BELA KNJIGA

10 področij, kjer so informacijski sistemi slovenskih podjetij najbolj ranljivi

Kibernetska varnost v 2018

Vladimir Ban

SMART COM

Kazalo vsebine

Uvod	1
1. Nezmožnost zaznavanja napadov	2
2. Dostopnost aplikacij z Internet omrežja brez močne avtentikacije	4
3. Visoka varnostna ranljivost industrijskih (OT) okolij	6
4. Nizka raven varnosti spletnih strani in aplikacij	8
5. Prevelika občutljivost na 'phishing' e-mail napade	9
6. Prevelika odprtost VPN dostopov	11
7. Nezadostno varovanje pri napadih z zlonamerno kodo	13
8. Nezadostno izvajanje popravkov notranjih strežnikov	15
9. Nezadostna oz. nična omejitev prometa v notranjost omrežja	17
10. Slaba varnostna osveščenost uporabnikov (in skrbnikov)	19

Uvod

V podjetju Smart Com smo v zadnjih letih izvedli številne varnostne preglede različnih okolij. Na osnovi izkušenj lahko tako dokaj dobro ocenimo varnost informacijskih sistemov v slovenskih podjetjih. Glede na specifiko posameznega okolja pri oceni stanja informacijske varnosti le te tudi upoštevamo.

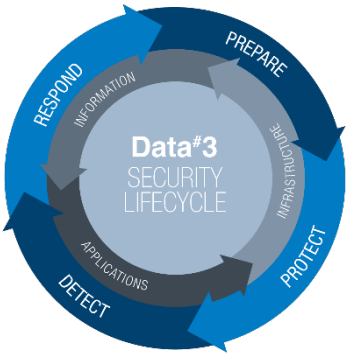
A neodvisno od tega lahko zaznamo nekatere skupne težave in izzive, ki veljajo za vse. Na osnovi našega poznavanja in praktičnih izkušenj smo tako identificirali 10 področij, na katerih so informacijski sistemi v slovenskih podjetjih najbolj ranljivi.

1.
poglavje

Nezmožnost zaznavanja napadov

Z namenom varovanja svojih informacijskih sistemov so podjetja do sedaj večino svojih aktivnosti, sredstev in energije usmerjala v implementacijo varnostnih rešitev, ki so bolj ali manj uspešno preprečevale zlorabo informacijskih sistemov. Zagotavljanje varnosti z implementacijo mehanizmov zaščite je seveda pomembno, a žal nezadostno.

Vsi smo že velikokrat slišali stavek: »Če nekdo res želi vdreti v IT sistem, mu bo to tudi uspelo«. In res se lahko v praksi izkaže, da je praktično nemogoče popolnoma preprečiti vdor. Za vsak varnostni sistem se gotovo najde način, kako ga zaobiti.



Vsekakor to ne pomeni, da ustrezne varnosti ni možno vzpostaviti.

Če velja prepričanje, da je nemogoče vnaprej preprečiti vdor v informacijski sistem, potem zagotovo velja tudi prepričanje, da je vdor nemogoče izvesti na način, ki bi ostal neopažen. Ali menite, da se lahko s to trditvijo strinjamo?

Prav v tem delu vidimo pri slovenskih podjetjih in njihovih informacijskih sistemih ranljivost oz. največjo možnost za izboljšave. Ocenjujemo, da je ena izmed največjih pomanjkljivosti oz. ranljivosti nezmožnost podjetij, da zaznajo varnostne incidente, ki se dogajajo.

Če si predstavljamo napadalčevo pot od začetne do končne točke vdora, lahko hitro vidimo, da se na tej poti pojavi veliko poskusov izrabe ranljivosti, zlonamernih klicev, tehnik socialnega inženiringa in podobnih zavajanj mehanizmov informacijske varnosti. Na vsakem posameznem koraku napadalec pušča sledi. Te se kažejo v povečanem prometu, v nenavadnih zapisih v log datotekah, nenavadnih vzorcih mrežnega prometa, uporabniki opazijo neobičajna e-mail sporočila itd. Namigi, da se dogaja vdor so vedno prisotni in napadalec je stalno v nevarnosti, da bo opažen. Če vdora ne moremo onemogočiti s tehničnimi mehanizmi, imamo na voljo različna sredstva, s katerimi lahko namige ustrezno prepoznamo in vdor še pravočasno odkrijemo.

Pri izvedbi vdorov v sklopu testiranj informacijskih sistemov naročnikov, smo naleteli na dve vrsti okolij:

- Prva so brez varnostnih mehanizmov, ki bi zagotavljali spremljanje

varnostnih dogajanj. Napadalec takšno situacijo zelo hitro razbere, kar seveda predstavlja zelo veliko tveganje. Če napadalec ne naleti na prepreke, bo eden izmed njegovih zlonamernih poskusov prej ali slej uspešen. To je enako, kot če bi okrog hiše postavili kamere in namestili močna protivlomna vrata, za kar bi porabili veliko denarja. Vse to daje vtis visoke varnosti.
A nato nihče ne spremlja kamer oz. nihče ne ukrepa, če napadalec s kladivom udari po oknih.

- Pri drugih pa mehanizmi spremljanja obstajajo, a so nezadostni in neučinkoviti. Skrbnik sistem spremlja preko dnevniških datotek. Obstajajo tudi avtomatizirani mehanizmi »zaklepanja« dostopov, redko kje pa so popolni in zadostni. Spremljanje dogajanj je več kot samo spremljanje dnevniškega zapisa na požarni pregradi ali npr. namestitev Dark Trace sistema . Zadosten in delujoč način zaznavanja napadov je kompleksna kombinacija tehničnih sredstev, procesov v podjetju, znanja in človeških virov. Na žalost je to le redko kje ustrezno rešeno. Zato pri vdorih največkrat nismo bili opaženi, ali pa smo v dani točki celo bili, a so bile reakcije neustrezne, kar nam je omogočilo, da smo kasneje oz. na drugačen način lahko nadaljevali z vdorom.

