Financováno Evropskou unií
NextGenerationEU

NÁRODNÍ PLÁN OBNOVY

Školení energetických poradců a manažerů

Tento projekt je financován Evropskou unií v rámci Národního plánu obnovy.

Podpora vzdělávání a zvyšování odborných kompetencí energetických poradců a manažerů poskytujících poradenské služby v oblasti energetiky, klimatu a renovací budov.

Ministerstvo životního prostředí

STÁTNÍ FOND ŽIVOTNÍHO PROSTŘEDÍ ČESKÉ REPUBLIKY

ŠKOLENÍ ENERGETICKÝCH PORADCŮ A MANAŽERŮ

Podpora vzdělávání a zvyšování odborných kompetencí energetických poradců a manažerů poskytujících poradenské služby v oblasti energetiky, klimatu a renovací budov.

Tento projekt je financován Evropskou unií v rámci Národního plánu obnovy.

Financováno Evropskou unií
NextGenerationEU

NÁRODNÍ PLÁN OBNOVY

Ministerstvo životního prostředí

STÁTNÍ FOND ŽIVOTNÍHO PROSTŘEDÍ ČESKÉ REPUBLIKY

Lektor: JUDr. PhDr. Petr Maule, MBA
Školitel: Česká fotovoltaická asociace, Ústav Fotovoltaiky a Elektromobility, z.ú.

JUDr. PhDr. Petr Maule
Ing. Petr Maule, LL.M., MBA
Doc. Ing. Jiří Vaněk, Ph.D.
Ing. Milan Hošek

Kybernetická bezpečnost. Základy bezpečnosti pro energetická zařízení

Financováno Evropskou unií NextGenerationEU
NÁRODNÍ PLÁN OBNOVY
Ministerstvo životního prostředí
STÁTNÍ FOND ŽIVOTNÍHO PROSTŘEDÍ ČESKÉ REPUBLIKY

Tento projekt je financován Evropskou unií v rámci Národního plánu obnovy.

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association
Ústav Fotovoltaiky a Elektromobility
Institute of Photovoltaics and Electromobility

Úvod do kybernetické bezpečnosti

- Kdo jsme?
- Jakou máte představu a zkušenosti o kybernetické bezpečnosti?
- Jaká je souvislost kybernetické bezpečnosti a „obecné“ bezpečnosti?

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do kybernetické bezpečnosti

- NZKB vychází primárně ze Směrnice NIS 2

- SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do kybernetické bezpečnosti

- Kybernetickou bezpečnost by měl řešit každý – ne každý na to ale má, proto je působnost směrnice omezena (typicky tam nespadají malé a mikropodniky)

- Finance?
- Lidské zdroje?
- Čas?
- Důvod?

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Co je kybernetická bezpečnost

- Kybernetická bezpečnost může být definována několika různými způsoby. Obecně jde o celkovou ochranu sítí před kybernetickými útoky a hrozbami, aby byla zachována bezpečnost informací (vlada.cz)

- Kybernetická bezpečnost, známá také jako digitální zabezpečení, se zabývá způsobem, jakým chráníme své digitální informace, zařízení a aktiva. To zahrnuje osobní údaje, účty, soubory, fotky i peníze (microsoft.com)

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Co je kybernetická bezpečnost (utb.cz)

- Kybernetická bezpečnost se zabývá způsobem, jakým chráníme své informace, zařízení a aktiva.
- Zahrnuje činnosti nezbytné k ochraně sítí a informačních systémů, uživatelů těchto systémů a dalších osob dotčených kybernetickými hrozbami.
- Označuje soubor nástrojů, technologií, technik, činností, zásad a procesů, jejichž cílem je prevence, ochrana a související správa zabezpečení počítačových systémů a technologií před kybernetickými útoky

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do kybernetické bezpečnosti

- Vztah Informační a kybernetická bezpečnost?
- Název NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost
- Někdy zaměňováno
- Informace jsou „všechno“ a digitální část

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Přístupová práva v organizaci

- Kdo co vidí a k čemu má přístup?
- Nejedná se pouze o přístupová práva – „přihlášení“
- Posílání e-mailů
- Posílání bankovních plateb
- Sdílené soubory v úložiště – uživatelská práva
- Mají všichni zaměstnanci přístup ke všemu v organizaci?
- Jak je to s přístupem do kanceláří? Máte klíče od vedlejší kanceláře?

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Používání přihlašovacích hesel

- Sdílené počítače?
- Hesla pravidelně měníte?
- Bezpečnost hesel?
- Vícefaktorové ověřování?
- Kdy pracovník pracuje? Co posílá za obsah a odkud? Pokud je to jinak - ODPOJIT

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Kybernetická bezpečnost v odvětvích

- Značná rozdílnost v potravinářství x vodohospodářství x zdravotnictví x energetice

- Vždy jsou odlišné dopady

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Důvody kybernetických útoků

- Peníze?
- Získání informací?
- Politická motivace?
- Náhodné útoky?
- Upozornění na chyby?
- Upozornění na chyby za účelem zisku?
- Způsobit škodu?

