

D A T A
S Y S

Jak se chránit před kybernetickými hrozbami?

RADIM PRACUCH

+420 724 065 027 | pracuch@datasys.cz

Nový pohled

Kybernetická bezpečnost potřebuje Vaši nepřetržitou pozornost


Doba si vyžaduje pokročilejší ochranu ICT aktiv

- Zvyšuje se sofistikovanost útoků a počet útočníků.
- Roste počet zranitelných míst – více aplikací, IoT, cloudů, home office ...
- Roste množství legislativních požadavků (**nový zákon o kybernetické bezpečnosti**), regulací (DORA, TISAX, NIS2), ISO27k, NIST Cybersecurity Framework, CVS aj.

TIP pro vás

Používejte zdravý selský rozum

- Začněte pečlivým určením toho, co potřebujete chránit.
- Definujte smysluplnou granularitu aktiv.
- Využijte známý efekt 80/20 a usilujte o pevný řetěz.
- Neřešte za každou cenu vše interními týmy.
- Hledejte kreativní řešení s vysokou přidanou hodnotou a rychlým přínosem.

The image shows a close-up of the European Union flag, featuring a blue field with twelve gold stars arranged in a circle. The flag is waving against a background of a blue sky with white clouds. A thick teal curved line separates the image from the text on the right.

Tento pohled je
užitečný i pro subjekty,
které nepodléhají
regulaci NIS2.

- **Aktiva, dopad** – co chráníme a proč
- **Opatření** – co potřebujeme dělat
- **Politiky** – jak to budeme dělat
- **Lidé** – s kým to budeme dělat
- **Povinnosti** – co musíme splnit

Oproti předchozí legislativě dochází
ke **kvalitativnímu posunu:**

Místo ochrany kritické infrastruktury
a významných informačních systémů se **více zaměří na
dostupnost tzv. regulovaných služeb**
a především praktické hledisko:

**nutí nás k zamyšlení jaké dopady může mít kybernetický
incident na Váš business či poslání.**



Děje se to běžně...

- Vedení podceňuje vlastní lidi a jejich doporučení.
- Mají ale jasnou představu co nechtějí – ztráta dat, narušení chodu, pokuty...
- Mají důvěru v to, že se o jejich bezpečnost někdo nějak postará, ale vůbec tomu nerozumí.
- IT si nerozumí s bezpečáky nebo jejich spolupráce vážne.

**NEUSILUJTE O DOKONALOST – JE DRAHÁ A TRVÁ DLOUHO.
VĚNUJETE TOMU 20 % ÚSILÍ A DOSÁHNETE 80% POKROKU.**

Znáte své slabiny a rizika?

Pro ochranu je důležité problémy vidět a znát je

MIKRO SLUŽBY

- Stanovení rozsahu – analýza stavu KB – GAP analýza
- Správa zranitelností
- Školení vedení a zaměstnanců
- Phishingové testy
- Odolnost vůči ransomware
- Testování výkonnosti a bezpečnosti sítě
- Aktivní ochrana DNS provozu
- Konfigurační audit / rizika
- Zhodnocení bezpečnostní reputace
- Posouzení postupů zálohování a obnovy.

Poskytneme vám nástroje nebo službu, díky které jasně uvidíte, jak na tom jste, a zkrátíte i čas nápravných opatření.



Chybí vám lidé?

Kybernetická bezpečnost vyžaduje nepřetržitou pozornost!
Doplňte svoje lidi zkušenými profesionály se zkušenostmi z jiných projektů.

Chybí vám specialisté na kybernetickou bezpečnost?
Nemáte zkušenosti s identifikací a řešením incidentů?
Nemáte dostatek lidí na zajištění bezpečnosti nebo provozu v režimu 24x7x36?

Zaveďte bezpečnostní dohled = SOC!

Proč SOC službu?

Pokud u vás přestává být zvládnutelné a efektivní udržovat si vlastní týmy zaměstnanců s velmi specializovanými dovednostmi v oblasti sítí a kyberbezpečnosti.

Nabízíme unikátní koncept pružného aktivního bezpečnostního centra eSOC, který se vám přizpůsobí.

