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 (Security 401)"
at http://www.giac.org/registration/gsec

Intrusion Detection:
Ideas for Today and Tomorrow

By: Chris Lanzilotta

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

A Look Back in the Past

During the early 1990's, both the US DoD and the British Ministry of Defense spent an enormous amount of time, money and other resources trying to secure their computer networks by applying the philosophy of Risk Avoidance. The philosophy of Risk Avoidance simply stated that a computer system should not be deployed if it contained any exploitable security flaws. This philosophy became apparently unachievable for the DoD through repeated penetration tests. Studies showed that after approximately 8800 intrusion attempts, one in six were detected, and only 4% were reported. This seemed to prove that even with unlimited resources, we as human beings are not smart enough to build a Secure Distributed Computing System that is usable.

There is no such thing as 100% security. Despite massive expenditures and the time spent the DoD was unable to develop and operate a system that was 100% secure… the DoD did not even know that their systems were under attack… and the DoD did not know what actions to take in response to an attack.

Risks of Today

The Internet is virtually extending our business networks beyond the traditional "Brick and Mortar" Boundaries. Business requirements are driving IT initiatives to take advantage of Internet-based standards and extend their services and networks to internal constituents requesting Internet resources, Business Partners, and customers. By doing this, we are increasing our exposure to threats from trusted and unknown users attempting to probe and potentially cripple or corrupt those applications we seek to provide.

E-commerce is symmetrical in nature. Today's networks are designed with symmetric communication as its primary enabler for commerce. As we open our networks up to these new services, we increase our exposure to new threats. As the hacker community is growing at an exponential rate, the Information Security Specialist shortage increases.

© SANS Institute 2000 - 2005 Author retains full rights.

Hackers are developing more complex and sophisticated tools that are becoming freely available to all levels of "hacker Types" from Script Kiddies to Governments.

Hacking has become the hobby of choice for some people all around the world. Using a search engine, Internet users can easily locate numerous sites describing tactics to disrupt or break into systems. The tools used for hacking are becoming more powerful and easier to use. Anyone with enough of a motive to break into a system can quickly attain the necessary information without being an expert hacker.

Lessons Learned

History shows that "Risk Avoidance" did not work for the Trojans. Troy was a walled city, capable of sustaining itself without outside assistance. The Greeks sailed to Troy and waited 9 years to retrieve Helen. After waiting outside of thee city, the Greeks up and left. However, they left behind what the Trojans considered a "Victory Prize." They proceeded to open the gates of Troy and accepted the gift in within the city walls. During the night, the Greeks soldiers who had been hiding in the giant horse descended, and sacked the whole city!

The Great Wall of China and the Berlin Wall are examples of the "Fortress Mentality" proving ineffective.

The problem is though, as an industry, we are taking these approaches to Information Protection and Security. We need to mature as an industry. Firewalls cannot be used as the "Silver Bullet" security technologies that keep the attackers out. As long as we allow communications within and beyond our networks, we expose ourselves to vulnerabilities. The communications of our networks must be symmetrical to allow commerce.

Vision for the Future

The vision for the future is to "*Reduce the Exposure of Information Security Risks by adopting Adaptive Security solutions and practices that provide effective Protection, Detection, and Reaction to Security Incidents*." Information Protection is about protecting the business process with Policies, Processes, and Technologies that provide Confidentiality, Integrity, and Availability.

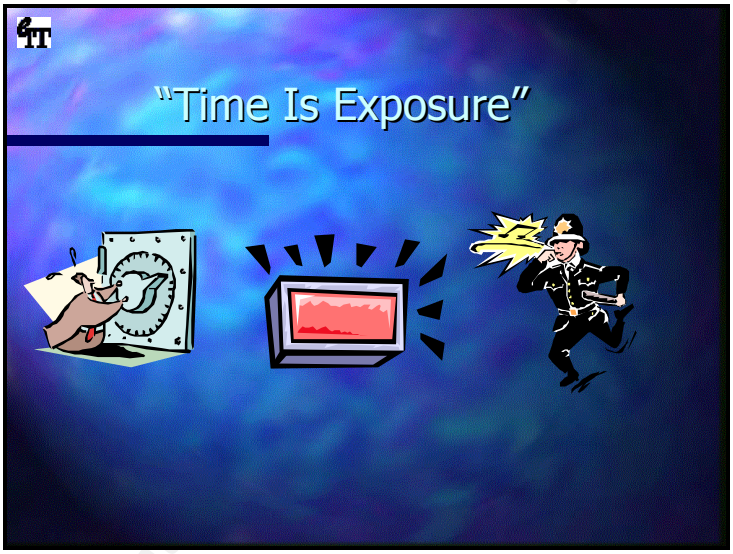
Our organizations cannot solve Information Protection problems by just adding technology and ignoring the fact that we are not monitoring for

© SANS Institute 2000 - 2005 Author retains full rights.

security incidents. Additional technology adds complexity and room for misconfiguration. Much of Information Protection is attained through a combined effort of Policy, Process and Technology that provides Protection, Detection and Reactionary measures.

