Global Information Assurance Certification Paper

Online Information Security Assistance

By Kevin Johnston

Introduction

As more and more IT professionals enter the Information Security arena, it becomes increasingly important to put the resources they need at their fingertips. Many do not know where to start. I can't count the number of times on a mailing list I see requests such as “Help, I’m new to information security. Where do I start?”

When I plunged into information security, I didn’t know where to start either. I asked several colleagues about resources I needed. Some people were tight lipped about it because they feel security will only impair their work. Some were open about it. Most had a very narrow view of information security. I would often get the old response “Use a Firewall, that’s good enough.”

At first, it was extremely frustrating. I surfed the web for hundreds of hours. I would get tens of thousands of hits. Most of which were totally irrelevant. I can’t fathom the number of hours I put in SORTING through all the information I found. (Boy did I get good at surfing after all this). I found bits and pieces and ever so slowly did I start to see the big picture.

After seeing so many messages for help and remembering the countless hours I put in during my research, I began organizing my resources by topic so others wouldn’t have to painstakingly surf the net and be overwhelmed with information. Not all of my research is included here but you will have enough resources to get started and stay current in the information security field.

NOTE: All URLs listed in this document were verified as of August 25, 2000.

Incident Response Centers

Probably the most important resources on the Internet are Incident Response Centers. They keep the world informed of all the latest threats, vulnerabilities, and countermeasures available.

These centers have become focal points in information security. Most vendors funnel all their discovered vulnerabilities and patch information to these centers. You don’t have to monitor each site hourly or daily. Most offer the ability to subscribe to their mailing list so you can get notified immediately of any new risks. Several centers offer whitepapers and/or FAQs with more detailed information on a particular topic. A visit to such sites is a must.

Australian Security Emergency Response Team (AUSERT)

http://www.auscert.org.au/

Air Force Computer Emergency Response Center (AFCERT)
http://afcert.kelly.af.mil/

Computer Emergency Response Team Coordination Center (CERT)
http://www.cert.org

Computer Incident Advisory Capability (CIAC)
http://ciac.llnl.gov

Defense Information Systems Agency Center for Automated Systems Security Incident Support Team (ASSIST)
http://www.disa.mil/ciss

Center for Education and Research in Information Assurance and Security (CERIAS) – formerly COAST
http://www.cerias.purdue.edu

Department of Defense Computer Emergency Response Center (DOD-CERT)
http://www.assist.mil/

Federal Computer Incident Response Capability (FedCIRC)
http://www.fedcirc.gov

Forum of Incident Response and Security Teams (FIRST)
http://www.first.org

National Infrastructure Protection Center (NIPC)
http://www.nipc.gov

National Security Agency (NSA)
http://www.nsa.gov/

Nation Institute of Standards and Technology (NIST) - Computer Security Resource Center
http://csrc.ncsl.nist.gov/

European CERTs
http://www.cert.dfn.de/eng/csir/europe/certs.html

Anti-Virus

Another crucial realm of information security is anti-virus protection. Viruses are definitely on the rise and have seen a lot of publicity in the news in the past few years. In the recent 2000 Computer Crime and Security Survey, it was reported that 85% of all respondents detected computer viruses.

Fortunately, there are many vendors and organizations with web sites that keep up-to-date information on the latest virus threats and how to counter-act them. If they offer mailing lists, I highly recommended you use them.

AVP Virus Encyclopedia
http://www.avpve.com

CERT® Coordination Center
http://www.cert.org

Computer Virus Myths
http://www.vmyths.com/

DataFellows Anti-Virus
http://www.datafellows.com/virus-info/

IBM's Anti-Virus Online
http://www.av.ibm.com

Network Associates Virus Alerts
http://www.mcafeeb2b.com

Sophos Anti-Virus
http://www.sophos.com

Symantec Anti-Virus Center
http://www.symantec.com/avcenter

Trend Micro
http://www.antivirus.com/pc-cillin/vinfo/

Virus Bulletin Home Page
http://www.virusbtn.com

Mailing Lists, Online Magazines, and Digests

A great way to stay current is to subscribe to mailing lists, online magazines, digests, bulletins, etc. By doing this, you get the information when it's released. You don't have to hunt for it. It comes to you.

Mailing lists involve e-mail discussions on various topics such as firewalls. There is a lot of useful information to find here. Many information security professionals will gladly help you or point you in a direction. Some sites archive this information for future use. I have included some links below to get you started.

And if any of your vendors have mailing lists or security bulletin boards, get on them!

