Geeknet

sourceforge Slashdot DELL

10 Potential Risk Facing Your IT Department: Multi-layered Security & Network Protection

September 2011

It's common to read stories about security breaches at large enterprises. But big institutions and global brands aren't the only targets – or even the prime targets – of today's computer crime. Today's profit-oriented professional hackers have automated tools enabling attacks on many 'soft' targets with little effort or risk. So smaller businesses are probed for vulnerabilities on an increasingly-frequent basis, and they can make for easy pickings.

Smaller organizations are rarely secured to the same degree as large enterprises. They often lack budget for complex infrastructure and administrative protocols. For logical reasons, they tend to favor IT generalists over security specialists, creating a skills gap in security solution planning and implementation, and a bandwidth gap in management and monitoring. For productivity and cultural reasons, they often have liberal policies for mobility, use of in-office WiFi, installation of unauthorized applications, use of unapproved mobile devices and online services – "technology populism" that brings with it a host of potential vulnerabilities. Many smaller businesses are hard-pressed even to keep up with endpoint, server and asset software patches, so may leave common vulnerabilities in place for exploitation over long periods of time.

In general, SMBs are no match for professional interlopers – from organized crime to rogue nation-states – launching a palette of attacks ranging from email phishing to social engineering to so-called Advanced Persistent Threats. And SMB defenders need to at least try to thwart every possible attack, but attackers only need to find one vulnerability to wreak havoc.

A layered security strategy – overlapping security solutions for VPN, network, servers, data and endpoint device management and policy enforcement – protects assets behind several lines of defense. But a fully-articulated layered security system is something that even large enterprises – with resources and specialized IT talent – are sometimes challenged to deploy. Enterprise-scale solution suites are expensive, complex, and involve many moving parts.

What smaller organizations need is a simplified solution for layered security: where non-specialized IT personnel package core infrastructure pieces for easy installation, configuration, management, and use. Here are ten reasons why such a right sized layered security solution may be the right choice for your business.

- **The Internet is out there (but also in here).** Your business cannot run without the Internet. But most threats to your security originate there – in fact, a recent Symantec study noted that over 98% of threats to confidential information involved remote access; and denial-of-service (DoS) and other transactional attacks typically strike from the 'Net. But it's also wrong to view network security in terms of a simple, "inside vs. outside" model. For example, about a third of incidents reported by SMBs involve insider misuse of network or server access. This is, of course, not all malicious – a guest who hops onto your WiFi or plugs into a spare LAN port is probably just checking their email. But in some cases unauthorized access can become a real threat.

  Zone-based firewalls are the classic answer. Modern firewalls protect against unsponsored traffic, can be used to "black-hole" DoS attacks, and can maintain internal VPN zones that isolate guest network services, and provide controlled access to intranet and application servers. The trouble is that firewalls can be complex and hard to configure – something that SMB layered security solutions take pains to manage by providing intelligent defaults and simple, Wizard-based configuration and management interfaces. The top solutions package core firewall functionality with VPN remote access and content filtering (see below), creating a "one-box" solution that covers a range of threats from inside and outside your organization, and can even offer a secure portal enabling outsourcing and remote intervention by specialized security service providers.

- **Remote access threats.** It's a given that you need to give employees, partners and others access to your network from outside. But the only safe way to do this is via a Virtual Private Network or VPN, which authenticates and encrypts traffic from authorized endpoints to your network edge and provides controlled access to critical assets. Making VPN a part of a high-performance, one-box network security solution makes huge sense: earning economies of scale through sharing of underlying compute, storage, network interface and network-content processing components, and providing a single interface for user-account creation, management, and revocation.

- **Browser threats.** The web is critical to productivity, but browsers represent fairly serious threats to security: they vector malware, carry phishing attempts, enable esoteric remote attacks like Cross-Site Request Forgery and can be compromised to communicate your data or reveal your passwords to bad actors in the outside world. Web filtering, performed at the network edge, provides a bulwark against all these potential threats. But like firewalls, filtering systems can be hard to configure and keep up to date unless they're packaged and maintained as part of a comprehensive network security appliance solution.

