

# O2 IT Services

První praktické zkušenosti s NIS2 v praxi

Tomáš Svoboda / 9. 11. 2023

O<sub>2</sub> IT Services

# Jak to vidí O2 ITS

Za několik málo posledních měsíců přinesly konzultace se zákazníky první zkušenosti, příklady dobré praxe i poučení jak se na novou legislativu připravit

Nejčastější kroky zákazníků:

1. krok – GAP analýza – jak jsme na tom a co bude dál
2. krok – aktiva, rizika, řízení dodavatelů, kontinuita, školení, procesy – incidenty, změny, hlášení NUKIB a co s tím?

# Vybrané kapitoly z NIS2, které jsou vnímány zákazníky jako klíčové

- Tlak na odpovědnost statutárního orgánu za kybernetickou bezpečnost organizace
- Řízení aktiv a rizik: identifikace a klasifikace aktiv, řízení rizik,...
- Bezpečnost dodavatelského řetězce
- Školení
- Řízení kontinuity činností
- Procesní oblast
  - Řízení incidentů
  - Řízení změn
- Ocenění práce NUKIB v komunikaci změn

# Řízení aktiv

Je nezbytné vědět, jaká aktiva jsou pro společnost klíčová

**V 90% dostáváme od zákazníka otázku – „a co je to to aktivum a k čemu je to dobré?“ 😊**

- Primární – informace nebo klíčová služba, která je poskytována
- Podpůrná – HW, SW, lidské zdroje, dodavatelé, lokality
- Jak máme identifikovat aktiva?
- Jak máme identifikovat garanty aktiv?
- Klíčový vstup do řízení rizik
- **Aktiva nejsou pouze CMDB položky IT infrastruktury!**

# Řízení rizik

Je nezbytné vědět, jaká rizika mají vliv na zajištění regulované služby

- Hrozby, zranitelnosti

**U zákazníků nejsou ve většině případů uchopeny procesy řízení rizik**

**Nejčastější dotazy:**

Odpovědnost v procesu řízení rizik

- bezpečnostní role, vedení

Analýza rizik aneb hrozby, zranitelnosti a kde je najít? 😊

Vyhodnocení rizik – prioritizace a kritéria pro řešení

Zvládání rizik

- akceptace, přenesení, sdílení, vyhnutí se riziku a jejich význam pro organizaci

# Řízení dodavatelů

**U zákazníků nejsou ve většině případů identifikováni významní dodavatelé a odpovídající smluvní zajištění**

## **Nižší režim**

Propsání požadavků do smluv s dodavateli

- CIA, audit, řetězení, řízení změn, NDA, exit strategie, BCM, sankce

## **Vyšší režim**

Identifikace, informování a evidence dodavatelů

Pravidelný audit – interní i třetí stranou

Hodnocení rizik před uzavřením smlouvy, jak zohlednit varování NUKIB???

Požadavky KB ve smlouvách s dodavateli, pravidla chování dodavatele

- Bezpečnostní politiky, incidenty, aktiva, rizika, likvidace dat, odstoupení od smlouvy, předání dat do jiného státu.

# Školení

**Většina organizací spadajících nově pod NIS2 řeší pouze částečně nebo vůbec**

**Prokazatelné:**

- Školení vrcholového vedení, zaměstnanců, školení dodavatelů

**Vyšší režim**

Školení bezpečnostních rolí

Co školit - doporučená školení v příloze č.8

- Sociální inženýrství, VPN, elektronická komunikace, cloudová uložení, aktuální hrozby, detekce zranitelností, používání zařízení pro soukromé účely.

# Řízení kontinuity

**Kontinuita činností není pouze zálohování a distaster recovery**  
**Kontinuita činností = procesy a činnosti organizace, nejen IT systémů.**

## **Nižší režim**

- Vazba na primární aktiva - pořadí obnovy primárních aktiv
- Odpovědnosti, pravomoci
- Zálohování

## **Vyšší režim**

- Metodika pro stanovení analýzy dopadů
- Vstup do hodnocení rizik
- Stanovení minimální úrovně poskytovaných služeb
- BC plán per služba
- Testování plánů kontinuity činností

**Příklad: pandemie COVID 19 a vliv na lidské zdroje**  
**Zákazníci vnímají kontinuitu pouze z pohledu IT nebo vůbec.**

# Řízení incidentů

## Nižší režim

- Jak posuzovat incidenty? Metodický postup – vazba na řízení kontinuity činností
- Hlášení incidentů s významným dopadem

## Vyšší režim

- Hlášení **VŠECH** kyber. bezp. incidentů.
- Aktualizace analýzy rizik, BCP
- **Prvotní hlášení do 24 hodin**
  
- **Zákazníci řeší řízení incidentů pouze z pohledu IT**
- Neexistují formalizované metodické postupy pro klasifikaci incidentů a workflow pro jejich řešení.
- Stanovit role, pravomoci a odpovědnosti při řešení incidentů
- Table-top cvičení

# Řízení změn

## Nižší režim

- Řízení změn u dodavatelů

## Vyšší režim

- Změny mající vliv na kybernetickou bezpečnost
- Politika řízení změn
- Významné změny – co to je????
- **Zákazníci ve většině případů neřeší řízení změn**
- Neexistují formalizované metodické postupy pro klasifikaci změn a workflow pro jejich řešení.
- Stanovit role, pravomoci a odpovědnosti při řešení změn
- Post- analýza

# Děkuji za pozornost

Prostor pro dotazy

O<sub>2</sub> IT Services