GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Fighting Cyber Terrorism – Where Do I Sign Up?
10/15/01

Could this happen?

> *Flight 780, a late night flight originating from Houston, is heading toward Las Vegas. Nothing out of the ordinary seems apparent to all of the passengers and flight crew. Flight 123 from Los Angeles is also heading to Las Vegas, and also seems to be a normal flight. And then, the unthinkable happens. The two planes collide over the Rocky Mountains, killing everyone on board. Air traffic control is stunned, because according to their screens, these planes were not in the same flight path. And then, another report comes of other planes colliding in different parts of the country. What had happened to the state-of-the-art air traffic control systems? Had there been a system glitch? Or was there a power failure? No, what had actually happened was that a terrorist was able to gain control of the air traffic system, and route the planes to their destruction. Seems far fetched? Like something out of a movie? Is this closer to reality than we think?*

September 11, 2001 is a date that will be burned into the minds of all Americans. You can ask anyone, and they will be able to tell you with precise detail, where they were when the atrocities of the terrorist act happened. Almost immediately we were resolute to fight back, to fight the terrorist demon that bestowed such devastation on us. Ever since this country was in its infancy, we have had forces of armed men and women trained to fight these physical, defensive battles. Yet, why have we not paid the same attention and training to fighting those that would compromise us electronically?

Information Warfare

Taken from Citigal Labs research site,

> According to [DoD96], *information warfare* is defined as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks." *Information Warfare* (IW) is a global threat that faces all highly developed nations. IW represents the easiest and cheapest way for less developed nations and other political organizations to anonymously and grievously attack much more powerful nations and companies. [2]

Cyber attacks have historically not been treated in the same fashion as physical defense of the country. In fact, many companies refuse to admit that they were infiltrated by an outside source illegally. A frightening fact is a most seemingly innocuous computer program can wreak havoc and cost millions of dollars in

© SANS Institute 2000 - 2005 Author retains full rights.

lost productivity.

According to Cigital Labs research, the following is a list of just a few attacks that has happened over the past decade:

- MCI Communications switch and credit card penetration resulted in a $50 million loss.
- Russian Organized Crime Electronic Funds Transfer (EFT) Attack on Citibank resulted in a $12 million loss, Aug 1994.
- Sniffer intrusions against DoD computers over the past two years may be centrally coordinated, by a state-sponsored enemy, in preparation of a massive disruptive attack.
- USAF Captain hacks into US Atlantic Fleet ship computer. [2]

Another incident, cited in Newsweek:

> "Last spring someone broke into the computer systems of the California Independent System Operator (Cal-ISO), the state manager of long-distance electricity transmission. According to Cal-ISO, the target was a test system unconnected to the grid. There was no damage. Still, the electronic intrusion, looked at in the light of the Sept. 11 attacks, unnerves the organization." [7]

It's highly possible that we can expect hacking events due to our retaliation against the Taliban and the Al Qaeda network. Yet its unlikely the attacks will come directly from these groups. More than likely, sympathizers to their cause will be those who will try to cripple our infrastructure. We've seen cyber retaliatory attacks against the United States before. One of the most recent cases involves the downing of the U.S. Spy Plane and a Chinese fighter plane. Denial of Service events increased, new viruses like Code Red and Nimda were released, and U.S. Web sites were defaced with anti-American slogans in response to this event.

The latter issue, now called Hacktivism, has increased greatly. According to an article from the Mercury News,

> Malicious hactivists in the past have downloaded potentially sensitive information from India's Bhabha Atomic Research Center and stolen credit-card numbers from a database belonging to the American Israel Public Affairs Committee, a powerful pro-Israel lobby.
> But cyber-attacks have been growing in scope and sophistication in recent years. During the NATO air strikes in Serbia and Kosovo in 1999, some NATO Web servers were disabled after sustained attacks by hackers who NATO believes were working for Serbia, according to the Dartmouth report. [4]

Power supply networks, telecommunication networks, financial networks are all vulnerable to an attack by a terrorist. Yet, we are still behind in the race to secure all critical networks. According to a government report, quoted from a

© SANS Institute 2000 - 2005 Author retains full rights.

