Foto: Depositphotos

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

Kako se ubraniti pred spletnimi izsiljevalci

Podjetja lahko sama storijo veliko, da ne postanejo žrtve spletnih izsiljevalcev in prevarantov. Poskrbite za preventivo, dokler je čas.

Barbara Perko

V začetku maja je svet ohromila izsiljevalska okužba WannaCry, ki je izkoristila ranljivost Microsoftovega operacijskega sistema Windows. V enem dnevu je bilo okuženih več kot 230.000 računalnikov v več kot 150 državah. Okužbi so med drugim podlegle britanske bolnišnice, španska Telefonica, FedEx in Deutsche Bahn. V Sloveniji je odmevala zaustavitev proizvodnje v novomeškem Revozu. Zaradi napada se je ustavilo delo v petkovi nočni izmeni, stroji pa so obmolknili za cel konec tedna. Delo se je v normalne tirnice vrnilo šele v ponedeljek. V Sloveniji so poleg omenjenega primera zabeležili še sedem primerov.

Zahvaljujoč 22-letnemu Britancu Marcusu Hutchinsu, ki je po naključju prišel do rešitve za napad, so bile posledice manjše, kot bi lahko bile. Kljub temu, da se je napad zaključil relativno hitro, so ljudje, ki so stali za njim, od svojih žrtev dobili skoraj 30.000 dolarjev v bitcoinih, je poročal BBC.

Prav denar je bil glavni cilj napadalcev, ki so od svojih žrtev zahtevali plačilo odkupnine v zameno za podatke. V kolikor odkupnine ne bi plačali v treh dneh, bi zahtevano vsoto podvojili, po enem tednu pa bi bili zašifrirani podatki izgubljeni.

Izsiljevalski virusi, s katerimi storilci zašifrirajo datoteke, so čedalje pogostejši. Pri SI-CERT so samo maja poleg že omenjenega WannaCry imeli opravka tudi z izsiljevalskim virusom Jaff, ki se širi prek elektronske pošte in zašifrira podatke. Do njih pa je nato možno dostopati le v primeru plačila odkupnine, ki je konec maja znašala 780 evrov. V času pisanja tega članka še ni bilo na voljo orodja, s katerim bi lahko dešifrirali datoteke.

»Še tako močne varnostne rešitve ne preprečijo vdora, če zgolj eden od zaposlenih klikne tja, kamor ne bi smel.«

Nataša Klenovšek Arh, SI-CERT

Priporočila za podjetja

1. Podjetja morajo zaposlene obvestiti o mobilnih tveganjih.
2. Zaposleni, ki uporabljajo lastne mobilne naprave za dostopanje do podatkov in sistemov podjetja, morajo upoštevati navodila podjetja in poskrbeti za ustrezno zaščito ter previdnost.
3. Napravam, ki niso v skladu z varnostnimi politikami podjetja, ne sme biti omogočena povezava v omrežje podjetja.
4. Podjetje naj namesti mobilne rešitve pred grožnjami, s čimer se zaščitijo pred tveganji.
5. Zaposleni naj bodo previdni, ko do podatkov podjetja dostopajo prek javnih omrežij Wi-Fi, saj zanje na splošno velja, da niso varna.
6. Operacijske sisteme naprav in aplikacij je treba nenehno posodabljati.
7. Aplikacije namestite samo iz virov, ki jim zaupate.
8. Preprečite, da bi uporabnik na napravi odstranil varnostne omejitve, ki jih je uvedel prodajalec operacijskega sistema.
9. Razmislite o možnostih shranjevanja v oblaku.
10. Če prejmete sms-sporočilo ali telefonski klic iz podjetja, v katerem od vas zahtevajo osebne podatke, preverite, če gre za verodostojen klic.
11. Med brskanjem po spletu na mobilni napravi se prepričajte, da je povezava zavarovana prek https, kar je zapisano na začetku naslova URL.
12. Nikoli ne kliknite na povezave in priponke v nezaželenem elektronskem sporočilu ali sms-sporočilu. Takšno sporočilo takoj izbrišite.
13. Če se znajdete na spletni strani ali prejmete sporočilo polno pravopisnih in slovničnih napak, bodite še posebej previdni.

