
Foto: Depositphotos

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

Kibernetska varnost

# Nujno je sodelovanje s strokovnjaki

**Skladno z razvojem tehnologije napredujejo tudi načini, kako jo izkoristiti za manj ugledne namene. Poznavalci priporočajo, da podjetja za zagotavljanje kibernetske varnosti poiščejo strokovno pomoč.**

*Mihael Nagelj, Sekcija za kibernetsko varnost, ZIT, GZS, in Jerneja Srebot*

**Izzivi kibernetske varnosti so vedno bolj kompleksni**

»Številni dogodki v tem letu izpostavljajo naraščanje groženj v kibernetskem prostoru. Poizkusi napadalcev so vedno bolj kompleksni in zahtevni za branitelje informacijske varnosti in s tem poslovnih interesov podjetja,« pravi Mihael Nagelj, vodja Sekcije za kibernetsko varnost Združenja za informatiko in telekomunikacije (ZIT) pri GZS.

V dobi intenzivne digitalizacije s stalnim razvojem tehnologije napredujejo tudi taktike kibernetskih napadov. Poleg povečanega števila naprav v omrežju se je razširil tudi obseg uporabe številnih tehnologij, ki so sicer nujne za nadaljnji razvoj, a hkrati predstavljajo tudi nova tveganja. Kibernetska varnost ni več samo problem posameznih strokovnjakov, pač pa vodilnih v podjetjih in javnem sektorju ter držav v celoti.

»Če smo v preteklosti številne težave lahko reševali z nujnimi organizacijskimi in tehnološkimi ukrepi obvladovanja že poznanih ranljivosti sistemov, dandanes vse bolj prevladuje izkoriščanje ranljivosti, ki so poznane samo hekerjem. Ti jih lahko izkoriščajo za izvedbo kibernetskega napada do trenutka, ko jih avtorji opreme ne odpravijo,« opozarja Nagelj in dodaja, da kompleksnost izzivov zahteva drugačne in bolj intenzivne ukrepe.

**Ukrepi so uspešni, če se jih držijo vsi zaposleni**

Med napadi še vedno prevladuje izkoriščanje človeških lastnosti z metodami socialnega inženiringa, ki omogoči lažji dostop do dragocenih informacijskih virov podjetja. Ker številna podjetja ne morejo zagotoviti ustrezno usposobljenega kadra za spopadanje s stalnimi varnostnimi grožnjami, je po mnenju strokovnjakov nujno intenzivno sodelo-

**Kibernetska varnost ni več samo problem posameznih strokovnjakov, pač pa vodilnih v podjetjih in javnem sektorju ter držav v celoti. Poizkusi napadalcev so vedno bolj kompleksni in zahtevni za branitelje informacijske varnosti in s tem poslovnih interesov podjetja.**

vanje s specializiranimi podjetji, ki lahko ugotovijo stanje odpornosti in kibernetskih tveganj glede na poslovne interese ter pomagajo pri pripravi optimalnega programa ukrepov. Pri tem ne gre zanemariti, da so ukrepi uspešni samo, če jih uresničujejo vsi zaposleni, tako vodilni kot običajni uporabniki informacijskih tehnologij.

Posebno pozornost si pri tem zaslužijo organizacije, ki so del kritične infrastrukture ali pa premorejo procese v okolju operativne tehnologije (OT okolja), brez katerih ne morejo poslovati. Mednje sodijo industrijska podjetja, tovarne, banke, energetska podjetja, logistična in transportna podjetja ipd.

**Dandanes vse bolj prevladuje izkoriščanje ranljivosti, ki so poznane samo hekerjem.**

»V splošnem velja, da kibernetska varnost OT oz. procesnih sistemov okoli 10 do 15 let zaostaja za današnjimi poslovnimi sistemi, ki so bili deležni stalnih vlaganj. Različni industrijski obrati, tovarne, elektrarne, elektroenergetski sistemi in vodovodni sistemi so bili v preteklosti popolnoma izolirani, danes pa se povezujejo v druga omrežja z namenom izmenjave podatkov. Ta okolja so postala zelo zaželene tarče, saj si organizacije ne morejo privoščiti izpada poslovanja ali zastoja v proizvodnem procesu ali dobavni verigi. Poslovodstvo, ki se zaveda in želi zmanjšati varnostna tveganja, poskuša dvigniti raven kibernetske varnosti z vpeljavo ustreznih tehnologij, procesov in znanja,« pravi strokovnjak za kibernetsko varnost ter etični heker Matjaž Katarinčič, vodja tehnološkega področja v podjetju Smart Com.

**Kibernetska varnost OT oz. procesnih sistemov okoli 10 do 15 let zaostaja za današnjimi poslovnimi sistemi, ki so bili deležni stalnih vlaganj.**

## Ključna bo zaščita digitalne identitete

Z množičnim prehodom na delo na daljavo so se morale spremeniti številne dotedanje prakse podjetij. Veliko organizacij se je odločilo, da svoje podatke shrani v oblak, ta prehod pa je bil mamljiva priložnost za nove kibernetske napade. V mnogih primerih oddaljeni delavci za opravljanje svojega dela uporabljajo lastne računalnike in povezavo, zaradi česar so še bolj ranljivi za kibernetske napade.

»Varnost v oblaku postaja glavna skrb mnogih organizacij. Strokovnjaki za kibernetsko varnost bodo imeli nalogo izboljšati sisteme kibernetske varnosti za ublažitev vdorov v oblak,« pojasni vodja varnostno-operativnega centra v podjetju Unistar PRO Alen Jamšek. Po njegovem bo razvoj omrežja 5G prinesel desetkratno povečanje števila naprav interneta stvari, medsebojna povezanost naprav pa povečuje tudi verjetnost kibernetskih napadov zaradi pomanjkanja varnostne infrastrukture in vidnosti med napravami.

Organizacije se začenjajo odmikati od navideznih zasebnih omrežij (virtual private network – VPN) proti brezstopenjskemu dostopu do omrežja z ničelnim zaupanjem (zero trust network access – ZTNA), ki zagotavlja večjo varnost, saj od posameznikov zahteva, da se prijavijo z večfaktorsko avtentikacijo ter preprečuje notranje grožnje z omejevanjem dostopa zaposlenih le do podatkov, ki so potrebni za opravljanje njihovega dela.

»Skupna tema vseh prihajajočih trendov je identiteta. Svojega poslovnega premoženja, vrednosti in ugleda ne moremo zavarovati brez uveljavljanja zaščite digitalne identitete posameznikov in naprav/storitev, zato je ta ključnega pomena za zagotovitev trdne drže podjetja v kibernetski varnosti,« poudarja Jamšek. gg