Procesa zaznavanja napadov in varnostnih incidentov ni enostavno vzpostaviti. Zmožnost izhaja iz ustrezne kombinacije tehničnih sistemov, procesov v podjetju, znanja ter človeških virov. V prihodnjih letih ravno na tem področju pričakujemo največ sprememb – največ investicij in izboljšav.

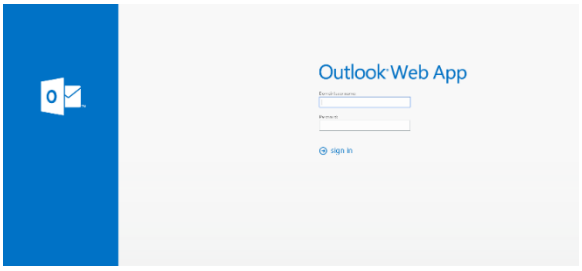
2.
poglavje

Dostopnost aplikacij z Internet omrežja brez močne avtentikacije

Mobilnost nas sili, da informacijski sistem odpiramo v svet. Naši zaposleni želijo dostopati do svojih servisov, tudi ko se nahajajo izven pisarne. Tako ni prav nič nenavadno, da lahko zaposleni preko Internet omrežja dostopajo do svoje elektronske pošte, CRM in BI sistemov ter ostalih aplikacij, ki nudijo določene storitve.

Takšne potrebe po dostopu so razumljive in naloga skrbnikov ni, da te dostope preprečujejo, ampak jih omogoči in hkrati naredi varne.

A v Sloveniji žal marsikje temu ni tako. **Nezadostna varnost oddaljenih dostopov do notranjih aplikacij je pomembna ranljivost pri informacijskih sistemih, ki smo jo zaznali v slovenskem poslovnem okolju.**



Kaj imam v mislih z nezadostno varnostjo? Vsekakor je uporaba zgolj statičnega gesla nezadostna. To velja tudi, če je geslo vezano na centralni AD imenik. 'Phishing' napadi s krajo gesla so realni in zelo učinkoviti.

Napadalec v primeru kraje gesla ne pridobi dostopa le do dotičnega vstopnega portala (npr. 'webmaila'). V primeru, da je ukradeno domensko geslo, pa lahko zelo učinkovito zlorabi še druge aplikacije. Poglejmo enostaven primer, ki je zelo uspešno deloval v praksi. Uporabniku pošljemo lažno sporočilo, da mora zaradi težav s ponovno prijavo v svoj 'webmail', obnoviti svoj uporabniški račun. Pri tem seveda podtaknemo lažni 'webmail' dostop, ki je identičen tistemu, ki ga uporablja podjetje. Uporabnik brez pomislekov vpiše svoje geslo. Napadalec si še namesti AnyConnect VPN klienta in vstopi v VPN točko podjetja z ukradenim domenskim geslom ter tako neovirano dostopa do virov v notranjem omrežju.

Kraja gesel enega portala torej ne pomeni nevarnosti samo za ta portal, ampak so posledice zlorabe bistveno širše.

Zato uporabo statičnih gesel raje nadomestimo z uporabo dvonivojske avtentikacije. Uporabnik mora najprej vpisati uporabniško ime in geslo, nato pa še dinamično geslo (npr. geslo-kodo, ki jo sistem pošlje preko SMS-a). Takšna avtentikacija je varnejša, a še vedno ni 100 %. 'Phishing' napad na dvonivojsko avtentikacijo je še vedno mogoč. Napadalec lahko podtakne lažni portal in vse kar uporabnik vpiše vanj, napadalec prestreže in vpiše v pravi portal. S pravimi skriptami so takšni napadi še vedno zelo učinkoviti. Pri tem pa se skriva še ena 'past'. Morebiti napadalec sploh ne želi zlorabiti dostopa. Navaden 'phishing' napad s krajo začetnega gesla napadalcu mogoče ne omogoči dostopa do aplikacije, mu pa omogoči

krajo domenskega gesla. Z njim lahko kasneje zlorabi marsikatero drugo aplikacijo, ki temelji na domenski avtentikaciji.

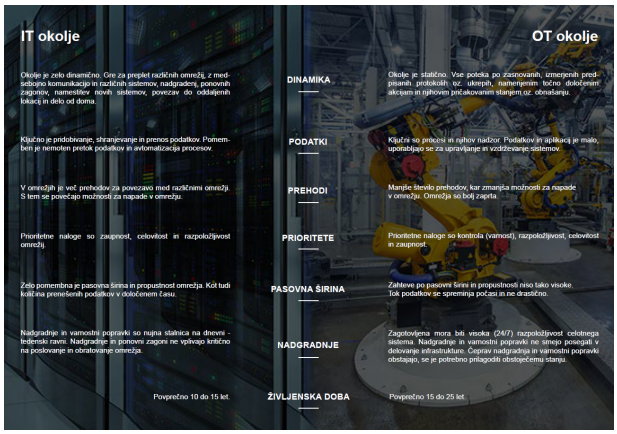
V resnici se prava avtentikacija prične šele z uporabo digitalnih certifikatov ali podobnih mehanizmov.

Vstopna okna, ki omogočajo dostop do notranjih aplikacij je potrebno omejiti. To pomeni, da so navzven dostopne le aplikacije, ki jih določena skupina uporabnikov zares potrebuje. Na voljo jim morajo biti le tisti servisi v aplikacijah, ki so potrebni. Dodatno je na teh dostopih potrebno poskrbeti za ustrezno avtentikacijo (recimo z digitalnimi certifikati) in vsebinsko kontrolo vnosov (recimo spretne požarne pregrade – ang. WAF). Zelo koristno pa je nato vsa dostopna okna budno spremljati (napačne prijave, prijave iz nenavadnih IP-jev oz. ob neobičajnih urah…).

