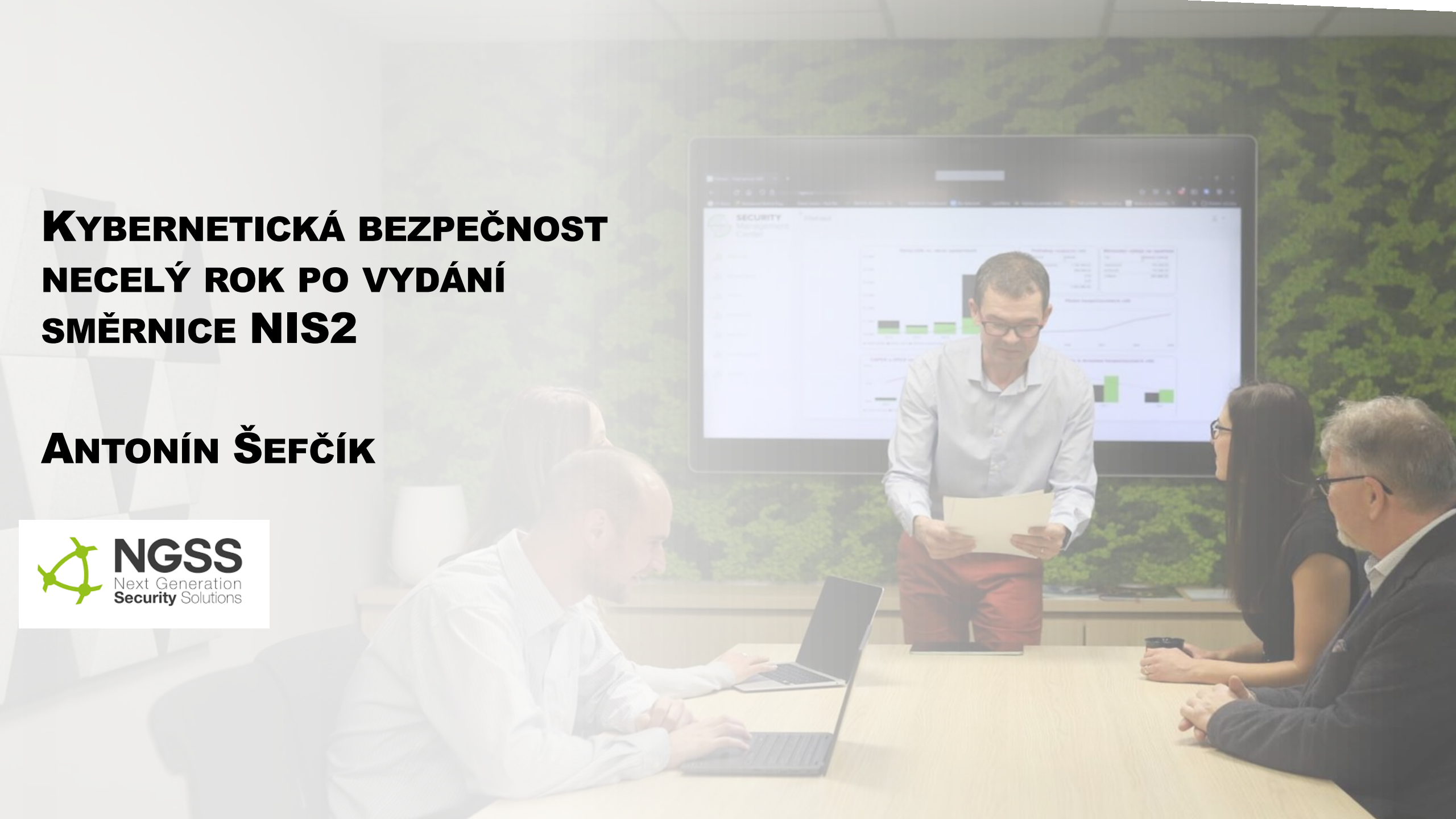
Kybernetická bezpečnost necelý rok po vydání směrnice NIS2

Antonín Šefčík

NGSS
Next Generation
Security Solutions



Směrnice NIS 2

- EU přichází s aktualizací požadavků na kybernetickou bezpečnosti v nová směrnici o kybernetické bezpečnosti **SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)**

- Publikace finálního znění směrnice NIS2 proběhla v **prosinci 2022**. Transpoziční lhůta (tj. lhůta, ve které musí členské státy směrnici promítnout do národního práva) je stanovena na **21 měsíců**

- NIS2 již nehledá systémy důležité pro společnost, ale definuje **celé služby důležité pro její fungování**

Klíčové změny

- **Rozšíření působnosti:** rozšíření organizací na které se bude vztahovat kybernetická bezpečnost ze 400 na 6000 (možná až 10 000) na základě zvýšení počtu regulovaných odvětví spolu s rozšířením stávajících regulovaných odvětví o nové regulované služby

- **Přísnější požadavky:** na management organizace (školení), řízení dodavatelů, dvoufaktorová autentizace, zkrácení času hlášení kybernetických bezpečnostních incidentů a používání podporovaného SW

-

- **Evropská integrace**: směrnice podporuje užší spolupráci na úrovni Evropy a vytváření jednotných databází, směrnice se snaží odstranit nedostatečnou míru kybernetického zabezpečení podniků a institucí působících v Evropské unii a snaží se vyrovnat rozdíly mezi jednotlivými členskými státy

