Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
IČO: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
350 - 302/2022
Číslo jednací:
2384/2022-NÚKIB-E/350

Brno, 25. února 2022

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno (dále jen „Úřad“), podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“), vydává toto

varování

před hrozbou v oblasti kybernetické bezpečnosti, spočívající v realizaci kybernetických útoků na informační a komunikační systémy v České republice, zejména pak na systémy veřejné správy, ale i dalších strategických organizací. Tyto útoky mohou mít dopady na dostupnost, důvěrnost či integritu informací u důležitých informačních a komunikačních systémů.

Úřad tuto hrozbu hodnotí na úrovni Kritická – Hrozba je velmi pravděpodobná až téměř jistá.

Úřad vzhledem ke Kritické hrozbě kyberšpionáže a dalších kybernetických útoků doporučuje:

1. **Zvýšenou ostražitost vůči nejčastěji používaným technikám útoků v kyberprostoru, kterými jsou zejména:**
   - T1059 (Command and Scripting Interpreter),
   - T1218 (Signed Binary Proxy Execution),
   - T1543 (Create or Modify System Process),
   - T1053 (Scheduled Task/Job),
   - T1003 (OS Credential Dumping),
   - T1055 (Process Injection),
   - T1027 (Obfuscated Files or Information),
   - T1105 (Ingress Tool Transfer),
   - T1569 (System Services),
   - T1036 (Masquerading),
   - T1486 (Data Encrypted for Impact),
   - T1082 (System Information Discovery),
   - T1497 (Virtualization/Sandbox Evasion),
   - T1498 (Network Denial of Service),

- T1566 (Phishing),
- T1078 (Valid Accounts),
- T1190 (Exploit Public-Facing Application),
- T1133 (External Remote Services),
- T1595 (Active Scanning),
- T1110 (Brute Force),
- T1561 (Disk Wipe).

2. **Provést aktualizace informačních systémů a jejich komponent tam, kde je taková aktualizace vzhledem k zajištění plynulosti provozu možná, aby bylo předejito zneužití známých zranitelností, kterými jsou aktuálně zejména:**
   - CVE-2018-13379 v systému FortiGate VPN,
   - CVE-2019-1653 v systému Cisco,
   - CVE-2019-2725 v systému Oracle WebLogic Server,
   - CVE-2019-7609 v systému Kibana,
   - CVE-2019-9670 v systému Zimbra,
   - CVE-2019-10149 v systému Exim Simple Mail Transfer Protocol,
   - CVE-2019-11510 v systému Pulse Secure,
   - CVE-2019-19781 v systému Citrix,
   - CVE-2020-0688 v systému Microsoft Exchange,
   - CVE-2020-4006 v systému VMware One Access a Identity Manager,
   - CVE-2020-5902 v systému F5 Big-IP,
   - CVE-2020-14882 v systému Oracle WebLogic,
   - CVE-2021-26855 v systému Microsoft Exchange,
   - CVE-2021-44228 v systému Apache Log4j.

3. **V reakci na hrozbu útoků typu distribuovaného odepření služby (dále jen „DDoS“) Úřad doporučuje následující:**

   3.1. Preventivní opatření doporučená všem organizacím (před DDoS útokem)
   - Prověřit možnosti blokování nežádoucí komunikace zahlcující nebo jinak omezující provozované systémy na hraničním prvku infrastruktury.
   - Zjistit a připravit si kontaktní údaje na poskytovatele internetového připojení. Ověřit kontaktní osoby v organizaci, které mají možnost a oprávnění kontaktovat poskytovatele internetového připojení a zajistit s poskytovatelem internetového připojení náhradní komunikační kanál (ideálně jeden off-line a jeden online kanál), pokud by došlo k zahlcení jeho linky. Připravit si identifikační údaje odebíraných služeb (číslo smlouvy apod.).
   - Kontaktovat poskytovatele připojení a zjistit možnosti blokování nežádoucí komunikace zahlcující nebo jinak omezující systém na straně poskytovatele internetového připojení, pokud tyto možnosti nejsou organizaci známy (např. FlowSpec, RTBH nebo na základě požadavku).
   - Připravit si strategii a případně konfigurace prvků pro extrémní situace zajišťující řízené omezování dostupnosti zbytných služeb a maximální zachování dostupnosti nezbytných služeb.
   - Ověřit možnost provozování systému v ostrovním režimu (tedy bez připojení k internetu, nebo při omezení dostupnosti, např. mimo Česko).

