud je to možné, měly by být počítače a další zařízení fyzicky chráněny proti neoprávněnému přístupu.
2. **Deaktivace nepoužívaných USB portů.** Zakázání nevyužívaných USB portů pomáhá zabránit nepozorovanému připojení zařízení se škodlivým kódem. Mějte na paměti, že USB porty nejsou jen na počítačích a noteboocích, ale i na síťových prvcích, tiskárnách, routerech, switchích a dalších zařízeních.

3. **Vícefaktorové ověření (MFA).** MFA výrazně zvyšuje bezpečnost i v případě, že dojde k úniku hesel. Doporučuje se minimálně pro administrátory, ideálně však pro všechny zaměstnance.
4. **Pravidelné aktualizace.** Nezapomínejte na průběžné aktualizace operačních systémů, bezpečnostních záplat a antivirových programů. Jen aktuální systém může efektivně čelit novým hrozbám.

Odkazy

MŠMT, NÚKIB:
„Dávej kyber“ pro učitele, Kybernetické útoky
https://osveta.nukib.gov.cz/mod/page/view.php?id=1928

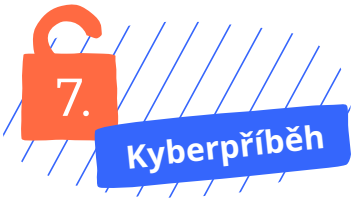
JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti: Cyber Security Glossary. 6. vydání. Praha: Centrum kybernetické bezpečnosti, z.ú., 2025.
Dostupné z: https://www.cybersecurity.cz/data/Slovnik_610_el.pdf

Klasifikace

Škodlivý kód (malicious code), shromažďování informací (information gathering), bezpečnost obsahu informací (information content security)

Klíčová slova

Keylogger, špehování, přístupové údaje, umělá inteligence



Narušení výuky

Žáci osmé třídy netrpělivě čekali na začátek hodiny zeměpisu. Učitel Havlíček si oblíbil nový **interaktivní panel,** který ovládal přes **školní tablet.** Panel mu výrazně usnadňoval výuku – umožňoval snadné bezdrátové sdílení obsahu, takže se mohl volně pohybovat po třídě a lépe reagovat na potřeby žáků. Díky tomu byly hodiny pro žáky dynamičtější, interaktivnější a zábavnější.

Několika žákům však hlavou probleskla jiná myšlenka: *„Co kdybychom se k panelu připojili taky?“* Filip, Anička a pár spolužáků se rozhodlo zjistit, jak těžké by bylo výuku trochu narušit. O pomoc požádali AI chatbota, kterému položili otázku: *„Jak se připojit k interaktivnímu panelu ve třídě, když nejsme učitelé?“*

Chatbot jim ochotně vysvětlil možnosti připojení pro různé typy zařízení. Poté, co žáci upřesnili model panelu, dostali i podrobný návod, jak postupovat. Stačilo si stáhnout oficiální aplikaci výrobce. Protože **panel ve třídě neměl nastavené žádné zabezpečení** proti neautorizovanému přístupu, nic jim nebránilo převzít nad ním kontrolu.

První připojení k panelu si žáci vyzkoušeli o přestávce, když ve třídě nebyl žádný učitel. **Žáci sdíleli obrazovky svých telefonů** a spouštěli na panelu různá zábavná videa. Fungovalo to.

V další hodině se rozhodli akci zopakovat. Využili moment, kdy učitel Havlíček stál zády k panelu a věnoval se výkladu. **Anička přes svůj mobil nasdílela na panel vtipné fotografie** – třída se začala smát a učitel nechápal, co způsobilo takový rozruch. Když se otočil, žáci už byli opět odpojeni a panel vypadal jako obvykle.

Po několika podobných situacích učitel Havlíček začal tušit, co se děje. Po hodině se obrátil na školního správce ICT, aby problém nahlásil. Společně zjistili, že panel skutečně nebyl nijak chráněn proti neautorizovanému připojení.

Následně byla ve všech učebnách zavedena bezpečnostní opatření – **přístup k panelům je nyní možný pouze po zadání PIN kódu nebo přihlášením pomocí učitelských školních účtů.**

Poučení

1. Zabezpečte interaktivní tabule a panely PINem nebo přihlašovacími údaji.
2. Pravidelně aktualizujte software zařízení, abyste předešli bezpečnostním zranitelnostem.
3. Pokud to panel umožňuje, aktivujte sledování neobvyklé aktivity nebo přístupů do administrace.
4. Ještě před pořízením zařízení si u výrobce zjistěte, jaké bezpečnostní možnosti daný model nabízí.

