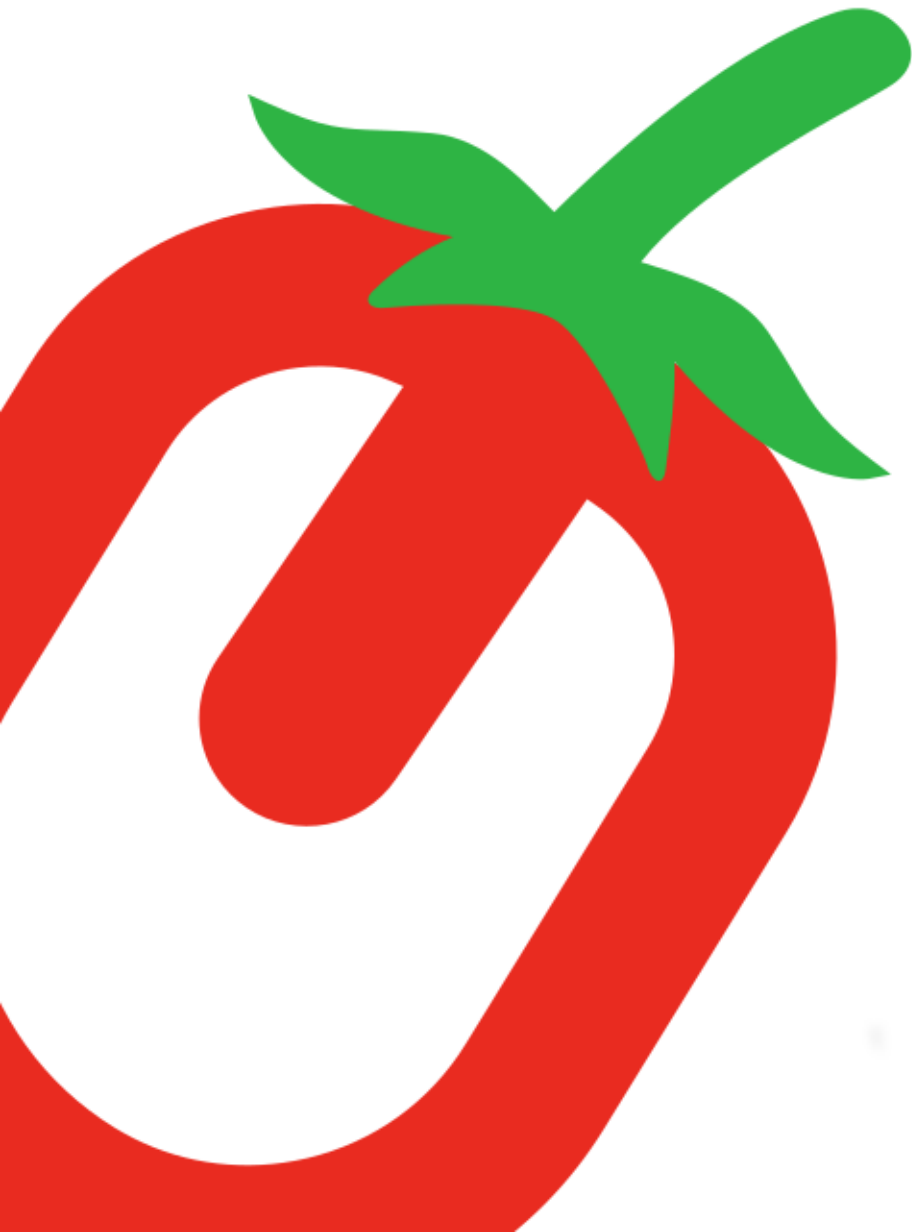


NIS2 v kontextu bezpečnosti informací

Ostrava

Petr Šubert

08.11.2023



Chcete-li něco efektivně vysvětlit, je klíčové přizpůsobit komunikaci úrovni porozumění a předchozím znalostem posluchače.

Co aktuálně hýbe světem bezpečnosti **informací**

- Nová norma ISO 27001:2022
- Příprava nového zákona o kybernetické bezpečnosti alias NIS2
- Válečné konflikty
- Hackeři různého typu
- Nepoučitelní manažeři a uživatelé různého typu,
- Obchodníci s kybernetickou bezpečností různého typu
- Příprava Cybersecurity Frameworku (NIST) verze 2.0

Co je to informace?

- Je abstraktní entita.
- Snižuje nejistotu (neurčitost znalosti) člověka o dění v jisté části reálného světa.
- Jejím zdrojem je poznání.
- Lze jí ukládat, transportovat a zpracovávat k získání jiné, pro daný účel požadované informace.
- Vždy je vázána na jazyk, který s ní umožňuje provádět výše uvedené operace.
- Člověku umožňuje jiný pohled na dění v reálném světě (vidění jiných jevů a souvislostí), než umožňuje působení interakcí, jež je klíčové pro přírodní i technické vědy.

(Wikipedie)



Co je to informace - zkráceně

**Informace je ta věc, na základě,
které děláme svá rozhodnutí.**

**Informace je aktivum, dokonce
primární - je na to zákon :-)**



Co potřebujeme pro správně rozhodnutí?