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do kybernetické bezpečnosti

- Bonboniéra sekretářce

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do kybernetické bezpečnosti

- Starbucks na Florenci?

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do kybernetické bezpečnosti

- Oslovit studenta na praxi nebo jednatele / majitele společnosti?

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do problematiky

- Ještě před pár lety byla fotovoltaika taková ta „ekologická vsuvka“
- Dnes?
- Základ energetiky – pro domácnosti, výrobní podniky napříč ČR i celé komunity

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do problematiky

- Po roce 2020 se v České republice s fotovoltaikou roztrhl pytel
- ❌ Mnoho instalací bylo doslova „na koleně“
- ❌ Slabé komponenty, špatná konfigurace, nulová bezpečnost
- Fotovoltaika už není jen technika
- Je to IT infrastruktura s energetickým přesahem

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Úvod do problematiky

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

- Kybernetický útok na fotovoltaiku není sci-fi nebo výjimečnost

- Nejde o to, že ti někdo „vypne panely“
  - 👉 Jde o to, že se dostane do ovládacího panelu tvojí elektrárny
  - 👉 A skrze něj do celé infrastruktury
- Zranitelnost není jen v levném střídači
  - 🔓 Může být v cloudové službě
  - 🔓 Nebo v webovém rozhraní
  - 🔓 Nebo v neaktualizovaném firmware řídicí jednotky

Úvod do problematiky

- Útok může být tichý (nejhorší varianta)
- Změna konfigurace, která se projeví až v kritický okamžik
- Když někdo synchronně napadne víc FV systémů, může způsobit výpadek části distribuční sítě

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Zranitelná místa FVS

- Fotovoltaika má spoustu míst, kde může něco selhat, a právě proto je potřeba rizika maximálně eliminovat
- Skutečný problém je mnohem větší - bezpečnost celé energetické soustavy
- Kybernetické útoky na vybrané výrobní zdroje mohou při vhodném načasování vyvolat dominový efekt, který by mohl vést k přetížení elektrizační soustavy
- Prevence kybernetických hrozeb je zásadním předpokladem pro stabilní a bezpečný provoz

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Zranitelná místa FVS

- **Střídače = Achillovka?**
  - Převádějí DC na AC a posílají ho do sítě.
  - Jsou připojené k internetu → tedy i k potenciálním problémům

- **Vzdálený přístup = pohodlí i riziko**
  - Moderní střídače mají software pro online správu
  - Pohodlné ovládání = otevřená vrátka pro útočníky

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Zranitelná místa FVS

- Problém není jeden střídač… ale deset najednou
- Napadení jednoho zařízení svět nezboří
- Ale pokud jich útočník trefí víc naráz, síť to může pocítit
- Výsledek? Krátkodobý chaos, který se musí hasit připojováním a odpojováním jiných zdrojů

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Zranitelná místa FVS

- **Komunikační linky = tichý slabý článek fotovoltaiky**
  - FVE dnes neřídíš šroubovákem, ale přes cloud
  - A když máš cloud, máš i riziko, že ho někdo jedním útokem vypne všem najednou
- **Komunikace uvnitř FVE může být zbraň**
  - Systém si posílá tisíce signálů mezi komponentami
  - Pokud útočník tyto signály pozmění, může jedna část systému poslat druhé úplný nesmysl
  - Výsledek? Špatná rozhodnutí, technické chyby, odpojení od sítě… a v horším scénáři zkrat

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Zranitelná místa FVS

- **FVE je silná jen tak, jak silná je její nejslabší součást**
  - Každý komponent je potenciální vstupní brána
  - Útočníci nikdy nechodí hlavním vchodem — vždy hledají ten nejslabší článek
- **Výběr technologií není formalita**
  - Pokud selže jedna jediná část, otevírá to cestu k ovládnutí celého systému
  - Stačí zranitelný software a útočník se dostane dál, než by měl.

