TechTarget

E-Guide

Secure Remote Access Tools and Techniques

Vendor neutral tips on assessing and implementing remote access software and best practices

Implementing effective remote access technologies *is a good first step in rethinking remote access control for your on-the-go mobile workforce, but how do you determine which tools will deliver the flexibility your users require without sacrificing security? And once you've made a purchase, how do you go about applying these tools to your own environment?*

Luckily, inside this exclusive guide, our experts provide key criteria to utilize when evaluating remote desktop access software and explore essential tips on leveraging that software as part of an effective remote access security strategy.

Contents

Remote access audit: Assessing remote desktop access software

By Randall Gamby, Contributor

In light of recent security issues involving remote desktop access software, we've been asked to audit the authentication capabilities of any remote access software used in our organization. What's your advice in terms of drawing conclusions on what is or isn't acceptable, especially since any application that fails would simply be banned?

This is a difficult question to answer because there are many determining factors in drawing a conclusion on whether to allow remote desktop access.

Before you proceed with a remote access audit, you must initially answer two questions that will influence any conclusion. First, what is the value for workers to have the ability to remotely connect to their desktops when away from the office? In the past, organizations have struggled to determine this number, but an estimate must be decided upon before proceeding. While it is

obvious that there is value for a worker to be able to get to files and applications while remote, it's hard to determine if it is worth the risk of exposure.

This leads into the second question: Is the risk of data exposure during remote access greater than the value of the data itself? If a worker has remote access to financial, PHI, intellectual property or other highly sensitive information, then the risk of data loss, severely damaging the organization's reputation, or even loss of customer confidence may override the convenience and/or necessity of using remote desktop access software.

Once it's been determined that the value of remote access is worth the risk, an organization can then evaluate the authentication capabilities and other mitigating controls along this same value curve. For example, an evaluation of an organization's remote access security should contain these parameters:

- **The level of authentication to be used** -- Username/password, two-factor authentication, biometrics, and the like.
- **Other risk-mitigation factors** -- Geo-tracking, workstation setup, current antivirus signatures installed, and so on.
- **Trustworthiness of the employee** -- Background checks have been run on key executives.
- **Days/times authorized for access** -- Times/dates are valid for executing remote access.

Once these parameters have been assigned a value it is then possible to derive a conclusion by adding the risk and data value and subtracting the mitigating controls from the sum. While this may sound like a strong practical evaluation, the values and variances will be subject to a certain modicum of subjectivity that only the organization can assess.

Contents

Tips for enforcing remote access security policies

By Christina Torode, Editorial Director

Contents

Scott Crawford, a security veteran and research director at Enterprise Management Associates Inc. in Boulder, Colo., explains how CIOs can prevent users from sidestepping remote access security policies and lays out the technology paths CIOs can take to securely manage mobile devices.

SearchCIO.com: How should CIOs start determining their requirements in order to develop their remote access security policies?
Crawford: You need to be aware of not only where that data resides, but also how it can be accessed and how it moves throughout your IT organization. That will help you identify where you need to place your emphasis. You'll have a better idea for taking a look at where it's accessed from and by what kinds of endpoints. It will give you use-case scenarios that will help you determine what an appropriate policy would be. Then you can start evaluating the technology that would help you solve those problems.

You need insight into how things are moving around in your organization. Are people paying attention to that?
Well, that is part of the fuel for the adoption of DLP [data loss prevention] technologies going back a few years now -- the fact that there was so much content moving around the organization, inside the organization, to employees, to business partners, to organizations that have no relationship with the enterprise. How do we get a handle on that? DLP gives you visibility into that activity, but it has its limits. It's really good for identifying highly structured data like account numbers; it faces some really serious challenges when it comes to unstructured data.

How can the IT department stop users from sidestepping remote access security policies?
You can start with the most common use cases that you encounter as a starting point. Email would likely be the first. This is not to say that DLP [tools are] a silver bullet; it means you need to have insight into how content moves in your organization. There are also the paths of egress to consider for how data leaves and falls into the wrong hands. The mobile issue does exacerbate that. The point is that you have to consider, first, just the sheer number of these devices and the things people want access to from them.

And, by the way, you're probably not going to get extra head count just to deal with consumer devices appearing in large numbers in your organization.