- Připravit se na možnost blokování IP adres, IP rozsahů nebo IP adres dle čísla autonomního systému (ASN) publikovaných na webových stránkách Úřadu. Blokovat komunikaci dle případně publikovaných indikátorů (Úřad tyto informace poskytne ve strojově čitelném formátu).
- Připravit se na nutnost blokování překladu některých domén na DNS (např. na DNS resolveru).
- Připravit komunikační strategii a komunikační kanály (např. sociální sítě) pro informování veřejnosti v případě nedostupnosti poskytovaných služeb.
- Sledovat web NÚKIB pro případ vydání dalších varování nebo doporučení.

3.2. Opatření doporučená všem organizacím při probíhajícím DDoS útoku

- Blokovat nežádoucí komunikaci před zahlcením linky mezi poskytovatelem internetového připojení a hraničním prvkem, a to i za cenu blokování legitimní komunikace (GeoBlocking, blokace na základně ASN).
- V případě zahlcení linky kontaktovat poskytovatele internetového připojení a koordinovat s ním řešení zahlcení.
- Bezodkladně kontaktovat Úřad a nahlásit rozsah omezení poskytovaných služeb včetně typu nežádoucího provozu a IP adres, ze kterých pocházel.

3.3. Preventivní opatření doporučená poskytovatelům internetového připojení (před DDoS útokem)

- Prověřit možnosti blokování nežádoucí komunikaci zahlcující nebo jinak omezující provozování systémů.
- Připravit se na blokování nežádoucí komunikace dle požadavků zákazníků, tzn. maximálně automatizovat proces blokace (pro zákazníky s BGP připravit RTBH a komunikovat s nimi tuto možnost).
- Je-li to možné a efektivní, konzultovat a připravit s partnery možnost zajištění blokování nežádoucí komunikace již v předcházejících (z hlediska směru přenosu „*upstream*“) sítích, například pomocí technologie Remotely Triggered Black Hole (RTBH).
- Připravit se na možnost blokování IP adres, IP rozsahů nebo čísel autonomních systémů (ASN) publikovaných na webových stránkách Úřadu. Blokovat komunikaci dle případně publikovaných indikátorů (Úřad tyto informace poskytne ve strojově čitelném formátu).
- Provést zálohu konfigurací kritických síťových zařízení a uchovávat jí v režimu záloh 3-2-1 (3 kopie, 2 různá média, 1 záloha mimo pracoviště) a zajistit jejich integritu (kontrolní součty, sledování změn verzí).
- Zavést aktivní monitoring změn konfigurací.
- Provést fyzickou inventuru náhradních kritických komponent (např.: routery, switche a jiné), zajistit v případě potřeby dostupnost těchto komponent.
- Provést kontrolu aktuálnosti připomenutí postupů obnovy při havárii (*Disaster Recovery*) a provést školení pracovníků za účelem jejich připomenutí.
- Zajistit, aby všechny linky měly dostatečnou rezervu přenosových kapacit.
- Připravit monitoring infrastruktury pro účely zjišťování směru útoku, např. sledování MAC adres s cílem zjistit, ze kterého směru (peeru) DDoS útok přichází.
- Sledovat web NÚKIB pro případ vydání dalších varování nebo doporučení.

3.4. Opatření doporučená poskytovatelům internetového připojení při probíhajícím DDoS útoku

- Blokovat nežádoucí komunikaci dle požadavků zákazníků.
- Prioritizovat blokace nežádoucí komunikace směřující na systémy kritické informační infrastruktury, informačních systémů základních služeb a významných informačních systémů.
- Bezodkladně kontaktovat Úřad a nahlásit rozsah omezení poskytovaných služeb včetně typu nežádoucího provozu a IP adres, ze kterých pocházel.

4. Sledovat web Úřadu pro případ vydání dalších upozornění, doporučení nebo varování.

ODŮVODNĚNÍ

1. Na základě skutečností zjištěných při výkonu své působnosti, stejně tak jako na základě skutečností, které se Úřad dozvěděl od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí i tuzemských partnerů, dospěl Úřad ke zjištění hrozby v oblasti kybernetické bezpečnosti spojené s možností závažných kybernetických útoků na informační a komunikační systémy v České republice. Tato hrozba je spojená s ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou a působí vůči většímu množství cílů v České republice. Vyšší míru této hrozby lze předpokládat zejména u strategických institucí veřejné správy (významné informační systémy), prvků kritické informační infrastruktury, informačních systémů základních služeb či médií. Ohroženy však mohou být i další tuzemské organizace.

2. Úřad v rámci své činnosti podle § 22 písm. u) zákona o kybernetické bezpečnosti monitoruje a analyzuje hrozby a rizika v oblasti kybernetické bezpečnosti, stejně tak čerpá i z podkladů poskytnutých mu od partnerů. V rámci této činnosti získal Úřad informace o tom, že by útočníci, kteří provedli kybernetické útoky na ukrajinskou infrastrukturu a strategické organizace, mohli zaměřit své útoky i na organizace v České republice.

