FOCUS

Best Practices for Preventing Virus Attacks

February 18, 2011

topics: best practices | expert content | information technology | anti-virus software | malware | IT security | data security

Best Practices for Preventing Virus Attacks

Best Practices for Preventing Virus Attacks

February 18, 2011

by Kevin Beaver, Anton Chuvakin, Erik Goldoff, Glen Marshall, Richard Stiennon, Fred Stuck

topics: best practices | expert content | information technology | anti-virus software | malware | IT security | data security

Executive Summary

Malware is getting meaner and more malicious as hackers become more sophisticated and serious. Adware, spyware, Trojan horses and garden-variety viruses can bring your network to a halt. An ounce of prevention is, of course, worth a pound of cure and — as Focus Expert Erik Goldoff reminds us — "Security is a process, not an event!" So what are the best ways to prevent virus attacks in the ongoing war on malware? In this guide, Goldoff and fellow Focus Experts Kevin Beaver, Anton Chuvakin, Glen Marshall, Richard Stiennon and Fred Stuck share their top 6 best practices for preventing virus attacks

After reading this guide, be sure to check out the entire discussion and join the conversation: http://www.focus.com/questions/information-technology/anti-virus-best-practices-what-are-your-3-tips-preventing/.

Best Practices Checklist

1. Educate your end users.
2. Evaluate your systems thoroughly to ensure you are well-protected.
3. Accept the fact that you cannot stop all attacks, and work on minimizing damage.
4. Maintenance, patching, updates and periodic reviews are key — be vigilant.
5. Deploy ingress, egress and Web filters.
6. Maintain assurance contracts on your anti-virus/ anti-malware solutions.

Best Practices for Preventing Virus Attacks

Best Practices

1. Educate your end users.

"Most viruses enter the network via careless users. While modern and up-to-date automated protections are important, user education and re-education and reminders are essential. This includes terminating users' rights (and maybe their employment) if they are found to be careless." (Marshall)

"Educate the end user on appropriate use, what to look out for and what to avoid. Social engineering is still a major vector for exploitation." (Goldoff)

2. Evaluate your systems thoroughly to ensure you are well-protected.

"It's relatively simple, if you can get past the mentality that simple anti-virus software combined with a strategy of 'we hope nothing happens' is good enough. Here's what you've got to do: 1) know what you've got (systems, sensitive data, and so forth — and, yes, Windows is more susceptible to attack but others are not impervious); 2) understand where the risks are (hint: They're in more places than you can imagine, including your smartphones). Ignore the obvious and the odds are against you." (Beaver)

3. Accept the fact that you cannot stop all attacks, and work on minimizing damage.

"Realize that you will not stop all virus attacks. One AV vendor told me two weeks ago that they have to sort through 300,000 new variants of malware a day! And from personal experience, I know that a targeted variant that never makes it into the wild may never be caught by AV products. So, assume you will get infected and take measures to minimize the damage. Use network defenses to block access to command and control (CnC) servers and prevent exfiltration of data. Use your PC's firewall to prevent connections to outside servers. And finally, develop an effective methodology for re-imaging PCs. You will need it." (Stiennon)

"Be aware of the limitation of today's AV tools. Don't take them for granted like we used to in the 1990s. The tools are fairly likely to miss a modern threat. Even though the exact stats on this differ wildly, people often expect 30 to 70 percent failure rate for modern malware." (Chuvakin)

4. Maintenance, patching, updates and periodic reviews are key — be vigilant.

"Don't just leave your security up to a network firewall and the anti-virus software that came preloaded on your computers: Periodic and consistent system maintenance is key." (Beaver)

"Make sure you send your firewall logs to a syslog server and review them periodically. A simple plot of number of log entries a day may indicate a problem and prompt you to dig deeper. You can also choose to help the Internet community by sending your logs to http://www.dshield.org/howto.html." (Stuck)

"If you are not using Automatic Update for Windows, use some other method to check for and install patches for the operating system and don't forget to install patches for your applications. Patches and hot-fixes will reduce or eliminate vulnerabilities that exploits hit to compromise your system. Not all exploits are considered to be a virus or malware and not addressed by all anti-virus software. Keep your anti-virus/anti-malware product's definition files current. The anti-virus software is like a bouncer at the door, and the definitions are like a mug-shot book that the bouncer uses to identify criminals and deny them access. If you do not have a current mug-shot book, it doesn't matter how good your bouncer is, he'll not know about the newest criminals to block. " (Goldoff)

5. Deploy ingress, egress and Web filters.

"The first item I would like to suggest is ingress and egress filters on Internet routers or firewalls. Most organizations will filter ingress (or inbound) traffic however many do not filter egress (or outbound) traffic. This may not prevent your organization from being infected, however it may prevent your organization from infecting others. Using a Web Content Filter may prevent infection by blocking resolution of known malicious domains. For example: OpenDNS.com, which has free as well as paid service that can block Web content on a variety of topics including adware and pornography." (Stuck)

6. Maintain assurance contracts on your anti-virus/ anti-malware solutions.

"Maintain support and software assurance contracts on your anti-virus/malware software and if possible opt for the centrally managed enterprise versions. This should allow you to push updates and verify updated signatures. It also simplifies management by utilizing the same anti-virus throughout your organization. " (Stuck)

Read the entire discussion, and join the conversation:

http://www.focus.com/questions/information-technology/anti-virus-best-practices-what-are-your-3-tips-preventing/

Contributing Experts

Kevin Beaver
Independent Information Security Consultant, Author, Expert Witness and Speaker, Principle Logic, LLC
www.focus.com/profiles/kevin-beaver/public/

Anton Chuvakin
Consultant, Security Warrior Consulting
www.focus.com/profiles/anton-chuvakin/public/

Erik Goldoff
IT Systems & Security consultant, Goldoff Consulting
www.focus.com/profiles/erik-goldoff/public/

Glen Marshall
Principal, Grok-A-Lot, LLC
www.focus.com/profiles/glen-marshall/public/

Richard Stiennon
Chief Research Analyst, IT-Harvest
www.focus.com/profiles/richard-stiennon/public/

Fred Stuck
Network Security Engineer, Sungard
www.focus.com/profiles/fred-stuck/public/

About this Report

Focus Best Practices Reports are designed to help professionals understand business and technology Best Practices for particular topic areas. The best practices included in each report are sourced from Focus Experts who have exhibited expertise in the particular topic. Best Practices Reports are designed to be practical, easy to consume and actionable.

About Focus

Focus.com makes the world's business expertise available to everyone. At the heart of Focus is a network of thousands of leading business and technology experts who are thought leaders, veteran practitioners and upstart innovators in hundreds of different topics and markets. You can connect with the Focus experts in three primary ways: Q&A, Research and Events. Personalize your Focus.com experience by following specific topics and experts and receive the Q&A, research and events of interest to you. Focus is easy to use and freely available to anyone who wants help making better business decisions.