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Zranitelná místa FVS

- **Dodavatel je stejně důležitý jako hardware**

- U softwaru musí hrát prim ověření, reputace a transparentnost

- V energetice nejde jen o funkčnost, ale i o geopolitickou bezpečnost

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- **Vícefaktorové ověření není „nice to have“ Je to základ hygieny**
  - Minimálně 2FA — pro uživatele *i* zařízení
  - Jednofaktorové přístupy jsou dnes jako nechat klíče ve dveřích

- **Certifikáty, tokeny, identity systémy — malá věc, velká obrana**
  - Digitální certifikáty ověří, že přistupuje opravdu ten, kdo má
  - Hardwarové tokeny znemožní jednoduché prolomení účtu
  - Identity systémy drží pořádek v tom, kdo co smí dělat

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- **Proti jednoduchým útokům je to neprůstřelná stěna**
  - Velká část útoků není sofistikovaná — jen spoléhá na laxnost uživatelů

- **Oddělit IT a provozní technologie? Absolutní nutnost**
  - FVE nemá běžet na stejné síti jako firemní notebooky
- **Oddělené role = méně chyb, méně rizik**
  - Kyberbezpečnost musí řídit někdo jiný než běžné firemní IT

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- **Totéž platí i pro domácnosti**
  - FVE rozhraní nemá viset na stejné síti jako televize, telefon a dětský tablet
- **Proč na tom záleží?**
  - Izolované systémy jsou výrazně odolnější vůči útokům
  - Když se útočník dostane do IT, nemá dveře otevřené i k technologii
  - FVE zůstane v klidu běžet, i když někdo klikne na špatný e-mail

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Kyberbezpečnost není jen software. Je to i obyčejná fyzická bezpečnost

- I perfektně zabezpečený systém je k ničemu, když se k němu může dostat kdokoliv

- Rodinný dům? Stačí zvědavé dítě a máte rázem „neplánovanou odstávku“

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Bytové domy = další riziko

- Ovládací prvky FVE bývají ve společných prostorách

- Bez kontroly přístupu je to otevřená pozvánka pro každého, kdo jde kolem

- Řešení? Uzamčené prostory, fyzická izolace komponent, jasně definovaná oprávnění

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Podniky mají stejný problém — jen ve větším měřítku
- Přístup má často půlka firmy: uklízečky, vrátní, údržba, technici „od všeho“
- Většina z nich nemá žádné proškolení pro FVE
- Výsledek? Omylem vypnuté jističe, poškozené komponenty, chaos v provozu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- **Kybernetický útok není otázka „jestli“, ale „kdy“. Proto musí existovat plán**
  - Obranná strategie + plán obnovy provozu = základní povinná výbava
  - Kdo ho nemá, ten jen doufá — a doufání není strategie
- **Papír je váš nejlepší přítel**
  - Plán MUSÍ existovat v tištěné verzi
  - Když systém padne, elektronické dokumenty vám budou tak akorát k ničemu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Zálohování není jen o fotkách z dovolené

- Malé a střední podniky musí mít jasné zálohovací schéma
- Nestačí uživatelská data, ale zálohovat se musí všechno:

– konfigurace FVS
– logy
– provozní data
– postupy pro obnovu provozu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Jednotná rada pro FVE? Bohužel neexistuje

- Rodinný dům, malý podnik, komunální FVS — každý má úplně jiné potřeby

- Proto jsou obecná doporučení omezená

- Každý provozovatel musí mít vlastní, šitou strategii

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- „Kupuj bezpečně“ není jen rada, ale obranná strategie
- Poměr cena/výkon/bezpečnost?
- Jedno z nejúčinnějších opatření? Omezit FVE hardware/software jen na produkty z EU
- Ještě lepší? Pouze od ověřených dodavatelů vedených na státním seznamu (např. NÚKIB)

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- EU dodavatelé = menší riziko státem podporovaných útoků
- EU má přísnější regulace i kontrolu dodavatelských řetězců
- Menší šance, že se do systému dostane škodlivý kód „na státní zakázku“

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Jenže, nepříjemná skutečnost…

- Většina FVE komponent prostě není z EU
- Takže přísné omezení by sektor fotovoltaiky postavilo před obří problém
- Realita? Vyšší bezpečnost × nižší dostupnost. Těžká volba, ale nezbytná debata

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- **Když většina FVE komponent není z EU, musíme hledat jinou cestu**
  - Realita trhu je jasná — většinu věcí kupujeme mimo Evropu
  - Přísný „EU-only“ režim by fotovoltaiku prakticky zastavil
- **Řešení? Sdílení zdrojových kódů se státní autoritou**
  - Výrobci softwaru by museli poskytnout zdrojové kódy institucím jako NÚKIB nebo DIA
  - Nejde o bizarní nápad — jde o způsob, jak ověřit, že systém neobsahuje skrytá rizika

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Výhoda? Reakce na útoky je rychlejší a přesnější
- Stát má přístup ke kódu → lépe rozumí tomu, jak systém funguje
- A když dojde k útoku, umí rychleji najít slabé místo

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Když už nejde získat zdrojáky, musí přijít kompromis
- Ne každý dodavatel pustí stát ke svému kódu — realita trhu je neúprosná
- Podmínka vstupu na trh je zpřístupnění zdrojových kódů nebo?
- Nechat to být? To by byla bezpečnostní sebevražda

