R·I·T

Institute Audit, Compliance & Advisement Newsletter

the Quaestor Quarterly

Volume 4, Issue 3 Fall 2009

quaes·tor [kwes'tôr] 'one who asks questions'

IACA's Mission

Institute Audit, Compliance & Advisement promotes a strong internal control environment by objectively and independently assessing risks and controls; evaluating business processes for efficiency, effectiveness, and compliance; providing management advisory services; and offering training to the University community. We focus on preserving the resources of the University for use by our students as they prepare for successful careers in a global society.

Inside This Issue **page**

Internal Controls Training Sessions	2
Fraud in the Workplace Training Sessions	3
Word on the Street	4
RIT Ethics Hotline	4
Control of the Quarter	5
Ask the Auditor	6
Pop Quiz	6

IACA Institute Audit, Compliance & Advisement

Websites Here, Websites There, Websites Everywhere…, but are they secure?

We know that websites are a wonderful communication tool; they not only let us spread information to coworkers and students in seconds, but also to the whole World Wide Web. However, just as much as they let us send information out to the world, they also open a window from the world into our network. There are risks associated with this free flow of information.

If you have been watching the news in the past few years, you have probably heard about many successful attacks on organizations via their websites. Cybercriminals are no longer the average teenager without anything else to do; they have evolved into organized criminals looking for information that they can quickly sell on the black market, such as credit card or social security numbers. There is financial gain now associated with hacking into organizations' websites.

This has resulted in cybercrime becoming more sophisticated than before. We now live in a time of "zero day" attacks, which means that hackers are coming up with exploits to applications so fast that there is a significant number of applications that have vulnerabilities of which developers are not yet aware, but that hackers are already exploiting.

For known vulnerabilities, application developers are now being more proactive in issuing patches to their applications as soon as they know about the vulnerabilities. However, this also results in having information regarding the vulnerabilities of most applications readily available on-line. Nowadays leaving systems unpatched is leaving an open door for an attack, since it would be a lot easier for hackers to exploit known vulnerabilities than to try to discover new vulnerabilities on their own. In his keynote address to attendees of the 2008 Hackerfest conference, Paul Henry, founder and CEO of Forensics & Recovery LLC and SANS Certified Instructor, stated that 90% of attacks exploit known vulnerabilities for which a patch already exists.

Although there are many areas to discuss when it comes to protecting our network and our information from cybercrime, this article will concentrate on websites. Here at RIT, the most common incident category for which the Information Security Office has to attend deals with website attacks. In addition, the SANS Institute ranked web application security exploits number eight in their 2008 list of "Top Ten Cyber Security Menaces." Web security vendor ScanSafe states in their 2008 Annual Global Threat Report:

"In 2008, the Web was indisputably established as the preferred platform for malware distribution, with the majority of distribution occurring through mass compromise of legitimate websites. The sheer number of impacted websites is immeasurable, but certainly it is conservative to say that the number exceeds hundreds of thousands and is more likely in the millions."

ScanSafe as well as OWASP, the Open Web Application Security Project, agree on naming *vulnerable code* as the main source of website vulnerabilities, with SQL injection and Cross-Site Scripting (XSS) as the most popular attack techniques.

continued on p. 2

Websites Here, Websites There, Websites Everywhere…, but are they secure?

(continued from p. 1)

These attacks allow the perpetrators to run their own code in the compromised computer, which could lead to the following problems:

- Private and confidential information disclosure
- Installation of malware on legitimate websites
- Defacement of the website whereby it may be used for advertising of prescription drugs or various illegal activities
- Turning the compromised computer into a "bot," which means that it is now under the complete control of the individual who attacked it, who would have the same rights in the network as the compromised computer, and who can use it to conduct other attacks, including installing malware in other computers in the local network
- Address Resolution Protocol (ARP) spoofing that could result in a denial of service attack, which renders the compromised systems unavailable
- Alteration of data in databases, compromising data integrity
- Stealing the compromised computer's cookies for session hijacking, allowing the perpetrator to pose as the compromised machine on a user web application session

Websites that are susceptible to these types of attacks are those that have forms to be filled in by site visitors and those that have a database application in the background.

So, what can you do to defend your website from these attacks? Start by considering the use of RIT web resources for your website. These resources include RIT's Online Learning's *Confluence* wiki and *people.rit.edu*. These resources are supported by professional web and system administrators, who are familiar and experienced with systems security.

