INTERVJU: **Marko Kašić, vodilni IKT-inženir pri A1 Slovenija**

Zaradi pandemije smo veliko bolj ranljivi tudi na spletu

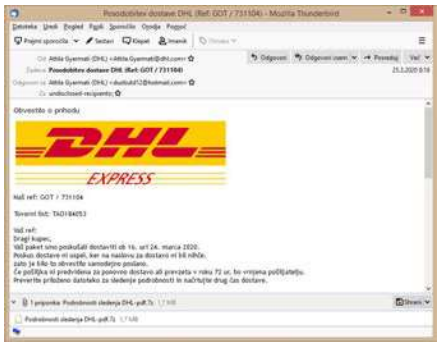
Kdo je najpogostejša tarča kibernetskih napadov?
Izkušnje nas učijo, da so glavne žrtve napadov mala in srednja podjetja, povprečni stroški takšnega napada presegajo 35 tisoč evrov. Velikost ali panoga sicer nimata vpliva na priložnostne napade, ki so največkrat destruktivni in lahko v nekaj minutah zaustavijo celotno poslovanje. Po podatkih evropske konfederacije malih podjetij (ESBA) naj bi kar 60 odstotkov podjetij, ki so bila tarča kibernetskega napada, preživelo le še največ pol leta.

Lahko navedete kakšen primer napada pri nas in kako veliko škodo je povzročil?
Stroški odprave posledic napada so lahko enormni. Spomnimo se odmevnih primerov, kot sta Revoz in Lekarna Ljubljana. Pri prvem je prišlo do zaustavitve proizvodnje, v primeru lekarn pa so stroški odprave posledic incidenta po besedah njihovega direktorja presegli dva milijona evrov.

Ali med podjetji narašča zavedanje o pomembnosti varnostnih rešitev na spletu?
Vsekakor se zavedanje o pomembnosti vsako leto dviguje, o tem pričajo predvsem naložbe na tem področju. Kljub temu je še vedno na voljo veliko prostora za izboljšave. Pri nekaterih podjetjih je zavedanje na tako visoki ravni, da povpraševanje po zelo naprednih rešitvah. Obenem beležimo porast povpraševanja po varnostnih pregledih, ki jih izvajamo tudi na A1 Slovenija. Predvsem je porast pri podjetjih, ki niso zavezana izvajanju, temveč jih izvajajo zaradi lastnega interesa oziroma varnostnega zavedanja.

In katero področje zaščite je trenutno med podjetiji najbolj aktualno?
Trenutno največje zanimanje beležimo na področju zaščite e-pošte. Spremembe načina dela zaradi pandemije so prinesle tudi višjo stopnjo ranljivosti,

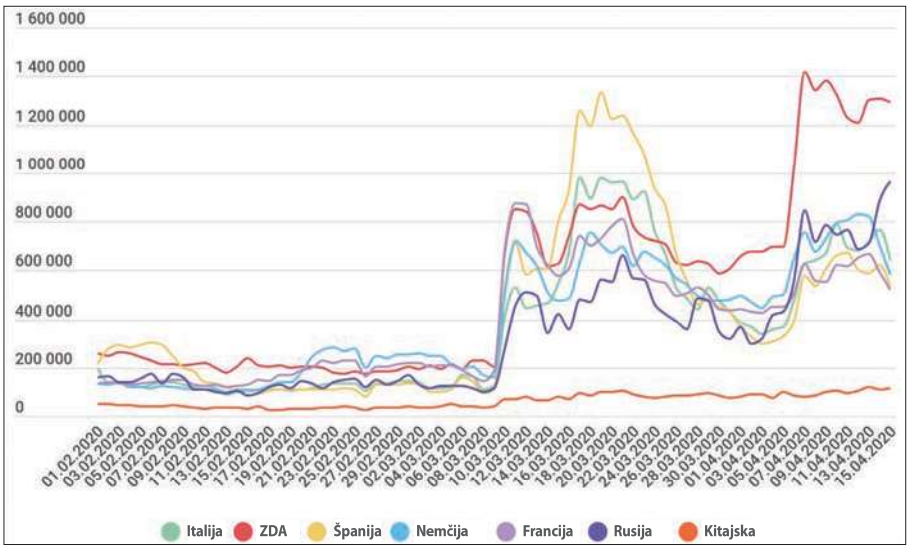
Primer lažnega sporočila DHL o spodleteli dostavi, ki v priponki z dvojnim podaljškom namesto podatkov o pošiljki vsebuje trojanskega konja



