Zakriptirali so mi podatke in želijo odkupnino!

Kaj naj storim?

Zadnje leto in pol nejevoljo med poslovnimi in zasebnimi uporabniki sejejo t. i. izsiljevalski virusi. Gre za škodljive kode, ki se najpogosteje širijo s pomočjo priponk v elektronskih sporočilih. Izsiljevalski virusi, kot so Cryptolocker, CryptoWall, CTB-Locker, Synolocker in podobni na okuženem računalniku zaklenejo vse dokumente z geslom in od uporabnika zahtevajo odkupnino. Kdor nima izdelane varnostne kopije dokumentov/podatkov, lahko računa z več sto ali celo tisoč evrov odkupnine, če želi svoje podatke pridobiti nazaj.

Uporabniki vrednost svojih podatkov in dokumentov žal pogosto spoznamo šele takrat, ko ostanemo brez njih. Ne glede na to, ali gre za zasebne ali poslovne dokumente in datoteke – diplomsko nalogo, finančna ali razvojna poročila, poročne fotografije in video posnetki –, izguba digitalnega dela našega življenja boli. Posebno, če se zgodi zaradi lastne neprevidnosti ali malomarnosti.

A tudi uničenje ali poškodbo prenosnika ali tablice lažje prebavimo, kot okužbo z izsiljevalskim virusom. Neupoštevanje osnovnih načel varne rabe elektronske pošte in spletnih brskalnikov so v zadnjem letu in pol botrovale številnim primerom okužbe z izsiljevalskimi virusi. Ob odprtju okužene priponke v elektronskem sporočilu ali okužene povezave na spletni strani se računalnik ali pametna naprava uporabnika okuži z virusom, nakar ta »zaklene« oziroma kriptira vse dokumente (in celo druge datoteke). Odšifriranje datotek je možno le z zasebnim ključem, ki je v lasti storilca. Tega spletni nepridipravi ponujajo proti plačilu odkupnine, ki v primeru izsiljevalskih virusov Cryptolocker, CryptoWall, CTB-Locker, Synolocker in podobnih tipično znaša med 300 in 1000 evrov.

Mar res ni obrambe?

Ko je naš računalnik okužen in so datoteke zakriptirane, jih lahko nazaj pridobimo le s plačilom odkupnine in pridobitvijo ustreznega gesla. Preventiva je tudi v tem primeru bistveno cenejša od kurative. Klasični protivirusni program ne zadošča več. Spletni napadalci vsak dan v obtok pošljejo okoli 300 tisoč škodljivih kod. Tradicionalne protivirusne rešitve v prvih 24 urah ne prepoznajo kar 18 odstotkov teh škodljivih kod, dobra dva odstotka najbolj trdovratnih virusov pa ne prepoznajo niti po treh mesecih!

Velikokrat ne pomaga niti varnostna kopija podatkov. Zakaj? Čeprav z njeno pomočjo obnovimo datoteke in dokumente, nam lahko napadalci zagrozijo, da bodo naše ukradene dokumente objavili na spletu, če ne bomo plačali odkupnine.

N**apredna prilagodljiva varnostna rešitev**

Podjetje Panda Security je razvilo varnostno rešitev Panda Adaptive Defence, ki poleg izsiljevalskih virusov prepozna in zaustavi še številne druge nove in neznane škodljive kode. Panda Adaptive Defence natančno spremlja vse delčke kode, ki na napravo prihajajo z interneta. V primeru, ko prepozna znane vzorce škodljive kode ali pa opazi sumljivo obnašanje kode, le-to v celoti blokira. Na napravi dovoljuje le izvajanje zaupanja vrednih aplikacij in programov. Po zaslugi kolektivne inteligence rešitev pozna ogromno zaupanja vredne poslovne programske opreme kot tudi vzorcev okužb. Vsako aplikacijo – lokalno ali iz računalniškega oblaka – ustrezno klasificira.

V Panda Security so nov varnostni model načrtovali pet let in zagotovili, da v njem ni »razpok«. Varnostna rešitev temelji na treh principih – stalnem spremljanju obnašanja aplikacij na računalnikih in strežnikih podjetja, avtomatski klasifikaciji aplikacij, podprti s strojnim učenjem ter Pandino platformo v oblaku in delu Panda Laboratorijev, kjer varnostni strokovnjaki stalno analizirajo nove aplikacije ali nove različice aplikacij, ki jih uporabljajo uporabniki širom sveta.

Rešitev je združljiva z vsemi obstoječimi protivirusnimi in omrežnimi rešitvami, Panda Active Defense pa omogoča tudi napredno integracijo s sistemi za odkrivanje vdorov (SIEM). Ker je rešitev Panda Active Defense na voljo kot varnostna storitev iz oblaka in deluje izjemno avtonomno in učinkovito, močno poenostavi delo sistemskim in varnostnim skrbnikom v podjetju. Ti so o poskusih napadov s škodljivimi kodami takoj obveščeni, saj rešitev podatke analizira v realnem času in takoj tudi ukrepa.