Security Dollars: Focus on IT Training

Melissa McCoy
CTO
Kaizen Approach, Inc.

Problem

- Too many data breaches occur because of human error: whether actions of end users or IT staff.
- Despite a plethora of security products available and deployed, breaches continue to mount for the public and private sectors.

Data Breach Scope

- The costs of data breaches can be estimated using the 2013 Cost of Data Breach Study, which the institute conducted for IT security provider Symantec. The average global cost of a data breach is pegged at $136 a record in 2012.
- The Privacy Rights Clearinghouse notes that 867,217,832 RECORDS breached through April 30, 2014 from just 4,257 data breaches made public since 2005.

Data Breach Causes

- In Verizon's 2014 Data Breach Investigations Report, gathered from more than 50 organizations across the world as well as its own research, at least 1,367 confirmed data breaches, along with more than 63,000 security incidents were found.
- For the public sector, of the nine factors that Verizon identifies as the most common ways hackers infiltrate a target, the most frequent (34% of cases) is a miscellaneous error. The next highest is insider misuse, at 23%, followed by crimeware and theft, at 21% and 19%, respectively. **The entity usually responsible for the miscellaneous error is a systems administrator, at 43% of cases.**

Reducing Breaches Through IT Education

- A successful and evolving security program requires the buy-in of upper management and the education of IT staff and end users.
- It is proposed that more of the security budget should be devoted to training IT staff on how to securely develop, configure, manage and monitor IT systems and software.
- It does no good to implement sophisticated security products, and not have knowledgeable and trained people to run them.

Breach Exacerbated by IT Staff: Target

- Even with FireEye and antivirus installed and configured, Target security staff ignored the alerts generated by the tools when malware was detected.

- Target had begun installing FireEye malware software six months before the attack and as soon as the hackers began uploading their code, alarms allegedly went off. On November 30th, 2013, the hackers deployed their custom-made code, triggering a FireEye alert that indicated unfamiliar malware: malware.binary.

- As the hackers inserted more versions of the same malware FireEye sent out more alerts, each the most urgent on FireEye's graded scale. Target's Symantec anti-virus system also apparently found suspicious activity around the same time. FireEye software could have even automatically deleted the malware automatically, but the function was turned off.

- In this case, though, it appears that nobody stepped in to take action. It's not clear why exactly Target wouldn't have responded.

Target Outcome

- There’s a limit to what security systems can do: at some point people must take the reins and investigate alerts, review events, research solutions and configure systems. The most sophisticated security solutions can’t operate without human intervention, as the Target data breach demonstrates.

- Target’s CIO and CEO have resigned
- 110 million customer records exposed
- $61 million in fourth quarter losses, estimated total cost of the breach $400-450 million according to Gartner

Educating Management to get Buy-In

- Commitment to IT security needs to come from the top: if upper management doesn’t see IT security and education as a priority in their risk management process, money will not follow.
- **Educating management to the security threats and then the benefits that security training can provide to the business is as important as educating employees and staff. Continuing to keep management in the loop as to how the security investment is paying off is critical.**

Continue to Educate End Users

- An annual security awareness class is the minimum requirement for end user education. Many companies have a program, but the 2013 Ponemon/Symantec cost of data breach report shows that 62% of breaches are caused by employee and system errors, there’s clearly some work to be done.

- Successful security awareness programs provide frequent (monthly) updates and reminders of what to watch for. Alerting staff to current data breaches and new vulnerabilities highlighted in the media makes it relevant to employees: the issue is real rather than abstract. SANS offers free monthly newsletters which can be distributed to employees on a monthly basis:
- http://www.securingthehuman.org/resources/newsletters/ouch/2014

- Free tools to jumpstart a security awareness program:
- http://www.sophos.com/en-us/security-news-trends/it-security-dos-and-donts/training-tools.aspx

Educate IT Staff

- How much security training is spent on IT staff ? Do developers know how to create secure code ? Do they have the tools to test their code for security vulnerabilities ? Do system admins know how to harden systems ? Do they know the security vulnerabilities in their systems and the best practices for securing virtual systems, databases and network devices?
- There's many online and classroom classes to educate IT staff, with some focusing on securing types of systems (Windows, UNIX), virtual systems, databases and networking/firewalls. There are also classes on forensic analysis and penetration testing.
- https://www.isc2.org/liveonline/default.aspx
- http://www.sans.org/courses
- Other training classes deal with secure coding principles, such as the SANS classes below:
- http://www.securingthehuman.org/developer/swat
- http://www.securingthehuman.org/developer/demo-training-lab

Create Own Training

Companies can take their own steps to educate their IT staff according to their own security policy and relevant standards (FISMA, NIST, PCI, HIPAA, ISO). Creating a process to evaluate and integrate new applications and systems into their environment would be an example. A checklist to follow for such new systems might go as follows:

1. Any external data connections ?
2. Interfaces with existing systems ?
3. Classification of data managed—PII? NPI ? Sensitive ?
4. Ability to monitor or manage existing systems
5. How is the system managed and monitored itself ?
6. Authentication and authorization within the application – are there interfaces to external authentication engines like AD, LDAP, Top Secret, RACF ?
7. Access to underlying operating system privileges /programs
8. Documented backdoors or vulnerabilities
9. Functionality which could be used for purposes other than intended
10. Use of known insecure programs or protocols (telnet,ftp,nfs..)
11. Software requires admin or root authority to run

Developing a secure template/standard for operating systems and major subsystems is a tangible means of encoding the knowledge of employees and passing it on to others. Virtualization has made it easier to spin up systems using a ‘gold standard’ image.

Tools to discover Vulnerabilities

- There are freeware and COTS tools to scan code and servers for vulnerabilities. These include well known tools such Metasploit, Nessus, Nmap, Retina and Nikto.

- US CERT offers their own free tools:
- http://www.cert.org/secure-coding/tools/index.cfm
- http://www.cert.org/vulnerability-analysis/tools/index.cfm

- Developers and systems administrators /engineers can use these to identify issues in the systems, and remediate them. Make these tools part of a secure systems development/configuration process.

Building Internal Expertise

- Get buy-in from the key knowledgeable people in IT: ask them what they consider to be security risks within the enterprise and document their concerns and their suggested mitigations.
- Use these internal experts to create an internal security working group, one composed of security professionals, IT professionals and audit/compliance staff.
- Leverage this group not only to identify security issues and solutions, but to build the IT security training curriculum. Their insight and suggestions will be invaluable input for an ongoing IT security training program. People tend to take care of what they have invested time in: make IT part of the training plan, not passive recipients of it.

Summary

- Ensuring that IT staff knows the security standards/policy of the organization AND how to securely develop, configure and maintain the systems is an effective means of mitigating risk: it is also a continuous process.
- Tools and education are not that expensive compared to costs of security software and hardware
- Spending money on sophisticated security solutions only pays off if employees know how to leverage the systems.
- Training IT staff ensures that when confronted by new software and systems, the ground work for implementing and running secure systems is in place: rarely are systems so innovative and esoteric that they require specialized knowledge to secure them.
- Security products alone won’t a safe enterprise make: skilled and savvy IT staff and employees are the biggest factor when considering the ROI of a company’s security investment