Osvěta v oblasti kybernetické bezpečnosti

Martin Hájek

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Představení NÚKIB

- vznik v 2017 oddělením od NBÚ,
- gestor kybernetické bezpečnosti a ústřední správní orgán pro oblast kybernetické bezpečnosti (včetně utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany),
- působnost je dána zákonem o kybernetické bezpečnosti a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Činnost NÚKIB

Zdroj: Národní strategie kybernetické bezpečnosti České republiky 2020 – 2025, str.19

Proč to celé děláme?

OSTATNÍ DŮVODY:
- zero day, phishing, backdoor...

LIDSKÁ CHYBA:
- špatná konfigurace systému
- neaktualizované aplikace
- použití defaultních přihlašovacích údajů
- použití slabých hesel
- ztracené notebooky a telefony
- vyzrazení citlivých informací skrze chybné emailové adresy

Vybrané incidenty

Nemocnice Bohunice

Kdy:

- 13. 3. 2020

Co se stalo

- Malware Defray zašifroval data a zničil zálohy
- Vyřazeny klíčové IT systémy a ochromená nemocnice
- Ztracena data z mnohaletého výzkumu z mnoha lékařských oblastí

Doba vyřešení útoku

- Některé části infrastruktury se obnovují i v současné době

Celkové náklady

- Více než 150 milionů korun

Centrum pro regionální rozvoj

Kdy:

- prosinec 2021

Co se stalo

- Ransomware zašifroval data na serverech -> byla nutná obnova
- Díky dobrému zálohován ztracena data jen za cca 14 dní
- Vyřazení interních systémů, nešlo také například komunikovat přes e-mail

Doba vyřešení útoku

- Více než rok

Celkové náklady

- Několik milionů korun

Magistrát města Olomouc

Kdy:

- 6. 4. 2022 zašifrována data -> útočníci požadovali výkupné
- 26. 4. 2022 opakovaný útok doplněný o DDoS útok

Co se stalo

- Ransomware napadl více než polovinu počítačů a notebooků se vzdáleným přístupem
- Ochromení využívaných IT systémů a služeb -> návrat k tužce a papíru
- Ukradená a zašifrována data za 1 den

Doba vyřešení útoku

- Více než 14 dní

Celkové náklady

- Několik milionů korun

Ředitelství silnic a dálnic

Kdy:

- Květen 2022

Co se stalo

- Ransomware Hive RaaS zašifroval data na serverech včetně záloh
- Vyřazeno více jek 1000 serverů včetně aplikací
- Činnost organizované skupiny, která takto napadla přes 1300 společností

Doba vyřešení útoku

- 5 měsíců

Celkové náklady

- Přes 30 milionů korun

Ústav jaderného výzkumu

Kdy:

- Prosinec 2022

Co se stalo

- Ransomware zašifroval data na serverech včetně záloh
- Útok na ekonomický úsek ÚJV Řež → výpadek ekonomického systému → pomalé generování výplat
- ÚJV nezaplatil výkupné → útočníci zveřejnili získaná data na internetu
- Útok neohrozil fungování experimentálních reaktorů

Doba vyřešení útoku

- Několik měsíců

Osvětové aktivity NÚKIB

Osvětový portál (e-learning)

- kurzy ro úředníky napříč celou státní správou
- speciální kurzy pro úředníky územních samosprávních celků
- kurzy pro pedagogy a veřejnost

Speciální osvětové stránky

- Směrnice NIS2
- EU certifikace kybernetické bezpečnosti

Z pozice garanta KB poskytujeme osvětové aktivity zdarma.

