KNOWING VERSUS FEELING: SECURING YOUR BUSINESS WITH BUSINESS CONTINUITY MONITORS AND NETWORK ACCESS CONTROL

KEVIN T MCDONALD, iCEO #27674

The Current Threat Level: Red

The cost of a single suspect intrusion is now roughly $90 to $305 USD per record[1]. This figure can be compounded by the loss of future business, the cost of locating, notifying and mollifying the impacted individuals and by the loss of productivity imposed post-incident. The most expensive intellectual property security loss was probably the Manhattan project's loss of nuclear technology in the fifties. The Manhattan project alone cost $20B USD[2]. The most recent modern victim was TJX loss of customer credit card data, the result of a single Wifi hub attached to the network, estimated to cost 1.6 Billion USD[3]. In these dark days, how secure do you feel?

What is the ideal security profile?

Within the current environment, it depends a great deal on the enterprise. Most security models laid flat look like a cross-section of a golf ball. The most valuable information lies protected at the center, surrounded by rings of assurance. Each ring could present one or more hurdles requiring the aspirant to provide a card, a pin, a password, a fingerprint or other biometric id. Once granted access, there is still the possibility that eavesdropping may circumvent the entire process. If the information being protected is similar in value to the above, it warrants all the attention you can spare.

What are some of the threats faced by today's enterprises?

During the cold war, governmental security services devised a means to read data off of electronic devices at a distance of electronic emanations. The counter-measures to this type of eavesdropping are grouped into a class of devices known as Tempest controls. The Tempest controls limit, surround or broadcast noise to reduce the risk of eavesdropping. Tempest attacks are not as likely to affect low

[1] Source Informationweek.com 'Security Breaches Cost $90 To $305 Per Lost Record ' Forrester Research surveyed 28 companies that had some type of data breach and found it difficult to calculate the expenses that resulted. By Sharon Gaudin quoting Forrester Report by Khalid Kark' - http://www.informationweek.com/news/showArticle.jhtml?articleID=1990002221)

[2] Brookings Institute - http://www.brook.edu/FP/PROJECTS/NUCWCOST/MANHATTN.HTM

[3] Source hackreport.net Inside Job? TJX Hack Loss Estimated at 1.6 Billion,Martin Hack, Hack Report quoting Protegrity) - http://hackreport.net/2007/04/12/inside-job-tjx-cost-of-breach-estimated-at-16-billion/)

echelon targets due to the cost and sophistication of the equipment required, but high value financial, R&D and governmental entities should take note.

There are a number of on-ramps to the average network today. The typical website is one of the most likely places to be attacked. Since these are complex and change often, there are opportunities to exploit newly discovered vulnerabilities and holes left when new programs are introduced. Without specific blocking techniques, these sites are a weak link. Hackers will scan thousands of sites looking for a particular weakness. They may not be targeting your organization in particular. Yours is just one that appears vulnerable.

Security services refer to this environment in terms of threats, vulnerabilities and countermeasures. For example, if you leave your home unguarded for a few days and the mail and newspapers pile up, the burglar will try your door first. The threat is the burglar. The vulnerability is the house appears to be unoccupied. The doors, locks and alarms are countermeasures. If on the way up the path to your house, he sees a sign advertising a burglar alarm, this additional countermeasure may be enough for him to skip your home and go on to the next house.

Major Threats

Unpatched Systems:
In a typical week, newly discovered software security vulnerabilities number in the tens to hundreds. If these vulnerabilities are not secured, there will be someone on the net who tries to use them to gain access to networks. Since the typical IT staff does not generally have time or opportunity to install the software or hardware update (called a patch) that will secure the system immediately, there is a chance that a hacker may notice the vulnerable systems and exploit the vulnerability. The only challenge for the hacker is finding them.

Public Networks:
One web request can pass through up to 15 or more routers, any one of which could be compromised by a third party without the host's knowledge. Once in, all traffic passing through a router is open to capture by a sophisticated actor. This ease of attack, due to the number of unsophisticated players, presents the highest level of threat today. Since hackers tend to attack targets of opportunity, looking for weaknesses, the least prepared are likely to be attacked before more sophisticated targets.

Wireless Access:
With the advent and popularity of WiFi, WiMax, GSM and EVDO wireless data transmission, attacks are even simpler, since laptop cards have vulnerabilities that can be attacked without even logging on to corporate nets. An unsecured laptop can be corrupted with stealth software that will render the laptop a virtual servant of the hacker. The laptop will often check back for orders from the hacker. With the subsequent instructions, there are numerous negative scenarios that can result.

