COMMON-SENSE SECURITY FOR UNCOMMON THREATS

Dell couples multilayered security with systems management to help protect midsize businesses.

By Sandra Gittlen

IT security threats today are more sophisticated, come in greater numbers, and can be sparked by political or financial motivations or launched just to wreak havoc. Whatever the origin or intention, this evolving and multilayered threat landscape requires a multilayered security strategy. No single IT security solution can protect your organization from all the different threats that exist now.

According to a recent report by Forrester Research, Inc., "...data security remains the top security priority for SMBs." ("The State Of SMB IT Security And Emerging Trends: 2009 To 2010," Forrester Research, Inc., January 2010.) But despite understanding the urgency of this threat, many midsize businesses struggle to build a security strategy that is simple, cost-efficient and easy to deploy. The answer to doing just that lies within a layered approach that enables protection from known and unknown threats and breaks security down into a less complex strategy. Dell's multilayered security portfolio of hardware, software and services takes the complexity out of IT security and provides comprehensive, cost-effective protection at the network, endpoint and user layers. Dell also offers managed services to supplement in-house skills and infrastructure. Just like large enterprises, midsize companies are under siege by an array of threats. Viruses and malware arrive in so many different ways that it's difficult for companies to thwart them.

While it may seem overwhelming to combat such threats, not doing so can have serious financial repercussions, not to mention damage a company's reputation. The Ponemon Institute found in its "2009 Annual Study: Cost of a Data Breach" that the average cost per compromised data record breach was $204. The study, released in January 2010, also revealed that the average organizational cost of a data breach in the United States increased from $6.65 million in 2008 to $6.75 million in 2009. Often, costs come from customer notifications, damage control and reimbursements. For some companies, the effects of such breaches are long lasting and can even lead to shutdowns.

This fallout is not reserved for large companies alone. In fact, compliance mandates, which aim to address the potential for data leaks, often apply to businesses of all sizes. For instance, all those in the healthcare industry must work to protect the privacy and security of patient data, and any organization that handles card payments must ensure that sensitive customer data is not exposed.

Data security remains the top security priority for SMBs.

The escalated use of smartphones andother mobile devices as well as social networking increases the burden on IT to identify and shore up potential attack points.

Managing mayhem.

IT teams have started to fight these threats with disparate network, software and security devices, often purchasing them in piecemeal fashion. For businesses that need reduced complexity and are tight on staff and budget, oversight of such infrastructure is expensive and burdensome, and it can be tough to determine what each solution offers and how they overlap to increase IT security. Even more difficult is gaining control of what is on the network, managing the endpoints, and enforcing security policies. This makes data protection strategies extra challenging to integrate into the business and to manage proactively and efficiently. Other IT teams have tried to implement a PC lockdown policy in which they control endpoint systems to varying degrees, from removing local admin rights to restricting Internet browsing abilities. Unfortunately, a rigid PC lockdown strategy can negatively impact business. For instance, support calls could shift from security issues to usability issues.

To reduce costs and simplify management, Dell provides a multilayered security strategy that features integrated network and security management. To do so, Dell went out into the market and assessed the best approaches to security. The result is a multilayered strategy that integrates best-of-breed expertise from across the industry to protect against the proliferation of threats and to enable reporting and compliance.

Dell's multilayered strategy provides security hardware and software at the network, endpoint and user layers, and offers services to plug gaps in in-house expertise and infrastructure. This cohesive approach provides a uniform, easy-to-manage and cost-effective alternative to bringing in new solutions while also integrating existing purchases.

For instance, the network layer should be the first line of defense to proactively protect network-attached devices from threats. Too often, midsize businesses suffer vulnerabilities at this layer because they are trying to manage separate firewalls, VPN and intrusion prevention systems (IPS). Correlating information from each of these devices is time-consuming and can cause IT to miss the opportunity to stop critical threats. Dell's PowerConnect J-SRX is a router, firewall and VPN appliance that includes a unified threat management suite to protect against viruses, spam and malware. It also features an IPS and intrusion detection system — all in a single enterprise-class network security appliance. That way, IT can consult a single console to set security policies, such as URL and content filtering, and create automated responses when a threat is detected. Some IT teams try to block off any Internet source that may result in endpoint corruption as a part of their PC lockdown strategy. However, this extreme approach often blocks processes that are essential for the day-to-day functions of an organization.

Marrying systems management and IT security.

The endpoint security layer is also a tricky one for midsize companies because the number of devices on the network continues to increase exponentially. Yet, IT still has to ensure that threats that bypassed the secure network are addressed by endpoint security. This is the layer that ensures systems are protected from malware downloaded from the Internet, through email attachments or via USB drives.

To adequately protect the endpoints, IT should intertwine systems management and IT security. They must be a united force against intruders. Traditionally, IT has had to deal with these two tasks separately. IT has had to configure each machine manually and try to avoid the errors that could lead to holes or vulnerabilities. Then, if holes were spotted or patches missed, IT had to go in and rectify the configurations, manually, to bring the machines up to date.

To unify and automate these tasks, Dell recently acquired KACE and the Dell KACE K1000, a systems management appliance. The KACE K1000 Management Appliance enhances endpoint security by identifying and remediating vulnerabilities across end nodes. It helps manage and enforce compliance with company policies across desktops, laptops and servers, reducing the risk of malware, spyware and viruses compromising endpoints.

To start, the K1000 can discover all the resources on the network. It then creates a systems inventory and maps it to standard configurations. If patches are missing or antivirus software is out of date, a machine can be quarantined until these issues are remediated.

