Implementace NIS 2

a nového ZKB v organizaci jako součást compliance

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.

Policejní akademie ČR v Praze | 7.2.2024

Barbora Vlachová je vedoucí advokátkou právního týmu, který se zabývá především kyberbezpečností, digitální transformací, právem IT a ochranou osobních údajů. Barbora je zapsána jako rozhodce Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky. Je členkou sekce České advokátní komory pro IT a GDPR. Aktuálně vyučuje na Policejní akademii České republiky v Praze a na Vysoké škole ekonomie a managementu. Pravidelně publikuje v oblasti práva informačních technologií, občanského, obchodního, finančního a správního práva. Zúčastňuje se také odborných konferencí a seminářů.

AKCČS již více než 30 let poskytuje své služby vrcholným představitelům podnikatelského prostředí i významným státním institucím. Vedle běžné advokátní činnosti navrhujeme pro naše klienty služby napříč oborem IT práva šité na míru jejich hospodářské činnosti, od nastavení optimálních smluvních podmínek pro údržbu, podporu a rozvoj software, pořízení hardware, zajištění souladu se zákonem o kybernetické bezpečnosti, řešení problematiky vendor lock-in a další.

30 1993-2023 CÍSAŘ ČEŠKA SMUTNÝ

Aktuální výzvy v kyberbezpečnosti

Kybernetická bezpečnost jako součást compliance I Nový zákon o kybernetické bezpečnosti I Implementace NIS 2

Aktuální výzvy

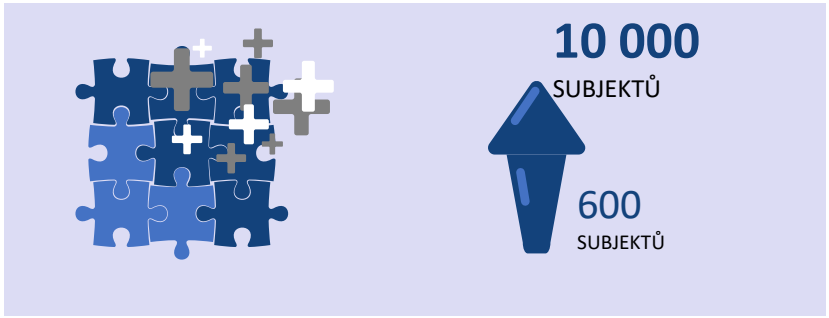
- Implementace NIS 2
- Nový zákon o kybernetické bezpečnosti
- Následuje 1 rok pro implementaci opatření

Stávající povinné osoby

- Nutnost reagovat na nové povinnosti
- Revize a audit aktuálních bezpečnostních opatření
- Příležitost smazat technologický dluh

Nové povinné subjekty

- Proces sebeidentifikace
- Povinnosti dle kategorie regulovaného subjektu
- Zavedení opatření



Compliance program a jeho přínosy

Compliance program

- systém vnitřních opatření společnosti za účelem zajištění souladu mezi jím vykonávanou činností a zákonnými i obecně závaznými pravidly pro předcházení protiprávnímu jednání společnosti

Nastavení systému

- preventivních opatření
- detekčních opatření
- kontrolních opatření
- nápravných vnitřních opatření a zásad
- řízení rizik

Přínosy compliance

- prevence
- dobrá pověst a zvýšení důvěryhodnosti
- konkurenční výhoda
- včasná detekce porušení právních předpisů
- předcházení sankcím

Oblasti compliance programu

Trestněprávní

Soutěžní

Správněprávní

Vnitřní organizace
a
koncernová struktura

Strategická
a
krizová komunikace

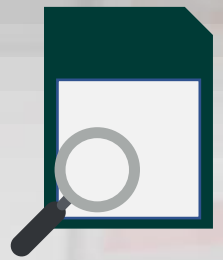
Business partner
check

Veřejné zakázky

Kybernetická
a
informační bezpečnost

Kybernetická a informační bezpečnost jako součást compliance

- Zvýšení počtu kybernetických útoků a jejich dopadů jako následek digitalizace
- Nárůst regulatorních nároků, včetně nárůstu počtu povinných osob
- Nutnost brát kybernetickou a informační bezpečnost jako součást širšího compliance



Jinak dochází k přijímání atomizovaných řešení a jednotlivé interní směrnice či doporučení mohou působit protichůdně.

