BELA KNJIGA

7 VARNOSTNIH POMANJKLJIVOSTI, KI SO IZSTOPALE V 2019

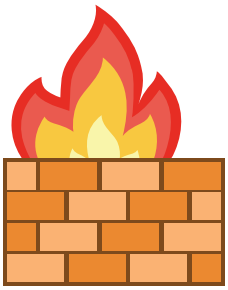
Na katerih področjih bi morala slovenska podjetja okrepiti kibernetsko varnost

Smart Com d. o. o.

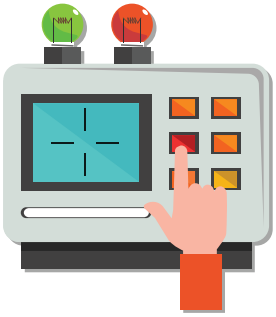
Kazalo vsebine

Izhodišče

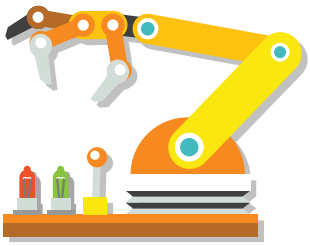
Glede na IT trende pa tudi stanje v vsakodnevni praksi v zadnjih letih, je področje kibernetske varnosti vse bolj v ospredju. V Smart Comu temu sledimo in se odzivamo na potrebe z varnostnimi rešitvami in storitvami za **zagotavljanje celovite zaščite IT in OT sistemov pred naprednimi kibernetskimi grožnjami.**



Z umeščanjem opreme naslednje generacije npr. požarnih pregrad, poskrbimo,da z mehanizmi kot so (IDS-Intrusion Detection Systems ali IPS-Intrusion Prevention Systems) potencialnim napadalcem onemogočimo ali vsaj dodobra otežimo dostop do lokalnih omrežij uporabnikov. Sicer ugotavljamo, da veliko uporabnikov, ki imajo takšne sisteme že implementirane, varnostnih mehanizmov zaradi slabih izkušenj nimajo vključenih. Le ti v številnih primerih preprečijo delovanje osnovnih funkcij, kot so preveliko filtriranje elektronske pošte, onemogočen varen oddaljen dostop in podobno ali pa predstavljajo sistemskim administratorjem kompleksnejše upravljanje.



Vsekakor se je takšnim situacijam mogoče izogniti, vendar je za to potrebno poznavanje delovanja omenjenih mehanizmov in optimalne nastavitve, za kar pa po navadi zmanjka časa, včasih pa tudi volje. V takšnih primerih priskočijo na pomoč naši strokovnjaki, ki na podlagi dolgoletnih izkušenj in poglobljenega znanja poskrbijo za **optimalne nastavitve** in tudi **vzdrževanje takšnih sistemov.**



Poleg vpeljave tehnoloških mehanizmov zaščit ter poznavanja delovanja, upravljanja in vzdrževanja opreme varnost krepimo tudi z **izvajanjem specializiranih storitev**, s katerimi preverimo varnost tako v IT kot OT (industrijskem) okolju, kamor spadajo varnostni pregledi, preverjanje varnostne osveščenosti zaposlenih ter izvajanja izobraževanj in usposabljanj o varnostnih grožnjah.

Ob vseh izvedenih varnostnih pregledih različnih okolij v preteklem letu, smo naleteli na varnostne pomanjkljivosti, težave in izzive, ki so skupna vsem, zato jim velja posvetiti več pozornosti. Na podlagi vseh praktičnih izkušenj smo pripravili seznam **sedmih najpogostejših ranljivosti**, ki so bile v ospredju v letu 2019. Podamo pa tudi načine oz. **ukrepe za zmanjšanje tveganj.**

1 Socialni inženiring – 'phishing'

Kadar v podjetju nameščamo računalniško opremo lahko rečemo, da je vedenje in znanje izvajalcev, tako notranjih, npr. sistemskih administratorjev, ali zunanjih izvajalcev, navadno na zelo visoki ravni. Napadalci niso vedno v bližini potencialne žrtve, da bi pridobili informacije in ker je poizvedbo najlažje delati 'iz naslonjača', se napadalci najprej lotijo **preverjanja ranljivosti opreme, nameščene pri uporabniku**, ki služi kot zaščita pred morebitnimi napadi.

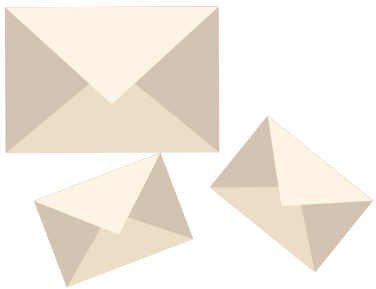
Danes je tovrstna oprema, npr. požarne pregrade, tudi nižjega cenovnega razreda, z nekaj osnovnimi nastavitvami dovolj dobra za preprečevanje hekerskih vdorov v lokalno omrežje. Poizkušanje in iskanje ranljivosti pomeni tudi za napadalca veliko izgubo časa in dodatnega nepotrebnega dela. Zavedajo se, da **so uporabniki računalniških naprav najšibkejši člen**. Če jim uspe zavesti uporabnika, se lahko dokaj hitro zgodi, da pridobijo dostop do njegovega računa, preko katerega nadalje dostopajo »kot uporabnik« do aplikacij, npr. elektronske pošte ali še huje preko »varnih« VPN-povezav.

Eden izmed najpogostejših načinov, s katerim nas napadalci zavedejo in jim nevede predamo podatke za dostop, je uporaba tako imenovane 'phishing' metode. Za izvedbo 'phishinga' se napadalci odločajo, ker ta oblika socialnega inženiringa **skoraj 100 % zagotavlja prevzem nadzora nad uporabnikom**. Glede na naše izkušnje pa to trditev lahko le potrdimo, saj smo v sklopu izvedenih varnostnih testiranj ugotovili, da jih v povprečju **med 15 % in 20 % nasede na to obliko zavajanja**.

Zakaj uporabniki nasedemo?

Napadalci se seveda v elektronskih sporočilih, ki jih pošljejo uporabnikom, predstavljajo z lažno identiteto, kot njihovi prijatelji, predpostavljeni, nadrejeni ali pa sodelavci iz IT-oddelka. Tudi sami v fazi testiranja uporabljamo podobne metode in ker je v naši naravi, da smo pripravljeni pomagati (velikokrat tudi preveč), se kaj hitro zgodi, da na zahtevo ali prošnjo vnesemo podatke (uporabniško ime in geslo) s klikom na določeno povezavo, ki je sestavni del lažnega elektronskega sporočila. Na tak način napadalci pridobijo podatke, ki jih uporabijo pri dostopu do elektronske pošte uporabnika preko spletnega portala. Če je prevara dobro pripravljena, se velikokrat zgodi, da uporabniki niti ne posumijo, da so bili tarča napada, napadalec pa lahko dlje časa črpa podatke iz korespondence elektronske pošte.

'Phishing' metoda se ne uporablja le za pridobivanje podatkov za dostop do portalov kot je elektronska pošta, ampak je bila metoda v osnovi mišljena za nepooblaščeno pridobivanje podatkov s področja bančništva, npr. kreditnih kartic. Seveda se tak način uporablja še danes, vendar smo uporabniki kljub vsemu že toliko ozaveščeni, da teh informacij nismo pripravljeni več slepo deliti.



Nikakor pa ne smemo pozabiti na **'spear phishing' metodo**, ki je zelo podobna 'phishingu', vendar se v tem primeru napadalec odloči, da bo **ciljal točno določene osebe** in se zato lažno predstavlja, da je povezan z njimi. Zelo pogost primer je, ko direktor podjetja (v našem primeru napadalec) prosi računovodjo, da nujno nakaže določen znesek na njegov 'zasebni' račun, ker je na službeni poti in potrebuje denar. Takšna tehnika seveda zahteva veliko raziskav s strani napadalca, prav tako pa mora spremljati obnašanje točno določenih oseb. To danes seveda ni prav težka naloga, saj preko družbenih omrežij delimo prenekatero informacijo iz zasebnega kot tudi poslovnega življenja.

Kako se ubraniti?

Najprej seveda pomislimo na tehnično rešitev, vendar so v današnjem času takšne rešitve ali zelo drage ali pa še ne dovolj zanesljive, da bi se lahko na njih 100 % zanesli. Z dobro pripravljenim 'phishing' napadom, nakupom lažne sorodne domene, ki jo izkoristimo za napad, se lahko popolnoma regularno predstavljamo in zaobidemo mehanizme, ki nam preprečujejo dostavo elektronske pošte.

Ker je zaradi pogostosti napadov in uporabe takšnega načina veliko napadalcev še vedno uspešnih, si razvijalci zaščite prizadevajo najti čim boljše rešitve, ki so pri svojem delu vedno bolj uspešne. Predvsem nam je v zadnjem času pri tem v vse večjo pomoč uporaba mehanizmov strojnega učenja in umetne inteligence.

Kar se je pa v praksi pokazalo kot najbolj učinkovito, pa je ozaveščanje uporabnikov v obliki izobraževanj. Naše stranke, ki so v okviru varnostnega pregleda izvedle 'phishing' test, so dokaz, da se že po drugem izobraževanju oz. izvedbi ozaveščanja zaposlenih **zmanjša število tistih uporabnikov, ki so na prvem testiranju 'podlegli', iz 35 % na 3 %**. Z gotovostjo lahko trdimo, da je ozaveščanje zaposlenih in uporabnikov v obliki izobraževanja oz. predavanja najboljša oblika širjenja informacij oz. ozaveščanja za obrambo pred 'phishing' napadi.

2 Socialni inženiring – 'USB dropping' oz. podtikanje USB ključev

Ali ste že kdaj našli USB ključ in vam radovednost ni dala miru, da ne bi pogledali, kakšna je njegova vsebina? Podtikanje USB ključev je zelo priljubljena hekerska metoda, ki prav tako zagotavlja skoraj 100 % uspešnost. Iz naših izkušenj lahko povemo, da so le redka podjetja, ki imajo na svojih **delovnih postajah onemogočen priključek USB**. Tak primer dobre prakse smo večinoma našli v bančnem sektorju. Na ta način se težavam s podtikanjem USB ključev že na prvem koraku izognemo. Žal pa takšno prakso srečamo le redko kje.