3.
poglavje

Visoka varnostna ranljivost industrijskih (OT) okolij

OT okolje je industrijsko IT okolje. Ta okolja so sestavni del marsikaterega podjetja. Res je, da niso prisotna v vseh podjetjih, vendar se problematika varnosti v industrijskih okoljih nanaša na širši krog podjetij, kot to lahko sklepamo iz imena oz. izgleda na prvi pogled. Podobne izzive imajo lahko tudi trgovska ali logistična podjetja, ki imajo avtomatizirana skladišča, storitvena podjetja, ki imajo avtomatizirane stavbe ter podjetja, ki upravljajo kritično infrastrukturo ipd. OT se torej ne nanaša zgolj neposredno na klasično industrijo, ampak je obseg ranljivih podjetij veliko širši.



V čem je izziv?

Za varnost IT okolja in sistemov (računalnikov, strežnikov, tiskalnikov, drugih pametnih naprav, operacijskih sistemov, aplikacij, podatkov…) znamo relativno dobro poskrbeti. Celotno informacijsko okolje je seveda lahko zelo kompleksno, a takšnega sveta smo (skrbniki) vajeni in bolj ali manj uspešno obvladujemo varnostna tveganja.

V OT (procesnih) okoljih pa je povsem drugače. Ta okolja so prepletena z različnimi avtomatiziranimi vmesniki, kontrolerji. Skrbniki IT okolja največkrat nimajo točnega vpogleda v dejansko stanje naprav, niti v njihovo delovanje. Zelo pogosto avtomatizirane naprave delujejo na starejših (in seveda zelo ranljivih) operacijskih sistemih. Nadgradnja je pogosto nemogoča ali zelo težavna. Z vidika IT skrbnikov je to skoraj tako, kot da bi imeli del omrežja, za katerega ne bi točno vedeli, koliko računalnikov vsebuje, z nameščenimi Windows XP-ji, kaj na njih teče, kdo in na kakšen način z njimi komunicira. Gesla bi imela privzete nastavitve. Ničesar ne bi smeli spremeniti ali nadgraditi, saj posledično lahko tvegate nedelovanje krmilnega procesa. Seveda si ob tem lahko predstavljate, **kako ranljiva so ta okolja**, obenem pa je varnost (skorajda) nemogoče zagotoviti.

Dokler so bila OT okolja zaprta, izolirana od ostalega informacijskega okolja, njihova varnost ni predstavljala večjega problema. Za njih so skrbele posebne, za to usposobljene službe ali zunanji izvajalci. Na popisu IT groženj se OT okolja sploh niso pojavljala.

A sedaj temu ni več tako. OT okolja so zaradi digitalizacije in avtomatizacije procesov vse bolj odpirajo navzven in povezujejo z IT okoljem. S tem pa so postala 'dostopna' napadalcem z Internet omrežja ter raznim okužbam, ki prihajajo iz IT

sistemov. V zadnjih letih je smo bili priča kar nekaj (ne)posrednim napadom na OT omrežja. Najbolj znan primer pri nas je zagotovo napad z WannaCry virusom leta 2017, ki je prizadel podjetje Revoz, za nekaj dni ustavil njihovo proizvodnjo in povzročil ogromno škodo.

OT omrežja so še dodatno ogrožena zaradi dejstva, da so mikavnejša tarča od klasičnih IT sistemov. Veliko napadalcev namreč predvideva, da bo zlorabo lažje izvedel v OT kot v IT okolju. Prav tako lahko napadalci z zlorabo OT okolja bistveno bolj neposredno vplivajo na delovanje nekega podjetja, sistema ali celo države, škoda pa je posledično lahko veliko večja kot v klasičnih IT okoljih.

Varnostni pregledi v letu 2018 med slovenskimi podjetji jasno pokažejo, da velika večina izmed njih ni pripravljena na varnostne izzive OT omrežij.

OT omrežja v slovenskih podjetjih so večinoma varnostno zelo ranljiva, saj so v veliki večini primerov povezana z IT omrežji, hkrati pa na tej povezavi ni prave kontrole, zaznave incidentov, omejitev in avtentikacije. Večina podjetij se izziva reševanja varnostne problematike v OT okoljih sploh še ni zares lotila (ni jasno, kdo je za varnost odgovoren, IT oddelki ali vzdrževalci OT omrežja, ki varnostnih mehanizmov ne poznajo dovolj dobro ipd.).

4.
poglavje

Nizka raven varnosti spletnih strani in aplikacij

V zadnjih letih smo v naših strokovnih vsebinah v obliki raznih prispevkov, novic in belih knjig velikokrat opozorili na ranljivost spletnih aplikacij.

V IT svetu so namreč spletne aplikacije zelo pogoste. Lahko trdim, da v Sloveniji ni podjetja, ki ne bi ponujal takšne ali drugačne spletne aplikacije. Ravno zaradi svoje kompleksnosti prinašajo celo vrsto groženj. Skrbniki se vseh marsikdaj niti ne zavedajo v celoti, saj jim za to primanjkuje poznavanje in razumevanje tehničnega vidika groženj.

Prvi izziv nastane že pri definiciji pojma spletna aplikacija. Marsikdo pod ta pojem še vedno uvršča le klasične aplikacije, kot so spletne trgovine, spletne banke ipd. Seveda gre za spletne aplikacije, a še zdaleč niso edine. Pod pojem spletne aplikacije sodijo namreč tudi ostale aplikacije, vključno s splošnimi spletnimi stranmi podjetja. Zakaj je to pomembno? Ker ima marsikatera ranljivost enak ali zelo podoben destruktiven učinek tudi na navadne spletne strani. Pri aplikacijah, ki so že na videz kompleksne, obstaja visoko zavedanje, da je groženj veliko. Pri navadnih aplikacijah in spletnih straneh pa se tega premalo zavedamo. Podcenjevanje posledic ranljivosti za t. i. «enostavne« aplikacije in spletne strani je v veliko primerih **pomemben dejavnik za doseganje nižjega nivoja varnosti.**

Drug pomemben izziv nastane pri razumevanju lastništva, skrbništva oz. odgovornosti za varnost. V praksi se veliko spletnih aplikacij in spletnih strani nahaja nekje izven podjetja, v gostovanju pri ponudniku tovrstnih storitev. Naleteli smo na veliko primerov, ko se skrbniki premalo zavedajo, da velik del groženj za njihov informacijski sistem še vedno obstaja in da ponudnik gostovanja v večini primerov ne poskrbi za varnost v zadostni meri, ker je osredotočen zgolj na »obratovanje« storitve.

