



Digitalizace, bezpečnost a NIS 2

Michal Vejvoda

Naše služby a řešení...

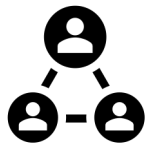


SLUŽBY A ŘEŠENÍ



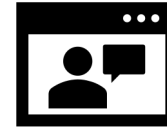
Digitalizace úřadu

- Portál občana – online komunikace úřadu
- Formulářové řešení
- Portál úředníka
- Rada a zastupitelstvo (komise a výbory)
- Integrace



IDM

- Řízený přístup uživatelů
- Licence, implementace a podpora



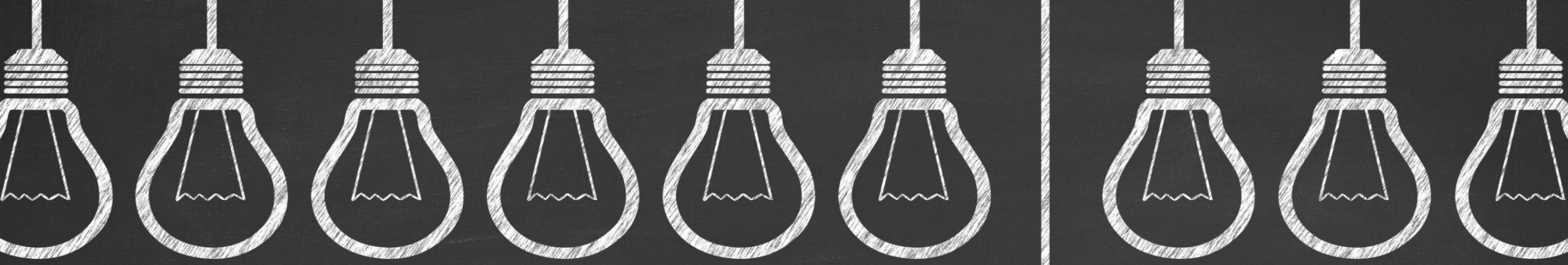
Digitalizace procesů/agendy

- ISMS (analýza rizik) a NIS 2
- HelpDesk
- Rezervace aut a zdrojů
- Interní směrnice a další agendy

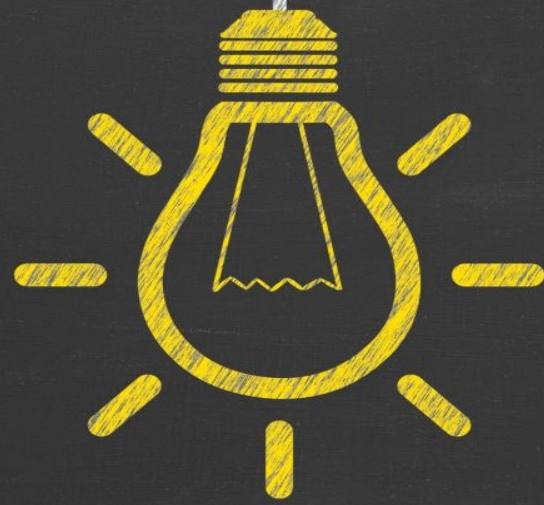


Vzdělávání/bezpečnost

- Školení zaměstnanců (kyberbezpečnost)
- Online kurzy
- Evidence školení a jejich realizace



Aktuální situace (NIS 2)...



Aktuální situace NIS 2

2021-23

2023

2023

?

HW infrastruktura

Obnova a rozvoj

Realizace projektů

Legislativa

05/2023 – 09/2023 Připomínkové řízení

4Q Předložení návrhu Poslanecké sněmovně

Transpozice NIS 2 do 17.10.2024

Příprava

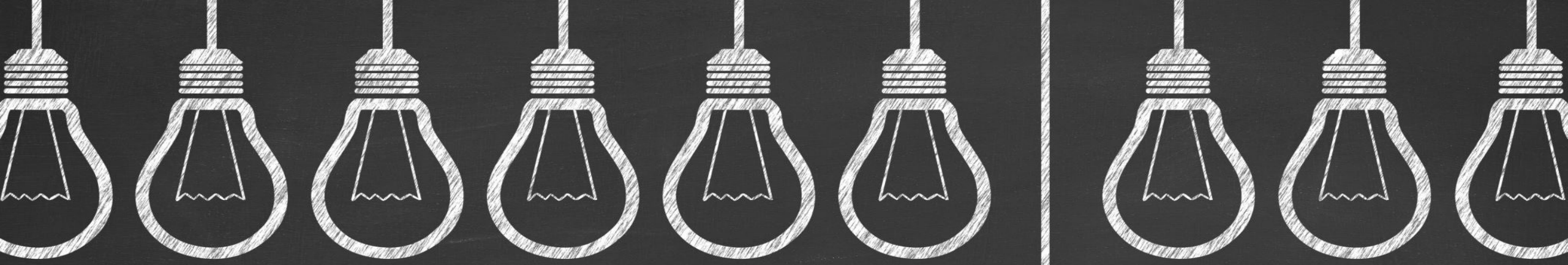
Lidské zdroje

Procesní zpracování

Řešení rizik

Realizace

Jak na to?



Jak na to? Ve 3 krocích...