3. V návaznosti na výše popsané skutečnosti již Úřad zveřejnil dvojici doporučení k zabezpečení tuzemských systémů, a to dne 17. ledna 2022 a dne 28. ledna 2022. Toto varování tak navazuje na dříve vydaná doporučení.

4. Úřad na základě historických dat, výše popsaných vlastních analýz hrozeb a rizik a podkladů získaných od partnerů identifikoval 14 taktik, technik a procedur (TTPs) (dále jen „techniky“) podle platformy MITRE ATT&CK, které se nejčastěji objevovaly v letech 2020-2021. Vyjma toho bylo dodatečně identifikováno 7 technik často využívaných škodlivými aktéry v kyberprostoru. Informace o nich lze využít ke zvýšení odolnosti organizace před kybernetickými útoky provedenými pomocí těchto technik, jak Úřad rovněž v tomto varování doporučuje.

5. Níže uvedené odkazy u jednotlivých technik odkazují na doporučení k mitigaci možných útoků využívajících konkrétní techniku. Úřad doporučuje technikám a odpovídajícím mitigačním procesům věnovat pozornost a zvýšit tak odolnost svých regulovaných informačních a komunikačních systémů.

Technika	Informace
T1059 (Command and Scripting Interpreter)	Zneužití příkazové řádky ke spuštění škodlivého kódu.

T1218 (Signed Binary Proxy Execution)	Zneužití legitimních binárních souborů k proxy spuštění škodlivého kódu.
T1543 (Create or Modify System Process)	Zneužití možnosti vytvořit nebo upravit procesy na úrovni operačního systému k opakovanému spuštění škodlivého kódu.
T1053 (Scheduled Task/Job)	Zneužití plánování úloh k prvotnímu či opakujícímu se spuštění škodlivého kódu.
T1003 (OS Credential Dumping)	Pokus o vypsání přihlašovacích údajů pro získání přístupu k účtu OS a nainstalovanému softwaru.
T1055 (Process Injection)	Vložení škodlivého kódu do legitimního procesu, a to zejména kvůli vyhnutí se odhalení bezpečnostními nástroji.
T1027 (Obfuscated Files or Information)	Snaha ztížit detekci či analýzu škodlivého souboru obfuskací (např. zašifrováním nebo zaheslováním).
T1105 (Ingress Tool Transfer)	Přesunutí nástrojů či dalších souborů útočníkem z externího do kompromitovaného systému.
T1569 (System Services)	Zneužití legitimních systémových služeb nebo démonů ke spuštění škodlivého kódu či programu.
T1036 (Masquerading)	Snaha upravit škodlivý kód a soubory, aby je bezpečnostní nástroje považovaly za legitimní nebo neškodné.
T1486 (Data Encrypted for Impact)	Zašifrování dat na cílovém systému.
T1082 (System Information Discovery)	Pokus o získání detailních informací o OS a hardwaru.
T1497 (Virtualization/Sandbox Evasion)	Prostředky využité pro detekci a vyhnutí se virtualizačnímu či analytickému prostředí.
T1566 (Phishing)	Phishingové e-maily, jež mohou obsahovat škodlivou přílohu v podobě odkazu či přiloženého dokumentu.
T1498 (Network Denial of Service)	Zahlcení sítí, na kterých je závislé poskytování služeb.
T1078 (Valid Accounts)	Zneužití legitimních uživatelských účtů, které útočník napadl (např. znalost či krádež přihlašovacích údajů).
T1190 (Exploit Public-Facing Application)	Zneužití zranitelností aplikací či programů přístupných ze sítě Internet.
T1133 (External Remote Services)	Zneužití vzdálených služeb (např. VPN) k získání prvotního přístupu.
T1595 (Active Scanning)	Aktivní skenování IP rozsahů a potenciálně zranitelných systémů.
T1110 (Brute Force)	Využívání hrubé síly za účelem získání přístupu k účtům, u nichž nejsou známá hesla nebo jsou získány jejich hashe.

T1561 (Disk Wipe)	Zablokování fungování operačního systému pomocí smazání nebo poškození dat.

6. Úřad dále na základě historických dat, výše popsaných vlastních analýz hrozeb a rizik a podkladů získaných od partnerů identifikoval 14 nejčastějších zranitelností, jež jsou využívány ze strany aktérů, kteří provedli útoky na ukrajinskou infrastrukturu a strategické organizace. Ve vztahu k těmto zranitelnostem Úřad doporučuje prověřit přítomnost vyjmenovaných systémů v infrastruktuře, dále pak prověřit jejich aktuálnost a případně tyto systémy aktualizovat tak, aby došlo k odstranění níže uvedených známých zranitelností.

