

Canaudit Perspective

September 2008
Volume 9, Issue 1

TOPICS OF INTEREST:

- The security function is ineffective in some organizations
- Intrusion detection and prevention may not be effective
- Monitoring services work best when properly configured
- Incident response procedures may not be effective
- The hacker may be sitting beside you
- Conclusion

HACKERS DO NOT TAKE VACATIONS



I have become very disturbed after attending several audit and security conferences over the summer. It seems that the profession has slowed down their efforts over this vacation period, June through the end of August. In many of my conversations and discussions, it was mentioned that staff shortages due to vacations are causing

businesses to postpone security discovery and remediation efforts and IT audits until after Labor Day. This information has been confirmed by our project bookings. Our bookings have now taken off since the Labor Day holiday as people rush to complete their audit and security work by year end. For many of us, year end is the deadline for meeting our performance objectives and earning our bonuses. As a result, everyone is now redoubling their efforts to complete their assignments by the end of their performance year.

Well, here is some news: Hackers did not take a vacation over the summer. In fact, it appears that they were working overtime. You just have to take a short Internet visit to the Attrition.org Data Loss Archive and Database (<http://attrition.org/dataloss/dataloss.csv>) to see the activity over the summer. For the purposes of this article, I excluded items like lost laptops and lost or stolen media (backup tapes), etc. and focused solely on web or hacking incidents. The total number of reported lost identities in these categories was 2,513,317. This was just over the summer months. Let me emphasize that these are only the reported incidents. If an organization lacks effective intrusion detection, they will not notice the

breach until after their customers are scammed, resulting in the authorities tracking the loss of confidential information back to a specific organization.

Thank goodness for the FBI and the local commercial crime divisions of our police forces! Without them, we would not know of many of the breaches due to the failure to implement effective incident prevention, detection and investigation procedures. The rest of this article will provide you with my opinions on the reasons many organizations are not effectively secured. Just today, September 15, 2008, a new announcement was published at Consumerist.com that demonstrates the efforts our law enforcement agencies are making:

Forever21 announced Friday that the Secret Service found criminals had illegally accessed 98,930 credit and debit card numbers from store customers.

See the full article at <http://consumerist.com/5050173/98930-affected-in-forever-21-data-breach>

It must have been a surprise for Forever21 management to find out from the Secret Service that they had a control breach!

THE SECURITY FUNCTION IS INEFFECTIVE IN SOME ORGANIZATIONS

One of my pet peeves is that many IT security functions focus on policies and procedures. They do an excellent job of creating new policies and procedures and updating existing ones. My concern is that policies and procedures alone do not protect our information infrastructure, software and data. While

they are certainly required, we need more enforcement of the policies and procedures. We also need mechanisms to detect incidents and determine if the installed security products are working properly. When we do our first remediation test for a client after an IT Security Baseline or Network Penetration Audit, management is often shocked to find that items reported as corrected are, in fact, not remediated. This is usually caused by a failure to communicate up and down the command structure. When we ask the people on the bottom of the structure, they usually **tell us the way things actually are** - in need of a significant security enhancement. When we ask people in the middle of the structure, they **tell us how they believe things are**. The difference is the filtering that goes on as information moves up the chain of command.

Let me be frank. The CEO and other senior executives want to have a secure environment. The people on the bottom know the environment is not secure. The people between the two groups want to please their superiors and put a favorable spin on the issues. The "Serious items that are not remediated" become "Audit items that are under control" or "We are handling the issues". This is a natural tendency as middle management is often isolated from the lower level staff. As a result, the actual situation is distorted as it climbs the command and control structure. Needless to say, when our test results are reported to executive management, there is an outcry as the executives believe that they were deceived. Once the heat of the moment has passed, middle management learns to check their facts before they commit a second and possibly career-limiting misstatement. Executive management now asks for proof of remediation, usually independent verification from an external party or the internal audit department.