BBC article,

> Recent reports and events indicate that these efforts are not keeping pace with the growing threats and that critical operations and assets continue to be highly vulnerable to computer-based attacks. Despite the importance of maintaining the integrity, confidentiality, and availability of important federal computerized operations, federal computer systems are riddled with weaknesses that continue to put critical operations and assets at risk. [1]

Denial of Service attacks and viruses are just the beginning. What if terrorists were able to access our power grids or water supply systems and control them from their desktop PC in their country? According to Tim Belcher, the chief technology officer for Riptech, a Virginia-based information security firm:

> "Many computer systems, such as those controlling power grids and water supplies, are surprisingly accessible through the Internet". "It's not like the typical battlefield where the Army with more tanks wins," he said. ``This is technology. This is something that anybody can embrace and become expert in." [4]

The hard truth is, it is easy to become a cyber terrorist. By taking the correct computer classes and with a little determination, a cyber terrorist can be born within a short amount of time.

Prevention

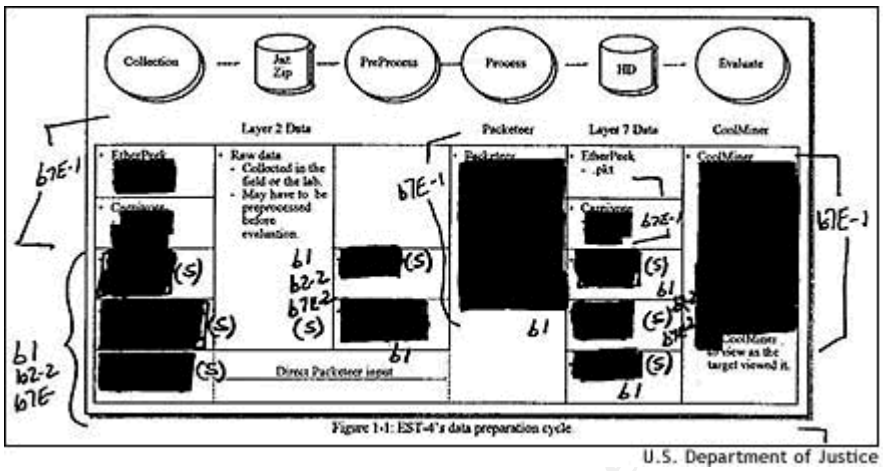
Because of the current critical nature of the security of our electronic infrastructure, the President has created a new advisory position. Richard Clarke, who currently heads a counter-terrorism team, will fill the position of Special Advisor to the President for Cyberspace Security. This position will coordinate government agency and private sector efforts towards securing critical networks. Clarke will report to Gov. Tom Ridge, who will head the Office of Homeland Security.

One of the legislative acts under review from the House of Representatives and the Senate, is the **Combating Terrorism Act of 2001**. This act broadens existing laws and some of important points that came from this act are:

- **Sec 201 AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO COMPUTER FRAUD AND ABUSE OFFENSES.** [9] This also includes the ability of the FBI to use their Carnivore system. This Windows-compatible system works like a sniffer or other diagnostic tools, but it provides the FBI with the ability to distinguish between lawful and unlawful communications depending on the configuration of the Carnivore system. [5]

© SANS Institute 2000 - 2005 Author retains full rights.

The following is a declassified diagram explaining how Carnivore works: 6



U.S. Department of Justice

According to recently declassified documents, Carnivore is actually part of a trio of programs, called Dragon Ware Suite. Dragon Ware Suite has the ability to be used to fully track and reproduce a correspondence trail for suspected terrorists. 6

- **SEC. 103. INCREASED FUNDING FOR THE TECHNICAL SUPPORT CENTER AT THE FEDERAL BUREAU OF INVESTIGATION**. 9 To help meet the demands to combat terrorism, enhance the technical support, and tactical operations of the FBI, this act allocates $200,000,000 for each of the fiscal years 2002, 2003, and 2004.

- **SEC. 210. SCOPE OF SUBPOENAS FOR RECORDS OF ELECTRONIC COMMUNICATIONS.** 9 ISPs will now have to comply with government agency requests to pull any email communication thought to have terrorist connotations.

In 1998, President Clinton announced that he signed President Decision Directives 63 titled Critical Infrastructure Protection Directive. The major points of this directive include:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- Developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

This directive also created the NIPC, National Infrastructure Protection Center. According to their website, the NIPC: 11

> Serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The

© SANS Institute 2000 - 2005 Author retains full rights.

NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The mission of the NIPC is to:

- detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures;
- manage computer intrusion investigations;
- support law enforcement, counter-terrorism, and foreign counterintelligence missions related to cyber crimes and intrusion;
- support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests; and
- coordinate training for cyber investigators and infrastructure protectors in government and the private sector.

Along with these government agencies, there are many private organizations also created to respond to cyber terrorism. Below is a short list:

- Computer Emergency Response Team (CERT) http://www.cert.org/
- Computer Security Division (CSD) of the National Institute of Standards and Technology. http://csrc.nist.gov/
- Forum of Incident Response and Security Teams (FIRST) http://www.first.org/
- International Computer Security Association (ICSA 2) http://www.trusecure.com/
- SANS Institute http://www.sans.org/newlook/home.htm

As the government and these private organizations take steps towards protecting our critical networks, all businesses, great and small, also need to develop their own security policies.

Everyone has a responsibility

There is no excuse for any company that is currently in operation today, to not have a security policy created and enforced. These policies need to be complete, concise, and understandable to all employees that work in the company. They need to be kept up to date and need to reflect the needs of your business. These policies can be pre-written by an outside source or written by the company's security department. Included in those policies, should be references to Password Policies, Internet and Intranet Usage Policies, Network Administration policies, etc. [8]

Every employee needs to understand the importance of a secure password or the consequence of not having virus prevention software installed on each company PC. There must be consequences bestowed upon the employee if these policies are constantly breached. As an old saying goes, "A chain is only

© SANS Institute 2000 - 2005 Author retains full rights.

as strong as it's weakest link". Just one employee with a lackadaisical approach to security to cause a great financial loss (or worse) to a company.

At the same time, any business conducted from the home to the corporate network should also be properly protected. In recent years, it has be the norm for employees to access their company's network via a home connection. It is up to the employee to use all tools necessary to protect the company network. Strong passwords and Virus software are all too important in the battle to secure our networks.

Conclusion

The story at the beginning of this paper was purely fictitious. I don't know enough about our air traffic control systems to know if that type of act is feasible. But knowing how these systems work should not be part of our "job description" as citizens of the United States. The only knowledge that we need to be imparted with is to know that every critical system is secured from these cyber terrorists. We need to know that these types of detrimental acts will never happen to us. We need to know that we can live without the fear of a full-scale infrastructure network disruption. Unfortunately, at this point and time, I don't have that knowledge.

Its clear that this country, and others, have a long way to go to fully prepare and defend against a major electronic attack. I believe that the government and the private sector are starting to realize the importance of a good cyber defense. The events of the past month have changed all of our lives. Perhaps some of us are ready to join this fight against these cyber criminals? I know I am.

© SANS Institute 2000 - 2005, Author retains full rights.

1. Hermida, Alfred **"Doomsday Fears of Terror Cyber-attacks"** Thursday, October 11, 2001
http://news.bbc.co.uk/hi/english/sci/tech/newsid_1593000/1593018.stm

2. Cigital Labs, **Research resources**.
http://www.cigitallabs.com/resources/definitions/information_warfare.html

3. [DoD96] Office Of The Under Secretary Of Defense For Acquisition & Technology**. "Report of the Defense Science Board Task Force On Information Warfare - Defense (IW-D)",** November 1996 Washington, D.C. 20301-3140. No URL sited.

4. Puzzanghera, Jim and Ackerman, Elise **"U.S. Networks Run Big Risk of Cyber-strikes, Experts Assert"** 10/03/01 Mercury News. Found in the **CLASS III TERRORISM** link in http://www.infowar.com/

5. FBI Website , "**Carnivore Diagnostic Tool"**
http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm

6. Meeks, Brock N **"FBI's Carnivore has Partners."** 10/17/00 MSNBC Technology section. http://www.msnbc.com/news/477749.asp

7. Sherman, Erik Newsweek article: **" Terror's Next Target?"** 10/15/01
http://www.msnbc.com/news/638690.asp?0dm=C11LT

8. Information Security Policy World. "**The Information Security Policies / Computer Security Policies Directory"** http://www.information-security-policies-and-standards.com/

9. Senate Bill # S1510, **THOMAS – Legislation on the Internet**
http://thomas.loc.gov/cgi-bin/query/D?c107:3:./temp/~c107d5orDQ::

10. WHITE PAPER **"The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63"** May 22, 1998 **Http://www.terrorism.com/homeland/pdd63.htm**

11. National Infrastructure Protection Center , **Home Page**
http://www.nipc.gov/index.html

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS