

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **89** ze dne **12.11.2024**

Každý třetí útok ransomwaru na české firmy začíná zneužitím zranitelnosti

Nejčastějším zdrojem ransomwarových útoků na české společnosti v roce 2023 bylo zneužití zranitelnosti systému zabezpečení. Firmy se na kybernetické útoky připravují, ale stále nedostatečně - pouze 57 % z nich zálohuje data a 42 % zaměstnává specialisty na kybernetickou bezpečnost nebo provozuje interní SOC. Ještě hůře na tom jsou firmy s plány obnovy nebo plány na zachování kontinuity provozu.

Z průzkumu, který na zadání společnosti Sophos provedla nezávislá výzkumná agentura IPSOS a který mapuje reálné zkušenosti českých firem s ransomwarovými útoky a dopady těchto útoků na jejich podnikání v roce 2023, vyplývá, že loni čelily nějakému kybernetickému útoku tři pětiny firem, každá pátá pak byla napadena ransomwarem. Nejčastější vstupní branou do podnikových systémů byla nedostatečná bezpečnostní opatření (34 %), phishing (24 %) a nelegálně získané přístupové údaje (23 %).

Phishing je stále účinný

U každé páté firmy (24 %), která byla v roce 2023 zasažena ransomwarem, se kyberzločinci dostali do podnikových IT systémů prostřednictvím phishingových zpráv. "Obliba phishingu jako metody získání přístupu k datům ukazuje, že firmy mají stále co zlepšovat v oblasti vzdělávání svých zaměstnanců. Pokud uživatel obdrží phishingový e-mail a následně klikne na škodlivý odkaz, odvede práci za kyberzločince a vpustí je do systému společnosti. Proto je tak důležité zaměstnance vzdělávat a vysvětlovat jim, jaké prvky zprávy, by měly vyvolat jejich pozornost. Těmi nejzřetelnějšími jsou vyvíjení tlaku na rychlou reakci, gramatické a stylistické chyby, neobvyklé požadavky nebo zprávy, které člověk neočekává," zdůraznil Chester Wisniewski, technologický ředitel společnosti Sophos.

Dalšími nejčastějšími metodami, které kyberzločinci používali a jejichž prostřednictvím získali přístup do systémů napadených společností, byly zneužití zranitelnosti zabezpečení (34 %) a nelegálně získaných přístupových údajů (23 %). Deset procent respondentů průzkumu uvedlo, že podvodníci získali přístup do IT systémů v důsledku neoprávněného přístupu nebo škodlivé činnosti zaměstnanců či jiných osob spojených s firmou.

Informační technologie a umělá inteligence by měly podporovat zaměstnance

V dotazovaných společnostech hrají při ochraně před kybernetickými útoky významnou roli specialisté na kybernetickou bezpečnost. Vlastní bezpečnostní specialisty nebo interní bezpečnostní dohledové centrum SOC (Security Operation Center) schopné útoky zastavit má 53 % českých firem, které loni čelily ransomwaru. Každá pátá společnost (21 %) pak spolupracuje s externími specialisty na kybernetickou bezpečnost a specializovanými týmy pro reakci na útoky.

Že má dostatečný počet odborníků na zajištění kybernetické bezpečnosti si myslí 37 % českých firem, které loni čelily ransomwaru. Stejný počet (37 %) organizací si současně stěžuje, že nemá dostatek prostředků na zvýšení počtu těchto odborníků. O zvýšení počtu odborníků na kybernetickou bezpečnost, které se ale nedaří najít, se snaží 24 % loni ransomwarem zasažených českých firem.

Při pohledu na firmy bez zkušenosti s útokem je patrné, že na ochranu dat dbají o něco méně – vlastní specialisty nebo SOC má pouze 32 % z nich a s externisty spolupracuje jen 15 % těchto firem, současně 23 % z nich nemá dostatek prostředků na zvýšení počtu bezpečnostních specialistů a osm procent chce jejich počet

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **89** ze dne **12.11.2024**

zvýšit, ale nedaří se je najít.

"Ze zjištěných data vyplývá, že společnosti na bezpečnostní specialisty a jejich dovednosti spoléhají. Je však důležité si uvědomit, že klíčem k účinné ochraně je podpora IT oddělení správnými řešeními a nástroji, aby mohla včas odhalit incidenty a provést nápravná opatření. Týmy kybernetické bezpečnosti jsou bohužel často zahlceny velkým množstvím různých upozornění. Proto stojí za zvážení sáhnout po umělé inteligenci (AI), která by mohla některá upozornění analyzovat a automaticky na ně reagovat. Využití AI nenahradí odborníky zcela, ale může pomoci vyplnit mezeru v kompetencích v oblasti IT," vysvětlil Wisniewski.

Zálohy a plány obnovy

Dvě třetiny (66 %) loni ransomwarem zasažených společností používají zálohování, aby se ochránily před následky kybernetických útoků a ransomwaru. Zálohy v cloudu má 56 % těchto organizací a 37 % je ukládá ve fyzické podobě. Specifickou ochranu proti ransomwaru, například speciální bezpečnostní software, firewally nebo filtry obsahu, má 39 % společností se zkušeností s útokem. Významný pokles těchto opatření vidíme u firem, které ransomwarem zasaženy ještě nebyly - zálohy používá 47 % z nich (cloud 39 %, fyzické 24 %), specifickou ochranu má 32 %.

Průzkum společnosti Sophos také ukázal, že firmy ve snaze ochránit se před následky útoků ransomwaru využívají v menší míře i kybernetické pojištění – deset procent firem se zkušeností s ransomwarem, dvě procenta firem bez zkušenosti s útokem. Ze zprávy společnosti Sophos Cyber Insurance and Cyber Defenses 2024 věnované kybernetickému pojištění však vyplývá, že v roce 2023 přesáhly celkové náklady na obnovu pojistný limit ve 63 % případech.

Dalšími účinnými nástroji na ochranu před kybernetickými útoky jsou plány obnovy a plány na zachování kontinuity provozu. Úplný a podrobný plán obnovy má 29 % českých organizací, které loni čelily ransomwaru. Dílčí plán obnovy, který však nezahrnuje všechny možné scénáře, má 53 % těchto firem, a plánem na zachování kontinuity provozu disponuje 16 % firem se zkušeností s ransomwarem. I zde vidíme nižší míru těchto opatření u firem, které ransomwarem zasaženy ještě nebyly - úplný a podrobný plán obnovy má jedenáct procent, dílčí plán obnovy nezahrnující všechny možné scénáře má 27 %, a plánem na zachování kontinuity provozu disponuje 28 % českých firem bez zkušenosti s útokem. Průzkum také zjistil, že ani plán obnovy, ani plán na zachování kontinuity provozu stále nemají dvě procenta firem, které byly zasaženy ransomwarem a 28 % firem, které zkušenost s útokem zatím nemají.

Kybernetický útok do budoucna očekává 36 % českých firem, které dosud útoku nečelily. Naopak 29 % takových firem si myslí, že se obětí kyberzločinců nestane.

Zdroj: AVcentrum ČR