Nepridipravi so hitro po začetku karantene pričeli z akcijami razpošiljanja dokaj prepričljivih lažnih sporočil o nedostavljenih paketih, brezplačni zaščitni opremi, potrebi po spremembi računa za nakazilo denarja in podobno. Sodobne zaščite za varovanje elektronske pošte, kakršna je tudi Vade Secure, takšna sporočila z lahkoto prepoznajo in preprečijo, da bi prišla v predale uporabnikov.

saj uporabniki odnašajo službene računalnike v domača omrežja, ki jih podjetja nimajo pod nadzorom. Zato je vsak vstopni vektor potrebno še bolj preveriti. E-pošta je najbolj izpostavljena, saj se prek 90 odstotkov napadov in vstopov v okolja zgodi ali s phishing sporočilom ali z okužbo, poslano kot priponko. Sledi povpraševanje po varnih dostopih do informacijskih sistemov. Predvsem gre za zaščito privilegiranih uporabnikov oziroma administratorjev, da lahko ti na varen način dostopajo do strežnikov. Brez VPN tehnologij seveda ne gre, zato je bil predvsem v začetku pandemije porast tudi na področju požarnih pregrad, ki omogočajo VPN.

Povečanje števila poskusov vdorov čez dostop na daljavo glede na državo v času epidemije COVID-19



S prehodom podjetij na delo od doma so tudi nepridipravi hitro začeli napadati na novo odprte dostope na daljavo. Zaradi uporabe slabih gesel so lahko prek njih vdrli v podjetja, dostopali do zaupnih podatkov in v nekaterih primerih tudi zakodirali podatke in zahtevali odkupnino. (Vir: BleepingComputer.com)

Kaj pa naprednejše rešitve, ki uporabljajo umetno inteligenco?
Analitska hiša Gartner je že pred dvema letoma napovedala, da bosta strojno učenje in umetna inteligenca vpeljana v dve tretjini varnostnih rešitev do konca leta 2022. Pri rešitvah, ki jih mi priporočamo, se umetna inteligenca aktivno uporablja za bolj natančno zaznavanje neželene e-pošte, še posebej pa je rešitev specializirana za preprečevanje t. i. phishing sporočil ter usmerjenih phishing sporočil (spear-phishing). Na tem zadnjem delu se pojavi moč umetne inteligence, ki je sposobna z veliko učinkovitostjo zaznati tovrstna sporočila in naslovnika bodisi obvestiti o tem, da je bolj pozoren, bodisi preprečiti dostavo v celoti.

Drugo področje je zaznavanje vdorov, ki se izvaja prek analize dogodkov na delovnih postajah in strežnikih ter z analizo omrežnega prometa. V obeh primerih se aktivno iščejo vzorci obnašanja napadalca, saj so kljub različnim metodam napadalcev nekatere aktivnosti vedno videti enako, čeprav ne uporabljajo istih orodij. Tako je metoda ali orodje napadalca pravzaprav nepomembno.

Kako lahko A1 Slovenija pomaga podjetjem pri vprašanju kibernetske varnosti?
Prednost A1 Slovenija je, da smo del mednarodne skupine in smo v stalnem stiku z razvojem dogodkov in rešitev tudi na drugih trgih, ki so že dalj časa izpostavljeni napadom bolj kot Slovenija. Povečanje nevarnosti čedalje bolj občutijo tudi slovenska podjetja, tem pa lahko pomagamo na več ravneh. Osnova vsake dobre obrambe sta zadostna raven zavedanja in izobraženost uporabnikov. Že z nekaj dobrimi treningi in izobraževanji lahko v podjetjih dokazano občutno dvignemo raven varnosti. Potem nastopijo seveda najbolj osnovne, a nujne rešitve, kot na primer dobra protivirusna zaščita, požarna pregrada naslednje generacije (UTM), storitev varnostnega kopiranja na oddaljeno lokacijo in zaščita prometa elektronske pošte. Vse bolj pa se uveljavljajo tudi omenjene napredne rešitve, kot denimo sistemi za zaznavanje in odzivanje na vdore, tako na nivoju delovnih postaj in strežnikov kot nivoju omrežja, ter rešitve za upravljanje pravic uporabniških računov ter njihovih dostopov. Na koncu seveda ne smemo pozabiti tudi rednih varnostnih pregledov informacijskih sistemov in zaščito pred DDoS-napadi.