Global Network and Computing Firewalls Mailing List
http://lists.gnac.net/firewalls

NFR Firewall-Wizards Mailing List
http://www.nfr.net/forum/firewall-wizards.html

SecurityFocus Mailing Lists:
http://www.securityfocus.com

- Bugtraq Software/Hardware Bugs
- Focus-IDS Intrusion Detection Systems
- Focus-IH Incident Handling
- Focus-LINUX Linux
- Focus-MS Microsoft
- Focus-SUN Sun Solaris
- Focus-VIRUS Viruses
- Incidents Information Security Incidents
- Pen-Test Penetration Testing

Internet Security Systems Mail Lists
http://xforce.iss.net/maillists/index.php

- Alerts
- Intrusion Detection Systems

SecurePoint Mailing Lists Archives
http://search.securepoint.com

There are also some great digests and online magazines you can subscribe to. Some will mail you hard copies. I strongly recommend you visit all and subscribe to at least a few. The information they offer usually can't be found elsewhere.

Information Security Magazine
http://www.infosecuritymag.com

Security Wire Digest
http://www.infosecuritymag.com/newsletter

Internet Security Systems Digests
http://xforce.iss.net/maillists/index.php

- NSA Digest
- NT Security Digest
- SecNews Digest
- SecTech Digest

InternetWeek Magazine

http://subscribe.internetwk.com

Network Computing Magazine
http://subscribe.networkcomputing.com

Risks Digest
http://catless.ncl.ac.uk/Risks

SANS Security Digests
http://www.sans.org/newlook/digests/index.htm

- SANS Security Alert Consensus
- SANS Windows Security Digest
- SANS NewsBites

Organizations

Information security professionals everywhere recognize these organizations and others. They have contributed significantly to the information security community. They are a wealth of knowledge. They offer information on threats, vulnerabilities, countermeasures, policies, procedures, incident handling, security software and hardware, etc. You name it, they either have information (whitepapers, FAQs, etc.) on it or they can point you to it. They have dedicated staffs to keep the information up-to-date. They do not, however, offer exploit tools. This would be counter-productive to the image of information security by promoting their use.

Most organizations offer training and some offer certifications. Some offer memberships to their associations and all have conferences to go to. The bottom line – here's where you can get involved - SO GET INVOLVED!

Computer Security Institute (CSI)
http://www.gocsi.com

Information Systems Security Association (ISSA)
http://www.issa-intl.org

International Computer Security Association (ICSA)
http://www.icsa.net

International Information Systems Security Certification Consortium (ISC^2)
http://www.isc2.org

SANS Institute
http://www.sans.org

Alternative Websites

It is extremely difficult to categorize these sites due to the nature of the information they offer. They offer some similar information that recognized information security organizations do. However, unlike them, they offer exploit information and tools (mostly public domain).

These tools are useful to information security professionals, who use them to test their own security. However, they are just as accessible to would be hackers with malicious objectives. Because of this, some information security professionals and users may label them as hacker sites.

They do offer us a glimpse of the hacker community and what tools are prevalent on the Internet. I personally keep myself apprised of new scanning tools, which are great for testing my security perimeter from a hacker's point of view. Please be cautious using any site of this nature, especially if you download something. You may get more than you bargained for. You should always use a test machine, which is NEVER EVER connected to your network, to avoid any possible contamination.

Here are some of my favorite links.

Active Matrix's Hideaway
http://www.hideaway.net

AntiOnline
http://www.antionline.com

Fyodor's Exploit World
http://www.insecure.org/sploits.html

InfoSysSec
http://www.infosyssec.org/

Packet Storm Security
http://packetstorm.securify.com

Security Bugware
http://oliver.efri.hr/~crv/security/

Security Focus
http://www.securityfocus.com

Security Portal
http://www.securityportal.com

Technotronic Security Information
http://www.technotronic.com

Standards

IT Standards offer professionals generally accepted practices for developing, implementing, and managing your IT environment. They define what is considered acceptable and offer guidelines to fulfill these objectives and more. Some have very broad scopes like the GASSP, which encompasses many facets of information security. Some are very specific, like the CMV, which focuses on Cryptographic Algorithms. Not all are specific to information security but it's a good idea to be aware of all standards since they intertwine with each other.

Many are ongoing efforts, continually updated. Some of them are rather large and can be overwhelming. Start with the introductions of each, then dive deeper into the ones you feel most comfortable with and which ones will benefit you and your organization the most.