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- **Technická dokumentace jako povinnost**
  - Dodavatelé by museli předat kompletní dokumentaci k systému

- Žádné hádanky, žádné schované mechanismy

- Stát musí vědět, jak systém funguje, aby ho uměl chránit

Auditovatelnost je klíč

- Povinnost umožnit audit — pravidelný, nezávislý a bez omezení

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Opatření pro posílení kybernetické bezpečnosti

- Bezpečnostní funkce definované zákonem
- Nouzové odpojení
- Logování
- Diagnostika a ověřování integrity
- Dozorový orgán by mohl v krizové situaci tyto funkce aktivovat

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Legislativní rámec a normy FVS

- **Fotovoltaika je nově „kritická infrastruktura“**
  - Evropská směrnice NIS2 rozšiřuje definici kritické infrastruktury i na energetiku
  - A ano — patří sem i fotovoltaické elektrárny
- **Rodinné domy jako povinné subjekty? Realita budoucnosti**
  - Malé instalace přestávají být „mimo radar“
  - Regulace bude mít dosah až k domácím střídačům
  - Ochrana infrastruktury prostě začíná u každého jednotlivého zdroje

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Legislativní rámec a normy FVS

- **NÚKIB vydává varování, která nelze ignorovat**
  - Rizikové technologie
  - Rizikové subjekty
  - Rizikové praktiky
  - Když úřad zveřejní varování, znamená to, že problém je reálný

- **Praktický dopad?**
  - Provozovatelé musí sledovat aktualizace a řídit se varováními

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Legislativní rámec a normy FVS

- Legislativa pro OZE nestačí. Do hry vstupuje i krizové řízení
- Kromě zákonů zaměřených na obnovitelné zdroje sem spadá i zákon č. 240/2000 Sb.
- Evropská směrnice 2008/114/ES o kritické infrastruktuře
- Fotovoltaika už není jen „energetické zařízení“, ale prvek krizového řízení státu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Legislativní rámec a normy FVS

- **Nejde jen o to, že FVE míří mezi kritickou infrastrukturu**
  - To je důležité — ale není to hlavní důvod
  - Klíčové je, že roste její *váha* v českém energetickém mixu
  - A čím větší podíl výroby… tím větší dopad má jakýkoli výpadek
- **Více fotovoltaiky = více odpovědnosti**
  - Vyšší podíl OZE zvyšuje citlivost přenosové i distribuční soustavy
  - Každé narušení, ať technické nebo kybernetické, má větší efekt než dřív
  - Stabilita sítě už není jen technická otázka — je to otázka bezpečnosti státu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Doporučení

- **Fotovoltaika už není „jen ekologická alternativa“**
  - S rostoucím podílem v energetickém mixu se FVE stávají plnohodnotným pilířem výroby
  - A s tím přichází i povinnosti, které dosud měly jen tradiční elektrárny
- **Digitalizace přinesla pohodlí… ale i nová rizika**
  - FVE jsou dnes téměř vždy připojeny online
  - To znamená vzdálené ovládání, monitoring, aktualizace — a bohužel i nové cesty útoku

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Doporučení

- **Zásadní rozdíl oproti tradiční energetice:**
  - Klasické elektrárny mají řídicí centra fyzicky na místě
  - Data necestují internetem, ale uzavřeným systémem
  - U FVE je přenos dat online — a tím je exponovanější vůči kybernetickým hrozbám

- Čím víc digitalizace, tím víc nutnosti chránit FVE jako kritickou infrastrukturu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Doporučení

- **Jednotný bezpečnostní recept? Bohužel neexistuje.**
  - Fotovoltaiky nejsou „one size fits all“
  - Každá instalace má úplně jiné rizikové profily
- **Bezpečnostní požadavky se liší podle několika faktorů:**
  - velikosti systému
  - způsobu připojení (distribuce vs. přenosová soustava)
  - a hlavně podle toho, zda provozovatel spadá mezi významné nebo kritické subjekty

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Doporučení

- Nelze mít jeden univerzální bezpečnostní model pro všechny FVE
- Co stačí rodinnému domu, je pro velkou instalaci směšně málo
- Co vyžaduje NIS2 pro kritické subjekty, je pro malé provozy ekonomicky i technicky mimo realitu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti

- 264/2025 Sb., o kybernetické bezpečnosti

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 1

- Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby a zranitelnosti v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury
- Téměř zcela transpozičním předpisem směrnice NIS 2
- stanovuje pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti, především Úřadu a pracovišť Národního a Vládního CERT

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 2

- V rámci odstavce 1 jsou definovány následující pojmy – data, informace, aktivum, primární aktivum, podpůrné aktivum a technické aktivum
- Data jsou digitálně i analogově uložené nebo přenášené kvantitativní a kvalitativní hodnoty, fakta nebo statistiky, které jsou shromážděny nebo vytvořeny pro analýzu, zpracování nebo interpretaci. Data mohou existovat ve formě textu, čísel, grafů, obrázků, zvuku, videa či v jiných formátech.