Another typical path of egress is access to the application itself, and that's where you can exert some more control. Access to the network, as a means of accessing other resources, obviously would give you pretty broad access to a wide range of things within the environment, but not all access is equal from a mobile device. Most [mobile devices] have a browser, of course, but that begs the question of how are you enabling access to Web applications in the first place. So, mobile may be the catalyst for a lot of this, but it's not as if mobile is the only thing to consider.

What approaches are you seeing for BYOD [bring-your-own-device] programs?
There are vendors that can really enable a BYOD strategy and give an organization a lot of latitude over what people are allowed to bring in or access. The vendors in the VDI [virtual desktop infrastructure] space, that's one of their big talking points. If you use VDI technology, the data doesn't find its way to the endpoint.

When people are getting to the point of choosing a technology for remote access security, what is your advice?
People are torn over whether to get into mobile device management for this, or if it's OK to just take a containerized approach to enterprise applications or applications that would be a point of sensitivity. In other words, you can isolate these applications and give the mobile user access to the business content, but can you also protect them from unwanted or malicious interaction with other apps or the mobile device itself. Virtualization technology is one way to deal with it, but there are existing container approaches in the market today. There's also some NAC [network access control] players who have deep insight into really granular, policy-based control on access to a network environment where mobile is a factor.

Contents

Remote access security controls for a mobile world

By Christina Torode, Editorial Director

Contents

As a 15-year security veteran, Scott Crawford witnessed the remote access security panic CIOs experienced when Wi-Fi came onto the scene. The same is happening in the bring-your-own-device (BYOD) era. Crawford, a research director at Enterprise Management Associates Inc. in Boulder, Colo., recently explained to SearchCIO.com why some tried-and-true security measures remain relevant, and why mobile devices have led to newer network access security measures.

SearchCIO.com: How can CIOs maintain control over network remote access security in a BYOD era?

Crawford: We've kind of been down this road before in the enterprise. When Wi-Fi was starting to be a big issue, access was coming in on consumer devices and becoming a standard part of laptops. It wasn't too hard to set up consumer gear that would give you wireless access to a wired network, and everyone was tearing their hair out, saying, "This is the end of the world for control over our network."

But we got to a point where we reached some dynamic equilibrium around this notion of control. To some extent, I expect the BYOD trend is going to be somewhat like that in the enterprise.

But there are some very distinct differences. The real issue, in a lot of cases, is this tremendous influx of very consumer-oriented devices. They're being provided by vendors who have not historically shown all that much interest in enterprise manageability for those devices. At the same time, a lot of the [consumer devices] adhere to a very different security model from authorized traditional enterprise endpoints, so things like sandboxing are a native aspect of applications for a lot of these [mobile] platforms. They incorporate this notion of application prominence through application distribution channels like app stores. There are some things that we never had on traditional endpoints that we have in this mobile world, so in some respects there are some advantages to these [consumer devices].

Contents

What remote access security policies and technologies for the corporate network can CIOs put in place for mobile devices, while still giving users flexibility?

There are remote access control technologies that can give organizations a lot more granular insight into the context of access, which can be really valuable. You may be able to display this data remotely via Web applications, but you don't want to send the data itself down to the endpoint in the form of content, like a spreadsheet or a document. So, there are technologies that enable you to determine the context of access: Where is this device connecting from? What kind of device is it, and what kind of control do I have over this device? If it's wholly owned by the consumer, the business may not want to get into the business of managing that mobile device, but they may be interested in containers for the application that isolate that application from other activity on that endpoint.

Another approach is not sending the data down at all. You may want to use endpoint virtualization to do the execute and even the display of the data in the data center, and what is sent down to the user is a representation, not the actual content itself. There are techniques that can determine the context of access -- the type of device, where it's accessing from, who the user is, [whether it's] legitimate access to this data or application -- and use those techniques to begin to build a policy around what is and what is not appropriate for these devices, which are usually not managed, period.

Should enterprises build a separate wireless network for mobile device access?

It depends on what's the need for protection and policy and control. Do you have compliance concerns that you have to meet, such as PCI, that would have some specific requirements? Is there a technique that would take certain aspects of the environment out of scope for the requirements of PCI? These are the things you have to consider before you consider what architectural solution would be best for you. The advantage of a segmented network is that you can isolate that activity on the network and provide a point of control at any point where that network connects with other networks, which in turn connects to sensitive resource that might be a target.

Contents

Secure remote access? Security-related remote access problems abound

By Eric B. Parizo, Senior Site Editor

An attacker seeking to penetrate an enterprise's defenses typically has many "easy" options to choose from: unpatched Windows machines, website cross-site scripting flaws, or social engineering against employees.