This leads me to another critical missing element in many IT security functions. It is what I call a "sweep team". In most small to medium-sized organizations there should be one or two sweepers who conduct regular scans of the network. In larger organizations, additional sweepers may be required. The sweepers' task is to constantly scan the network looking for poorly secured machines and databases. We have assisted several clients by providing the tools and training necessary to identify flaws and correct them before a hacker or disgruntled insider can take advantage of the weakness. We believe that the sweepers should be part of the IT Security group to ensure that they are independent of normal operations. The sweepers' task is to identify issues and turn them over to IT to fix. They then retest to ensure that the issues have been remediated. It is essential that each security group have a team specifically tasked to seek out and identify

weaknesses, report them, and ensure that they are remediated. Once the sweepers are in place, executive management will have greater confidence in the reported remediation results.

INTRUSION DETECTION AND PREVENTION MAY NOT BE EFFECTIVE

An Intrusion Prevention System (IPS) and an Intrusion Detection System (IDS) do not always provide the level of protection required. Also, we have found that some services that monitor networks and web events for security breaches may not be effective. During most of our initial IT Security Baselines and Network Penetration Audits, we have been able to successfully avoid detection. The most common causes are lack of an IPS or IDS or poor configuration of the IPS and IDS. We have also been able to remain below the horizon on remote-monitoring organizations.

Let us look at the common flaws relating to IDS and IPS. In many cases, they are set up to identify the normal precursor to an attack, the network scan. Our project team techniques are designed to avoid detection. If we suspect that there is an IPS in place, we will locate a printer, video conferencing device or an exploitable Voice over IP (VoIP) system. It is a simple matter to obtain these MAC and IP addresses and masquerade one of our machines as any of these systems. If this ploy is successful, it means that the IPS was not properly implemented. It is common to ignore implementing IPS on some of the devices as they generate a large number of false positives. The false positives have the security folks running down false alarms. My response to ignoring troublesome devices is that I would rather send fire trucks out and find the house is not on fire, then to not send the fire trucks out when there is a fire.

Once we gain undetected access to an IPS-protected network or a network running no intrusion detection at all, we avoid scanning the network. The network scan will normally set off alerts or hit an embedded honey pot (a device intended to attract hackers so they can be detected.) Instead we use a command prompt window and issue the net view command as shown below:

```
net view /domain:XYZ or net view
/domain:XYZ.com where XYZ is the
organization's domain name
```

This lists all of the machines in the Active Directory or Domain. Using the IP addresses for these machines, we run a single port scan looking for port 1433, the MS-SQL port. If the IDS or IPS does not flag a single port scan, then we are able to stay under the radar from a detection standpoint. We have several exploits for MS-SQL that can give us local system access,

which is higher than administrator access. The easiest is to test for accounts with default passwords (sa, admin, and probe). Once in, we use the local system access to see the LSA secrets or capture passwords that will help us gain domain administrator rights.

To accomplish the same objective another way, we set up a single port scan of port 1521, the Oracle Listener port. This locates the Oracle databases running in the Windows environment. Once this is done, we use the Canaudit Oracle Scanner to connect to the listener port, download relevant information, and identify DBA-like accounts that have default passwords. Once we have this access, we can take the Oracle accounts and encrypted hashes, as well as access the database. At this point, hackers would write a query to harvest the confidential information.

These are just two techniques used to gain undetected access to databases. There are similar issues with other databases. We test all of the major databases in our IT Security Baseline or Network Penetration Audits. Needless to say, we normally gain access to many of them.

MONITORING SERVICES WORK BEST WHEN PROPERLY CONFIGURED

Some of our clients use an outside firm to monitor their security. If properly used, these services are great! When a reportable event is detected, emails are sent to the security folks. That said, there are a couple of common flaws that need to be discussed. We have had several incidents with clients where our team was able to avoid detection as we kept below the alert thresholds. Thresholds are usually set to ignore false positives. As a result, with careful use of hacker tools and software, we can remain under the critical thresholds until we reach our objectives and glean confidential information.