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 2

- Informacemi se rozumí data, která byla zpracována, interpretována nebo organizována tak, aby získala význam a kontext. Informace vznikají z analýzy, zpracování nebo kombinace dat, čímž se zvyšuje jejich užitečnost, relevance nebo srozumitelnost pro konkrétní účel nebo rozhodování. Informace slouží k podpoře pochopení, komunikace, rozhodování a předávání znalostí a jsou základním stavebním kamenem pro tvoření znalostí a inteligence v organizacích i společnosti.

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 2

- Aktivem může být prakticky cokoli relevantního, s čím je potřeba v rámci řízení kybernetické bezpečnosti počítat, resp. to zohledňovat a vést o tom úvahu. Definice aktiva již ve svém obsahu tuto relevanci stanovuje, a to vázaností na zpracování informací a dat v elektronické podobě.
- Technickými aktivy jsou technické nebo programové prostředky nebo vybavení, tvořící informační systémy nebo průmyslové, řídicí a jiná obdobná specifická aktiva tvořící např. průmyslové a řídicí systémy.

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 2

- Kybernetický prostor podle definice v návrhu zákona představuje soubor sítí elektronických komunikací a dalších technologií (včetně internetu, telekomunikací a počítačových systémů), ve kterém dochází ke zpracování dat (včetně ukládání a přenosu).

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 2

- Kybernetický prostor zahrnuje všechny digitální platformy, zařízení a informační systémy, jež jsou využívány pro komunikaci, obchodování a služby. Jedná se přitom i o taková zařízení, informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu.
- Kybernetickou bezpečnostní událostí je událost bez reálného negativního následku, kybernetickým bezpečnostním incidentem je pak samotné narušení bezpečnosti informací s negativním dopadem.

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 3

- Regulovaná služba je stěžejním institutem zákona

- Musí jít o službu, která je určitým způsobem významná pro fungování společnosti a zajištění důležitých společenských nebo ekonomických činností

- Regulovanou službou se pak služba stává na základě rozhodnutí Úřadu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 4

- Podmínky pro registraci regulované služby podle tohoto ustanovení slouží pro potřeby tzv. samoidentifikace

- Samoidentifikace regulovaných služeb probíhá na základě relativně jednoduchých a v zásadě jednoznačných kritérií, neměla by tedy pro povinné subjekty představovat významnější komplikace

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 5

- Toto ustanovení specifikuje další podmínky pro registraci regulované služby rozhodnutím Úřadu

- Principiálně jde o podmínky zohledňující důležitost subjektu pro celou společnost nebo určité odvětví

- Podmínky jsou záměrně formulovány tak, aby k nim Úřad mohl přihlédnout v souvislosti s konkrétním zjištěným skutkovým stavem

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 6

- Pro vlastní splnění ohlašovací povinnosti návrh zákona stanoví objektivní lhůtu 60 dnů ode dne, kdy k splnění podmínek pro registraci regulované služby došlo
- Vzhledem k relativní jednoduchosti podmínek by měly být navrhované lhůty plně dostačující i pro subjekty s komplikovanější organizační strukturou.
- Oproti zákonu o kybernetické bezpečnosti bude většina regulovaných subjektů zařazena do působnosti návrhu zákona na základě samoidentifikace a následného ohlášení regulované služby

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 7

- Podmínka velikosti podniku je založena na doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků
- Výjimky pro počítání velikosti podniku se budou zohledňovat již v rámci posuzování splnění podmínek pro registraci regulované služby subjektem
- Úřad má možnost si posouzení splnění podmínek pro registraci regulované služby a aplikaci výjimek pro počítání velikosti podniku u subjektů zkontrolovat

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 8

- Režim poskytovatele regulované služby - nový institut, který je stěžejní pro stanovení rozsahu povinností uložených poskytovateli regulované služby
- Základ ve směrnici NIS 2, která povinné osoby rozděluje do dvou skupin, tzv. „základních subjektů“ (*essential*) a „důležitých subjektů“ (*important*)
- Zákon stanoví základní pravidla pro rozřazení subjektů do jednotlivých režimů, podrobnosti je potřeba hledat v prováděcím předpisu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 8

- Ve vyšším režimu jsou subjekty, kteří jsou z důvodu své velikosti nebo jiných charakteristik, zejm. počtu uživatelů, geografického rozšíření služby, dopadu na fungování odvětví či jiného poskytovatele regulované služby nebo rizikovosti provozu, významnou měrou ekonomicky, společensky nebo bezpečnostně významní pro Českou republiku

