Aplikāciju Baltais Saraksts

efektīva aizsardzība pret vīrusiem

Toms Pēcis

IT risku vadītājs

2015.gada 29.aprīlis

lattelecom

Par ko šodien runāsim?

- Kas ir Aplikāciju Baltais Saraksts?
- Darbs ar ierobežotām lietotāja tiesībām un kā tas ir saistīts.
- Vai Aplikāciju Baltais Saraksts ir jauna tehnoloģija/metode?
- Pret ko **nepasargā** šī metode.
- Microsoft un citu izstrādātāju pieeja?
- Kādām operētājsistēmām ir pieejami šie risinājumi?
- Aplikāciju Baltā Saraksta pielietojums uzņēmumos.
- Aplikāciju Baltā Saraksta tendences

Tradicionālās pretvīrusu sistēmas

- Darbojas pēc melnā saraksta principa, izmantojot zināmo vīrusu datubāzi, tāpēc efektivitāte nevar būt 100%. No pretvīrusu sistēmas viedokļa tiek atļauts viss, izņemot to, ko sistēma atpazīst kā apdraudējumu.
- Mēģina atpazīt vīrusus pēc dažādām pazīmēm, taču nereti to dara kļūdaini, bloķējot leģitīmus failus.
- Ietekmē sistēmas veiktspēju, jo katrs fails tiek analizēts un salīdzināts ar miljoniem ierakstu vīrusu datubāzē.

Kas ir Aplikāciju Baltais Saraksts?

- No angļu valodas Application Whitelisting (AWL)
- Metode, ar kuras palīdzību tiek ierobežota programmatūras izpilde izmantojot baltā saraksta principu.
- Aizliegts ir viss, izņemot to, kas ir iekļauts baltajā sarakstā.
- Gandrīz netiek ietekmēta sistēmas veiktspēja, jo netiek analizēti faili, bet gan salīdzināti ar salīdzinoši niecīgu atļautās programmatūras sarakstu meklējot ceļa (path) vai jaucējfunkcijas (hash) atbilstību
- Efektivitāte ir tuvu 100% un ir atkarīga tikai no konfigurācijas un pielietojuma.

Pret ko nepasargās šī metode?

- Netīša, bet apzināta ļaunas programmatūras instalācija
  - Vīrusi, kas izprovocē aizsardzības atslēgšanu, lai veiktu pārlūka spraudņa, kas ir inficēts, instalāciju. Labs piemērs ir vīruss, kas tika izplatīts Facebook 2013. gadā, kā saite uz video, ko sūtījis draugs.
- Apzināta ļaunas programmatūras instalācija
  - Torentos vai kur citur iegūta programmatūra, kuras legalitāte vai izcelsme ir apšaubāma, kas var saturēt vīrusus.
- Programmatūras ievainojamības, kas ļauj veikt ļauna koda injicēšanu un izpildi operatīvajā atmiņā. Pret šādiem uzbrukumiem var pasargāt tādas tehnoloģijas kā
  - Data Execution Prevention (DEP)
  - Enhanced Mitigation Experience Toolkit (EMET)
  - Citas līdzīgas tehnoloģijas

Darbs ar ierobežotām tiesībām

- Programmatūra normāli tiek izpildīta ar tām tiesībām, kādas ir Jums, kā lietotājam, programmatūras izpildīšanas brīdī.
- Administratoram ir tiesības mainīt sistēmā ko vēlas, tātad arī atslēgt ABS.
- Piemēram, uzbrucējs var izmantot atmiņas injicēšanas ievainojamību Java platformā. Ja process būs izpildīts ar administratīvām tiesībām, tad uzbrucējs varēs izdarīt visu ko vēlas.
- Tas ir būtisks iemesls, lai pārliecinātos, ka lietotājiem ir tiesības tikai tur kur nepieciešams un tikai tādas, kādas tiešām ir nepieciešamas.

Vai ABS ir jauna tehnoloģija?

- Aplikāciju Baltā Saraksta metodika ir pazīstama jau sen
- Tā nav specifiska konkrētai platformai vai operētājsistēmai, taču plašu pielietojumu tā ir guvusi tieši Microsoft Windows platformā jau kopš Windows XP laikiem un saucas Software Restriction Policy.
    - Pārvaldība notiek ar Grupu Politikām
    - Pieejams Windows Pro, Ultimate, Enterprise, sākot ar XP
- Sākot ar Windows 7 tika ieviests šīs tehnoloģijas pēctecis AppLocker. Tam ir plašāka funkcionalitāte, taču tas ir pieejams tikai
    - Windows 7, 8, 8.1 Enterprise versijās
    - Windows server 2008 R2 un augstāk

Citi izstrādātāji un risinājumi

- Citu izstrādātāju specializētie risinājumi arī ir pieejami jau gana sen.
- Jau 2009. gadā starp TOP 5 izstrādātājiem bija tādas kompānijas kā Bit9, Lumension, CoreTrace un SignaCert un arī pretvīrusu risinājumu izstrādātājs McAfee
- Šodien šādus risinājumus piedāvā krietni lielāks skaits izstrādātāju
    - Joprojām starp TOP izstrādātājiem ir Bit9 un Lumension, kā arī ir vairāk kā 10 jaunpienācēji, piemēram, AppSense, Faronics, NextLabs u.c.
    - Starp pretvīrusu ražotājiem ir tādas kompānijas kā McAfee, Symantec un Kaspersky.

