RDP – Povećanje sigurnosti

Predgovor

U vrijeme Coronavirusa i pandemije COVID-19 naglo je poraslo korištenje udaljenog pristupa računalima putem RDP-a (Remote Desktop Protocol) i programa “mstsc”, ali i drugih načina udaljenog spajanja (VNC, TeamViewer, …). Budući da je napad na RDP jedan od najčešćih napada u zadnje vrijeme, na žalost prečesto i uspješnih, ovdje ćemo nabrojati neke mjere opreza koje trebate poduzeti da biste povećali sigurnost tog načina komunikacije.

Pretpostavljeni konzumenti ovih uputa su poduzeća s manjom i srednje velikom mrežom računala kojima konačan cilj nije postizanje potpune sigurnosti nego postizanje razine sigurnosti koja je veća od susjedove, što će biti dovoljno da obesrabri besciljne napadače koji besciljno vrludaju internetom u potrazi za “slabim ulaznim vratima” i prilikom da se okušaju kao provalnici. Nastojali smo da upute budu jednostavne i razumljive osobama koje brinu o takvim mrežama, a kojima to možda i nije primarni posao nego tek usputna obveza ili hobi.

U grubim crtama, “besciljni napad” teče ovako – napadači “skeniraju” računala vidljiva svima s Interneta (a budući da se želite spojiti od kuće na njega, vaše računalo u uredu jest dostupno svima na Internetu) i traže je li dostupan RDP; ako jest prvo se pokušaju prijaviti općepoznatim korisničkim nazivima (“administrator”, “tech”, “podrska”, “support”, …) pogađajući lozinke (prvo pokušavaju s popisom od 10.000 najčešćih, a nakon toga ponekad idu redom od “a”, pa dok ih se ne prekine). Takvi napadi mogu ostati neprimijećeni mjesecima i nerijetko uspijevaju kod slabih i/ili kratkih lozinki. Što je slaba / kratka lozinka? “Admin / admin” je primjer najgore moguće kombinacije korisničkog naziva i lozinke koja se još uvijek pojavljuje u stvarnom životu. Kombinacija “Admin / Admin123” izgleda kao mnogo bolja solucija.. ne. Ona to nije. Ovakvi napadi znaju trajati mjesecima ako administratori (barem neredovito) ne provjeravaju dnevnike računala.

Ove upute vam neće pomoći protiv onih koji znaju koga, kada, kako, čime i zašto napasti. Iskustvo pokazuje da protiv takvih napadača nijedna zaštita neće mnogo pomoći.

Ove upute ne uključuju niti mogućnost postojanja “*0-day*” sigurnosnog propusta (“zero-day” propust je onaj za koji ne zna nitko osim onoga tko za njega zna). Npr. možda postoji *bug* koji se aktivira kad imate lozinku dulju od 32 znaka, a manifestira se tako da je dovoljno upisati bilo koje slovo i sustav će vas pustiti unutra? Ne bi bilo prvi puta da se takvo što dogodilo.

Kako povećati sigurnost računala povećanjem sigurnosti korisničkog računa te smanjenjem mogućnosti da se neželjeni entiteti u neželjeno vrijeme i s neželjene lokacije prijave na nj te počine neželjene radnje

---

Windows – Korisnički račun (User Account)

Ukratko: Nemojte korisničkim računima dodjeljivati općepoznate nazive/imena (Prodaja, Tech, Ivan, …)

Opširno: Ovo je teže promijeniti jednom kada je sustav već u uporabi, ali ako kreirate nove korisnike – stavite broj na kraj naziva (Frank74) moguće i poneko nasumično slovo na početak (ABNorma1). Naime, ako napad nije ciljan i ako napadači već ne znaju točan naziv korisnika, onda će pokušati s poznatim nazivima korisničkih računa, a oni uključuju nazive odjela poduzeća i/ili najčešća osobna imena.

