Za kybernetický útok může nést odpovědnost i zaměstnanec

27.6.2022 - Věra Tůmová | INFOPROFI GROUP s.r.o.

Chránit firemní data je v době rostoucího počtu kybernetických incidentů stále těžší. Firmy, které kyberhrozby a zabezpečení proti nim podcení, se navíc vystavují možnému trestnímu postihu při úniku dat svých klientů. Kromě zabezpečení firemních sítí je však nutné dbát také na školení zaměstnanců. IT experti varují, že většině kybernetických incidentů se dá díky vzdělávání uživatelů vyvarovat. Právníci pak upozorňují, že je v případě pravidelných školení snazší určit, kdo za případnou škodu způsobenou kybernetickým útokem nese odpovědnost.

O firemní data se dá přijít hned několika způsoby. Na kyberútoku i zcizení dat se kromě hackerů mohou podílet úmyslně i neúmyslně také vlastní zaměstnanci. Firmy by proto ve svém vlastním zájmu měly nastavit základní pravidla kybernetické bezpečnosti. Zároveň by opatření pro zaměstnance měla být uživatelsky přívětivá a neměla by jim bránit v plynulé práci.

Cílem závažných hackerských útoků nebývají jen firmy, ale také stát a veřejné instituce. Připomeňme například útok vedený na portál veřejné správy spravovaný ministerstvem vnitra, web Úřadu vlády ČR, Českou televizi nebo Ředitelství silnic a dálnic.

Častou příčinou poškození či ztráty firemních dat bývá neopatrné chování uživatelů. Podle průzkumu společnosti Algotech si téměř tři čtvrtiny zaměstnanců odnášejí na nejrůznějších přenosových zařízení soubory mimo firmu. Zpravidla tak činí proto, aby mohli na projektech pracovat doma,

ojediněle pak vynášejí data za jiným účelem. Obojí je však špatně. „Každá firma by měla IT systémy a data zajistit jak fyzicky, aby je nemohl nikdo odnést, tak i virtuálně na úrovni firewallů, antivirových nástrojů, nástrojů na sledování sítě či pohybu dat v síti," konstatují experti Algotech. Vedle kvalitního IT zabezpečení je dnes už možné se proti kybernetickým incidentům i pojistit, jak uvádí advokát Ondřej Brostík: „Pojištění kybernetických rizik už nabízí na našem trhu řada pojišťoven."

Kdo za kyberútok nese odpovědnost? Firma, nebo zaměstnanec?

Při posuzování odpovědnosti za kybernetický incident je podle právních expertů rozhodující, zda má firma nastavená interní pravidla ohledně kybernetické bezpečnosti, zda je dodržuje a zda podle nich srozumitelně školí své zaměstnance. „Obsahují-li taková interní pravidla povinnosti i pro zaměstnance, jak se v konkrétních případech kybernetických hrozeb chovat, jaká bezpečnostní opatření přijmout a podobně, pak porušení takto stanovených povinností zaměstnancem by naplnilo předpoklady nedbalostního jednání zaměstnance. Bylo by pak možné, nárokovat i náhradu způsobené škody," varuje Brostík.

Příslušná česká právní úprava ovšem neupravuje podle právníků odpovědnost ve vztahu ke koncovému uživateli a je proto nutné postupovat v režimech civilní a trestní odpovědnosti. „V civilněprávní rovině by bylo v souvislosti s kybernetickými útoky možné aplikovat obecné pravidlo, že každá osoba včetně zaměstnance odpovídá za škodu, kterou způsobí svým zaviněným protiprávním jednáním." Takové zavinění zaměstnance by bylo ale nutné v konkrétním případě prokázat a reflektovat i další okolnosti případu (například zákonné omezení povinnosti k náhradě škody zaměstnance rovnající se maximálně čtyřapůlnásobku jeho průměrného měsíčního výdělku). „V trestní rovině bychom pak mohli hovořit o trestných činech obecného ohrožení či poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti," dodává Brostík.