K-12 Security Assessment Pilot Program

Overall Findings and Recommendations

Prepared by:
Matthew Jonkman, CISSP
September 30, 2003

Table of Contents

Scope

This report is a compilation of five complete security assessments performed by Infotex on behalf of Purdue's CERIAS. These tests were undertaken to assess the security and controls in place in a sample of Indiana school corporations. This step was taken because the mainstream sources of data and statistics regarding security exposures, expenditures, risks, and challenges faced are based solely on corporations and businesses with very different sets of resources and goals. The public education system receives limited grants and discounts to provide equipment and Internet connections, but very little in the way of staffing and training assistance. This study is designed to assess the state of network and information security and the controls in place to maintain and protect our students and their personal information.

These tests were performed using industry-standard methods and tools. The focus of these assessments is to determine the external and internal exposure and penetrability of the school networks. This is accomplished by performing testing in two phases.

The first phase is an external information gathering exercise and an external attack. The testing team is only given the name of the school to assess and the range of Internet Addresses (IPs) they are allowed to attack. This identifies any weaknesses in the network perimeter and any extraneous information that should not be available publicly. The response of local staff and their attack detection abilities are measured as well to determine their ability to respond to a real attack.

The second phase is a full-scale internal network assessment. All servers and workstations on the network are attacked and assessed for vulnerabilities and misconfiguration. Security devices are tested and relationships and traffic on the network are assessed and understood by the testing team to build a picture of the network and its architecture.

The range of IT and security experience and knowledge among the IT staff members tested was widely varied, providing a good representative set of results. One school has an IT staff that is very experienced and active in the networking and security community, yet was compromised relatively easily via oversight related issues. Several others had very inexperienced administrators and yielded very similar results.

Executive Summary

The overall results of this testing process are concerning. Every network assessed was exploitable from the Internet. Two of the five schools tested were penetrated from the Internet, the remaining three had vulnerabilities that would have caused irreparable damage to systems if they were exploited and thus were not attempted. The testing team was able to easily obtain a complete list of all students and staff and some sensitive (FERPA protected) information from three of the five schools from the Internet, and from all schools once on the internal network. CIPA measures in place to prevent students from accessing inappropriate material could be easily circumvented in all of the schools using basic tools or techniques well within the grasp of the average student. Payroll and grade processing systems were relatively easily penetrated in four of five schools, although not actually penetrated due to their sensitive nature. The testing team's attacks and compromises were not detected by any school IT staff without intentional disclosure where emergency changes were requested to protect the school's systems from immediate threats.

Holding the schools to the standards and industry norms present in the commercial security world, none of these networks would receive a positive rating or even passing grade. The primary recommendations of this report are related to process controls and checks and balances. In mainstream security best-practices every security project and network is subject to internal review and assessment as well as third-party assessment. Many of the security vulnerabilities that become problems are the result of oversight or lack of information and are a very natural and unavoidable part of any network's evolution. The process controls and regular assessments are in place to catch and correct these issues before they are exploited internally or externally. Peer review of network design and architecture as well as

security devices and their configuration are invaluable tools in the security process.

The testing team feels that, based on the results of these tests and the makeup of the networks assessed, it is valid to apply the same techniques and methods to schools as in other areas and markets of security. The school networks are relied upon in the same way commercial networks are, they hold the same critical data, and are used by similar numbers of users and varieties of systems. They have the same exploitable resources available and face the same risks as do their commercial counterparts. It is therefore logical to apply the same tested and mature processes and controls to achieve the same levels of security, reliability, and confidentiality. This includes implementing proactive intrusion detection systems, regular third-party assessments, training to facilitate internal self-assessments, and outside assistance in network design, technology selection and deployment. The data being protected on these networks is among the most valuable in our collective information landscape, and should be secured with the same vigor.

Method

NMAP, Nessus, LANGuard, Legion, SuperScan, L0ftcrack, and many other tools and techniques were used to attack the school's external networks. These tools are the same as used by 'hackers' as well as the casual vandal or curious insider. Our methods are designed to assess the vulnerability of the school from the Internet as well as from internal users or network accidents. The overall goal of this process is an assessment of not only the penetrability of the network, but the stability and internal controls in place to maintain this posture.

Internal scans were performed through the use of a system placed on the internal network in coordination with the IT staff. This system then gave access to the testing team after hours to perform network scans and attacks, while minimizing impact on staff and resources.

