Čekání na Yettiho

aneb co před tím, a co potom

Jaromír Látal
info@datron.cz

Na co vlastně čekáme

- Všichni vědí, že to bude
- Jak to asi bude
- Ale nikdo to ve finále neviděl

Yetti =====> **Zákon o kybernetické bezpečnosti**
(vytvořený dle NIS2)

Co o něm „přesně” víme

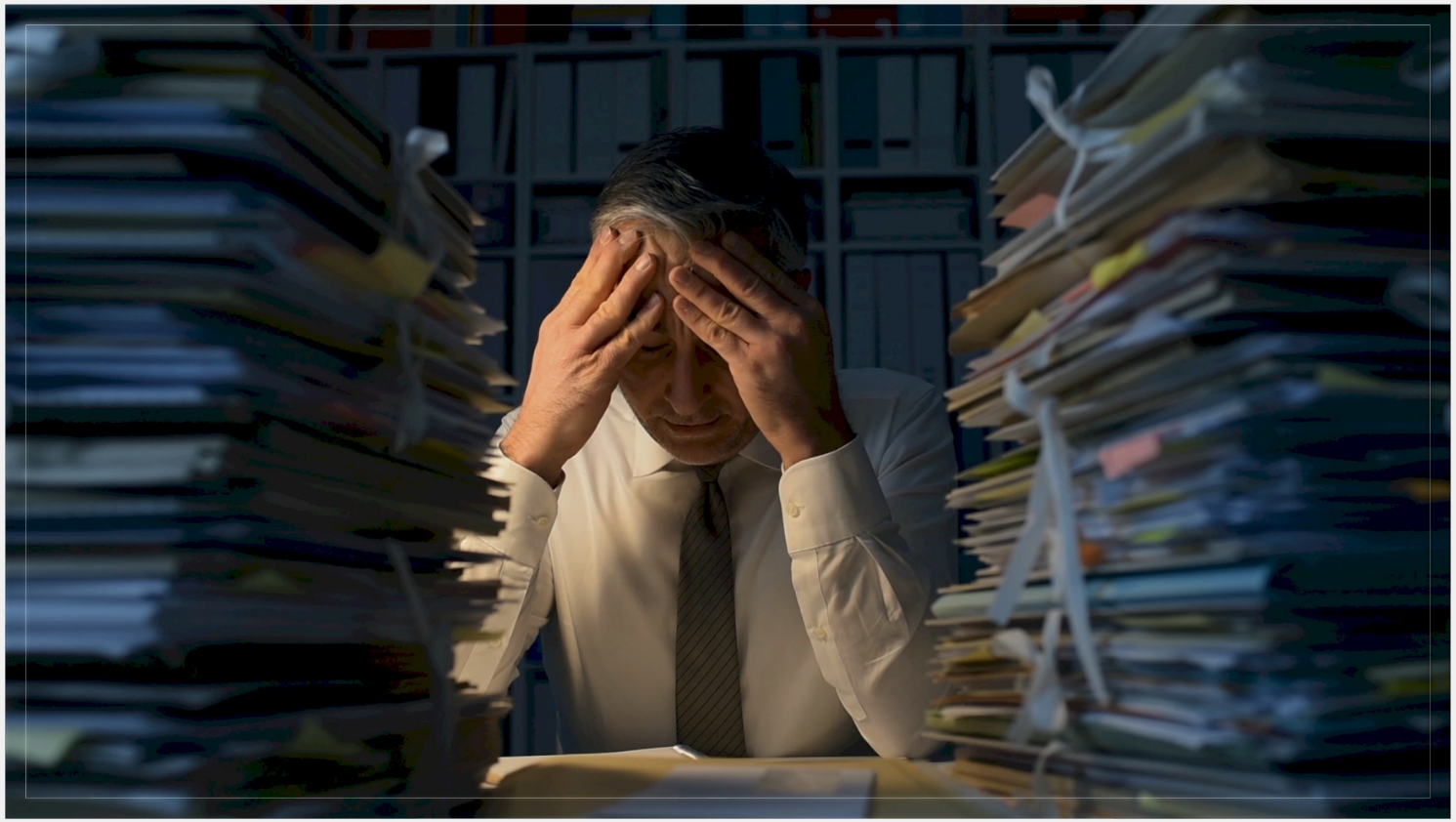
Vychází z NIS2 a navazuje na stávající Zákon o kybernetické bezpečnosti

