Katasztrofális kibertámadásokhoz vezethet a generatív mesterséges intelligencia terjedése

Jelentősen nőtt (27%-ról 36%-ra) azoknak a vállalkozásoknak az aránya, amelyek 1 millió dollárt meghaladó értékű adatvédelmi incidenst tapasztaltak az elmúlt egy évben, ennek ellenére a cégek több mint egyharmada nem tett kockázatkezelési erőfeszítéseket, és csak minden negyedik vállalat javította kiberrezilienciáját. A generatív mesterséges intelligencia terjedése tovább nehezítheti a támadások elleni védekezést, a válaszadók több mint fele szerint alkalmazása katasztrofális kibertámadásokhoz vezethet a jövőben, és ezek kivédésére az üzleti vezetők többsége nincs felkészülve – derül ki a PwC idei Global Digital Trust Insights felméréséből.

A kibertámadások által okozott kár tovább nőtt, különösen az egészségügyi ágazatban

A PwC 71 ország 3 800 üzleti és technológiai vezetőjének körében végzett felmérése rámutat, hogy az információbiztonsági incidenseket elszenvedő vállalkozások száma tovább nőtt az elmúlt egy évben. A támadások az egészségügyi ágazat szereplőit érintették leginkább. A káros kibertámadások globálisan átlagosan 4,4 millió dolláros kárt okoztak a vállalkozásoknak, míg az egészségügyi ágazatban ez a költség 25%-kal magasabb – 5,3 millió dollár volt. A vizsgált időszakban az egészségügyi szervezetek válaszadóinak közel fele (47%) számolt be 1 millió dolláros vagy azt meghaladó értékű adatvédelmi incidensről. A többi szektor esetében ez az arány: technológiai, média és telekommunikáció 43%, pénzügyi szolgáltatók 38%, energiaszektor 37%, ipar- és autógyártás 33%, kiskereskedelem 28%.

Mesterséges intelligencia: egyszerre áldás és átok

Az üzleti és a technológiai vezetők körében egyre nagyobb aggodalomra ad okot a kiberbiztonsággal kapcsolatban a generatív mesterséges intelligencia (MI) elterjedése, hiszen alkalmazásával többek között jobban célozhatóak és sokkal hihetőbbé tehetőek a munkavállalókat célzó átverések. A generatív mesterséges intelligencia olyan technológia, amely múltbeli adatokra támaszkodva hoz létre újat legyen szó szövegről, képről, videóról, kódról, stb. Az informatikai szakemberek számára intő jel, hogy a válaszadók 52%-a szerint a generatív MI katasztrofális kibertámadásokhoz vezethet a következő 12 hónapban. Ugyanakkor az is elgondolkodtató, hogy tízből közel nyolc válaszadó (77%) kívánja a generatív MI-t etikus és felelősségteljes módon használni.

Miközben látják a kockázatait, a vezetők háromnegyede kifejezetten érdeklődik a generatív mesterséges intelligenciában rejlő üzletfejlesztési lehetőségek iránt: 77%-uk egyetértett azzal, hogy a következő három éven belül segíteni fogja szervezetüket új üzletágak kialakításában, míg 75%-uk szerint az alkalmazottak produktivitását fogják növelni a következő 12 hónapban.

> „A vezetők technológiába vetett hite nem alaptalan, hiszen a generatív MI kiválóan alkalmas egy kiberincidensről - különböző rendszerekből és forrásokból származó - nagy mennyiségű adat szintetizálására, ezzel segítve a vezetőket a történtek megértésében, azaz egy incidens felismerésére és gyors elemzésére is kitűnően alkalmazható. A generatív MI képes arra is, hogy könnyen érthető nyelvezettel mutassa be az összetett fenyegetéseket, tanácsot adjon a megelőzési és megoldási stratégiákkal kapcsolatban,

valamint segítséget nyújtson az incidensek kivizsgálásában” – emelte ki Durojaiye Péter, a PwC magyarországi és közép-kelet-európai kibervédelmi csoportjának, valamint az EMEA régió Cybersecurity Impact Centerének vezetője.

A fenyegetettségek növekedése ellenére a vállalatok jelentős része nem ismeri és nem elemzi a kiberkockázatokat

Az éghajlatváltozással kapcsolatos természeti katasztrófák számának folyamatos növekedése, a Covid-19-világjárvány szűnni nem akaró hatásai és a növekvő egyenlőtlenségek ellenére a megkérdezett vezetők a digitális technológiát a legfontosabb kockázatok közé sorolták a következő 12 hónapra nézve.

