

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **85** ze dne **8.10.2024**

V kybernetické bezpečnosti jsme zaspali dobu

Když se podíváme na to, jaké narativy se v souvislosti s novým zákonem o kybernetické bezpečnosti objevují, najdeme několik opakujících se témat. Zákon přináší další byrokracii, je příliš přísný a Národní úřad pro kybernetickou bezpečnost (NÚKIB) si prý uzurpuje příliš vysoké pravomoci. Dále slýcháme o vysokých pokutách a o tom, kolik to firmy bude všechno stát a že už včera bylo na přípravu pozdě.

Ve veřejné diskuzi ale bohužel zaniká to podstatné. Jako společnost jsme zaspali dobu a stále se nedokážeme probudit. Řada firem kybernetickou bezpečnost řeší pouze formálně nebo dokonce vůbec. Dnes už přitom firmy více než zamčené a hlídané kanceláře potřebují zamčené a hlídané IT, protože veškerý firemní provoz se odehrává zde. Potřebují tedy vědět, jaké dveře dovnitř sítě vedou a které z nich jsou otevřené. A ty potom zavřít a zamknout. Pokud vám totiž dnes někdo z kanceláře ukradne počítače a osobní věci, není to taková ztráta, jako když vám hackeři zašifrují firemní data.

Samozřejmě najdeme hodně firem, které si rizika uvědomují a snaží se je minimalizovat. Mimochodem, pro ně je téma NIS2 celkem marginální, zvláště pokud se jich bude týkat režim nižších povinností. Ať totiž slýcháme cokoli, pokud někdo bude chtít pouze obstát u případné kontroly, zase tolik práce ho nečeká. Zákon je nyní nastavený tak, že při troše snahy umožňuje obstát i firmám, které nesplňují ani základní hranice kybernetické hygieny. A těch je překvapivě hodně. Vidíme to jak z naší praxe, tak z praxe dalších firem zabývajících se bezpečností, a můžeme to odvodit také z celé škály průzkumů, které téma kybernetické bezpečnosti pravidelně pokrývají.

Za firemní bezpečnost bude zodpovědné vedení

V této souvislosti je proto pozitivní, že alespoň u firem, kterých se bude nový zákon týkat, bude za kybernetickou bezpečnost a odolnost zodpovědné vedení, konkrétně statutární zástupce. A vedení se bude muset naučit, co firmě reálně hrozí. Pro mnohé to bude budiček, ale firmám to v konečném důsledku pomůže. Manažeři firemní bezpečnosti totiž dnes často narážejí na nepochopení ze strany vedení, které v těchto výdajích vidí pouze čistý náklad. Těžko se jim vysvětluje, proč mají nabírat další lidi, investovat do nákladných technických řešení a služeb externích specialistů nebo do nepopulárních interních opatření, jako je zákaz používání osobních telefonů a počítačů, zákaz instalace programů na firemních zařízeních už na úrovni operačního systému, nebo blokáce přístupu na sociální sítě či služby pro sdílení dat jako typu Dropbox. Doufejme, že od příštího roku, budou mít tyto diskuze zase o něco snazší.

NIS2 by měla vést ke změně myšlení

Vraťme se ale k tomu, co bychom si z diskuze ohledně NIS2 měli odnést především, a to je změna pohledu na IT bezpečnost, která by se měla stát přirozenou součástí uvažování firmy. Změna by měla začít u vedení a následně se propsat do celé firemní kultury. Všichni zaměstnanci by měli alespoň v obecné rovině vědět, co firmě může hrozit, jak mají poznat podezřelé aktivity a jak se mají a nemají chovat a proč. Taková změna je totiž nakonec tou nejúčinnější a nejlevnější ochranou před hackery, bez ohledu na to, jaká technická opatření ve firmě aktuálně fungují. Sama o sobě ji neochrání, ale výrazně zvýší účinnost jednotlivých opatření tím, že útočníkům omezí prostor pro jejich aktivity.

V této oblasti je přitom stále co zlepšovat. Pouze čtvrtina zaměstnanců má aktuálně pocit, že jejich zaměstnavatel dbá na to, aby měli přehled o digitálních hrozbách. Lidé z těchto firem si přitom nejen osvojují bezpečnější pracovní návyky, ale také dokážou lépe rozeznat pokročilé phishingové podvody i v osobním

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **85** ze dne **8.10.2024**

životě.

Pro celou naši společnost by proto dobré, aby v diskuzi ohledně NIS2 zaznívalo také to, proč je důležité brát kybernetickou bezpečnost vážně, proč vůbec zákon vzniká a že určitě máme co dohánět. Zda se regulace dotkne 6 tisíc firem, nebo 12 tisíc, jak tvrdý bude požadavek na prověřování dodavatelů a kolik papírů budou firmy potřebovat, je sice také důležité, ale zakrývá to podstatu celého problému. Tou je, jak jako společnost přistupujeme ke kybernetické bezpečnosti a jestli ji bereme dostatečně vážně. Roky se snažíme zvýšit finanční gramotnost, ale digitální gramotnost je podobně důležitá. Neměli bychom ji povinně vyučovat na školách? A jak zajistíme, abychom měli v budoucnu dostatek odborníků na oblast kybernetické bezpečnosti? Mimochodem, zákonu se mimo jiné vyčítá, že nedostatečně vyčísluje náklady na regulaci. Neměli bychom se ale bavit také o nákladech za neregulaci a pokračování v pštroší taktice schovávání se před hrozbami měnícího se světa?

Zdroj: AVcentrum ČR