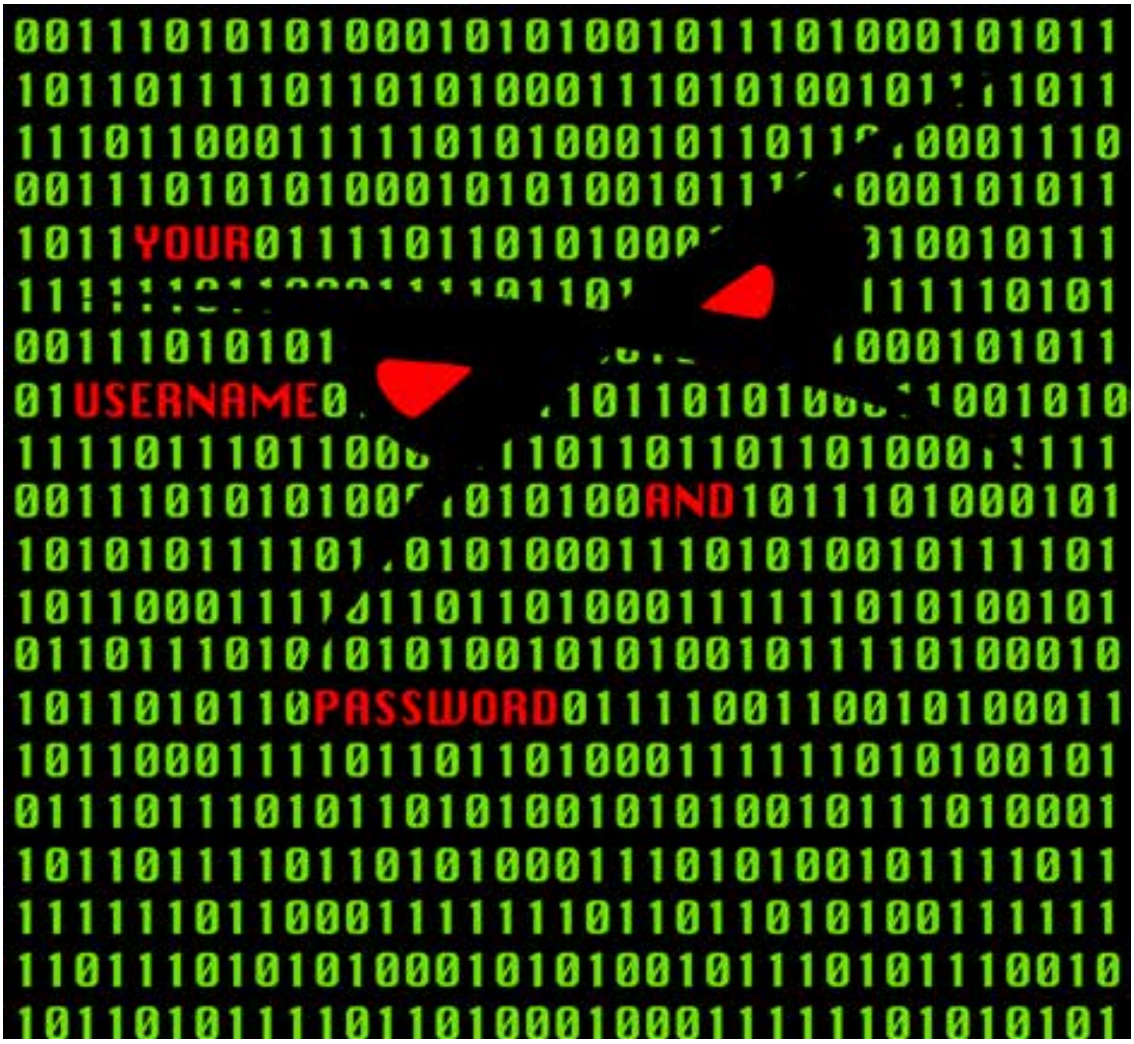

Foto: Depositphotos

Ker tri četrt podjetij zagotavlja le osnovno raven kibernetske zaščite, je prostor za napade na podjetja in organizacije ogromen in postaja tudi vse večji.