Računu "Administrator" bi bilo dobro promijeniti naziv.

Detalji:

- BleepingComputer – hxxps://www.bleepingcomputer.com/tutorials/rename-administrator-account-in-windows/ (*1)

Video: (*nema*)

Windows – Lozinke

Ukratko: Lozinke trebaju imati imaju barem 12 znakova i za svakog korisnika (i aplikaciju!) neka bude drugačija. Jednu lozinku koristite samo za jednu uslugu.

Opširno: Mnogo sigurnija je dugačka lozinka koja se lako pamti nego kratka koja poštuje "pravila kompleksnosti" – pravila kompleksnosti su kompleksna samo ljudima koji lozinku trebaju zapamtiti. Programima je svejedno čime rukuju. Većina web aplikacija koje možete pronaći na Internetu, a koje služe za provjeru kompleksnosti lozinke, su varljive i ne treba ih baš slijediti sa strahopoštovanjem. Npr. na mnogim takvim stranicama lozinka "111111111111111" će dobiti nižu ocjenu od lozinke "837jsu645KEU.-!" iako je u stvarnosti to vrlo sigurna lozinka i programima koji pokušavaju provaliti metodom uzaludnih pokušaja ("brute force") će trebati milijuni godina dok na nju dođe red. Osim ako se netko ne dosjeti: -"*Hm, a možda je netko za lozinku odabrao pet puta po tri jedinice?*" Tad ste gotovi. Zato dodajte uskličnik u sredinu – "111111!1111111". Teško da će se netko dosjetiti: -"*Hm, a možda je netko za lozinku odabrao dva puta po sedam jedinica stavivši uskličnik između njih e ne bi li nam otežao pogađanje?*"

Dakle, lozinka "*Ponedjeljak Utorak Srijeda Cetvrtak Petak Subota Nedjelja 2020*" je praktički "neprobojna", a vrlo lako ćete ju zapamtiti. Pazite na "čžš" – ako sjednete za računalo koje ima samo englesku tipkovnicu… na istoj tipkovnici pazite na "Y" i "Z" koji nisu na istim mjestima. Pazite na raspored specijalnih znakova – uskličnik i dolar su uglavnom uvijek na istim tipkama na mnogim jezicima, ostali specijalni znakovi baš i nisu.

Najmanju duljinu lozinke možete postaviti i pravilom tako da korisnici moraju upotrijebiti onoliko znakova koliko ste propisali i kada budu sami mijenjali lozinku.

Ili zabranite korisnicima da sami kreiraju lozinke nego ih kreirajte vi.

```
GPEdit.msc
   -> Computer Configuration[\Policies]\Windows Settings\Security Settings\Account Policies\Password Policy\
   -> Minimum password length
```

Detalji:

- Microsoft – https://docs.microsoft.com/hr-hr/windows/security/threat-protection/security-policy-settings/minimum-password-length

- Microsoft – https://docs.microsoft.com/hr-hr/windows/security/threat-protection/security-policy-settings/password-policy

Video: https://youtu.be/dF6Qx1LV6VI

Windows – RDP – Admin

Ukratko: Onemogućite administratorskim računima pristup RDP-om

Opširno: Ukoliko je moguće, pristup RDP-om dopustite samo korisnicima tog računala koji i inače rade na njemu. Administrator bi trebao posao organizirati tako da se spoji na svoje računalo kao Administrator, a onda se putem lokalne mreže (LAN) može spajati na računala korisnika kao Admin ako je potrebno.