Operētājsistēmu atbalsts

- Teju visi specializēto risinājumu izstrādātāji piedāvā savus produktus vairākām platformām, tajā skaitā Linux un MacOS
- MacOS lietotājiem ir jau iebūvēts mehānisms «Parental Control». Kaut arī domāts bērnu netīšas rīcības ierobežošanai, taču visnotaļ labi izmantojams kā ABS risinājums.
- RedHat, Fedora, CentOS un SuSe ir iekļauts risinājums SELinux. Tas strādā pēc marķieru principa, bloķējot tos failus, kam nav, baltajā sarakstā iekļauta, marķiera.
- Debian, Ubuntu, u.c. ir iekļauts risinājums AppArmor. Pēc būtības tas nav Aplikāciju Baltais Saraksts, taču to var izmantot lai uzlabotu drošību. Tas strādā pēc profilu principa, ierobežojot konkrēto aplikāciju vai procesu tādā kā slēgtā vidē.

Pielietojums uzņēmumos

- Lielākais izaicinājums ABS pielietošanai uzņēmumos ir šo balto sarakstu pārvaldīšana. Šajā ziņā specializētie risinājumi ir soli priekšā citiem risinājumiem, taču to lielākais mīnuss ir cena.
- Kaut arī trešo ražotāju risinājumu pieeja un funkcionalitāte ir atšķirīga, tie parasti nodrošina centralizētu pārvaldību tādām būtiskām funkcijām kā:
    - incidentu reģistrs;
    - pašapkalpošanās portāls;
    - IT atbalsta portāls;
    - integrācija ar pretvīrusu risinājumiem;
    - programmatūras inventarizācija
    - dažādu operētājsistēmu atbalsts;
    - programmatūras labojumu pārvaldība.

Pielietojums uzņēmumos

- Gadījumā ja Jūsu uzņēmumā tiek izmantotas tikai Windows operētājsistēmas versijas, kas atbalsta Software Restriction Policy vai AppLocker un datori ir vienotā Windows domēnā, Jūs varat pārvaldīt Aplikāciju Balto Sarakstu centralizēti, izmantojot Grupu Politikas.
- Diemžēl šajā gadījumā Jums nebūs pieejams:
    - - incidentu reģistrs (daļēja funkcionalitāte);
    - - pašapkalpošanās portāls;
    - - IT atbalsta portāls;
    - - integrācija ar pretvīrusu risinājumiem;
    - - programmatūras inventarizācija (daļēja funkcionalitāte);
    - - dažādu operētājsistēmu atbalsts;

Aplikāciju Baltā Saraksta tendences

- Kā jau iepriekš tika minēts, kopš 2009. gada, izstrādātāju skaits, kuri piedāvā kādu ABS risinājumu ir vismaz trīskāršojies.
- Pēc Gartner 2014. gada Q3 pētījuma
  - vismaz 25% uzņēmumu jau aktīvi lieto kādu no ABS risinājumiem
  - vismaz 50% no pārējiem uzņēmumiem nopietni apsver iespēju izmantot kādu no risinājumiem savā infrastruktūrā
- Sakarā ar pēdējā laika izspiedējvīrusu lielo aktivitāti un nodarīto postu uzņēmumiem visā pasaulē, tiek uzskatīts, ka līdz 2018. gadam kāds no Aplikāciju Baltā Saraksta risinājumiem būs iekļauts katrā operētājsistēmā un arī viedtālruņos un planšetdatoros

Aplikāciju Baltais Saraksts Latvijā

- Latvijā ir vairāki uzņēmumi, kas jau ilggadēji izmanto kādu no ABS risinājumiem.
- Uzņēmumu skaits, kuri šobrīd ievieš vai nopietni apsver ABS ieviešanu savā infrastruktūrā strauji aug.
- Diemžēl visbiežāk ABS ieviešana tiek apsvērta tikai tad, kad jau ir nācies saskarties ar kādu no izspiedējvīrusiem vai cita veida vīrusiem pret kuriem ABS būtu pasargājis.

Izmantojiet Aplikāciju Balto Sarakstu!

- Tā ir efektīva aizsardzība pret mūsdienu vīrusiem un uzbrukumiem
- Efektivitāti var ievērojami palielināt to kombinējot ar kādu no pretvīrusu risinājumiem
- Jūs vienmēr zināsiet kas tiek bloķēts un kāpēc
- Jums nebūs jābaidās un jācer, ka Jūsu pretvīrusu risinājums paspēs saņemt īsto jauninājumu pirms kādu no Jūsu darbiniekiem sasniegs kārtējais vīruss
- Tas vienkārši … strādā!

Jautājumi?

PALDIES!