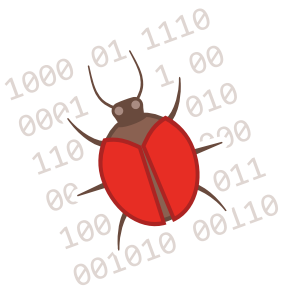
Če v okviru varnostnega pregleda izvajamo takšno metodo, jo izvedemo v sodelovanju z naročnikom. Čeprav imajo uporabniki na svojo delovno postajo možnost priključiti zunanjo enoto (v tem primeru USB ključ), je v večini primerov protivirusna zaščita učinkovita in ne dovoli zagona izvršljivih datotek ali raznih makrojev v dokumentih, ki jih za namene testiranja podtaknemo na USB ključ. Naročnik v takšnem primeru doda datoteko, ki jo podtaknemo na listo dovoljenih aplikacij, saj želimo opraviti testiranje zaposlenih in ugotoviti, kakšna je njihova **stopnja ozaveščenosti o informacijski varnosti.**

Vsekakor pa ne smemo upati, da nas bo protivirusna zaščita vedno ubranila pred izvršljivimi datotekami, ki se bodo znašle na USB ključu. Napadalci so po navadi vsaj en korak pred tovrstnimi zaščitami in lahko kaj hitro **podtaknejo skripto, ki jo protivirusni programi še ne zaznajo.**

Kdaj so uporabniki 'brezpogojno' pripravljeni preveriti vsebino USB ključa?

Pri testiranjih smo ugotovili, da se obnese več metod, vsekakor pa so med njimi najbolj uspešne tiste, ki burijo človeško domišljijo ali pa se vsebini nikakor ni mogoče upreti. Če se na USB ključu nahaja nalepka, na kateri piše 'Plačilne liste' – 'Ime podjetja' ali 'Privat - posnetki', se v skoraj vseh primerih izkaže, da je človeška radovednost prevelika, da najdenega USB ključa najditelji ne bi pregledali. Napadalci na USB ključ ponavadi skrijejo razne **'makroje' ali izvršljive datoteke, skripte, ki jim omogočijo dostop do žrtvinega računalnika.** Če želi uporabnik na najdenem USB ključu odpreti Excellovo datoteko, ki jo je napadalec pripravil, mora uporabnik najprej omogočiti urejanje vsebine, za ogled vsebine pa je potrebno omogočiti 'makroje'. Ko uporabnik vse to izvede, je žal že prepozno in če protivirusna zaščita ni preprečila odpiranja datoteke, je napadalec skoraj zagotovo prevzel nadzor nad delovno postajo oz. računalnikom žrtve.

Nadaljevanje je seveda odvisno od napadalca, ki pa lahko pritajeno nadzira, prenaša in spremlja vsebino elektronske pošte, datotek, nenazadnje pa se lahko v določenem trenutku odloči, da **preko oddaljenega dostopa aktivira virus, ki uporabniku zašifrira vse datoteke.** To je najbolj črn scenarij, ki se lahko zgodi kot posledica človeške radovednosti.



V okviru varnostnih testiranj naš cilj zagotovo ni prevzem nadzora nad uporabniško delovno postajo, ampak priti do statističnih podatkov, koliko USB ključev je bilo uporabljenih. Žal so rezultati v praksi precej zaskrbljujoči, saj **že v prvi uri testiranja večina USB ključev pristane v delovnih postajah zaposlenih**, prav tako pa so za dostop do vsebine pripravljeni onemogočiti in zaobiti vse varnostne mehanizme.

Kako se ubraniti?

Kakor je bilo že omenjeno je najbolj priporočljiva uvedba varnostne politike, ki **onemogoča uporabo USB priključkov na delovnih postajah**. Čeprav precej enostaven in hiter postopek, s katerim lahko to dosežemo tudi na večjem številu delovnih postaj, preko tako imenovanega group policy-a, pa smo ga v praksi zaznali le v organizacijah z zelo podrobno razdelano varnostno politiko.

Istočasno pa bi kot zelo pomemben ukrep izpostavil **ozaveščenost uporabnikov**. Dokler uporabniki ne slišijo, kaj vse jih lahko doleti, se ne zavedajo pomena pravilnega ravnanja z najdenim USB ključem. V podjetjih, kjer smo izvajali tovrstne teste in nato tudi izobraževanje, se je stopnja zavedanja o nevarnostih zelo povečala.

3 Nizka varnostna ozaveščenost uporabnikov

Čeprav smo v letu 2020 in računalniško tehnologijo aktivno uporabljamo že več kot dve desetletji, smo ob izvajanju varnostnih pregledov, ki vsebujejo socialni inženiring, zelo presenečeni, saj pričakujemo višji nivo ozaveščenosti uporabnikov, kot pa se to izkaže v praksi. Je pa za trenutno situacijo verjetno 'krivo' stanje in število hekerskih napadov, ki so javno objavljeni in znani na področju Slovenije.

