5 Trends That Will Impact Your IT Planning in 2012

Layered Security

DELL

TREND MICRO

Windows 7 Professional

Small Business Computing.com™

Executive Brief

Layered Security

Many of the IT trends that your organization will tackle in 2012 aren't new, but that doesn't mean your IT staff can sit still while technology continues to evolve. This Executive Brief is one of five installments in this series that will examine trends you need to include in your IT planning in 2012.

By now the fundamentals of computer and network security are familiar to almost everyone who interacts with a PC on a regular basis: install antivirus software, choose good passwords and protect them and download and install software updates. Despite these measures, businesses of all sizes continue to suffer security breaches.

When large businesses like Sony and TJX suffer data breaches, it makes international news. Partly because of the publicity and partly because of the size of the budgets and IT staff at large businesses, cybercriminals are increasingly turning their attention to small and medium size businesses (SMBs), where security is more likely to be soft, breaches are less likely to be discovered in a timely manner and where the rewards for criminals can be high. According to Verizon's 2011 Data Breach Investigations Report, small to medium sized businesses (SMBs) have become hackers' main targets.

Other surveys come to a similar conclusion:

- 40 percent of SMBs have experienced a security breach resulting from employees navigating to a site that hosted malware, according to GFI Software
- SMBs lost 30 million man hours in rectifying issues that result from security problems, according to GfK NOP
- The same survey found that U.S. SMBs that experienced security problems spent $5.6 million, or an average of $1,570 per business, replacing hardware. They also lost $11.3 million (average of $4,800 per business) in terms of lost sales or revenue opportunities

It's easy for SMBs to overlook security. It doesn't directly add to the bottom line in the same way the new products or new clients drive revenue. The true worth of security usually isn't determined until something goes wrong and a business hasn't invested in it — it's a lot like insurance in that regard. Establishing solid security practices early in the life of an SMB is important because that security strategy can grow with the business, which is a far better plan than finding a growing business without solid security that's exposed to all variety of threats.

The 2012 Threat Landscape

Malware has come a long way since the ILOVEYOU virus infected millions of computers in the year 2000 with a simple email with an infected attachment. Attachment-based viruses still exist, but users and email security products have both caught up.

The attacks that SMBs face in 2012 are far more targeted and rely on delivery

mechanisms other than email. They are more likely to be the work of an organized ring of criminals who are trying to find personal information like account numbers and passwords. Web-based applications, ranging from internal business apps to popular online destinations like Facebook, can be used to introduce malware using tactics like SQL injection.

Phishing scams still exist, but instead of casting a wide net in an attempt to garner sensitive information from millions of users, they are more likely to use social engineering, using what seems to be a personal appeal, to build trust with potential victims.

Mobile devices and wireless connections mean that business machines and data aren't restricted to the office. It used to be that maintaining a secure network provided reasonable protection, but now data travels over outside networks that can put SMBs at risk.

While sophisticated criminals are behind many of today's attacks, the amateurs are still out there, and their work is potentially potent. Kits like the one that spawned the Zeus phishing virus are available for purchase online, allowing anyone to be become a self-taught cybercriminal.

What Needs Protecting

When it comes to an SMB's PCs and network resources, it all needs protecting. And while a little common sense can go a long way when it comes to keeping laptops out of sight when they're in a car or choosing solid passwords, other parts of the technical infrastructure require more diligence.

Here is a partial list of computer and network security tips from the SmallBusinessComputing.com website:

- Keep operating systems patched and up to date
- Minimize the use of administrator accounts on PCs
- Use full disk encryption for laptops
- Use WPA2 to secure wireless networks
- Disable remote administration options
- Limit access to shared folders

Both endpoints and networks need to be protected, which means antivirus software and strong passwords are only the start. You need to protect the different layers of infrastructure that exist at even the smallest of businesses. Firewalls and what some technology vendors call unified threat management (UTM) help protect small business networks from external attacks. Endpoint security tools like VPNs and antivirus protection help protect from internal attacks. Access protection and encryption work to protect the data. SMBs that work in certain industries like government might require security information management (SIM) systems to comply with industry regulations.