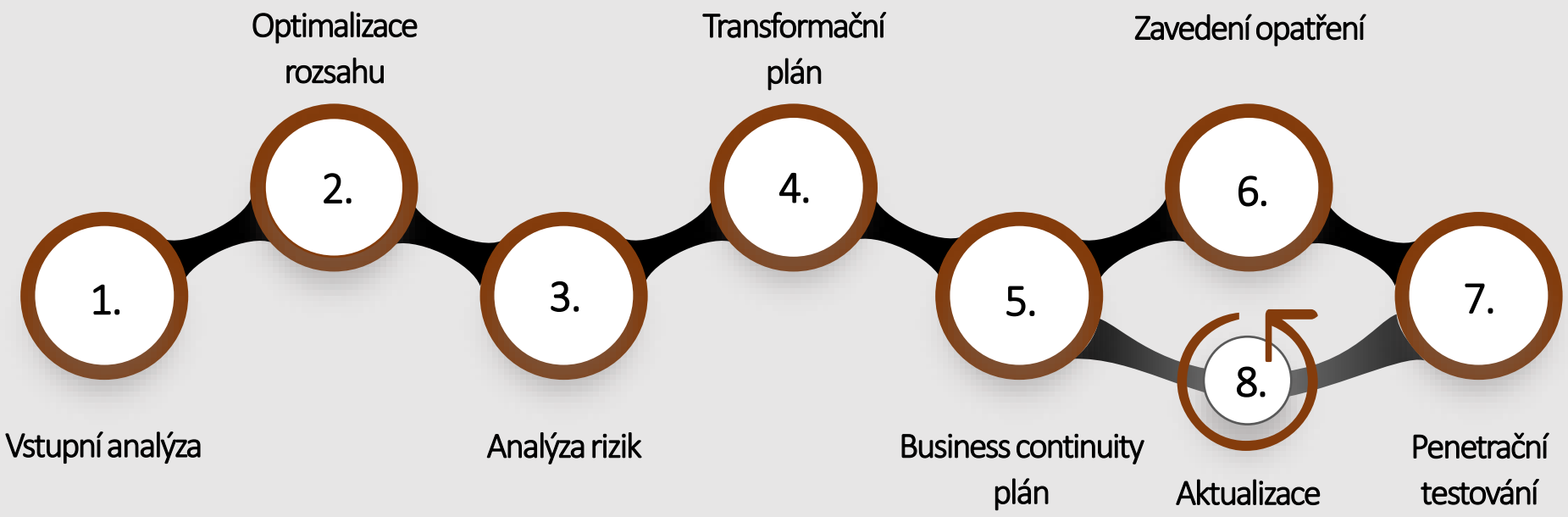
Povinnosti
NIS 2 + ZKB

- Analýza **rizik**
- **Hlášení incidentů**
- **Kontinuita** činností
- Bezpečnost v rámci **dodavatelského řetězce;**
- Bezpečnost v rámci **pořízení, vývoje a údržby systémů;**
- Bezpečnostní **politiky a postupy**
- **Vzdělání** v oblasti kybernetické bezpečnosti;
- Využívání **kryptografie a šifrování;**
- Bezpečnost lidských zdrojů, **řízení přístupů a aktiv**;
- Využívání vícefaktorového ověření identity, bezpečných **komunikačních nástrojů** a nástrojů pro **nouzovou komunikaci**.

Cíle compliance v oblasti kybernetické bezpečnosti

- nutná **koordinace technické**, **organizační** a **právní** části k zajištění kybernetické bezpečnosti v souladu s legislativou
- **ochrana** před porušením právních předpisů a snížení rizika sankcí za jejich porušení
- jednotně **nastavený** a vnitřně **souladný** standard řízení kybernetické a informační bezpečnosti
- **ochrana managementu** před osobní odpovědností

Nastavení compliance v oblasti informační a IT bezpečnosti v organizaci



Postup implementace

IMPLEMENTACE SMĚRNICE NIS 2

PLNĚNÍ POVINNOSTÍ

KONTROLA VZTAHŮ S DODAVATELI

ÚČEL

Implementace NIS 2

Nutnost zajištění souladu s novou legislativou v organizaci

Doporučené kroky v rámci implementace:

- Sledovat a průběžně monitorovat legislativní proces
- Příprava metodiky implementace NIS 2 v prostředí organizace, včetně harmonogramu provedení jednotlivých kroků
- Nutné provést identifikaci primárních a podpůrných aktiv a určit rozsah řízení kybernetické bezpečnosti v prostředí organizace
- Revize interních předpisů a interních procesů organizace
- Kontrola smluvních vztahů s dodavateli, zda je řádně ošetřena problematika kybernetické bezpečnosti, v případě nedostatků určit postup k nápravě
- Příprava metodiky školení zaměstnanců a managementu v oblasti kybernetické bezpečnosti – úvodní školení k nové právní úpravě + periodická školení v rámci rozvoje bezpečnostního povědomí v organizaci

30 1993-2023 CÍSAŘ ČEŠKA SMUTNÝ

Diskuze/Dotazy

Děkuji za pozornost.

KONTAKT

VLACHOVA@AKCCS.CZ

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.