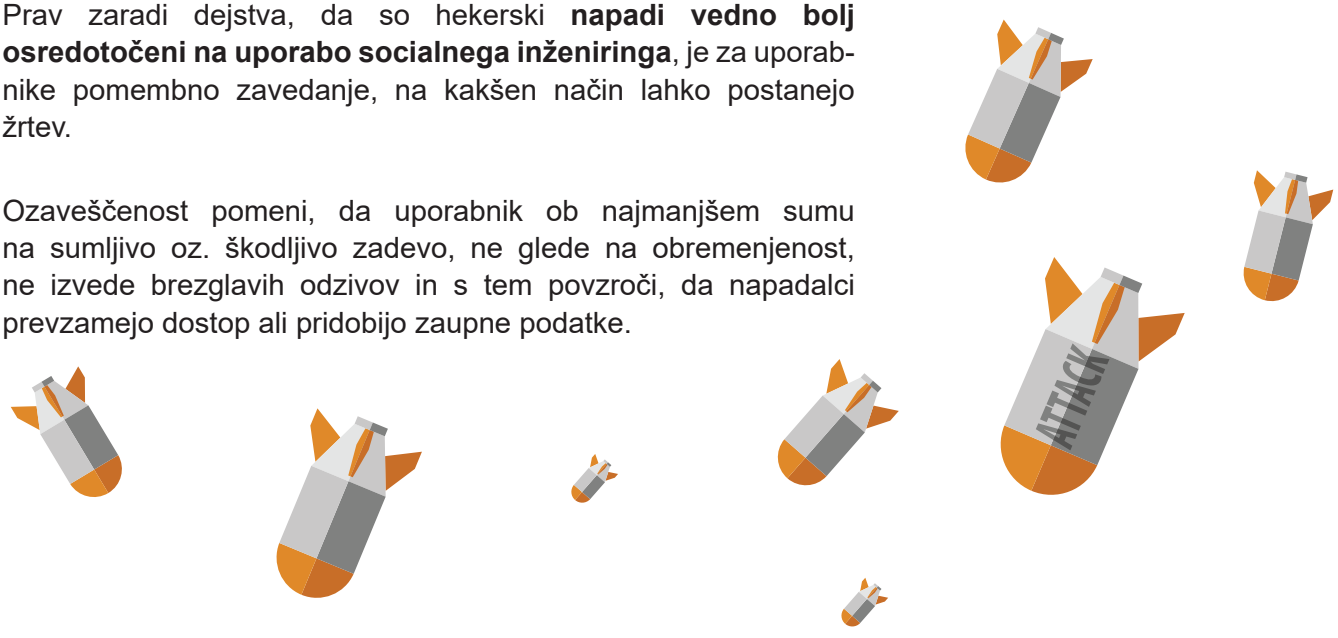
Iz odziva udeležencev izobraževanj imam občutek, da so še vedno mnenja, da so hekerski napadi nekaj, kar se njim ne more zgoditi, oz. se to pri nas ne dogaja. Pozornost pri uporabnikih pritegnejo medijsko odmevni dogodki, na primer v letu 2019 hekerski napad na lekarno. Šele takrat so mogoče pomislili, da kljub vsemu ne gre za znanstveno fantastiko, ampak dejstvo, ki lahko vpliva na naš vsakdan.

In kaj imajo dejanski napadi z ozaveščenostjo uporabnikov računalniških sistemov?

V naši naravi je, da o zaščiti začnemo razmišljati šele takrat, ko smo že neposredno ogroženi. Takrat smo pripravljeni vložiti tudi čas in denar. Velikokrat so uporabniki na izobraževanjih, ki jih izvajamo, precej presenečeni, ko ugotovijo, da se v resnici ne bomo pogovarjali o tehničnih vidikih, ampak **o kibernetski varnosti z vidika zavedanja, kako in kdaj nas lahko nepridipravi napadejo**.

Prav zaradi dejstva, da so hekerski **napadi vedno bolj osredotočeni na uporabo socialnega inženiringa**, je za uporabnike pomembno zavedanje, na kakšen način lahko postanejo žrtev.

Ozaveščenost pomeni, da uporabnik ob najmanjšem sumu na sumljivo oz. škodljivo zadevo, ne glede na obremenjenost, ne izvede brezglavih odzivov in s tem povzroči, da napadalci prevzamejo dostop ali pridobijo zaupne podatke.



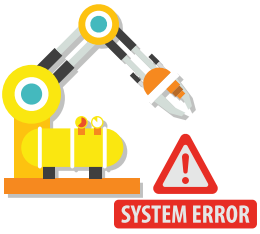
Kako se ubraniti?

Res je, da 100 % obrambe pred hekerskimi napadi ni. Lahko pa potencialne težave precej omilimo, če smo se pred tem o njih podučili. V zadnjem času se pojavlja tudi vedno več oblik e-izobraževanja, kjer naj bi se uporabniki preko spletnih portalov izobrazili in pridobili osnovno ozaveščenost, vendar v večini primerov temu žal ni tako.

V pogovoru z uporabniki smo izvedeli, da je taka oblika sicer zaželena, ker lahko prilagajajo čas izvedbe, vendar pa velikokrat izobraževanje izvedejo parcialno ali zelo površinsko, da ugodijo zahtevam, ki jih naloži delodajalec. Ozaveščanje na temo kibernetske varnosti so sicer imeli, ne vemo pa, kako učinkovito je bilo.