Je to rychlá cesta, jak dosáhnout ochrany informací, dat a služeb!



ELISA SECURITY MANAGER

Centrální provozní a bezpečnostní monitoring



**DETEKCE
BEZPEČNOSTNÍCH
RIZIK**



**NÍZKÉ
NÁKLADY**



**PŘEHLEDNÉ UŽIVATELSKÉ
PROSTŘEDÍ**

Robustní nástroj pro sběr a analýzu bezpečnostních událostí.

Získáte chytřejší konzoli bezpečnostního dohledu.

**Odhalte a odstraňte problémy v infrastruktuře dříve,
než negativně ovlivní chod vaší organizace.**

Náš tip: Využijte našeho bezpečnostního specialistu!

Jedno řešení mnoho výhod

- Viditelnost a rychlý rozbor problému.
- Výpočet míry rizika pro každou událost.
- Soulad se zákony a normami.
- Interaktivní rozhraní, vč. vizuálního editoru pravidel.
- Podpora kontextových korelací.
- Integrace s OpenVAS, GSM, Flowmon, Greycortex aj.
- Integrace s Microsoft Cloud (Azure, Office 365)
- Zabudovaný „Change auditor“.
- Centrální správa agentů.
- Distribuovaný sběr logů.

Nevíte co chránit, kde začít?

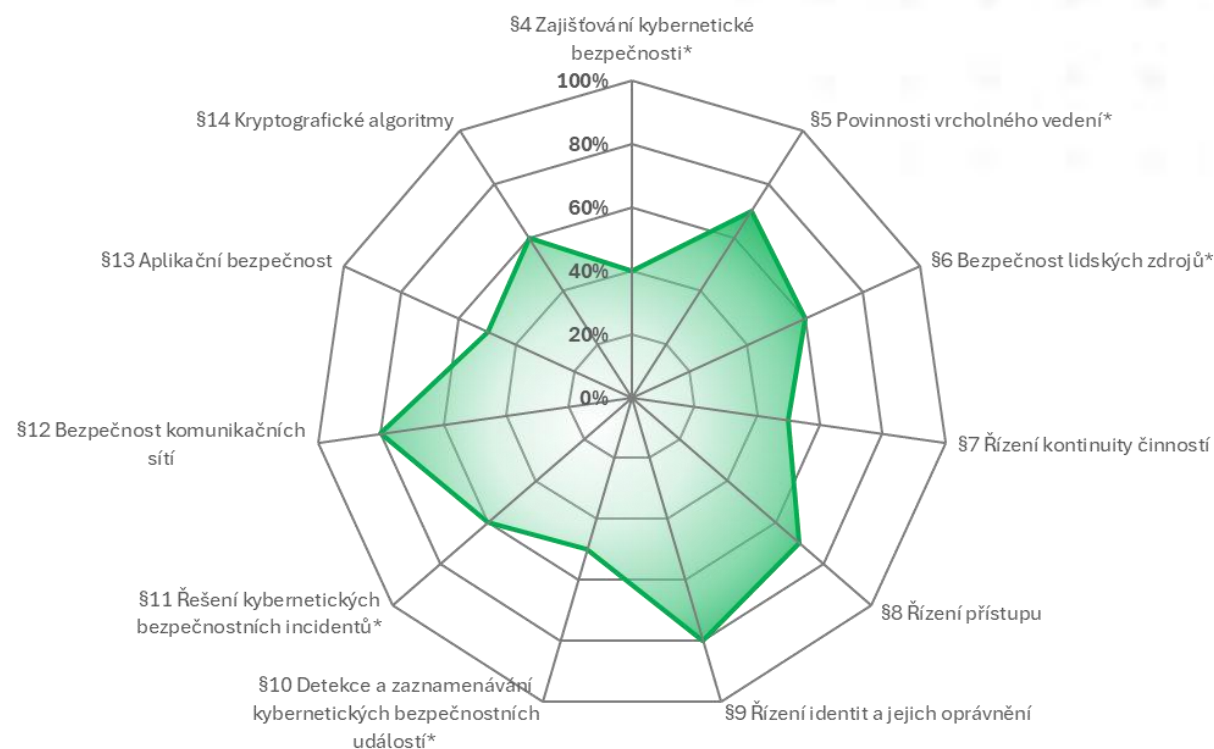
Začněte stanovením rozsahu kybernetické bezpečnosti

