Národní knihovna
České republiky

Kybernetický útok na Národní knihovnu ČR

Prezentace pro konferenci
CACIO

22. 02. 2022

Národní knihovna
České republiky

Úvod

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

O NÚKIB | INFOSERVIS | ÚŘEDNÍ DESKA | KYBERNETICKÁ BEZPEČNOST | OCHRANA UI V ICT | GALILEO PRS | KONTAKTY | CS / EN

- Aktuality
- Hrozby a zranitelnosti
- Doporučení
- Dokumenty a Publikace
- Konference

Aktuality

NÚKIB › Infoservis › Aktuality › Kybernetické incidenty pohledem NÚKIB: říjen 2021

Kybernetické incidenty pohledem NÚKIB: říjen 2021

9. listopad 2021

Říjen se co do počtu incidentů stal druhým nejrušnějším měsícem tohoto roku. NÚKIB evidoval 14 kybernetických incidentů. Většina z nich nicméně neměla vážné následky a podařilo se je rychle vyřešit.

Podobně jako v předchozích měsících se v hlášeních objevovaly DDoS útoky, phishingové kampaně nebo škodlivé kódy v sítích českých organizací. Mezi incidenty byl také jeden ransomware, který zašifroval část infrastruktury oběti a následně na svých stránkách vyhrožoval zveřejněním jejích dat.

Více informací si můžete přečíst zde: https://www.nukib.cz/download/publikace/vyzkum/Kybernetické_incidenty_2021-10.pdf

› Předchozí

› Následující

Zpráva NÚKIB, 09. 11. 2021.

ČTK ČESKÉ NOVINY

ČR | Svět | Ekonomika | Kultura | Sport | Magazín | Speciál | 26°C

AKTUÁLNĚ: Koronavirus | Olympiáda v Tokiu

Počet vyděračských útoků v ČR letos stoupl o 259 pct

Aktualizace: 13.05.2021 17:18 Vydáno: 13.05.2021, 17:18

Počítač, klávesnice, zabezpečení, ochrana - ilustrační foto. CTK/A3817 Tobias Felber, DPA

Praha - V České republice vzrostl od začátku roku počet vyděračských hackerských útoků o 259 procent. Celosvětově největší počet ransomwarových útoků přitom cílí na zdravotnictví, průměrně jde o 109 útoků na jednu organizaci za týden. Následují veřejné služby s 59 útoky a pojišťovny a právní společnosti s průměrně 34 útoky týdně na jednu firmu. V tiskové zprávě to dnes uvedla bezpečnostní firma Check Point, podle které je dopad ransomwaru na české společnosti aktuálně na více než dvojnásobku celosvětového průměru. Bližší údaje neuvedla.

Kyberzločinci v souvislosti s ransomwarovými útoky úspěšně využívají taktiku dvojitého vydírání. Požadují výkupné za zašifrovaná data a zároveň hrozí zveřejněním ukradených dat na speciálních webových stránkách. Průměrná výše výkupného se za poslední rok zvýšila o 171 procent na přibližně 310.000 dolarů (zhruba 6,5 milionu korun). V roce 2020 došlo k úniku dat z více než 1000 společností, které odmítly splnit požadavky a zaplatit výkupné.

Přibližně 40 procent všech nových ransomwarových programů využívá nějakým způsobem kromě šifrování i krádeže dat. Je tedy zřejmé, že útočníci hledají způsoby, jak zvýšit efektivitu hrozeb a donutit oběti k zaplacení výkupného. Posledním zveřejněným případem ransomwaru byl útok na produktovody Colonial Pipeline v USA, který má na svědomí hackerská skupina Darkside.

Novinkou je tzv. trojité vydírání. Prvním takovým případem byl útok na finskou psychoterapeutickou kliniku Vastaamo, která má více než 40.000 pacientů. Útočníci požadovali platbu výkupného nejenom od kliniky, ale menší částky chtěli i od pacientů, kteří požadavky útočníků obdrželi individuálně e-mailem. Kyberzločinci ve zprávách zároveň vyhrožovali, že pokud nedojde ke zaplacení stanovené částky, zveřejní záznamy z terapeutických sezení.

