The Ten Most Important Security Trends of the Coming Year

Experts Predict the Future
The Ten Most Important Security Trends of the Coming Year

Mobile Devices

1. Laptop encryption will be made mandatory at many government agencies and other organizations that store customer/patient data and will be preinstalled on new equipment. Senior executives, concerned about potential public ridicule, will demand that sensitive mobile data be protected

2. Theft of PDA smart phones will grow significantly. Both the value of the devices for resale and their content will draw large numbers of thieves.

Government Action

3. Congress and state governments will pass more legislation governing the protection of customer information. If Congress, as expected, reduces the state-imposed data breach notification requirements significantly, state attorneys general and state legislatures will find ways to enact harsh penalties for organizations that lose sensitive personal information.

Attack Targets

4. Targeted attacks will be more prevalent, in particular on government agencies. Targeted cyber attacks by nation states against US government systems over the past three years have been enormously successful, demonstrating the failure of federal cyber security activities. Other antagonistic nations and terrorist groups, aware of the vulnerabilities, will radically expand the number of attacks. Targeted attacks on commercial organizations will target military contractors and businesses with valuable customer information.

5. Cell phone worms will infect at least 100,000 phones, jumping from phone to phone over wireless data networks. Cell phones are becoming more powerful with full-featured operating systems and readily available software development environments. That makes them fertile territory for attackers fueled by cell-phone adware profitability.

6. Voice over IP (VoIP) systems will be the target of cyber attacks. VoIP technology was deployed hastily without fully understanding security.

Attack Techniques

7. Spyware will continue to be a huge and growing issue. The spyware developers can make money so many ways that development and distribution centers will be developed throughout the developed and developing world.

8. 0-day vulnerabilities will result in major outbreaks resulting in many thousands of PCs being infected worldwide. Security vulnerability researchers often exploit the holes they discover before they sell them to vendors or vulnerability buyers like TippingPoint.

9. The majority of bots will be bundled with rootkits. The rootkits will change the operating system to hide the attack's presence and make uninstalling the malware almost impossible without reinstalling a clean operating system.

Defensive Strategies

10. Network Access Control will become common and will grow in sophistication. As defending laptops becomes increasingly difficult, large organizations will try to protect their internal networks and users by testing computers that want to connect to the internal network. Tests will grow from today's simple configuration checks and virus signature validation to deeper analysis searching for traces of malicious code.

How these trends were determined

Twenty of the most respected leaders in cyber security developed this list. First each proposed the three developments that they each felt were most important. Then they compiled the list of more than 40 trends and voted on which were most likely to happen and which would have the greatest impact if they did happen. That resulted in a prioritized list. To validate their prioritization, they asked the 960 delegates at SANSFire in Washington to each prioritize the 40 trends. More than 340 did so. The SANSFire delegates' input reinforced the experts' prioritization and helped target the Top Ten.

Experts involved with the project

- Stephen Northcutt, President of the SANS Technology Institute
- Johannes Ullrich, CTO of the Internet Storm Center
- Marc Sachs, Director of Internet Storm Center
- Ed Skoudis, CEO of Intelguardians and SANS Hacker Exploits course director
- Eric Cole, author of "Hackers Beware" and SANS CISSP Preparation Course Director
- Jason Fossen, SANS Course Director for Windows Security
- Chris Brenton, SANS Course Director for Firewalls and Perimeter Protection
- David Rice, SANS Course Director for Microsoft .Net Security
- Fred Kerby, CISO of the Naval Surface Warfare Center, Dahlgren Division
- Howard Schmidt, President of ISSA
- Rohit Dhamankar, editor of the SANS Top 20 Internet Security Vulnerabilities and @RISK
- Marcus Ranum, inventor of the proxy firewall
- Mark Weatherford, CISO of Colorado
- Clint Kreitner, CEO of the Center for Internet Security
- Eugene Schultz, CTO of High Tower Software
- Koon Yaw Tan, Security Expert for the Singapore Government
- Brian Honan, Irish Security Consultant
- Roland Grefer, Security Consultant
- Lenny Zeltser, Security Practice Leader at Gemini Systems
- Alan Paller, Director of Research at the SANS Institute