Vir: Mobile Malware, Europol, European Cybercrime Centre

Močno je poraslo tudi število okužb z izsiljevalskimi virusi, ki jih napadalci namestijo prek vdorov v odprto storitev za oddaljen dostop do namizja. SI-CERT opozarja, da so tarča sistemi, ki imajo javno odprt dostop do katere od storitev, ki se uporabljajo za oddaljen nadzor in upravljanje s sistemom, kot so Remote Desktop, Team Viewer in VNC. Napadi so usmerjeni predvsem na podjetja in organizacije, saj te najpogosteje uporabljajo te storitve. Po vdoru napadalci izklopijo varnostne mehanizme in zašifrirajo datoteke. Od svojih žrtev pa praviloma zahtevajo odkupnino, ki se giblje vse od 1.000 do 10.000 evrov.

Zgodi se lahko vsakemu

Dr. Andrej Rakar, vodja informacijske varnosti v SIQ, opozarja, da podjetja informacijske varnosti še vedno ne jemljejo dovolj resno. »Prepogosto naletimo na izjave kot na primer, 'Nam se to že ne more zgoditi'. Pa se jim potem to vseeno zgodi. Prav nepoznavanje dejanskega stanja varnosti informacijskega sistema je pogosto razlog za večjo izpostavljenost napadom,« pojasnjuje Rakar.

Nataša Klenovšek Arh iz SI-CERT med pogostimi napakami, ki vodijo do izkoriščanja varnostnih lukenj, izpostavlja neposodobljene operacijske sisteme in antivirusne programe, stare varnostne kopije, manjkajoče varnostne kopije ter nameščene različne »brezplačne« programe, ki lahko v ozadju odpirajo vrata za različne vdore in napade.

»Druga vrsta pomanjkljivosti, morda še pomembnejša kot te 'tehnične' napake, pa je slabo obveščanje in izobraževanje zaposlenih o informacijski varnosti. Uporabniki smo namreč eden od pomembnih členov v celotni varnostni verigi, po navadi tisti najšibkejši člen. Še tako močne varnostne rešitve ne preprečijo vdora, če zgolj eden od zaposlenih klikne tja, kamor ne bi smel,« poudarja Klenovšek Arh.

Kako naj se podjetja obnašajo?

Rakar poudarja, da morajo podjetja celovito pristopiti k upravljanju varovanja informacij. Celovit

Dešifrirna orodja na enem mestu

Europol je skupaj s podjetjema Kaspersky Lab in Intel Security zagnal iniciativo No More Ransom (www.nomoreransom.org). Glavni cilj je pomagati žrtvam izsiljevalskih virusov, da spet lahko dostopajo do svojih podatkov, ne da bi plačali odkupnino. Hkrati želijo izobraževati uporabnike o tem, kako tovrstne okužbe delujejo in kakšne protiukrepe lahko sami uvedejo, da bi se izognili okužbi.

Na spletni strani so na voljo tudi dešifrirna orodja, ki jih lahko posamezniki uporabijo, če postanejo žrtev spletnih napadov. Na strani so zbrana vsa do sedaj odkrita in trenutno dostopna orodja za odšifriranje dokumentov. Od aprila letos je portal dostopen tudi v slovenski različici.

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

pristop zajema vse, od varnega načrtovanja informacijskega sistema, ustrezne varnostne politike, sistema neprekinjenega poslovanja, upravljanja s popravki, ozaveščanja zaposlenih in seveda preverjanja dejanskega stanja varnosti z rednimi varnostnimi pregledi.

Kot primer izpostavlja obsežen izpad informacijskega sistema British Airways konec maja. »Ta varnostni incident je jasno pokazal, da njihov sistem neprekinjenega poslovanja ni ustrezen oz. pri načrtovanju niso ustrezno identificirali vseh tveganj,« opozarja Rakar.

Klenovšek Arh kot najbolj zanesljivo »orodje« za zaščito izpostavlja varnostne kopije. »Teh se lahko oprimemo v primeru, da pride do okužbe z izsiljevalskim virusom, ki zašifrira datoteke na disku in zanj še ne obstaja orodje za povrnitev datotek.« Redno je treba posodabljati operacijski sistem in vse programe na njem.

Samozaščitni ukrep je tudi previdnost pri uporabi elektronske pošte. »Paziti je treba, da ne klikamo na povezave in odpiramo kakršnihkoli priponk v sporočilih, ki jih nismo pričakovali,« poudarja Klenovšek Arh. »Pozorni moramo biti tudi na priponke elektronske pošte, ki vsebujejo dokument, ki od nas za ogled vsebine zahteva vklop makroja.«

Videti je pravo, v resnici pa gre za prevaro

Konec lanskega leta je slovenska policija zabeležila primere, ko so bila podjetja žrtve prestrezanja elektronske pošte med družbo in njenimi poslovnimi partnerji v tujini. Policija podjetjem svetuje, da dobro preverjajo pristnost elektronske pošte.

Kako postopajo storilci? Na elektronski naslov računovodstva ali tajništva podjetja pošljejo lažno

Foto: SIQ

»Ključna vprašanja, na katera je treba odgovoriti, so:

- ali je vzpostavljen informacijski sistem ranljiv na spletne napade;
- ali zaposleni in pogodbeni sodelavci lahko zaobidejo varnostne politike ter nepooblaščeno dostopajo do podatkov organizacije;
- ali imajo uporabniki poslovnih aplikacij res dostop le do tistih podatkov, ki jih potrebujejo.«

dr. Andrej Rakar, vodja informacijske varnosti v SIQ

Foto: Depositphotos

Primer obvestila, ki ga napadalci pošljejo, ko zašifrirajo podatke, v primeru, ko napadejo prek odprte storitve za oddaljen dostop do namizja.
Vir: www.cert.si

Pazite, ko nameščate aplikacije

Policija opozarja, da niso ranljivi samo računalniki, ampak tudi mobilne naprave, zato je treba poskrbeti za njihovo varno uporabo. Previdnost je potrebna pri nameščanju aplikacij, uporabi spletnih bank ter povezovanju v brezžična omrežja.

Pred prenosom aplikacije preverite verodostojnost aplikacije in njenih izdajateljev. Preglejte mnenja in ocene drugih uporabnikov. Preberite navodila, ki se nanašajo na dovoljenja aplikacij. Namestite aplikacijo za mobilno varnost, ki preveri vse aplikacije na napravi in vse, ki jih boste še nameščali.

elektronsko sporočilo, ki je videti kot pravo, saj je ponarejeno zaglavje sporočila. Videti je, kot bi ga poslal direktor ali drug vodstveni delavec podjetja. V lažnem elektronskem sporočilu storilec od odgovorne osebe v podjetju zahteva, da nujno plača nek račun v tujino, pri čemer je sporočilu pripet račun.

Policija podjetjem svetuje izredno previdnost. Še posebej morajo biti pozorna, če dobijo sporočilo, v katerem nekdo iz podjetja, s katerim sodelujejo, naroča neobičajna nakazila v tujino. V takem primeru je treba osebno preveriti okoliščine pri naročniku nakazila.

Storilci podatke o podjetju večinoma pridobijo na spletu, saj tam lahko najdejo tako številke transakcijskih računov podjetij, elektronske naslove, davčne številke in druge podatke. S pomočjo teh podatkov lahko ustvarijo sliko, kot da je njihova zahteva legitimna.

Kaj storiti, če postanete žrtev prevare?

Na vprašanje, kako se odzvati, če je podjetje žrtev izsiljevalske okužbe, Rakar odgovarja: »Organi pregona po navadi svetujejo, da izsiljevalcem odkupnine ne plačamo, saj s tem spodbujamo nadaljnje tovrstno početje. Brez varnostnih kopij pa je žal za nekatera podjetja plačilo odkupnine edini način povrnitve podatkov. Glede na očiten porast tovrstnih napadov v preteklem letu pa je morda res že čas za celovit pristop k zagotavljanju varnosti.«

Klenovšek Arh svetuje, da podjetje poda prijavo na SI-CERT, kjer nato poskušajo ugotoviti vrsto okužbe in možnost odšifriranja okuženih datotek. »V primeru, da za tovrstno okužbo še ne obstaja orodje, s katerim bi lahko datoteke odšifrirali, so na prvem mestu varnostne kopije. V primeru, da podjetje nima strokovno usposobljene IT osebe, se lahko obrne na računalniški servis.«

Kaj prinaša prihodnost

Rakar ocenjuje, da se bo v prihodnje število takšnih napadov le še povečevalo. »S kompleksnostjo, raznolikostjo in mobilno dostopnostjo informacijskih sistemov narašča namreč možnost varnostnih

pomanjkljivosti, težje pa jih je tudi odkriti. Pojavljajo se že druge hujše oblike izsiljevanja, kjer hekerji neopazno vderejo v sisteme in pridobijo občutljive oziroma zaupne podatke organizacije. Za njihovo javno neobjavo pa nato zahtevajo odkupnino. V takšnem primeru varnostne kopije prav nič ne pomagajo,« o novih načinih napadov pove Rakar.

»Oportunistični goljufi na uporabnike dnevno prežijo z različnimi načini prevar, kjer je sam nivo prevare prilagojen tako, da le-ta zajame vsaj manj ozaveščen del populacije. Če se vsak uporabnik drži splošnih preventivnih ukrepov, se tveganja za kakršne koli zlorabe vsekakor zmanjšajo, tako je upoštevanje dobrih praks tukaj na mestu,« svetuje Klenovšek Arh.

»Tovrstnim napadom smo podvrženi vsi. Ne smemo namreč pozabiti na dejstvo, da je vedno več naprav priključenih na internet, s tem pa se dostopnost iz »kjerkoli in kadarkoli« hitro spremeni v »kdorkoli in karkoli«. Pri tem povezljive naprave (IoT, Internet of Things – internet stvari) predstavljajo posebej resen problem, saj proizvajalci premalo pozornosti namenjajo varnosti,« o problemu izpostavljenosti pove Rakar. gg

Najpogostejše vrste napadov

Foto: arhiv SI-CERT

Poleg izsiljevalskih virusov SI-CERT beleži napade s trojanci, ki se po okužbi skrijejo v sistemu in napadalcu pošiljajo zajeta in shranjena gesla ter druge podatke (npr. prijavo v spletno bančništvo). Obravnavali so tudi primere, ko so napadalci ciljali na mala in srednja podjetja oz. organizacije, kjer napadalci pošljejo navodilo za nakazilo denarja v tujino, pri tem pa ponaredijo pošiljatelja, tako da je videti, kot da je sporočilo poslal direktor.

Pogosti so tudi primeri, ko napadalci vdrejo v sistem elektronske pošte podjetja, nekaj časa prikrito spremljajo vso komunikacijo, nato pa ob primernem trenutku s pomočjo različnih filtrov komunikacijo preusmerijo k sebi in posledično tudi nakazila. »Oškodovanja v teh primerih so običajno zelo velika, tudi več 10 oz. 100 tisoč evrov, pregon storilcev s strani policije pa je tudi zaradi krajevne oddaljenosti praviloma neuspešen,« opozarja Klenovšek Arh.

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