SANS 20 Critical Security Controls

Peter Silva, 2011-23-08

A couple days ago, The SANS Institute announced the release of a major update (Version 3.0) to the 20 Critical Controls, a prioritized baseline of information security measures designed to provide continuous monitoring to better protect government and commercial computers and networks from cyber attacks. The information security threat landscape is always changing, especially this year with the well publicized breaches. The particular controls have been tested and provide an effective solution to defending against cyber-attacks. The focus is critical technical areas than can help an organization prioritize efforts to protect against the most common and dangerous attacks. Automating security controls is another key area, to help gauge and improve the security posture of an organization.

The update takes into account the information gleaned from law enforcement agencies, forensics experts and penetration testers who have analyzed the various methods of attack. SANS outlines the controls that would have prevented those attacks from being successful. Version 3.0 was developed to take the control framework to the next level. They have realigned the 20 controls and the associated sub-controls based on the current technology and threat environment, including the new threat vectors. Sub-controls have been added to assist with rapid detection and prevention of attacks. The 20 Controls have been aligned to the NSA's Associated Manageable Network Plan Revision 2.0 Milestones. They have added definitions, guidelines and proposed scoring criteria to evaluate tools for their ability to satisfy the requirements of each of the 20 Controls. Lastly, they have mapped the findings of the Australian Government Department of Defence, which produced the Top 35 Key Mitigation Strategies, to the 20 Controls, providing measures to help reduce the impact of attacks.

The 20 Critical Security Controls are:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on the Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

And of course, F5 has solutions that can help with most, if not all, the 20 Critical Controls.

ps

Resources:

- SANS 20 Critical Controls
- Top 35 Mitigation Strategies: DSD Defence Signals Directorate
- NSA Manageable Network Plan (pdf)
- Internet Storm Center

- Google Report: How Web Attackers Evade Malware Detection
- F5 Security Solutions

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com