Ugotovili smo, da so **med najbolj ranljivimi predvsem novo zaposleni**, ki v nekaterih primerih sicer od delodajalca dobijo gradivo na temo kibernetske varnosti, vendar brez ustreznega nadzora oz. povratne informacije. Sicer vsi podpišemo, da smo seznanjeni z vsebino, vendar v primeru uspešnega napada, ki je izkoristil človeški faktor, to bolj malo pomaga. Vsekakor svetujemo, da se **izobraževanja oz. ozaveščanje zaposlenih** izvaja vsaj enkrat letno, obvezna pa bi morala biti takšna izobraževanja za novo zaposlene.

4 Dostop do okolij OT (operativne tehnologije) oz. industrijskih okolij

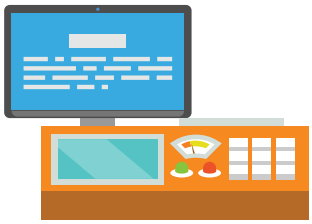


Razvoj informacijske tehnologije (IT) se danes odvija tako hitro, da mu je skoraj nemogoče slediti. Kaj pa razvoj v okoljih OT (operativne tehnologije)? Najprej si na kratko poglejmo, kaj sploh spada pod operativno tehnologijo in kako dolgo se z njo že srečujemo.

Le malokdo se zaveda, da je operativna tehnologija tista, ki skrbi, da svet okoli nas teče, tako kot smo vajeni. Poglejmo si primer. Če živite v večstanovanjskem objektu, veste, da se v zimskem času stopnja ogrevanja čez dan zmanjša, v večernih urah poveča, ponoči od 23. ure dalje pa zopet zmanjša. V mestih z več takšnimi objekti je regulacija toplote krmiljena iz toplarn ali drugih nadzornih centrov z uporabo tako imenovane operativne tehnologije. Do pred nedavnim so takšna okolja bila strogo ločena, celo namensko izolirana od IT-okolja (informacijske tehnologije).

To je le eden izmed primerov, seveda pa krmiljenje, vodenje in spremljanje najdemo tudi drugje, celo na veliko bolj pomembnih področjih. Elektro distributerji, industrijska okolja, komunalna podjetja, promet in še bi lahko naštevali, se poslužujejo enakih načinov **oddaljenega krmiljenja**. Krmiljenje se (na primer odpiranje, zapiranje ventilov, vklop ali izklop energetskih vodov, odčitavanj vrednosti...) izvaja preko t. i. enot PLC (programabilni logični kontroler), RTU (Remote Terminal Unit) idr. SCADA (Supervisory Control And Data Acquisition) pa je skupno ime za sisteme, ki so namenjeni nadzoru in krmiljenju različnih tehnoloških procesov.

Sistemi v okolju operativne tehnologije delujejo že zelo dolgo in prve omembe sistema SCADA najdemo v zgodnjih 70-ih letih. V našem okolju še vedno najdemo naprave iz 90-ih let. Pri razvoju različnih naprav RTU ali PLC takrat še ni bilo potrebe razmišljati o mehanizmih zaščite, saj so bile ločene od ostalih sistemov, o napadalcih pa tudi še ni bilo govora.



Kje se pojavijo težave?

Za industrijska okolja in omenjene naprave je zelo značilno, da uporabljajo protokole, ki se popolnoma razlikujejo od protokolov v IT-okolju. Med njimi so najbolj znani **Modbus, DNP3, HART** itd., ker so proizvajalci v večini ustvarjali svoje protokole, vendar imajo bolj kot ne vsi **pomanjkljivosti na področju varnosti**. Pri varnostnih pregledih, ki smo jih izvajali v teh okoljih, smo ugotovili, da je naprave, ki uporabljajo omenjene protokole, zelo preprosto nadzorovati ali celo krmiliti oz. spreminjati njihova stanja z javno dostopnimi hekerskimi orodji. Zaradi pomanjkanja varnostnih mehanizmov in ker v tem okolju veljajo drugačne zakonitosti kot v poslovnem okolju je že pri samem varnostnem pregledu potrebno biti zelo previden in se držati določenih pravil – pregledi se izvajajo le v času vzdrževanja ali izven delovnega časa, če je to le mogoče.

Če bi IT in OT-okolji ostali ločeni, verjetno sploh ne bi bilo težav; poskrbeti bi morali le, da ne pride do nezaželenega fizičnega dostopa. Kot smo že omenili, so bili sistemi SCADA v veliko primerih nameščeni pred 15 ali več leti in nemalokrat naletimo na primere, da **delujejo na operacijskih sistemih, za katere varnostni popravki niso več na voljo** (npr. Windows XP ali celo starejši). Mlajše generacije se takšnih operacijskih sistemov verjetno niti ne spomnijo, s stališča varnosti pa je najbolj zaskrbljujoče to, da takšnih sistemov 15 ali več let nihče ni posodabljal. Danes se nam to seveda zdi malce nenavadno, ampak, zakaj bi nekaj posodabljali, če deluje v skladu s pričakovanji v popolnoma od zunanjega sveta izoliranem okolju. Torej držimo se reka “ne popravljaj, dokler deluje”, saj bi si s tem lahko nakopali le težave.

