Proč se účastnit Cyber Europe

Věra Mikušová • 04.10.2025

CZ.NIC | SPRÁVCE DOMÉNY CZ

CSIRT.CZ

- CSIRT.CZ je národní CSIRT České republiky, který od 1. 1. 2011 provozuje sdružení CZ.NIC. CSIRT.CZ je historicky druhým nejstarším týmem v Česku (nejstarší je tým CESNET)
- Mezi hlavní činnosti týmu patří:
  - Řešení bezpečnostních incidentů nahlašovaných dle zákona 264/2025 udržování mezinárodní spolupráce
  - Spolupráce s bezpečnostní komunitou v České republice, Evropě i ve světě
  - Poskytování bezpečnostních služeb, jako je řešení incidentů, penetrační testování, CTI
  - Osvětové aktivity
- Naše konstituenci se od 1. 11. 2025 rozšiřuje na všechny subjekty, které zákon označuje jako **subjekty spadající do režimu nižších povinností**
- Od roku 2012 organizujeme cvičení Cyber Europe

CSIRT.CZ

cesnet

ENISA

- Přispívá k politice kybernetické bezpečnosti EU
- Zvyšuje důvěryhodnost produktů, služeb a procesů ICT prostřednictvím certifikačních schémat kybernetické bezpečnosti
- Spolupracuje s členskými státy a orgány EU
- Pomáhá Evropě připravit se na kybernetické výzvy
- Hlavní organizátor a koordinátor cvičení

O cvičení

- Organizováno od roku 2010

Hlavní cílové skupiny:

- Vedení členských států EU
- Národní centra kybernetické bezpečnosti
- Soukromý sektor zajišťující provoz klíčové infrastruktury
- Mezinárodní organizace (EUROPOL, ENISA, CyCLONe, CNW)

O cvičení

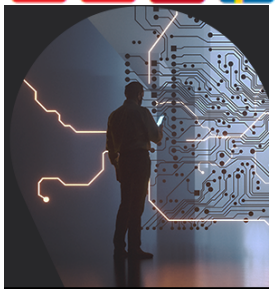
- Cvičení nabízí:
  - Realistické scénáře, které testují reakce na kybernetické hrozby, jako jsou útoky na kritickou infrastrukturu nebo rozsáhlé úniky dat, a poskytují prostředí pro zlepšování reakce na incidenty bez následků skutečné události
  - Platformu pro zvyšování povědomí o kybernetických otázkách mezi týmy a podporu lepšího porozumění v rámci řetězce reakce na kybernetické incidenty
  - Účastníci si mohou rozvíjet individuální i kolektivní dovednosti a schopnosti v oblasti odolnosti

CE 2024 - International Context

Účastnilo se 29 zemí

- všechny členské státy EU (s výjimkou Francie kvůli Olympijským hrám)

  +Norsko, Velká Británie a Švýcarsko



- Každá země má svého národního organizátora (Country Organizer)
- Tento je jmenován NLO (National Liaison Officer) dané země
- Seznam NLO je dostupný na webu ENISA
- Každý národní organizátor nominuje lokální koordinátory (Local Planners) pro cílené sektory a organizace
- Je možné a doporučené zapojit se do procesu již od samého začátku plánování cvičení a pomoci s tvorbou scénářů a „injectů“
- Odborníci na kybernetickou bezpečnost z různých oblastí jsou vítáni. Pokud máte zájem, kontaktujte mě na mail vera.mikusova@nic.cz

2024

Primární cílová skupina

Sekundární cílová skupina

Czechia

- **Účastníci**
  - **16 organizací ze všech cílených sektorů**
  - **více než 120 cvičících**
- **Primární cílová skupina:**
  - DSO (distribuční soustavy): ČEZ, PRE, ČEPRO
  - TSO (přenosová soustava): ČEPS
  - GSO (plynová soustava): ČEPS, RWE, NET4GAS
- **Sekundární cílová skupina:**
  - **DCSP**: ALEF NULA, KPBI, CESNET, MUNI, SPCSS
- **Autority v oblasti kybernetické bezpečnosti**
  - DCSP (poskytovatelé digitálních služeb): ALEF NULA, KPBI, CESNET, MUNI, SPCSS
  - CSA
  - NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
  - Národní agentura pro kybernetickou bezpečnost
  - CyCLONe
  - CNW
  - GŘ HZS – Generální ředitelství Hasičského záchranného sboru
  - IZS a krizové řízení
  - Dvě ministerstva
  - PČR – NCTEK (Národní centrála proti terorismu, extremismu a kybernetické kriminalitě)