Informace o kurzu:

- 4. verze kurzu
- víc než 80 000 uživatelů za rok
- závěrečný test & certifikát o absolvování

Okruhy kurzu:

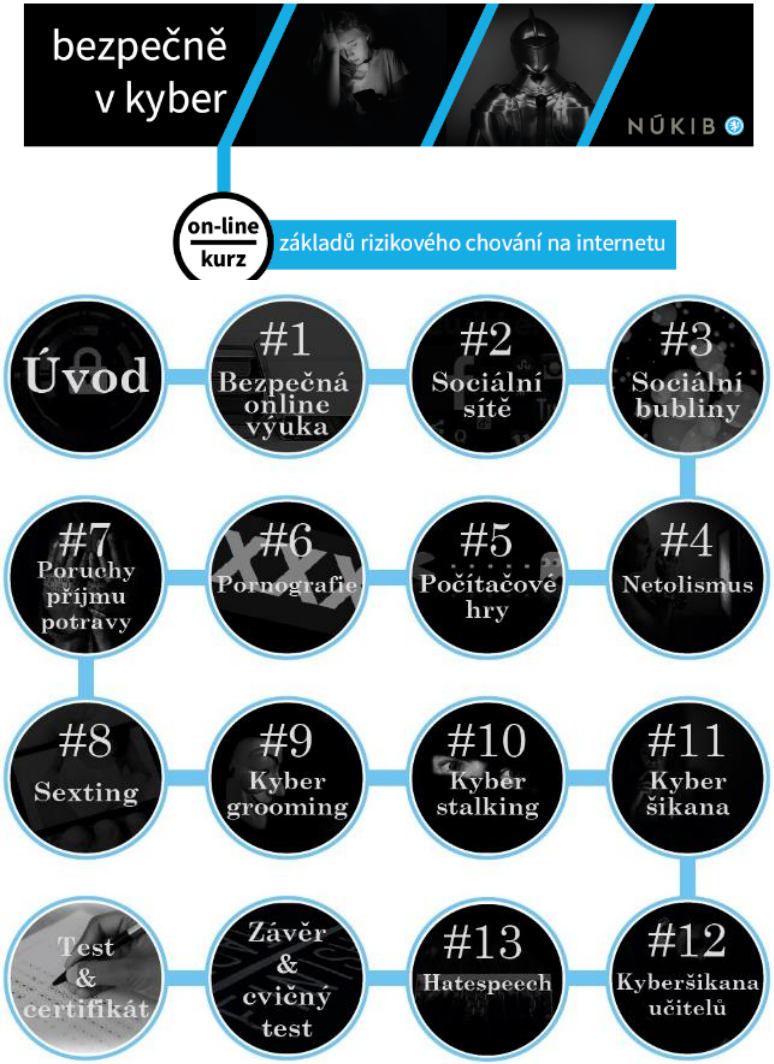
- Hesla a přihlašování
- Uzamykání zařízení
- Sociální inženýrství
- Důvěryhodná komunikace
- Škodlivé soubory
- Ochrana zařízení
- Stahování aplikací
- Připojení a soukromí

Informace o kurzu:

- 3. verze kurzu
- víc než **2000** uživatelů za rok
- závěrečný test & certifikát o absolvování

Okruhy kurzu:

- seznámení s Vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti
- Nejdůležitější paragrafy 3 - 16
- Interaktivní workshop



Informace o kurzu:

- 2. verze kurzu
- víc než **1200** uživatelů za rok

- závěrečný test & certifikát o absolvování

- 2 varianty – základní 9 témat
  – rozšířená 17 témat
- Nová verze plánována na rok 2024

Vítejte na webových stránkách věnovaných blížící se regulaci kybernetické bezpečnosti v České republice – směrnici Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. směrnice NIS2 a změnám, které tato směrnice pro kybernetickou bezpečnost v České republice přinese. Tyto změny nastanou až s účinností nového zákona o kybernetické bezpečnosti (podle plánu v druhé polovině roku 2024).

Směrnice NIS2 přináší mnoho změn v oblasti zajišťování kybernetické bezpečnosti a týká se nejen organizací, které jsou již nyní podle aktuálního zákona o kybernetické bezpečnosti povinny své systémy zabezpečovat, ale i velkého množství organizací, které budou do regulace spadat nově a do dnešního dne žádné povinnosti plnit nemusely.

