

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **56** ze dne **23.1.2024**

Jak bojovat proti AI útokům?

Kdybyste se zeptali skupiny generálních ředitelů na tři jejich největší obavy v tomto roce, byla by mezi nimi i kybernetická bezpečnost? Podle nedávné studie provedené společností Gartner nikoliv, protože ředitelé uváděli jako prioritní oblasti růst, technologie a nové talenty. Tutéž odpověď byste od nich zřejmě dostali i na otázku ohledně pokroku v oblasti umělé inteligence a její využití k útokům na firemní kybernetickou bezpečnost.

Vzestup nástrojů, jako je ChatGPT, činí organizace zranitelnějšími vůči hrozbám kybernetické bezpečnosti, které využívají umělé inteligence více než kdykoli předtím. A ke zmírnění těchto hrozeb se sofistikovanými nástroji potřebnými k jejich úspěšnému odvrácení jsou zapotřebí chytře zaměřené investice.

Tři hlavní oblasti využití AI

Generativní nástroje umělé inteligence zejména pak ChatGPT zažily v roce 2023 velký nástup. Organizace používají AI k automatizaci úloh a k zefektivnění pracovních postupů. Bohužel stejně tak i kyberzločinci. Sociální inženýrství a tvorba malwaru s podporou ChatGPT jsou na vzestupu, takže následující útoky jsou sofistikovanější a hůře odhalitelné:

- **Phishingové / nevyžádané e-maily:** ChatGPT je nástroj založený na jazykovém modelu LLM, který kyberzločincům poskytuje mnohem lepší jazykové a kódovací schopnosti. Ti mohou pomocí ChatGPT a podobných nástrojů vytvářet realistické, přesvědčivé phishingové e-maily, které neobsahují gramatické a pravopisné chyby v mnoha jazycích.
- **BEC e-mailové podvody:** ChatGPT může hackerům poskytnout schopnost napodobit styl e-mailů konkrétních vedoucích pracovníků a automaticky reagovat v reálném čase, aby mohli realizovat přesvědčivější útoky. Technologii hlasového deep fake postavenou na umělé inteligenci lze také použít ke klonování hlasu manažera při útocích založených na hlasových hovorech a k překonání hlasové autentizace při online bankovních transakcích.
- **Automatizace:** Nejvíce znepokojivým prvkem kybernetických bezpečnostních hrozeb využívající AI je schopnost ChatGPT zefektivnit, personalizovat a rozšiřovat útoky nebývalou rychlostí. Do budoucna lze očekávat více útoků ve větším objemu, protože generativní AI je stále dokonalejší.

EDR jako klíčová zbraň

Kybernetické hrozby s podporou umělé inteligence využívají skrytost a vytrvalost, aby se vyhnuly systémům kybernetické bezpečnosti. A kyberzločinci se nezastaví u prvního systému, který prolomí. Číhají a pokoušejí se napadnout další koncové body, přičemž se šíří pomalu, aby se vyhnuli odhalení.

Jak se lze proti nim ochránit? Novou generací kybernetické bezpečnosti je ochrana koncových bodů (EDR). Poskytuje možnost odhalit pokročilé, skryté hrozby a zabránit jim v průniku do systémů s využitím přímé viditelnosti všech koncových bodů. EDR chrání před generativními hrozbami využívajícími AI následujícími způsoby:

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **56** ze dne **23.1.2024**

- Proaktivní vyhledávání hrozeb a reakce na ně: Sofistikovaný EDR využívá podrobné údaje o detekci hrozeb k proaktivní analýze činnosti systému a k eliminaci hrozeb. Po identifikaci hrozeb pak radí bezpečnostním týmům, jak nejlépe postupovat při nápravě incidentů dříve, než dojde k jakémukoliv narušení bezpečnosti.
- Průběžný monitoring a historické záznamy: Řešení EDR nepřetržitě monitoruje všechny koncové body sítě a zaznamenává aktivitu, aby identifikovalo potenciální kybernetické hrozby nebo zranitelnosti. Prostřednictvím průběžného sledování a historických záznamů poskytuje EDR ucelený pohled na síť v reálném čase a nejkompaktnější dostupnou ochranu.
- Jistota dodržení zákonných požadavků: V případě působení v oblasti nebo odvětví, které podléhá úředním nebo soukromým regulacím, je narušení bezpečnosti nejen noční můrou pro pověst organizace, ale také pro její finance, protože sankce za porušení předpisů mohou být velmi nákladné. Nově vznikající oborové předpisy navíc vyžadují dodržování konkrétních směrnic pro zabezpečení koncových bodů a ochranu dat, jinak hrozí sankce.

Ohněm proti ohni

Umělá inteligence je tu s námi a každou minutou je stále sofistikovanější. Úspěšné kybernetické útoky už nejsou otázkou kdyby, ale kdy. Pokud je třeba organizaci ochránit před zranitelnostmi a náporům útoků s podporou AI, nelze než bojovat ohněm proti ohni. Tedy chránit před útoky postavenými na AI s využitím nástrojů založených na umělé inteligenci.

Zdroj: AVcenturm ČR