CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Proactive Remedies for Rising Threats

Key Message: Threats to information security are increasingly stealthy, but they are on the rise and must be mitigated through sound policy and strategy.

Executive Summary

Today's threat environment is dynamic and dangerous. Malicious code can spread around the globe in minutes with no human intervention. Attackers are motivated more and more by money rather than by simple curiosity. Perhaps as a result, new forms of attack are evolving, requiring increased vigilance and proactive strategy on the part of defenders. And international law has not kept up; an attacker in another country may be beyond the reach of law enforcement.

It's no wonder security seems like a daunting proposition. But choosing to ignore the threat is a dangerous tactic that can affect not only the organizations that employ it, but also all other entities connected to the Internet. Instead of practicing "security by obscurity," the best tactic against attackers is being informed. In this podcast, we will discuss the current threat environment and explore ways to mitigate the threat.

PART 1: THE EVOLVING THREAT

Recent Changes

- Motivated adversaries now seeking financial gain through phishing, identity theft, or selling credit card numbers. One example is the 2004 arrest of Shadowcrew members.
- This is apparent in identity theft attacks as well as Distributed Denial of Service (DDoS) attacks. DDoS occurs when an attacker floods a target computer or network with traffic from many other computers connected to the Internet so that the target cannot perform its intended function.
- Companies are threatened with downtime if they don't pay money to attackers.

Contrast with the Past

- 2001: Code Red worm -- done for bragging rights
- Two or three years ago, motivation started to shift toward financial gain
- Blaster was probably the last worm released purely for bragging rights
- There's really been a drop-off in the number of worms you **hear about**

Zero-Day Vulnerabilities

- A zero-day vulnerability is a software flaw that is unknown to the good guys, so there is no fix for it
- Bad guys find zero-day vulnerabilities by reverse-engineering software products such as vendor operating systems
- They then can theoretically write malware to exploit the vulnerability
- This can be profitable:
  - Bad guys exploit the vulnerability
  - Bad guys threaten to exploit the vulnerability (extortion)
  - Bad guys sell their malware to other bad guys

The Black Market

- In some countries, it is not illegal to **write** malware (such as viruses and worms). It is only illegal to **use** it.

- Therefore, many people write malware and then sell it on the underground market.

Attackers Out of Reach

- Bad guys don't need many resources -- they piggyback on others' computers and the Internet.
- It only takes one successful entry point to cause a major problem. It's a similar model to terrorism as it's impossible to defend all points of entry.
- Internet has no borders, making things even more difficult for the good guys and even easier for the bad guys.
- Often no way to prosecute or even reach the bad guys. In many cases:
  - We know where the bad guys are
  - We know who the bad guys are
  - For legal reasons, there is no way to go get them
- Their home country may not even deem their activity to be illegal.

PART 2: REDUNDANCY AND DIVERSITY

Redundancy and Diversity

Redundancy: You have more than one of everything
Diversity: You have more than one of everything, but they're actually different.

With these strategies, the motivated attacker must think harder about which part of your organization he will target.

Other mitigation strategies:

- Distribute your workload
- Do risk analysis in advance to understand what an attack might mean to your business. For more information on risk assessment and ROI, see our show notes for The ROI of Security.

Where to Pay Attention

Focus on three issues:

- An event, such as identity theft, is going to happen at some point, so what are you going to do about it? Consider treating this as a business continuity planning issue.
- Assume that not all your employees and contractors are trustworthy, and that there is going to be an attack from the inside
- Be aware of current vulnerabilities and best practices related to the product set that you operate

Sources of reputable security advisory and vulnerability reports include CERT, US-CERT, National Vulnerability Database, and sector-specific Information Sharing and Analysis Centers.

Trade-Offs

Diversity is often successful in mitigating risk. For example, you can run Windows in one place and run Linux somewhere else. However, this doubles the amount of manpower and expertise you need. It's a risk trade-off.

Bottom line: Diversity costs a lot of money, but it works.

Benefits of diversity:

- Recovery time is shorter
- If an incident takes down one system, you still have a similar system that likely wasn't affected. This is true for an attack, patch rollout, or almost anything else.

Keep in Mind

- Scrutinize, analyze, and test all patches in advance of installing them on a production network
- Automated patch distribution has benefits **and** potential risks; could be used maliciously (potential tie to insider threat). A bad patch can take down a network in one click of a mouse.
- Again, diversity can help, though we recognize it is costly and may not be practical for some organizations

All organizations can benefit by implementing the "Fundamental Five" security practices, which are (refer to the Corporate Information Security Working Group report called out in references below):

1. Malware protection, including worms and viruses
2. Change management, including patch management
3. Identity and access management, including privilege assignment and authentication
4. Firewalls including workstation, host, sub-network, and perimeter as required
5. Configuration management

PART 3: OTHER STRATEGIES AND CONCLUSION

Overall Strategies

- Sit down and understand what core services are keeping your business up and running, Treat these (and the information, software, and systems that provide them) as critical business assets.
- Isolate and protect those services from other, non-essential services
- Pay attention to patches, best practices, and proper training
- Separate services, rather than creating single points of failure (For example, have a separate email server, web server, etc.)
- Use a test network when experimenting with new software, hardware, or settings
- Use firewalls to their full potential

Firewalls
People often view firewalls as devices that keep bad guys out. They are much more than that. Firewalls can be either hardware devices or software programs, and they can filter traffic coming into or going out of a network, a sub-network, or a specific computer (host). They are configured to obey a list of rules that can become quite complex.

- **Best mode**: Default Deny All (and permit what's good) vs. Permit All (and deny what's bad)
  - Do not assume everything is good unless it meets "bad" criteria
  - Instead, assume everything is bad unless it meets "good" criteria
- Use **both** ingress filtering (for incoming traffic) and egress filtering (for outgoing traffic)
  - Permit only known good data to **enter** your network
  - Permit only known good data to **exit** your network (helps avoid worm and virus propagation)
  - This can even mitigate against some forms of corporate espionage if only authorized connections to the outside are allowed
- Test rule configuration on a test network before rolling out to production firewalls
- Write firewall rules into your security policy

For more detailed information about firewalls, see CERT's Defense-in-Depth Curriculum at http://www.cert.org/archive/pdf/Defense_in_Depth092106.pdf.

Wrap-Up

- Identify your key assets
- Spend time and money to make sure those assets are protected at the highest level
- Pay attention to mailing lists, trade associations, market-sector specific groups, and other news sources dealing

with Internet security

References

Allen, Julia. "Information and Infrastructures at Risk: What Shall We Do?" SEPG 2006 keynote presentation, Software Engineering Institute, Carnegie Mellon University, March 2006.

Corporate Information Security Working Group. Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. "Report of the Best Practices and Metrics Teams, Appendix C" November 17, 2004; updated January 10, 2005. http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661.

Eazel, William. "Organized cyber criminals dominate malware creation." SC Magazine, February 21, 2006.

McCormick, John and Gage, Deborah. "Shadowcrew: Web Mobs." Baseline Magazine, March 7, 2005. http://www.baselinemag.com/article2/0,1397,1774393,00.asp.

Nyanchama, Matunda. "Enterprise Vulnerability Management and Its role in Information Security Management." Information Security Management Magazine, July/August 2005. Cites Computer Economics figures on worldwide impact of malicious code (p 40); also http://www.computereconomics.com/article.cfm?id=133.

Background sources

Kshetri, Nir. "The Simple Economics of Cybercrimes." IEEE Security & Privacy Magazine, IEEE Computer Society, January/February 2006.
