Global Information Assurance Certification Paper

Managing Security in a Mobile Environment

The world of business is becoming more mobile. "In 2005, more than 65 percent of workers worldwide will be equipped and trained to work as relocatable, mobile employees"[1] and "the worldwide mobile PC market grew by 32.7 percent in the third quarter of 2000 compared with the third quarter of 1999."[2] As employees gain mobility through the use of laptops, smart phones and PDAs, the threat to organizational security grows. As the devices become more powerful and less expensive, more and more personally owned devices make there way to the connected edge of the network. The rise of the Internet as an accepted vehicle for business use has dramatically increased the points of entry to the corporate network. In this report, we are going to examine the requirements for effectively managing security in such an environment, in order to take advantage of the productivity gains that the mobile worker offers, while limiting the exposure to the enterprise.

In dealing with information security, we refer to the "three pillars" – confidentiality, integrity and availability. With mobile devices these three pillars still apply, they just become more difficult to manage. With remote security there are also four main threats that need to be understood and addressed – threat to the device, threat to the communications channel, threat to the corporate network from the remote device and the threat to the data.

We must address all three of our pillars, and must acknowledge where the risks to the organization are in developing security processes that can apply to mobile devices. There are five steps that should be followed to ensure success:

1. Develop Information Security Policies and Standards (specifically for remote devices)
2. Design the Information Security Architecture and Processes
3. Implement Information Security Awareness and Training
4. Implement Information Security Technologies and Products
5. Auditing, Monitoring and Investigating[3]

---

[1] Wilderman, Jack. "The New Mobile and Remote Work Environment: Making the World Your Office." Page 17. Stamford: GartnerGroup. October 2000.
[2] Maarouf, Mostafa. "Worldwide Mobile PC Market: Third Quarter 2000 in Review." Update: 15 January 2001. http://www3.gartner.com/DisplayDocument?id=319048&acsFlg=accessBought (February 9, 2001).
[3] Malik, William. "Do Security Products Alone Solve the Problem?" Updated: 16 January 2001. http://www3.gartner.com/DisplayDocument?id=319335 (February 9, 2001)

1. Develop Information Security Policies and Standards

The most import step that must take place in order to effectively manage remote users involves the development of policies that are tailored to the needs of the remote user. They must be strong enough to protect the organization, yet flexible enough not to disrupt the user and negatively affect productivity. The organization must be conscious of the need to develop policies that specifically address the remote user.

> "We recommend that enterprises first define their corporate information security policy and control standards that will provide the qualitative criteria for measurement. … Our research indicates that, without exception, leading-edge information security organizations identify the information security policy and standards as the most important foundational component driving all other security activity. We believe that enterprises should consider security policy and standards as the most-critical security initiative. The information security standards are the cornerstone of security for the enterprise. We recommend that the standards be defined independently of the dynamically changing technology and include roles and responsibilities, baseline security standards, a risk assessment methodology, and escalation and deviation criteria".[4]

When developing the policy document, it is important to build it so that everyone in the organization can read and understand it. It is important not to get too bogged down in details. "We recommend that a strong information security policy be stated as a separate one-page document and contain five to 10 significant control points that will be communicated to all employees, vendors, contractors and outsourcers. A statement of ownership of information, definition of employee's responsibility for the protection of the information asset and intended recourse for noncompliance should also be included in the policy statement."[5]

Policies that address the remote user could include requirements for certain types of documents to be encrypted, the use of digital certificates to ensure authenticity of communications and mandating the use of physical security products while traveling.

---

[4] Malik, William. "Do Security Products Alone Solve the Problem?" Updated: 16 January 2001. http://www3.gartner.com/DisplayDocument?id=319335 (February 9, 2001).

[5] Malik, William. "Do Security Products Alone Solve the Problem?" Updated: 16 January 2001. http://www3.gartner.com/DisplayDocument?id=319335 (February 9, 2001).