The wireless network hub is also vulnerable with improper configuration or weak encryption that can be broken within a short time. These hubs are deployed by many IT staffs because they are inexpensive and the risk is thought to be low because it requires some proximity to the network to listen in to the

traffic. However, this is the very technique used by a hacker over a six month period to capture millions of customer credit card numbers in the TJX attack. The network can be completely protected in all other ways and the hacker merely bypasses all that security with one poorly secured WiFi hub. This is equivalent to having a diplomatic passport onto your network. No waiting in line, no baggage inspection.

The Audit Function in IT: Internal Versus External

Typically a security audit is conducted along with the annual accounting audit to make sure minimal security safeguards are in place and functioning. These audits typically have been performed by external IT auditors, seconded from public accounting firms. Using Sarbanes-Oxley, BASEL, HIPAA or Gram-Leach Bliley to drive corporate compliance, these audits cover the basics of disaster recovery and IT best practices. However, since they typically only occur annually and the IT department looks upon them as externally mandated rather than internally requested, there is still a good bit of resistance and minimal effort to adopt standards as an internal benchmark.

As firms adopt more proactive business philosophies such as Six Sigma and CMM5, the drive to go from reactive to proactive has finally reached critical mass in IT. Now the push is on to adopt internal IT audit and generate continuous instead of discrete vigilance, i.e. adopting standards of behavior instead of exhibiting good behavior only when someone is watching.

There is still a good bit of resistance to Internal Audit since it is still in the inspector role. Quality has to originate from within a system, not be inspected into it. In order to get to the next level, I recommend establishing a Business Continuity Monitor instead of internal audit. A BCM conducts exercises to discover weaknesses. An exercise is different from an audit test. A test is pass/fail with the group failing getting poor marks as a result. By conducting exercises, everyone shares the same goal, finding weaknesses. Rewarding the identification of weaknesses is a much more powerful tool than conducting audit tests. By establishing Business Continuity as the framework, the audit function is not viewed as adversarial by the internal staff.

This also eliminates a potential source of conflict between management and IT. Since IT generally likes to have the latest and greatest, it is generally assumed that what they ask for from management contains a good bit of fluff. If the request comes from an independent third party, the request can be relied upon. “They need to replace their widget so we have a better chance of not experiencing what XYZ went through last month.” By having the BCM sign off on acquisitions, the C level has more assurance that the acquisition can be monitored for security and that the continuity plans can be updated to include new computing resources.

Technology to the rescue:

In conjunction with the BCM, you can also deploy a monitoring device. The next generation of firewall devices on the horizon are called Network Access Control systems (NAC). A NAC is a smart firewall that pre-registers all devices on the network. If a new device comes onboard, the NAC looks up the profile. If it doesn’t match a preexisting box, the device is sequestered to guest status. Guest status

might allow network printing and web browsing, but no access to corporate servers. The security staff, once alerted to the new device, can investigate further whether it is a visiting vendor, a new corporate PC, or a bad guy attempting to access the network. If the device is identified as the CFO's new Blackberry for instance, the profile will be updated and the next time the Blackberry accesses email, it may be granted additional access. If the Blackberry's user is unknown, it is relegated to guest access with relatively low risk it can access any sensitive information. This technology has been marketed under the labels Network Admission Control (NAC) by Cisco and Network Access Protection (NAP) by Microsoft. The basic premise remains the same, change the security for networks from everyone is welcome to prove who you are before we grant you access to anything beyond the basics.

Another technology that can be deployed with NAC is called patch management. A patch manager looks at each network packet, determines if it represents the identified vulnerabilities and changes it to remove the weakness. The original server still has the problem, but the Patch Manager prevents it from being exploited. The IT staff can patch the server on their normal maintenance cycle without compromising security.

All of these techniques are starting to converge within more sophisticated appliances. The new generation will allow self-updating, downloading new profiles to take into account new threats, new viruses and new device types as they become available.

In conclusion, by first making enterprise security a function of Business Continuity and deploying next generation network monitors such as NAC, the enterprise can adopt a proactive profile with less resistance from internal stakeholders. This can lead IT to the next level, where the numbers of vulnerable systems are shrinking and IT can resume a central role in creating value for the enterprise. At that point, we should all know we are more secure.

KEVIN T MCDONALD

About CEO Europe (www.ceo-europe.com)
Thanks to its unique expertise and positioning, CEO Europe is now able to link the worlds of interim management with the executive search. Featuring superior flexibility and a reaction time of less than three weeks from initial demand to final placement, Management on Demand™ is perfectly tailored to the modern day constraints on most companies. Drawing from its pool of over 9500 senior executives worldwide, each with a proven entrepreneurial profile, CEO Europe is able to offer managers who are prepared for local or cross border Interim projects that could turn into full-time positions in one of the 168 countries covered