



Pittsburgh

Incident Response Group

FALL 2003

Volume 1, Number 1

W

elcome to the First Issue of the Pittsburgh FBI InfraGard chapter's Incident Response Group Newsletter. With this issue, we establish the **Pittsburgh Incident Response Group**.

We plan on discussing the Issues of having an Incident Response Team defined and ready. How these teams can benefit employers, not only in the safety provided by having a team defined to respond to emergencies, but also as a morale builder for the technical development of the staff. There are many benefits to an incident response team, too many to list in these paragraphs alone. We will attempt to provide information to be used in these organizations, who should be included in them, potential reviews, as well as some issues which should be considered.

Some of you may be asking, what is an Incident Response Group? It is business personnel representing a business' various operations groups, brought together to manage a threat to the operations of the business. Our focus for the Incident Response Groups will be primarily focused on the organization's Computing Environment.

We want to thank the countless hours of effort which are contributed by the InfraGard's Board and their supporting membership. Without everyone's combined contributions, this publication would not be possible. We hope that you find the information we provide insightful, resourceful, as well as beneficial.

In
This
Issue

Editors' Welcome Page 1
Security Lessons Page 2
Patch Management Page 3
What is an IRT? Page 4

Editors:
John Kostuch
Albert Whale

<http://www.pittsburgh-infragard.org>

Repeating Computer Security's Lessons

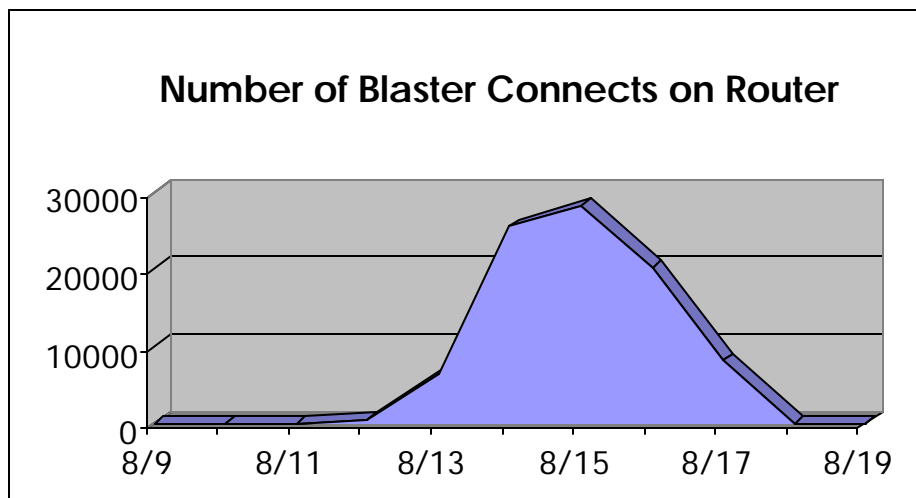
M

any of us remember 2001, *A Space Odyssey*. I for one, wondered about a day when computers would perform more of our daily chores, manage our life support systems, balance our checkbooks, even drive our cars. That day is upon us and computers are with our every day lives. This, the first edition of the Incident Response Group's newsletter, is being produced by a series of computers networked together working in harmony.

My point is, that we have grown more accustomed to working with computers, and using them as tools for our convenience. We have also grown complacent with our approach for securing our environments and networks. August 14th 2003, the worst blackout in the nation's history, many of us were lucky not to experience first hand, but could observe live on a minute to minute basis as it happened on television.

I am a security consultant and work on the Internet to secure environments on a daily basis. In the last couple of years, my work on the Internet has evolved from a relatively open stance, to a more secure posture only permitting that which I allow into my company's network. A cursory view of the firewall logs proves the concept that the world is intimately closer than the same world we grew up in. Essentially, nearly every point in the globe is a router hop away (give or take a few milliseconds). A review of the router logs for August yielded the following logging information against port 135, a well documented port used by various Internet Worms, and Viruses attacking Microsoft systems. Here again, hindsight is 20/20. No wonder *Computer World* picked up on the

story line **Blaster worm linked to severity of blackout** (<http://www.computerworld.com/printthis/2003/0,4814,84510,00.html>). However, I was not surprised. While the story unfolded on CNN, I was emailing associates and asking them about the hidden story. Since then Congress has investigated the blackout and the possible effects of Internet worms such as the Slammer/Blaster/SoBig and others may have had on the nation's worst blackout in history.



However, blaming the Blaster worm is an excuse for not paying enough attention to the security that is implemented. Although security has been a growing budget item since 9/11/2001, most organizations are not able to justify the budget to support the investment. But compare that investment to the number of services unavailable or crippled on or about August 14th.

As a security consultant, I cannot stress enough the importance of due diligence and its associated hidden benefits. I think that it is becoming overwhelmingly clear what the costs are for not applying security in today's world. Lest we repeat it, let us learn from history.

Albert E. Whale, CISSP
Vice President, Pittsburgh FBI – InfraGard
President, ABS Computer Technology, Inc.

You can reach the author for more information on-line
at aewhale@ABS-CompTech.com

Patch Management – Your Responsibility



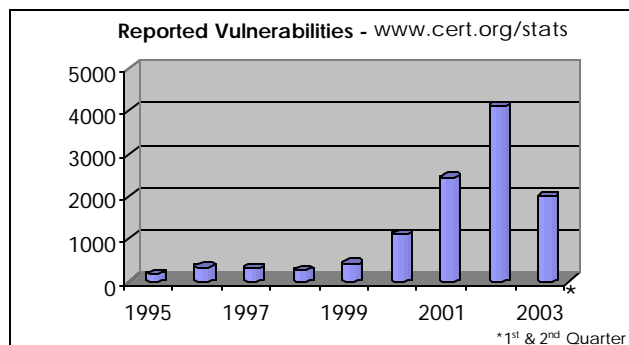
recent report by the *Computer & Communications Industry Association* called Microsoft's dominance in desktop computing a national security risk to the nation's computer infrastructure. Even if this is the only reason, you should have a patch management plan in place and functioning. No matter the shortcomings of a particular application or operating system, it is still your responsibility to keep your systems secure and current.