Let me explain the types of thresholds. Critical events, such as the creation of a new domain administrator account, generate immediate alerts to the security folks. Next are medium events, which may be reported overnight and sent out to the security staff. It is up to the security staff to determine if any of the events should be investigated. Lastly, there are the low-level alerts. These alerts are tracked, but it is up to the security staff to log on to view these alerts. The monitoring service may also send out weekly reports that summarize the week's events. These reports are usually available online as well.

So, what is my concern? Based on our project testing, we can usually avoid the critical alerts. We have no need to set up an administrator-empowered account when we glean this access by other means. Also, the

medium-level alerts may be sent overnight. This means that the security folks may not see it until they get into work in the morning, or even later. In most cases, we do not generate many medium-level alerts. Those that are generated may be discounted by security as false positives.

In our testing, we do generate thousands of low-level alerts. These clearly show up in the daily or weekly summaries. Someone just has to view the alerts and act upon them. I believe that a better methodology would be to triage the medium and low-level alerts. Let us say that 25 medium-level alerts are generated on a normal day when there are no attacks. I would use this level to trigger a high-level alert. As soon as 25 medium-level alerts are identified, a single high-level alert is flashed to the security staff. If normally there are 50 low-level alerts on a normal day, then I would set this as a threshold for generating a medium-level alert. If 100 low-level alerts are encountered, I would generate a high-level alert. Obviously, my examples are arbitrary. A full analysis should be performed to determine the escalation process for monitoring alerts that fits your organization.

Not monitoring the correct things is another issue. We have had clients who use the monitoring service solely for external Internet threats. Other clients may not take the appropriate level of service for internal threats as they are budget conscious. Well, if you are going to use a professional monitoring service, then you should fund it properly. A visit to the Tech//404® Data Loss Cost Calculator (<http://www.tech-404.com/calculator.html>) will let you quickly determine the cost of an intrusion. I used the loss of 25,000 records in my example, and I found the cost of notifying the victims and providing them with ID theft services was over \$4,000,000. This does not include the cost of litigating the class action lawsuit that is sure to follow. There are numerous examples of class actions you can use. TJX and Certegy Check Services are two recent examples that will give your management an estimate of the litigation costs resulting from breaches. The lesson to be learned here is that if you are going to use a monitoring service, then ensure that you pay for all of the features needed to ensure early detection and alerting of potentially dangerous situations.

INCIDENT RESPONSE PROCEDURES MAY NOT BE EFFECTIVE

Many of our clients have incident response procedures; however, what concerns me is that they do not test them until there is an actual incident. I believe that it is essential to test incident response procedures on a regular surprise basis. The method we prefer is to have the sweeper team perform

random attack simulations approximately once a month from various locations within the network. The security team should have to determine that an attack is underway and invoke the incident response procedure. They should then have to track down the offenders, isolate and then “apprehend” them. The secret to early detection and isolation of a computer incident is repeated drills to ensure that the correct methodology is followed and that each person on the response team understands and is comfortable executing their role.

A key component in incident response is the command center. This is a facility that is available at all times to serve as the headquarters for the investigation of the incident in question. The incident response team should assemble and work from this facility. Remote members of the team should video conference into the center. It is important that video conferencing be available as this creates better synergy amongst the team members. They could also teleconference into the facility if video conferencing is not an option. We suggest that GoToMeeting or some other remote presentation tool be used to enable remote participants to see what is on display or monitor.

THE HACKER MAY BE SITTING BESIDE YOU

I mentioned earlier in this article that hackers do not take vacations. They are diligent in their activities. Often they work together in groups to ensure that they successfully attack multiple targets. These hackers may not be just in the North America. As reported in a recent article in the Boston Globe:

Prosecutors said both men were key players in a loose-knit ring spanning countries from China to Ukraine that stole or trafficked in more than 40 million payment cards in all, causing more than \$400 million in damages.

