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

Spisová značka:
350 - 231/2020
Číslo jednací:
2601/2020-NÚKIB-E/350

Brno, 20. května 2020

UKONČENÍ ÚČINNOSTI VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno, vydává v souladu s § 154 a násl. zákona č. 500/2004 Sb., správního řádu, ve znění pozdějších předpisů, toto

ukončení účinnosti varování ze dne 16. dubna 2020, č. j. 2066/2020-NÚKIB-E/350,

varujícího před hrozbou v oblasti kybernetické bezpečnosti spočívající v realizaci rozsáhlé kampaně závažných kybernetických útoků na informační a komunikační systémy v České republice, zejména pak na systémy zdravotnických zařízení.

ODŮVODNĚNÍ

1. Národní úřad pro kybernetickou a informační bezpečnost (dále jen „Úřad“) dospěl 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, k zjištění hrozby v oblasti kybernetické bezpečnosti spojené s kampaní závažných kybernetických útoků na informační a komunikační systémy v České republice, zaměřenou na větší množství cílů v České republice, zejména pak na zdravotnická zařízení. Úřad pozoroval zvýšené množství kybernetických útoků, jejichž dopady by mohly být zvláště nebezpečné v kontextu aktuální situace spojené s výskytem koronaviru (označovaného jako SARS CoV-2) na území České republiky, vyhlášeného nouzového stavu a nezbytnosti zajistit fungování důležitých informačních a komunikačních systémů a jimi podporovaných služeb.
2. Úřad na základě zjištěných skutečností vydal 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“) varování ze dne 16. dubna 2020, č. j. 2066/2020-NÚKIB-E/350 (dále jen „varování“).
3. Obsahem varování bylo varování před hrozbou v oblasti kybernetické bezpečnosti spočívající v realizaci rozsáhlé kampaně závažných kybernetických útoků na informační a komunikační

systémy v České republice, zejména pak na systémy zdravotnických zařízení. Tato kampaň byla způsobilá způsobit závažné dopady na dostupnost, důvěrnost či integritu informací u důležitých informačních a komunikačních systémů. Z informací dostupných Úřadu bylo možno realizaci hrozby očekávat v nejbližších dnech po vydání varování, avšak už v době vydání varování disponoval Úřad indiciemi, že přípravná fáze těchto útoků již probíhala, a to zejména prostřednictvím spear-phishingové kampaně. Úřad tuto hrozbu hodnotil na úrovni Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná.

4. Součástí varování bylo také důrazné doporučení Úřadu k provedení následujících úkonů:

   - mimořádně upozornit uživatele o hrozbách spear-phishingu a připojit výzvu, aby se uživatelé, kteří v posledních dnech otevřeli podezřelé přílohy, obrátili na správce infrastruktury,
   - upozornit uživatele na možnost „maskování“ spustitelných souborů v phishingu, např. „obrazek.png.exe“, „text.txt.exe“, „dokument.pdf.exe“ apod.,
   - pokud je to možné, tak pomocí centrálního nastavení zabránit spouštění aktivního obsahu a maker, zejména v .doc a .docx dokumentech,
   - okamžitě zablokovat vzdálené přístupy do infrastruktury a zablokovat otevřené služby do veřejné sítě, vyjma těch nezbytně nutných (veřejné IP rozsahy lze zkontrolovat v dostupných vyhledávačích zařízení připojených do sítě a zjistit tak i historicky otevřené či zapomenuté porty, nebo služby dostupné z veřejné sítě),
   - okamžitě vytvořit offline zálohy a postupovat v zálohování dle důležitosti dat v organizaci,
   - zkontrolovat konzistenci již vytvořených záloh a okamžitě aktualizovat antivirové řešení v infrastruktuře.

5. Úřad dále pro možné prověření škodlivé činnosti uvedl v obsahu varování hashe škodlivých souborů:

   File type: Win32 EXE
   - MD5 28e1786bd652942f0be31080a9452389
   - SHA-1 44cb931ee16f1f6e3b408035efcd795d8aa0c9be
   - SHA-256 7aa996ff7551362f42ba31d4cd92d255a49735518b3f4dc33283fdd5c5a61b42

   File type: Win32 EXE
   - MD5 e20ee9bbbd1ebe131f973fe3706ca799
   - SHA-1 4e92e5cbe9092f94b4f4951893b5d9ca304d292c
   - SHA-256 f632b6e822d69fb54b41f83a357ff65d8bfc67bc3e304e88bf4d9f0c4aedc224

