REMOTE-ACCESS LOCKDOWN

Securing user access hinges on realizing that the endpoint is wherever employees plug into the network.

Nearly universal availability of broadband access to the Internet — combined with a huge variety of low-cost, portable computing devices — has untethered the performance of work from a fixed location. Staffers now see remote access and telework as answers to the challenges of productivity, work-life balance, the "greening" imperative and transportation bottlenecks.

Between the workers outside of a corporate location and the information resources housed in the corporate network lies a set of practices and technologies known as remote access. In fact, it is not merely employees who need access. A growing number of organizations now provide Internet-based links for customers, distributors, vendors and contractors.

The trend toward distributed network access creates both benefits and challenges for businesses. It's a practice that brings productivity as well as efficiency to the business cycle. However, one of the biggest challenges is ensuring that remote workers have secure remote access (SRA) to critical systems and information.

Today, remote access involves balancing an array of technologies and end-user access devices with carefully crafted policies. The art of providing external access hinges on protecting a company's enterprise assets while giving maximum flexibility to remote workers who expect their computing experience to be indistinguishable from that of their office-bound colleagues.

THROW AWAY THE KEY:

A time-synchronous, one-time password authenticator can generate a new OTP every 60 seconds.

Source: RSA Security

Potent and Changing

The days when work was considered a place are gone. Over the past few years, improved Internet access and broadband connectivity in more locations, along with technologies such as virtualization, voice over IP (VoIP) telephony and mobile/wireless applications have made it more feasible for people to work from remote locations.

Of course, the security implications of anything involving the Internet make the task of providing remote access a complex one. The cybersecurity threat environment is an always-changing scenario. Experts agree that the principal developments in cyberthreats include:

- Cybercriminals and hackers acting on financial motivations. They seek financial and banking credentials, credit card numbers, passwords and Social Security numbers — anything that can give them the keys to financial intrusion and electronic transfer of funds. "It's the criminalization of the threats," says Sam Curry, chief technology officer for RSA Security. "They are financially and profit motivated, and well-organized."
- Obtaining intellectual property for commercial or national interests, a motivation that is as old as "dumpster diving" itself.
- Organized criminals and, in some cases, nation-states involved in cyberattacks. They have not merely the motivation but also the resources and the time to be persistent.
- A changing means of egress as perimeter detection and intrusion-prevention techniques have become much more effective. This is making the direct attack rare. Still, highly sophisticated, socially engineered phishing and use of rented botnets — resident but dormant on millions of computers — are on the rise.

Adding to the secure remote-access challenge is what Curry and others refer to as the rise of consumer devices and services that users want for enterprise access use. These incude things, for example, like smartphones along with Twitter and Facebook accounts. >>>

The risks that social network services present are hardly confined to end users — be they remote or onsite. After all, Twitter and Facebook have become staples in many corporations' marketing toolkits.

Threat Techniques

Remote-access solutions are subject to a variety of threats. Most of these are independent of the technology used. Remote-access security threats cluster around four salient techniques. These include:

Denial-of-Service (DoS) Attacks: These are typically aimed at high-volume or transactional websites, with the goal of preventing normal and legitimate access. Hackers use several techniques to deny service, including exploitation of bugs in operating systems or misconfigured router ports. Some attacks flood a port with traffic, usurping all available bandwidth. And some malware is adept at occupying all of a processor's cycles

Traffic Analysis: This is a technique with roots originating in signal interception of World War I radio messages but replicated on the Internet. In radio, listeners would detect volume, direction and endpoints of signals to infer enemy plans, even if they couldn't decode the content of the messages. In modern cyberspace, traffic analysis applies the same techniques to packets, using algorithms to glean information about what the packets may signify.

Dictionary Attacks: This form of intrusion is still effective at ferreting out passwords because so many companies fail to enforce strong password policies. This includes requiring a minimum number of characters and the use of characters other then letters. When account lockout is in place — as it should be — these can be run as so-called "low and slow" attacks that may not trigger IDS and log analysis alerts.

Man-in-the-Middle Attacks: These involve a third party inserting itself between two communicating endpoints and, by obtaining their public encryption keys, spoofing messages so the users on either end believe they are communicating directly. MITM active eavesdropping has been used to intercept banking credentials and other sensitive information. The technique can also be used to relay information to another party.

Not precisely an MITM are unauthorized keyloggers. They often download information to knowing users by compromising websites that ferret out in plain text whatever the unknowing victim is typing. Still another more recent variant is the "Man-in-the-Browser," in which malware infects a browser in such a way as to modify web pages or change or intercept transactional information.

And don't overlook a basic security issue with remote users: loss or theft of the devices themselves, especially portable computers with big hard drives that might be stuffed with confidential or personally identifiable information. Scarily, smartphones have more storage with dense memory cards than many notebook computer hard drives did just a few years ago.

All of this is not to say an IT organization can rest when it comes to systematic patch management and perimeter security. Those remain important pieces of any plan for secure remote access. In fact, the number and variety of remote-access devices has made patch management even more important because the IT shop doesn't have 24x7 network (or physical) access to the endpoints.

By the Book

Secure remote access starts with corporate policies. Enforceable policies should govern who has access to what and by what means. Working from a policy makes it easier to plan out the technical strategy for ensuring secure access.