Varnostni pregledi v letu 2018 so jasno pokazali, da večina podjetij v Sloveniji uporablja ranljive spletne aplikacije in ima ranljive spletne strani. Zaznane ranljivosti mnogokrat prinašajo hujše posledice kot le nepooblaščeno spremembo vsebin oz. nepooblaščen dostop do omejenega dela »nepomembnih« podatkov. V nekaterih primerih so ranljivosti spletnih strani celo omogočile poln dostop do notranjega omrežja in vseh pomembnih podatkov v podjetju.

Hitrih in enostavnih navodil, kako to stanje izboljšati, ni. Potrebno je izvajati podrobne varnostne preglede spletnih strani in aplikacij po metodologiji OWASP TOP 10 ter seveda upoštevati popravke, ki jih tovrstni pregledi identificirajo kot potrebne. Najbolj učinkovit način zagotavljanja varnosti je, da se preglede aplikacij vključi že v fazo razvoja in vzpostavitve nove aplikacije ali spletne strani.

5.
poglavje

Prevelika občutljivost na 'phishing' e-mail napade

Tehniko 'phishing' e-mail napadov smo v tem dokumentu že omenili. 'Phishing' napadi oz. ribarjenje so najpogostejši način, s katerim napadalci izvedejo napad na informacijski sistem. Kompleksnejši napadi seveda vključujejo še druge korake in tehnike, a 'phishing' e-mail je velikokrat sestavni del napada. V marsikaterem pogledu celo najpomembnejši del napada.

V tehničnem smislu je take napade nemogoče preprečiti. S tem, ko grožnjo uvrščamo med najbolj pomembne grožnje slovenskih informacijskih sistemov, ne želimo podjetja strašiti, da so napadi možni (ker praksa potrjuje to dejstvo). Poudariti želimo, da niso upoštevana osnovna varnostna pravila, ki tovrstne napade v podjetjih omejujejo ali vsaj otežijo.

Napadi z zlonamerno elektronsko pošto so lahko zelo raznoliki. Lahko gre za poskuse kraje gesel ali podobnih podatkov, ki jih uporabniki nehote vpišejo v lažna vnosna okna na spletni strani, kamor jih preusmeri povezava v zlonamerni e-pošti. Lahko gre za poskuse vnosa zlonamernih datotek. Lahko pa gre za raznorazne

prevare, kjer napadalec uporabnika želi zavesti k plačilu fakture na bančni račun, po svoji želji. Vsem tem napadom je skupno to, da želi napadalec tako ali drugače zavesti uporabnika in ga prepričati, da je poslano elektronsko sporočilo resnično.

Visoka ogroženost pred 'phishing' napadi je tudi povezana z drugimi grožnjami, ki jih v tem dokumentu izpostavljamo v ločenih poglavjih. Recimo nezmožnost zaznavanja napadov, lovljenja okuženih datotek z neznanimi virusi, slaba varnostna osveščenost uporabnikov, nepotrebno odprt ali nezadostno zavarovan 'webmail' dostop v svetovnem spletu in še bi lahko naštevali. Vse to ima neposreden vpliv na visoko uspešnost in destruktivnost 'phishing' napadov v nekem okolju.

Na tem mestu želim izpostaviti dodatne nastavitve oz. sisteme, ki so zelo pomembni pri zagotavljanju večje varnosti pred napadi z zlonamerno elektronsko pošto. Gre predvsem za nastavitve poštnih sistemov, ki znižajo nivo nevarnosti in omejujejo načine, s katerimi napadalec pretenta uporabnike, da zaupajo lažni e-pošti. Nastavitve bodo poskrbele, da bodo napadalci bistveno težje prepričali uporabnike, da je poslano elektronsko sporočilo resnično.

Gre za 4 zlata pravila:

- Ne omogočimo prejemanja elektronske pošte, ki trdi da prihaja od notranjega uporabnika, v resnici pa prihaja od zunaj.
- Ne omogočimo prejemanja elektronske pošte iz domene, ki v resnici sploh ne obstaja ali pa je na črni listi.
- Elektronsko pošto, ki prihaja iz znanih domen, a ne prihaja s strani avtenticiranih strežnikov (ali pa tega ni možno preveriti) je potrebno označiti kot 'spam'.
- Vso elektronsko pošto, ki po svoji obliki, manjkajočih podatkih v zaglavju ali drugih podobnih tehnični parametrih odstopa od normalne pošte, je potrebno označiti kot 'spam'.

Marsikatero podjetje v Sloveniji na svojih poštnih sistemih ne upošteva navedenih pravil, zato je zloraba preko lažnih in zlonamernih elektronskih sporočil zelo realna in resna.

Kako točno se navedena pravila implementirajo v posamezno okolje, je odvisno od tehničnih specifik okolja. Prav tako veljajo posebnosti v primeru, ko je sistem elektronske pošte v oblaku. Ob neupoštevanju zlatih pravil bo okolje bistveno bolj ranljivo za napade z zlonamerno elektronsko pošto, ko pa bi bilo sicer.

6.
poglavje

Prevelika odprtost VPN dostopov

Pri oddaljenih dostopih imamo v mislih bodisi uporabnike, ki se na centralno lokacijo povezujejo samostojno (preko VPN klientov), bodisi uporabnike, ki se povezujejo skupinsko (preko VPN 'site-to-site' tunelov). Med uporabnike, ki dostopajo do informacijskega sistema 'od zunaj', spadajo tako notranji kakor zunanji uporabniki.

Skoraj vsako podjetje ima oddaljene lokacije, ki se povezujejo s centralnim omrežjem, zunanje partnerje z različnimi dostopi do centralnega omrežja (za izvajanje vzdrževanj, konfiguracij ipd.) in/ali posameznike-zaposlene, ki se morajo občasno 'od zunaj' prijaviti v centralni informacijski sistem.