In order to measure the effectiveness of Information Protection, a common variable needed to be identified. It is has been stated that most human endeavors can be effectively measured in time. Time is the constant element throughout life and is no different in the "Cyber world."

In the financial world the phrase "Time is Money" seems to be similar for Information Protection, "Time is Exposure." To exemplify the Protection, Detection, and Reaction Formula we can look to the Bank Security Model…



All banks today have some type of vault that contains the bank's primary asset, money. This vault is usually a mirror-finish stainless-steel door that is twelve feet high, eight feet wide, three feet thick, and weighs approximately forty-two tons. Massive eighteen-inch-thick deadbolts lock the door into the concrete and steel reinforced walls that surround the vault on six sides. If the door is closed and locked, is the vault secure?

After some consideration it can be said that a very determined thief could potentially penetrate the vault. The point is that banks have taken additional security precautions by installing an alarm and arranging for either the police or an onsite security guard to handle the security event. Without alarms and security guards, banks would have no idea they were being robbed.

© SANS Institute 2000 - 2005 Author retains full rights.

"What?" and "Why?" Intrusion Detection Systems

Intrusion Detection Systems are the "Alarms" on a computer network. The software "alarm sounds" when computers and networks are used in an unauthorized fashion. They are, simply put, a form of network surveillance.

Intrusion Detection Systems perform identification of anomalies in network traffic and host based events. This is accomplished by reviewing data packets and/or host audit logs to recognize actual or potential attacks. Intrusion Detection Systems facilitate the ability for immediate response to a security event just like the bank's alarm system.

Intrusion Detection Systems are a cost effective method of monitoring computer networks for attacks rather than hiring and training personnel for each log. Automating the monitoring and analysis of audit logs is a logical approach that provides a consistent amount of accuracy. This is ever more important as companies are building networks of more complexity.

These networks are also the open doors to hackers along with the business partners and suppliers. Like mentioned before, networks must be symmetrical in nature, but today's traditional security tools don't cover the "big picture." That's where Intrusion Detection Systems come in. Open networks require these necessary "alarms" because they are more susceptible to attacks.

Conclusion

Our organizations cannot solve Information Protection problems by just adding technology and ignoring the fact that we are not monitoring for security incidents. Additional technology adds complexity and room for misconfiguration. Much of Information Protection is attained through a combined effort of Policy, Process and Technology that provides Protection, Detection and Reactionary measures.

As business requirements drive IT initiatives to take advantage of Internet-based standards and extend their services and networks, we as Security Specialists should be there to install our alarms. Intrusion Detection Systems are those "Alarms" on a computer network. The Automation of monitoring and analysis of audit logs is a great step to provide a consistent amount of accuracy and coverage not manually possible. This

© SANS Institute 2000 - 2005 Author retains full rights.

is ever more important today as companies are building networks of more complexity that span the globe.

References:

Schwartau, Winn. “Solving ‘Dumb Days’ with Security Visualization.” 2000. URL: http://www.esecurityinc.com/productcorporateliterature/whitepapers/winn.pdf

Spitzner, Lance. “Know Your Enemy.” July, 21 2000. URL: http://www.enteract.com/~lspitz/enemy.html

Spitzner, Lance. “Know Your Enemy: II .” July, 7 2000. URL: http://www.enteract.com/~lspitz/enemy2.html

Spitzner, Lance. “Know Your Enemy: III.” March, 27 2000. URL: http://www.enteract.com/~lspitz/enemy3.html

Perrine, Tom. “Security as Infrastructure.” Dec 11, 1998. URL: http://www.sdsc.edu/~tep/Presentations/1998.LISA.Security.Infrastructure/index.htm

The SANS Institute. “Essential Security Actions: Step By Step.” 1999. URL: http://www.sans.org/newlook/resources/esa.htm

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.