Detalji:

- Microsoft – https://support.microsoft.com/hr-hr/help/2258492/you-notice-that-the-check-box-deny-this-user-permissions-to-logon-to-a

Također – onemogućite pristup računalima bez odgovarajuće antivirusne zaštite (ako se spajaju djelatnici drugih poduzeća koji Vam održavaju dijelove sustava i/ili programe)

Windows – Shared folders

Ukratko: Preciznim pravilima usko ograničite pristup dijeljenim mapama

Opširno: Vrlo precizno definirajte pravila koji korisnici što smiju raditi na kojim folderima u mreži prema pravilu “Najmanja potrebna prava”. Čest je slučaj da se direktorij podijeli svima (Everyone = Full; Svi = Sve), pa ako napadač jednoga dana uspije “provaliti” u jedno od računala na mreži – šifrirat će dokumente na njemu ali i na svim folderima svih računala u mreži u kojima ima pravo pisanja/brisanja.

Detalji:

- Microsoft – https://support.microsoft.com/hr-hr/help/4092694/windows-10-file-sharing-over-a-network
- Microsoft – https://support.microsoft.com/hr-hr/help/4027674/windows-10-share-files-in-file-explorer

Video: https://youtu.be/6_zf1yd2A1g

Windows – RDP Port 3389

Ukratko: Pomaknite RDP port sa 3389 na neki drugi

Opširno: Svi napadači će uvijek prvo isprobati je li port 3389 na vašoj mreži otvoren prema internetu. Ako jest – počet će s napadima. Ako imate slabu ili kratku lozinku – napad će uspjeti i dokumenti će biti šifrirani. Iskustvo je pokazalo da premještanje porta (npr. umjesto 3389 stavite 4567) smanjuje broj / učestalost napada. Naravno,

neki od napadača će pokušati s drugim portovima, no neki će se jednostavno prebaciti na drugu IP adresu i vaš server ostaviti na miru. Ako imate kompleksniju mrežu i sofisticirane uređaje (firewall, IDS) oni će prepoznati takvo “skeniranje portova” i zabraniti daljnji pristup sa sumnjive adrese. Ako ste instalirali ESET Internet Security na desktop operacijski sustav (Windows 10, 8, 7) on također može u nekim uvjetima prepoznati skeniranje portova i blokirati pristup.

```
Regedit
   -> Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
   -> PortNumber
```

Detalji:

- Microsoft: https://docs.microsoft.com/hr-hr/windows-server/remote/remote-desktop-services/clients/change-listening-port

Video: https://youtu.be/5kQBhPdkXhM

ESET, Windows, Router, … – Firewall

Ukratko: (vezano u promjenu porta RDP-a) Ako je potrebno, u firewallu ESET-a i / ili u firewallu Windowsa (i firewallima svih uređaja na putu između klijenata i servera) omogućite spajanje na RDP sa određene ili bilo koje adrese na Internetu.

Opširno: Kada promijenite port sa 3389 na neki drugi (npr. 4567) Windows firewall ne mora automatski prilagoditi svoja pravila, pa RDP može ostati nedostupan. Isto tako i ESET-ov program se ne mora uvijek 100% savršeno sinkronizirati s Windows Firewallom, pa i on može blokirati pristup. Provjerite u oba programa jesu li prihvatili novu situaciju, a ako nisu – ručno to promijenite.

Detalji:

- NORT – https://www.nod32.com.hr/podrska/kb867
- ESET – https://support.eset.com/en/kb3218
- ESET – https://support.eset.com/en/kb6532
- ESET – https://support.eset.com/en/kb3112
- Microsoft – https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-inbound-port-rule

Pozor: Ako se korisnici na RDP spajaju od kuće iz tipične “kućne internetske veze” onda je vrlo vjerojatno da će svakih toliko dobiti novu IP adresu. Ako ste u pravilima firewalla naveli da dopuštate pristup sa specifične IP adrese – sutra to pravilo može prestati vrijediti jer se korisnici više neće spajati s te IP adrese nego s neke druge koju su dobili tijekom noći. U ovom slučaju morate dopustiti pristup rasponu IP adresa (IP range) dotičnog ISP-a (pružatelja usluga) odn. svih ISP-ova sa kojih se spajaju vaši legitimni korisnici. Ili ćete dopustiti pristup cijelom svijetu u kojem slučaju posebno obratite pozornost na sve druge ovdje spomenute vrste zaštite jer ESET i Windows firewall od tog trenutka sada dopuštaju pokušaj pristupa svima.