Rešitev, ki rešuje problem varnega prenosa podatkov, je VPN tehnologija. Tehnologija je razširjena in pri uporabi ni težav. Zaplete se pri avtentikaciji VPN dostopov (glej drugo poglavje) ter pri pravicah, ki jih VPN uporabniki imajo – več o tem v nadaljevanju.

Generalno ocenjujemo, da so pravice VPN uporabnikov (bodisi posameznikov, bodisi celotnih oddaljenih lokacij) pri dostopih v notranja omrežja, neustrezne. VPN dostopi tako predstavljajo eno izmed večjih groženj našim informacijskim sistemom. Zavedati se moramo, da so VPN dostopi zelo mikavna tarča za napadalce. Napadalcu je bistveno lažje vdreti na oddaljeno lokacijo, kot da se ukvarja z varnostnimi sistemi na centralni lokaciji. Preko VPN povezav ima potem neoviran dostop do centralnega omrežja. Grožnje ne predstavljajo samo napadalci, neustrezno omejeni VPN dostopi so namreč idealni za hitro in neomejeno širjenje virusnih okužb z ene lokacije na drugo.

Tipični primeri situacij, ko VPN dostopi dajejo uporabnikom preveč pravic:

- **Posamezni uporabniki imajo preko VPN povezave odprt dostop do celotnega omrežja, čeprav zares potrebujejo dostop le do posameznih storitev**
  (princip, da se uporabnika preko oddaljenega dostopa obravnava enako kot uporabnika ki dostopa iz delovne postaje v lokalnem omrežju, ni dober).

- **Zunanjim izvajalcem in partnerjem dopuščamo preširok dostop do omrežja.**
  Zunanji izvajalci marsikdaj vzdržujejo vse in praviloma jim zaupamo. A tu ne gre za vprašanje, da bodo zlorabili svoj dostop. Gre za to, da bo širok dostop izkoristil napadalec oz. virus. Zakaj bi recimo dopuščali odprt dostop na vrata TCP 445 preko VPN povezav, če ga zunanji izvajalci ne uporabljajo.
- **VPN povezave na videz omejimo na posamezne točke, a dostopi so takšni, da lahko uporabniki brez problema dostopajo do kjerkoli v omrežju.**
  V enem primeru je dostop neomejen 'any-any-allow'. V drugem primeru, pa se je skrbnik potrudil in lahko VPN uporabniki dostopajo le do terminalskega strežnika preko RDP dostopa. Sta ti dve na videz zelo različni omejitvi res tako zelo različni? V resnici niti ne.
- **Oddaljenim lokacijam (še posebej iz tujine) dopuščamo preširok dostop.**
  Povsem razumljivo je, da morajo naše oddaljene lokacije dostopati do pomembnih delov našega informacijskega sistema. Njihovi delovni procesi so podobni našim. Vendar pa moramo nekje narediti varnostni rez. Če imajo lokacije enako ali primerljivo varnost kot je varnost na centralni lokaciji (protivirusna zaščita, požarna pregrada z vsemi funkcionalnostmi in omejitvami prometa ipd.), potem so lahko notranji VPN dostopi med lokacijami široki. Če pa varnost na oddaljenih lokacijah ni primerljiva (in marsikdaj ni), pa temu ne sme biti tako. Tipična napaka slovenskih podjetij je, da imajo recimo manjše predstavništvo v tujini, s petimi delovnimi postajami, ki so z enostavno požarno pregrado neposredno povezane v Internet omrežje. Če primerjamo njihovo varnost z varnostjo delovnih postaj na centralni lokaciji, je ta neprimerljiva. Na tej oddaljeni lokaciji ni 'proxy' strežnika, ni APT zaščite, ni 'nadležnega' požarnega zidu. In nenazadnje ni 'nadležnega' skrbnika. Oddaljena lokacija je na zelo enostaven način povezana v svet. Vendar tej isti lokaciji preko VPN tunela odpremo dostop do našega celotnega informacijskega sistema, saj uporabniki potrebujejo dostop do ERP sistema, elektronske pošte, CRM sistema… Kar pa je s stališča varnostno zelo sporno.

7.
poglavje

Nezadostno varovanje pri napadih z zlonamerno kodo

V tehničnem smislu je vnos zlonamerne kode v okolje podjetja, ki je tarča napada, eden izmed najbolj klasičnih načinov napada. Ne nujno edini, vsekakor pa zelo pogost.

Z različnimi prenosnimi podatkovnimi mediji (npr. USB ključki) lahko napadalec v podjetje pretihotapi različne 'key-loggerje' ali podobne 'vohunske' programe. S posebnimi programčki, ki so del zlonamernih kod, lahko prevzeme kontrolo nad notranjimi delovnimi postajami, lahko pa vsebuje tudi destruktivno kodo, kot je na primer kripto-virus. Napadi in nameni so različni, praviloma pa zelo nevarni.

Zlonamerna koda se nahaja v različnih programčkih in napadalec jo želi prenesti do uporabnika. Koda se nato zažene avtomatsko ('autorun' na USB ključku) oziroma s pomočjo uporabnika, ki odpre datoteko.

Tovrstni napadi niso nič novega. Vsi uporabniki in skrbniki so že slišali za virus. Prvi virusi segajo v začetek uporabe Windows okolij in računalniških iger. V resnici je bil izziv virusov oz. zlonamerne kode v preteklosti že rešen. Vzpostavili so se mehanizmi protivirusne zaščite in bolj ali manj so vsa urejena okolja upoštevala osnovna načela varovanja pred virusi, zato zadeve niso bile kritične. Res je tu in tam še prihajalo do kakšne okužbe, a incidenti so bili zelo lokalno omejeni in povečini manj pomembni.

A danes nezadostna zaščita pred vnosom zlonamerne kode v notranjost omrežja predstavlja enega izmed glavnih ranljivosti podjetij.