Hlavní cíle:

- Otestovat připravenost energetického sektoru na rozsáhlou kybernetickou krizi z právního, operačního a technického hlediska
  - Prověřit připravenost organizací a postupů na zvládání složitých situací souvisejících s řízením kontinuity podnikání
  - Pomoci organizacím lépe se připravit na řízení kybernetických krizí a otestovat jejich interní procesy
  - Zajistit sladění s právními požadavky
  - Prohloubit důvěru mezi aktéry ekosystému kybernetické bezpečnosti napříč Evropou

EVENTS AND INCIDENTS

Event ID	Event	Incident ID	Incident	Incident type	Difficulty	Target Entities	Threat Actor
1	GasOut	02	SCADA modification	Technical	Easy	GSO	APT Group
		14	Mobile Malware	Technical	Medium		
		03	Insider Threat	Technical	Easy		
		01	SIM Swap	Operational	N/A		
2	BlackOut	05	Supply Chain Attack	Technical	Hard	TSO, DSO	APT Group
		15	Network Forensics	Technical	Easy		
		04	Spear Phishing	Technical	Medium		
		06	Wiper Malware	Technical	Medium		
3	OutOfService	08	DDoS	Operational	N/A	DCSP, GSO, TSO, DSO	Cybercriminals
		07	Control Systems	Technical	Medium		
		09	Ransomware	Technical	Medium	DCSP	
		16	Infected Document	Technical	Easy		
4	RepDamage	10	Data Breach	Operational	N/A	NER, GSO, TSO, DSO	Hacktivists
		12	Defacement	Operational	N/A		
		11	Server Compromise	Technical	Hard	NER	
		17	Attack through unsecure WiFi	Technical	Easy		
5	WaterHole	13	Water-holing	Technical	Medium	DCSP, NER, GSO, TSO, DSO	Cybercriminals
		09	Ransomware	Technical	Medium		

Průběh cvičení

9 Událostí

21 Incidentů

178 Injectů

Datacentra – První den

Inject

- **09:35** – DDoS – nedostupný helpdesk organizace
- **10:00** – Smazání složek zaměstnanců (soubory s osobními údaji, bankovními účty a informacemi o sociálním zabezpečení) a podezření na jejich exfiltraci.
- **12:13** – CEO požaduje report o tom co se děje

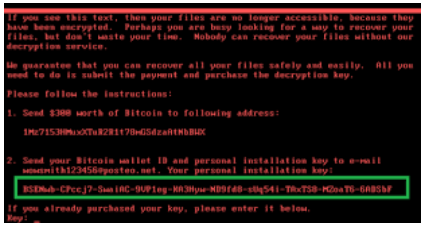
Vybrané reakce cvičících

- 09:57 – ISP dané organizace byli požádáni o blokaci škodlivých IP adres a zákazníci informováni o kybernetickém útoku prostřednictvím odkazu na dočasný web. Zahájení kontroly vnitřní sítě.
- 10:13 – Objevili uniklá data na sociálních sítích
- 13:01 – Report pro CEO odeslán – znehodnocený web, uniklá data, malware v monitorovacím systému a detekce příkazů které vedly k tomu, že útočník získal administrátorský přístup k databázi SQL a exfiltroval další data

Datacentra – První den

Inject

- 13:05 – Klient se dožaduje okamžité informace o tom co se děje
- 13:20 – **23 zařízení v síti bylo zašifrováno**
- 16:20 – další rozzlobení zákazníci se dožadují informací



Vybrané reakce cvičících

- 13:12 – Klientovi byla odeslána rychlá odpověď
- 14:08 – Byl **nalezen dešifrovací nástroj proti ransomwaru a sdílen s komunitou**
- 16:33 – České komunitě byl zaslán podrobný popis způsobu útoku
- 16:34 – Zákazníci dané organizace byli ujištěni, že vše funguje jako obvykle **díky redundantním serverům** a že se incident vyšetřuje

