Scenario three

Technology, Internet

Question: How do you think this situation could have been prevented? Could the IT department have conducted regular inventories of the software on each computer to identify missing patches? Could the IT department have implemented a process to ensure that no computer is moved outside the boundaries of the firewall?

There are steps that the IT department could have taken to avoid the situation that occurred. There should have been policies in place to ensure that antivirus/malware software was installed on the computer before it was allowed to connect to any network. A machine build checklist could be implemented to where after a computer is initially setup with appropriate operating software, all relevant applications needed would then be installed, including the antivirus software.

The endpoint protection software could be installed in a standalone mode if the system being deployed was not going to be part of the larger domain network or if it was going to be used for short term testing. Otherwise it could be deployed from a central management server. It would at the very minimum have that protection on it. Most antivirus vendors have auto update features in their software so that in the event the virus definitions become outdated the software automatically checks in to download the latest definitions.

Proper operating system patching would have to be done as well to reduce the risk of software vulnerabilities. Patching could be done from an internal update server like Microsoft’s WSUS server so that a connected system would contact the internal server at a scheduled time and pull down the appropriate updates it needs for the software that is installed. There are also many third party tools, like GFI’s LanGuard, that can be used to scan systems for vulnerabilities and patches and install them on demand without having to wait for a scheduled time to download (GFI, 2012).

There are several ways you can try and lock down a network so that unauthorized computers cannot connect to and communicate on them. If a network is using DHCP to distribute IP addresses to computers that connect to it, reservations can be made on the DHCP server so that a particular computer with a unique MAC address is assigned one of the IP addresses in the scope (Smith, 2003). If all DHCP leases were reserved, a computer would not be able to automatically be assigned a network IP address, preventing it from communicating on the network. This is not a guaranteed option as an informed user could assign the computer a static IP address on the network which would allow it to communicate as long as there was not a conflict with another one on the same network. That user would have to know the relevant network information however.

One common security misconception I hear often is that if an organization has a firewall implemented on their network, they are protected from attacks from outside of the network. I believe that this could have been true many years ago, but I have seen attackers taking more of a targeted approach (Pirch, 2009). I do still continually see random port scans against the firewall on my own corporate network, unsuccessfully breaching the network. If there are no open ports on the outside of the firewall, they have no path into the network. If this were only true. The breaches that I have seen to be successful have originated from internal users, or client side attacks.

They occur when they visit compromised websites or open phishing emails thus launching malicious code that allows external attackers a clear path into the network. There are safeguards that can be put in place to help protect the workstation from these type of attacks, like antivirus software, proper patching of the browsers, or even content filtering firewalls. Content filtering gateways can be effective at blocking access to known malicious sites thus preventing the download of the malicious content (McAfee, 2004). I have not been able to find anything that will always secure us against the human variable.