Má zajistit zvýšení kybernetické bezpečnosti organizací, firem, úřadů a ostatních společností

Co o něm „asi“ víme

- Měl by platit od října 2024
- Budou vysoké sankce za neplnění
- Bude mít minimálně dvě úrovně
- Má na všechny zúčastněné poměrně hodně požadavků

Čím si zkrátit čekání



?

Zavádění opatření ke zvýšení kybernetické bezpečnosti

Bez ohledu na to, jestli do ZKB organizace „spadne“ nebo ne

Na základě všeobecných principů bezpečnostních norem

např. stávajícího Zákona o kybernetické bezpečnosti

Zavádět opatření v několika úrovních

- Analýza stavu
- Zavedení evidence stavu a hodnocení rizik
- Návrh opatření
- Zavádění „exekutivních“ výkonných nástrojů pro zvýšení kybernetické bezpečnosti

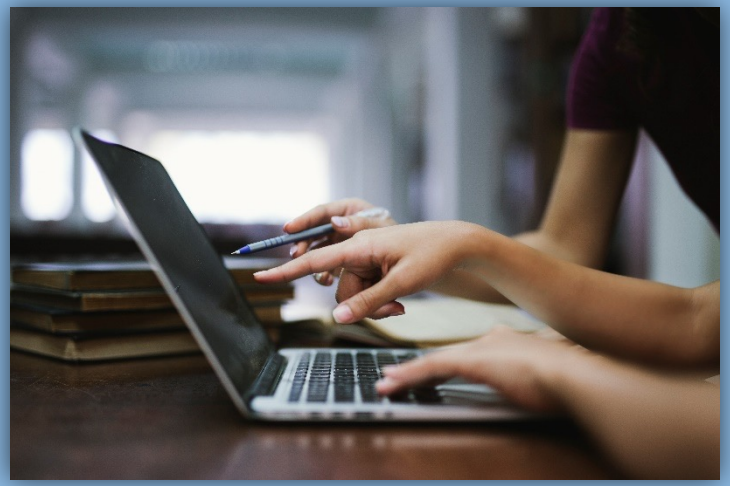
Zjišťování a analýza stavu

HealthCheck

- ověření stavu a funkčnosti informačních systémů a sítí

Vstupní analýza kyberbezpečnosti

- zjištění aktuálního stavu kybernetické bezpečnosti organizace
- popis a definice aktiv
- identifikace hlavních rizik, hrozeb a zranitelností, které mohou ohrozit informačních systémů a data



Zavedení evidence stavu a hodnocení rizik

Doporučujeme nasazení softwaru, který umožní automatizovat proces zavádění kybernetické bezpečnosti informačních systémů a dat

Software by měl obsahovat

- Detekce, analýza a řešení hrozeb
- Evidence a správa aktiv
- Evidence zranitelností, bezpečnostní událostí a incidentů
- Analýza a řešení rizik
- Zavedení Workflow procesů pro řízení rizik

- Evidence dokumentace (DR plány apod.)
- Evidence a vliv dodavatelů na jednotlivá aktiva
- Evidence a plán zavádění průběžného vzdělávání

Návrh a realizace konkrétních opatření

- Na základě zpracování informací z HealthChecku a analýzy kybernetické bezpečnosti
- Systému hodnocení rizik
- Zavádění „exekutivních“ – výkonných nástrojů pro zvýšení kybernetické bezpečnosti

Akceptace vyhlášky Kybernetického zákona

- Detekce, analýza a řešení hrozeb
- Evidence a správa aktiv
- Evidence zranitelností, bezpečnostní u[illegible] incidentů
- Analýza a řešení rizik
- Zavedení Workflow procesů pro řízení rizik
- Evidence dokumentace
- Evidence a vliv dodavatelů na jednotlivá aktiva
- Evidence a plán zavádění průběžného vzdělávání
- Všechna následně realizovaná opatření

Co může nabídnout DATRON, a.s.

