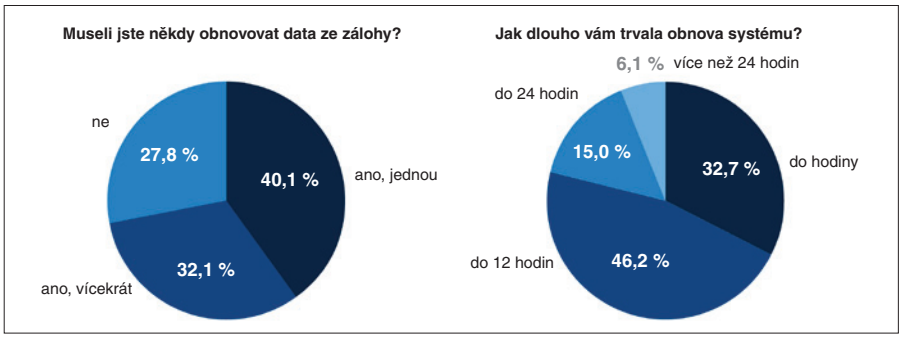
Kybernetickou ochranu průmyslových podniků je třeba integrovat do jednoho systému

Kybernetické útoky často vnímáme, jako by to bylo něco jako přírodní katastrofy, které se stávají druhým, ale nám ne. Takto uvažuje i mnoho manažerů průmyslových podniků, kteří se utěšují tím, že kybernetičtí útočníci se přece zaměřují hlavně na zdravotnictví, veřejnou správu či bankovnictví. To je ale nepochopení situace: útočníci jdou tam, kde mohou potenciálně způsobit nejvíce škody a potom žádat co nejvyšší výkupné. A to jsou i průmyslové a energetické podniky.

Například letos se stala terčem útoku americká společnost Colonial Pipeline, která prostřednictvím potrubí vedoucího z Houstonu do New Yorku zásobuje palivem 45 % východního pobřeží USA. Poté, co bylo zašifrováno více než 100 GB provozních dat, firma musela odstavit své počítačové systémy, zastavit provoz ropovodu a zajistit náhradní zásobování s využitím kamionů a cisteren.

Dobrá zpráva je, že již 90 % běžných uživatelů IT zálohuje svá data, přičemž 72 % se již muselo někdy spolehnout na obnovu dat z těchto záloh. Avšak pouze třetina zmíněných uživatelů dokázala obnovit přístup ke svým datům do jedné hodiny, což značí problémy s procesem obnovy, jehož rychlost a spolehlivost jsou pro uživatele ještě důležitější než samostatné zálohování (*obr. 1*).



Obr. 1. Již 90 % běžných uživatelů IT zálohuje svá data, přičemž 72 % se již muselo někdy spolehnout na obnovu dat z těchto záloh

Tehdejší odhady hovořily o tom, že systémy a provoz se podaří plně obnovit nejdříve za šestnáct dní. Výkupné, náklady na obnovu a ani obchodní ztráty nebyly zveřejněny, ale lze předpokládat, že jsou enormní.

Pro příklad z tuzemska není nutné chodit daleko do historie – na konci roku 2019 postihl kybernetický útok také společnost OKD.

Z útoků na kritickou průmyslovou infrastrukturu vyplývají ponaučení pro celé průmyslové odvětví, které si nemůže dovolit dlouhé výpadky. Zaprvé je to pravidelné zálohování dat a možnost okamžité obnovy, zadruhé posílení kybernetické bezpečnosti tak, aby zálohy byly v bezpečí a nemohly být zničeny.

Průzkum uživatelů a správců IT

Letošní zjištění společnosti Acronis, která vyplynula z dotazování více než 4 400 uživatelů a administrátorů IT z 22 zemí celého světa, ukazují, že stále více běžných uživatelů sice zálohuje, ale nemá představu o tom, jak dlouho by trvala obnova dat v případě jejich ztráty či zašifrování. A pouze menšina administrátorů zodpovědných za bezproblémovou kontinuitu podnikových systémů testuje systémy obnovy alespoň jednou měsíčně.

Obr. 2. Celkem 86 % administrátorů testuje obnovu dat ze zálohy alespoň jednou za tři měsíce

Na rozdíl od běžných uživatelů si profesionálové v oboru IT plně uvědomují, že nejen časté zálohování, ale i úspěšná obnova systémů jsou klíčem k zachování obchodní kontinuity a produktivity. Pro většinu administrátorů IT to znamená, že musí proces obnovy systémů pravidelně testovat, aby se ujistili, že v případě potřeby proběhne v pořádku. Celkem 86 % z nich obnovu testuje alespoň jednou za tři měsíce a stále více z nich svou testovací frekvenci zvyšuje na jednou měsíčně až jednou týdně (*obr. 2*).

Mnoho administrátorů IT se vedle zálohování a obnovy též zaměřuje na kybernetickou ochranu spravovaných systémů – důvodem je hlavně to, že polovina z nich zažila v uplynulém roce ztrátu dat, často vlivem kybernetického útoku, vedoucí k zastavení provozu organizace. To, kolik času a finančních prostředků je investováno do údržby těchto systémů a řešení případných provozních výpadků, svědčí o nízké efektivitě jejich správy. Ve srovnání s loňským rokem počet organizací s utrpěnou ztrátou dat vzrostl o 7 %, zatímco o rok dříve činil nárůst 11 %.

Doporučení: sjednotit bezpečnost do jednoho systému

Jedním z nejčastěji zmiňovaných důvodů této situace je, že téměř každý administrátor IT musí při své práci používat stále více různých systémů a časem ztrácí přehled o celkové úrovni zabezpečení organizace. Nejenže si musí pamatovat, které systémy zabezpečují kterou část infrastruktury IT, ale navíc musí neustále přepínat mezi ovládacími panely, což vede k nepřehledné a neefektivní správě.

A protože problémy ochrany a zabezpečení dat, aplikací a systémů v postpandemickém světě pouze porostou, musí se průmyslové organizace účinně bránit. Acronis doporučuje pět jednoduchých kroků:

První je *vytvořit zálohy důležitých dat* a zároveň udržovat několik kopií, např. jednu lokálně pro případnou rychlou obnovu a jednu mimo firmu, nejlépe v cloudu, pro případ poškození lokálních dat včetně jejich zálohy.

Druhý krok je *aktualizovat operační systémy a aplikace*. Neaktualizované systémy a aplikace nemají bezpečnostní záplaty, které brání hackerům v úspěšném útoku. Pravidelné záplatování pomůže vyhnout se těmto problémům.

Třetí krok je *eliminovat podezřelé e-maily, odkazy a přílohy*. Většina malwarových infekcí je výsledkem technik sociálního inženýrství, které přimějí uživatele otevřít nakažené přílohy či kliknout na webové odkazy s malwarovou infekcí.

Začtvrté, *instalovat antivirové, antimalwarové a antiransomwarové systémy*. Měly by to být systémy umožňující automatizované aktualizace na bázi umělé inteligence, které jsou účinné proti útokům typu *zero day*.

A nakonec, zvážit použití *uceleného řešení kybernetické ochrany*, které integruje všechny zmíněné prvky efektivní obrany pod jednou centrální správou.

Aleš Hok, obchodní ředitel
ZEBRA SYSTEMS