22. 9. 2021

ID: 113602

Je potřeba „přitvrdit“ v legislativě kybernetické bezpečnosti?

Na úvod si dovolím citovat sám sebe – Kybernetická a informační bezpečnost není otázkou zákonů, je otázkou pudu sebezáchovy – jednotlivců, firem, státních institucí, unií atd.

A jelikož život ukazuje, že pud sebezáchovy nefunguje, tak nastupuje přitvrzení legislativy.

V čem je problém a proč je to problém na úrovni EU?

Stávající evropská směrnice o bezpečnosti sítí a informací (NIS) přes nesporná pozitiva, která přinesla, už prostě nestačí. Zde stojí za zmínku, že český zákon 181/2014 Sb. o kybernetické bezpečnosti v době vydání této směrnice už existoval a když ostatní evropské země měly za povinnost přizpůsobit, některé země teprve zavést, svoji legislativu kybernetické bezpečnosti, tak ten náš se se směrnicí NIS shodoval z 95 procent.

Epidemie Covid-19 byla jedním z impulsů, které si revizi směrnice NIS vynutily. Živelný přechod do on-line světa, bezskrupulózní útoky na zdravotnická zařízení, útoky na distribuční kanály vakcín apod. vedly k závěrům, že něco je ne sice možná úplně špatně, ale také ne úplně dobře.

Na základě hodnocení fungování směrnice NIS byly při posouzení dopadů zjištěny následující problémy:

- nízká úroveň kybernetické odolnosti podniků a institucí působících v EU;
- nekonzistentní odolnost mezi členskými státy a odvětvími a nízká úroveň společného situačního povědomí a nedostatečná společná reakce na krize.

Konečně se stalo zřejmým i to, že například velké nemocnice v některých členských státech nespadají do oblasti působnosti směrnice o bezpečnosti sítí a informací a tím i pod národní legislativu, a proto nejsou povinny zavádět bezpečnostní opatření. A v jiné zemi téměř každá nemocnice v zemi je pokryta bezpečnostními požadavky NIS. Situace v České republice byla taková, že díky úsilí ministerstva zdravotnictví před účinností směrnice NIS pod zákon o kybernetické bezpečnosti nespadala žádná nemocnice, po její účinnosti jen 16 největších. Když už se nepovedlo to, že pod zmíněný zákon nespadá žádná, tak dobrá, jen ty největší. Díky novele legislativy kybernetické bezpečnosti se konečně dostalo pod zákon o kybernetické bezpečnosti až 46 zdravotnických zařízení. Ale i to je málo. Když si uvědomíme, že kybernetický útok na takovéto zařízení může mít fatální dopady, tak se odborníci úsilí Ministerstva zdravotnictví jen diví. Toto úsilí se vymstilo při útocích na nemocnice jako např. Benešovská nemocnice, Fakultní nemocnice Brno a další. A bohužel nejde jen o hmotné škody, které jen v těchto nemocnicích dosáhly stovek milionů korun, ale jde i o dopady na zdraví pacientů. V Německu byl dokumentován případ pacientky, která měla akutní zdravotní problém a sanitka ji vezla do nemocnice. Jenže ta byla pod hackerským útokem a tedy nefunkční. Sanitku museli odklonit do nemocnice o 32 kilometrů dál a ty minuty k záchraně pacientky prostě chyběly a zemřela. Tato nešťastná událost byla dána do přímé souvislosti s hackerským útokem na nemocnici.

Ale zpátky k revizi směrnice NIS, které se také říká NIS 2, co nového přináší?

Revize NIS předpokládá tři obecné cíle:

1. Zvýšit úroveň kybernetické odolnosti komplexního souboru firem a institucí působících v Evropské unii ve všech příslušných odvětvích zavedením pravidel, která zajistí, aby všechny veřejné a soukromé subjekty na vnitřním trhu, které plní důležité funkce pro hospodářství a společnost jako celek byly povinny přijmout odpovídající opatření v oblasti kybernetické bezpečnosti.

2. Omezit nesrovnalosti v odolnosti na vnitřním trhu v odvětvích, na která se směrnice již vztahuje, dalším sladěním

(1) de facto rozsahu,

(2) požadavků na bezpečnost a hlášení incidentů,

(3) ustanovení upravujících národní dohled a

(4) schopnosti příslušných orgánů v členských státech.

