PS August Ask the Expert

Stephen Dominguez // Worldwide AIX Security Lead, IBM Systems Lab Services

[bio]

Stephen Dominguez is the worldwide AIX security lead for IBM Systems Lab Services. Email him at sdoming@us.ibm.com if you'd like to arrange a conference call to discuss AIX and Linux security consulting services. To learn more about the cybersecurity services he provides for IBM visit his blog, www.securitysteve.net.

Q: Does IBM have an anti-virus solution for AIX?

Yes, IBM has the AIX* Trusted Execution tool that serves as a solution for anti-virus cyber defense. That said, it should be paired with a traditional third party anti-virus solution to achieve a comprehensive defense-in-depth cyber defense for not just viruses, but all types of malware. AIX Trusted Execution and traditional anti-virus solutions use completely different but complimentary approaches to virus protection, and I recommend both solutions for all AIX organizations.

AIX Trusted Execution is part of the AIX base OS for version 6 and above, but when adopting Trusted Execution, I also recommend using the PowerSC* GUI, which has useful centralized management functionality that supports Trusted Execution integration. Turn to “tktktk” on page TK to learn more about how PowerSC simplifies security and compliance.

AIX Trusted Execution provides kernel-based whitelisting, which is a very powerful countermeasure to not just viruses, but all types of malware. In addition to whitelisting, AIX Trusted Execution provides a database containing digital signatures of AIX operating system files. Trusted Execution allows you to use these digital signatures to cryptographically verify that the AIX executables installed on your system are absolutely identical to the ones published by IBM and thus ensure they haven't been altered by a hacker.

What is whitelisting? Whitelisting is a cybersecurity defense that consists of controlling what executables are allowed to execute by defining a list of authorized executables. If a file is not whitelisted, it would be considered as not authorized for execution. Whitelisting isn't just applicable to standard binary executables, but also to libraries and scripts.

Two approaches are available for implementing whitelisting. The easier option is to simply detect executables that aren't whitelisted. An alternative approach is to prevent the execution of files that aren't whitelisted. The latter reduces security risk to a greater degree but requires more effort to correctly implement.

Why is whitelisting important? In numerous security breaches, attackers commonly use malware. In some breaches, attackers have used multiple types of malware to facilitate their successful breach. Attackers can also use hacking tools to enable them to further penetrate a victim's environment.

When whitelisting is properly implemented, all types of malware, including viruses and hacking tools, would be either prevented from execution or immediately detected, depending on which whitelisting approach you implement. Whitelisting also protects you from malware that hasn't been identified nor registered to anti-malware vendor databases—this is what sets it apart from traditional anti-virus solutions.

What priority should whitelisting be given? In the recently released Center for Internet Security 7.1 controls (cisecurity.org/controls/), which provides universal cybersecurity prioritized best practices for all types of organizations from small to large, sub-controls 2.7, 2.8, and 2.9 recommend whitelisting for Implementation Group 3 organizations, organizations with security staff trying to prevent zero-day attacks and attacks from sophisticated adversaries. Sub-controls 2.7-2.9 fall under control 2, which is priority 2 out of 20, which places it under the next to highest control priority.

What priority should traditional anti-virus be given? Traditional anti-virus solutions fall under CIS control 8 (malware), which is six control priorities lower than the control whitelisting is found under. Although this control has a lower priority than whitelisting, CIS recommends all types of organizations, Implementation Groups 1, 2, and 3, are expected to implement CIS sub-control 8.2, 'Ensure Anti-Malware Software and Signatures are Updated'.

Why should Trusted Execution be paired with a traditional anti-virus solution? Traditional anti-virus solutions utilize a database of signatures of known malware in order to detect the presence of malware on a system. This database is constantly updated as new malware is identified and is used to scan your AIX file systems to locate malware on your filesystems.

This type of countermeasure would be good for ensuring that a network Samba share running on AIX isn't exposing viruses to the Microsoft Operating System. Even if a virus is not being executed by the AIX kernel nor exported via a Samba share, it might be copied from your AIX system to other systems, and you would want to be able to detect its presence.

In conclusion, when considering anti-virus solutions, I recommend implementing whitelisting using AIX Trusted Execution and pairing it with a traditional anti-virus solution to achieve a comprehensive defense-in-depth approach to protecting your AIX environment from not just viruses, but all types of malware.

Descriptions of the AIX & Linux Security consulting services he provides, can be viewed at his security blog:
https://securitysteve.net/consulting-services/

[sidebar]
Traditional Anti-Virus Solutions for AIX
The products below are traditional anti-virus solutions that may be considered for use with AIX. It is not a recommended list of solutions. Ultimately, I recommend that clients work with their CIO to vet solutions and determine which is best for their particular organization and security requirements. Options include:

1. Carbon Black CB Response
   https://www.carbonblack.com/products/cb-response/

2. ClamAV
   https://www.clamav.net/

3. F-PROT Antivirus for AIX
   http://www.f-prot.com/products/corporate_users/ibm/aix/

4. McAfee VirusScan Command Line Scanner
   https://kc.mcafee.com/corporate/index?page=content&id=KB52944

5. Powertech Antivirus from helpsystems:
   https://www.helpsystems.com/products/virus-protection-software-linux-aix-and-ibm-i

6. Sophos Anti-Virus for UNIX
   https://community.sophos.com/kb/en-us/118625

   (None of these tools are endorsed by IBM.)