Tento trend je přitom stále výraznější. Například v únoru 2021 zveřejnila hackerská

PRÁVĚ ZVEŘEJNĚNO

- Benzin je v ČR nejdražší od prosince 2014, cena se blíží 34 korunám za litr
- Judista Krpálek postoupil na OH do semifinále a čeká ho Harasawa
- Schoenmakerová triumfovala na 200 m prsa ve světovém rekordu
- Knižní thriller, podle kterého natáčí Netflix svůj nejdražší film.
- The Independent: Ve Vancouveru v rámci boje s drogami rozdávají kokain zdarma
- Sněmovna projedná zvýšení důchodů a odškodnění za výbuch ve Vrběticích
- ČSÚ zveřejní první odhad vývoje ekonomiky ve druhém čtvrtletí

Všechny zprávy

Zpráva ČTK, 13. 5. 2021.

Národní knihovna
České republiky

Národní knihovna ČR a její role v oblasti digitálních dat a služeb

- Knihovní zákon (257/2001 Sb.):
  - §9, 2)
  - „Národní knihovna je centrem systému knihoven. V systému knihoven vykonává **koordinační, odborné**, informační, vzdělávací, **analytické, výzkumné, standardizační, metodické a poradenské činnosti**…“

- Zřizovací listina NK ČR
  - Článek 2), bod b)
  - „Národní knihovna **získává elektronické dokumenty, a to od jiných osob i vlastní digitalizací dokumentů, sklízením obsahu volně dostupného internetu** a na základě dobrovolného nebo povinného odevzdávání publikovaných elektronických dokumentů…“

  - Článek 2), bod b)
  - „Národní knihovna spravuje a ochraňuje knihovní dokumenty a fondy.“
  - „**Spravuje a ochraňuje též fondy elektronických dokumentů**.“
  - „Formuluje **strategie a postupy dlouhodobé ochrany elektronických dokumentů a provozuje důvěryhodné digitální úložiště**.“

Národní knihovna
České republiky

Národní knihovna ČR a její role v oblasti digitálních dat a služeb

- DIGITALIZACE:
  - ročně je v prostředí českých knihoven digitalizováno zhruba **4 500 000 stran dokumentů**
  - **NK ČR a MZK Brno provozují největší digitalizační pracoviště** v segmentu paměťových institucí na území ČR
  - NK ČR v rámci svého poslání v oblasti dlouhodobé archivace digitálního obsahu (LTP) **ukládá i data dalších knihoven** – například dat vzniklých za podpory dotačního mechanismu VISK 7
  - NK ČR provozuje celosvětově unikátní (celistvost dat, pravidelnost sklizní) **systém Webarchiv – nyní asi 410 TB dat**
  - prezentace digitálního obsahu v rámci knihoven **Manuscriptorium a Národní digitální knihovna** (opět i data dalších českých knihoven) – tyto digitální knihovny **jsou součástí nadnárodních agregačních portálů** (například Europeana), což patří mezi prioritní oblasti požadované EU po ČR

- PROVOZ CENTRÁLNÍCH KNIHOVNICKÝCH SYSTÉMŮ
  - **Souborný katalog ČR (k 31. 12. 2020 celkem 7 830 891 záznamů**; počet knihoven umožňujících sklízet záznamy do Souborného katalogu ČR prostřednictvím OAI-PMH protokolu v roce 2020 **vzrostl na 136**, tj. cca o jednu třetinu oproti předcházejícímu roku)
  - **Národní autority** (silný dopad na další instituce; spolupráce s Národním archivem)
  - **Manuscriptorium** (zapojení nejen českých institucí, ale i dalších evropských knihoven; centrální portál pro zpřístupnění digitalizovaných rukopisů a starých tisků)
  - **Registr digitalizace** (ústřední autorita pro ověřování unikátnosti digitalizačních aktivit na území ČR)
  - **Seznam děl nedostupných na trhu** a s ním spojené **zpřístupnění děl nedostupných na trhu** (unikátní přístup k digitálnímu obsahu v době složité epidemické situace)
  - **Číslo České národní bibliografie** (systém na kontrolu duplicit a unikátnosti fyzických dokumentů)
  - **Přidělování ISBN** (unikátnost fyzických dokumentů v moment jejich vydání)

Národní knihovna
České republiky

Stav bezpečnosti ICT v době „před kybernetickým útokem“

- NK ČR má vydanou a platnou Směrnici č. 3/2019 „Systém řízení bezpečnosti informací“ včetně jejích příloh.

- Na základě vydané směrnice probíhala 2x ročně školení vedená Ředitelem odboru kybernetické bezpečnosti, který byl zároveň Manažerem kybernetické bezpečnosti. Školení byla povinná pro všechny zaměstnance NK ČR.