This approach, known as layered security, is essential to protecting both infrastructure and information in 2012. Given the damage that malware can cause, layered security should be considered essential to protecting the business.

How to Implement Layered Security

Make no mistake; a comprehensive approach to security requires an investment in terms of time and money. The first step to a holistic

"While sophisticated criminals are behind many of today's attacks, the amateurs are still out there, and their work is potentially potent"

approach to security is to make security a priority in the business.

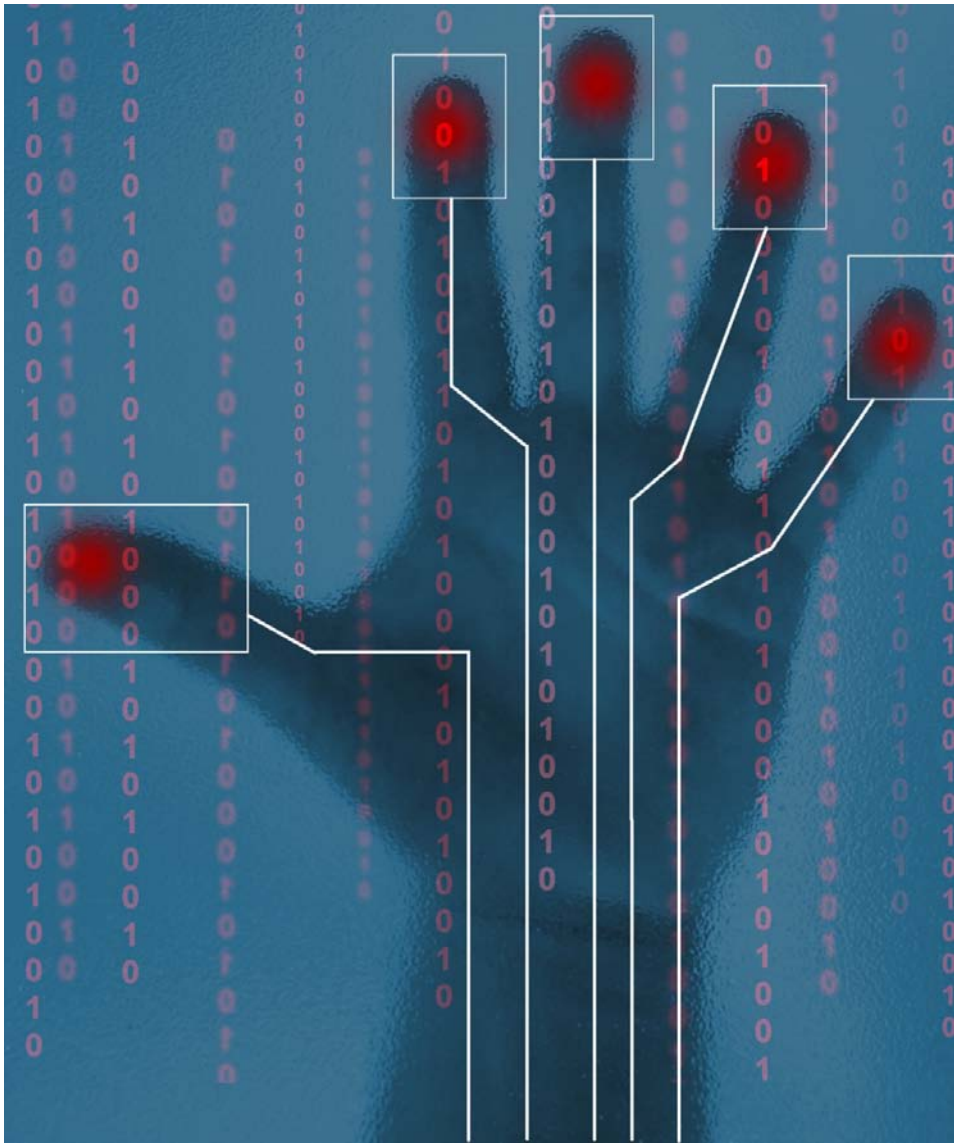
At many SMBs, security and other IT issues are covered by the person with the most experience working with computers or by an IT generalist. This approach can work at the smallest businesses, but it's unlikely to scale well as the business grows. Another popular approach is to outsource all of some of the IT responsibilities to a systems integrator or IT services firm that is a channel partner for the leading IT vendors. SMBs are more likely to get people experienced and certified in IT security when they work with such a partner.