Ob vpeljavi novih tehnologij oz. digitalizaciji želimo nadzor nad napravami od kjer koli, zato se zgodi, da se IT in OT-okolji združujeta, na vidik varnosti pa ob tem pozabimo. Iz vsakodnevne prakse ugotavljamo, da sta IT in OT-okolje dva različna svetova, ki ju vzdržujeta različni ekipi. IT svet je v domeni vzdrževalcev, osebja, specializiranega za informacijsko tehnologijo, vzdrževalci operativne tehnologije pa so elektro vzdrževalci, ki so v večini primerov sisteme tudi postavljali. Mnenja in praksa teh dveh svetov je nemalokrat različna in če ni pravega sodelovanja lahko hitro pride do povezanih sistemov s premalo zaščite.

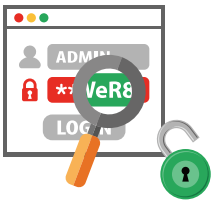
Če je združevanje IT in OT-okolja nepravilno, je to odlična priložnost za nepridiprave. V kolikor jim uspe priti v OT-okolje, lahko zaradi neposodobljenih sistemov prevzamejo popoln nadzor nad OT-okoljem ali celo naprej nad IT-okoljem. Lahko pa se zgodi tudi obratno. Noben od naštetih primerov ni v prid industrijski organizaciji 4.0.

Kako se ubraniti?

Žal tudi na tem področju ne moremo reči, da lahko zagotovimo 100 % zaščito, saj se neželena dejanja lahko zgodijo z uporabo različnih scenarijev. Vsekakor bi veliko pripomoglo, če se IT in OT okolji čim bolj ločita, ampak smo že ugotovili, da trendi narekujejo drugačen tempo in je **združevanje neizbežno.**

Pravilna segmentacija omrežij je eden izmed prvih korakov na tem področju. Je pa seveda potrebno razmišljati o dodatnih zaščitah. **Dodatna požarna pregrada** med IT in OT-okoljem, pravilna umestitev strežnikov, na katerih so nameščeni sistemi za nadzor in upravljanje, ter celo uporaba **namenskih požarnih zidov za OT-okolja** je skoraj obvezna. Določen varnostni nivo pa lahko dosežemo že z uvedbo osnovnih postopkov za zaščito in varovanje, kamor spadajo uporaba **močnih zaščitnih gesel, omejitev dostopov** iz posameznih naprav (uporaba access list) ter **kontrola in nadzor fizičnega dostopa** vzdrževalcev do OT-okolja.

5 Dostop do spletnih strani in do njihovega administratorskega vmesnika



Varnostni pregledi omrežij, aplikacij oz. spletnih strani nam velikokrat že v prvi fazi testiranja razkrijejo vstopna okna za administracijo. Prvo vprašanje, ki se pojavi je, ali je res potrebno, da imamo do administrativnega dela spletne strani/spletne trgovine dostop iz katerega koli dela sveta.

Poglejmo si primer, ki v praksi ni tako redek.

Slovensko podjetje ima spletno stran narejeno v CMS okolju Wordpress, za spletno trgovino pa uporablja Wordpressov vtičnik Woocommerce. Stran je namenjena izključno slovenskemu tržišču in je tudi vsebinsko izključno v slovenskem jeziku. Navadno so takšne spletne strani oz. trgovine dokaj redno posodobljene in ker za posodobitve oz. varnost skrbi skupnost, smo lahko skoraj brez skrbi, da ne bomo naleteli na ranljivosti, kot so XSS - Cross Site Scripting, SQL Injection ali podobne. Ker se v primeru takšnih pregledov prav tako postavimo v vlogo potencialnega napadalca, seveda najprej preverimo verzije Wordpressa in vtičnikov. Prvi del hekerskega napada kakor tudi varnostnega pregleda obsega poizvedovanje, med katerega spada tudi pridobivanje podatkov o uporabniških imenih.

Glede na zasnovo določenih sistemov kot je omenjeni Wordpress je uporabniška imena skoraj nemogoče prikriti. In ko ima napadalec uporabniška imena, je metod, po katerih lahko pridobi gesla, kar nekaj. Ena izmed priljubljenih je brute force, kjer lahko z ugibanjem najde pravo kombinacijo. Sicer precej zamuden postopek, vendar velikokrat uspešen, predvsem zaradi tega, ker uporabniki uporabljamo predvidljiva gesla.

Če izvzamemo klasične spletne strani oz. spletno trgovino si poglejmo še vstopne portale, ki jih velikokrat najdemo v okviru varnostnih pregledov in so zelo aktualni pri koriščenju in izvajanju kibernetskih napadov. Eden izmed takšnih je seveda **vstopni portal do elektronske pošte**, bodisi povezan z Microsoft Outlookom ali katerim koli drugim sistemom elektronske pošte.

Tudi tukaj se postavlja vprašanje, če je res nujno potrebno, da imamo od povsod dostop do elektronske pošte, ki lahko vsebuje zelo občutljive podatke. Pri nas smo dostop do portala omejili in omogočili le iz lokalnega omrežja ali preko VPN-povezave. Torej je za dostop najprej **potrebno vzpostaviti varno tunelsko povezavo**, šele nato odjemalec elektronske pošte prične z izmenjavo podatkov s poštnim strežnikom.

Kakšna je varnost, če koristite elektronsko pošto in ostale podatke kot oblačno storitev?