From the policy, the organization creates a concept of what secure remote access should look like. Underlying many of the strategies for carrying out the concept is data encryption. "We never encourage remote access without encryption," says Craig Mathias, an analyst with Farpoint Consulting of Phoenix, Ariz.

With secure remote access, some of the basics still apply even as the threat vectors and technologies change. These include:

- Antivirus software remains an important tool — perhaps more important than ever as social networks and third-party resources for cloud services and Software as a Service (SaaS) become part of corporate network ecosystems.
- Password protection is useful insofar as it goes. But many organizations are adding — or even replacing — traditional passwords with token generators coupled with biometric or smart card tools. This has grown especially common for accessing highly sensitive data.

Another principal strategy of secure remote access may seem obvious, but it bears repeating: strong authentication. The IT team should build in validation so it can assure that an accessing user is in fact an authorized user and that the user's device is certified, Mathias says.

Preventing Data Leakage from Remote Devices

They're every IT professional's security nightmare: smartphones, notebook computers, tiny USB storage devices and tablets chock-full of sensitive corporate data. What if they get lost, stolen or hacked? The world of mobile applications, regardless of the device platform, exposes the corporate network to a very broad and largely uncontrollable system of connections and data.

Rather than try to stem the tide, IT departments have begun establishing policies and applying technologies that enable remote workers to use the devices they love while also ensuring security for corporate data assets.

Some important strategies to adopt:

1. Encrypt data in mobile devices at the hardware level. But also have a policy that users don't put passwords — to the devices or to anything else — in memo files and other insecure places on the devices themselves. Major carriers also offer a service to remotely disable or even wipe a device when it's reported lost or stolen. Also be sure to retrieve the old device when a user obtains a new one. IT doesn't need to confiscate the old one, just be sure that it is cleansed to its out-of-the-box state.
2. Restrict network access from portable devices to a secure sockets layer virtual private network (SSL VPN). Be sure to scan all traffic, whether from a smart phone or computer, for malware. Keyloggers, sniffers, botnets and the like can be transmitted by any of these devices, not just PCs.
3. Control use of USB devices. Configure ports to recognize only IT-issued devices, and issue only those with built-in encryption.
4. Consider full-disk encryption for notebook computers, coupled with comprehensive key management.
5. Don't attempt to support every device. Limit corporate support to the three most popular platforms among your users: for example, RIM Blackberry, Motorola/HTC Android and Apple iPhone.

You don't want authorized users logging in with an unknown device riddled with malware, such as someone's five-year-old home PC. Further, you don't want an authorized device to grant access to a thief. "Strong authentication plus encryption — it's a matter of what resources each user is given access to on the network," Mathias adds.

Encryption begins with the channel of communication between the end user and the enterprise network. That's why secure sockets layer virtual private networks (SSL VPN) "are the next-generation of remote access to trusted and untrusted devices," says Matthew Dieckman, product line manager for secure remote-access solutions at SonicWALL. "SSL VPNs allow companies to manage employees, customers and suppliers."

Dieckman adds that SSL VPNs have grown in popularity over Internet Protocol Security (IPSec) VPNs because the former don't require the user to have a thick client, which allows more flexibility in the ways that users gain access to the network. Plus, network administrators can more easily fine-tune which users have access to which particular network assets, he adds.

IT departments typically work in a universe of trusted and untrusted devices. However, it's much harder to control when users tap into the network remotely, Dieckman says.

Trusted devices are basically those issued by the IT department, whether notebook PCs or smartphones. But, much access comes from untrusted devices such as public web portals. You may want to restrict access to less critical resources but still positively identify the users.

Given this reality, the first task for a secure VPN is identifying the endpoint. Products such as SonicWALL's Aventail Smart Access are capable of challenging remote clients to determine whether, for example, a firewall or antivirus software is installed and if the versions are up-to-date.

Trusted devices can be remotely verified via their serial numbers or client certificates assigned by IT. This information is then used to control the applications to which the device is granted access.

Other SSL VPN capabilities, to promote secure access, include "cache cleaning" of untrusted endpoints, so that all temporary files in the browser are cleared after a user logs off. Also growing in importance is the virtual desktop environment, which places the remote user in a secure container that prevents local storage of data.

Judicious Encryption

Full-disk encryption of portable devices, and full encryption of data at rest, including backup, might sound tempting if your goal is to create a fortress. But they also carry problems, including sometimes tricky procedures for users, according to RSA's Curry.

"If you encrypt the drive and lose the key, the drive is lost," he says. Moreover, even with everything encrypted, cybercriminals will simply look for a way to nab the passwords rather than crack the encryption. Beyond that, large enterprises that might be the targets of state-sponsored cybermischief face adversaries who have the time and resources to crack even strong encryption. "Nothing is impossible," Curry says.

"The issue is management of your key infrastructure — how are the keys stored and what are the access policies," he adds. On top of that, you need to constantly review your policies and practices in a risk-management framework.

A risk-management approach extends to firewalls, which have evolved from basing their rules on sources of access to rules based on data types. That would mean, for example, that Social Security or credit card numbers would be visible only to specific applications and users. Curry says that with time such rules "can become part of the fabric of an organization." ◊