The appliance provides patch management for automated and reliable patching of Windows and Mac operating systems as well as a wide range of applications. The K1000 also features security and audit capabilities that enforce security and antivirus settings, disallow the running of specified executables, and quarantine infected machines.

In Tennessee, the City of Columbia was able to save more than 4,100 IT department hours annually using the KACE K1000 Management Appliance to improve physical inventory, patch management, configuration management and service-desk tasks. The city has 300 computers located across multiple offices. Before deploying the KACE appliance, the IT team had no choice but to physically visit each of the computers to carry out routine desktop maintenance such as software distributions, configuration management and patch management.

Rick Harrison, MIS director for the City of Columbia, says many of the systems did not have the latest in patching fixes and therefore they were very vulnerable. The KACE K1000 enabled the city to automate this task and reduce the time spent on patch management by 75 percent, while making the systems more secure.

The KACE appliance also supports OVAL (Open Vulnerability and Assessment Language), the information community standard for vulnerability scanning endorsed by the U.S. Computer Emergency Readiness Team and the Department of Homeland Security. The appliance includes more than 1,700 predefined tests, and new tests are added as they are defined and published. IT can schedule OVAL scans for recurring periods such as daily, weekly, monthly, etc., or trigger the scans manually. The results are easy to interpret as each vulnerability is listed as pass/fail. The list also matches vulnerabilities to machines for rapid remediation.

The Dell KACE K1000 provides an optimal PC lockdown solution by allowing IT teams to assign flexible user privileges so that security and end-user productivity can be maintained. The self-service portal enables organizations to publish approved software titles, license keys, files and scripts that users can access to install applications or configure their systems. Assets from the self-service software portal can be installed by users on the network even if they don't have local admin rights. An integrated service desk seamlessly merges with the system management console so that administrators can view employee requests regarding user privileges and address them from a single location.

Snuffing out danger before it arrives.

Since the Internet is such a large-threat vector, Dell also launched the Dell KACE Secure Browser. The Dell KACE Secure Browser is a virtual instance of an Internet browser application and is isolated from the rest of a user's system. Once installed, all changes made by the browser happen within a virtual container and can be cleared with a single click. IT can further control security by creating whitelists and blacklists to limit the sites a user may visit and what processes the browser is permitted to run.

The Dell KACE Secure Browser can be centrally deployed and managed with the Dell KACE K1000 Management Appliance, providing consolidated endpoint security management for IT.

"Businesses are being attacked day in and day out, 24/7/365, by cyber criminals that are financially motivated," says Barry Hensley, vice president of the Atlanta-based SecureWorks Counter Threat Unit.℠ "Every day, these attackers become more sophisticated and more organized, which is why your security needs to keep getting stronger, too. In Q1 2010, SecureWorks saw 45 percent more vulnerabilities than in Q1 2009, and we, on average, detected and mitigated more than 6,000 security events a day."

In addition to the KACE lineup, Dell offers Trend Micro Worry-Free Business Security to block viruses, POP3 spam and spyware. Trend Micro also performs URL

Dell's multilayered security portfolio of hardware, software and services simplifies IT security and provides protection at the network, endpoint and user layers.

filtering to restrict access to unproductive, offensive or risky sites, and provides continuous protection to the mobile workforce. Customers can manage security through an admin console and extend it to multiple PCs already in the environment. The solution is maintained by Trend Micro's security experts so it doesn't require dedicated hardware or highly skilled IT staff.

Another key piece to Dell's multilayered strategy is user security. Dell and Credant Technologies have teamed up on endpoint-based encryption with remote management for desktops, laptops, devices and USB drives with Credant Mobile Guardian Dell Edition. It includes a management console and provides audit trails for compliance, including proof of end-to-end data security and date stamp of encryption.

The software-based encryption also features one-touch compliance through preset templates that, coupled with the management and audit trails, can provide a safe harbor from liability. In the event that a system with sensitive data is lost or stolen, IT can use the Credant offering to prove through an audit that data on a system was encrypted and rendered unusable.

Supplementing in-house expertise.

Just as important as the hardware and the software that businesses install at various points in the network are the services that they use to supplement in-house capabilities. Midsize businesses that are resource-strapped or lack the time and staff expertise to properly address security can rely on Dell and global security services expert SecureWorks to provide a full range of security services. For instance, they'll help organizations identify and manage security risks and compliance needs. Among the areas they'll assess: PCI, SOX, HIPAA, and regulatory and regional mandates.

Dell and SecureWorks will minimize risks and help ensure compliance using log monitoring, security information management, threat intelligence, vulnerability assessments, and Web and application scanning. Businesses can pick and choose the services that best meet their needs.

Multilayer protection.

While there is bound to be no letup in the number and diversity of threats coming at midsize businesses, they can be prepared with Dell's multilayered security strategy. Deploying hardware, software and services at the network, endpoint and user layers helps readily thwart internal and external attacks. IT also can create an environment that is capable of enforcing policies and handling compliance audits.

Dell's years of delivering IT solutions for small and medium businesses remain unmatched, with a standards-based approach to technology as well as environmental responsibility that have helped businesses everywhere grow and thrive.

Dell is also the top provider to SMBs in the United States and serves SMB customers all over the world.

Dell's multilayered security strategy of integrated devices, sophisticated software and managed services consolidates and simplifies network and security management, including systems management, for midsize businesses. Dell's broad portfolio provides a simple, affordable, flexible and scalable approach to multilayered security.

Sandra Gittlen is a freelance business and technology writer based near Boston.

More Information @

Dell.ie/business/security