Odkazy

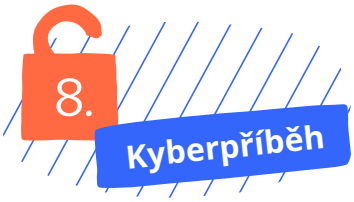
AYRE, Jim, EdICTs a EUROPEAN SCHOOLNET. Pořiďme si interaktivní tabuli – rady a doporučení (2012). Dostupné z: https://www.dzs.cz/sites/default/files/2020-08/Po%C5%99i%C4%8Fme%20si%20interaktivn%C3%AD%20tabuli.pdf

Klasifikace

Bezpečnost obsahu informací (information content security)

Klíčová slova

Interaktivní panel, narušení výuky, zabezpečení panelu



Nevinné sdílení fotek v mateřské škole

Paní učitelka Jitka pracovala v ostravské čtyřtřídní mateřské škole už několik let a své povolání dělala srdcem. Rodiče i děti ji měli rádi, jelikož se snažila vytvářet přátelské prostředí. Vymýšlela zajímavé didaktické aktivity a tematické akce, které pravidelně sdílela s rodiči na sociálních sítích a webových stránkách mateřské školy. **Jednoho dne se rozhodla zveřejnit na Facebooku několik snímků z lekce plavání.**

Za pár dnů si ji však zavolala ředitelka školy a řekla jí, že obdržela **stížnost od maminky jednoho chlapce,** který nastoupil teprve minulý měsíc. Bohužel paní učitelka nevěděla, že právě zákonní zástupci tohoto chlapce neudělili souhlas se zveřejňováním fotografií či jakýchkoli mediálních souborů, kde by byl zachycen jejich syn. **Na žádost rodičů musela mateřská škola smazat veškeré související fotografie a videa.**

Bohužel situaci se nepodařilo podchytit včas. O měsíc později jeden z rodičů upozornil na to, že se tato **fotka zobrazila u blogového článku o pohybu dětí.** Vedení školy bylo jasné, že **takto neměla být pořízená fotka určitě použita.**

Škola začala situaci okamžitě řešit. Vedení školy připomnělo zaměstnancům, že je nutné mít ke zveřejňování fotek souhlas rodičů. Fotky, které byly jednou nahrané na internet, mohou být kdykoli zkopírovány a zneužity.

Od té doby mateřská škola změnila pravidla. Paní ředitelka zrevidovala seznam udělených souhlasů od rodičů a pravidelně jej předává učitelkám. **Fotografie a videa se sdílejí jen prostřednictvím chráněného úložiště, které je přístupné pouze zákonným zástupcům.** U dětí, jejichž rodiče neudělili souhlas se zveřejňováním fotek, začaly učitelky rozostřovat obličeje dětí nebo snímky vůbec nepublikují.

Poučení:

1. Vždy pečlivě zvažujte, zda je pořízení a následné zveřejnění záznamu s vizuálními identitami dětí pro daný účel skutečně nezbytné.
2. Preferujte **skupinové fotografie** před individuálními portréty. Minimalizujete tak identifikovatelnost jednotlivců.
3. Důkladně zkontrolujte platné **souhlasy zákonných zástupců,** a to nejen podle **GDPR,** ale také podle **občanského zákoníku (OZ).**
4. Pro pořizování záznamů používejte primárně **služební zařízení.**
5. Zásadně se řiďte dohodnutými podmínkami se zákonnými zástupci nezletilých, a to zvláště u záznamů dokumentujících školní aktivity.
6. **Nastavte** jasná **pravidla** pro pořizování, uchovávání i sdílení fotek, videí a zvukových záznamů v interní směrnici. Vytvořte chráněné úložiště.

Odkazy

Jak na pořizování fotek a videí ve škole
https://digitalizace.rvp.cz/files/kyberprevence-fotografie-a-videa-ditete.pdf

Digitální stopa ve škole
https://digitalizace.rvp.cz/clanky/digitalni-stopa-ve-skole

Shrnutí problematiky na edu.gov.cz, MŠMT
https://edu.gov.cz/fotky-a-ochrana-soukromi-v-zivote-skoly/

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost (ČR):
Osvětový projekt Kyber tabu
https://osveta.nukib.gov.cz/course/view.php?id=205

Digitální stopa, Internetem bezpečně:
https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

KYBCAST, Sharenting a sdílení fotografií na internetu
https://share.transistor.fm/s/8243f66e

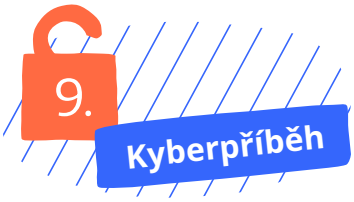
SCHWEINER, Pavel. Řada lidí zveřejňuje fotografie svých známých na sociálních sítích, aniž by si byli vědomi možných právních rizik s tímto spojených. Za jakých podmínek můžete umístit fotku druhých osob na sociální sítě? E-Bezpečí, roč. 7 (2022), č. 1, s. 72–76. ISSN 2571-1679. Dostupné z: https://www.e-bezpeci.cz/index.php?view=article&id=2661

Klasifikace

Zneužívající obsah (abusive content)

Klíčová slova

Nevhodné sdílení, fotografie dětí, zneužití obsahu



Deepnude: zneužití fotek z Instagramu

Tereza byla na jihlavské střední škole nová, byla spíše introvertní a moc se do dění ve své třídě nezapojovala. Stála trochu stranou. Měla problém najít si kamarády, což ji už dlouho trápilo.