Ugyanakkor a három legfontosabb kiberfenyegetés - a felhőhöz kapcsolódó kockázatok, a csatlakoztatott eszközök elleni támadások, valamint a hackelés és kiszivárogtatás - ellenére a vállalatok több mint egyharmada nem tett kockázatkezelési erőfeszítéseket, és csak minden negyedik vállalat javította kiberrezilienciáját az elmúlt 12 hónapban.

A szervezeteknek mindössze két százaléka optimalizálja és fejleszti folyamatosan a kibertámadásokkal szembeni ellenállóképességét valamennyi területen. Egy másik megdöbbentő eredmény, hogy a megkérdezett vezetők több mint 40%-a nem érti a feltörekvő technológiák, például a virtuális környezeti eszközök, a generatív MI, a vállalati blokklánc, a kvantum-számítástechnika és a kiterjesztett valóság jelentette kiberkockázatokat.

„A szervezeteknek fel kell ismerniük, hogy a jövő technológiáinak alkalmazása nem csak üzleti előnyt hozhat, hanem új kockázatokat is jelent, ezért ezek elemzése és kezelése kiemelten fontos a sikeres bevezetéshez. Például az MI széleskörű alkalmazásához figyelembe kell venni a hagyományos biztonsági és adatvédelmi kockázatok mellett a tanulási folyamattal és bemeneti adatokkal kapcsolatos kibervédelmi és üzleti kockázatokat is. Ugyanígy egy virtuális környezetben új értelmet nyer a személyes adatvédelem a nagyfokú biometrikus adatfeldolgozás révén, ami szintén túlmutat a korábbi adatvédelmi gyakorlaton” - összegezte Gyimesi Csaba, a PwC Magyarország kibervédelmi csoportjának igazgatója.

Mit nyerhetnek a cégek a kiberbiztonsági gyakorlatok bevezetésével?

A vállalatok csak kevesebb mint egyharmada alkalmazza folyamatosan és konzekvensen a legfontosabb kiberbiztonsági gyakorlatokat, holott ez kulcsfontosságú az incidensek elleni védekezésben. A felmérés szerint a kutatásban résztvevő cégek mindössze 5 százaléka rendelkezik információbiztonsági gyakorlatokat következetesen alkalmazó kiberbiztonsági csapatokkal - ők a digitális bizalom letéteményesei.

Ezek a szervezetek kisebb értékű kibertámadásokat szenvedtek el a vizsgált időszakban, mint azok a vállalatok, akik nem alkalmazzák rendszeresen az információbiztonsági gyakorlatokat: míg az összes szervezet 36%-át érte 1 millió dolláros kárt meghaladó kibertámadás, ez az arány a digitális bizalom letéteményesei esetében csak 29%.

„A gyakorlatok nem csak a tudatosságot és így a megelőzést segítik elő nagymértékben, de a begyakorolt reagálási tervek mentén sokkal hatékonyabban kezelik a bekövetkező incidenseket is” - tette hozzá Gyimesi Csaba.

A többi válaszadóhoz képest pozitívabban látják a generatív MI lehetséges hatását is, szerintük:

- új üzletágakat fog kialakítani (49%, szemben az összes válaszadó 33%-ával);
- generatív MI-alapú eszközöket fognak használni a kibervédelemhez (44%, szemben az összes válaszadó 27%-ával);
- kevésbé valószínű, hogy a generatív mesterséges intelligencia katasztrofális kibertámadásokhoz fog vezetni (33%, szemben az összes válaszadó 22%-ával);
- nem várható, hogy a generatív MI-alapú eszközöket a vonatkozó belső szabályzatok bevezetése előtt alkalmazni fogják.

A Global Digital Trust Insights eredményei

A felmérésről: *A 2024-es Digital Trust Insights felmérésben globális üzleti és technológiai vezetőket kérdeztünk vállalatuk kiberbiztonságának javításával és átalakításával kapcsolatban. A 2023 májusa és júliusa között végzett kutatás 3 876 vezető válaszain alapul 71 földrajzi területről. A felmérésben különböző méretű és iparágú szervezet vett részt, amelyek 40%-a 5 milliárd dollárt meghaladó árbevétellel rendelkezik. A válaszok 88%-a (3 428) külső szolgáltató felületén keresztül érkezett, 12%-a (448) a PwC hálózatából.*

Sajtókapcsolat:

- Szőke Cecília, PR Vezető Menedzser
- PwC Hungary
- +36 1 461 9100

Eredeti tartalom: PwC Magyarország

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/7615/katasztrofalis-kibertamadasokhoz-vezethet-a-generativ-mesterseges-intelligencia-terjedese/