



Národní knihovna
České republiky

Kybernetický útok na Národní knihovnu ČR

Prezentace pro konferenci
Archivy, knihovny, muzea v digitálním světě 2021

01. 12. 2021

Národní úřad pro kybernetickou a informační bezpečnost



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

Aktuality

Hrozby a zranitelnosti

Doporučení

Dokumenty a Publikace

Konference

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 nejnižším 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/kyberneticke_incidenty_2021-10.pdf

[Předchozí](#)

[Následující](#)

Aktuality



ČTK ČESKÉ NOVINY

Počet vyděračských útoků v ČR letos stoupl o 259 pct

Situace 13.05.2021 07:08 | Vydáno 13.05.2021, 07:08

Práva zveřejněno

Benny je v ČR nejoblíbenější od prosince 2014, cena se blíží 54 korunám za litr

Južita Wypiólek postoupila na OH1 do senátů a čeká ho Hlasava

Schrammův první triumf na 200 m prave ve světovém rekordu

Krůňák štrlel, podle klanové rakši Netflix svůj nejdražší film

The Independent: Ve Varsovu v rámci boje s drogovými kartely zadrželi kokain stáma

Sedmátná projektová zpráva vřichů a odškodnění za výbuch ve Větráckách

ČSÚ zveřejnil první odhad vývinu vlnovanky ve druhém čtvrtletí

Všechny zprávy

ENDORPHIN REPUBLIC

Útoky na úřady



- 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.“



➤ 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)



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 měli 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.

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 zařízeních, 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.



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 dalším pátrání 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.



Kybernetický útok – první zabezpečení

- Obratem byl aktivován Krizový štáb NK ČR
- Členové Krizového štábu podepsali Dohodu o mlčenlivosti
- Probíhala pravidelná jednání, kde byli členové Krizového štábu detailně informováni o průběhu obnovy ICT systémů a služeb
- Dle možností byly sdíleny informace zaměstnancům NK ČR
- **Z jednání Krizového štábu byli pořizovány zápisy, které jsou uloženy u Bezpečnostního ředitele**
- Krizový štáb nerozhodoval jen o dalších činnostech směřujících k obnově všech ICT systémů, ale i jednotlivých krocích v oblasti běžných služeb a dalších aktivit NK ČR



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

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.



Kybernetický útok – obnova zařízení uživatelů

- Na pracovních stanicích byla zahájena kontrola stavu a byly použity domluvené procesy pro obnovu zařízení pomocí utility Rescue Disc, souběžně s tzv. čištěním PC probíhal update všech systémů Microsoft a reinstalace klientského antivirového programu. Tyto činnosti byly časově velice náročné a příprava jednoho zařízení na přepojení do nového síťového prostředí trvala průměrně 2 hodiny v závislosti na stáří a technického vybavení jednotlivých PC.
- PC, které obsahovaly zašifrované soubory byly uživatelům odebírány. Následně na PC došlo k výměně pevných disků a nainstalování operačního systému a kancelářských programů.
- Součástí procesů obnovy byl proveden import/export lokální zálohy .pst souboru k obnově e-mailové komunikace.
- Pro klíčové interní systémy docházelo k postupnému vytvoření zcela nové infrastruktury na posledních verzích operačního systému Windows včetně instalace antivirového systému a jejich obnovy dat ze záloh tam, kde zálohy byly dostupné.
- Proběhlo první nastavení firewallu v souvislosti s vytvořením nového prostředí a došlo k prvnímu update na vyšší verzi firmware a aplikaci bezpečnostních patchů.
- Následně byl zajištěn chod klíčových knihovnických systémů, které nebyly napadeny.
- **Celkový počet uživatelských zařízení – 1178 (PC a notebooků).** Nejde jen o osobní počítače, ale i pracovní stanice určené k ovládání strojového vybavení NK ČR (například vakuová komora, plotter), kontrolu klimatu či koncových zařízení studoven a vybavení pro čtenáře.
- **Celkový počet obnovených serverů - 67 fyzických, 223 virtuálních serverů**



Kybernetický útok - obnova infrastruktury

➤ Systémy obnovené obratem

- ALEPH, Kramerius, Manuscriptorium, Webarchiv

➤ Systémy obnovené od jednoho týdne od incidentu:

- Active Directory, MS Exchange, DNS, DHCP, LDAP, Centrální antivirový program Kaspersky, ekonomický systém K2, WSUS, Spisová služba, Registr digitalizace, Asset Web systém, Nástroje Haly služeb vč. počítačů

➤ Systémy obnovené v dalším období po incidentu

- Resolver URN:NBN, GitLab profil, Shibboleth, Evidence smluv, Centrální tiskové řešení, Intranet, Micos, Service Desk, webové servery NK ČR a další

Součástí obnovy systémů nebylo jen jejich znovuspuštění, ale i obnova dat, nastavení politiky záloh, obnova pracovních stanice atd. = procesy obnovy probíhaly paralelně.

Národní knihovna ČR byla schopna obnovit svůj základní provoz již 24. května 2021, studovny otevřeny 2. června 2021.

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.



- 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.



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

Lesson 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.**

Lesson 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.).
- **NK ČR je ochotna** (zatím v míře dané limity probíhajícího vyšetřování) **sdílet své zkušenosti a nabyté znalosti.**



Děkujeme za pozornost a
vítáme Vaše dotazy.