Parta kluků z 3. ročníku střední školy se dozvěděla o nové „svlékací aplikaci“, díky které vytvořili falešné fotky své spolužačky Terezy, a dokonce i videa, na nichž byla zobrazena nahá a při intimním styku. **Stačily jim k tomu běžné fotky,** které postovala na Instagramu.

Kluci tento obsah **sdíleli v uzavřených skupinách na online platformách jen s ostatními spolužáky,** proto Tereza nejdřív vůbec nerozuměla posměchu. Až Jitka jí tyto fotografie po pár dnech ukázala. Tereza byla úplně v šoku. Šla bez omluvy domů a celý týden se odmítala do školy vrátit.

Terčini rodiče se strachovali a snažili se od ní dozvědět, co se stalo. Až po několika dnech se jim svěřila. Rodiče **začali** záležitost **řešit přímo s ředitelem školy.** Ten si vážnost situace hned uvědomil. Na jména chlapců, kteří měli tuto krutou legraci na svědomí, se záhy přišlo. Ani ostatním spolužákům už to vtipné nepřipadalo.

Ředitel školy navrhnul **společnou schůzku** s rodiči chlapců, které výchovný postih neminul. Terčini rodiče se obrátili i na policii, která zahájila vyšetřování podezření z trestného činu zneužití identity k výrobě pornografie a jejího šíření.

Změna školy by pro Terčinu rodinu byla velmi obtížná. **S pomocí metodika prevence a školního psychologa** se však mohla opět cítit ve škole bezpečně, a dokonce se z nich s Jitkou staly kamarádky.

Škola následně přistoupila k následujícím bezpečnostním opatřením:

- Byl nasazen systém pro monitorování vnitřní sítě školy a nástroje filtrující nevhodný obsah (adresy). Svlékací aplikace byla totiž použita na školních počítačích, aniž by to správce sítě zachytil.
- Byla zorganizována školení pro zaměstnance o bezpečném chování na internetu a nových fenoménech a prevenci rizikového chování.
- Do preventivních programů pro žáky bylo zařazeno téma kyberšikany, deepnude aj.
- Byly vytvořeny krizové scénáře pro různé případy rizikového chování online.

Poučení

1. **Reagujte rychle a citlivě** – řešte podezření na kyberšikanu okamžitě, abyste chránili oběť a zabránili dalšímu šíření.
2. **Spolupracujte s rodiči a policií** – v závažných případech neváhejte zapojit orgány činné v trestním řízení a informujte rodiče všech zúčastněných.
3. **Poskytněte oběti podporu** – zajistěte psychologa, metodika prevence a bezpečné podmínky pro návrat do školy.
4. **Školte zaměstnance a žáky** – věnujte se prevenci kyberšikany, deepfake a bezpečnému online chování ve výuce i na školeních pro pedagogy.
5. **Zajistěte technická opatření** – implementujte monitoring školní sítě, filtraci nevhodného obsahu a pravidelně kontrolujte využívání školní techniky.
6. **Budujte bezpečné klima** – podporujte důvěru, aby se žáci nebáli svěřit, a pracujte se třídou, aby se zabránilo stigmatizaci oběti.

Odkazy

Digitální stopa ve škole
https://digitalizace.rvp.cz/clanky/digitalni-stopa-ve-skole

Profil metodika prevence - co dělá a co umí?
https://digitalizace.rvp.cz/clanky/profil-metodika-prevence-co-dela-a-co-umi

DigiKoalice (ČR):
Kyberprevence – katalog preventivních programů v oblasti kyberprevence
https://digikoalice.cz/kyberprevence/

E-Bezpečí (ČR):
Deepfake a svlékací aplikace – varování a doporučení, jak se chránit
https://www.e-bezpeci.cz/index.php?view=article&id=3997

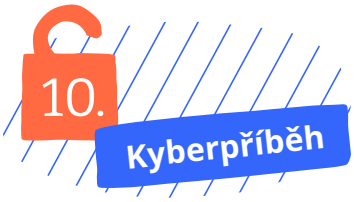
Asociace pro rozvoj AI v ČR:
Varování – svlékací aplikace a AI DeepNude: jak reagovat v případě zneužití fotografie
https://asociace.ai/varovani-svlekaci-aplikace-a-ai-deepnude-jak-reagovat-v-pripade-zneuziti-fotografie/