- V pravidelných intervalech docházelo k aktualizaci pracovních zařízení včetně antivirového systému, pravidelné údržby koncových stanic, aktualizaci firewallů apod.

- V souvislosti s nárůstem spamů docházelo průběžně k nastavování antispamových filtrů.

- Na podzim 2020 byla zahájena příprava aktivit na rok 2021, které měly za cíl zvýšit kvalitu poskytování služeb, zvýšit bezpečnost a zajistit stabilizaci jednotlivých ICT systémů. Prvním krokem bylo rozdělení systémů:
  - Do třech oblastí:
    - Infrastruktura
    - Interní uživatelé
    - Externí uživatelé
  - a třech základních skupin:
    - Interní
    - Knihovní
    - Weby

- Ve všech oblastech byl zahájen provisioning a performance tuning.

Národní knihovna
České republiky

Kybernetický útok – vznik incidentu

- V úterý ráno 18. května 2021 chtěl pracovník podpory koncových zařízení provést standardní kontrolu stavu aktualizace jednotlivých pracovních stanic pomocí konzole antivirového programu, která však byla nedostupná. Při další diagnostice stavu bylo zjištěno, že je celý server zašifrován.

- Na základě zjištění uvedený pracovník ihned informoval své nadřízené.

- Okamžitě poté byli kontaktováni pracovníci externích dodavatelů i všichni interní IT pracovníci a byli povoláni do prostor NK ČR.

- Byl informován generální ředitel.

- **REAKCE NK ČR BYLA OKAMŽITÁ BEZ PRODLEVY DLE STANDARDNÍCH BEZPEČNOSTNÍCH PROTOKOLŮ**

- Na jednom zařízení pracovníka sekce Digitalizace a technologie bylo zjištěno, že v brzkých ranních hodinách došlo ze strany doménového administrátora k přihlášení na zařízení. Vzhledem k tomu, že se jedná o nestandardní situaci, došlo k dalším kontrolám na ostatních zařízení, kde bylo přihlášení doménového administrátora také zjištěno.

- Vzhledem k tomu, že došlo k zneužití účtu doménového administrátora, došlo ze strany vedení sekce Digitalizace a technologie k rozhodnutí o okamžitém zahájení odpojování serverů a koncových stanic od sítě tak, aby se předešlo větším škodám a ztrátám, a to jak finančním, tak i na uložených datech jednotlivých ICT systémů a tím minimalizovat dopady.

Národní knihovna
České republiky

Kybernetický útok – první zabezpečení

- Následně byla zahájena komplexní diagnostika k odhalení rozsahu a bylo zjištěno, že:
  - **kybernetický útok proběhl v noci z pondělí 17. na úterý 18. května 2021 na systémy používané Národní knihovnou ČR,**
  - **měl za cíl znemožnit poskytování služeb čtenářům a paralyzovat chod Národní knihovny ČR poškozením/znepřístupněním klíčových systémů, které poskytují jak externí, tak interní služby a pracovních stanic zaměstnanců Národní knihovny ČR,**
  - **kybernetický útok byl úspěšný a jeho rozsah chod Národní knihovny ČR citelně zasáhl.**
- Při prvotní analýze po vzniku dané situace jsme identifikovali **e-mail z adresy pracovníka Slovenského hydrometeorologického ústavu, který vyzýval k obnově hesla do systémů Windows pomocí odkazu**, na který několik zaměstnanců NK ČR reagovalo kliknutím a vyplněním svých údajů.
- **Šlo tak o sofistikovaný útok a zdroj** (pro připomínku – **Klementinum je spojené více než 200 let s hydrometeorologickým měřením**; mail tak bylo jen obtížné možné lidsky i „strojově“ odhalit a předem minimalizovat lidské selhání). Následně byl kontaktován bezpečnostní ředitel Slovenského hydrometeorologického ústavu, který potvrdil problémy i na jejich straně.

Národní knihovna
České republiky

Kybernetický útok – první zabezpečení

- Byl kontaktován externí dodavatel podpory antivirového systému Kaspersky, který okamžitě sjednal schůzku přímo s vydavatelem antivirového systému, požádal o vzorek daného ransomware a po zhodnocení situace doporučil postup pro obnovu zařízení.

- O dané situaci byl nejdříve telefonicky, následně písemně **informován Národní úřad kybernetické a informační bezpečnosti** a jeho pracovníci byli požádáni o konzultaci.

