30. 9. 2022

ID: 115320

Nová evropská legislativa v kybernetické bezpečnosti

O novele evropské směrnici o bezpečnosti sítí a informací (NIS2), která je probírána a propírána v odborné veřejnosti, již bylo řečeno mnohé, i když ne úplně vše. Postoj některých institucí je, že je lepší nevědět, anebo radši nedomýšlet.

O čem NIS2 je? Říká, že zajištění kybernetické a informační bezpečnosti je čím dál tím významnější součástí všech procesů v instituci. Nicméně **neustále platí, že kybernetická a informační bezpečnost není otázkou zákonů, ale je otázkou pudu sebezáchovy**. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) zřídil specializované internetové stránky, které se problematikou NIS2 a hlavně jejími dopady zabývají. Mezi nejvýznamnější změny podle vyjádření NÚKIB na zmíněných stránkách patří:

- rozšíření počtu povinných osob (odhady hovoří o nejméně 6 000 soukromých i státních organizacích), a to jednak rozšířením regulovaných odvětví (např. odvětví odpadového hospodářství), dále rozšířením stávajících regulovaných odvětví o nové regulované služby (např. stávající odvětví digitální infrastruktury o nové regulované služby cloud computingu nebo poskytovatele služeb a sítí elektronických komunikací), a nebo změnou způsobu identifikace povinných osob (kdy primárním kritériem pro zařazení do regulace bude velikost organizace);
- povinné vzdělávání vrcholového vedení organizace a větší odpovědnost managementu za zajišťování kybernetické bezpečnosti v organizaci;
- dobrovolné hlášení relevantních incidentů, událostí, hrozeb a zranitelností;
- podrobnější požadavky na vedení registru internetových domén nejvyšší úrovně a činnost registrátorů;
- větší důraz na sdílení informací mezi povinnými organizacemi;
- prohloubení spolupráce mezi regulátorem a povinnými organizacemi;
- významné zvýšení pokut za nedodržení uložených povinností (nově se stanovuje úroveň pokut až ve výši 2 % celkového obratu společnosti nebo 10 milionů EUR).

Co to bude znamenat v praxi, až vstoupí NIS2 na konci letošního roku v platnost? V první řadě během následujících 21 měsíců bude muset být harmonizována národní legislativa, která kybernetickou a informační bezpečnost reguluje, zejména tedy zákon 181/2014 Sb. o kybernetické bezpečnosti a navazující předpisy. Asi největší problém způsobí rozšíření počtu povinných osob, tedy těch institucí (firem, státních organizací) které tzv. spadnou pod zákon o kybernetické bezpečnosti.

Nárůst z cca 360 na 6000 způsobí obrovské zvýšení poptávky po odbornících na kybernetickou bezpečnost. Tím nejsou myšleni jen ti, kteří kybernetickou a informační bezpečnost řeší na technologické úrovni. Větší problém je v hledání těch, kteří umí kybernetickou a informační bezpečnost zavést, provozovat, řídit a neustále rozvíjet.

Takovéto odborníky žádná škola nevychovává, kromě jedné jediné což je Vysoká škola CEVRO Institut z.s. Kybernetická a informační bezpečnost není jen záležitost nasazení technických opatření, ale je i o změně procesů od těch řídících až po provozní. Proto je velmi důležitý i výše uvedený bod,

který hovoří o povinném vzdělávání vrcholového vedení organizace. Je velmi těžké přesvědčit vedení o tom, že něco neví a také o tom, že je tato oblast v jeho přímé a plné zodpovědnosti. Zaznamenal jsem velmi časté úporné snahy o to, přesunout zodpovědnost na nešťastníky z oddělení IT, což je naprosto zcestný postup. Problém je možná v tom, že i přesto, že škody způsobené zanedbáním kybernetické a informační bezpečnosti jdou do stovek milionů Kč (jen ve zdravotnictví), tak nikdo z vedení postižených organizací za to nebyl potrestán. A ne že bychom na to neměli použitelnou legislativu. Tak snad zvýšení pokut za zanedbání povinností bude to motivací pro vedení organizací. Pokud tedy bude pokuta někdy někomu udělena.

Další problém, který není v dopadech NIS2 na stránkách NÚKIB zmíněn, je odklon od bezhlavého nakupování „škatulí" (SIEMy, Firewaly apod) k zdůvodnění navrhovaných a aplikovaných opatření pečlivou analýzou rizik. A tady opět máme personální problém. Analýza rizik je nikdy nekončící proces, který se musí provádět pravidelně, a nebo při každé významné změně. Například přesunu vašich informačních systémů do cloudu musí předcházet velmi pečlivá analýza rizik. Ta by měla předcházet jakékoliv změně, která má vliv na procesy v organizaci. V některých případech stačí dokumentované mentální cvičení. Dobré ovšem je i při tomto mentálním cvičení držet se zásad řízení informačních rizik. Kdo to ale umí? Většinou jsem se ve své praxi setkal s „riskaři", kteří dokázali zpracovat analýzu rizik v případě povodní, požárů, zemětřesení apod. Informační rizika jim ovšem nic neříkají.

Takže lze opět očekávat velkou převahu poptávky nad nabídkou odborníků na řízení informačních rizik. Což znamená dovzdělat ty „klasické" odborníky na řízení rizik, ale hlavně začít vychovávat nové, orientované na informační rizika. Dá se totiž předpokládat, že každá střední až velká organizace je bude potřebovat mít na plný úvazek. Vzdělávací instituce tedy mají prostor k zamyšlení a také málo času k hledání pedagogů, kteří zvládnou vyučování problematiky řízení rizik. Ono to není jen o tom, nastudovat si literaturu. Je to i o praxi.

Ing. Aleš Špidla

Ing. Aleš Špidla je čestným předsedou 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.

Další studijní skupinu zahajujeme 25. listopadu 2022!

Další články:

- Prémiový rezidenční komplex Bakers Court přináší na realitní trh komfortní bydlení s 5* službami
- ESG Simple jako praktická opora pro ESG reporting malých a středních podniků
- Digitální důkazy z webu v soudním řízení: jak doložit, co bylo online zveřejněno?
- V lednu přišel šok. Ze seznamu zmizely tisíce soudních překladatelů
- Koupě nemovitosti v Rakousku: vedlejší náklady v praxi
- Legal Innovation Day 2026: Praktické využití umělé inteligence v právní praxi
- Prémiový rezidenční komplex Bakers Court přináší na realitní trh komfortní bydlení s 5* službami
- Festival jako prestižní teambuilding
- Spojení Generali České a Právní ochrany D.A.S. přináší první výhodu: navýšení pojistného limitu na 5 milionů
- Kultura jako prestižní benefit: Proč by právní firmy měly sázet na „inteligentní zážitky“? Rozhovor s JUDr. Martinou Jankovskou
- Wolters Kluwer uvádí na český trh AI právní pracovní prostor Libra s integrovaným obsahem ASPI