Trent Giever

Ch 9 case project 9-5

7/12/18

Application Whitelisting/Blacklisting

Many people and companies want to be safe online and not gain unwanted attachments. One solution is to have a whitelist that prevents unknown applications from running. Also, the ability on servers to block certain IP addresses, and many other items depending on how it is set up. The ability to block unwanted items on the computer system is important for all users.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Pros | Cons | Ease of Use |
| Bit9 | Uses hashing for authorization of the file to verify the source and allows a predefined list of allowed file sources or types. Like accept all files that have a digital signature and can block all unknown files from running (Priveon). | Bit9 got hacked in an SQL injection hacked that gave the hackers a bit9 signature. Once having a signature, the attackers went after bit9 customers systems. No system is perfect (KrebsOnSecurity, 2013). | By being on of the more well-known companies has an advantage for having the need for ease of use for most users and a larger staff to do so |
| Microsoft AppLocker (Microsoft, 2016) | Can create rules for a group or a single person. The program can block executable files, installer files, DLL files, and packaged apps. Can have custom error messages, import and export new rules to all users evenly, and can block unwanted scripts, etc. | Only runs on servers 2008 & 2012, and on computers with enterprise versions 7+. The program does not filter out unsigned items, and does seem limiting compared to Bit9 | Requires little time and money after setting up |
| SELinux (Selinuxproject, 2017) | Similar to Microsoft AppLocker for windows. Even allows to specify to unlink data from certain users. Enabled by default with red hat Linux version. | Open sourced designed by NSA | Since it is built into Linux it is easier to use than a 3rd party that has to have more permissions. |
| Netflix FIDO (The Netflix Tech Blog, 2015) | The system Netflix has been using got released for everyone to use after 4 years of testing. Designed to record more accurately the activities on the network, like firewall attempt, failing hard drive and alert the it help desk. Designed to work with a strong database and processing ability along with some other programs. | Flaw in limited ability of what it can protect the user from, and requires Netflix for updates with limited support | Since it is not open source it is a gamble if it will work for every system |

After doing some research onto the varies different types it is important to have some level of whitelisting or blacklisting to protect the system. The website that I found that listed all the major whitelisting recommended to use a non-3rd party program that has limited ability (Cooprider, 2016). The best kind is one made by the company like Microsoft or Apple, and not one that is limited to the surface. The one that I would use is the one that comes built in and designed for the system to avoid the possibility of failed communication. The best practice is to always use the program that comes with the system.

# References

Cooprider, N. (2016, February 3). *Whitelisting is Dead, Long Live Whitelisting!* Retrieved from threat stack: https://www.threatstack.com/blog/whitelisting-is-dead-long-live-whitelisting

KrebsOnSecurity. (2013, Febuary 13). *Bit9 Breach Began in July 2012.* Retrieved from KrebsonSecurity: https://krebsonsecurity.com/tag/bit9-breach/

Microsoft. (2016, August 31). *What is applocker.* Retrieved from Microsoft: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/ee424367(v%3dws.11)

Priveon. (n.d.). *What is Bit9 parity and application whitelisting.* Retrieved from PRIVEON: http://www.priveon.com/csamigration/bit9-parity-faq

Selinuxproject. (2017, April 7). *New Users.* Retrieved from selinusproject: http://selinuxproject.org/page/NewUsers

The Netflix Tech Blog. (2015, May 4). *Introducing FIDO: Automated Security Incident Response.* Retrieved from The Netflix Tech Blog: https://medium.com/netflix-techblog/introducing-fido-automated-security-incident-response-1961f34f7da3