2. Design the Information Security Architecture and Processes

Once policies are in place, the organization needs to define the overall processes by which the policies will be implemented, monitored and enforced. Policies become valueless if they cannot be enforced, and enforcement is not feasible without monitoring. There are a number of policy management applications available on the market. The organization needs to tread a careful path on this issue, as it is important for the employees to understand the value of security, while at the same time not feeling intimidated by "Big Brother".

3. Implement Information Security Awareness and Training

Once the architecture is in place, the next step is to raise awareness and train the employees of the organization. This is the next most important step after policy definition. The majority of security programs fail because employees do not use the security products effectively, if at all. Only an awareness program and training can address this issue. The employees need to understand why security is critical to the organization, and how what they do on a day-to-day basis can have serious consequences. The employees need to be thoroughly trained on the new security applications, and their use of those applications needs to be monitored to ensure that policies are being adhered to. Only when security is adopted as part of how people do their jobs, will the threat to the organization be reduced.

4. Implement Information Security Technologies and Products

Once the policies are in place, the organization needs to look to define and procure the technologies that will make up the security architecture. For remote PCs, this involves the procurement of a number of technologies:

Anti-virus: At the heart of any security architecture is a strong anti-virus product that includes automatic updates of definitions when the PC is connected to the server. This process must be automated, and should not require user intervention.

Personal Firewall: A personal firewall product is a necessity for the modern road warrior. As hotels and conference centers wire themselves for high speed Internet access, many of them do so by implementing a shared network, similar to cable modem access in the home market. This leaves the PC extremely vulnerable. Personal firewall products can be configured for dual-zone protection – leaving system access unrestricted while on the trusted local network, and providing tight security while on the untrusted Internet.

Encryption: Either file/folder or full disc. The only way to ensure that the data remains secure, even if the device is not is to encrypt the data on the PC. A product that also offers e-mail encryption provides enhanced security.

Virtual Private Network (VPN): All connections between the remote PC and the corporate network should take place over a VPN. This ensures that the communication channel remains secure.

Physical Security: The device must be protected. This can be done by using hardware like locks and cables, or via software by using software products like Computrace, from Absolute Software. "Computrace is the ultimate computer watchdog. The moment your stolen computer is connected to a phone line or has access to the Internet, Computrace silently reports your PC's location to the Computrace Monitoring Center. The Computrace Recovery Team then works with law enforcement to get it back."[6] The combination of physical protection coupled with the ability to recover the PC in the event that it is lost or stolen is a potent combination.

5. Auditing, Monitoring and Investigating

The policies that are developed, and the processes that are put in place to enforce them are only going to be effective if there are regular audits of the system. Monitoring of adherence to policy and investigation into non-compliance is required on a regular basis. "No matter what security software and hardware you provide your mobile workers with, if they don't use it or know how to use it, or worse still, don't bother to use it, then you already have a weak link. It is this weak link that will always be your biggest security dilemma."[7]

Understanding where the weaknesses in your system are is the best way to find measures to correct them. Above all, polices and processes need to be reviewed and updated on a regular basis. Policy should never be considered static.

[6] "Computrace Theft Recovery." November 2000. http://www.computrace.com/PDF/Theft_Recovery_Info_Sheet.pdf (February 15, 2001).

[7] Bellamy, Jay. "July 2000 Test Centre A Moving Story." July 2000. http://www.check-mark.com/artframe_ad2000.html (February 9, 2001).

Information security is a difficult subject to address when the devices in question are safely tucked away behind the corporate firewall. Once they move outside the corporate firewall, managing those devices becomes much more difficult. Fortunately, many of the lessons learned in developing the security for the organization can be applied to the remote user – they just need to be modified and enhanced.

The installation of some common software applications onto the remote PCs can go a long way to addressing our three pillars of information security, and can also address the main threats to the organization. However, installing products is not enough. It is critical that the users of the devices be educated as to their features and benefits, and must be made aware of how critical security is to the well being of the organization. Education is made possible by defining the expectations of the user in doing his or her job by way of policy. As such, it is critical to remember that the organization needs to define policies that take into consideration the remote user and their unique needs.

Warren Cartwright