Datacentra – druhý den

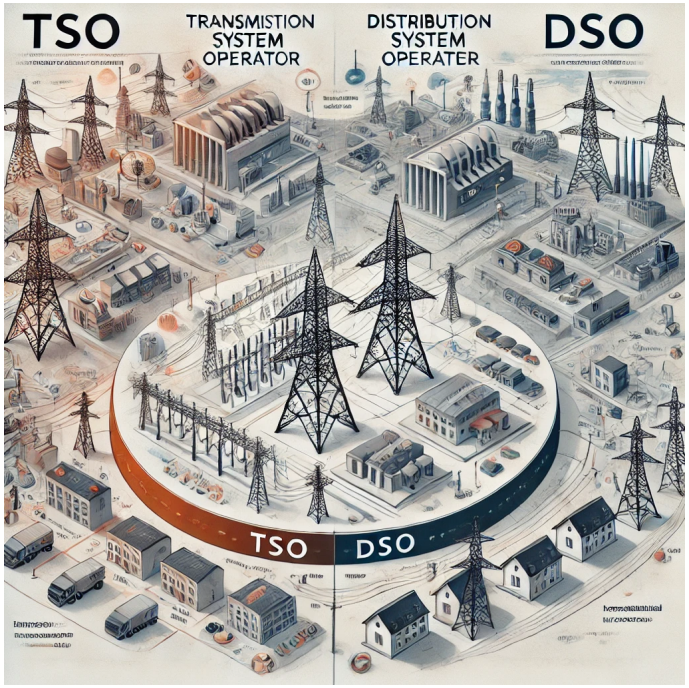
Injects

- **09:05** – Potvrzen únik dat. Ukradené přihlašovací údaje byly již nabídnuty k prodeji
- **09:38** – **Z infikovaných strojů byl získán podezřelý soubor a předán k analýze**
- **13:35** – Vyžádána podrobná zpráva o technických aspektech incidentu (vstupní vektor, rozsah malwaru, odhad ztracených informací), dále o krocích k obnově, opatřeních proti budoucím zranitelnostem a také o provozních, finančních a reputačních dopadech, včetně ohlasu v médiích a na sociálních sítích

Reakce cvičících

- 09:35 – byl proveden vynucený reset hesel pro všechny zaměstnance
- 09:38 – bylo oznámeno, že je připraveno veřejné prohlášení upřesňující, která data na sociálních sítích jsou skutečná a která jsou falešná
- **10:24 – Analýza podezřelých souborů byla správně dokončena za 48 minut a podrobná zpráva byla sdílena s komunitou**
- 16:51 – Sdílena závěrečná zpráva

Podobný akorát o trochu intentzivnější scénář s více injecty pro DSO, TSO and GSO



Vybraný report DSO

Červen 19, 2024

9:11 – Byl zjištěn podezřelý přístup k citlivým dokumentům mimo pracovní dobu (data zaměstnanců)

9:30 – Byl interně vyhlášen **stav zvýšeného kybernetického nebezpečí** a aktivován IT a OT bezpečnostní personál (dle jejich interní metodiky)

9:31 – Nahlášen výskyt nestandardních dat v distribuční síti

9:36 – Došlo k **přerušení fakturačních služeb**

10:03 – Potvrzena **exfiltrace citlivých dat** (údaje zaměstnanců)

10:31 – Ohlášena **porucha dodávky elektřiny**, která zasáhla 15 % distribuční oblasti

10:45 – NÚKIBu nahlášen incident porušení ochrany osobních údajů zaměstnanců

11:54 – SOC požádalo o ověření nestandardního síťového provozu

12:15 – NÚKIBu odeslána zpráva o škodlivém kódu

12:37 – Informace o probíhajícím útoku a výpadcích byly zveřejněny na sociálních sítích a předány ČTK a hlavním médiím

12:50 – Byl **aktivován krizový štáb**

13:09 – Informace o kyberútocích a výpadcích byly zaslány všem příslušným orgánům

13:25 – Byla dokončena analýza dat, která odhalila, že data neobsahovala pravdivé informace

13:35 – Proběhlo ověření IOC a byl identifikován ransomware

14:00–16:45 – **Jednání krizového štábu**

14:05 – **Na základě doporučení NÚKIB** jsme **přešli na ostrovní provoz** pro PREdi (oddělení IT a OT sítí)

14:39 – V distribuční oblasti byl vyhlášen stav nouze a bylo rozhodnuto o posílení havarijního systému Skupiny a zvýšení fyzické bezpečnosti na energetickém dispečinku

