Energetika in informacijska varnost

PANDEMIJA POVEČALA ŠKODO HEKERSKIH NAPADOV

mr. sc.
Ivo Tokić
MBA

Iz najnovejših poročil podjetij za računalniško varnost je razvidno povečanje števila incidentov te vrste kriminala in povečanje povprečne škode po incidentu, ki so jo utrpela napadena podjetja.

Ameriško podjetje IBM Security že leta zbira in analizira podatke o hekerskih napadih v različnih državah. Glede na rezultate njegove analize je v zadnjem letu dni povprečna škoda zaradi vdora do podatkov znašala 4,24 milijona dolarjev na incident. To je največja povprečna škoda, ki jo je zabeležilo to podjetje v 17 letih spremljanja podatkov. Pomembno je, da so bili incidenti vdora v ZDA daleč najdražji, v povprečju so presegli 9 milijonov dolarjev na incident.

Podobne rezultate kaže tudi poročilo neodvisnega inštituta Ponemon, ki je analiziralo incidente vdorov v 537 podjetij in organizacij po vsem svetu v obdobju od maja 2020 do marca 2021. Zaznani incidenti so se zgodili v 17 državah in v različnih panogah industrije. Ugotovitve potrjujejo, da število incidentov na splošno z leti narašča – nekatera leta malo več, nekatera leta malo manj, vendar je trend stalne rasti še vedno prisoten.

Zanimivo je, da se je energetika lansko leto presenetljivo dobro držala v boju proti kibernetskim kriminalcem. Povprečna škoda zaradi vdora v energetiki se je zmanjšala s 6,39 milijonov dolarjev na incident, kot je zapisano v poročilu za leto 2020, na letošnjih 4,65 milijona dolarjev na incident. Glede na

to, da so energetska podjetja precej občutljiva za kibernetske napade in so zaradi tega nenehno podvržena napadom te vrste, so verjetno okrepila zaščitne ukrepe za zmanjšanje škode, ti pa so obrodili sadove.

VPLIV PANDEMIJE COVIDA-19

Čeprav za kibernetske napade obstajajo različni razlogi, strokovnjaki na podlagi analize preteklega leta ocenjujejo, da je prav povečano število ljudi, ki delajo od doma zaradi ukrepov za zmanjšanje širjenja covida-19, omogočilo povečanje škode zaradi hekerskih napadov. Raziskava je pokazala, da so škode v povprečju večje za 1,07 milijona dolarjev pri incidentih, pri katerih je bilo delo na daljavo dejavnik kršitev varnosti podatkov, v primerjavi z incidenti, pri katerih ni bilo tako. Preprosto povedano, po prehodu za delo na daljavo med pandemijo je prišlo do znatnega povečanja vdorov v podjetja in organizacije.

Mnoga podjetja so bila lani prisiljena hitro prilagoditi svoje poslovanje, pri čemer so spodbujala delo od doma ali ga zahtevala od zaposlenih. Približno 60 % podjetij je med pandemijo začelo uporabljati tehniko dela v oblaku. Analiza kaže, da informacijska varnost verjetno ni dovolj uspešno sledila uvedbi teh prisilnih in hitrih sprememb v informatiki in telekomunikacijah. To je oviralo sposobnost podjetij, da zaščitijo svoje podatke in se tako odzovejo na kibernetske napade.

Študija je pokazala, da so ukradene poverilnice uporabnikov najpogostejši vzrok za kršitve. Poleg tega so bili najpogostejši ukradeni podatki osebni podatki uporabnikov, kot so imena, e -poštni naslovi in gesla. Kar 44 % incidentov je vključevalo tovrstne podatke in problem je večji, kot se zdi na prvi pogled, ker strokovnjaki opozarjajo, da bi kombinacija teh dejavnikov lahko povzročila spiralni učinek. Namreč, kraja uporabniških imen in gesel napadalcem omogoča, da vplivajo tudi na prihodnje vdore v podatke in procese.

LAHKO POMAGA UMETNA INTELIGENCA?

Analiza kaže, da je je bil povprečni čas za odkrivanje in boj proti kršitvam podatkov 287 dni (212 za odkrivanje in 75 za odpravljanje težav), kar je teden dni dlje kot glede na poročilo za leto 2020. Pomembno je tudi to, da se čas za odkrivanje in odpravo škode od leta 2017 vsako leto podaljšuje.

Kot eno od možnih dobrih rešitev za boj proti kibernetskemu kriminalu strokovnjaki za informacijsko varnost predlagajo vključitev umetne inteligence. Zdi se, da umetna inteligenca in varnostna avtomatizacija lahko pomagata pri skrajšanju časa za odkrivanje in odpravo škode ter znižanju povezanih stroškov. Analiza je namreč pokazala, da se je pri popolnoma spremenjenem varnostnem sistemu povprečna škoda zaradi vdorov zmanjšala za skoraj tretjino, tj. na 2,9 milijona dolarjev na incident.

Umetna inteligenca se uporablja pri analizi velikih množic istih podatkov, pa tudi različnih naborov podatkov in je učinkovita pri iskanju korelacij ali potencialnih področij interesa, ki bi predstavljala prevelik izziv za človeške sposobnosti. Pri tem lahko umetna inteligenca hitro oceni veliko količino podatkovnih točk in označi tiste postavke, ki bi jih moral strokovnjak potem natančneje oceniti. Tako lahko človek analizira te ločene primere in ugotovi, kaj je pri njih pravilno in kaj sumljivo. Na ta način umetna inteligenca pripomore k hitrejšemu odvijanju teh operacij, tako da lahko ljudje učinkoviteje opravijo svoje delo za zaščito podatkov. ■