

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **75** ze dne **20.7.2024**

Ransomwarovému útoku vloni čelilo 20 % českých firem

Průzkum společnosti Sophos, který mapuje reálné zkušenosti českých firem s ransomwarovými útoky a dopady těchto útoků na jejich podnikání v roce 2023, odhalil, že tři pětiny firem loni čelily nějakému kybernetickému útoku a každá pátá pak byla napadena ransomwarem. Odpovídající bezpečnostní opatření nemělo v době útoku zavedeno 15 % napadených společností a zaplatilo výkupné.

Rozsah kybernetických útoků na podniky je značný. Téměř 60 % českých společností v roce 2023 čelilo nějakému kybernetickému útoku, přičemž každá pátá se stala obětí útoku ransomwaru. Zatímco v regionu Evropa, Amerika, Asie a Tichomoří je procento útoků ransomwaru stejné jako v Čechách (59 %), v Polsku a Maďarsku, kde ransomware zasáhl 20 %, resp. sedm procent společností, je situace lepší. Dosud bylo ransomwarem napadeno 41 % českých firem.

Třicet šest procent českých společností prohlašuje, že ačkoli k útoku na ně ještě nedošlo, jsou si vědomy, že by k němu dříve či později dojít mohlo. Naopak celých 29 % dotázaných odpovědělo, že jejich společnost v minulosti kybernetický útok nezažila a nepředpokládají takovou situaci ani v budoucnu. Zkušenosti i očekávání kybernetického útoku se častěji objevují ve větších firmách. Ty menší mají s útoky ojedinělé zkušenosti a ani se jimi necítí být ohroženy.

Českým firmám se podařilo loni zmařit 39 % útoků ransomwaru, protože útok byl zastaven ještě před zašifrováním dat. Ve více než polovině případů se ale kyberzločincům povedlo data zašifrovat (53 %) nebo k datům alespoň získali přístup (6 %). Z průzkumu společnosti Sophos vyplývá, že firmám v Maďarsku se více daří útoky ransomwaru zastavovat (67 % pokusů), zatímco v Polsku tak firmy úspěšné nejsou a mají shodné skóre s českými podniky (39 %).

Zranitelnosti a phishing - hlavní brány do podnikových systémů

Třetina (34 %) českých společností uvedla zneužití zranitelnosti systému za hlavní zdroj útoků. Bezpečnostní chyby v podnikových systémech jsou celosvětově nejčastější příčinou útoků ransomwaru, selhávají ve 26 % případů. Druhým nejčastějším zdrojem útoků ransomwaru na české firmy byl loni phishing (24 %). Jde o typ online podvodu založený na hromadném šíření zpráv prostřednictvím e-mailu nebo SMS, při kterém se pachatel vydává za jinou osobu nebo instituci s cílem vylákat důvěrné údaje.

České firmy mezi prvotními příčinami ransomwarových útoků uvedly také nelegálně získané přihlašovací údaje (23 %) a interní zdroje včetně nekalého jednání zaměstnanců nebo neoprávněného přístupu (10 %). V šesti procentech případů se zdroj útoku nepodařilo identifikovat.

"Prostředí hrozeb se neustále mění, ale zločinci i nadále používají metody, které nejlépe fungují, jako je například phishing. Průzkum ukázal, že v případě ransomwarových útoků na firmy jde o nejčastější vstupní bránu do systému. Jedním z klíčových bezpečnostních opatření pro firmy je proto nevyhnutelně vzdělávání. Tým by měl být co nejlépe obeznámen s hrozbami a způsoby ochrany a měl by si všimnout všech varovných signálů, že by mohlo být něco v nepořádku. Rovněž doporučujeme provádět pravidelná cvičení a simulace útoků, aby všichni věděli, co mají v případě incidentu dělat," upozornil Chester Wisniewski, technologický ředitel společnosti Sophos.

České firmy nejsou ochotné platit výkupné

K platbě výkupného se v roce 2023 rozhodl jen malý podíl českých firem, většina dokázala data obnovit

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **75** ze dne **20.7.2024**

jiným způsobem - nejčastěji ze záloh, které k obnově dat využilo 69 % napadených podniků, 16 % pak použilo jiné prostředky. Kybernetickému vydírání podleho a výkupné loni zaplatilo 15 % napadených firem, přičemž u třetiny z nich to bylo v rozmezí 600 000 až tři miliony korun a u třetiny v rozmezí tří až šesti milionů korun. Pětina napadených zaplatila méně než 600 000 korun, desetina odmítla výši uhrazeného výkupného zveřejnit.

Procento těch, kteří zaplatili, je v České republice výrazně nižší než v Evropě, Americe a asijsko-pacifickém regionu, kde zaplatilo výkupné, aby obnovilo svá data, 56 % společností. V Polsku zaplatilo výkupné 38 % a v Maďarsku tři procenta společností.

"Každá společnost, bez ohledu na její velikost nebo odvětví, ve kterém působí, je zranitelná vůči kybernetickým útokům. Je proto iluzí předpokládat, že nás se to netýká a že nám takové riziko nehrozí. Každý bez výjimky by měl být na takovou situaci připraven. Většina společností napadených ransomwarem nebude schopna obnovit všechny své soubory, ani když zaplatí výkupné. Proto je nutné používat zálohy dat. Zaplacení výkupného nejenže zlepšuje finanční situaci hackerů, ale také zpomaluje reakci na incident úniku dat. V konečném důsledku to zvyšuje již tak vysoké náklady na nápravu po kybernetickém útoku," uzavřel Wisniewski.

Zdroj: AVcentrum ČR