Kaj se je spremenilo, da je ta nevarnost zopet postala resna?

1. **Napadalci so ponovno prevzeli princip zlonamernih kod kot enega izmed glavnih vektorjev napada.**
   Vzporedno s tem so se razvili bistveno bolj destruktivni virusi, kot smo jih poznali. Danes virusi brez usmiljenja brišejo datoteke, prevzemajo nadzor nad delovnimi postajami ter uničujejo in podirajo vse, kar najdejo.
2. **Hitrost širjenja zlonamerne kode se je korenito spremenila.**
   Vsem nam dobro poznana protivirusna zaščita ima namreč eno pomanjkljivost, ki izhaja iz njene logike delovanja. Protivirusna zaščita vsebuje bazo znanih virusov. Nadzor datotek se izvaja tako, da se preveri, če vsebujejo katerega izmed virusov iz baze. To pa pomeni, da je virus vsaj na začetku vedno uspešen. Ko se pojavi nov virus, bo ta seveda najprej neopažen in

bo šele par ur ali dni kasneje dodan v bazo znanih virusov. Ta pomanjkljivost včasih ni bila pomembna. Širjenje virusov je bilo relativno počasno in v večini primerov so se naše protivirusne zaščite pravočasno posodobile, še preden so nas dosegli novi virusi. Danes pa temu ni več tako. Ko se na enem koncu pojavi WannaCry virus, bo uspel okužiti delovne postaje globalnih razsežnosti, še preden bodo protivirusni sistemi doumeli, kaj se dogaja.

3 **Pospešen razvoj sistemov za izdelavo novih virusov.**
Marsikdo ob tem pomisli, da je vse zgoraj zapisano res, ampak da mora biti zmožnost kreiranja vedno novih virusov vseeno nekako omejena. Sklepamo lahko, da ni najbolj enostavno napisati popolnoma novega virusa. In res ni. Vendar napadalci pri svojih napadih mnogokrat sploh ne uporabijo novih virusov. Razvile so se namreč različne delujoče tehnike, ki datoteke preoblikujejo tako, da njihovo osnovno delovanje ostaja nespremenjeno, po svoji strukturi pa so popolnoma drugačne. Protivirusni sistemi na ta način niso zmožno zaznati starih že znanih virusov, saj je za njih to popolnoma nov virus.

Zaščita pred zlonamerno kodo, ki bi slonela zgolj na protivirusni zaščiti, danes ni več zadostna.

Potrebno je uvesti nove sisteme. Sistemi, ki učinkovito naslavljajo ta izziv so sistemi APT. Njihovo delovanje temelji na principu 'Sand-box' tehnologije, ki namesto iskanja znanih virusov raje 'opazuje' obnašanje programov. Ti sistemi predstavljajo bistveno bolj kvalitetno in robustno zaščito pred zlonamerno kodo in njeno širitvijo. Čeprav je rešitev znana, ocenjujemo, da še ni implementirana v zadostni meri:

- Številna okolja tovrstnih sistemov še ne uporabljajo.
- Pri nekaterih smo sicer opazili, da tehnologija obstaja, a je zaščita nepopolna. Nadzoruje se le promet med notranjim in zunanjim omrežjem – t. i. N-S promet, ne nadzira pa se notranji promet med delovnimi postajami in strežniki – t. i. E-W promet, kjer se najprej pojavi širjenje virusa. Obstaja pa še tretja možnost in sicer, da se nadzira vse, razen SSL prometa.

8.
poglavje

Nezadostno izvajanje popravkov notranjih strežnikov

Strežniki so postali pomembni deli informacijskih sistemov. Na njih tečejo aplikacije, podatkovne baze in podobne zadeve. S tem pa so postali tudi zelo zaželena tarča napadalcev.

Klasičen napad na informacijski sistem praviloma poteka na sledeč način. Napadalec naprej želi tako ali drugače vstopiti v notranjost omrežja. Ko mu to uspe, pa želi priti do strežnikov. Strežnikov se praviloma ne napada neposredno iz Internet omrežja, saj je dostop do njih od tam zaprt. Strežnike se napada preko notranjih delovnih postaj, do katerih je napadalec predhodno uspel pridobiti dostop.

Strežniki delujejo na različnih operacijskih sistemih. Na njih tečejo različni servisi in aplikacije. **Pomemben del varnosti strežnika so nastavitve, še bolj pomemben del pa je varnost programske opreme.** Programska oprema ter operacijski sistemi strežnikov prinašajo celo vrsto potencialnih ranljivosti.

Ko napadalec pride do točke, da se lahko 'dotakne' notranjega strežnika, je nadaljnja uspešnost vdora skoraj vedno odvisna od storitev, ki jih strežnik ponuja in ranljivosti na strežniku. V kolikor je teh več, bo za napadalca enostavneje najti način vdora, v kolikor jih je manj, pa težje, mogoče celo nemogoče.

Izkušnje nas učijo, da skrbniki razumejo pomen popravkov, a se pri njihovi implementaciji vseeno zapleta. Problem nastane zaradi velikega števila strežnikov. Nič nenavadnega ni, da ima srednje veliko podjetje 100 ali več strežnikov. Število na novo odkritih ranljivosti na različnih operacijskih sistemih pa je vedno večje. Če torej upoštevamo število strežnikov, različne operacijske sisteme in nenazadnje še vso programsko opremo, ki teče na strežnikih, lahko hitro ugotovimo, **da pravočasna, popolna in kvalitetna implementacija popravkov še zdaleč ni enostavna naloga.**

Enostavna res ni, je pa nujno potrebna. Napadalci bodo prej ali slej prišli v stik z našimi strežniki. Neposredno, ali posredno preko virusa oz. podobne zlonamerne kode, niti ni pomembno. In ko se to zgodi, je prav od nameščenih popravkov odvisno, ali bo napad uspešen ali ne.

