

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **142** ze dne **6.5.2026**

Více než polovina IT profesionálů si myslí, že firmy přeceňují svou připravenost na kybernetický útok

Téměř tři čtvrtiny respondentů (74 %) uvedly, že se podle nich jejich organizace více soustředí na předcházení útokům než na přípravu na obnovu po incidentu. Zároveň zhruba čtvrtina (26 %) uvedla, že jejich organizace má robustní detekci hrozeb napříč primárním úložištěm, zálohami a sítí. Pro region EMEA také platí, že 43 % účastníků průzkumu připustilo, že jejich zálohy nejsou chráněné v takové míře, jako by měly být.

"Firmy a organizace v posledních zhruba deseti letech neustále zvyšují svou kybernetickou odolnost – nasazují pokročilejší firewally, sofistikovanější kontrolu identity a nyní se ve stále větší míře využívá AI. Přesto se pod povrchem může rozevírat nenápadná, ale nebezpečná mezera, tedy rozdíl mezi tím, z jakých útoků si organizace myslí, že se dokážou zotavit, a tím, jak se z bezpečnostních hrozeb reálně vzpamatují. A stejně jako každý neřešený dluh se v čase kumuluje a může se velmi bolestivě projevit při dalším vážném incidentu," řekl David Průša, data protection and cyber recovery solutions systems engineer z české pobočky Dell Technologies.

Bezpečnostní "dluh"

Studie také upozorňuje na takzvaný "resilience debt", tedy určitý dluh vůči úrovni kybernetické ochrany. "Jde o hromadění provozního rizika ve chvíli, kdy připravenost na obnovu nedrží krok s rostoucí komplexitou a vyspělostí kybernetických hrozeb. Průzkum Dell Global Cyber Resilience Insights ukazuje, že tento dluh není jen teoretický pojem, ale jde o reálnou situaci. Firmy by se proto měly zaměřit na to, aby jejich bezpečnost nebyla jen na papíře, ale dokázala odolat reálným útokům," doplnil David Průša.

Z globálních dat také vyplývá, co nejčastěji dluh vůči kybernetické odolnosti prohlubuje. Jedním z důležitých faktorů je pravidelné testování obnovy. Pro region EMEA platí, že podle průzkumu přibližně polovina organizací, které každý měsíc nebo častěji provádějí simulované kybernetické útoky, uvedla, že se dokázala z incidentů úspěšně zotavit.

Útoky míří stále častěji na zálohy

Globální data ukazují, že útočníci stále častěji míří přímo na zálohy – poškozují snapshoty, manipulují katalogy a zneužívají postupné odchylky v konfiguraci. Mnoho organizací přesto zálohy stále vnímá jako „nedotknutelné“, místo aby je chránily podobně jako produkční systémy. Dalším problémem je, že dokumentace a recovery playbooky zůstávají statické, zatímco prostředí, lidé i infrastruktura se rychle mění.

"Bezpečnostní dluh – například v podobě neopravených zranitelností nebo zastaralých bezpečnostních kontrol – dnes zná téměř každý. Dluh vůči kybernetické odolnosti je ale zrádnější v tom, že zůstává skrytý až do nejhorší možné chvíle, a to do okamžiku, kdy firmy skutečně potřebují obnovit provoz po útoku. Ty organizace, které k obnově přistupují strategicky, a ne pouze jako k provoznímu detailu na konci projektu, dosahují v praxi výrazně lepších výsledků než ty, které ji dál odsouvají na druhou kolej," dodal David Průša.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **142** ze dne **6.5.2026**

Cestu k vybudování robustní kybernetické odolnosti lze podle studie shrnout do tří kroků: Secure, Detect a Recover. V praxi to znamená posílit ochranu pomocí bezpečnostních kontrol na úrovni BIOSu, šifrování a izolovaných cyber vaultů, využít AI/ML pro detekci hrozeb napříč primárním i zálohovacím úložištěm a pravidelně testovat obnovu – ideálně alespoň jednou měsíčně.

AV centrum ČR