Zranitelnost	Zranitelný systém
CVE-2018-13379	FortiGate VPN
CVE-2019-1653	Cisco Small Business RV320 a RV325
CVE-2019-2725	Oracle WebLogic Server
CVE-2019-7609	Kibana
CVE-2019-9670	Zimbra
CVE-2019-10149	Exim Simple Mail Transfer Protocol
CVE-2019-11510	Pulse Secure
CVE-2019-19781	Citrix
CVE-2020-0688	Microsoft Exchange
CVE-2020-4006	VMware One Access a Identity Manager
CVE-2020-5902	F5 Big-IP
CVE-2020-14882	Oracle WebLogic
CVE-2021-26855	Microsoft Exchange
CVE-2021-44228	Apache Log4j

7. Úřad v reakci na specifickou hrozbu útoků typu distribuovaného odepření služby (Distributed Denial of Service – DDoS) přistoupil také k doporučení konkrétních opatření, která organizacím pomohou ve zmírnění dopadů kybernetických bezpečnostních incidentů v souvislosti s případnými útoky. Opatření doporučená v bodech 3.1. a 3.2. jsou univerzálně použitelná jakoukoli organizací, a to buď preventivně před útokem (3.1.), nebo při probíhajícím útoku (3.2.). Doporučení obsažená v bodech 3.3. a 3.4. jsou pak specificky určena poskytovatelům internetového připojení.

8. Další upozornění, doporučení nebo varování mohou být zveřejňovány na webu Úřadu, a to na následujících odkazech:

- https://www.nukib.cz/cs/infoservis/hrozby/
- https://www.nukib.cz/cs/infoservis/doporuceni/
- https://www.nukib.cz/cs/uredni-deska/

9. Uvedené skutečnosti ve svém souhrnu vedou k důvodné obavě z hrozby realizace závažných kybernetických útoků na významné cíle v České republice, a proto Úřad podle § 12 odst. 1 zákona o kybernetické bezpečnosti vydává toto varování.

10. Pravomoc Úřadu pro vydání tohoto varování je dána ustanovením § 22 písm. b) zákona o kybernetické bezpečnosti, které jej zmocňuje k vydávání opatření. Podle § 11 odst. 2 zákona o kybernetické bezpečnosti patří mezi tato opatření i varování podle § 12 zákona o kybernetické bezpečnosti. Varování vydá Úřad podle § 12 odst. 1 zákona o kybernetické bezpečnosti, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti. V souladu s § 12 odst. 2 zákona o kybernetické bezpečnosti Úřad zveřejní varování na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3 zákona o kybernetické bezpečnosti.

11. Úkolem Úřadu je podle § 22 písm. j) zákona o kybernetické bezpečnosti zajišťovat prevenci v oblasti kybernetické bezpečnosti. Součástí této preventivní činnosti je také poskytování informací o zjištěných hrozbách v oblasti kybernetické bezpečnosti. Pokud však hrozba dosahuje takové intenzity, že informování o ní nelze pokrýt běžnými způsoby preventivní činnosti Úřadu, je v souladu s výše uvedeným Úřad nucen přistoupit k vydání varování podle § 12 zákona o kybernetické bezpečnosti.

12. Úřad upozorňuje, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, v souvislosti s řízením rizik podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti při hodnocení rizik a v plánu zvládání rizik zohlední opatření podle § 11 zákona o kybernetické bezpečnosti. Jedním z těchto opatření je i varování podle § 12 zákona o kybernetické bezpečnosti. Na základě výše uvedeného Úřad považuje hrozbu ve výroku tohoto varování za velmi pravděpodobnou až téměř jistou. Orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, jsou proto povinny tuto hrozbu hodnotit na odpovídající úrovni, tedy na úrovni Kritická. V případě, že povinná osoba využívá v souladu s odst. 5 přílohy č. 2 vyhlášky o kybernetické bezpečnosti jinou metodu pro hodnocení rizik, je nutno tuto hrozbu hodnotit v rámci této metody na srovnatelné úrovni jako by tomu bylo v případě postupu podle § 5 odst. 1 písm. d) vyhlášky o kybernetické bezpečnosti.

Digitálně podepsal:
Ing. Karel Řehka
Národní úřad pro kybernetickou a informační bezpečnost
Dne: 25.02.2022 16:00

NÚKIB

Ing. Karel Řehka
ředitel
Národní úřad pro kybernetickou a informační bezpečnost
elektronicky podepsáno