So it's impossible to ignore the irony that enterprise remote access services -- technologies constructed to provide authorized employees and partners with managed, secure remote access to corporate networks and data -- have become one of the most exploited IT resources in use today.

For the information security industry, it's disheartening. Many enterprises, large and small, have made huge investments in remote access services, but recent findings suggest these technologies come with a variety of inherent problems and few easy answers.

The most recent and perhaps most powerful evidence of remote access problems comes in the 2012 Verizon Data Breach Investigations Report, the industry bellwether for data breach trends. Verizon found that in 2011, remote access services were involved in 88% of all hacking breaches in its data set, and of all the reported incidents involving malware last year, compromised remote access paved the way for infections 95% of the time.

In the DBIR, Verizon references remote access services such as Virtual Network Computing (VNC) and Remote Desktop Protocol (RDP), but the remote access security problem is far broader. Consider the following:

- Many enterprises permit (or fail to regulate) the use of third-party file storage services to facilitate remote access to data, but when files end up in cloud-based repositories, enterprises lose control. When Dropbox left user accounts wide open last June without realizing it, it's likely many ad-hoc enterprise data repositories were exposed.
- Screen sharing and remote administration software weaknesses are an increasing concern. A 2011 report from Trustwave found remote

Contents

management software was one of the most commonly used attack vectors. And good luck to anyone using Symantec Corp.'s Norton pcAnywhere software; the ambiguous technical document released last month does little to assuage fears that the product has been completely compromised in the wake of Big Yellow's 2006 source code breach. Plus, recent research by Rapid7 CSO HD Moore found thousands of systems using pcAnywhere with open ports that could be accessed by an attacker.

- VPNs risks can't be ignored either. Trustwave also found a VPN or similar remote access method was exploited in more than half of the data breaches it investigated last year. Few though were as devastating and public as the Gucci network attack, in which a former employee used a VPN connection to wreak network havoc from afar.

Insecure or insecurely used remote access technologies – mechanisms that most security teams assume pose little risk – in reality offer an abundance of options for attackers to infiltrate enterprises.

"The biggest concern is that attackers will exploit that remote access connection as a jumping-off point, a hop along the way, to get deeper into an organization," said Chris Hopen, co-founder of TappIn, a secure file-sharing vendor. Few understand remote access better than Hopen, one of the inventors of the SSL VPN and CTO and co-founder of VPN pioneer Aventail, which was acquired in 2007 by SonicWall.

What's confounding, said Hopen, is that the largest underlying problem with remote access technologies isn't with remote access; it's poor identity validation and weak authentication.

"There have been so many purported solutions to this end-user identity and authentication challenge over the years, with millions and millions of dollars spent," Hopen said. "We've never found a solution people could live with that's cost-effective and adds an enhanced layer of security over traditional passwords. To me, that kicks me in the stomach."

Contents

The problem is more acutely felt in small and midsize businesses, especially those that operate point-of-sale (PoS) systems. As Verizon's 2012 DBIR points out, SMBs have proven highly vulnerable because they commonly outsource PoS management to third-party solution providers, many of which fail to properly secure the remote access technologies they use to "help" their customers.

"The message I've been trying to get out there is, if you're a VAR or reseller providing that service, it's to your competitive advantage to have security be in the upper tier of your priorities," said Ed Moyle, co-founder of Amherst, N.H.-based consultancy SecurityCurve and a former PCI DSS QSA.

He said this year's DBIR should serve as an opportunity for solution providers to reach out to their SMB customers to talk about these kinds of security problems and ways to improve them.Moyle stressed security fundamentals to keep remote access usage in check, such as monitoring for remote access system traffic that isn't being transmitted over HTTP, and restricting admin rights on workstations. "It's not a panacea," Moyle said. "It's something everyone already knows about, but few actually do it."

Hopen said organizations should consider emerging security products that offer enhanced forensic analysis and directory and data monitoring capabilities to better detect when remote access technologies are being used in support of an attack. However, even with better supplemental security products, he said enterprises must shift more of the responsibility for proper use of remote access products to their end users.

"You've got to have better solutions to drive up productivity while mitigating and managing risk," Hopen said, "but I think end users who are given access to these services are a big part of the equation in enhancing and maintaining trust."

Contents

Free resources for technology professionals

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

Related TechTarget Websites

SearchConsumerization

SearchMobileComputing

SearchSecurity