Foto: Depositphotos

Zagotavljanje dobre varnostne drže postaja v današnjem času res velik izziv.

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

Kibernetska varnost

Z avtomatizacijo do obvladovanja kibernetsko-varnostnih tveganj

Organizacije posedujejo informacijska sredstva v obliki podatkov, ki so večinoma shranjeni na računalniških sistemih. Ti sistemi pa so bolj ali manj ranljivi. Vendar je dobra novica ta, da je danes na voljo popolnoma avtonomno računalniško gnano penetracijsko testiranje, s katerim lahko podjetja sproti korigirajo morebitne ugotovljene slabosti v kibernetski obrambi.

Matjaž Kosem, Carbonsec

Danes skorajda ne mine dan, ko na spletu ne preberemo novice o kakšnem hekerskem vdoru in preštevanju poslovne škode, o kakšni novi ranljivosti v sistemih, ki so prisotni v skoraj vsakem podjetju, ali pa o spet novih inovativnih tehnikah socialnega inženiringa, pa tudi o bajnih zaslužkih, do katerih določeni posamezniki pridejo s pomočjo hekerskega izsiljevanja … Zagotavljanje dobre varnostne drže postaja v današnjem času res velik izziv, zato ni čudno, da si marsikateri vodja informacijske varnosti (angl. Chief Information Security Officer – CISO) zastavlja vprašanje, kako naprej oz. kako zares učinkovito obvladovati varnostna tveganja.

Kaj vse vpliva na kibernetsko-varnostna tveganja in kako jih učinkovito obvladovati? Glavna skrb pri varovanju informacijskih sredstev je, da bodo ta vedno na razpolago tistim, ki imajo za njihov dostop pravico, in to v točno takšni obliki, kot morajo biti. Organizacije posedujejo informacijska sredstva v obliki podatkov, ki so večinoma shranjeni na računalniških sistemih. Ti sistemi imajo manjšo ali večjo mero ranljivosti, ki jo lahko izkoristi heker – slednje poenostavljeno imenujemo grožnja. In ker si seveda želimo, da bi bila verjetnost realizacije grožnje čim manjša, bomo naredili vse, da bi to preprečili.

Ker si želimo, da bi bila verjetnost realizacije grožnje čim manjša, bomo naredili vse, da bi to preprečili.

Foto: Depositphotos

Ranljivosti se ves čas spreminjajo. In tudi grožnje se nenehno spreminjajo.

Tveganja, da bi do uresničitve groženj prišlo, lahko praviloma zmanjšujemo na tri načine:

1. Sredstva varujemo z varnostnimi napravami in rešitvami: od relativno majhnega nabora osnovnih zaščit, kot so klasične požarne pregrade in protivirusni programi, več kot desetletje nazaj, se danes v organizaciji lahko najde tudi več kot 100 različnih varnostnih rešitev.
2. Pomagamo si s sistemi za upravljanje z ranljivostjo: na ta način ves čas vemo, kateri sistemi nimajo nameščenih varnostnih popravkov ter katere popravke bi bilo bolj nujno namestiti kot druge.
3. Grožnje spremljamo s pomočjo naprednih orodij za varnostne grožnje, t. i. TI (angl. Threat Intelligence): namen je, da dovolj zgodaj izvemo, ali se nekje dogajajo napadi, specifični za določeno industrijo, ki pa se lahko zgodijo tudi nam.

Že od nastanka računalnikov je obstajala ideja o umetni inteligenci, ki bi človeštvu močno olajševala napredek.

Ker je informacijski sistem »živ organizem«, pomeni, da se vse troje neprestano spreminja. Dodajanje novih sistemov, prenavljanje delov omrežij, povezovanje z oblačnimi storitvami, vpeljevanje novih storitev – ranljivosti se ves čas spreminjajo. Že samo pogled v podatkovno bazo ranljivosti CVE (angl. Common Vulnerabilities and Exposures) razkrije, da se ta neprestano povečuje. Tudi grožnje se spreminjajo, pa naj gre za nove hekerske skupine ali pa nove kampanje s še nikoli videnimi tehnikami napada.

Preverjen, a časovno zamuden način

Eden izmed najboljših načinov preverjanja, kje dejansko smo, je stari dobri vdorni test. Kljub priljubljenosti pa imajo tovrstna testiranja varnosti vendarle nekaj pomanjkljivosti. Test traja vsaj dva tedna, lahko pa tudi precej več, in je zaradi pomanjkanja ekspertov relativno drag. Rezultati so praviloma odvisni od izkušenosti in talenta »pentesterja«, včasih celo dnevne forme ali počutja. Zaradi omenjenega se vdorna testiranja največkrat izvajajo enkrat letno in imajo pravo vrednost le na dan zaključka (»rok trajanja« velja torej do prve spremembe sistema).

Kakšna bi bila možna rešitev?

V idealnem svetu bi bil vdorni test hitrejši, cenejši in popolnejši, torej neodvisen od ekspertize posameznika. Če se nekoliko pošalim, lahko rečem, da bi potemtakem potrebovali 1.000 popolnih pentesterjev v eni škatli in vedno na voljo, po možnosti s pritiskom na gumb. Na srečo je tehnologija, ki lahko popolnoma nadomesti pentesterja v notranjem delu omrežja, danes že na voljo. Že od nastanka računalnikov je obstajala ideja o umetni inteligenci, ki bi človeštvu močno olajševala napredek. Tako je bil slavni šahist Gari Kasparov prvič v zgodovini s strani računalnika premagan že leta 1996. Slavni Stephen Hawking se je umetne inteligence celo bal, saj naj bi po njegovem pomenila tveganje za obstoj človeštva, kar samo pomeni, kakšen velikanski potencial dejansko ima. Razvoj tehnologije je tako prišel tudi do tistih, ki so se zavedali potrebe po vsakodnevnem preverjanju kibernetske varnosti.

Popolnoma avtonomno računalniško gnano penetracijsko testiranje je danes tu in omogoča podjetjem, da vsakodnevno testirajo svojo kibernetsko varnostno držo ter sproti korigirajo morebitne ugotovljene slabosti v kibernetski obrambi.

Danes v kibernetiki ni stalnic. Podjetja, ki se že poslužujejo tovrstne obravnave svoje varnosti, so tako veliko bolj odporna na morebitni vdor, ki lahko močno omaja ugled in stabilnost poslovanja. gg