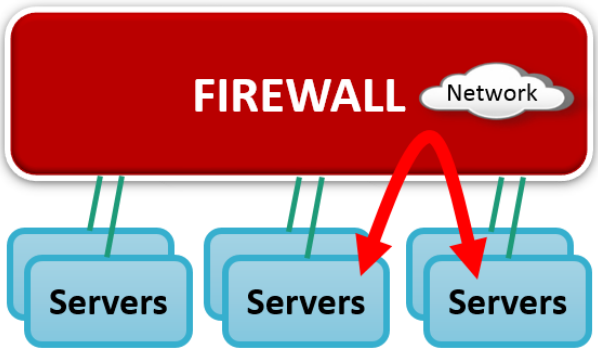
Varnostni pregledi izvedeni v letu 2018 kažejo, da je povprečna varnost notranjih

strežnikov na relativno nizki ravni. Praktično ni okolja, kjer ne bi našli vsaj enega strežnika brez nameščenih popravkov. Je pa tudi veliko primerov, ko popravki niso 100 % popolni in pravočasni. V večini primerov implementacija popravkov nima ustreznega mesta v procesih dela IT oddelkov. Bodisi tej nalogi ni dodeljenega dovolj časa in virov, ali pa je podrejena ostalim nalogam, oziroma se navezuje na ustrezno časovno okno, ko se popravki lahko nameščajo.

Takšna situacija je lahko zelo nevarna. Ponovno si za ponazoritev poglejmo znan primer WannaCry napada. Vsi vemo, kakšno škodo je napad povzročil po svetu. Tudi v Sloveniji. Pomembno je razumeti, da se je napad zgodil v začetku maja 2017, vsi popravki, ki bi napad ustrezno zaustavili, pa so bili javno objavljeni že v marcu 2017. Če bi torej skrbniki pravočasno poskrbeli za popravke na strežnikih, žrtev WannaCry napada ne bi bilo.

9.
poglavje

Nezadostna oz. nična omejitev prometa v notranjost omrežja



Malo se še zadržimo pri notranjem omrežju in notranjih strežnikih. Pri zagotavljanju varnosti strežnikov (in tudi drugih delov omrežja) je zelo pomembna ustrezna porazdelitev omrežja (segmentacija) ter seveda ustrezne omejitve med razdeljenimi deli omrežja.

Zgolj zunanji 'ovoj' med notranjim in zunanjim omrežjem za zagotavljanje varnosti ni dovolj. Ta se lahko na različne načine zaobide.

Za ustrezno varnost celotnega sistema je torej nujno potrebno postaviti varovalke (varnostna območja) in omejitve tudi znotraj omrežja.

Varnostni pregledi so jasno pokazali, da skoraj nobeno podjetje ne izvaja notranjih omejitev prometa. Če pa omejitve obstajajo, so v večini primerov prešibke, nepregledne in neučinkovite.

Postavitev ustreznih notranjih kontrol je lahko zelo zahtevna:

- Količina notranjega prometa je bistveno večja, kar pomeni da morajo biti varnostni sistemi zelo propustni, kar pa ni nujno poceni.
- Za postavitev ustreznih omejitev je ključno, da skrbniki zelo dobro poznajo vse sisteme in arhitekturo aplikacij v omrežju. Pri sistemih sicer lahko trdimo, da jih skrbniki dobro poznajo, pri aplikacijah pa marsikdaj in marsikje ni tako. Poznavanje vseh notranjih aplikacij, kjer bi skrbniki morali poskrbeti za filtre in notranje požarne pregrade, ni zadostno.
- Logika varovanja mora biti drugačna, kot je logika varovanja med Internet omrežjem in lokalnim omrežjem. Če slepo sledimo enaki logiki in postavimo notranje požarne pregrade, hitro pridemo do situacije, ko imamo več sto varnostnih pravil. Skoraj nemogoče je znotraj takšne množice pravil zagotoviti ustrezno varnost ter preglednost.
- Postavitev varovalk med segmentom delovnih postaj in strežniki je še dokaj realna. Ko pa pričnemo postavljati omejitve med samimi strežniki, hitro naletimo na izziv virtualizacije.

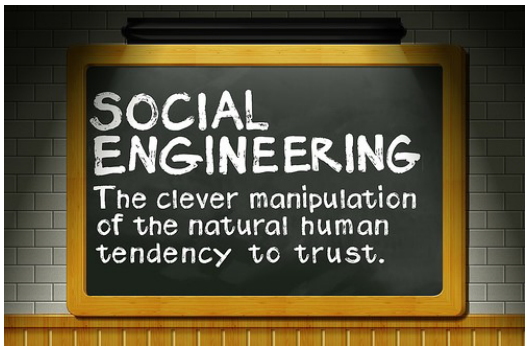
Obstaja torej veliko razlogov, zakaj rešitev tega izziva ni enostavna. A to ne sme biti izgovor, da se tovrstna varnost ne vzpostavi. Brez nje je omrežje bistveno bolj podvrženo tveganjem, kot bi bilo sicer.

Za začetek je smiselno postaviti vsaj določene varnostne zapore, kjer navedene težave niso tako očitne. Na primer zapora med učilnicami in ostalim omrežjem, zapora med IT in OT okoljem, zapora med segmenti kamer, tiskalnikov ipd. (kjer se dostopi preverjajo) s preostalim omrežjem itd.

10.
poglavje

Slaba varnostna osveščenost uporabnikov (in skrbnikov)

Za konec se vrnimo k uporabnikom. Posredno smo jih v poglavju o zlonamerni pošti že izpostavili. Če smo takrat ugotovili, da so slovenska podjetja ranljiva na tovrstne napade, lahko upravičeno zaključimo, da pri tem velik del 'krivde' nosijo varnostno neosveščeni uporabniki.



Ni pa zlonamerna pošta edina točka, kjer se slabše vedenje uporabnikov pozna na varnosti. Poglejmo še ostale.

Uporabniki imamo velik vpliv na varnost informacijskega sistema. Želje in zahteve uporabnikov so pomemben parameter odločanja o načinih varovanja določenih delov informacijskega sistema. Prav tako pa je doslednost varovanja informacij neizbežno prepuščena tudi uporabnikom.