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 8

- V režimu nižších povinností jsou pak především subjekty, které směrnice NIS 2 řadí do kategorie „důležitých subjektů“; tyto subjekty neposkytují žádnou službu, pro kterou by byly zařazeny do vyššího režimu, případně u nich ani na základě žádného dalšího pravidla uvedeného v návrhu zákona nedošlo k jejich převedení do režimu vyšších povinností

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 8

- Poskytovatel regulované služby, který poskytuje více regulovaných služeb a alespoň jedna z nich splňuje podmínky pro zařazení poskytovatele do vyššího režimu, musí ke všem regulovaným službám přistupovat z pohledu režimu vyšších povinností

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 8

- Praktický příklad
- Společnost X po vyhodnocení kritérií v prováděcím právním předpisu zjistí, že se jí týká regulace tří služeb – služby A, služby B a služby C. Prováděcí právní předpis stanovil, že podmínky, které ve vyhlášce společnost X splňuje, odpovídá u služeb A a B režim nižších povinností, ovšem u služby C zařazuje společnost do režimu vyšších povinností. Výše popsané ustanovení v návrhu zákona však stanoví, že společnost X může mít stanoven pouze jeden režim povinností, společnost proto bude postupovat a zavádět povinnosti vůči službám A, B i C tak, jako by byly všechny v režimu vyšších povinností již podle prováděcího právního předpisu. Pokud by společnost X službu C neposkytovala, poskytování služeb A a B by vedlo ke stanovení jejího režimu na režim nižších povinností.

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 9

- Na ohlášení změny regulované služby je tedy možné pohlížet tak, jako by poskytovatel poskytoval pouze jednu službu, u které ke změně došlo
- V případě, kdy jeden poskytovatel poskytuje více regulovaných služeb, z nichž například služba A je důvodem, proč je tento poskytovatel v režimu vyšších povinností, tak zároveň platí, že musí hlásit i změny regulované služby B, pokud by tato změna znamenala, že v případě poskytování pouze této služby, by její poskytovatel byl přeřazen z režimu nižších povinností do režimu vyšších povinností (a naopak)

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 10

- Řízení o zrušení registrace regulované služby může být zahájeno buď na žádost poskytovatele regulované služby, nebo Úřadem z moci úřední, pokud se Úřad ze své činnosti dozví, že regulovaná služba již podmínky pro registraci regulované služby nesplňuje
- K hlášení údajů částečně dochází již při prvotním ohlášení regulované služby
- K hlášení ostatních údajů musí dojít nejpozději do 30 dnů od doručení rozhodnutí o registraci regulované služby do evidence regulovaných služeb

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - §§ 11 - 23

- Dobře strukturovaný zákon, kdy to co hledat je v názvu §
- § 11 - Hlášení údajů
- § 12 - Stanovení rozsahu řízení kybernetické bezpečnosti
- § 13 - Bezpečnostní opatření
- § 14 - Seznam bezpečnostních opatření
- § 15 - Hlášení kybernetických bezpečnostních incidentů
- § 16 - Postup hlášení kybernetických bezpečnostních incidentů

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - §§ 11 - 23

- § 17 - Zvládání kybernetických bezpečnostních incidentů
- § 18 - Zvláštní ustanovení o povinnostech poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb
- § 19 - Informační povinnost
- § 20 – Protiopatření
- § 21 – Výstraha
- § 22 – Varování
- § 23 - Reaktivní protiopatření

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 11 - Hlášení údajů

- Tato povinnost spolu s ohlášením regulované služby v zásadě odpovídá hlášení kontaktních údajů podle § 16
- Hlášení relevantních údajů přitom bude probíhat prostřednictvím standardizovaných formulářových podání vyplněných pomocí Portálu Úřadu
- Důležitost dostupnosti reprezentanta poskytovatele regulované služby, nemělo by tak docházet k situacím, kdy budou pověřené kontaktní osoby nedostupné a bez jakéhokoli zástupu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 11 - Hlášení údajů

- Nedostupnost kontaktních osob je třeba považovat za nesplnění povinnosti

- Dostatečnou zastupitelnost, tedy odpovídající počet kontaktních osob, nelze exaktně určit

- V praxi se však doporučuje u menších organizací uvést minimálně dvě nebo tři kontaktní osoby

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 12 - Stanovení rozsahu řízení kybernetické bezpečnosti

- Základem řízení kybernetické bezpečnosti poskytovatelem regulované služby je správné stanovení jeho rozsahu pomocí správného určení aktiv
- Cílem tohoto ustanovení je zpřesnit a v praxi zjednodušit poskytovateli regulované služby stanovení rozsahu a zároveň dodržet požadavky směrnice NIS 2
- Za řádné stanovení rozsahu řízení kybernetické bezpečnosti je považován okamžik, kdy je jeho stanovení prokazatelně evidováno, resp. přezkoumáno a aktualizováno

