

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **57** ze dne **30.1.2024**

Polovina firem vloni zažila kybernetický útok nebo incident, který jim znemožnil přístup k datům

Průzkum společnosti Dell Technologies hovoří jasně: roste náročnost ochrany dat i riziko výpadků IT a narušení bezpečnosti. Z dotazování mezi 1 500 IT manažery vyplynulo, že 90 % z nich se setkala s nějakou formou kyberútoku a že průměrné náklady spojené s útoky a souvisejícími incidenty meziročně vzrostly z 0,66 na 1,41 milionu USD.

"Data jsou v dnešním digitálním světě klíčová. To z nich dělá životně důležitý zdroj i prioritní cíl," uvedl Dermot O'Connell, seniorní viceprezident pro služby v regionu EMEA společnosti Dell Technologies. Právě nedostupnost dat byla důsledkem kyberútoků, jejichž obětí se v roce 2023 stala více než polovina firem.

Podle respondentů je narušení IT běžnou věcí, v uplynulém roce se s ním setkala naprostá většina z nich (90 %). Více než polovina útoků (55 %) začala prostřednictvím zaměstnanců. Uživatelé klikali na spam nebo phishingové e-maily a škodlivé odkazy, kompromitovali přihlašovací údaje, popřípadě byla napadena jejich mobilní zařízení. Vnější narušení bezpečnosti bylo nejčastější příčinou (40 %) ztráty dat nebo výpadku systémů.

Z pohledu čísel přišel v roce 2023 kyberútok, který zahrnoval ztrátu dat, v průměru na 2,61 milionu USD. V částce je započítáno 26 hodin neplánovaných odstávek a 2,45 TB dat. Náklady spojené s kybernetickými útoky a incidenty jako takovými se meziročně zdvojnásobily. Konkrétně z 0,66 milionu USD v roce 2022 na 1,41 milionu o rok později.

Generativní AI a kybernetická bezpečnost

Generativní umělá inteligence se stává strategickým nástrojem pro posílení obrany. Polovina dotázaných (52 %) uvedla, že integrace GenAI přinese jejich společnosti výhodu v oblasti kybernetické bezpečnosti. Nicméně 88 % respondentů se shodlo, že umělá inteligence bude generovat velké objemy nových dat. To ukazuje dvojsečnost GenAI; na jednu stranu je zdrojem vyšší bezpečnosti, na druhou pak vyšší složitosti. Stejně procento (88 %) souhlasilo s tím, že GenAI zvýší hodnotu konkrétních typů dat.

"Vzestup generativní umělé inteligence a rozšiřování fungování do hybridních a multicloudových prostředí staví do popředí zájmu společností kybernetickou odolnost a efektivní obnovu po incidentech," dodal Dermot O'Connell.

Pojištění proti vydírání nemusí krýt rizika

Pokud se podíváme na útoky ransomwaru, respektive na jejich následky, odpovědi naznačují přílišnou důvěřivost a optimismus. Tři čtvrtiny respondentů (74 %) věří, že v případě útoku dostanou po předání výkupného zpět všechna svá data. Dvě třetiny (66 %) jsou pak přesvědčeny, že po zaplacení již nebudou znovu napadeny.

Většina dotazovaných (93 %), resp. jejich organizací a firem má pojištění proti ransomwaru. Z odpovědí však plyne, že tyto pojistky mají řadu "ale". Například 57 % respondentů uvedlo, že jejich společnost musí pro pojištění prokázat "osvědčené postupy" (best practise) prevence kybernetických hrozeb. Zhruba dvě pětiny se setkaly s omezeným pojistným plněním (43 %) nebo dokonce zrušením pojistky (40 %) kvůli scénáři, jakým byl kyberútok proveden. Plnou náhradu od pojišťovny získalo pouhých 28 % napadených.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **57** ze dne **30.1.2024**

Údaje vyplývají z průzkumu Global Data Protection Index společnosti Dell Technologies vedeného mezi 1 000 IT manažery a 500 specialisty na IT bezpečnost.

Zdroj: AVcenturm ČR