Video: https://youtu.be/8LKyMAWbM_4

ESET – Lozinka za “Napredna podešavanja”

Ukratko: Postavite lozinku na “Napredno podešavanje” (Advanced settings password) ESET-ovih programa

Opširno: Ako napad na RDP uspije i napadači se prijave na računalo, trebate znati da to računalo od toga trenutka više nije vaše te su sve razine i vrste zaštite vrlo upitne, pa i ESET-ova. Prvi sljedeći korak će napadačima biti pokušaj isključivanja ili deinstaliranja ESET-a kako bi mogli pokrenuti malware i šifrirati dokumente. Ako postavite lozinku na ESET-ov program – morat će se dodatno potruditi da ga isključe ili deinstaliraju, što nije lagan posao, pa će mnogi odustati i naći manje zaštićenu žrtvu. Ovime će aktivnom ostati barem jedna razina zaštite koja može spriječiti šifriranje.

Detalji:

- NORT – https://www.nod32.com.hr/podrska/kb506
- ESET – https://help.eset.com/eis/13/hr-HR/idh_change_password.html

Video: https://youtu.be/F_PQ0BO4m1Q

Windows – Account Lockout Policy

Ukratko: Uključite “Account Lockout Policy”

Opširno: Prema standardnim postavkama Windowsi će dopustiti neograničen broj pokušaja prijava na računalo putem RDP-a. To svakako promijenite i ograničite, a posebno ako firewall dopušta pristup s više IP adresa ili iz “cijelog svijeta”. Nekakva naša okvirna preporuka je da dopustite 3 pokušaja prijave (“*Account lockout threshold*“), pauza između neuspjelih prijava (“*Reset account lockout counter after*“) neka bude 1 minuta, a nakon 3 pokušaja treba zabraniti prijave sljedećih 15 minuta (“*Account lockout duration*“). Imajte na umu da se i aplikacije mogu prijavljivati, pa ako imate aplikaciju koja koristi staru lozinku – ona će zaključati pristup (“*Account is locked out*“).

```
GPEdit.msc
   -> Computer Configuration[\Policies]\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\
```

Detalji:

- Microsoft – https://docs.microsoft.com/hr-hr/windows/security/threat-protection/security-policy-settings/account-lockout-policy
- TenForums – hxxps://www.tenforums.com/tutorials/87665-unlock-local-account-windows-10-a.html (*1)

Video: https://youtu.be/E3vZi52YM3k

Windows – EventLog

Ukratko: Morate aktivno nadzirati EventLog Windowsa i provjeravati ima li pokušaja neovlaštenog spajanja na

RDP te reagirati.

Opširno: Pod pretpostavkom da ste aktivirali Account Lockout Policy, svi neuspjeli pokušaji prijave na računalo će biti zabilježeni u EventLogu. Praćenjem aktivnosti u tom dnevniku možete uočiti pokušava li se netko prijaviti na računalo s adresa s kojih to ne očekujete – pretpostavka je da većina korisnika ipak pristupa s jednog od lokalnih pružatelja usluga; vanjske korisnike koji putuju također možete staviti u popis poznatih, kako ne bih izazivali sumnju. Osim toga, nisu samo korisnici ti koji se prijavljuju, prijavljivati se mogu i aplikacije, pa tako ako imate neku staru aplikaciju koja se pokušava prijaviti starom lozinkom ona može zaključati račun i onemogućiti korisniku rad.

Uglavnom, ručna metoda je da pokrenete EventVwr (Event Viewer), otvorite "Windows logs" -> "Security" i tražite EventID 4625 (neuspjeli pokušaji prijave; "*An account failed to log on*") i EventID 4740 (račun je zaključan nakon nekoliko neuspjelih pokušaja; "*A user account was locked out*").

