

Náklady na kyberútoky můžou vaši firmu zruinovat, říká Kaspersky

20.9.2024 - | PROTEXT

Největším problémem jsou finanční ztráty. Příkladem je útok na společnost Johnson Controls, významného hráče v odvětví stavebních technologií, která čelila rozsáhlému ransomwarovému útoku spáchanému skupinou Dark Angels. Útočníci tvrdili, že ukradli 27 terabytů citlivých dat, a požadovali výkupné 51 milionů dolarů. Útok měl za následek vážné narušení systémů společnosti a škodu ve výši víc než 27 milionů dolarů.

Útok ovlivnil i obchodní operace společnosti, včetně narušení fakturačních systémů a zvýšených nákladů na obnovu provozu. Jelikož se jde o společnost s celosvětovou působností, dotklo se to významně i obchodních vztahů a činností dalších firem.

Jak může kyberútok poškodit vaši firmu:

Finanční ztráty

Kybernetické útoky mají často za následek přímé finanční ztráty. Jasným příkladem jsou ransomwarové útoky, kdy hackeři požadují platbu za obnovení přístupu k datům, nebo přímé krádeže finančních prostředků. To je však pouze začátek, protože v důsledku toho může dojít k významným nepřímým finančním ztrátám. Ty mohou snadno přesáhnout částku, o kterou společnost přišla přímo kvůli incidentu.

Narušení provozu

Kybernetické útoky mohou zablokovat váš provoz. Mnoho firem je při své každodenní činnosti závislých na digitální infrastruktuře. Pokud jsou tyto systémy ohroženy, klesá produktivita. V závažných případech může dojít k narušení celého provozu na několik dnů nebo dokonce týdnů, což má za následek ztrátu příjmů, snížení kvality služeb, zklamání klientů a partnerů a s tím související další dopady na reputaci vaší firmy.

Nepřímé dlouhodobé náklady

I po bezprostřední likvidaci následků kybernetického útoku se firmy často potýkají s dlouhodobými finančními dopady. Obnova systémů, zlepšení infrastruktury kybernetické bezpečnosti a řešení právních následků jsou jen některé z přetrvávajících nákladů. Kromě toho může trvat měsíce nebo i roky, než se vykompenzují ztracené obchodní příležitosti a napraví poškozené vztahy se zákazníky.

Poškození pověsti

Důvěra vašich zákazníků je neocenitelná. Pokud však dojde k odcizení jejich dat, může to vážně poškodit pověst vaší značky. Tato ztráta důvěry může vést k odchodu zákazníků a dlouhodobému poklesu obchodování. V některých případech stačí jediné narušení k tomu, aby se obraz společnosti v očích veřejnosti nenapravitelně pokazil.

Pokud se vaše firma stane obětí útoku, může to mít dopad i na vaše vztahy s partnery a dodavateli. Partneři třetích stran mohou ztratit důvěru ve vaši schopnost chránit sdílené údaje. Stejně tak mohou být narušeny vztahy důležité pro podnikání, pokud se vám nepodaří rychle obnovit provoz nebo pokud vaše systémy dokonce ohroží činnost partnerů.

Právní otázky a dodržování předpisů

S ohledem na předpisy o ochraně údajů, jako je GDPR v Evropě nebo HIPAA v USA, může firma při úniku dat čelit vysokým pokutám. Neochránění citlivých údajů zákazníků nebo zaměstnanců může vést k sankcím a soudním sporům. Společnosti, které se stanou obětí narušení bezpečnosti, se navíc musí často potýkat se zdoluhavými právními spory, které zvyšují finanční zátěž a ohrožují jejich pověst.

Ztráta duševního vlastnictví

Pro mnoho firem patří duševní vlastnictví (IP) k jejich nejcennějším aktivům. Kybernetické útoky zaměřené na duševní vlastnictví mohou ukrást návrhy produktů, marketingové strategie nebo unikátní informace. To působí škody zejména ve vysoce konkurenčních odvětvích, jako jsou moderní technologie a farmaceutický průmysl, kde krádež duševního vlastnictví může zničit výhodu, kterou firma léta budovala.

Kaspersky k ochraně firem před kyberhrozbami doporučuje následující:

<https://www.ceskenoviny.cz/tiskove/zpravy/naklady-na-kyberutoky-muzou-vasi-firmu-zruinovat-rika-kaspersky/2571145>