BS7799
http://www.bsi.org.uk/bsi/products/msr/bs7799/index.xhtml

Common Criteria Project
http://csrc.nist.gov/cc

Cryptographic Module Validation (CMV) Project
http://csrc.ncsl.nist.gov/cryptval

Defense Information Systems Agency (DISA) JIEO – Center for Information Technology Standards
http://www.itsi.disa.mil

European Association for Standardizing Information and Communication Systems (ECMA)
http://www.ecma.ch

European Telecommunications Standards Institute
http://www.etsi.org

Generally Accepted System Security Principles (GASSP)
http://www.all.net/books/GASSP2.html

Information Systems Security Organization
http://www.nsa.gov/isso

International Electrotechnical Commission
http://www.iec.ch

International Organization for Standardization (ISO)
http://www.iso.ch

Internet Engineering Task Force (IETF)
http://www.ietf.org

Internet FAQ Consortium
http://www.faqs.org

Internet Society
http://www.isoc.org

Institute of Electrical and Electronic Engineers (IEEE)
http://standards.ieee.org

National Institute of Standards and Technology (NIST)
http://www.nist.gov

National Security Telecommunications and Information Systems Security Committee (NSTISSC)
http://www.nstissc.gov

Hacker Websites

It can be argued that not all the URLs listed below are "Hacker" websites. They all reveal know vulnerabilities to anyone seeking the knowledge. Most also offer exploit information and the tools to use. Even though they pose a great risk by presenting would be hackers with tools of the trade, the information is extremely helpful to information security professionals. By monitoring these sites, information security professionals can be aware of new exploits, sometimes before vendors can patch their products.

There are hundreds, even thousands, of hacker websites easily accessible via the Internet if you choose to search for them, but BE WARNED!!! Visiting some of the sites below may pose a security risk unto itself. You may be exposing yourself to hackers, who could in turn come back to haunt you!

Below are some of my favorite haunts.

2600 Hacker Quarterly	http://www.2600.com
7th Sphere	http://www.7thsphere.com
Attrition	http://www.attrition.org
Badgerz Den	http://www.nauticom.net/www/badgerz/badgerz.htm
Bernz's Social Engineering	http://members.tripod.com/~bernz/soceng.html
Chaos Computer Club e.V.	http://www.ccc.de
CISCO - Pass the Password	http://www.alcrypto.co.uk/cisco
Computer Underground Digest	http://www.soci.niu.edu/~cudigest
Cult of the Dead Cow	http://www.cultdeadcow.com
D.T.M.F.	http://www.johnhead.demon.nl/index.htm
DEF CON	http://defcon.org
DigiCrime, Inc.	http://www.digicrime.com
El Fuckero's House of Hackers	http://cupid.bianca.com/mforums/e/elfuckero
Hacker.Org	http://www.hacker.org
Hackers Club	http://www.hackersclub.com
Hackers Home Page	http://www.hackershomepage.com

Hackers.Com	http://www.hackers.com
HNC - Hack Net	http://www.hack-net.com/html/Main/interface.html
L0pht Heavy Industries	http://www.l0pht.com
Nomad Mobile Research Centre	http://www.nmrc.org
Outpost 9	http://www.outpost9.com
Phrack Magazine	http://www.phrack.com
PLaGuEZ's Armory	http://home.virtual-pc.com/spartan/plaguez
Puppet's Place	http://www.clic.net/~hello/puppet
Rhino9 Security Team	http://www.rhino9.com
Rootshell	http://www.rootshell.com
Satanic Sysadmins	http://www.satanic.org
Undeground News	http://www.undergroundnews.com

Summary

Information Security has exploded in the last few years. I see more information on the Internet than ever before. It's impossible to keep up with every new threat and vulnerability.

You can, however, narrow your focus to those that are relevant to you and your organization. Only in this manner can you hope to keep current. Don't expect to know everything about everything, you can't. With the information and links presented, you can start compiling your own list of resources, which best suit you and your organizations needs.

And in the spirit of writing this document and sharing my knowledge, I hope you also contribute to the effort in years to come.

References

SecurityFocus, Mailing Lists, URL: http://www.securityfocus.com (25 Aug. 2000)

DCI Center for Security Evaluation Standards Group, "An Inventory of Standards Affecting Security (U)", September 15, 1995, URL: http://www.fas.org/sgp/othergov/inventory.html (25 Aug. 2000)

Fred Cohen & Associates, Standards, URL: http://www.all.net (25 Aug. 2000)

Internet Security Systems, X-Force – Mail Lists, URL: http://xforce.iss.net/maillists/index.php (25 Aug. 2000)

NASA Automated Systems Incident Response Capability, Security Organizations, URL: http://nasirc.nasa.gov/NASIRC_home.html (25 Aug. 2000)

NIST, Computer Security Resource Center, URL:
http://csrc.nist.gov/csrc/advisories.html (25 Aug. 2000)

Johnson, Neil. “Security Related Organizations”, URL:
http://www.jjtc.com/Security/org.htm 25 Aug. 2000)

CSI, Press Release on 2000 Computer Crime and Security Survey, 22 Mar. 2000, URL:
http://www.gocsi.com/prelea_000321.htm (25 Aug. 2000)

Ohlson, Kathleen. “Virus Battle Rages On”, 23 Jul. 1999, URL:
http://www.info-sec.com/viruses/99/viruses_082699a_j.shtml (25 Aug. 2000)