All of the issues discovered in these tests were rated with two scores by the testing team. The first score is a rating of the risk to the organization. This is a number from one to ten, with ten being the highest risk. This is primarily based on the security community's ratings of the vulnerability or severity with a subjective portion reflecting the system's value to the organization, or the resultant new exposures that may result after a compromise of that host.

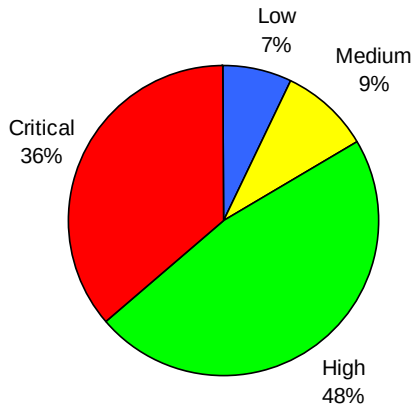
The second rating is the Effort Factor. This is a more subjective reflection of the expected resources required to remedy the issue. This is based on any of a combination of several areas that could be impacted. Included in this consideration are potential financial impacts, man-hours to be expended or political/policy changes required within the organization. This rating is also a one to ten scale with ten being very difficult, one requiring little to no resources to remedy.

These two factors are then used in a calculation to provide the rank for the issue. The Vulnerability Matrix prepared for each school is ordered by rank, highest to lowest. The calculation to provide the rank takes the severity of the issue into account exponentially higher than the resources required to remedy, thus providing a list of the highest risk and least effort to remedy issues moving toward least risk and more difficult to remedy. Generally, an organization can make a great impact to their overall security by addressing the top 20-30% of these issues. The remaining issues can then be organized and well planned to provide a long-term improvement in security. The Vulnerability Matrix itself functions as a very effective project management tool. A representative set of the issues detected in all schools have been stripped of identifying features and combined into a single Vulnerability Matrix distributed with this report.

Results

The following charts show two different data sets used to rate Security Assessments. These are created directly from the Vulnerability Matrices from all five tests. The intent of these metrics is to show the change over time and to compare to commercial organizations.

Priority Distribution

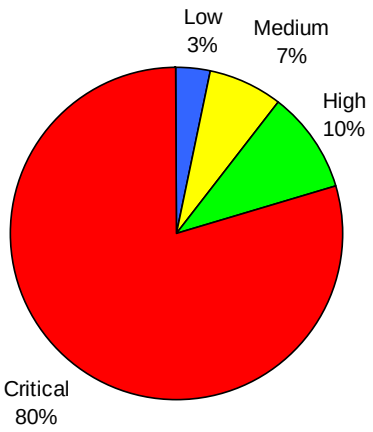


Risk Severity Distribution is the raw Risk Severity of each identified issue scored in four quadrants. This is on a scale of one to ten, with ten representing a direct compromise risk and a one representing an informative issue with little threat. This chart shows a vast majority of Critical Issues. An average network in general has an even spread of risk issues detected, with the better scored networks leaning more toward all low risk issues.

The average Risk Severity rating is 8.03 out of 10. This is significantly higher than normal. An average rating would be in the 4 or 5 range, 7 being a network in very bad shape, 2 to 3 being ideal. Over time the Average Risk Rating should decrease as more security controls and more regular assessments are employed.

The Priority Distribution is a simple ratio of the Risk Severity rating as listed in Figure 1 as related to the Effort and Resource factor required to fix the problem. This set of numbers provides the "low hanging fruit" scale for remediation. The largest portion of issues is in the High category, indicating that these are not of a critical risk and should lead to a relatively fast remediation process. The goal of an ongoing security program should be to get the majority of issues into the Low and Medium categories.

Risk Severity Distribution



The Resource average for all the issues is 1.86 out of 10. This indicates that the majority of issues will be relatively easy to fix and require little or no new funding or equipment.

Overall Recommendations

The recommendations made to all five schools were relatively similar. These have been compiled and generalized to be applicable to the majority of school systems. These are presented in no particular order.

1. Network DMZs
In general, servers that are intended to be exposed to the Internet for general public access (web servers, mail servers, dns servers, etc) are housed in a DMZ'd portion of the network. This area is protected and controlled by a firewall, but does not have unrestricted access to any internal networks, nor does the Internet have unrestricted access to the DMZ. This is easily accomplished by using extra network interfaces present in most firewalls encountered, or using VLANs in existing equipment. This network architecture design protects servers that must be exposed from being attackable on ports or services that are not intended for general public access.

2. Wireless Networks
Wireless Networks are in use in three of the five school corporations. Two of the three were penetrable using easily obtainable software and commercial wireless cards and antennas. These wireless links should be secured using MAC address controls and internal VPN's to augment the standard but breakable WEP encryption in use. This is often easily done using existing routers or firewalls to build point to point VPN tunnels, and has little to no impact on network speed or reliability.

3. Patch Management

A key process that must be in place in any network is the ability to recognize in a timely manner new vulnerabilities that will affect any system on the network. The organization must then have an effective plan in place to detect and locate affected systems and then remediate these vulnerabilities. Recent rounds of worms and viruses have shown clearly that this plan must be able to be executed within 24 hours of vulnerability detection and publication. During testing every school had systems that were vulnerable to exploits that were very commonly known and more than a month old, some having issues that had been public knowledge for more than a year. Several worm infected systems were found and cleaned eliminating mysterious network instabilities. To improve this process the testing team recommends some form of unified vulnerability alerting system, similar to Purdue CERIAS's Cassandra (http://cassandra.cerias.purdue.edu) and mandatory enrollment in alerting. Every school corporation must have a responsible person and backup to develop a response plan to evaluate these reports and assess their impact. An effective plan must be in place and practiced to perform detection and remediation.

4. Administrative Networks/Overall Architecture
The testing team found that many of the networks assessed mixed administrative (or Trusted) traffic with student and lab (or Semi-Trusted) traffic on the network. This allows internal students direct access to administrative systems such as payroll, grade management, web servers, etc. Security best-practices would deem that administrative traffic should be contained in a logically separated network with strict rules to control traffic from semi-trusted areas of the network. This prevents idle tampering and probing of critical systems, possibly protecting a system until patches can be applied and preventing sensitive traffic from being intercepted in the clear. These types of separations can generally be very easily accomplished using existing routers and security devices by simply utilizing the full feature set of these devices. These types of changes also provide a more stable network that is more easily monitored and troubleshot.

5. Policies
The key of any security program in any organization is policy. Technology is implemented to facilitate and enforce the policies set by the organization. Most of the schools had very weak or no computing policies. The issues that should be addressed are password complexity requirements, acceptable Internet use, acceptable resource use, etc. The full range of policies found in commercial organizations should be in place in every school corporation.

6. CIPA Enforcement
While all of the schools had some form of web content filtering, none had effectively addressed methods that are available to circumvent these controls relatively easily. CIPA also states that the school is responsible for ensuring that students are not able to attack other systems from school resources, or be at significant risk of attack while using school resources. There were no detectable measures in place to address this risk, or the web filter circumvention in any school.

7. Proactive Security Controls
One of the most important elements of a network security policy is instituting some form of proactive incident detection method. This can be something as simple as a log correlation system, or something as effective as Network Intrusion Detection Sensors (NIDS). An IDS or NIDS can alert the staff instantly to external attacks, internal users circumventing CIPA controls, internal users probing or attacking administrative systems, or everyday issues such as imminent network failures. These types of technologies are free or low cost, very mature and effective, simple to deploy, and provide an invaluable view into a network. The testing team recommends that some form or IDS or NIDS be implemented by or made available to every school corporation.

8. Internal Assessment
More in-depth and mandatory training should be provided for school corporation IT staff. A focus on security awareness and the tools available to perform self-assessments would make a great difference in network security postures and scores. There are a great number of free tools that are very mature and produce easily understood results. Corporations should require internal staff to perform these tests on a regular basis and report their results and action plans to remediate on a regular basis.

9. Third-Party Assessment
A key element of any security plan is outside expert review. Corporations commission regular security reviews on a very regular basis. Several industries are regulated to require this at certain intervals, while most perform these voluntarily. The testing team feels that a yearly third-party assessment followed-up by at least quarterly self-assessments would be a very effective control to maintain and measure the security posture of school networks. Standards should be agreed upon by state-wide organizations as to the scope of these tests and the requirements for the parties performing these tests.

Conclusion

While this is a very grim report, the majority of the issues raised can be relatively quickly remedied on a large scale by implementing global policies requiring security assessment, and providing local staff the education and authority to make the necessary changes to their networks and processes.

These controls and processes are very well defined in the industry and freely available. None of the issues to be addressed require untested or immature technology and processes, and very few require significant funding.

For More Information

To learn more about the school vulnerability tests and other CERIAS school security initiatives, visit the CERIAS website at:

http://www.cerias.purdue.edu/k-12/

or contact:

Melissa Dark, Assistant Director

CERIAS, Purdue University
646 Oval Drive
West Lafayette, IN 47907

dark@cerias.purdue.edu