If you are unable to use RIT resources and need to develop a web application on your own, your application's source code would be the first line of defense against intruders.
Some steps you could take to secure your code are the following:

- Familiarize yourself with the web development application (e.g., ASP.NET, PHP, Perl) that you use. It is extremely important that you are comfortable and familiar with your web development application in order to know how to avoid common coding pitfalls. Some ways to familiarize yourself with your web application are obtaining the necessary training, reading on-line resources, and sharing information with your peers.
- Conduct code reviews. The sophistication and abundance of attacks are such that many times a vulnerability cannot be detected by a scanner or by conducting penetration testing. The best defense is looking at the code. Establish a quality control process for your web applications that involves using your peers to review your code. OWASP offers a free "Code Review Guide" on their website that can be used as a starting point for a code review process. It can be found at https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf. According to this guide *"…Despite the many claims that code review is too expensive or time consuming, there is no question that it is the fastest and most accurate way to find and diagnose many security problems. There are also dozens of serious security problems that simply can't be found any other way."*
- Validate and sanitize user input before executing it. In addition, avoid displaying user input, and, if this cannot be avoided, validate and sanitize it before displaying it.
- Customize your error messages. Avoid giving away information such as whether a username is correct, what web application is being used, and the version number of the web application in use.
- If your website is a blog, wiki, forum, or other similar application, review the content of postings by others. Postings could have malicious content that you will need to stop before they cause any damage. Also, require user authentication for any postings.

continued on p. 3

Ensure that your department has established and is maintaining good internal controls.

To learn more about internal controls, sign up for Internal Controls Training.

Upcoming sessions:

January 12, 2010
9:00 am - 11:00 am
Location: CIMS 2140

April 27, 2010
9:00 am - 11:00 am
Location: CIMS 2140

July 27, 2010
9:00 am - 11:00 am
Location: CIMS 2140

Sign up at the CPD website https://finweb.rit.edu/cpd/leadership/cares.html

Websites Here, Websites There, Websites Everywhere…, but are they secure?

(continued from p. 2)

Some steps you could take to secure your code are the following (continued):

- Connect to databases with the minimum required privileges. Never connect users as superusers or database owners.
- Eliminate typical test user name and password combinations (test/test, admin/admin, guest/guest) before a website is put into production.
- Do not store credit card numbers in your web server. The payment card industry has strict technical standards for systems that process credit card data. Vendors that take credit card numbers, even if only temporarily, need to comply with this standard. To address this issue, RIT utilizes a third party vendor for credit card processing through the use of an e-commerce web application. For further information regarding this e-commerce application, contact the Student Financial Services office.
- Do not post RIT private and/or confidential information on websites that can be accessed by the general public.
- Test your web application in a secure environment. Isolate the server from the outside world when the web application is under development and only allow minimal access when an outside world connection is needed for testing. Remember not to use actual/real data for testing; create your own test data.
- Stay current with your web development application patches as well as with the OS patches of your web server.
- Utilize RIT's Information Security Office (ISO) quarterly web server vulnerability scan reports. Contact your system administrator to request the results of the scan for your web server.
- Comply with the RIT Information Security Standards. RIT web servers are required to comply with the relevant Standards issued by the ISO. To determine the Standards with which your server needs to comply, please go to http://security.rit.edu/standards/index.html.
- Harden the security of your web server. If your web application grants it, do not just implement the level of security that is required by ISO Standards, go beyond. ISO Standards are produced for the whole Institute and, as such, have to remain at a level that is reasonable for all RIT systems. However, if your web application requires increased security, or if you are passing RIT credentials within your application, go the extra mile and make your server even more secure. The Payment Card Industry Data Security Standard (PCI DSS) – the standard mentioned above that is required by the payment card industry from vendors who process credit card data – is one of the most comprehensive and detailed technical standards currently available and can be used as a guide to what constitutes strong security for a web server. It can be found at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml. In addition, the ISO performs security reviews upon request. Their security report will provide you with suggestions and advice to improve security in your environment. Contact Infosec@rit.edu to request a security review.
- Subscribe to the ITSTech mailing list to stay informed regarding the latest security issues affecting your web server and applications, RIT policies and procedures regarding web development and IT services, and many other areas of interest for web developers.
- Report any incidents with your website to the ISO.

Finally, we would like to direct you to a great resource for web developers. It is OWASP's "Guide to Building Secure Web Applications and Web Services." It is available for free at http://www.owasp.org/index.php/Category:OWASP_Guide_Project.