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 13 - Bezpečnostní opatření

- Cílem bezpečnostních opatření (organizačního a technického typu) je zajistit řádné poskytování regulované služby a kybernetické bezpečnosti aktiv

- Poskytovatelé regulovaných služeb provedou zhodnocení bezpečnostních charakteristik jimi poskytovaných regulovaných služeb a na tomto základě si vytvoří a zdokumentují vlastní systém bezpečnostních opatření sestávajících z opatření organizačních a technických

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 13 - Bezpečnostní opatření

- Bezpečnostní opatření se zavádí v míře a způsobem nezbytným pro zajištění kybernetické bezpečnosti regulované služby a souvisejících aktiv

- Poskytovatel regulované služby tedy nemusí zavádět všechna bezpečnostní opatření v plném rozsahu, ale na základě své vlastní analýzy rozhodne, která bezpečnostní opatření a v jakém rozsahu jsou pro jeho organizaci relevantní

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 13 - Bezpečnostní opatření

- Poskytovatelé regulované služby jsou podle návrhu zákona povinni činit bezpečnostní požadavky součástí smluv, které s dodavateli uzavírají
- Povinnost zanášet bezpečnostní požadavky do smluv s dodavateli se vztahuje nejen na nově uzavírané smlouvy, ale i na ty již uzavřené

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 14 - Seznam bezpečnostních opatření

- Vzhledem k rozdílným nárokům na poskytovatele regulované služby v režimu vyšších povinností a poskytovatele regulované služby v režimu nižších povinností je i seznam bezpečnostních opatření rozdělen podle režimů a odráží rozdílnost požadavků pro tyto režimy
- Pro poskytovatele regulované služby v režimu nižších povinností je pak stanovena užší množina povinností, představující základní bezpečnostní opatření (organizačního a technického typu).

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 14 - Seznam bezpečnostních opatření

- Tato bezpečnostní opatření by měla být v dnešní době naprostým základem běžného provozu ICT:
- systém zajišťování minimální kybernetické bezpečnosti
- požadavky na vrcholné vedení
- řízení aktiv
- řízení rizik
- bezpečnost lidských zdrojů
- řízení kontinuity činností
- řízení přístupu

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 14 - Seznam bezpečnostních opatření

- řízení identit a jejich oprávnění
- detekce a zaznamenávání kybernetických bezpečnostních událostí
- řešení kybernetických bezpečnostních incidentů,
- bezpečnost komunikačních sítí
- aplikační bezpečnost
- kryptografické algoritmy

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 15 - Hlášení kybernetických bezpečnostních incidentů

- Poskytovatelé regulovaných služeb mají povinnost hlásit incidenty s původem v kybernetickém prostoru, u nichž nelze vyloučit úmyslné zavinění
- Úmyslnost zavinění incidentu se vždy posuzuje ve vztahu k útočníkovi
- Pokud tedy např. zaměstnanec neúmyslně stáhne přílohu e-mailu obsahující malware, který následně způsobí narušení bezpečnosti aktiv, jedná se o incident zaviněný úmyslně ze strany útočníka, který chtěl docílit způsobení škody

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 15 - Hlášení kybernetických bezpečnostních incidentů

- V případě jakýchkoliv pochybností např. ohledně posouzení vzniku incidentu nebo určení hranice mezi událostí a incidentem vždy platí, že je lepší incident (byť domnělý) nahlásit, a to i s ohledem na možnost dobrovolného hlášení událostí a incidentů

- Možnost dobrovolného hlášení incidentů, událostí a hrozeb v oblasti kybernetické bezpečnosti i pro subjekty, které nespadají do působnosti návrhu zákona

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 15 - Hlášení kybernetických bezpečnostních incidentů

- Úřad dobrovolná hlášení přijímá za účelem umožnění společného využití individuálních znalostí a praktických zkušeností subjektů i mimo působnost zákona na strategické, taktické a operativní úrovni

- Cílem je zlepšit schopnosti předcházet incidentům, odhalovat je, reagovat na ně, zotavovat se z nich nebo zmírňovat jejich dopad

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 16 - Postup hlášení kybernetických bezpečnostních incidentů

- Poskytovatelé regulovaných služeb v obou režimech hlásí kybernetické bezpečnostní incidenty bez zbytečného odkladu, nejpozději do 24 hodin od detekce incidentu
- Významnost dopadu na kybernetický prostor státu hodnotí Úřad na základě informací obsažených v prvotním hlášení o dopadu na regulovanou službu a dalších relevantních informací
- Úřad pak v rámci hodnocení zohledňuje např. úroveň útočníka, vektor útoku, aktuální hrozby a incidenty u subjektů ve stejném nebo příbuzném odvětví, známé zranitelnosti v používaných informačních systémech

