TISKOVÁ ZPRÁVA

Před hackerskými útoky se budou muset obrnit tisíce firem. Nařídí jim to poslanci

Riziko kybernetických hrozeb stále narůstá, kupříkladu počet útoků s cílem prolomit uživatelská hesla za minulý rok podle údajů Microsoftu vzrostl o 74 % a zejména požadavky na výkupné se v souvislosti s ransomwarovými útoky více než zdvojnásobily. Zvláště pro firmy, které neinvestují do odolnosti své digitální infrastruktury, to představuje značné riziko. Náprava škod po ransomwarovém útoku může firmy stát i desítky milionů korun, ale i ztrátu klientů a reputace jako takové. Zvýšit odolnost českých firem má nový zákon o kybernetické bezpečnosti, který pro tisíce firem definuje způsob, jak se chránit. Podrobnosti vysvětluje v komentáři Libor Šrám, odborník na kyberbezpečnost ze společnosti BDO.

Vznikající zákonná úprava vychází z evropské směrnice NIS2 přijaté v prosinci 2022, která zavazuje subjekty v rámci EU, aby zajistily bezpečnost svých sítí a informačních systémů. Tuzemský zákon, který aktuálně prochází připomínkovým řízením a s jehož účinností se předběžně počítá od druhé poloviny roku 2024, však bude v mnoha ohledech přísnější. Již nyní je navíc zřejmé, že se bude odhadem týkat minimálně šesti tisíc podniků, zatímco pod dosavadní zákon týkající se kybernetické bezpečnosti spadalo pouze okolo 400 subjektů. Spekuluje se zároveň o tom, že finální číslo může ještě o pár tisícovek narůst.

I malých firem se regulace může dotknout, zvláště když jsou v holdingu

Vznikající zákon o kybernetické bezpečnosti se bude týkat zejména odvětví energetiky, dopravy, zdravotnictví, nakládání s vodou a odpady. Dále se dotkne digitální infrastruktury a poskytování digitálních a ICT služeb, veřejné správy či výroby, zpracování a distribuce potravin. Stejně tak jako výroby počítačů nebo elektronických a optických zařízení. Podniky z těchto oblastí, které mají více než 50 zaměstnanců nebo dosahují ročního obratu alespoň 10 milionů euro (zhruba 250 milionů korun), mají téměř jisté, že se jich nová regulace bude týkat.

Kromě velkých a středních podniků by měly zbystřit i menší firmy, pokud jsou součástí holdingu. Zákon je totiž nebude posuzovat jednotlivě, ale spolu s ostatními firmami ve skupině jako celek.

Zákon se bude vztahovat i na všechny organizace, které jsou jedinými poskytovateli služby, která je nezbytná ze sociálního nebo ekonomického hlediska anebo by narušení jejich služby mohlo mít významný dopad na veřejnou bezpečnost, zdraví osob nebo by mohlo vyvolat významné riziko zejména s přeshraničním dopadem, a to bez ohledu na velikost.

Bezpečnostní procesy firem budou ověřovat inspektoři a pravidelný audit

Podniky si ze zákona budou muset stanovit rozsah řízení kybernetické bezpečnosti, konkrétně to bude znamenat například jasné určení bezpečnostních rolí, jako je manažer, auditor, architekt kyberbezpečnosti a garant aktiva. Rozsah opatření bude vždy záviset na tom, zdali podnik bude spadat do režimu vyšších, nebo nižších povinností. Do prvně zmíněné zákon rozřadí zpravidla 400 klíčových organizací, na které již nyní dohlíží stát a podléhají kybernetické regulaci. Ty budou muset zároveň řešit odolnost před kybernetickými hrozbami i u svého dodavatelského řetězce. Do režimu nižších povinností potom budou spadat všechny ostatní podniky, kterých se regulace dotkne.

Dále zákon přinese povinnost implementovat specifická bezpečnostní opatření s cílem zvýšit ochranu informačních systémů a dat. Tato opatření mohou být jak organizační formou procesů a politik, tak technická ve formě nástrojů pro zajištění bezpečnosti sítí, aplikací nebo datových úložišť.

Všechna bezpečnostní opatření budou ze zákona podléhat pravidelným auditům. U podniků v režimu nižších povinností je budou vykonávat pověření inspektoři, kteří budou muset složit certifikační zkoušku dle doplňkové vyhlášky o inspektorech, která mimo jiné definuje i nezbytně nutné vědomostní požadavky pro výkon funkce. V režimu vyšších povinností půjde přímo o inspektory dozorového orgánu, kterým je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Firmy také budou muset hlásit všechny zaznamenané kyberbezpečnostní útoky, a to právě NÚKIBu. Součástí tohoto incident managementu je i podávání zpráv o průběhu incidentu, jeho dopadech a protiopatřeních k jeho řešení a současně informování vlastních zákazníků.

Případné pokuty mohou dosahovat výše až čtvrt milionu korun

Při nedodržení zákonných povinností hrozí firmám sankce, které jsou rozlišeny podle režimu plnění povinností. Organizacím ve vyšším režimu hrozí za přestupek pokuta do 250 milionů korun, nebo do výše 2 % čistého celosvětového ročního obratu.

Subjekty v nižším režimu plnění povinností mohou dostat pokutu do 175 milionů Kč, nebo do výše 1,4 % čistého celosvětového ročního obratu. Rozhodující je v obou případech vyšší částka.

Autor: Libor Šrám, odborník na kyberbezpečnost ze společnosti BDO

TISKOVÁ ZPRÁVA

O společnosti BDO

BDO je poradenská společnost poskytující auditorské, daňové, právní, účetní a poradenské služby. Na českém trhu působí již 30 let. S více než 500 odborníky a dlouholetou praxí se řadí k předním společnostem s tímto zaměřením v České republice, kde má kanceláře v Praze, Plzni, Brně, Domažlicích, Českých Budějovicích a Jindřichově Hradci.

BDO je v České republice zastoupena společnostmi BDO Audit s.r.o., BDO Czech Republic s.r.o., BDO Consulting s.r.o., BDO Legal s.r.o., advokátní kancelář a BDO ZNALEX, s.r.o. Společnost je součástí mezinárodní sítě BDO, která celosvětově tvoří jednu z největších sítí auditorských a poradenských skupin. Zaměstnává více jak 91 tisíc odborníků a působí ve 167 zemích, v nichž čítá více než 1 650 kanceláří.

Kontakt:
Jan Kuliš, EPIC Public relations,
E-mail: jan.kulis@epicpr.cz
Tel.: +420 731 920 874,
Web: www.epicpr.cz