~~ by Elisa Cockburn, Sr. Internal Auditor, Institute Audit, Compliance, & Advisement
written with the help of Paul Lepkowski, Lead Engineer, Information Security Office
and Ben Woelk, Communications and Training Specialist, Information Security Office

Occupational fraud can be found in any workplace. Whether an organization is a non-profit entity such as a university or a large for-profit corporation, fraud has occurred and continues to occur.

To learn more about occupational fraud, sign up for Fraud in the Workplace Training.

Upcoming Sessions:

February 2, 2010
9:00 am - 11:00 am
Location: CIMS 2140

April 13, 2010
9:00 am - 11:00 am
Location: CIMS 2120

July 13, 2010
9:00 am - 11:00 am
Location: CIMS 2140

Sign up at the CPD website https://finweb.rit.edu/cpd/leadership/fraud.html

Word on the Street

In general, an audit is a methodical formal examination or review of a condition or situation. How can something sounding so benign render administrators, managers, and executives sleepless at night? It is probably not the fact that an audit is looming in the immediate future, but the fear that some unforeseeable thing will be found and appear in the audit report.

This reflected the reaction of the Information Technology Department (IT) and the Networking, Security, and Systems Administration Department (NSSA), both which reside within the Golisano College of Computing and Information Sciences (GCCIS), when the Institute Audit, Compliance & Advisement (IACA) group announced that they were conducting a computer security audit on the IT and NSSA computing environment. A computer security audit is like any other audit except it is an examination of security policies and processes and their implementation. It includes interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems and is generally viewed by many of the attention recipients as an invasion of their space. The audit concentrated on the methods established to protect private information (PI). Auditing private information on computer systems has the same standards as any other type of auditing and invokes the same paranoia. Please see (http://security.rit.edu/Pim.html) for the RIT description of PI.

It would not be accurate to state that the departments awaited the audit with bated breath, but it is safe to say the anxiety level was somewhat increased. The implementation of the process did not lower the level of anxiety, but the professionalism of the auditing staff certainly helped. Due to the size of the combined departments it was estimated that completion of the entire process would take several months. During this time, the audit team was very cooperative and patient. They understood that the audit is not the primary focus of the system administrators and were flexible on deadlines when job responsibilities needed to come first. The audit was actually much less intrusive than was anticipated and the entire process was actually not unpleasant and was quite helpful.

Organizations frequently get caught up in their day-to-day operations and do not take the time to reflect about current processes. This audit forced the departments to examine the policies, procedures, and practices in place, reinforced what was being done well, and provided direction on the changes needed to comply with RIT policy. A reasonable timeline for the completion of the needed changes was developed, accepted by the auditing staff, and scheduled for implementation by the system administrators in the departments.

So in the end, the "dreaded audit" was actually not an unpleasant experience even though it did result in a lot of work and time expended. Were violations found? Yes, and we have been working on our corrective action plans, all of which will be reviewed by IACA. This effort also resulted in some additional rewards. The policies and procedures of the departments were updated and new configurations of the devices were implemented; and there is the self-satisfaction that effort expended has the computing environment more secure.

In fact, we used the audit information to provide a training session for the other GCCIS departments. The goal was to familiarize the managers and staff with the audit process, to share the issues that were found, and to insure compliance with RIT's policies and procedures. The departments will use this information to enhance their operations.

It is a relief that the audit is completed and that it was not an unpleasant experience due in large part to the professionalism exhibited by the auditing staff. Elisa Cockburn and Steve Morse of IACA and Paul Lepkowski of the Information Security Office are commended for the non-intrusive and non-threatening manner in which they accomplished their task.

Contributed by Luther Troell, Director, School of Informatics, GCCIS
Pamela Venuti, Assistant Director, Technical Services, GCCIS
Kimeley Shearer, Director of Operations, GCCIS

What about *ethics* in the workplace?

To learn more about RIT's Code of Conduct and the Ethics Hotline, check out
http://finweb.rit.edu/svp/ethics/

Control of the Quarter

Internal Control over Procurement

Over the course of several Quaestor Quarterly Newsletters, we discussed the five interrelated components of internal control including:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

After reviewing each component of internal control as well as who is responsible for maintaining and monitoring the system, we've provided examples of how internal control is built into the University's infrastructure as a fundamental part of our operation. In the last issue we discussed control activities in place to ensure compliance with governing requirements. In this issue, we'll discuss controls over the procurement process.