- **Integrita (Integrity)** – znamená, že je správná a že víme co znamená
- **Dostupnost (Availability)** – znamená, že informace jsou k dispozici, když je potřebujeme
- **Důvěrnost (Confidentiality)** – znamená, že k informacím mají přístup pouze to co jí mají mít

Používá se pořadí C-I-A, ale já to mám rád takto, k čemu je mi dostupnost a důvěrnost u informace, která je nesmyslná?

**Pokud někdo útočí na informace,
tak se vždy snaží kompromitovat
alespoň jednu z těchto vlastností.**

Nosiče informací

1. Papírové dokumenty
2. Lidský mozek (znalosti a informace v hlavách lidí)
3. Mluvené slovo (např. schůzky, telefonní hovory)
4. USB disky, CD/DVD disky, externí pevné disky a jiné přenosné nosiče
5. Mobilní telefony a tablety
6. Fyzické servery a počítače (nejen data na nich, ale také hardware)
7. Vizuální a zvukové signály (např. informace zobrazené na monitorech nebo reproduktorech v otevřených kancelářích)
8. Aplikace, databáze (mohou být v cloudu nebo na fyzických serverech)
9. E-mail, různé komunikační platformy
10. Řídící systémy (CNC, SCADA, zdravotnické přístroje, měřící systémy, IoT apod.)
11. ...

Tři úhly pohledu

Pohled G – Governance (řízení/správa)

- Zainteresované strany a jejich potřeby (kdo co chce)
- Definice cílů (co s tím budeme dělat)
- Definice IT strategie (jak na to půjdeme a co použijeme)
- Zodpovědnost a odpovědné osoby (kdo za co ručí)
- Rozhodovací struktury (a kdo o tom rozhoduje)
- ... (viz. COBIT)

Pohled R – Risk (riziko)

- Rizikový profil (co jim hrozí)
- Expozice organizace (jak moc jim to hrozí)
- Appetit rizika (úroveň rizika, kterou jsou ochotni akceptovat)
- Strategie řízení rizik (co s tím budou dělat)

Pohled C – Compliance (dodržování)

- Globální a regionální regulační požadavky (zákony a standardy)
- Požadavky třetích stran (smluvní ujednání)
- Interní směrnice (doporučení – napište si jen to co opravdu potřebujete)
- Etické a společenské normy (co třeba udržitelnost?)
- Ochrana obchodního tajemství



Jak na to šel stát (EU)

- Stát resp. EU se rozhodl(a) řešit svou **SPRÁVU**
- V rámci toho si řekl(a), které věci/služby potřebuje pro základní fungování (další slide)
- Vytvořil(a) zákon (směrnici)
- Tím přidal povinnosti poskytovatelům těchto služeb do **SOULADU**
- A současně je vystavil(a) **RIZIKU**, že jim tam občas přistane nějaká ta pokutička

- ... ti se z toho osypávají, šílí apod.



SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential“.

ENERGETIKA



Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.



Subjekty poskytující službu dálkového vytápění nebo chlazení.



Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.



Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.



Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA



Komerční leteckí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.



Provozovatel dráhy celostátní nebo regionální anebo veřejně přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.



Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.



Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ



Sektor bankovníctví je regulován nařízením DORA.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT



Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

INFRASTRUKTURA FIN. TRHŮ



Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ



Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA



Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA



Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA



Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů.

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB



Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA



Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR



V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik“ a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik“ a „střední podnik“ dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important“ (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY



Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ



Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL



Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ



Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA



Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB



Poskytovatelé on-line tržišť, internetových vyhledávačů, platform služeb sociálních sítí.

VÝZKUM



Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

Jaké povinnosti NIS2 ukládá

- **Vyšší** – systém řízení bezpečnosti informací
- **Nižší** – zajišťování **minimální úrovně kybernetické bezpečnosti**

- **Ale pozor** – jen na vybrané (regulované) služby

NIS2 není komplexní systém na řízení bezpečnosti informací, ale jen požadavek regulátora.

Skutečnost je trochu horší.

NIS2 je docela dobrý rámec pro **určení základních požadavků na zajištění bezpečnosti informací.**



Chcete řešit bezpečnost informací nebo jen vyřešit NIS2?

Co teď s tím?

- Vysvětlit to vedení
- Sestavit a proškolit řešitelský tým
- **Stanovit rozsah implementace**
- Pustit se do toho

- ... opravdu není na co čekat

08.11.2023



Jak se mění framework KB

NIST CBF 1.1



NIST CBF 2.0



Govern (GV)

Organizational Context



Pozdrav z fronty

Výroční zpráva vojenského zpravodajství přišla s poměrně zajímavou informací - v Rusko – Ukrajinském konfliktu nebyly ve větší míře použity sofistikované útoky, ale masivně levné útoky typu wiper. Nikdo nikoho nevydíral, jen ničil.

A prý je slušná pravděpodobnost, že se to dostane sem k nám.

Zálohovat, zálohovat, zálohovat...





Díky moc

E: petr@pribehrajske.cz

M: +420 703 404 004

IT PRO TY, CO UMÍ
HLAVNĚ JINÉ VĚCI

Myslím, že na světě je spousta lidí, kteří dovedou úžasné věci, ale my jim nučíme svou představu IT světa, ve kterém se necítí zrovna komfortně.