1. Lidé



VZDĚLÁVÁNÍ A BEZPEČNOST



1

Vzdělávání/rozvoj dovedností

- Vzdělávání interních uživatelů
- Audit znalostí
- Online/prezenční kurzy dle potřeby

2

Konzultace/analýza

- Analýza procesů a přípravy na NIS 2
- Konzultace řešení prioritních rizik organizace
- Definování nástrojů pro interní uživatele

2. Procsy



PROCESY A NÁSTROJE



1

PROCESY

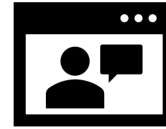
- Definice potřeb vlastní organizace
 - nižší vs. vyšší požadavky NIS 2
- Definice rolí a potřeb uživatelů

2

Nástroje/agenda pro NIS 2

- Přehledy aktiv a rizik
- Reporting, notifikace a vyhodnocení
- Řízení rizik v reálném čase

AGENDA ISMS (analýza rizik) a NIS 2



Hlavní vlastnosti

- Řízení/správa dat v oblasti kybernetické bezpečnosti
- Podpora norem:
 - ISO 27001
 - Zákon o kybernetické bezpečnosti
 - TISAX
- Kontrola rizik a jejich řízení
- Automatizace procesů (notifikace, reporting, vazby...)



AGENDA ISMS (analýza rizik) a NIS 2



„Moduly“ agendy ISMS a NIS 2

- Evidence
 - auditů
 - neshody/opatření
 - bezpečnostních událostí/incidentů
- Katalog hrozeb/informačních aktiv
- Kontrola rizik a jejich řízení
- Plán zvládnutí rizik
- Vzdělávání v rámci ISMS a NIS 2
- Úkoly, změnové požadavky...

AGENDA ISMS (analýza rizik) a NIS 2



Katalog „hrozeb“ a „informačních aktiv“

- Katalog „hrozeb“:
 - definice a možnosti úpravy
 - implementace v rámci více organizací
 - vazba na katalog opatření dle norem (ISO 27001, TISAX, „Kyber“ zákon)
- Katalog „informačních aktiv“:
 - seznam primárních aktiv
 - seznam podpůrných aktiv
 - N úrovní katalogu aktiv
 - definice jednotlivých aktiv

AGENDA ISMS (analýza rizik) a NIS 2



Rizika

- Automatické generování rizik na základě hrozeb a informačních aktiv
- Kategorizace rizik dle metodiky a správa vlastníky rizik
- Stavy rizika:
 - výchozí
 - aktuální
 - cílový
- Aktualizace hodnocení rizik včetně historie změn
- Vazba na úkoly plánů zvládnání rizik
- Automatizovaný výstup pro „Prohlášení o aplikovatelnosti“

AGENDA ISMS (analýza rizik) a NIS 2



Audity/neshody/bezpečnostní události

- Audity/neshody
 - evidence auditů a neshod
- Opatření
 - seznam předpisů
 - zodpovědnost vlastníků rizik
- Bezpečnostní události
 - evidence hlášení a událostí
 - výstup hlášení pro NÚKIB
 - evidence incidentů

NÁHLED AGENDY ISMS a NIS 2

Bezpečnostní události				
+ Úkol	Typ	Stav	Konec	Prodlení
	Bezpečnostní událost	Schváleno	19.07.2022 10:...	0
	Bezpečnostní událost	Zrušeno		0
	Bezpečnostní událost	Dokončeno	16.07.2022 00:...	0
	Bezpečnostní událost	Dokončeno	09.06.2022 00:...	0
	Bezpečnostní událost	Dokončeno	31.08.2022 00:...	0
	Bezpečnostní událost	Zrušeno	05.05.2022 00:...	0

Evidence auditů			
Číslo	Název	Termín od	Termín do
2017/01	EMS - Interní audit		
2017/02	Vývoj a vydání nových verzí aplikací ...		
2018/01	Implementace produktů		
2018/02	EMS interní auditový		
2020/01	EMS interní audit		
2020/02	Prodej vlastních výrobků a služeb (D...		
2021/01	Vývoj d.kurzů	04.03.2021	04.03.2021
2021/02	Vývoj DAS	07.04.2021	07.04.2021
2021/03	Impementace ISMS	14.10.2021	14.10.2021
2022/01	Spuštění ISMS	14.01.2022	14.01.2022

Rizika ISMS							
Číslo hroz...	Název hrozby	Frekvence cíl	Dopad cíl	Zraniteln...	RPN cíl	RPN start	RPN skut...
TT03	Selhání aplikačního software	■	■	■	●	●	●
TT04	Selhání komunikačních služeb	■	■	■	●	●	●
TT06	Selhání dodávky el. energie	■	■	■	●	●	●
TT09	Ztráta dat	■	■	■	●	●	●
TM02	Kybernetický útok z vnější sítě	■	■	■	●	●	●
TM03	Útok pomocí sociálního inženýrství nebo špionážních technik	■	■	■	●	●	●
TM04	Trvale působící a pokročilé hrozby	■	■	■	●	●	●
TM05	Neoprávněný přístup a manipulace s informačním aktivem	■	■	■	●	●	●
TM07	Neoprávněné nakládání s osobními údaji	■	■	■	●	●	●
TM09	Odposlech a manipulace komunikace	■	■	■	●	●	●
TM10	Škodlivé a destruktivní programy	■	■	■	●	●	●
TO01	Porušení legislativních požadavků	■	■	■	●	●	●
TO02	Porušení smluvních požadavků	■	■	■	●	●	●
TO03	Nevhodné nastavení přístupových oprávnění	■	■	■	●	●	●
TO04	Nedostatky v nastavení a dokumentaci procesů,	■	■	■	●	●	●
TO07	Závady v komunikaci (mezilidské)	■	■	■	●	●	●
TO11	Selhání služeb dodavatele	■	■	■	●	●	●



3. Praxe





PRAXE

1

Školení a rozvoj dovedností

- Zajištěné vzdělávání uživatelů => vyšší bezpečnost

2

Nástroje a agendy pro NIS 2

- Implementace agendy => fungující procesy pro NIS 2

3

Dokončení realizace a praxe

- Definování prioritních rizik => řízení jejich snižování



Více informací...
mvejvoda@datron.cz

