12/02/2025

Správné zavádění bezpečnosti dle NIS2 a nZKB

Prakticky, krok za krokem

BESECURED

Nový zákon o kybernetické bezpečnosti.

Časová osa

- 26. června 2025 – zákon podepsán prezidentem.
- Poté předán do Sbírky zákonů (lhůta na zveřejnění max. 30 dní).
- Účinnost: 1. listopadu 2025 - ODKAZ.
- 60 dní na ohlášení regulovaných služeb
- 12 měsíců přechodné období na zavedení bezpečnostních opatření a hlášení incidentů od potvrzení registrace.

BESECURED

Organizace spadají pod regulaci, pokud:

- Poskytují regulované služby (např. energetika, zdravotnictví, finance, doprava, veřejná správa apod.).
- Působí v regulovaném odvětví, i pokud nejsou přímo veřejnou institucí.
- Splňují vybraná kvantitativní kritéria, např. velikost (počet zaměstnanců, obrat).

Režimy povinností podle nZKB

- **Vyšší režim (ODKAZ):**
  - Rozšířené požadavky na bezpečnostní opatření, hlášení incidentů apod.
- **Nižší režim (ODKAZ) :**
  - Základní povinnosti – přiměřené rozsahu a typu služeb.

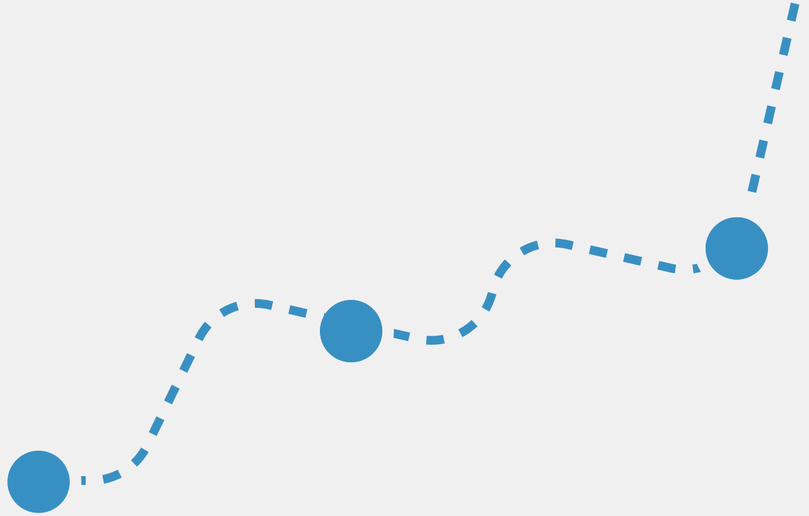
Režim se určí podle významnosti poskytované služby a velikosti organizace.

Nový zákon o kybernetické bezpečnosti.

BESECURED

10 kroků k implementaci nZKB.

BESECURED



KROK 1:

ZJISTĚTE, ZDA SE NA VÁS ZÁKON VZTAHUJE.

BESECURED

Vyhláška o regulovaných službách

- 22 odvětví
- Regulované služby
- Doplňující podmínky

Regulovaná služba:

- služba, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva,

Poskytovatel regulované služby

- orgán nebo osoba, které poskytují jednu nebo více regulovaných služeb,

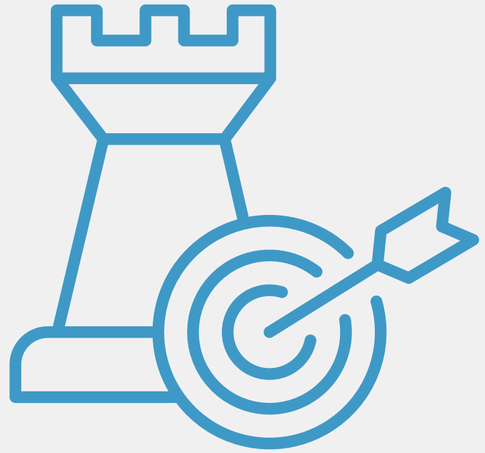
Pozor na “křížení” regulací

Jak to zjistíme?

