

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **13** ze dne **8.7.2022**

Až pětina organizací zažije výpadek provozu v důsledku ransomwarového útoku.

Acronis představil výsledky průzkumu, podle kterých 20 % českých organizací zažilo během posledních 12 měsíců výpadek provozu v důsledku ransomwarového útoku. Ransomwarovému útoku čelila zhruba polovina českých organizací, třetina útok dokázala odrazit, ve zbylých případech bohužel došlo k zašifrování dat a výpadkům provozu včetně aktuálně nejznámějšího případu Ředitelství silnic a dálnic (ŘSD).

Výpadky provozu po ransomwarovém útoku

Pokud se organizace stane terčem takového útoku, má řadu možností, jak se vyhnout nejhoršímu. Může jej například zcela bez následků odrazit s využitím antimalwaru či speciální ochrany proti ransomwaru. Pokud již dojde k zašifrování dat, stále mohou rychle obnovit provoz s pomocí disaster recovery či funkčních záloh. Jestliže ale selžou i zálohy, pak organizace musí čelit dlouhodobému výpadku provozu se všemi důsledky. Proto IT správci věnují speciální pozornost nejen ochraně ostrých dat ale také ochraně záloh.

Nejzajímavější zjištění průzkumu zahrnují:

- 47 % organizací se v posledních 12 měsících vůbec nesetkalo s ransomwarem, 33 % útok odrazilo, u 18 % došlo k zašifrování a krátkodobému výpadku, u 2 % došlo k zašifrování a dlouhodobému výpadku.
- Podle 61 % dotázaných IT správců je nejdůležitějším faktorem ochrany dat funkce nezměnitelnost záloh, 34 % uvedlo aktivní self-defense ochranu backup systému a 30 % umístění záloh v cloudu.
- 93 % IT odborníků zmínilo Windows systémy jako platformu, na kterou jsou nejvíce vedeny podobné útoky. Konkurenční macOS zmínilo jen 5 % IT správců.

"Nedávný útok na Ředitelství silnic a dálnic (ŘSD) ukázal, že dlouhodobý výpadek provozu následkem ransomwarového útoku není jen nějaké virtuální strašení," řekl Aleš Hok, obchodní ředitel společnosti ZEBRA SYSTEMS. "Podobné výpadky jsou obvykle důsledkem podcenění schopností útočníků a přecenění spolehlivosti stávajících záloh. Proto doporučujeme chránit zálohy například funkcí zajišťující jejich nezměnitelnost a pravidelně je testovat na obnovu."

Zdroj: AVcentrum ČR