Nový standard kybernetické bezpečnosti má dostat biliony dolarů z rukou hackerů

BEZPEČNOSTNÍ EXPERTI MLUVÍ O NOVÉ PODNIKATELSKÉ PŘÍLEŽITOSTI. FIRMY SE VŠAK SPÍŠE OBÁVAJÍ ZÁTĚŽE A DRAKONICKÝCH POKUT.

| Alžběta Vejvodová

Pohled na kybernetickou bezpečnost firem a institucí brzy dozná zásadních změn. Zatímco dosud muselo nejpřísnější zákonné požadavky plnit jen několik stovek podniků a institucí, nově jich budou tisíce. Nová úprava, kterou mají členské státy Evropské unie zanést do svého právního rámce do poloviny října, nastavuje zcela nový standard kybernetické bezpečnosti. Vyžádá si vznik desítek tisíc pracovních míst a otevře také nové příležitosti pro byznys. Česko je však zřejmě nebude moci naplno vytěžit. Potřební experti na zdejším trhu chybí.

„Pod novou regulaci spadne většina středních podniků a také státní správa," zdůrazňuje Hana Gawlasová, partnerka Deloitte Legal, která vede tým zaměřený na digitalizaci. Z pohledu povinností českých firem a institucí půjde o naprostou revoluci. „Taková úprava kybernetické bezpečnosti tady v českých luzích a hájích nikdy nebyla," upozorňuje lokální partner White & Case Tomáš Ščerba.

ČESKÉ FIRMY JAKO SLABÝ ČLÁNEK

IT systémy českých firem nyní patří k nejzranitelnějším v Evropě. Statistika společnosti Sophos ukázala, že v roce 2021 postihl vyděračský útok, při němž se hackeři snaží zablokovat důležitá data nebo informační systémy, 77 procent podniků. Hůře z evropských zemí dopadlo jen Rakousko s 84 procenty napadených z celkového počtu v zemi podnikajících firem. Na výkupném za uvolnění dat pak české firmy zaplatily v průměru přes 295 tisíc dolarů, tedy téměř 6,5 milionu korun.

„Existují případy malých rodinných firem, které zaplatily miliony korun. Data měly zašifrovaná několik týdnů, takže škodu navyšuje i ušlý zisk, kdy firmy nejsou schopny bez dat pracovat a dodržovat smluvní podmínky," popisuje konzultant Asociace malých a středních podniků v oblasti kybernetické bezpečnosti Martin Valdauf.

39 procent

uživatelů internetu se stalo terčem kybernetického útoku.

V nebývalé míře se do hackerských útoků po vypuknutí války na Ukrajině pustily i státy. „Cílem těchto útoků není někoho okrást, ale poškodit cílovou zemi, její infrastrukturu," upozorňuje Dalibor Kačmár, technologický ředitel společnosti Microsoft.

V posledních letech se také zvyšuje sofistikovanost útoků. Přibývá takových, kdy se útočníci do elektronických systémů nevlámou násilně, ale pomocí ukradené identity některého z uživatelů, kterou se běžně přihlásí. Takové útoky je přitom těžké odhalit.

Zisky útočníků z kybernetického zločinu celosvětově podle údajů společnosti Microsoft dosahují aktuálně šesti bilionů dolarů. A očekává se jejich další růst na 10 bilionů dolarů v roce 2025. „Tento nelegální byznys vykazuje principy standardního podnikání, ale na černém trhu. Má své dodavatele, odběratele a své řetězce," popisuje Kačmár. Některé skupiny v tomto řetězci se tak specializují čistě na krádeže identit, jež následně prodávají. Další skupiny „podnikatelů" se do systémů napadených organizací vlámou a ukradnou data. A ještě jiné subjekty pak ukradená data vytěží a zneužijí.

Vydírání napadených je přitom jen jednou z forem kybernetického zločinu. „Někdy útočníci napadený výpočetní prostředek využijí k těžbě kryptoměn. Nic neukradnou, nic nezničí. Ale napadený platí energii za těžbu a útočník odebírá vytěžené bitcoiny," uvádí obvyklý případ Kačmár.