See the full article at

http://www.boston.com/business/technology/articles/2008/09/12/hacker_pleads_guilty_in_breach/

Hackers are not necessarily invisible people from other countries. They could be your fellow employees, temporary workers, contractors or outsourced IT staff overseas. Hacking incidents do not only originate from the Internet or poorly secured wireless networks. They can originate from the inside of your network or the network of a trusted trading partner.

CONCLUSION

I am very concerned about the effectiveness of IT Security groups. IT Security is far more than policies and procedures. It is more than having a Chief Information Security Officer. Solid IT Security requires a team that sets standards, enforces the standards, and regularly scours the network to identify poorly secured machines, databases and devices. Your IT security group may already be performing the functions I mention in this article. If so, congratulate them with a dinner on the company or a gift card. They certainly have earned the praise. Forward-looking organizations with an effective security team are most likely to avoid the public embarrassment of a compromised network and sensitive information.

If your security group focuses strictly on the policies and procedures, then it is time to rethink the function of this critical group. Several of our clients have needed to reinvent the security function from the top down. I have been pleased to be a part of these efforts at our clients and look forward to working with more organizations to ensure that their IT security effort is well-organized, proactive and well-trained.

The opinions expressed in this article are mine and mine alone. I am always interested in your feedback, both positive and negative. Please send your comments to Gordon@canaudit.com. I will read and ponder each of them and send you a personal response. It is my hope that through open discussion, we can address potential threats, reexamine our practices, and improve our performance. Open dialogue is the beginning of change, and change is certainly required in the security profession.

If you read this far in the article, I would like to reward you for taking time away from your daily challenges to consider the thoughts presented above. If you would like to attend the December 8 – 12, 2008 Professional Development Week sessions in Simi Valley, California, you may take half off the full price. To use this discount, please register and pay by November 14, 2008. If you would like to have an IT Security Baseline or Network Penetration Audit performed by Canaudit, you can have a \$10,000 discount from the full price, provided the work is performed between November 1st, 2008 and March 15, 2009. Please use booking code GORD_2008_IT when reserving your class or your security project.

If you would like to receive articles like this in the future directly, please opt-in to our distribution list on the Canaudit website.

AUDIT & SECURITY SERVICES

Canaudit specializes in a variety of information system and technology audits, ranging from periodic network penetration testing to full network and operating system security review. Our tailored audits provide an objective, disciplined, and in-depth analysis to evaluate and improve the effectiveness of risk management, control and security within your organization's technological environment.

For interest in Canaudit to perform an IT audit for your organization, please email Gordon@canaudit.com or Tamra@canaudit.com, or call (805) 583-3723.

PROFESSIONAL DEVELOPMENT

Canaudit provides quality seminars to local chapters and major corporations. These seminars include technical information system audit classes aimed at everyone from an introductory level up to management. With a list of over 20 courses to choose from, we are sure to have a course that will meet your individual needs. In addition to chapter and private seminars, Canaudit also holds public courses. Upcoming public courses are posted on the website, www.canaudit.com.

Upcoming Public Courses:

Farmington Hills, MI

October 20-23, 2008
October 22-23, 2008

Hands-On: Performing an IT Audit and Security Baseline
Control and Security of PeopleSoft *NEW*

Simi Valley, CA

December 8-12, 2008
December 9-10, 2008
December 11-12, 2008

Hands-On: IT Audit and Security Boot Camp
Control and Security of Web Applications
Computer Forensics for Security and Audit Professionals

Albuquerque, NM

January 12-15, 2009
January 12-13, 2009
January 14-15, 2009

Hands-On: Performing an IT Audit and Security Baseline
Control and Security of Oracle *NEW*
Control and Security of Enterprise Wide E-Commerce

Registration for a Canaudit public seminar can be performed online at www.canaudit.com. For additional information or interest in hosting a Canaudit seminar, please email Brenna@canaudit.com or call (805) 583-3723.