88 % firem čelilo útokům na systémy, lidská chyba hraje klíčovou roli

17.1.2025 - | PROTEXT

Nejvíce bezpečnostních incidentů v síti zaznamenaly velké firmy, přestože mají zavedena nejkomplexnější ochranná opatření. S tímto typem problémů se potýkaly také malé a střední firmy, přičemž značné procento incidentů bylo přičítáno úmyslnému nebo neúmyslnému jednání jejich vlastních zaměstnanců.

Bezpečnostní hrozby v síti působí firmám stále největší potíže

Cílem síťových bezpečnostních hrozeb je zneužít zranitelnosti systému, proniknout do firemních sítí a způsobit škody na citlivých datech, aplikacích a provozních úlohách. Pokud kyberzločinec najde slabé místo v systému, využije ho k získání neoprávněného přístupu a instalaci malwaru, spywaru nebo jiného škodlivého softwaru. Tato slabá místa jsou také vstupní branou pro útoky pomocí sociálního inženýrství, kdy se jednotlivci stávají snadnější obětí a prostředkem pro překonání obrany.

Se stále větším objemem elektronicky vytvářených, ukládaných a přenášených dat roste i možnost kybernetických útoků, které mohou ohrozit citlivé informace. Jedním z klíčových faktorů, které přispívají k neustálému výskytu problémů se zabezpečením sítí, je rostoucí komplexnost a sofistikovanost kybernetických hrozeb. Kyberzločinci neustále vyvíjejí nové taktiky a techniky jak obejít dosavadní bezpečnostní opatření a pro firmy je tak náročné udržet si potřebný náskok. Útočníci mohou zneužít potenciálně zranitelných míst ve firemní síti mnoha způsoby, od phishingových podvodů a ransomwarových útoků až po útoky typu DDoS a APT.

V souvislosti s nárůstem práce na dálku a používáním osobních zařízení zaměstnanců (BYOD) navíc vznikla další rizika pro zabezpečení sítě. Zaměstnanci přistupují k firemním datům z různých míst a zařízení a tím se zvyšuje možnost narušení bezpečnosti. To v kombinaci s nedostatkem odpovídajících bezpečnostních protokolů a školení zaměstnanců vytváří zranitelné prostředí pro kybernetické útoky.

Dalším palčivým problémem je lidský faktor

Jiným klíčovým faktorem, který přispívá k bezpečnostním incidentům, je lidská chyba. Čtyřicet dva procent organizací nahlásilo případy, kdy jejich vlastní zaměstnanci svým jednáním či naopak nečinností vědomě či nevědomě napomáhali útočníkům, přičemž většina těchto případů se vyskytla v malých a středních firmách – velké firmy se s tímto problémem potýkaly mnohem méně.

Chyby nebo nedbalost zaměstnanců, ať už z důvodu nízkého povědomí o bezpečnosti nebo nedostatečného školení, jsou hlavní příčinou narušení bezpečnosti a úniku dat v organizacích. Častou hrozbou jsou phishingové útoky, kdy zaměstnanci neuváženě kliknou na škodlivé odkazy nebo poskytnou podvodníkům citlivé údaje. Významné riziko pro bezpečnost firem mohou představovat také situace, kdy interní pracovníci úmyslně nebo neúmyslně vynášejí důvěrné informace. Následky nedbalosti zaměstnanců v oblasti kybernetické bezpečnosti mohou být závažné, protože úniky dat často vedou k finančním ztrátám, poškození pověsti firmy a právním dohrám. V krajním případě mohou firmy čelit pokutám a žalobám za nedostatečnou ochranu citlivých údajů.

Malé a střední firmy bývají zranitelnější vůči únikům dat způsobeným jejich vlastními zaměstnanci, protože mohou postrádat potřebnou infrastrukturu a znalosti, které by jim umožňovaly dostatečně

chránit citlivé informace, což z nich činí snadný cíl pro kybernetické zločince, kteří chtějí využít slabých článků bezpečnostního řetězce. Velké společnosti mají oproti nim více prostředků na investice do důkladných kybernetických bezpečnostních opatření a školení zaměstnanců.

Doporučení pro lepší ochranu

Aby se snížilo riziko kybernetických útoků způsobených lidskou chybou, musí firmy podniknout kroky ke zvýšení povědomí zaměstnanců o kybernetických hrozbách a investovat do komplexních programů školení v oblasti kybernetické bezpečnosti .

Pravidelné bezpečnostní audity a monitorování mohou pomoci odhalit zranitelná místa a odstranit je dříve, než je zneužijí kyberzločinci. Specializovaná řešení, poskytovaná v rámci produktů pro firmy od společnosti Kaspersky, dokážou chránit aktiva všech typů organizací v reálném čase pomocí funkcí EDR a XDR ochrany, jako jsou zviditelnění hrozeb, jejich vyšetřování a automatické reakce na ně.

Pro dobrou ochranu dat a pověsti firmy v digitálním prostředí je však nejúčinnější prevencí kombinace jak technologických řešení, tak proaktivního vzdělávání zaměstnanců.

http://www.ceskenoviny.cz/tiskove/zpravy/88-firem-celilo-utokum-na-systemy-lidska-chyba-hraje-klicovou-roli/2621687