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 17 - Zvládání kybernetických bezpečnostních incidentů

- Úřad poskytuje bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení poskytovatelům regulovaných služeb své vyjádření k nahlášenému kybernetickému bezpečnostnímu incidentu
- Vyžadována součinnost za účelem odstranění možných překážek zabraňujících zvládání těchto incidentů - zpřístupnění prostor, ve kterých se nachází napadená infrastruktura
- Součinnost bude vyžadována pouze v nezbytných a důvodných případech

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 17 - Zvládání kybernetických bezpečnostních incidentů

- Požadovanou součinnost je možné Úřadu odepřít, bránila-li by tomu zákonná nebo státem uznaná povinnost mlčenlivosti nebo plnění jiné zákonné povinnosti

- Za zákonnou nebo státem uznanou povinnost mlčenlivosti nelze považovat smluvně sjednanou povinnost mlčenlivosti

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 17 - Zvládání kybernetických bezpečnostních incidentů

- Zachovávání obchodního tajemství neodpovídá pojmu „plnění jiné zákonné povinnosti“, neboť povinnost zachovávat obchodní tajemství není výslovně upravena na úrovni zákona a typicky bývá upravována smluvními ustanoveními či např. vnitřními předpisy

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - § 18

- § 18 - Zvláštní ustanovení o povinnostech poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 19 - Informační povinnost

- Poskytovatel regulované služby sám posoudí potřebu oznámit kybernetický bezpečnostní incident s významným dopadem
- Ohlašování hrozeb má zásadní význam pro předcházení tomu, aby tyto hrozby přerostly do kybernetických bezpečnostních incidentů
- Proaktivní přístup k hrozbám je zásadní složkou opatření k řízení kybernetických bezpečnostních rizik

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 20 – Protiopatření

- Obecně je možné říci, že protiopatřeními jsou úkony Úřadu, jichž je potřeba k ochraně aktiv před hrozbou nebo před zneužitím zranitelností v oblasti kybernetické bezpečnosti

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 21 – Výstraha

- Výstraha jako institut vychází z požadavků směrnice NIS 2
- Nástroj informování veřejnosti použitelný pouze v případě, že zveřejnění takové informace je nezbytné pro zajištění ochrany bezpečnosti České republiky, vnitřního pořádku, života a zdraví nebo majetkové hodnoty
- Benefit zveřejnění informace by měl převýšit možné negativní dopady jejího zveřejnění

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

§ 22 – Varování

- Účelem varování podle tohoto ustanovení je oficiální publikace informací o bezpečnostní hrozbě či zranitelnosti, tj. preventivní informování poskytovatelů regulované služby
- Vydání varování je vázáno na závažnou hrozbu či zranitelnost v oblasti kybernetické bezpečnosti
- Využíváno především v situacích, kdy bude hrozba společná pro širší okruh osob a její realizace by měla závažné dopady přesahující zájmy jedné regulované osoby

§ 23 - Reaktivní protiopatření

- Účelem reaktivního protiopatření je okamžitá reakce na výskyt kybernetického bezpečnostního incidentu
- Obsahem tohoto druhu protiopatření jsou povinnosti provést konkrétní úkony nutné k odvrácení kybernetického bezpečnostního incidentu nebo ke zmírnění jeho následků
- Jakákoli časová prodleva, byť v řádu hodin, může znamenat exponenciální rozvoj kybernetického bezpečnostního incidentu a násobení jeho škodlivého účinku

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

Nový zákon o kybernetické bezpečnosti - §§24 a násl.

- § 24 - Speciální úprava předání informací a dat od dodavatele
- §§ 25 a 26 - Strategicky významná služba
- §§ 27 až 32 - Mechanismus prověřování bezpečnosti dodavatelského řetězce
- § 33 - Zajištění dostupnosti strategicky významné služby
- §§ 34 a 35 - Osoba poskytující služby registrace doménových jmen a osoba spravující a provozující registr domény nejvyšší úrovně
- §§ 36 až 41 - Další nástroje zajišťování kybernetické bezpečnosti

ČFA
Česká Fotovoltaická Asociace
Czech Photovoltaic Association

JUDr. PhDr. Petr Maule, MBA

maule.petr@gmail.com
tel: 775 002 229

Vystudoval Západočeskou univerzitu v Plzni a CEVRO Univerzitu v Praze. Od roku 2013 se věnuje poskytováním právních služeb. Věnuje se také ústavnímu právu. V minulosti působil ve skupině PKF APOGEO a také jako místopředseda Legislativní rady v Asociaci malých a středních podniků ČR.

V současnosti působí jako právník ČFA UFAE. Od roku 2020 zde působí jako lektor pro právní a technickoprávní předměty, v rámci kurzů Fotovoltaiky, Elektromobility, Komunitní energetiky nebo profesního studia MSc.