- **Byla informována Policie České republiky**. Hlídka Policie ČR se dostavila na místo, zajistila prvotní informace a vyčkala na specialistu z odboru kybernetické bezpečnosti. Ten provedl došetření dané situace a následně bylo ze strany NK ČR podáno na služebně Policie ČR podáno trestní oznámení na neznámého pachatele.

- V následujících dnech probíhala s odpovědným pracovníkem Policie ČR další komunikace o průběhu incidentu.

- **Hlavní důraz byl v prvních fázích zaměřen na ochranu majetku a fondů NK ČR** – obratem byla posílena fyzická ostraha všech objektů, byl zvýšen dohled na fyzický stav fondů a ochrana klíčových perimetrů

Národní knihovna
České republiky

Kybernetický útok – první zabezpečení

- Proběhlo určení priorit postupy obnovy jednotlivých systémů.
- Na základě určených priorit byl sestaven plán obnovy.
- Byl zjištěn stav záloh jednotlivých systémů.
- Došlo k přípravě postupu pro obnovu pracovních stanic.
- Bylo vytvořeno zcela nové síťové prostředí oddělené od původního.
- Následně byla zahájena instalace infrastruktury v novém prostředí dle určených priorit.
- **Zasaženy byly zejména systémy na platformě Windows a uživatelské stanice**.
- **Systémy na platformě LINUX byly ochráněny** a tudíž bylo možné tyto systémy opět zpřístupnit.

Národní knihovna
České republiky

Kybernetický útok – došetření vzniku

- Následně proběhlo detailní šetření celého incidentu, v jehož průběhu bylo zjištěno, že se jednalo o cílený útok na prostředí NK ČR, neboť došlo ke zcizení přihlašovacích údajů jedné ze zaměstnankyň NK ČR.
- Ta dne 17. 05. 2021 v rámci Home Office pracovala z domova na služebním notebooku a pomocí služební VPN se hlásila k systémům NK ČR. Své aktivity ukončila ve večerních hodinách cca ve 20:30 hodin.
- V 19:30 hodin bylo navázáno spojení z Ruska, kdy VPN klient dostal jiné interní IP na shodné jméno. Obě VPN asi hodinu koexistovaly. V 19:39 hodin začal probíhat sken jednotlivých stanic na potencionálně rizikových portech, které využívá Microsoft prostředí.
- Tyto porty však měla NK ČR blokovány a proto útočník zvolil jiný směr útoku. Sken jednotlivých stanic na portu 3389 přivedl útočníka na e-mailový systém MS Exchange a další aktivity zaměřil proti němu.
- Útok byl veden na porty 445 a 3389, jenž jsou porty Windows technologií. Útočník svou aktivitu ukončuje kolem 05:00 hodin ráno 18. 05. 2021.
- V průběhu útoku dokázal převzít administrátorský účet doménového administrátora a s jeho přihlašovacími údaji, byl schopen přihlašovat se a následně vypínat antivirový systém na jednotlivých pracovních stanicích a serverech a zároveň pouštět ransomware, s jehož pomocí zašifroval data uživatelům a také některá data na serverech.

Národní knihovna
České republiky

Kybernetický útok – další kroky – optimalizace vnitřních postupů

- Bylo vydáno opatření generálního ředitele ohledně **kurzu základů kybernetické bezpečnosti** pořádané MZK/NÚKIB, které **je povinné pro všechny zaměstnance** (https://kurzy.knihovna.cz/enrol/index.php?id=14) a je zakončené certifikací. V případě potřeby bude probíhat doškolení zaměstnanců ve složitých otázkách.

- **Vedení NK ČR zahájilo jednání s NÚKIB o podpisu memoranda o spolupráci** ohledně vzdělávání a zvýšení povědomosti zaměstnanců v oblasti kybernetické bezpečnosti a připojení se k digitalizaci státu napojením na NIA a BankID.

- **Byl aktualizován vnitřní metodický postup – Bezpečnostní příručka uživatele**, která obsahuje povinnosti zaměstnanců NK ČR v oblasti kybernetické bezpečnosti. Na základě vydaného vnitřního metodického pokynu **vzniklo Desatero ISMS**, které bylo předěláno i do přehledné grafické podoby.

- Nadále probíhá aktualizace bezpečnostní směrnice a jejích příloh, jsou připravovány další metodické postupy, návody a upravují se procesy pro uživatele – údržba emailových schránek, používání certifikátů apod.