Kibernetska varnost

Umetna inteligenca spreminja obraz kibernetske varnosti

S pospešeno digitalizacijo družbe se pojavljajo tudi njene negativne posledice, in sicer v obliki novih ranljivosti za kibernetske napade. Večina podjetij in organizacij danes ni pripravljenih na sodobne kibernetske grožnje, medtem pa sodobni kibernetski kriminal s pomočjo umetne inteligence doživlja preporod in izjemno rast.

Mitja Trampuž, direktor podjetij CREAplus in CREApro

Treba se je zavedati, da bodo novi, še neuporabljeni ali neodkriti načini uporabe UI povzročili še večje spremembe, kot jih poznamo sedaj.

Poročilo »Kibernetska varnost za mala in srednja podjetja«, ki ga je junija letos predstavila Agencija EU za kibernetsko varnost (ENISA), kaže, da danes več kot 70 % podjetij zagotavlja le osnovno raven kibernetske zaščite. Ta običajno vključuje izvajanje rezervnih kopij, namestitev protivirusnega programa in požarne pregrade ter kolikor toliko redno posodabljanje programske opreme. Kar pomeni, da je prostor za napade na podjetja in organizacije ogromen in postaja tudi vse večji. Sodobni kriminalci v svoja orodja že uvajajo umetno inteligenco (UI), kar predstavlja še večjo grožnjo.

Umetna inteligenca je odvisna od podatkov

Po definiciji Evropskega parlamenta je umetna inteligenca zmožnost stroja, da izkazuje človeške lastnosti, kot so mišljenje, učenje, načrtovanje in ustvarjalnost. Gre za sisteme, ki lahko na podlagi analize učinkov

svojih predhodnih dejanj samostojno prilagajajo svoje vedenje. UI imamo za osnovno tehnologijo četrte industrijske revolucije, vključuje pa strojno učenje (ang. machine learning, ML), globoko ali poglobljeno učenje (ang. deep learning, DL) in nevronske mreže (ang. neural networks, NN). Za uporabo navedenih tehnologij je običajno treba zagotoviti ustrezne računalniške zmogljivosti.

UI zagotovo igra tudi ključno vlogo v digitalni preobrazbi gospodarstva in družb, ni pa nekaj povsem novega, saj so nekatere tehnologije prisotne že več kot 50 let. Današnji preboj je nastal predvsem zaradi treh dejavnikov: napredka v zmogljivosti in dostopnosti računalnikov, dostopnosti ogromnih količin podatkov ter razvoja novih algoritmov. Po podatkih družbe Gartner je v letu 2020 najmanj 37 % podjetij že uporabljalo UI pri svojem poslovanju.

UI danes torej vsakodnevno uporabljamo, obstaja pa še ogromen potencial za njeno uporabo. Nekaj primerov, kjer srečamo UI: digitalni osebni asistenti na mobilnih telefonih in osebnih računalnikih, pametno ogrevanje in hlajenje bivalnih prostorov, samovozeča vozila, inteligentno spletno nakupovanje in oglaševanje, pametno kmetijstvo, roboti v proizvodnji, pametno spletno iskanje, strojni jezikovni prevodi, optimiziranje izdelkov in prodajnih poti in podobno.

UI ima tudi nekaj slabosti in omejitev. Gre za to, da je UI odvisna od podatkov – modeli se učijo iz podatkov in če ni podatkov, ni UI. Pomembna sta tako količina kot kakovost podatkov, na katerih se učijo modeli UI – običajno je to tudi največja težava pri ustvarjanju dodane vrednosti. Uporabniki imajo včasih precej nerealna pričakovanja, pogosto pa tudi niso natančni pri oblikovanju realnih ciljev, kaj želijo in kaj sploh lahko dosežejo z UI. Upoštevati moramo še potencialno vplivanje zakritih dejavnikov, nedefinirano odgovornost za potencialno povzročeno škodo, pa etični vidik in še kaj. Treba se je zavedati, da bodo novi, še neuporabljeni ali neodkriti načini uporabe UI povzročili še večje spremembe, kot jih poznamo sedaj.