Primer:

Skrbnik želi v sistem vnesti dodatno avtentikacijo ali vzpostaviti kompleksnejšo politiko gesel. Uporabniki imamo velik vpliv na to, ali bo to v praksi tudi izvedeno. Sicer nimajo le uporabniki večinsko utež, a v praksi velja, da bo skrbnik svojo namero lažje izpeljal, če mu bodo uporabniki pri tem pomagali oz. se ne bodo upirali.

Podobno je z varovanjem podatkov. Podjetje ima vzpostavljen napreden sistem za hranjenje dokumentov, s podrobno opredeljenimi pravicami dostopov. Če bodo uporabniki dokumente izvažali in si jih shranjevali na namizje, deljene mape, ključke, ipd., ker jim je tako lažje, bo hitro nastal problem. Tipičen primer so Gmail računi. Včasih je uporabniku lažje, da si pomembne datoteke pošlje na svoj računalnik preko svojega Gmail računa, za kasnejši pregled in obdelavo doma. VPN dostop v podjetju je v njegovih očeh preveč zapleten za uporabo, zato raje izbere enostavnejšo pot, čeprav predstavlja veliko varnostno tveganje.

Vedenje uporabnikov oz. varnostna osveščenost uporabnikov ima zelo velik vpliv na dejansko varnost informacijskega sistema in podatkov v podjetju. Ocena o stopnji varnostne osveščeni uporabnikov je seveda subjektivna. **Na podlagi izvedenih testov pa si upamo trditi, da so uporabniki-zaposleni v slovenskih podjetjih varnostno (pre)slabo izobraženi.**

Ta trditev izhaja iz določenih vzorcev obnašanja, ki smo jih zaznali in jih izpostavljamo spodaj

- **Podjetja v varnostno osveščenost zaposlenih ne vlagajo skoraj nič.**
  Varnostna osveščenost ni samoumevna. Od uporabnikov ne moremo pričakovati, da bodo poznali varnostna tveganja in pravilna ravnanja, brez da bi jim kdo to razložil. Področje je povezano z razumevanjem in celo poznavanjem tehnologij, zato nepoznavanje razumljivo vodi v slabšo varnostno ozaveščenost. Podjetja bi morala v izobraževanje uporabnikov na temo varnosti in varnostne osveščenosti vlagati več. To lahko dosežejo z različnimi izobraževanji, pravilniki in nenazadnje 'požarnimi' vajami, saj se na lastnih izkušnjah največ naučimo.
- **Uporabniki včasih neodgovorno uporabljajo različne načine širjenja oz. hranjena informacij.**
  Tako na primer zelo pogosto najdemo večje število deljenih map s pomembnimi podatki, datotekami, ki se nahajajo na namizju in podobnih mestih. Sem sodi uporaba Gmail in Dropbox aplikacij za prenos informacij, ki so med uporabniki zelo priljubljene, pri tem pa zanemarijo sistem, ki jim ga omogoča podjetje. Posledica pomanjkanja izobraževanja je nezavedanje, da so nekatere stvari nevarne. Neodgovorno ravnanje pa izhaja tudi iz malomarnosti. Enostaven test si lahko naredi vsak sam pri sebi. Ko želimo pomembne podatke podjetja postaviti na neko mesto, se najprej vprašajmo: *»Bi enako storil z osebnimi podatki svojih otrok«*. Odgovor naj velja tudi za ravnaje s poslovnimi podatki podjetja.
- **Uporabniki imajo v podjetju preveč vpliva na varovanje sistemov.**
  Nemalokrat naletimo na situacijo, ko skrbniki povedo, da se groženj zavedajo in da tudi sami želijo vpeljati varovalne mehanizme. Morebiti so ga v preteklosti celo že uvedli. A so se nato uporabniki ali celo vodstvo pritožili in skrbnik je moral opustiti namero po spremembi. Seveda se strinjamo, da varnost ne more (preveč) otežiti uporabo informacijskih sistemov, a samo upoštevanje želja uporabnikov lahko privede do velikega varnostnega tveganja.
- **Podpora vodstva varnosti v podjetju še vedno ni dovolj visoka.**
  Kar ne velja več za vsa okolja, saj z optimizmom ugotavljamo, da je situacija bistveno boljša kot pred leti. Res pa je, da je prostora za napredek še dovolj (če ne preveč). Premalo podpore opažamo predvsem pri procesih in delovnih nalogah. Skrb za varnost ni lahka naloga. Zahteva veliko časa in veliko znanja. Nemalokrat naletimo na situacijo, kjer skrbniki in zaposleni v IT oddelkih v opisu svojih nalog, nimajo definiranih nalog, ki se tičejo varnosti. Tako je skrb za varnost prepuščena lastni iniciativi in prostemu času. Proaktivni skrbniki si zaslužijo pohvalo, a generalno gledano s stališča podjetja ga lahko takšna situacija pripelje v velike varnostne težave in na kocu tudi krajo podatkov oziroma intelektualne lastnine.

Preverite varnost na najbolj izpostavljenih točkah
vašega informacijskega sistema.

Naši strokovnjaki vam bodo pomagali pri oceni varnostnih tveganj
in svetovali, kateri je optimalen način za odpravo ranljivosti.

Vprašajte našega strokovnjaka za kibernetsko
varnost Vladimirja Bana

vladimir.ban@smart-com.si

SMART COM

Smart Com ima 28-letno tradicijo na področju IKT in je eden izmed vodilnih sistemskih integratorjev v Jugovzhodni Evropi. Naši strokovnjaki so specialisti za povezovanje vrhunskih tehnologij v sisteme, ki za stranke predstavljajo poslovne rešitve z visoko dodano vrednostjo. Mrežna infrastruktura, kibernetska varnost in nadzorni sistemi so naše najmočnejše strokovne specializacije. Prizadevamo se za vzpostavljanje partnerstev, ki temeljijo na medsebojnem zaupanju za udejanjanje strateških in poslovnih vizij.

www.smart-com.si