- Jsou aktualizovány přehledy jednotlivých systémů a subsystémů a jejich komponent (HW, SW), stanovení třídy dostupnosti, zabezpečení a integrity, včetně ohodnocení aktiv a určení garantů jednotlivých systémů.

- Vytváříme analýzu rizik, **release plány, disaster recovery plány, plány zálohování včetně obnovy ze záloh**, stanovení životních cyklů systémů.

Národní knihovna
České republiky

Kybernetický útok – další kroky – optimalizace vnitřní IT infrastruktury

- Spuštění interní certifikační autority PKI.
  - Instalace osobních (zaměstnaneckých) interních CA.
  - Instalace interních CA na zařízení pracovníků NK ČR.
  - Vytvoření interních CA pro dodavatele.
- **Vytvoření nové VPN**.
- Obnovení systému NDK
- Upgrade zařízení Fortigate, včetně úpravy základních pravidel a nastavení základních parametrů pro zajištění bezpečnosti.
- **Vytvoření nových segmentů sítě, rozložení dle potřeb obnovy a kritičnosti systémů.**
- **Upgrade centrálních síťových prvků**, změna topologie sítě.
- Zajištění HA režimu pro klíčové systémy NK ČR.
- Vytvoření virtuálního prostředí pro čtenáře NK ČR.

Národní knihovna
České republiky

Kybernetický útok – střednědobé a dlouhodobé plány

- Zpracování release plánů – připravit proces pro nasazování nových verzí ICT systémů, aplikací a služeb.
- Zpracování analýzy rizik – ohodnocení jednotlivých systémů, stanovení vlastníků aktiv.
- Zpracování architektury systémů, včetně popisu datových toků.
- **Zajištění dokumentace – provozní řády, administrátorská provozní dokumentace.**
- Vytvoření aktualizovaných havarijních plánů, DRP a BCP.
- Zpracování dalších metodik bezpečnosti a pracovních postupů.
- Zajištění dalšího školení uživatelů
- **Zajistit pravidelné testování obnovy jednotlivých systémů.**
- Spuštění systému testovacích zpráv, modelování útoky apod. k otestování chování pracovníků NK ČR

Národní knihovna
České republiky

Leasson Learned – lidský kapitál

- Organizace může být sebelépe připravená, rozhodující je však lidský faktor.

- **Je nezbytné změnit myšlení pracovníků a neustále zvyšovat jejich povědomí v oblasti každodenního využívání informačních a komunikačních technologií**. Informační bezpečnost představuje ochranu informací a jejich uživatelů ve všech jejich formách a po celý jejich životní cyklus – tedy během jejich vzniku, zpracování, ukládání, přenosu a likvidace.

- **Striktně dodržovat pravidlo „Co není povoleno, je zakázáno“**.

- Při obnově systémů se ukázal potenciál pracovníků NK ČR (přesčasová práce, víkendová práce, osobní zaujetí) a v pozitivním i negativním možnosti spolupráce s externími subjekty.

- Počet kybernetických útoků narůstá – je třeba najít modely intenzivní organizační, metodické i finanční spolupráce a pokrytí možných dopadů „v předstihu“.

- **Zajištění připravenosti jednotlivých institucí na obdobné případy**, vytvoření analýz připravenosti napříč institucemi.

- Je třeba sdílet Best practices, postupy při obnově systémů atd. = **zřízení týmu na úrovni MK ČR a významných státních příspěvkových organizací.**

Národní knihovna
České republiky

Leasson Learned

- Pro zvýšení zabezpečení využívat zabezpečené protokoly HTTPs, LDAPs, apod.

- Oblasti kybernetické ochrany je třeba věnovat se **systematicky, dlouhodobě a pravidelně do této oblasti investovat** (obměna softwaru i hardwaru alespoň v pětiletých cyklech).

- Nutno zabezpečit změnu jednotlivých systémů – zajistit jejich přepracování, zvýšit zabezpečení uživatelských dat.

- **Využívat více bezpečnostní nástroje – zátěžové a penetrační testy.**

- Systémově řešit **NEvyužívání „domácích" a neověřených externích komponent** (externí disky, USB flash disky, CD, apod.)

- Obnova dat je věcí časově velmi náročnou, je třeba mít k dispozici **funkční politiku zálohování** (oddělené geografické lokace, různé typy médií, cloudová řešení atd.).

Děkujeme za pozornost a vítáme Vaše dotazy.