15:30 – **Dodavatel poskytl informace o dešifrovacím nástroji**, který byl rozdistribuován mezi specialisty a předán kolegům v rámci jejich pracovní skupiny

16:26 – Byly prověřeny IOC poskytnuté ČEPS s negativním výsledkem

Vybraný report DSO 2

Červen 19, 2024

- 9:11 – Zaslán dotaz ohledně dodávek elektřiny na hranice Prahy
- 9:22 – Uživatelé varováni před phishingovou kampaní
- 9:30–10:24 – Probíhalo vyšetřování IoC
- 10:05 – PR zpráva o aktuální situaci zveřejněna na sociálních sítích
- 10:30 – V řídicím systému identifikován ransomware

11:00 – Výsledky jednání Interního krizového týmu

Malware smazal klíčový systém

Výpadky elektřiny: Přibližně 20 % odběrných míst zažilo výpadky elektřiny, probíhaly práce na obnovení dodávek

Obnova dat: Problémy se zašifrováním zařízení a škodlivým firmwarem byly vyřešeny dešifrováním a obnovou dat ze záloh

Izolační opatření: OT systémy zůstávají oddělené od IT systémů a internetu jako preventivní opatření

Probíhající analýza: Neustálá analýza IoC indikátorů a komunikace s příslušnými orgány, včetně NÚKIB

Vybraný report DSO

Červen 20, 2024

- 11:10 – NÚKIBu odeslána zpráva o ransomwaru v řídicím systému na TR
- 11:16 – Ohlášen výpadek elektřiny u 20 % odběrných míst; přijatá opatření (např. posílení obsluhy TR) postupně snižují rozsah výpadků
- 11:27 – NÚKIBu odeslána zpráva o stavu analýzy a žádost o pomoc
- 11:39 – Vznesen požadavek na svolání Ústředního krizového štábu
- 11:47 – ERÚ poskytnuty informace o aktuálním stavu
- 12:00 – Kontakt ze strany MPO ohledně svolání Ústředního krizového štábu
- 12:45 – Odpověď NÚKIBu ohledně nahrávání offline záloh na TR
- 13:31 – Zveřejněna informace o aktuálním stavu, varování před falešnými zprávami o blackoutech
- 14:17 – Požadavek Ústředního krizového štábu na poskytnutí informací
- 15:00 – Aktuální výpadek elektřiny v Praze klesl na 3 %; připravuje se aktualizovaná zpráva pro média
- 15:11 – Ústřednímu krizovému štábu odeslána vyžádaná zpráva o aktuálním stavu

Postup z pohledu státu 1. den

- Dne 19. června 2024 byly ve členských státech EU, včetně České republiky, hlášeny úniky plynu ze zásobníků a výpadky elektřiny, u nichž se předpokládalo, že byly způsobeny kybernetickými útoky na energetickou infrastrukturu.
- Na základě doporučení Národního úřadu pro kybernetickou a informační bezpečnost přešli někteří provozovatelé energetické infrastruktury na ostrovní provoz dispečerského řídicího systému.

Postup z pohledu státu 1. den

- 13:40 – Ministerstvo průmyslu a obchodu aktivovalo svůj krizový štáb
- 13:45 – Národní úřad pro kybernetickou a informační bezpečnost vyhlásil stav kybernetického nebezpečí podle § 21 odst. 2 zákona č. 181/2014 Sb.
- 14:10 – Státní pokladna Centrum sdílených služeb, s. r. o., omezila geolokaci pro území České republiky
- 14:39 – PREdistribuce, a.s., jako provozovatel distribuční soustavy vyhlásila stav nouze na celém svém licencovaném území (Praha a Roztoky u Prahy) podle zákona č. 458/2000 Sb. (energetický zákon)

Postup z pohledu státu 2. den

- 10:00 – Ministerstvo dopravy hlásí vážné narušení provozu na některých letištích v důsledku probíhajících výpadků elektřiny způsobených kybernetickými útoky na infrastrukturu EU. V tuto chvíli neexistuje žádný náznak, že by tyto výpadky postihly letiště v České republice, a další podrobnosti nejsou k dispozici
- 11:39 – PREdistribuce, a.s. navrhuje svolání Ústředního krizového štábu
- 12:28 – Ministr průmyslu a obchodu navrhuje aktivaci Ústředního krizového štábu vzhledem k bezpečnostní situaci spojené s kybernetickými útoky a výpadky elektřiny v České republice
- Stav kybernetického nebezpečí a stav nouze vyhlášený společností PREdistribuce, a.s. nadále platí na celém jejím licencovaném území (Praha a Roztoky u Prahy)
- 12:55 – Ústřední krizový štáb byl aktivován.