3. Zlepšit úroveň společného situačního povědomí a kolektivní schopnosti připravit se a reagovat přijetím opatření ke zvýšení úrovně důvěry mezi příslušnými orgány, sdílením více informací a stanovením pravidel a postupů v případě rozsáhlého incidentu nebo krize.

Odolnost v kybernetické bezpečnosti v celé Unii nemůže být účinná, pokud k ní bude přistupováno rozdílně prostřednictvím národních nebo regionálních hráčů.

Já osobně považuji za nejpodstatnější tyto oblasti:

Rozšíření seznamu odvětví, která „spadnou“ pod regulaci. Jsou to odvětví, která pod regulaci v této oblasti dosud nespadala. Podívejte se na konci článku na jejich výčet (není zde prostor pro rozebírání parametrů jednotlivých odvětví a pododvětví -např. přenášený výkon u distribuční soustavy apod.). Výčet považuji za podstatný, aby bylo zřejmé, jak obrovsky se rozšiřuje záběr legislativy kybernetické bezpečnosti a jak opravdu přituhuje. A jak tím roste i tlak na rozpočet na zajištění kybernetické a informační bezpečnosti nových osob povinných – cca o 12%. Pokud už to tedy mají alespoň v nějaké úrovni zavedeno a nečekají na průšvih, jak je naším národním zvykem. Ale také jak tím poroste hlad po odbornících na zavedení, řízení a rozvoj kybernetické bezpečnosti. Pokud si prohlédnete tento výčet, tak tam najdete řadu odvětví, která pod legislativu kybernetické bezpečnosti nikdy nepatřila. Např. výrobci a distributoři farmaceutických přípravků, výrobci automobilů, návěsů a přívěsů, výrobci počítačů, zdravotnických prostředků (to bude hodně zajímavé) a hodně se těším na regulaci poskytovatelů sociálních sítí.

Tímto výčtem ale revize NIS nekončí. Za zásadní považuji zdůraznění úlohy pečlivé analýzy rizik před jakoukoliv změnou nebo pořízením IT infrastruktury hlavně z pohledu kybernetické a informační bezpečnosti. Což znamená odklon od bezhlavého nakupování nejrůznějších bezpečnostních řešení jen proto, že se o nich mluví na konferencích. Tato řešení nakonec mají jediný efekt, že spotřebovávají elektrický proud a barevně blikají. Jedině pečlivá analýza rizik ve vztahu k službám, které firma nebo instituce poskytuje a k systémům, na kterých jsou tyto služby závislé, ukáže, jaká bezpečnostní opatření mají smysl. Když to přeženu, tak nedává smysl korunové hodnoty chránit milionovými opatřeními a naopak. A to vám ukáže právě analýza rizik.

Další zásadní moment jsou tzv. netechnické bezpečnostní požadavky. Díky NÚKIB, který na konferenci o 5G sítích v rámci tzv. Pražské iniciativy navrhnul tyto netechnické požadavky, se

dostaly i do revize NIS. Jde o to, že se nelze soustředit jen na technické (a bohužel i cenové) parametry bezpečnostních řešení, ale je nutno zvažovat i to, z jaké jurisdikce pochází výrobce nebo dodavatel těchto technologií a systémů, jaká je jeho vlastnická struktura, jestli není navázaný na zpravodajské služby nedemokratického režimu apod. Je třeba si uvědomit (a zase jsme u analýzy rizik) jaké informace vaší infrastrukturou potečou, jaké v ní budou zpracovávány, kdo s nimi bude pracovat. Přece byste nechtěli, aby k vašemu těžce vybudovanému know-how měla on-line přístup konkurence ze země, kterou autorská práva a ochrana duševního vlastnictví příliš netrápí.

Zaznamenal jsem i další posun, a to v tom, že se přestaneme soustředit na ochranu jednotlivých informačních systémů (no hurá), ale budeme budovat bezpečnou celkovou infrastrukturu. To znamená přesun od ochrany systémů k ochraně firmy – instituce. A to je dobře.

Převis poptávky nad nabídkou odborníků

Ještě jednou zdůrazním to, že očekávám obrovský převis poptávky nad nabídkou odborníků na kybernetickou a informační bezpečnost, a to možná ani tak ne v technických profesích jako spíše v těch manažerských. Budou chybět odborníci, kteří budou schopni kybernetickou a informační bezpečnost ve firmě nebo instituci zavést potom řídit a neustále rozvíjet. Budou chybět odborníci, kteří budou umět řídit rizika. Budou chybět architekti kybernetické bezpečnosti. Ale také budou chybět ti, kteří budou kontrolovat soulad s legislativou – u nás je to NÚKIB.