After the right people are found to manage security, the right products need to be found. Layered security, as mentioned earlier, requires everything from encryption software to access control to antivirus software, intrusion protection systems, mobile security and firewalls. SMBs can piece together their security defenses from a variety of vendors based on price and features and then integrate them into a layered security solution, but as with any IT integration project, things aren't guaranteed to go smoothly. Finding products from a single vendor that are designed to work together, or an integrator with a proven package of solutions that work together, is an effective way of developing seamless layered security.

SMBs that lack the resources to dedicate people to security and lack the expertise to create a system of layered security on their own also have the option of outsourcing their security to a managed security services provider (MSSP).

MSSPs can deliver all of the security functionality that an SMB needs to implement layered security, including security for emerging technologies like cloud computing and mobile platforms whose security problems might be unfamiliar to many SMBs. MSSPs can also provide services like an emergency response to a security incident or security training for employees.

Like any form of outsourcing, turning to an MSSP takes a specific part of an SMBs business and turns it over to experts who are trained in that area. This allows the employees at the SMB to focus on the core business, building new products and increasing revenue. MSSPs offer simple, comprehensive protection for SMBs that lack the time, resources and expertise to manage



the layered security they will need in 2012.

How Dell Can Help

Dell and its partners provide the security solutions that small and medium businesses can use to protect their machines and data in 2012. Dell works with some of the best-known brands in security to create simplified, comprehensive protection from attacks that are increasing in volume and sophistication.

At the data security layer, Dell Data Protection provides access control through data encryption to keep data secure. For endpoint security, Dell partners with Trend Micro Worry Free to keep machines and their data secure. Network security comes from Dell's partnership with SonicWALL, as well as Dell PowerConnect J-SRX services gateways.

Dell laptops and workstations powered by Windows 7 Professional provide the latest in operating system security, and when combined with Windows Server, help create a secure network for businesses of any size.

Dell SecureWorks delivers managed security services for businesses of all sizes. SecureWorks provides the key controls for important regulations like PCI, SOX, HIPAA and more. It also delivers email security, cloud security, mobile security, Web security, Web application scanning, intrusion prevention and detection and more. Customers that turn to Dell SecureWorks can choose the platform and service options that work for them so their protection fits their needs and budget.

Conclusion

SMBs are finding themselves firmly in the crosshairs of malicious online attacks. To combat such attacks, businesses interested in protecting their employees, infrastructure and data will increasingly turn to layered security. A layered security approach defends all levels of the infrastructure from attack and offers SMBs the most effective approach to comprehensive security.

When security expertise and resources aren't available, many SMBs will turn to managed security service providers to help them deploy layered security in 2012. MSSPs allow SMBs to focus on their core business and put security experts who otherwise wouldn't be available to a small business in charge of the security infrastructure. With malicious attacks increasing in frequency and volume, 2012 is the time to investigate layered security.

Dell and its security partners are equipped to help small and medium businesses protect their machines and data in 2012. Dell's layered security approach helps keep data safe and secure throughout the IT infrastructure, and its SecureWorks managed security service can deliver enterprise-level security to customers that want to concentrate on their business and let the pros handle their IT security. ■