17.februāra vebināra "Efektīva Windows ugunsmūra pārvaldība" laikā iesūtītie jautājumi un atbildes

Atbild CERT.LV kiberdrošības eksperts Andris Medjānis

1. **Ja Windows datoru pieslēdz pie nezināma tīkla, ugunsmūris ir ieslēgts, publiski viss ir liegts?**

   Atbilde: Viss liegts, izņemot tas, kas atļauts. Savukārt, atļauju ir bīstami par daudz. Tādēļ šīs atļaujas vienmēr ir jāpārskata un jāuzlabo.

2. **Kā ugunsmūris var atļaut savienojumu, kas nekad nav ticis atvērts no iekšējā tīkla, un tomēr tas nav drošības pārkāpums?**

   Atbilde: Atļaujas atver kā Windows operētājsistēma pati saviem servisiem un funkcijām, tā arī gandrīz jebkura programmatūra uzstādīšanas procesa laikā.

3. **Bloķēt visu ienākošo, ieskaitot *icmp,* ir diskutējama tēma. *Icmp* atbild ne tikai par "pingošanu", tas ir arī *MTU path discovery* u.c. kontroles un diagnostikas paciņas, kas reizēm salauž lietas.**

   Atbilde: Ja mēs apskatām vidējo ugunsmūra situāciju, tad drošāk ir visu noslēgt. Iespēja kaut kam salūst statistiski ir niecīga, un arī ietekme nejūtama. Par *icmp* ieslēgšanu konceptuāli taisnība, taču tas jādara pareizi un pārdomāti.

4. **Kā bloķēt, lai Microsoft pats neliek klāt jaunus mistiskus *permit rules* pie atjauninājumiem un instalācijas?**

   Atbilde: 1) Lietot grupu politiku ar (svarīgi!) aizliegumu apvienot nosacījumus ar lokālo datoru 2) izveidot ugunsmūra paraugu "wfw", kuru ar uzdevumu pārvaldnieku regulāri importēt.

5. **Jautājums - vai var realizēt šo Windows ugunsmūrī?**
   Es vēlos visu nobloķēt, bet ugunsmūra politiku atvērt/aizliegt realizēju pēc pieprasījuma. Piemēram palaidu programmu un ugunsmūris vaicā vai atļaut šai programmai piekļuvi internetam! Doma - uzraugu visas izejošā/ienākošās plūsmas un pēc pieprasījuma atļauju vai aizliedzu.

Atbilde: Nepieciešama sīkāka diskusija ap tehnisko, biznesa mērķi u.c. niansēm. Bet konceptuāli jāskatās komandu/skriptu virzienā. Piemēram, ja Windows Server SSL sertifikāta atjaunošanas pārbaudei jāatver http 80 ports no jebkuras publiskās IP.

1. New-NetFirewallRule -DisplayName "Atlaut TCP 80 no visurienes" -Name "In_TCP_80_Any" -Direction Inbound -Action Allow -Enabled True -Profile Any -Protocol TCP -LocalPort 80 -RemoteAddress Any
2. {izpilda ienākošo savienojumu}
3. Remove-NetFirewallRule -Name "In_TCP_80_Any"

Vai arī uzdevumu pārvaldniekā pie noteikta notikuma ID (Event ID) ar iepriekš pieminēto komandu atver portu un pie noteikta notikuma ID aizver.

5.1. Cik es zinu, pašā nevar, jālieto trešo pušu risinājumi.

Atbilde: trešo pušu risinājumi var kādu funkcionalitāti sniegt, bet kādu atņemt, piemēram, centrālo pārvaldību. Trešo pušu risinājumi rūpīgi jāizvērtē un jāizmēģina praksē slēgtā, nodalītā testa vidē.

6. **Liekas ļoti liels administratīvais slogs šo menedžēt no GPO natīvi. Vai ir kāds "downside" jeb trūkums šo menedžēt no kāda EDR risinājumu, kas pats pārņem *windows firewall settingus*?**

Atbilde: Jebkura ugunsmūra administrēšanā ir jāiegulda darbs, kas ir vērtīgi ilgtermiņā. Bieži ugunsmūris ir tas elements, kas būtu pasargājis no uzbrukuma, kad pārējās sistēmas to nav pamanījušas. Windows GPO piedāvā lielu pārvaldības detalizāciju, taču to var izmantot savā labā atbilstoši administratīvai kapacitātei. Ugunsmūri ar GPO var pārvaldīt etapos, sākot ar ātru, vienkāršu līmenī ieviest bāzes labās prakses bez riska apturēt uzņēmuma datoru darbību. Turpināt pa nelieliem posmiem (ugunsmūris nav jāievieš viss vienā piegājienā).
Atstāt pārvaldību kādai EDR sistēmai var radīt neparedzamas sekas.

7. **Intune gadījumā, ja *merge* izslēdz, ir jādabū visas *windows default rules* iekš Intune. Iepriekš bija kaut kāds MS skripts, kas spēja rules pārmigrēt no Windows uz Intune. Tagad vairs nestrādā. Kā šo risināt? Ar rokām visas veidojat Intune? Ir kādam pieredze?**

Atbilde: Windows ugunsmūra nosacījumus var eksportēt kā csv vai WFW. Abus tiešā veidā kā pilnu komplektu importēt InTune nevar. Taču InTune sniedz iespēju importēt apakštīklu adreses, portus u.c. liela apjoma datus.

