Tři čtvrtiny firem nezálohuje data jinde než v cloudu. Chyba, říká Gajdošech ze Solitey

**Až tři čtvrtiny firem, které svou IT infrastrukturu či správu dokumentů řeší pomocí cloudu, nezálohují svá data na žádném jiném úložišti. Podle experta na IT bezpečnost Petra Gajdošecha z mezinárodní technologické skupiny** [**Solitea**](https://solitea.com)**, která se na cloudová řešení specializuje, se tím firmy vystavují velkému riziku finančních, obchodních či reputačních ztrát. Firmy totiž podle experta často žijí firmy v omylu, že cloud je “neprůstřelný” a hackeři ho nemohou napadnout.**

Jako příklad uvádí zkušenost s mezinárodní firmou s více než 45 pobočkami. Ta Soliteu oslovila v letos v létě s tím, že její cloudovou infrastrukturu zablokoval kybernetický útok. Nefungovaly emaily, dokumenty.

„Přitom stačilo pravidelně data zálohovat například na separátní úložiště mimo cloud nebo i na separátním cloudu. Firmu by útok tolik neparalyzoval a hackeři by měli částečně smůlu,” vysvětluje Gajdošech.

V reakci na útok byla výše zmíněná firma nucená fungovat šest týdnů offline. Musela celou infrastrukturu vyměnit a znovu postavit, včetně serverů, síťových prvků i počítačů svých pracovníků.

„Cloud se dnes prezentuje jako velmi bezpečná IT infrastruktura. To je samozřejmě pravda. Poskytovatelé navíc řešení neustále vylepšují právě proto, aby se bezpečnost ještě zvyšovala. Přesto ani cloud není zcela bez rizika. Útočníci se každým dnem učí nové triky a většinou nemají moc dobré úmysly. Všem firmám, pro které pracujeme, proto důrazně radíme, aby si data ještě separátně zálohovaly, a tuto možnost jim nabízíme,” dodává Gajdošech.

Firem, které mají data na cloudu a podceňují jejich zálohování, je podle odhadů Solitey kolem 75 %.

Gajdošech dále vysvětluje, že cloudová úložiště data tzv. zrcadlí. To znamená, že stejná data ukládá na dvou různých serverovnách. Tento mechanismus ale dle jeho slov pouze vyvolává mylný pocit, že jsou data zálohovaná. Zrcadlově uložená data jsou totiž propojená a útoku nemusí uniknout ani jedno z umístění.

Aby se předešlo proniknutí útočníků i do záloh, je nutné, aby tyto zálohy byly oddělené od ostatních systémů a aby na ně ideálně nebyl přístup z internetu ani ostatních interních sítí. Zkrátka, aby aby byly zálohy izolované od sítí, do kterých by se hackeři mohlo dostat. Jak zmínil Gajdošech, může se ale jednat i o druhé cloudové uložiště, které by ale nemělo být s tím prvním propojené a měl by k němu mít přístup například jen správce sítí.

Záložní data navíc mohou být vybavená softwarem, který umožňuje pouze jejich čtení a neumožní jejich přepis nebo zašifrování. Existují také moderní řešení proti vyděračským útokům, které pracují na bázi umělé inteligence. Ta sleduje chování aplikací a zařízení, které se pokoušejí o úpravu dat v počítači nebo na serverech. Pokud je chování vyhodnoceno jako podezřelé, proces je pozastaven. Stane se tak například, jestliže se začnou šifrovat určité typy souborů. Uživatel dostane informaci o takovém chování aplikace a má na výběr, zda jí přesto povolí činnost, nebo potvrdí její zablokování.