TISKOVÁ ZPRÁVA

Útočníky v kyberprostoru pohání ideologie i rozvoj umělé inteligence. Bez správné ochrany hrozí firmám jak ekonomické ztráty, tak propad reputace

Praha, 19. 12. 2023 – Evropská unie zaznamenala v první polovině roku 2023 třikrát více kybernetických útoků než ve druhé polovině předcházejícího roku. Kromě četnosti jsou kybernetické útoky a jejich následky také rozmanitější. Významnou roli hrál nárůst počtu hacktivistických skupin, které provádí útoky s ideologickým pozadím, zvláště v souvislosti s válkou na Ukrajině, stejně tak jako rozvoj umělé inteligence i internetu věcí. Nejčastějším typem byly ransomware útoky (31 %), dále DDoS útoky (21 %) a následně krádeže osobních údajů (20 %). Mířily nejčastěji na veřejnou správu (19 %), jednotlivce (11 %), zdravotnictví (8 %), digitální infrastrukturu (7 %) a dále na výrobu, finance a dopravu. Vyplývá to z dat Agentury Evropské unie pro kybernetickou bezpečnost a analýzy společnosti BDO.

„Od února letošního roku až do června, do kterého jsou k dispozici zpracovaná data, počet kybernetických útoků v EU každoměsíčně stoupal. Konkrétně v březnu stoupl dokonce více než trojnásobně. Pro jednotlivce, firmy, organizace a veřejné instituce budou kybernetické útoky představovat čím dál větší riziko, na které je nutné mít zavedená adekvátní reaktivní opatření,“ komentuje Libor Šrám, auditor kybernetické bezpečnosti z poradenské společnosti BDO.

Nejčastějšími hrozbami jsou v současnosti **ransomwarové útoky**, který cílí na datový obsah informačních systémů se snahou jej zašifrovat, případně převzít. Takových útoků stále přibývá a nevypadá, že by trend měl v blízké době zpomalit. *„Útočníci většinou vyžadují výkupné za zpětné odblokování zašifrovaných dat, přičemž výsledek po zaplacení požadované částky je velmi nejistý. Pokud takový útok nastane, je třeba bez zbytečného odkladu zahájit rychlé a efektivní akce směřující k minimalizaci vzniklých škod,“* doporučuje Libor Šrám.

Nejdůležitější je rychlá izolace postižených systémů, omezení nebo zastavení veškerých kritických operací provozovaných informačními systémy a zahájení obnovy informačních systémů a dat z prověřených záloh. Po obnově normálního provozu je nutné provést podrobnou analýzu incidentu a vyhodnotit, jak zlepšit reakci na podobné útoky v budoucnosti. Základem účinné ochrany je ověřený plán pro řešení incidentů, plán obnovy a kontinuity podnikání.

Dalším nejčastějším typem kybernetických hrozeb jsou **DDoS útoky**, které cílí na informační systémy se snahou o jejich zahlcení a zamezení jejich fungování. *„DDoS útoky jsou často příčinou výpadků internetu nebo telekomunikačního provozu. Ty jsou historicky na nejvyšší úrovni*,“ doplňuje odborník z BDO. Cílem těchto útoků je narušení fungování informačních systémů, což je pro útočníky druhou

nejběžnější motivací po té finanční. Zároveň DDoS útoky často slouží jako doplňková aktivita většího útoku, který již může mít finanční motivaci.

V současné době bychom již našli jen zlomek jedinců, kteří by neměli osobní zkušenost s **phishingem**, tedy snahou o vylákání citlivých údajů pomocí podvodných mailů nebo falešných webových stránek, které napodobují známé servery, platební portály nebo weby státních institucí. Útočníci tak cílí na lidskou důvěru a zvědavost. *„Relativní novinkou je přitom klamání uživatelů například pomocí důvěryhodně probíhajících telefonátů s cílem získat cenné přístupové údaje*," uvádí Libor Šrám.

„Firmy by proto měly především pečlivě nastavit vhodná bezpečnostní opatření, poučit zaměstnance o existujících rizicích a také jim poskytnout školení, jak nejčastějším útokům odolávat a předcházet jim," radí Libor Šrám z BDO.

Umělá inteligence pomáhá jak při ochraně, tak při útocích

Zatímco nasazení umělé inteligence ve společnostech může na jedné straně pomáhat při odhalování podezřelého chování nebo škodlivého kódu, na straně druhé účinně pomáhá i útočníkům. *„Ti díky umělé inteligenci vytvářejí přesvědčivější phishingové e-maily, které dnes již netrpí špatnou češtinou, díky které šlo v minulosti snadno podvod odhalit,"* potvrzuje Libor Šrám.

Již dnes lze s využitím umělé inteligence napodobovat známé hlasy a vytvářet podvodná videa, které jsou čím dál více k nerozeznání od originálu.

„Pro firmy a další organizace je vedle důsledného proškolování zaměstnanců zásadní správně nastavit parametry ochrany proti kybernetickým útokům, zejména průběžně prověřovat jejich zranitelnosti a aplikovat opatření proti zjištěným zranitelnostem. Jinak se mohou kromě ekonomických ztrát potýkat také s dopadem na pověst společnosti," varuje Libor Šrám ze společnosti BDO.

TISKOVÁ ZPRÁVA

O společnosti BDO

BDO je poradenská společnost poskytující auditorské, daňové, právní, účetní a poradenské služby. Na českém trhu působí již 30 let. S téměř 500 odborníky a dlouholetou praxí se řadí k předním společnostem s tímto zaměřením v České republice, kde má kanceláře v Praze, Plzni, Brně, Domažlicích, Českých Budějovicích, Jindřichově Hradci a Ostravě.

BDO je v České republice zastoupena společnostmi BDO Audit s.r.o., BDO Czech Republic s.r.o., BDO Consulting s.r.o., BDO Legal s.r.o., advokátní kancelář a BDO Valuation, s.r.o. Společnost je součástí mezinárodní sítě BDO, která celosvětově tvoří jednu z největších sítí auditorských a poradenských skupin. Zaměstnává více jak 91 tisíc odborníků a působí ve 167 zemích, v nichž čítá více než 1 650 kanceláří.

Kontakt:
Jan Kuliš, EPIC Public relations
E-mail: jan.kulis@epicpr.cz
Tel.: +420 731 920 874
Web: www.epicpr.cz