Neizvērtējot konkrētā uzņēmuma prasības, vispārīgi Windows korektai darbībai (t.sk AD vidē) ugunsmūrim nav daudz nosacījumu. Savukārt, visi Windows noklusējuma nosacījumi ir pārāk plašs tvērums. Es ieteiktu nosacījumus veidot ar roku, tādējādi pilnībā kontrolējot situāciju un pārceļot tikai nepieciešamos, un papildus izmantojot minēto nosacījuma detaļu (piem., portus, adrešu apgabalus) importu. Nav perfekti, bet ir daļēja automatizācija.

7.1. Ar Graph imortēt Intune skaidrs. Bet kā tehniski un viegli izeksportēt no windows, lai pēc tam viegli iebarot caur Graph?

Atbilde: MS Graph lokālo iekārtas ugunsmūri (csv vai wfw) nespēs migrēt uz InTune. Ja kāds atrod strādājošu veidu, lūgums padalīties ar informāciju.
Par daļēju risinājuma piedāvājumu sk. iepriekšējo komentāru par importu.

8. Vai ugunsmūris nodrošina aizsardzību arī pret vīrusiem, kas tiek nosūtīti ar dažādiem dokumentiem?

Atbilde: Tiešā veidā nenodrošina. Taču ja ļaunatūra (vīruss) sāk aktivitātes tīklā, tās tiek bloķētas. Bieži datorā ar dokumentu tiek izpildīta komanda, kas šo vīrusu ielādē no tīmekļa, šo darbību ugunsmūris spēj bloķēt. Situācijas ir dažādas, bet ugunsmūris (kas ir tā tiešais pienākums) spēj kontrolēt vīrusa darbību tīklā. Salīdzinājumam, kā zaglis, kas spējis iekļūt dzīvoklī, bet nespēj aiznest mantas, jo iznešanu bloķē ugunsmūris.

9. Vai žurnalēšana nevar negatīvi ietekmēt diska brīvo vietu liela izmēra logfaila gadījumā? Maza izmēra logfails ātri var tikt pierakstīts pilns. Atkļūdošanai tiešām pietiek ar mazu žurnālfaila izmēru. Ar mazu žurnālfaila izmēru produkcijā pat neseni notikumi ātri var tikt pārrakstīti pāri.

Atbilde: Mūsdienu datori ir pietiekami jaudīgi, lai spētu veikt žurnalēšanu bez manāmiem veiktspējas samazinājumiem. Tikai ugunsmūra žurnāli datora ātrdarbību neietekmēs, taču žurnālu ir daudz un jāskatās kopējā aina. Tehniski ikviens drošības elements datoram uzliek papildu slodzi. Ir adekvāta robeža, kur žurnālu apjomu var samazināt bez drošības kompromisiem, taču tas jāizvērtē individuāli. Iesaku veikt testu uz viena, atsevišķi nodalīta datora.

10. **Vai ir kādi apsvērumi, kas būtu jāņem vērā žurnalējot veiksmīgos FW gadījumus? Faila izmēra limiti? Parrākstīšanās problēmas?**

Atbilde: Veiksmīgo savienojumu ir ļoti daudz un apjoms ir milzīgs. Vidējam uzņēmumam parasti veiksmīgie savienojumi būs nepieciešami atkļūdošanai, parasti reālā laikā ar nelielas vēstures prasībām. Incidentu izmeklēšanai vai paaugstinātām drošības vidēm es ieteiktu centrālu žurnālu ievākšanas un apstrādēs risinājumu, ar to atrisinot uz katras lokālās iekārtas limitu un pārrakstīšanas problēmas.

10.1. **Pastāv iespēja, ka sistēma nespēs izveidot norādīto mapi un attiecīgajam lietotājam (mpssvc) nebūs tiesību tajā izveidot žurnālu failus. Nepieciešams šo mapi izveidot un koriģēt pieejas tiesības.**

Atbilde: Ir bijuši gadījumi, kad nevar žurnālu mapi izveidot. Parasti iemesls ir mapes pieejas tiesības. Risinājums nelielam skaitam iekārtu manuāls, piešķirot "NT SERVICE\MpsSvc" tiesības. Domēna datoriem var centralizēti izveidot atskaiti par C:\Windows\System32\LogFiles\Firewall\pfirewall.log faila eksistenci un izmēru, un apdomāt labošanu manuāli vai automātiski (piem., icacls).

11. **Kāds ir efektīvākais veids kā uzņēmumā nobloķēt torentus?**

Atbilde: Jāskatās lietotņu un programmatūras kontrolēšanas virzienā (AppLocker vai ACB).

12. **Vai ir zināma droša recepte, kā pasargāties no nelūgta WPS office? Varbūt tagad, kad Win ugunsmūris var strādāt ar domēna vārdiem?**

Atbilde: lietotņu, programmatūras kontroles risinājumi, kā AppLocker un ACB. Ar šo varēs pasargāties arī no citām nelūgtām programmām, pat tādām, kuras vēl nav izveidotas un draudi vēl nav stājušies spēkā. Domēna vārdu bloķēšana aizsargātu šaurās situācijās, kuras lietotājs var apiet,

programmu datorā pārceļot, piemēram, ar USB zibatmiņu vai failiem.lv / GoogleDrive / OneDrive u.c. Turklāt Windows ugunsmūra domēna vārdi ir sarežģīti centrālā pārvaldībā.