   File type: Win32 EXE
   - MD5 9dbbfa81fe433b24b3f3b7809be2cc7f
   - SHA-1 b87405ff26a1ab2a03f3803518f306cf906ab47f
   - SHA-256 dfbcce38214fdde0b8c80771cfdec499fc086735c8e7e25293e7292fc7993b4c

   File type: Win32 EXE
   - MD5 7def1c942eea4c2024164cd5b7970ec8
   - SHA-1 b2f4288577bf8f8f06a487b17163d74ebe46ab43
   - SHA-256 c3f11936fe43d62982160a876cc000f906cb34bb589f4e76e54d0a5589b2fdb9

   File type: Win32 EXE
   - MD5 e6ccc960ae38768664e8cf40c74a9902

- SHA-1 d29cbc92744db7dc5bb8b7a8de6e3fa2c75b9dcd
- SHA-256 b780e24e14885c6ab836aae84747aa0d975017f5fc5b7f031d51c7469793eabe

File type: Win32 EXE

- MD5 b1349ca048b6b09f2b8224367fda4950
- SHA-1 44fac7dd4b9b1ccc61af4859c8104dd507e82e2d
- SHA-256 c46c3d2bea1e42b628d6988063d247918f3f8b69b5a1c376028a2a0cadd53986

File type: Win32 EXE

- MD5 0d7dbda706e0048aca27f133d4fc7c51
- SHA-1 1ed9dc8be0f925a5c23e6b516062744931697c78
- SHA-256 ac6b3f9e0848590e1b933182f1b206c00f24c3aa0aa6c62ca57682eff044d079

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. Jak vyplývá z odůvodnění varování, Úřad pozoroval zvýšené množství kybernetických útoků, jejichž dopady by mohly být zvláště nebezpečné v kontextu aktuální situace spojené s výskytem koronaviru (označovaného jako SARS CoV-2) na území České republiky, vyhlášeného nouzového stavu a nezbytnosti zajistit fungování důležitých informačních a komunikačních systémů a jimi podporovaných služeb.

6. S ohledem na charakter a časovou platnost informací, kterými Úřad disponuje v této věci, které vedly k vydání varování, dochází Úřad k závěru, že došlo ke snížení pravděpodobnosti výskytu hrozby, která byla předmětem varování, tedy ke snížení intenzity hrozby, pro níž bylo k vydání varování přistoupeno.

7. **Úřad však upozorňuje, že přestože dochází k ukončení účinnosti varování, jsou hrozby spojené s kybernetickými útoky především na povinné osoby ze zákona o kybernetické bezpečnosti běžnou součástí kybernetického prostoru a nelze očekávat náhlé a dramatické snížení jejich výskytu. Ukončení účinnosti varování nesmí vést k navození dojmu, že tato hrozba již není vůbec relevantní nebo že nemůže nastat. Varováním doporučená opatření a uvedené informace o hash škodlivých souborů (uvedené také výše v bodech 4 a 5) jsou i nadále použitelné. Povinné osoby ze zákona o kybernetické bezpečnosti jsou i nadále samozřejmě povinny provádět řízení rizik a další povinnosti v souladu se zákonem o kybernetické bezpečnosti a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).**

8. Od doby vydání varování po účinnost tohoto ukončení varování byly orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, povinny zohlednit varování podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti. Úřad v rámci varování uvedl, že považuje hrozbu za pravděpodobnou až velmi pravděpodobnou. Orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, byly proto povinny tuto hrozbu po dobu účinnosti varování hodnotit na odpovídající úrovni, tedy na úrovni Vysoká. V případě, že povinná osoba využívá v souladu

s odst. 5 přílohy č. 2 vyhlášky o kybernetické bezpečnosti jinou metodu pro hodnocení rizik, bylo 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. Ukončením účinnosti varování na základě tohoto dokumentu již není nutné varování zohlednit postupem podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti, avšak i nadále by měla být uvedená hrozba zohledněna postupem podle § 5 odst. 1 písm. d) vyhlášky o kybernetické bezpečnosti a hodnocena v souladu se všemi informacemi, které má povinná osoba podle zákona o kybernetické bezpečnosti k dispozici.

Ing. Karel Řehka

Digitálně podepsal Ing. Karel Řehka
Datum: 2020.05.20 13:02:53 +02'00'

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