Přínosy analýzy / auditu

- Posouzení požadavků zákona o kybernetické bezpečnosti a zajištění shody (GDPR, NIS2 atd.).
- Zpracování katalogu primárních aktiv.
- Mapování, analýza aktuálního stavu IT infrastruktury.
- Nezávislé hodnocení kybernetické bezpečnosti.

Zjištění z praxe

- Chybějící dokumentace a organizační opatření.
- Spoléhání se pouze na pečlivost a důslednost pracovníků IT oddělení.
- Nesoulad bezpečnostní politiky s realitou.





Vzděláváte se?

Nejlepší odpovědí na bezpečnostní hrozby jsou poučení a odolní zaměstnanci!



**IDEÁLNÍ JE KOMBINOVAT ŠKOLENÍ ZAMĚSTANCŮ
A NASAZENÍ TECHNOLOGIÍ PRO JEJICH OCHRANU**

Vodohospodářská společnost

vzdělávací platforma formou služby = žádná správa LMS, kompletní přizpůsobení obsahu a podpora při vytváření nových kurzů.

Skupina strojírenských společností

implementace, napojení, integrace a kompletní přizpůsobení kurzů KB, LMS do interní správy.

Nemocnice

dodávka LMS platformy, implementace, napojení a integrace na identitní systém, předání do interní správy.

Jak se připravit?

Nečekejte na bezpečnostní incident, předcházejte mu.

- **URČENÍ ROZSAHU ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI - ANALÝZA**
Je informační bezpečnost v souladu s akceptovanou dobrou praxí a s platnou legislativou?
- **VYHODNOCENÍ ANALÝZY A IMPLEMENTACE NAVRŽENÝCH ŘEŠENÍ**
Bezpečnostní opatření by měla být zavedena až na základě analýzy současného stavu.
- **DETEKCE A ZAZNAMENÁVÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ – TESTY**
Provedení praktických testů odolnosti vaší společnosti proti kyberbezpečnostním útokům.
- **VZDĚLÁVÁNÍ ZAMĚSTNANCŮ A VEDOUCÍCH PRACOVNÍKŮ**
Nejlepší odpovědí na bezpečnostní hrozby jsou poučení a odolní zaměstnanci.
- **SPECIALISTÉ KYBERBEZPEČNOSTI**
Chybí vám specialisté na kybernetickou bezpečnost? Nebojte se outsourcingu.



Spolupracujme na
bezpečnější budoucnosti

**EFEKTIVNÍ INVESTICE DO SPRÁVNÝCH
BEZPEČNOSTNÍCH OPATŘENÍ JSOU
KLÍČEM K ÚSPĚCHU**



ALL4CYBER

**Aliance firem poskytujících
komplexní řešení kybernetické
bezpečnosti a implementace NIS2**

Aliance All4Cyber

Sdružení předních poskytovatelů řešení kybernetické bezpečnosti a implementace NIS2

Zakládající členové:

- Antesto, CNS, Datron, DATASYS, TeskaLabs, IdStory, ELAT

Mise:

Poskytování komplexních služeb a řešení kybernetické bezpečnosti, podpora implementace legislativních požadavků (např. NIS2, ZoKB aj.), důraz na vzdělávání a sdílení znalostí a zkušeností.

Cíle a hodnoty:

- Edukace, sdílení zkušeností a mezioborová spolupráce.
- Osvěta široké veřejnosti i profesionálů o komplexnosti tématu a řešení kybernetické bezpečnosti.
- Kultivace trhu prostřednictvím informačních kampaní a vzdělávacích programů.
- Sdílení znalostí a zkušeností v oblasti kybernetické bezpečnosti.
- Mezioborová spolupráce pro posílení kybernetické odolnosti.

D A T A.....
S Y S

RADIM PRACUCH

+420 724 065 027 | pracuch@datasys.cz