Sodobni kibernetski kriminal

Pri sodobnem kibernetskem kriminalu poslovni modeli doživljajo preporod in pa izjemno rast. Sodobni kriminalci so izjemno inovativni in imajo za to tudi dober razlog – za svojo inovativnost so izjemno dobro nagrajeni. Na razpolago imajo praktično neomejene vire, čas, financiranje in skoraj vse sodobne tehnologije.

»Cybercrime as a Service (CaaS)« je danes standardna ponudba zlonamernih storitev, ki je prilagojena tako, da jih lahko najame praktično slehernik. V svojih orodjih pa kriminalne združbe vedno pogosteje vgrajujejo tehnologije UI in z njo že izvajajo avtomatizirane napade. Klasični mehanizmi zaščite – protivirusna programska oprema in požarni zid – takim napadom žal nikakor niso več kos. Pomembno se je zavedati, da je danes tarča kriminalcev vsak posameznik in vsako podjetje, brez izjeme. Ko kriminalci prečešejo in obdelajo najdonosnejše tarče, bodo algoritmi prej ali slej našli tudi nas.

Treba je opredeliti tveganja in razumeti uporabo UI kot napadalno orožje

Tehnologije UI zagotavljajo pozitiven vpliv na poslovanje podjetij, na delovanje kritične infrastrukture in na reševanje različnih izzivov celotne družbe. Žal pa povzročajo širok nabor groženj. Lastnosti UI, ki pozitivno prispevajo k poslovanju podjetij in razvoju družbe, so namreč natanko tiste, ki jih tudi kibernetski kriminalci zlorabljajo za svoja nečedna početja.

Pomembno se je zavedati, da je danes tarča kriminalcev vsak posameznik in vsako podjetje, brez izjeme.

Za zaščito pred kibernetskim kriminalom je potrebno najmanj 1) opredeliti tveganja v zvezi z zlonamernim izkoriščanjem tehnologij UI, in pa 2) razumeti, kako se UI uporablja kot napadalno orožje. Področja, kjer kriminalci zlorabljajo UI za svoje namene, so npr. globoki ponaredki (angl. deepfakes), razbijanje uporabniških gesel, lažno predstavljanje, vdiranje s podporo UI, analiziranje vedenja, zastrupljanje vhodnih podatkov idr.

Obramba z UI

Pri kibernetski obrambi je tako, da se je večina sodobnih orodij za kibernetsko varnost že prilagodila na nove grožnje in že uporablja UI. UI vidi v podatkih bistveno več in to hitreje kot človek ter tako pomaga ekipam varnostnih strokovnjakov pri zaznavanju, ocenjevanju in ukrepanju. UI lahko hitro analizira na milijone dogodkov in prepoznava veliko različnih vrst groženj – od zlonamerne programske opreme za izkoriščanje ranljivosti ničtega dne do prepoznavanja lažnega predstavljanja ali vnosa zlonamerne kode. To je nekaj, čemur človek nikakor ni več kos.

»Cybercrime as a Service (CaaS)« je danes standardna ponudba zlonamernih storitev, ki je prilagojena tako, da jih lahko najame praktično slehernik.

Pri sodobnih orodjih gre tudi za sposobnost analiziranja vedenja v preteklosti, s čimer gradijo profile uporabnikov, naprav in omrežij, kar omogoča hitro odkrivanje in odzivanje na odstopanja od običajnega vedenja.

Malo v šali, vendar veliko zares: prava strategija za boj proti sodobnemu kibernetskemu kriminalu bo verjetno »nad stroj s strojem, nad pametni stroj pa s še bolj pametnim strojem.«

Obraniti sleherni napad

Tehnologije UI imajo številne pozitivne primere uporabe, vendar pa se te iste tehnologije uporabljajo žal tudi v zlonamerne namene. Dejstvo je, da kriminalci že uporabljajo UI za povečanje dosega in obsega svojih napadov ter za izogibanje njihovih odkrivanj. Na nas je, da razumemo 1) zmogljivosti, 2) scenarije in 3) različne vrste napadov, ki jih kriminalci lahko izvedejo s pomočjo tehnologij UI.