- **Zvýšený dohled:** bude posílen dohled a donucovací pravomoci NÚKIB, přičemž NÚKIB bude mít více pravomocí kontrolovat a monitorovat dodržování nového standardu a širší pravomoc ukládat nebo iniciovat sankce

Co je potřeba

- Kybernetickou bezpečnost **budou muset zavést tisíce organizací**
- U stávajících organizací – povinných osob se jedná o **prohloubení již zavedených požadavků**
- U tisíců organizací se **jedná o zavedení nových požadavků**, u většiny v režimu nižších povinností
- Minimálně u **stovek (cca 600) však v režimu vyšších povinností“**
  - Hrozí slabá připravenost
  - Velká zátěž jak z hlediska prostředků, tak zejména porozumění problematice
  - Problém s obsazením bezpečnostních rolí (architekt kybernetické bezpečnosti)

Úprava dokumentace?

„V rámci našeho ….. bychom rádi provedli aktualizaci bezpečnostní dokumentace ISMS. Jednalo by se o (1) gapovou analýzu současné dokumentace, prověření kompatibility se ZoKB a VoKB, i s ohledem na dopady NIS2 a také její aplikovatelnosti v rámci struktury ….. (2) v závislosti na výsledcích analýzy navržení úprav této bezpečnostní dokumentace, tak aby byla kompatibilní a aplikovatelná podle bodu 1“

Jak to někdy organizace vnímají

- Nevím do jakého režimu organizace spadá (více odvětví)
- Zavedu bezpečnostní požadavky a ne systém
- Budu to řešit jako GDPR, časem to vyšumí
- Chci řešit role a zajištění bezpečnosti jen externím člověkem
- Nebudu zatěžovat vedení organizace nějakými požadavky
- Napište mi papíry ať je klid
- Je to věc informačních technologií, ať si to řeší

Je na co navázat

- Metodická pomoc NÚKIB
- ISMS dle **ISO/IEC 27001** (a další případné normy):
    - Novelizovaná norma
    - Široká základna více než 60 norem v řadě 27000
    - Široká základna řešitelů (www.iso27001security.com)
- **Informační systémy veřejné správy** (Informační koncepce, bezpečnostní dokumentace informačního systému veřejné správy)
- Krizové řízení
- Dosavadní opatření fyzické bezpečnosti
- Případné zavedené systémy
- ….

Jak na to – zavést ISMS

Jedná o **zavedení a provoz ISMS** s:

- vymezeným rozsahem
- výběrem opatření na základě hodnocení rizik
- který má zavedené role a opatření
- je pravidelně auditován a hodnocen

Zavádění ISMS – možný postup

1. Určení jaké požadavky kybernetické bezpečnosti se na mne budou vztahovat (nižší X vyšší)
2. Provedení srovnávací analýzy současného stavu kybernetické bezpečnosti vůči požadavkům stávající vyhlášky, minimálního bezpečnostního standardu nebo návrhům vyhlášek
3. Provedení identifikace a hodnocení aktiv, případně provedení analýzy dopadů.

Výše uvedené analytické kroky je možné realizovat v roce 2023, vlastní zavádění pak doporučujeme realizovat v roce 2024 po vydání nového zákona a navazujících vyhlášek.

4. Dokončení procesu zvládání rizik – návrh bezpečnostních opatření
5. Implementace vybraných bezpečnostních opatření zahrnuje návrh postupů, jejich popis v bezpečnostní dokumentaci, příprava a realizace technických opatření, rozpracování plánů kontinuity, školení …
6. Provedení interního auditu a přezkoumání ISMS uzavírá celý cyklus zavedení systému řízení bezpečnosti informací.
7. Přezkoumání ISMS

Dobře připravit zavedení ISMS

Před zahájením implementace je vhodné si **položit otázky**:

- Proč potřebujeme ISMS? Bude nám i k něčemu jinému, než naplnění požadavků kybernetické bezpečnosti? Co dalšího můžeme z této příležitosti vymáčknout?
- Kolik to bude stát? Spotřebuje všechny naše zdroje zabezpečení informací?
- Není to něco, co by mělo dělat IT? Jaký je význam pro zbytek organizace? Proč se máme zapojovat?
- Jaké máme možnosti? Jaké přístupy bychom mohli zvolit?
- Co si o tom myslí ostatní oddělení, odborníci a poradci? Kdo další je nebo by měl být zapojen? Jsou všichni plně zapojeni do návrhu a podporují jej, nebo by mohl vzniknout odpor k plnění? Dokážeme se vyrovnat se změnami, které pravděpodobně nastanou?
- Jaké překážky existují nebo mohou existovat a co s nimi můžeme/měli bychom dělat? Jaká jsou rizika spojená s realizačním projektem?
- Kdo by to měl provozovat? Jaké druhy dovedností a kompetencí potřebují? Můžeme si dovolit odvést je od jiných povinností na toto? A co zbytek týmu?
- Jak máme stanovit rozsah? Měli bychom ISMS omezit na určité části organizace (ty co realizují regulované služby), ať už prozatím nebo navždy?

Na co si dát pozor

- Navázat na to co již bylo v oblasti bezpečnosti zavedeno
- Připravit si plán zavedení
- Počítat s časovou a projektovou náročností, vyčlenění zdrojů
- Jednotný systém řízení bezpečnosti informací
- Neopakovat chyby spojené s GDPR

Děkuji za pozornost