Velikanom, kot sta Microsoft in Google, gre glede varnosti seveda zaupati, vendar previdnost ni nikoli odveč. Če želite omejiti dostop do portalov, lahko z nastavitvami dosežete, da je najprej potrebno narediti povezavo v vaše podjetje, dostop do elektronske pošte recimo na Microsoft pa je omejen iz javnega IP-naslova vašega podjetja.

Kako se ubraniti?

Splošno velja, da je za katero koli spletno stran, narejeno v CMS (Wordpress, Joomla, Drupall...) ali drugem načinu, z malo truda mogoče zelo omejiti dostop. Sam sem še vedno mnenja, da do spletne trgovine, ki cilja na določeno regijo kupcev, ni potrebno izpostavljati ostalim uporabnikom, ki ne razume jezika.

Na spletu obstajajo pripomočki, ki nam pomagajo pripraviti konfiguracijo datoteke *.htaccess*, le ta pa poskrbi, da se na spletni strani znajdejo le tisti, ki so zaželeni.

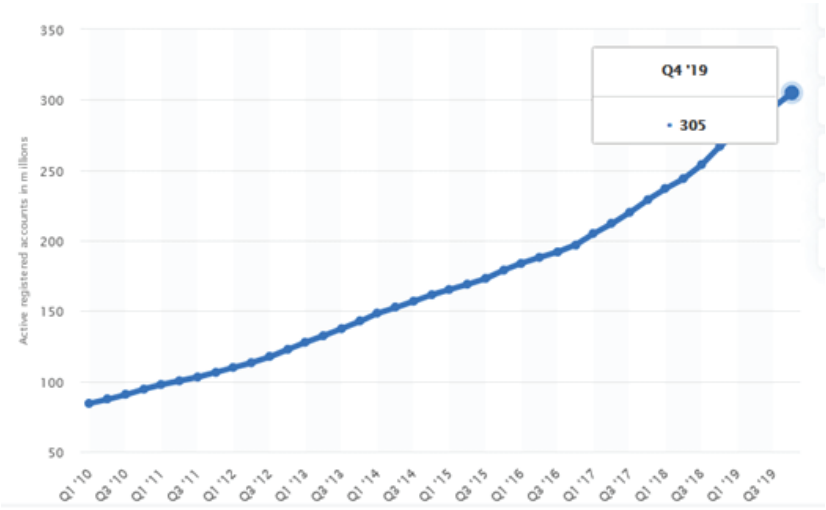
Če pa govorimo o dostopu do administrativnega vmesnika, pa je vsekakor priporočljivo, če ne že kar obvezno, da se **dostop omeji na točno določene IP naslove, iz vseh ostalih pa blokira.** Administratorjev navadno ni toliko, da bi bilo takšne omejitve težko obvladovati, zagotovimo pa si veliko večjo varnost.

Še nekaj priporočil za uporabo Wordpress-a:

- izključite WordPress REST AP, če te funkcionalnosti ne uporabljate,
- izključite WordPress XML-RPC, če ni v uporabi,
- nastavite konfiguracijo spletnega strežnika, ki bo blokiral */?author=<number>*,
- ne izpostavljajte dostopa do */wp-admin* ali */wp-login.php* neposredno iz Interneta.

6 Dostop do aplikacij brez uporabe 2FA

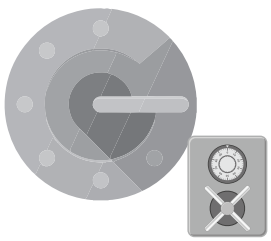
Kaj pa ostale aplikacije, ki jih srečamo na internetu ali v lokalnih omrežjih. Najlažje je, če ponazorimo s praktičnim primerom; s tem mogoče dobite še kakšno zamisel, kako zaščititi svoje zasebne aplikacije. PayPal je vsem dobro znana storitev, saj le malokdo, ki opravlja nakupe preko spleta, ne pozna tega načina plačevanja. V zadnjem kvartalu leta 2019 je imel PayPal 305 milijonov aktivnih uporabnikov. Ali ste kdaj pomislili, da nekomu uspe pridobiti uporabniško ime in geslo, ki ga uporabljate za dostop in plačevanje preko aplikacije PayPal? Že sama misel na to je neprijetna. PayPal vam predvsem zaradi takšnih možnosti omogoča **dodatno zaščito, s katero je potrebno izvesti dvo-nivojsko avtentikacijo.**



V Q4 leta 2019 305 MIO aktivnih uporabnikov PayPal (statista.com)

Takšno vrsto avtentikacije imenujemo 2FA (Two Factor Autentication) oz. dvofaktorska avtentikacija. Če pri PayPal-u zaščito vključite, boste morali ob vsaki prijavi v portal in pri vsakem plačilu poleg vašega uporabniškega imena in gesla vpisati še 6-mestno številko, ki se vsako minuto spremeni.

Podoben sistem smo v preteklosti poznali v e-bančništvu, z uporabo RSA žetona, ki je imel popolnoma enako funkcionalnost. Danes za uporabo 2FA oz. generiranje enkratnega gesla ne potrebujemo dodatnega RSA žetona, ampak imamo na voljo na primer **brezplačno aplikacijo Google Authenticator** in že s tem dvignemo raven naše zaščite.