BESECURED

KROK 2:

PROVEĎTE SEBEHODNOCENÍ A URČETE REŽIM POVINNOSTÍ.



Regulovaná služba

+

Kategorie podniku	Počet zaměstnanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Velký podnik	≥ 250	> 50 miliónů EUR	nebo	> 43 miliónů EUR
Střední podnik	< 250	≤ 50 miliónů EUR	nebo	≤ 43 miliónů EUR
Malý podnik	< 50	≤ 10 miliónů EUR	nebo	≤ 10 miliónů EUR
Mikro podnik	< 10	≤ 2 miliónů EUR	nebo	≤ 2 miliónů EUR

BESECURED

KROK 3:

ZÍSKÁNÍ PODPORY VRCHOLOVÉHO VEDENÍ.

Jak se projevuje?

- Oznámení budování ISMS
- Jmenování bezpečnostních rolí
- Schválení bezpečnostních cílů a projektů
- Vydání bezpečnostní politiky

Role podle nZKB

- **Vyšší režim:**
  - Manažer KB
  - Architekt KB
  - Auditor KB
  - Výbor KB
  - Garanti (vlastníci) aktiv
- **Nižší režim:**
  - Osoba pověřená kybernetickou bezpečností

Podpora nejvyššího vedení

BESECURED

KROK 4:

STANOVENÍ ROZSAHU KYBERNETICKÉ BEZPEČNOSTI VE VAŠÍ ORGANIZACI.

Rozsah kybernetické bezpečnosti

Co je součástí regulované služby:

- Technologie
- Software
- Lidé
- Budovy
- Data a informace
- Dodavatelé

Budeme potřebovat pro analýzu rizik

Rozdíl oproti ISO 27001/TISAX atd.:

- Jsou přímo určené hranice ISMS
- Regulovaná služba nemusí souviset k “core” činností společnosti

BESECURED

BESECURED

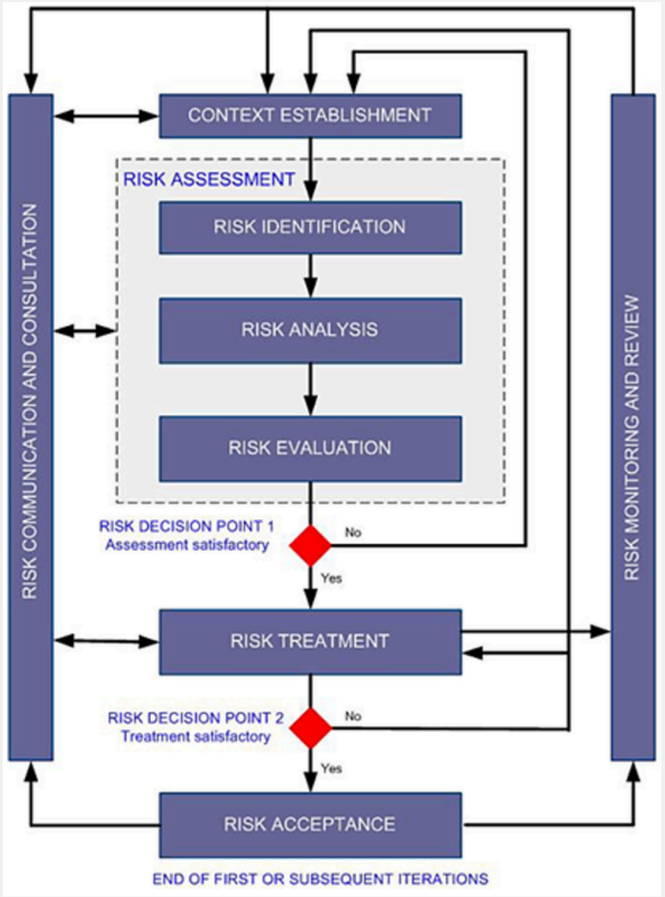
KROK 5:

PROVEĎTE ANALÝZU A ŘÍZENÍ RIZIK POKUD SPADÁTE DO VYŠŠÍHO REŽIMU (A I KDYŽ NE).

Řízení rizik

Fáze:

- **1:** Stavenovení souvilostí (primární a podpůrná aktiv, hrozby a zranitelnosti, metodika)
- **2:** Analýza rizik
- **3:** Hodnocení rizik
- **4:** Ošetření rizik



BESECURED

Řízení rizik

Na co pamatovat?

- Vedení schvaluje celkové řešení rizik
- Vlastník rizika schvaluje plánovanou hodnotu zbytkového rizika
- Revidovat účinnost nasazených opatření
- Pravidelná činnost - nekončí po prvním cyklu

Základní pravdy:

- Papír snese všechno... a excel taky
- Kdo zná své prostředí, tak ví, jaká rizika mu hrozí
- Pravidlem starý server nezabezpečím

BESECURED

BESECURED

KROK 6:

POLOŽTE STAVEBNÍ KAMENY KYBERNETICKÉ BEZPEČNOSTI (ISMS).

ISMS

Bezpečnostní politika

Kontext (co je důležité)

Kde leží rizika (co chráním)

Komunikace a spolupráce

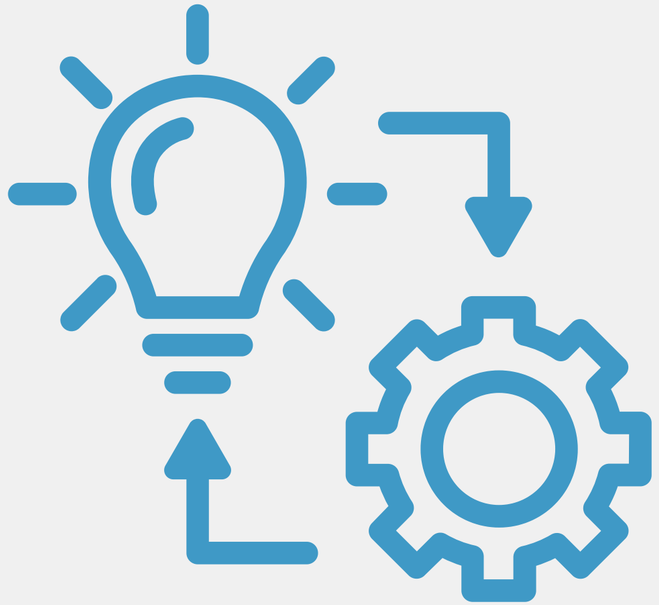
Co nám zajišťují dodavatelé

BESECURED

BESECURED

KROK 7:

IMPLEMENTUJTE BEZPEČNOSTNÍ OPATŘENÍ.



Budujeme ISMS

Vyšší režim

- Řízení aktiv a rizik
- Řízení dodavatelů
- Bezpečnost lidských zdrojů
- Řízení změn
- Akvizice, vývoj a údržba
- Řízení přístupů
- Zvládání incidentů
- Řízení kontinuity činností
- Auditování
- Fyzická bezpečnost
- Bezpečnost sítí
- Přístupová práva a oprávnění
- Detekce událostí
- Zaznemenávání událostí
- Vyhodnocování událostí
- Aplikační bezpečnost
- Kryptografie
- Dostupnost reg. služby
- OT bezpečnost

Nižší režim

- Bezpečnost lidských zdrojů
- Řízení kontinuity
- Řízení přístupů
- Řízení identit a oprávnění
- Detekce a zaznamenávání událostí
- Řešení incidentů
- Bezpečnost komunikačních sítí
- Aplikační bezpečnost
- Kryptografické algoritmy

Procesy - opatření - záznamy

BESECURED

BESECURED

KROK 8:

NASTAVTE PROCES ZVLÁDÁNÍ INCIDENTŮ A HLÁŠENÍ.

Řízení incidentů

Co je tady důležité:

- Připravte si jasný postup řízení incidentů
- Definujte konkrétní role (řešitele)
- Sestavte si plán reakce na incidenty
- Hlaste ve lhůtách 24h/72h/30d
- Testujte, testujte, testujte!

Povinnosti pro vyšší režim:

- Vše co se projevilo v rozsahu ISMS
- Má původ v kyberprostoru
- Nelze vyloučit úmyslné zavinění

Povinnosti pro nižší režim:

- hlásit jen významné incidenty

BESECURED

BESECURED

KROK 9:

PROVEĎTE AUDIT A PŘEZKUM SYSTÉMU.

Audit ISMS

Co vše je auditem ISMS:

- Systémový audit auditorem
- Test BCP, IRP a DRP
- Penetrační test
- Test technických zranitelností
- a každá další kontrolní činnost

Co je cílem:

- Odhalit nedostatky a slabá místa
- Ověřit funkčnost bezpečnostních mechanizmů a procesů

Kdo netestuje, ten neví, kudy pronikne útočník.

BESECURED

BESECURED

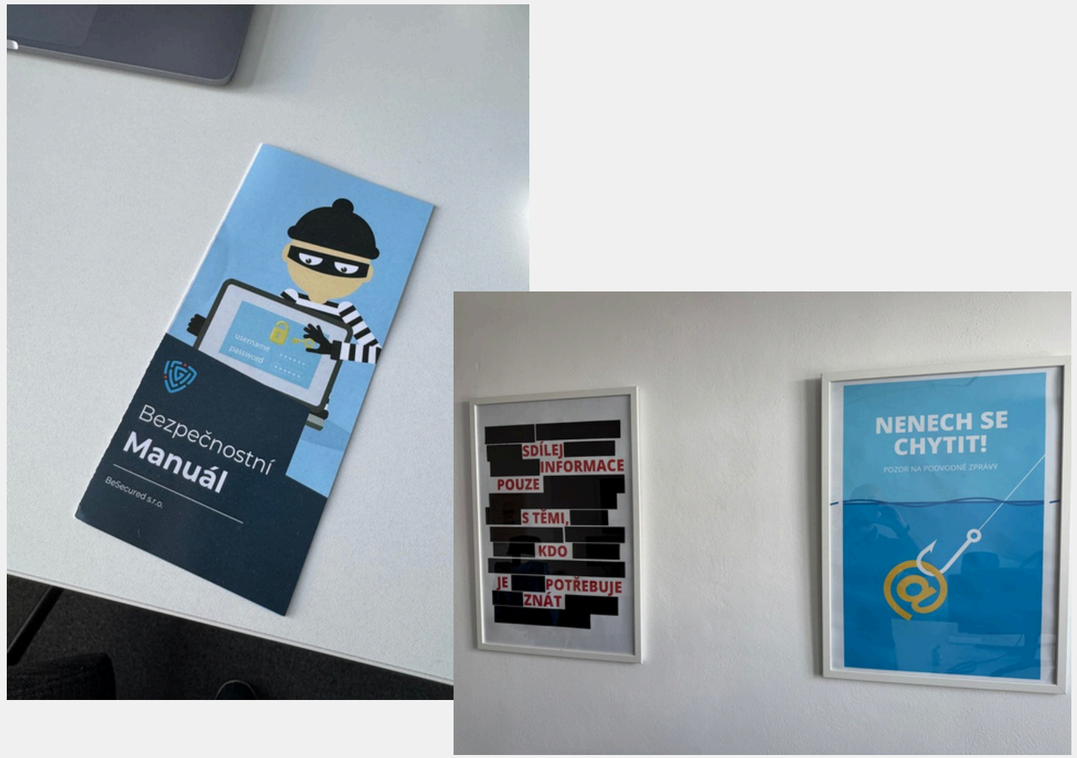
KROK 10:

BUDUJTE KULTURU KYBERNETICKÉ BEZPEČNOSTI.

Bezpečnostní kultura

Veďte příkladem, nestrašte trestem!

- Bezpečnostní školení
- Mail-learning kampaň
- Plakáty
- Videa a workshopy



BESECURED

BESECURED

Zůstaňme v kontaktu.

Jakub Marek
+420603747804
info@besecured.online

Propojme se na LinkedInu

www.besecured.online