Lastnosti UI, ki pozitivno prispevajo k poslovanju podjetij in razvoju družbe, so natanko tiste, ki jih tudi kibernetski kriminalci zlorabljajo za svoja nečedna početja.

Jasno je, da so tehnologije UI postale kritične tehnologije pri zagotavljanju informacijske varnosti. Z razumevanjem področja smo vsaj nekoliko bolje pripravljeni in lahko tudi lažje izbiramo ustrezne strategije, vire in orodja za ustrezno zaščito. Na žalost pa je tako, da morajo biti kriminalci pri napadu uspešni le enkrat, medtem ko morajo branilci vedno obraniti sleherni napad. gg

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

UI vidi v podatkih bistveno več in to hitreje kot človek ter tako pomaga ekipam varnostnih strokovnjakov pri zaznavanju, ocenjevanju in ukrepanju. Gre za nekaj, čemur človek nikakor ni več kos.

Globoki ponaredki
Pri globokih ponaredkih gre za uporabo tehnologij UI za izdelavo ali manipulacijo zvočne in vizualne vsebine, ki izgleda pristna. Gre za eno izmed najbolj priljubljenih zlorab UI. V Veliki Britaniji se je zgodil primer, kjer so kriminalci prisluškovali predsedniku uprave podjetja, naredili globoko ponarejeni zvočni posnetek in se interni službi uspešno predstavili kot predsednik uprave z nalogom za plačilo večje vsote na bančni račun kriminalcev. Šlo je za približno 200.000 funtov.
Za preprečevanje je najprej pomembno razumeti, kako realistični so lahko globoki ponaredki, ter se zavedati, kje vse bi jih kriminalci lahko zlonamerno uporabili.

Ugotavljanje gesel
Pri ugotavljanju uporabniških gesel z UI gre za uporabo globokih nevronskih mrež, kjer kriminalci analizirajo obsežne nabore gesel in ustvarijo različice gesel, ki najbolje ustrezajo statistični porazdelitvi. Rezultat takih prijemov so natančnejša in hitrejša ugibanja gesel z bistveno večjimi možnostmi za uspeh od klasičnih dolgotrajnih (»brute force«) poskusov razbijanja, kjer je potrebno preverjati vsa možna gesla.

Lažno predstavljanje
Pri lažnem predstavljanju gre za zlorabo UI za posnemanje človeškega vedenja s ciljem prevarati sisteme za odkrivanje botov, kjer zlonamerni sistemi to izvajajo s posnemanjem človeških vzorcev uporabe.
Kriminalci običajno z lažnim predstavljanjem, denimo na Spotifyju, Instagramu ali YouTubeu, ustvarjajo nek promet, kot da bi ga naredili dejanski uporabniki, in z njim ustvarijo finančne koristi.

Vdiranje
Tudi pri hekanju so kriminalci začeli uporabljat orodja s tehnologijami UI. Izjemno zanimiv je pojav orodij za analizo ukradenih ali razkritih gesel z uporabo globokih nevronskih mrež, s katerimi napovedujejo, kako bodo uporabniki spremenili svoje geslo pri naslednjem posodabljanju. Orodje zna torej napovedati, kakšna je verjetnost, da bo uporabnik spremenil svoje geslo v točno določeno znano geslo, kar kriminalci pozneje izkoristijo za zlorabo.

Ribarjenje
Razvijajo se že orodja z UI, ki spremljajo in nadzirajo spletno vedenje uporabnikov, s tem pa povečajo verjetnosti, da bodo uporabniki v lažnem e-poštnem sporočilu kliknili na zlonamerno povezavo – gre za zviševanje uspešnosti phishinga.

Zastrupljanje
Izjemno nevarno je tudi »zastrupljanje« vhodnih podatkov za učenje modelov UI, ki so namenjeni za različne namene, npr. tudi za prepoznavanje in preprečevanje kibernetskih napadov – s takim neopaznim spreminjanjem podatkov, iz katerih se učijo modeli UI za zaznavo napadov, postanejo ti modeli neučinkoviti in ne bodo nič zaznali oziroma ne bodo zaznali pravih groženj.
Primerov uporabe UI v zlonamerne namene je seveda še bistveno več, tukaj smo jih našteli le nekaj.