In today's ever changing world, you can not rest with the latest code update to ensure that an application is secure. Changes required today can be obsolete tomorrow. The window for reacting to code vulnerabilities decreases every year. Being reactive to vulnerabilities is no longer an option. The Slammer virus infected 90% of all vulnerable computers within 10 minutes of its release. The MSBlaster worm spread rapidly even though the patch was released nearly a month before. While intrusion detection systems (IDS), anti-virus software and firewalls are a must for security; they are not a replacement for being preventative measures. Take a proactive approach with an effective patch management process, preparing for when, not if, an exploit is released. Add to your organization's defense in depth security by not solely relying on reactive security measures.

Implementing a patch management process starts with a current technology inventory – what do you have, how many use it and what is the risk if the system is unavailable? Your inventory should include the applications in use and their current versions, the number of clients using the application and the logical risk to your organization's business if the application is attacked. Continue by identifying the latest patches, hot fixes and upgrades distributed for those applications. Based on your organization's need, determine the risk of not applying the patch. If it is necessary to apply the patch, it is important to test it in your environment to ensure it the "fix" does not break or expose another application.

Once tested, the most critical and difficult phase begins – deployment. An efficient deployment method is required. One that is easy for the IT staff to administrate and one that is invisible to or simple enough for clients. Silent installs or upgrades using logon scripts can be efficient, but

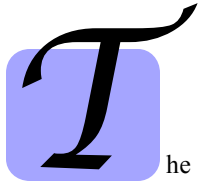
do not forget about your clients. They want to be helpful and to ensure the security of an organization's data assets, but it must be easy for them to understand. Complex steps or unannounced outages give clients an opportunity to delay installation or become irritated. Continued monitoring of your computer environment to make certain a patch has been applied minimizes risk. Nothing will frustrate your efforts to secure the organization more than an employee on vacation if their computer is not patched soon after they return to work. Remote clients and telecommuters are another problem point and illustrate the need for follow-up with computers not patched on a timely basis.



Standardized tools and corporate policies and procedures need to be in place to enforce compliance throughout the organization. Policies should address who manages software installation and upgrades and the employee's responsibilities to follow them. This entire effort is not the work of one or a few individuals. Sufficient resources need to be dedicated with clearly assigned responsibilities throughout the patch management plan.

Organizations are under increasing threat by vulnerabilities in application and operating system code with less and less time to react to their exploits. Proactively responding to patches, hot fixes and upgrades with an operational plan can a long way to protecting your organization from a vulnerability's exploit. However, patch management is one layer in your organization's blended security plan. It takes more than one approach – firewalls, anti-virus software, IDS and backups – to ensure an organization's security particularly in the post-September 11th world. Developing an effective patch management pan will minimize your organization's exposure to known exploits and vulnerabilities, reducing exposure to risk from attacks ensuring security and integrity of your environment.

CSIRT : Computer Incident Response Team



The normally quiet August summer days turned dark and noisy when back-to-back-to-back viruses struck cyberspace. Pagers and cell phones rang around the world as IT departments began to respond to the attacks on their infrastructure. For days and in some cases, weeks, companies and organizations worked aggressively to eliminate the threat and damage of the MSBlaster and Natachi virus and the Sobig.F mass mailer worm.

All of these organizations, both large and small, had a plan in place to handle this emergency situation. They might not have had a formal plan or even thought of a plan. Handling an emergency computer incident *ad-hoc* is a plan, poor planning to be sure, but still a plan. A small number of organizations had a formal and workable process. Those organizations had what is sometimes called an “incident response team” or “computer security incident response team.” A Computer Security Incident Response Team (CSIRT) is a group of IT workers who come together to manage threats and attacks on their organization. There is an established

process to call out the team, handle the incident, communicate with management and clients, and learn from the incident. As evidenced by the increasing number of vulnerabilities, computer crimes and terrorism threats, organizations need an established rapid response capability to limit damage, lesson recovery costs and to help prevent future incidents.

Even with the heightened awareness of computers in everyday life, not every organization is equipped to have a dozen or so of their IT staff on standby. But the need still exists to recognize, analyze, and respond to threats and attacks. The Pittsburgh Chapter of InfraGard understands this need and is establishing a chapter-wide CSIRT group. The **Incident Response Group** will provide members with the skills and the information to, not only; develop their own CSIRT, but to assist in incident response as well.

If you are interested in volunteering your skills or can provide CSIRT development expertise, please contact irg@pittsburgh-infragard.org. If you are interested in utilizing **Incident Response Group** services, look for our next issue.

InfraGard

*InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. The goal of **InfraGard Pittsburgh** is to enable the flow of information so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.*

InfraGard Pittsburgh Board of Directors

President	Helen L. Jones	helen.jones@pittsburgh-infragard.org
Vice-President	Albert E. Whale, CISSP	albert.whale@pittsburgh-infragard.org
Secretary	John Kostuch	john.kostuch@pittsburgh-infragard.org
Treasurer	Patricia Rossi	patricia.rossi@pittsburgh-infragard.org
Coordinator	Thomas X. Grasso	coordinator@pittsburgh-infragard.org