Různé Varianty HealtChecku
- Standardní
- Individuální dle požadavků zákazníka

Vstupní analýzu kybernetické bezpečnosti
- Základní dle ZKB
- Individuální dle požadavků zákazníka

Komplexní evidenční systém: DAS - eCyS

Konzultační týmy
- Konzultanti, právník, etický hacker

Partneři

DAS eCYS

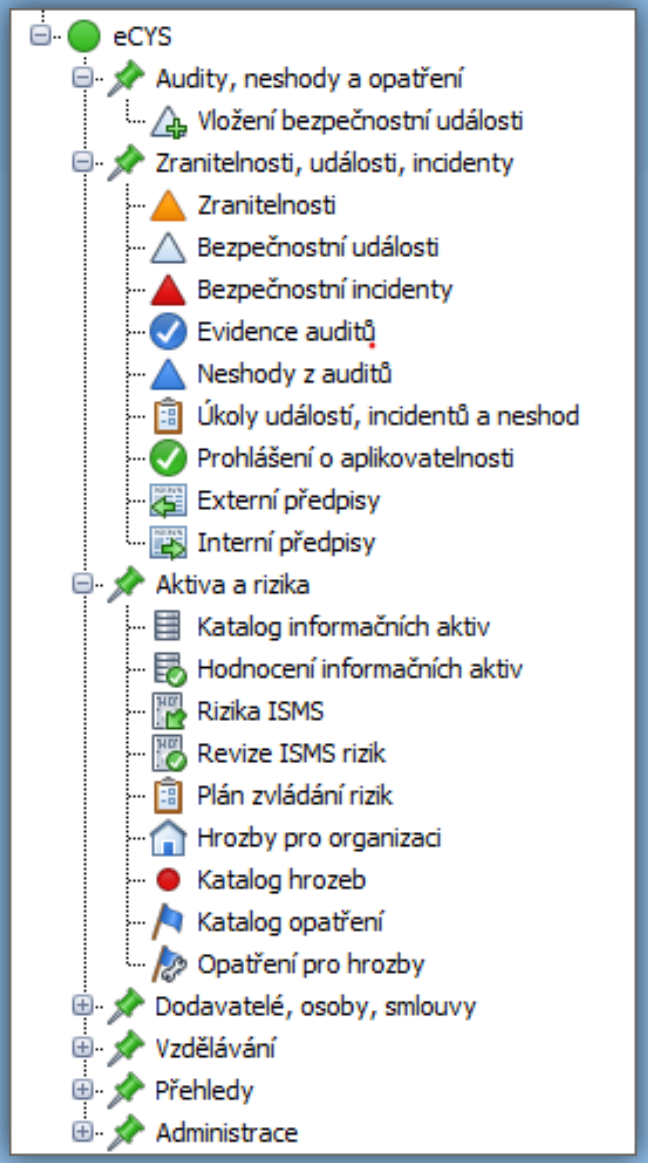
Systém pro komplexní evidenci a automatizaci bezpečnostních norem

Verze systému

- Projektová implementace včetně komplexní analýzy a napojení na další systémy
- Základní verze (krabice) pro vyšší povinnost
- Základní verze (krabice) pro nižší povinnost
- Hromadný cloudový prodej

Rozšiřující moduly

- Evidence dodavatelů a jejich vliv v rámci aktiv
- Evidence smluv
- Vzdělávání Kybernetické bezpečnosti
- Kurzy Kybernetické bezpečnosti



DATRON
INFORMATION TECHNOLOGIES

www.datron.cz I info@datron.cz