V kontextu řady změn i zájmu odborné veřejnosti o dané téma NÚKIB spustil tyto webové stránky, jejichž cílem je podávat přehledné a ucelené základní informace o tom, co nová směrnice NIS2 přináší, popsat největší změny stávajících požadavků a způsob, jak budou evropské požadavky promítnuty do národní legislativy.

Vybrali jsme 12 nejzajímavějších a nejdůležitějších témat spojených s budoucí úpravou kybernetické bezpečnosti, které vám chceme představit. Zveřejněné informace budeme průběžně doplňovat. Témata obsahují také návrhy změn v

Obsah stránek:

- Obecné informace o směrnici NIS2
- Koho se nové povinnosti týkají
- Rozdělení povinných organizací
- Povinnost zavádět bezpečnostní opatření
- Incidenty a způsob jejich hlášení
- Registrace organizací a komunikace s NÚKIB
- Způsob kontroly plnění povinností
- Sankce a donucovací prostředky
- Národní a mezinárodní spolupráce
- Další specifika úpravy v České republice
- Jak se připravit na novou právní úpravu
- Finanční aspekty
- **Nyní dostupné také v AJ**

Obsah stránek:

- Akt o kybernetické bezpečnosti
- Role NÚKIB a dalších orgánů
- Schémata EU certifikace
- Vizualizace EU certifikací
- Podpůrné materiály
- Zábavný kvíz
- Přehled akcí
- Vybrané aktuality
- FAQ
- Kontakty

▼ Vybrané aktuality

- 3. 10. 2023 – Návrh EUCC zveřejněn pro poskytnutí zpětné vazby Komisi (T: 31.10.2023)
- 21. 6. 2023 – K dispozici jsou prezentace a video záznam z webináře k EU certifikacím
- 5. 6. 2023 – Zveřejnění programu webináře k EU certifikacím kybernetické bezpečnosti

V červnu 2019 vstoupilo v platnost nařízení Evropského parlamentu a Rady (EU) 2019/881 (dále jen „**akt o kybernetické bezpečnosti**“, „Akt“), které zavádí **evropský rámec pro certifikaci kybernetické bezpečnost produktů, služeb a procesů informačních a komunikačních technologií (ICT)**. Cílem aktu o kybernetické bezpečnosti je zvýšení důvěry v produkty, služby a procesy v oblasti ICT skrze certifikaci jejich bezpečnosti. Tato jednotná evropská **certifikace osvědčí, že produkty, služby a procesy splňují stanovené bezpečnostní cíle** aktu o kybernetické bezpečnosti co do ochrany dostupnosti, autentičnosti, důvěrnosti a integrity.

Hlavním posláním evropského rámce pro certifikaci kybernetické bezpečnosti je **nastolit důvěru** v ICT produkty, služby a procesy, které budou firmy a občané na území EU využívat. A ačkoliv v současné době již některé členské státy pracují s vlastními certifikačními schématy, chybí jednotný a celoevropský systém zaručující stejná pravidla a úroveň zabezpečení pro všechny. To činí potíže především pro výrobce/poskytovatele, kteří pak případně musí podstoupit certifikaci v několika členských státech zvlášť, čímž se zvyšují jejich náklady. A právě na tyto problémy se zaměřuje akt o kybernetické bezpečnosti, jehož cílem je také harmonizace unijního trhu. Evropský rámec pro certifikaci kybernetické bezpečnosti tak **vytváří prostředí pro vznik schémat s konkrétními pravidly a požadavky na ICT produkty, služby a procesy**.

V kontextu zájmu odborné i neodborné veřejnosti o toto téma spouští NÚKIB tyto webové stránky, jejichž cílem je podat **přehledné a ucelené informace** o tom, co akt o kybernetické bezpečnosti

Osvětový portál NÚKIB

https://osveta.nukib.gov.cz/

Děkuji za pozornost