Endpoint Security

Sponsored by Sophos

Speaker: Mike Chapple, CISA, CISSP

Mike Chapple: Hi! I am Mike Chapple, and today we are going to talk about endpoint security. When times are tight we are all called upon to make more efficient use of the financial and human resources under our control. Chances are that you have been asked to take a hard look at your security budget over the past year and identify areas where you can help improve the bottom line. In this video, we take you back to basics to look at endpoint security and help you identify the truly critical components of your endpoint security program.

One area you might consider for cost savings is your malware protection budget. After all, antivirus and antispyware packages are boring technologies. They toil in silence and chances are you haven't had a significant malware outbreak in your organization in recent years. At the same time you are probably being asked to write very significant checks to your malware providers in order to pay for signature updates. Are these products really worth the cost, have you seen a decline in malware outbreaks in your organization, because the threat is going away or is it that malware protection solutions have become so effective that we hardly notice them protecting us. Well, the threat is not going away.

A recent study shows that the threat posed by malicious code continues to rise dramatically. In 2005 we saw only 333,000 new unique threats from viruses, worms, Trojan horses and other malicious code. Last year that number reached a staggering 16,495,000. Take a moment to think about the staggering nature of that statistic. It means that there are 1,883 new malware threats released every hour 365 days a year. At that rate it takes only one week today to produce all of the malicious code that was produced during the entire year in 2005. This trend results from the evolution of polymorphic malicious code.

Now, our authors understand the workings of signature detection system and now focus on developing malware that changes itself over time so that it becomes unrecognizable with existing signatures. Antivirus vendors are then forced to produce new signature updates to cover these evolved viruses and this cat and mouse game makes current malware protection critical and there is no evidence to suggest that things are going to change any time soon. In this environment it's important that you continue to maintain current antivirus subscriptions. The nature of the threat and the effectiveness of the solution, takes this off the table as something that you can completely eliminate from your security budget.

That said, this is also a good time to renegotiate your contracts with antivirus vendors especially if your renewal costs have stayed constant or increased over the past few years. Antivirus companies are feeling the same economic pressures that we are all experiencing and recognize that it's much cheaper to make price concessions to keep an existing client on board than it is to acquire a new client. Be fore warned you may need to play hardball to gain meaningful price concessions. Make it clear that you consider antivirus and antispyware technologies a commodity that several major vendors are all able to provide and that you are willing to switch if you current vendor isn't able to match the cost savings proposed by the competition. In fact it wouldn’t be a bad idea to go into those negotiations with a couple of other proposals in your hand to show that you mean business.

This strategy extends beyond the antivirus software as well. If you scatter your security budget, you will find recurring cost for product subscriptions maintenance and support. Scrutinize each one of these expenses to ensure that you are receiving the most value from your security dollar. You will probably find that you are paying for maintenance contracts on devices that are no longer in use and this is the obvious low hanging fruit that you can eliminate from your budget. As with your antivirus renewal costs remember that nothing is written in stone. Vendors are often willing to renegotiate support costs in this economic climate. I have seen in several cases recently where organizations were able to work with vendors to reduce product's renewal costs by 30-40% by renegotiating contracts. You may need to make some concessions to gain these discounts so be prepared to offer something in return. For example if you are currently renewing your firewall support contract on a year-to-year basis consider renewing for a three-year term in exchange for a discount from your vendor. Taking the time to analyze and renegotiate contracts is one way that you can make a meaningful contribution to your organization's bottom line without compromising endpoint security.

Let's turn our attention now to endpoint encryption. Well, viruses were the threat *de jour* in the early part of this decade. It seems security news in the past few years focused on the theft of unencrypted laptops or other storage devices and the data breaches that occurred as a result. We saw major news stories break over the theft of unencrypted data from the Veterans Administration and other organizations and quickly move to get our own houses in order. At the time we did not have very many options for endpoint encryption. Microsoft Windows included the encrypting file system EFS but it was awkward to use and required users to identify the files and folders that needed to be encrypted. So we turned to third party encryption solution. A wide variety of products quickly appeared on the market that fulfilled the promise of whole disk encryption. These products intervened in the boot process, requiring users to provide a user name a password or other authentication before the operating system gained access to the disk. The downside of these products, was their per installation cost. Of course we wanted to keep ourselves out of the headlines so we paid the bill but not without gritting our teeth.