- **Email threats.** Email is another classic attack vector for introducing malware, performing phishing and other forms of impersonation for social engineering, and is a common route for abuse and for the improper release (whether voluntary or involuntary) of PII and other regulated information. Email is also the mainstay of compliance, auditing, and proving due diligence under any regulatory regime. So email integrity is essential in managing all forms of business risk. For this reason, it makes sense, even within the context of an otherwise comprehensive layered security plan, to treat email as a special case and give it another layer of protection. The good news is that top-rated email security systems are improving radically, offering malware and spam protection, boundary encryption to protect partner communications, sophisticated administration controls, and end-user-empowering features such as the ability to define and manage whitelists, and tune spam settings within policy guidelines.

- **Vulnerable endpoints.** Laptops, desktops, and mobile devices can be targets for malware, rootkit, and other attack software insertion. Once compromised, the data they contain and the information they transmit becomes accessible to black hats, betraying company and employee security. Keeping endpoint devices protected, however, is a tall order. Safety depends on patching the OS and authorized applications regularly, maintaining antivirus and filtering apps, configuring machines for maximum resilience, and enforcing policies for which apps can be installed, and which can't. Doing this effectively demands automation: the best system management solutions use auto-discovery technologies to help you inventory equipment and track assets; provide and enforce configuration management; perform updates and patches; and insure that security configurations aren't altered by end-users. These are all important parts of the System Management functionality required by a layered security system.

- **OS deployment**. Upgrading desktop and laptop operating systems may be the single most effective move you can make for security – not only because newer operating systems are more secure, but because the upgrade process cleanses systems and provides a change-up point for negotiating new security protocols with users. For this reason, the System Management feature set of a layered security solution should provide an OS deployment facility.

- **Vulnerable browsing.** Despite web filtering, antivirus, and browser security, browser-based transactions always carry some risk of compromise. An effective solution is to deploy proxy browsers in place of standard desktop browsing software: a proxy browser is a virtualized instance – usually of a popular browser such as Firefox – that runs in a controlled 'sandbox' with zero access to host machine storage and other features. The use of virtualization insures that even exploits aimed at the model browser's known vulnerabilities can't be used to compromise your machines or data, or your users' security.

- **Vulnerable data**. Access control and intrusion prevention systems sometimes fail, and no peripheral defense is proof against an 'inside job.' Deep encryption of proprietary and critical files can mitigate this risk and help prevent data loss. Modern, enterprise file-based encryption solutions run transparently, encrypting files in ways that don't inhibit authorized use while protecting them in transit and in storage, both on the company premise and when files are copied to thumb drives or removable media.

- **Late night attacks**. The nature of Advanced Persistent Threats is just that: persistence. Automated attack machines probe for vulnerabilities around the clock, and DoS and other attacks can take place at any hour, a real threat when their goal isn't so much to deny service as to exploit buffer-overrun and other vulnerabilities to compromise your network perimeter. Security monitoring is the answer: a combo of human specialists and automated tools that review real-time network traffic and stay on top of the emerging threat landscape, so they can recognize suspicious activity and intervene before security is breached. Comprehensive SMB layered security solutions may use on-premise equipment to enable remote monitoring and intervention.

- **Endpoint authentication threats.** SMBs commonly use password-only protection for endpoint machines and even for access to critical shared assets. These days that's not enough – passwords are easy to crack, guess, or compromise through 'social engineering,' and compromised endpoint devices can easily become portals for accessing your proprietary information. Good authentication – ideally a two-factor authentication system requiring both a password and a token (i.e., "something you know and something you have") can help solve this problem. But two-factor authentication schemes can be complex, challenging to manage, and difficult for users. A complete layered security solution for SMBs will incorporate several options for improved endpoint and asset/server authentication – the best will support not just dongle and smartcard-based systems, but also biometrics, which may be easier to use and just as secure.