In fiscal year 2009, RIT departments expended over $200 million on the procurement of goods and services in support of the University's mission. This level of activity requires numerous control activities to be in place throughout the organization, occurring at all levels and in all functions. Control activities over the procurement process comprise a wide and diverse range of activities such as:

- Approvals
- Verification
- Segregation of duties

Approvals – All requisitions for goods and services require the approval of the appropriate budget authority who is authorized to act on behalf of the University. When the order amount exceeds the dollar limit set up in the purchasing system for the approver, the requisition is automatically directed to the next person in the hierarchy. This automated control activity ensures that only authorized individuals are able to commit funds of the University up to the limit of their authority.

Verification – Once a requisition is approved by the appropriate individual(s), staff in the Purchasing Department verify that orders of $5,000 or more are accompanied by three competitive price quotes. This control activity is designed to ensure that: 1) RIT is receiving the best value for the funds expended; 2) the goods and services are being purchased from a qualified and/or preferred supplier; and, 3) the purchase is in compliance with requirements set forth by external funding agencies.

Segregation of Duties – When goods are delivered, the order must be "received" in the purchasing / accounts payable systems by staff in Central Receiving; a supplier invoice cannot be paid until it is "received." This control activity ensures that someone other than the department that placed the order verifies that the goods have been received.

The information above reflects three examples of control activities over the procurement function; there are many more, each designed to ensure that necessary actions are taken in order for management directives addressing specific risks are carried out.

In the next Quaestor Quarterly Newsletter, we'll review examples of monitoring activities that have been put in place to assess the design and operation of controls, ensuring that the various components are operating effectively.

Contributed by Lyn Kelly, Controller & Assistant Treasurer

Did You Know?

Recent national rates of initial detection methods of occupational fraud were:

46.2 % ~ Tip

23.3% ~ Internal Controls

20.0% ~ By Accident

19.4% ~ Internal Audit

9.1% ~ External Audit

3.2% ~ Notified by Police

The sum of percentages exceeds 100% because in some cases respondents identified more than one detection method.

Source: Association of Certified Fraud Examiners *2008 Report to the Nation on Occupational Fraud and Abuse*

Ask the Auditor ~

Submit a question to the IACA webpage **http://finweb.rit.edu/iaca/forms/ask/** by December 18, 2009. If your question is chosen for publication in our newsletter, you will receive a prize valued at $15.

IACA TEAM:

Steven M. Morse '86, CPA
assistant vice president
475-7943

Patrick M. Didas '90, CPA, CFE
associate director
475-6826

Wendy J. Roy, CPA
senior internal auditor
475-7011

Nancy A. Nasca, CPA
senior internal auditor
475-5293

Elisa M. Cockburn, CPA
senior internal auditor
475-7849

Christine M. VanHemel
staff & audit assistant
475-7647

Daniel R. Dellaquila
co-op student internal auditor
475-4318

R·I·T

Ask the Auditor

Question: What is the authority of Institute Audit, Compliance & Advisement (IACA)?

Answer: The scope of internal audit coverage is enterprise-wide and no function, activity, or unit of the University is exempt from audit and review.

IACA is authorized by charter (http://finweb.rit.edu/iaca/aboutus/charters.html) from the Board of Trustees to:

- Have unrestricted access to all university functions, records, property, and personnel.
- Have full and free access to the Audit Committee of the Board of Trustees.
- Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives.
- Obtain the necessary assistance of personnel in units of the organization where they perform audits, as well as other specialized services from within or outside the organization.

IACA is not authorized to:

- Perform any operational duties for the organization or its affiliates.
- Initiate or approve accounting transactions external to the internal auditing department.
- Direct the activities of any organization employee not employed by the internal auditing department, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors.

Note: IACA follows the *International Standards for the Professional Practice of Internal Auditing* of The Institute of Internal Auditors.

Pop Quiz Challenge

Take the Pop Quiz Challenge! Correctly answer the question below and you will be entered in a drawing to win a prize worth $10. One lucky winner will be chosen randomly and notified by email.

Question: The greatest deterrence to fraudulent conduct is:

A. Controller's Office policies and procedures
B. The perception that the illegal act will be detected
C. Nosy co-workers
D. Inquisitive Auditors
E. The morals of the employees

See our Quiz webpage to post your answer:
https://finweb.rit.edu/iaca/forms/quiz/

The winner's name and answer will be included in the Winter '10 Quaestor Quarterly Newsletter.

****