



Fact or Fiction:

Debunking the Top 5 Misconceptions about Endpoint Security

Tuesday, May 13, 2008

www.lumension.com



Overview

Security experts have done a reasonable job over the past several years preaching to businesses about the increasingly porous nature of the enterprise network perimeter. Most organizations have gotten the message loud and clear, understanding the critical importance of enforcing security policies on the endpoints and shoring them up from attack.

Unfortunately, some enterprises have been less effective than others when acting on that message. This is because even in the wake of this increased enlightenment over the importance of endpoint security, there still remains many a misconception about the topic. We'd like to dispel a few of the biggest myths so that enterprises can better understand how to protect themselves from attacks against their clients.

Fiction:

Endpoints are more secure today than they were before.

The Facts:

Because most enterprises at this point have taken steps to protect their endpoints with traditional antivirus, personal firewall, anti-spam and antispymware and other HIPS products, many within these organizations are under the mistaken impression that their endpoints are more secure today than in the past. The truth is that endpoints continue to be one of the elements within IT infrastructure most vulnerable to attack.

According to the SANS 2007 Top 20 Internet Security risks, "Critical vulnerabilities in software on personal computers inside and outside enterprises (client-side vulnerabilities) allowing these systems to be turned into zombies and recruited into botnets and also allowing them to be used as back doors for stealing information from and taking over servers inside large organizations" remain a top priority.

Unfortunately, traditional defenses that protect endpoints from attacks against these vulnerabilities are becoming increasingly ineffective as crafty attackers learn to beat them. According to Gartner, these signature-based technologies have less than a 50 percent chance of catching completely new threats and can miss up to 10 percent of old threats in the wild.¹ The

¹ Magic Quadrant for Endpoint Protection Platforms, 2007, Peter Firstbrook, Arabella Hallawell, John Girard, Neil MacDonald, Dec. 21, 2007



dilemma that these signature-based solutions face is that they try to block all of the bad processes from running rather than only allowing the good ones to operate. The challenge is that they can't keep up with all of the new attacks that crop up each day. And they certainly can't keep up with targeted attacks, for which signatures have not been created.

Fiction:

Applications are becoming more inherently secure.

The Facts:

Even in this era of skyrocketing data breaches, many companies still fail to implement actionable security policies to protect their endpoints.

According to a recent survey conducted among 160 global enterprises, only 41 percent of firms have documented and ratified security policies in place and as many as 13 percent have no security policy in place at all.²

Simply having a security policy doesn't always guarantee that it is adequate, either. There are many organizations with policies in place that are too broad to be actionable, are outdated or simply make the end user apply their own judgment in questionable situations.

And even if a solid security policy is written that is no guarantee that employees will know about it and follow it. In order to ensure this happens it is critical that organizations not only plan and budget for the development of the policy itself, but also of a robust awareness and training program to complement it. After all, a security policy is only as strong as its awareness and enforcement.

Fiction:

Organizations can rely on end-users to follow endpoint best practices.

The Facts:

Even companies with a strong security policy in place face endpoint security risks if they fail to adequately enforce their policies. Unfortunately, too many enterprises today still trust their users to self-police themselves while working on the endpoint.

² CISOHandbook.com, Current State of Security Policies



Even the employees who should know better—IT professionals—are known to regularly break the rules. A recent survey of IT professionals by the Ponemon Institute found that more than half copied confidential company information into USB memory sticks in spite of a company policy that banned the practice.³

The issue of weak policies only exacerbates the problem. The hitch is that not only are employees likely to break a policy if they view it as inconvenient, but many conscientious users might also indulge in risky behavior when the policy is too vague to understand or enforce.

Clearly, organizations that leave it up to the user to implement endpoint security best practices are exposing themselves to increased risk. The only way to truly mitigate these risks is to not only develop strong policies, but to also put measures in place that automatically enforce those rules. This takes the burden of security from the users' shoulders and allows them to work without worry.

Fiction:

Isolating non-compliant endpoints from the network solves your security problem.

The Facts:

The main idea behind most network access control (NAC) solutions is that by quarantining vulnerable endpoints from the network, an administrator can effectively mitigate the risk these non-compliant machines pose to the infrastructure.

The difficulty is that deployed in a vacuum, most NAC solutions are purely preventative—they simply deny network access to non-compliant or infected machines. While most NAC vendors position themselves as providing the overall solution to both quarantine and remediation capabilities, few actually offer the full framework for access control without working with partners that offer automated vulnerability assessment, remediation and continuous validation.

Without some way to automate the remediation of these machines, these NAC solutions can actually cause more problems than they solve. A lack of automated remediation puts these endpoints into 'PC purgatory,' putting users in a non-productive situation where they are unable to

³ Ponemon Institute, Data Security Policies are Not Enforced, December 2007



access company resources and must wait for IT personnel to fix their machine before reconnecting.

In order to avoid this black hole problem, administrators need an easy and seamless way to fix the problems identified and admit the user back onto the network with as little inconvenience as possible.

Lumension Security's Proactive Approach to Vulnerability Management

Lumension Security understands the inherent insecurity of traditional signature-based technology. Lumension Security's Sanctuary endpoint security solution allows organizations to proactively operate on the supposition that only allowing the known good applications and processes to run is more effective than trying to block all of the bad ones.

Lumension Security also understands the importance automation plays within a successful security management program. Combined with a strong and detailed endpoint security policy, Lumension Security's Sanctuary Application and Device Control can automate policy enforcement so that enterprises needn't rely on their users' word when it comes to following the rules. Plus, Lumension Security's vulnerability and patching capabilities can automate the endpoint remediation process in order to prevent quarantined users from falling into that 'PC purgatory' which stymies so many when their endpoints aren't compliant.