Klasifikace

Zneužívající obsah (abusive content)

Klíčová slova

Deepnude, kyberšikana, svlékací aplikace



Kluk z vedlejší školy

Anežka, žákyně sedmé třídy základní školy, se jednoho dne svěřila své nejlepší kamarádce Janě, že si píše s Martinem – starším klukem, který prý studuje na střední škole ve stejném městě. Povídala si s ním o společných zájmech, posílali si fotky a Anežka byla z jejich komunikace nadšená. **Martin byl milý, pozorný a zdál se jí opravdu skvělý.** Dokonce plánovali, že se brzy setkají osobně.

Jana měla ale zvláštní pocit. Něco jí na celé situaci nesedělo. Zeptala se proto svého staršího bratra, který danou střední školu navštěvoval. Od něj se dozvěděla překvapivou zprávu – žádný **Martin toho jména a popisu na škole nestuduje.**

Když se Anežka kamarádce svěřila, že ji **Martin začal žádat o „odvážnější" fotky,** Jana zpozorněla. Anežka se nejdřív zdráhala, ale Martin na ni začal naléhat a vyvíjet tlak. Když mu neodpovídala tak, jak si přál, změnil tón – začal být nepříjemný a naléhavý. Jana měla o kamarádku strach a rozhodla se jednat. **Svěřila se jejich třídnímu učiteli.**

Třídní učitel s Anežkou citlivě promluvil. Podle toho, co mu dívka popsala, rozpoznal varovné znaky kybergroomingu – nebezpečného chování dospělých, kteří se v online prostředí vydávají za vrstevníky, aby si získali důvěru dítěte a zneužili ji. Po chvíli Anežka se slzami v očích přiznala, že **Martinovi nakonec jednu odhalenou fotografii poslala.** Nyní jí vyhrožuje, že ji zveřejní, pokud mu nezaplatí.

Učitel přivolal školního metodika prevence. Společně zajistili důkazy a zahájili další kroky. O celé situaci informovali Anežčiny rodiče, kteří podali trestní oznámení na Policii ČR.

Anežce byla poskytnuta **psychologická pomoc** a škola následně **posílila preventivní aktivity** v oblasti online bezpečnosti. Zdůraznila také důležitost kybernetické bezpečnosti a prevence a správného nastavení soukromí na sociálních sítích.

Poučení

1. **Budujte důvěru** – podporujte prostředí, kde se žáci nebojí svěřit s problémy – i z online světa.
2. **Mějte připravený krizový scénář** – sepište jasné postupy pro případy kybergroomingu a zajistěte, aby je všichni znali.
3. **Spolupracujte v týmu** – zapojte metodika prevence, psychologa, rodiče i Policii ČR, pokud je to nutné.

4. **Školte pedagogy** – vzdělávejte učitele v oblasti kyberprevence a rozpoznávání varovných signálů.
5. **Zařaďte prevenci do výuky** – učte žáky bezpečnému chování online a ochraně soukromí.
6. **Podpořte oběť** – zajistěte psychologickou pomoc a ochraňte žáka před stigmatizací.

Odkazy

DigiKoalice (ČR):
Kyberprevence – katalog preventivních programů v oblasti kyberprevence
https://digikoalice.cz/kyberprevence/

Profil metodika prevence – co dělá a co umí?
https://digitalizace.rvp.cz/clanky/profil-metodika-prevence-co-dela-a-co-umi

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost (ČR):
Kybergrooming
https://osveta.nukib.gov.cz/mod/page/view.php?id=1114

E-Bezpečí
Kybergrooming
https://www.e-bezpeci.cz/kybergrooming/

Internetem bezpečně
Kybergrooming
https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

RVP.CZ – Portál pro pedagogické pracovníky,
Kybergrooming
https://clanky.rvp.cz/clanek/22970/KYBERGROOMING.html

Česká televize
Edu
Kybergrooming
https://edu.ceskatelevize.cz/video/2848-kybergrooming

Nebuď oběť
Kybergrooming
https://nebudobet.cz/kybergrooming/

Klasifikace

Zneužívající obsah (abusive content)

Klíčová slova

Kybergrooming, zneužití fotografie

Kyberpříběhy
Motivační příběhy o kybernetické bezpečnosti ve škole

Autorři:
Lucie Gregůrková
Jaroslav Šindler
Veronika Němcová
a kolektiv projektu AIDIG

1. české vydání

Národní pedagogický institut České republiky, Praha, 2025

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

Národní pedagogický institut České republiky
2025
www.npi.cz