Druhý den cvičení 12:27

*** EXERCISE ** EXERCISE ** EXERCISE ***

MINISTERSTVO PRŮMYSLU A OBCHODU

Ing. Jozef Síkela
ministr

V Praze dne 20. 6. 2024
Č. j.: MPO 206/2024/01300/01000

Vážený pane předsedo vlády a předsedo Bezpečnostní rady státu,

v návaznosti na pokračující výpadky elektrické energie velkého rozsahu v důsledku rozsáhlých kybernetických útoků na infrastrukturu v České republice a v zemích Evropské unie, které vedly k vážnému narušení provozu některých letišť členských zemí, fakultních nemocnic a dalších zařízení, je navrhováno, v souladu s čl. 3 Statutu Ústředního krizového štábu, svolat Ústřední krizový štáb (dále jen „ÚKŠ").

Pokud členové ÚKŠ shledají situaci jako závažnou, bude doporučeno vyhlásit pro část nebo celé území krizový stav podle souvisejících právních předpisů.

Děkuji.

S pozdravem

Ing. Jozef Síkela

Vážený pan
prof. PhDr. Petr Fiala, Ph.D., LL.M.
předseda vlády a předseda Bezpečnostní rady státu
Úřad vlády České republiky
Nábřeží Edvarda Beneše 128/4
11800 Praha 1

Zápis ze zasedání ÚKŠ byl doručen v rámci pár hodin od žádosti o reporty zúčastněných organizací

- Rozhodnutí předsedy vlády dne 20. června 2024 na návrh ministra průmyslu a obchodu projednat vyhlášení stavu kybernetického nebezpečí podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, § 21 odst. 2, v reakci na aktuální rozsáhlé výpadky elektřiny.
  - Účastníci: zástupci všech ministerstev, předseda Správy státních hmotných rezerv, ředitel Národního úřadu pro kybernetickou a informační bezpečnost, předsedkyně Státního úřadu pro jadernou bezpečnost, vedoucí Úřadu vlády České republiky, hlavní hygienik České republiky, prezident Policie České republiky, generální ředitel Hasičského záchranného sboru České republiky, náčelník Generálního štábu Armády České republiky, ředitel Českého hydrometeorologického ústavu, zástupce Asociace krajů České republiky, vedoucí Kanceláře prezidenta republiky, ředitel Sekretariátu Bezpečnostní rady státu, předseda Rady Českého telekomunikačního úřadu

Cílová skupina pro Cyber Europe 2026

Primární cílová skupina:

Doprava

- Námořní :)

  a naštěstí ještě

- **Vlaková**
  - Národní/regionální dopravní úřady
  - Správci železniční infrastruktury
  - Železniční dopravci
  - Poskytovatelé služeb odbavení jízdenek

Sekundární cílová skupina: Subjekty zajišťující podpůrné služby (ISP, datová centra, poskytovatelé digitálních služeb)

Proč se účastnit

Strategické cíle

- Zvýšení povědomí u všech relevantních aktérů
- Posílení důvěry a spolupráce v oblasti kybernetické bezpečnosti v rámci jednotlivých států a státy v rámci EU mezi sebou

Operační cíle

- Otestování řízení kontinuity podnikání
- Prověření procesů řízení incidentů
- Testování odolnosti a nastavení procesů během rozsáhlé krize

Taktické cíle

- Procvičení komunikace mezi organizacemi s rozdílnou úrovní vyspělosti v oblasti kybernetické bezpečnosti (doufejme)
- Identifikace nedostatků v procesech a jejich zlepšení
- Ověření sektorových závislostí a společných postupů při zmírňování dopadů

Více info, žádost o informaci o spuštění registrace, návrh specifického scénáře

vera.mikusova@csirt.cz

Věra Mikušová • 04.10.2025

CZ.NIC | SPRÁVCE DOMÉNY CZ

Moc děkuji za Váš zájem

vera.mikusova@csirt.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