Kaj pa uporaba 2FA v drugih aplikacijah. Seveda je v večini primerov možna. Na primer Microsoft Office kot oblačna storitev, vam za dostop do vaših podatkov omogoča uporabo 2FA. Prav tako smo zaznali porast uporabe mehanizma 2FA tudi pri drugih dostopih oz. aplikacijah. Ker sem že omenil, je pogosto omogočen odprt dostop do administracije spletnih strani; potencialnim napadalcem lahko prav z dodatno zaščito 2FA zelo otežimo, da najde pravo kombinacijo za dostop.

In kakšno je stanje pri nas v praksi?

Po pogovoru z naročniki ali udeleženci izobraževanj 2FA uporablja le peščica ljudi v zasebnem življenju, prav tako so redka podjetja, ki imajo implementiran tak način avtentikacije za dostop do pomembnih vsebin podjetja (elektronska pošta...).

Kako se ubraniti?

Z uporabo 2FA lahko v glavnem preprečimo, da bi lahko napadalci z uporabo naših uporabniških imen in gesel dostopali do občutljivih informacij ali plačevali z naših računov. Žal pa je tudi tukaj potrebno povedati, da tak način zaščite ni 100 %. Če nas hekerji s pomočjo “phishinga” zavedejo in naše vnose spremljajo v živo na lažnem portalu, jim lahko z malo sreče uspe izvedeti kodo za 2FA. In če jim uspe le enkrat, je lahko že dovolj.

7 Nadzorovanje dogajanja v IT in OT-okoljih

»Ali ste zaznali, da se je v zadnjem mesecu karkoli dogajalo na vašem omrežju,« je vprašanje, ki ga velikokrat zastavimo strankam, pri katerih smo opravili varnostni pregled. Statistično jih slaba polovica pokaže podatke, kdaj smo bili opaženi in kaj smo izvajali še manj pa je tistih, ki nas predvsem pri zunanjih pregledih tudi blokirajo.

Varnostne preglede največkrat izvajamo v 'tajnosti', ko zaposleni v IT-oddelkih niso obveščeni o tem, kaj bomo počeli, saj vodstvo želi ugotoviti, kakšno je dejansko stanje.

Druga polovica, ki naših poizvedb na svojih omrežjih ne zazna, v večini primerov ne uporablja nadzornega sistema. Zavedamo se, da je investicija v kvalitetni nadzorni sistem precejšnja in jo IT-osebje težko upraviči, saj ne prinaša dobička. Po drugi strani lahko to primerjamo s požarnim zavarovanjem poslovnih objektov.

Ugotovimo lahko, da so podjetja podhranjena, ko gre za nadzorovanje dogajanja v omrežjih, bodisi na javnih IP-naslovih ali lokalnih in redko uporabljajo sisteme za nadzor npr. SIEM - Security Information and Event Management.

Kot sem že omenil je prvi razlog cena, potrebujemo pa še ekipo strokovnjakov, ki morajo te sisteme spremljati, da se ob pojavu anomalij poglobijo v pregled dogajanja in po potrebi pravočasno ukrepajo. Vedeti morajo, kaj je pomembno in kako pravilno odreagirati. V zaključku pridemo do ugotovitve, da za aktivno izvajanje nadzorovanja potrebujemo ekipo ustrezno izobraževanih specialistov iz določenih področij, ki bi morala dogajanje spremljati 24/7. To pa je že zametek varnostno operativnega centra t. i. SOC - Security Operations Center.

Glede na zapisano ugotovimo, da si ne glede na želje takšen način spremljanja dogajanja lahko privoščijo le redka podjetja, kar se nam je potrdilo tudi v praksi preko izvedenih testiranj.

Kaj lahko storite?

S finančnega vidika je lahko postavitev SOC-a ter zaposlitev in izobraževanja ustreznega kadra velik zalogaj, v praksi pa se pokaže, da se naložba v večini primerov hitro povrne. Najrazličnejši vdori v omrežje, katerih spremljanje in odkrivanje je sicer v domeni SOC-a, lahko neposredno vplivajo na razpoložljivost in delovanje omrežja, kar pa je v sodobnem poslovanju za potrebe neprekinjenega poslovanja zelo pomembno.

Kaj pa, če ste s sredstvi in kadri resnično omejeni?

Manjši IT-oddelki z dvema ali tremi administratorji, ki skrbijo za delovanje in vzdrževanje IT sistema, si lahko pomagajo z odprtokodnimi rešitvami. Seveda imajo v primerjavi z licenčnimi sistemi svoje omejitve. Na ta način je z osnovnimi postavitvami možno zagotoviti shranjevanje dnevniških zapisov in prometnih tokov, ki nam lahko ob spremljanju in preverjanju vsaj enkrat na dan nakažejo, da se pripravlja ali dogaja nekaj sumljivega.

Na voljo je še ena alternativa, in sicer **najem storitev Nadzorno operativnega centra (NOC)** pri zunanjem ponudniku, s čimer pridobite vse prednosti, ki ji ta zagotavlja, ob ceni, prilagojeni vašim potrebam oz. obstoječi omrežni infrastrukturi.

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 stokovnjaka za kibernetsko varnost in etičnega hekerja Borisa Krajnca.

boris.krajnc@smart-com.si

Smart Com ima 30-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