Dobře jsem si vybral svůj obor, je to nekonečný boj, nekonečný adrenalin.

Doporučuji vám to samé.

A nakonec je tady ten výčet – najdete se tam? A překvapí vás to?

Základní subjekty

1. Energetika
    a. elektřina
    b. dálkové vytápění a chlazení
    c. ropa
    d. zemní plyn
    e. vodík
2. Doprava
    a. letecká
    b. železniční
    c. vodní
    d. silniční
3. Bankovnictví
4. Infrastruktura finančních trhů
5. Zdravotnictví
6. Dodavatelé a distributoři vody určené k lidské spotřebě
7. Odpadní voda
8. Digitální infrastruktura
9. Veřejná správa (I regiony)
10. Vesmír

Důležité subjekty

1. Poštovní a kurýrní služby

2. Nakládání s odpady
3. Výroba, produkce a distribuce chemických látek
4. Výroba, zpracování a distribuce potravin
5. Výroba
    a. výroba zdravotnických prostředků a diagnostických zdravotnických prostředků *in vitro*
    b. výroba počítačů, elektronických a optických přístrojů a zařízení
    c. výroba elektrických zařízení
    d. výroba strojů a zařízení j. n
    e. výroba motorových vozidel, přívěsů a návěsů
6. Digitální poskytovatelé
        i. poskytovatelé on-line tržišť
        ii. poskytovatelé internetových vyhledávačů

poskytovatelé platforem služeb sociálních sítí

Ing. Aleš Špidla

Ing. Aleš Špidla je prezidentem Českého institutu manažerů informační bezpečnosti, garantem a pedagogem MBA programu „Management a kybernetická bezpečnost“ a spolugarantem a pedagogem LL.M. studijního programu „Ochrana informací“.

CEVRO Institut je soukromou vysokou školou práva, politologie, mezinárodních vztahů, ekonomie a bezpečnostních studií. Na českém vysokoškolském trhu působí více už čtrnáct let. Nabízí prestižní vzdělání, individuální přístup a špičkové vyučující. Vybrat si lze z bakalářských, magisterských i postgraduálních programů. Přednáší zde elitní profesoři i experti přicházející z praxe justice, veřejné správy a byznysu.

Postgraduálním program MBA Management a kybernetická bezpečnost, který nabízí soukromá vysoká škola CEVRO Institut, je určen pro klíčové manažery, bezpečnostní pracovníky a vedoucí pracovníky v ICT v soukromé i veřejné sféře se zaměřením na ochranu podnikové i státní IT infrastruktury a pochopení principů řízení kybernetické bezpečnosti. **Více informací o tomto programu naleznete ZDE.**

Postgraduální program LL.M. Ochrana informací nabízí právní a manažerské znalosti z oblasti ochrany informací, Compliance Managementu, trestní odpovědnosti právnických osob, kybernetické a informační bezpečnosti (ZKB), která je zaměřena na ochranu osobních údajů (GDPR), a elektronických identit (eIDAS). Díky špičkovým odborníkům budete po absolvování studia připraveni na výkon funkce Compliance Officer a Data Protection Officer. **Více informací o tomto programu naleznete ZDE.**

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- LLM online program PRÁVO & MEZINÁRODNÍ SEKTOR jako odpověď na rostoucí nároky globální právní praxe
- ČVUT už ušetřilo díky projektu EPC od ČEZ ESCO za energie přes 140 milionů korun
- Solkind: Když přátelství, společné hodnoty a specializace vytvoří novou sílu na advokátním trhu
- Po svátcích přichází vlna reklamací: Jaká práva mají spotřebitelé?
- D.A.S. posiluje svou roli lídra právní ochrany
- Teplo z elektrárny Mělník proudí do Prahy už 30 let. Spolehlivé dodávky do budoucnosti zajistí nízkoemisní zdroje
- Jak si zvolit sídlo pro OSVČ a firmy
- Agilita a umělá inteligence jako nové paradigma právních služeb: praxe AgiLawyer
- Řešení sporů z oblasti kryptoměn a digitálních aktiv u Rozhodčího soudu
- LLM Soukromé právo: Když se teorie mění v právní praxi
- SLUTO DAŇOVÁ & ÚČETNÍ firma roku 2025