Now, you think that times would have changed and beyond worrying about the loss or theft of unencrypted data but nothing could be farther from the truth. We haven't fully encrypted all of our sensitive information. In January 2009 alone the Privacy Rights Clearinghouse recorded ten separate high profile security incidents that could have been prevented with the use of endpoint encryption. Fortunately the world of endpoint encryption has changed for the better. It's now easier and cheaper to encrypt your sensitive data mostly by taking advantage of the encryption technology built into the products that you already use.

For laptops and desktops Windows Vista Enterprise edition now ships with BitLocker built in. This volume encryption software allows you to manage encryption through the use of Active Directory Group Policy and takes advantage of the computational power provided by the trusted platform module or TPM chip that’s built into most laptops and desktops today. It also provides important key escrow capabilities that allow enterprises to recover data in the event an employee leaves the organization or a password is forgotten. Don't forget the importance of encrypting other types of mobile devices as well. Blackberrys in particular provide excellent encryption software that can be centrally managed through the use of Blackberry Enterprise Server or the BES server.

So good news on the endpoint encryption front, you can now replace the costly products you purchased a few years ago with free solutions built into the operating systems you already license. There is yet another way that you can positively impact the bottom line without negatively affecting endpoint security. Ask any security manager who has been through a lost laptop incident and they will agree. The real damage that occurs when a laptop turns up missing is not the $2000 of hardware that’s lost it's the fear, uncertainty and doubt that results from not knowing what information was on the missing device. We just spend some time talking about encryption and you might be wondering why you need to worry about data loss if you have encrypted your endpoints. Even though you have encrypted your devices it's important to remember that there are many other threats that can cause sensitive information on that device to become vulnerable to compromise. Once you log into the operating system you provide access to the encrypted disk and if the endpoint falls victim to a malware infection or is compromised by user error the data on that device is vulnerable to compromise.

One of the most effective strategies for protecting your sensitive data is minimization. Quite simply store sensitive information in as few locations as possible. You will probably find that you have no need to have extremely sensitive information such as credit card numbers or Social Security Numbers on any of the endpoints in your organization. Many organizations believe in this approach but don't know how to begin. Sensitive data might be strewn across a variety of documents, databases, e-mails, and other locations in all sorts of different formats and it's extremely difficult to find it all. Fortunately there is software available to help you with this process. Sensitive data often comes in patterns that are very easy to match. Social Security Numbers for example are typically formatted in a very unique three, two, four-digit pattern that’s easy for software to recognize. Credit card numbers can contain a check digit and you can simple algorithm called the Luhn algorithm to validate suspect numbers.

When selecting a software package to search for sensitive data in your organization, you will need to choose from two different approaches, centralized or decentralized scanning. In the centralized approach you purchase an enterprise solution that scans all of the systems in your organization, severs and desktops for the presence of sensitive information and then provide centralized reporting back to an administrator to analyze those results for false positives and data that does need to be removed. This is a very time consuming approach for IT staff and is by far the most expensive way to approach the problem but it also provides the highest degree of assurance.

With the decentralized approach you purchase a desktop scanning solution that runs on the endpoint and provides the user with the ability to scan his or her own system for the presence of sensitive information. This is often the most effective way to solve the problem as the user knows the context of the files on the system and can use that context to identify false positives. For example if a user scans a system and finds that there is a file that’s flagged that’s containing credit card numbers but knows that file contains recipes for example it's obvious to the user that file does not contain Social Security Numbers. Well, an administrator on the other hand would probably have to go through and verify that manually. This also tends to be a less expensive approach as desktop licenses can also be purchased in bulk. However it places the burden and responsibility for scanning in the hands of the end user and is only effective if you are able to enforce accountability as well.

The use of these tools whether centralized or decentralized rounds out our endpoint security strategy and combine with anti-malware software and encryption forms a solid foundation for protecting your endpoints both in and out of the office. Hopefully you found this information on endpoint security useful and can find ways to apply it in your organization today. Thanks for watching I am Mike Chapple and we hope to see you watching another SearchSecurity.com video.