

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo 74 ze dne 2.7.2024

Jakou hodnotu mají vaše data?

Předpokladem efektivního zabezpečení je analýza rizik a vyčíslení jejich hodnoty.

Mezi nejobávanější dopady kybernetických útoků patří výpadky provozu klíčových systémů a ztráta či odcizení důležitých dat. Ale zatímco následky narušení provozu firmy asi dokážeme (alespoň přibližně) vyčíslit, jak ocenit podniková data?

Moderní technická řešení nabízejí vysokou úroveň kybernetického zabezpečení před různými typy útoků. Jak sofistikovanou (a nákladnou) ochranu ve skutečnosti potřebujete, ale nemůžete zjistit bez analýzy možných rizik. V některých případech to jde snadno. Například e-shop z historie objednávek celkem jednoduše spočítá, o kolik přichází každou hodinu výpadku kvůli kyberútoku. Podobně to umí vyčíslit výrobní závody nebo poskytovatelé on-line služeb. Na základě těchto výpočtů je pak možné stanovit rámec investice do kybernetického zabezpečení, která bude odpovídat potenciálním škodám.

"Kybernetické zabezpečení můžeme vnímat podobně jako pojištění nemovitosti proti živelním pohromám či vykradení. Nemovitost a věci v ní mají nějakou odhadovanou hodnotu, a od té se odvíjí výše pojistky. V kyberbezpečnosti je to podobné, jen výpočet hodnoty nehmatatelných, digitálních dat nemusí být vždy úplně snadný. Firmy se proto někdy dopouštějí chyby a přeceňují hodnotu fyzického majetku právě na úkor dat," vysvětluje Milan Ryšavý, architekt kybernetické bezpečnosti ve společnosti Seyfor.

Ve skutečnosti ale právě data dnes ve většině podniků představují největší část jejich majetku a současně i naprosto nezbytný prostředek pro každodenní fungování. I proto musí být identifikace konkrétních typů informací a jejich hodnoty nedílnou součástí efektivní přípravy na kyberútoky. Hodnotu dat je přitom zapotřebí posuzovat jak z hlediska jejich dostupnosti, tak i z hlediska jejich kompromitace. Taktika útočníků, kteří cílí primárně na data, se totiž mění: **"Zatímco dříve byla data napadené organizace zašifrována ransomwarem a útočník na oběti vymáhal výkupné za jejich opětovné zpřístupnění, dnes dochází při většině ransomwarových útoků i k likvidaci dostupných záloh a především k odcizení podnikových dat. Kyberzločinci tak znemožní firmě obnovu dat vlastními silami a navíc mají další páku v jednání o zaplacení výkupného – hrozí totiž, že odcizená data zveřejní na internetu,"** popisuje evoluci praktik kyberzločinců Milan Ryšavý.

Aby firma věděla, jaká data vlastně potřebuje před zničením nebo odcizením chránit, musí začít s identifikací informací a určením jejich hodnoty. Od toho se pak bude odvíjet i úroveň jejich ochrany a související investice. Základním krokem je roztřídění informací do několika úrovní – od těch nejméně důležitých až po nejcitlivější informace, bez kterých nemůže firma fungovat. Současně je také nutné data kvantifikovat a udělat si představu, jak rychle poroste jejich množství. Například data z různých senzorů (třeba o pohybu firemních vozidel) mohou růst obrovskou rychlostí, ale jejich důležitost není tak značná, aby na ně bylo nutné aplikovat nejvyšší stupeň zabezpečení a robustní zálohování. Narozdíl třeba od dokumentů souvisejících s podnikovým know-how, údajů o zákaznících nebo finančních dat, jejichž objem sice roste pomaleji, ale zato mají strategický význam a vyžadují nejvyšší úroveň ochrany.

"Identifikace a klasifikace informací v rámci podniku je klíčová nejen kvůli návrhu vhodných bezpečnostních opatření, ale také kvůli splnění legislativních požadavků. Klasifikace dat a jejich ochrana je totiž i jednou z klíčových oblastí řešených v připravované novele zákona o kybernetické bezpečnosti na základě směrnice NIS2," upozorňuje Milan Ryšavý na nové povinnosti, které bude novelizovaný zákon ukládat poskytovatelům regulovaných služeb.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **74** ze dne **2.7.2024**

Úkolem bezpečnostních opatření na ochranu dat je zajistit nejen jejich dostupnost a možnosti obnovy v případě úspěšného útoku, ale také jejich integritu (neměnnost) a důvěrnost nejen při zpracování a ukládání v podnikových systémech, ale i během přenosu po internetu. "Ochrana veškerých dat na nejvyšší úrovni by pro organizaci znamenala náklady zdaleka převyšující možná rizika. Proto je hlavním úkolem analýzy rizik stanovit hodnotu konkrétních informací a následně zvolit adekvátní způsob a úroveň jejich ochrany, který bude odpovídat potenciálním škodám. Zpravidla se to neobejde bez konzultací se specialisty, kteří pomohou jak s klasifikací dat, tak i s návrhem vhodných opatření," dodává Milan Ryšavý.

Zdroj: AVcentrum ČR