CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

How to Become a Cyber Warrior

Key Message: Protecting the internet and its users against cyber attack requires a significant increase in the number of skilled cyber warriors.

Executive Summary

Every country whose citizens and organizations use the internet are vulnerable to a massive cyberattack, "where financial, transportation, telecommunications, and even military operations are now deeply dependent on data networking. U.S. security officials say the country's cyberdefenses are not up to the challenge. In part, it's due to a severe shortage of computer security specialists and engineers with the skills and knowledge necessary to do battle against would-be adversaries. The protection of computer systems essentially requires an army of cyberwarriors, but the recruitment of that force is suffering." [1]

In this podcast, Dennis Allen, a member of CERT's Workforce Development Team, discusses useful approaches and resources for becoming a capable and skilled cyber warrior.

PART 1: GROWING DEMAND FOR SKILLED PROFESSIONALS; STARTUP RESOURCES FOR GETTING SMARTER

What is a Cyber Warrior?

A cyber (aka computer) warrior is your traditional information technology or information security professional who is responsible for computer network operations. This role may include dealing with attacks on the network, network defense, and network exploitation.

Most of today's organizations (government and commercial) conduct business on the internet. The internet provides ready (and often anonymous) access for criminals, foreign militaries, and other bad actors, which can result in the compromise of critical infrastructure and information for financial gain, and theft of intellectual property.

As a result, there is a growing demand for skilled professionals, for both defensive and offensive operations.

Getting Started

Here are some guidelines, based on level of expertise (high school, college, professional, and business leader).

Start with readily available resources: websites, videos, tutorials, common threat descriptions, online safety websites, and specific technologies (refer to the Resources section)

- For younger kids: Carnegie Cyber Academy, an online gaming environment to learn about phishing and cyber bullying
- For leaders: Stop Think Connect, a U.S. Department of Homeland Security leadership campaign to promote security awareness
- For more indepth information, including scenarios:
  - 2600 Hacker Quarterly
  - Stealing the Network Series; How to Own a Continent
- Movies such as Sneakers, The Net, War Games, Firewall, Hackers, and The Matrix
- Professional organizations such as the Information System Security Association

---

PART 2: GAINING PRACTICAL, HOW-TO EXPERIENCE

Get Your Hands Dirty

Create your own operational "sandbox" and start experimenting with, for example:

- VMware
- VirtualBox from Sun/Oracle
- Installing Linux and Windows operating systems
- Downloading a CD image, an ISO file, and run this within a virtual environment
- Downloading firewall distributions, such as one from Endian. This will help you learn about access control lists, proxy and filter capabilities, intrusion detection, network monitoring, and anti-virus.
- Trying out security tools distributions such as BackTrack

High school and college students may want to consider cyber camps, cyber quests, and competitions including:

- Cyber Foundations
- Cyber Patriot
- National Collegiate Cyber Defense Competition

Helping Family and Friends

Most people are not familiar with all of the ins and outs of computer security. Here are some additional resources to consult when you're asked to help:

- OnGuard Online tutorials on securing home networks
- Security Tango if your computer is running slow

Be very careful. Don't plug a bad computer into your network. Have an isolated connection or don't use the internet at all. Make sure your diagnostic tools and utilities are on a separate CD.

If you see something that you think might be illegal, consult the U.S. Department of Justice's Computer Crime & Intellectual Property Section website for information about reporting cyber crimes.

Cautionary Advice

Don't go rogue such as randomly downloading tools and running them on your home, college, or work network as this may violate terms of service and acceptable use policies. And you may end up doing something illegal, even by accident.

Practice in an isolated environment. If you seek help online, make sure the source is reputable and trusted.

Be careful with whom you make contact. Criminals such as Albert Gonzalez are always looking for willing and skilled associates to commit cybercrimes.

PART 3: PURSUING FORMAL EDUCATION AND CERTIFICATION

Formal Education

A bachelor's or master's degree in information assurance or computer science is important for career advancement. Programming classes in Java, C, and Python help develop skills in evaluating logic problems, finding programming flaws, and troubleshooting.

Taking programming and operating system courses at a community college is also a good step.

However, most formal degree programs will not teach you how to think like a bad guy or develop malicious code.

Certifications

Certifications do help in providing specialized training but they too concentrate on career advancement, not necessary thwarting attacks. Some of the leading ones include:

- U.S. Department of Defense Directive 8570 for training, certification, and workforce management
- Certified Information Systems Security Professional (CISSP)
- CompTIA Security+ certification
- Certified Ethical Hacker

Breadth and Depth

Most cyber security professionals have a breadth of knowledge but are missing technical depth. Most attackers are experts in a specific area such as writing an exploit or wireless hacking. Cyber warriors also need to specialize in areas such as forensics, intrusion detection, or network situational awareness.

Organizational leaders need to understand the skills and expertise of their staff, so they know who to call upon when dealing with an attack.

Resources

[1] Gjelten, Tom. "Cyberwarrior Shortage Threatens U.S. Security." July 19, 2010.

Primary Resources

CERT

- CERT Program web site
- CERT XNET (Exercise Network)

US Government

- US Department of Homeland Security cybersecurity information
- US-CERT
- US Department of Defense education, training, and awareness
- Reporting computer crime

Getting started

- OnGuard Online.gov
- Stop Think Connect

College and high school

- High school and college competitions: US Cyber Challenge
- Carnegie Cyber Academy (includes resources for parents and educators to go along with this fun gaming experience for children)

General information

- Tips and tech videos from IT ninjas
- CNET Buzz Out Loud podcasts

- Step-by-step cleanup guides for Windows, Mac, and Linux

Additional Resources

Technology and vendor-specific; general security guidance

- VMWare
- Oracle VirtualBox
- Microsoft VirtualPC
- Windows Security (not affiliated with Microsoft)
- Microsoft Safety and Security Center
- Linux security
- Cisco Security Intelligence Operations
- Juniper Networks Security Intelligence Center
- Symantec Security Response
- Get started with programming in Python
- The Open Web Application Security Project (OWASP)

Tools

- Microsoft Windows Sysinternals Tools
- BackTrack Linux: Penetration testing distribution
- McAfee free tools
- Trend Micro
- Top 125 network security tools

Scholarships

- ISC2 scholarships
- Scholarship for Service (SFS) program