U detaljima tih stavki ćete vidjeti i s koje ili kojih IP adresa dolaze pokušaji ("*Source Network Address*"). Ako pokušaji dolaze s Interneta, a IP adresa ne pripada nijednom izvoru koji vam je poznat – firewallom možete zabraniti pristup toj adresi ili tom rasponu adresa ("*IP range*"). Ako pokušaji pak dolaze s vaše lokalne mreže ili čak i sa tog samog računala ("*Source Network Address: 127.0.0.1*") to može značiti dvije stvari – (a) napadač je u vašoj mreži i u tom slučaju ste gotovi. No, mnogo češći slučaj je (b) da se neka aplikacija pokušava prijaviti, a u sebi ima definiranu staru lozinku.

Detalji:

- Microsoft – https://docs.microsoft.com/hr-hr/windows/security/threat-protection/auditing/event-4625
- Microsoft – https://docs.microsoft.com/hr-hr/windows/security/threat-protection/auditing/event-4740

Video: https://youtu.be/mfwYi5XWmlw

Pogovor

Kao što ste vidjeli, većina savjeta se odnosi na promjene i podešavanja u Windowsima, a ne u ESET-ovim programima jer je ova vrsta zaštite ipak više "mrežno" i "sistemski" nego "virusno" orijentirana, iako ESET i ovdje nudi neke mogućnosti. Članak trenutačno podrazumijeva da ste na routeru već napravili odgovarajuća pravila za port forwarding i da ne koristite vlastitu VPN mrežu, RDP gateway, dvočlanu autentikaciju (2FA) i druge napredne tehnike. Također, uvjeti rada u mrežama koje imaju AD (Active Directory) mogu biti drugačiji od opisanih.

Prijedlozi se primarno odnose na radne skupine ("*Windows Workgroup*") i jednostavnije, manje mreže koje najčešće postanu žrtvom napada putem RDP-a.

Primjena savjeta podrazumijeva poznavanje osnova administracije Windowsa; mi možemo pomoći u konfiguriranju ESET-ovih programa, no pomoć oko primjene konfiguracije u Windows OS ćemo prepustiti njihovoj službi tehničke podrške (https://support.microsoft.com/hr-hr/contactus/).

Valja razmisliti i o dodjeli statičkih IP adresa računalima u mreži ako portove sa routera preusmjeravate na lokalne IP adrese kako vam lokalni DHCP ne bi poremetio planove dodjelom nasumičnih IP adresa.

Osim vrlo dugačke lozinke, nijedna od spomenutih metoda sama za sebe ne može spriječiti uspješan napad (a i

lozinka je upitna ako postoji “*0-day*” napad). No, sve metode zajedno mogu obeshrabriti napadača i natjerati ga da potraži drugu žrtvu koja nije posvetila toliko pozornosti svom sustavu.

Neke poveznice vode na stranice sa tekstom koji se ne odnosi na operacijski sustav za desktop, nego na servere i sl. ili vode na zastarjele tekstove (npr. za Windows server 2003). To smo učinili u slučajevima kada su postavke jednake ili slične za obje kategorije ili mogu uputiti na rješenje u novijim operacijskim sustavima.

(*1) Na mjestima gdje nismo mogli pronaći naš, ESET-ov ili Microsoftov članak smo stavili link na stranice trećih poduzeća; iz sigurnosnih razloga smo, ma kako pouzdane bile te stranice, uklonili “živu” poveznicu stavljanjem hxxps umjesto https što ćete morati ručno promijeniti.

ESET-ovo izvješće o sigurnosti za 2020 pokazuje povećanje broja napada na RDP za >700%:
https://www.welivesecurity.com/2021/02/08/eset-threat-report-q42020/

---

rdp xrdp sigurnost xsigurnost security xsecurity