远程访问安全

远程访问安全

在有些时候，你可能需要有远程用户连接到你的网络上。远程计算在生产力和环境上有些得到证明的优势，但是并不是没有缺点——大部分的时候以信息安全风险的形式出现。如果远程用户的电脑感染了病毒或者他们在不安全对的无线连接上传送敏感的电子邮件和即时消息时， 会发生什么事儿呢？当没有受到练好保护的系统连接到你的网络上会怎么样呢？这些网络可以为任何想要恶意进入或者试图进入的人提供直接的入站连接。管理安全远程访问是一项艰难的工作。因为远程系统可能直接和互联网连接，而不是通过企业防火墙，这就增加了你的网络环境的危险。

远程访问威胁

对于移动员工而言，有很多种远程访问的解决方案。SSl VPN 是一种基于 Web 的 VPN 设备。还有不同类型的 Webmail，以及 Outlook Web Access。Citrix 等较大的功能还有安全网关。经典的 IPsec VPN，以及各种不同类型的入口、企业内网和外延网也可以用于移动计算。然而，这种移动通信模式上的漏洞是很明显的。除了恶意代码的一般危胁，这些计算机没有任何物理访问限制。

- ❖ 远程访问和攻击

远程访问策略

管理安全远程访问是一项艰难的工作。因为远程系统可能直接和互联网连接，而不是通过企业防火墙，这就增加了你的网络环境的危险。病毒和间谍软件防御，以及通用 VPN 网络策略并不足以保护这些系统——和他们连接的网络——的安全。本部分将介绍提供安全的远程访问的五个最佳的做法。

- ❖ 安全远程访问的五点策略

- 远程访问与便携设备数据保护策略的制定

远程访问控制

网络访问中普遍存在的安全错误是将网络和应用程序视为从来都不会互相作用的不同实体。你可能会让不同的人来维护、使用不同的安全策略、不同的程序等等。在保护这些服务器上数据的完整性方面，强化 Windows 服务器会大有帮助，但是你也必须要强化网络基础设施本身。本部分将介绍可以采取的五个步骤。

- 控制网络访问的五个步骤

远程访问中的企业

家庭用户感染了互联网病毒，然后和公司网络建立 VPN 连接，受到感染的家庭系统就成为内部网络的扩散源——散步恶意代码以及绕过你的边界防御，包括互联网防火墙。而目前，很多企业都没有适当地解决通过远程电脑感染恶意代码的潜在威胁。

- 预防恶意软件危及远程用户
- 使用远程接入工具访问系统是否安全?

远程访问用户

当远程用户连接到你的网络上时，可能发生很多恶劣的事情，例如对信息的未授权访问、信息泄露，并且总是可能有恶意软件深入到你的网络边界中。本部分提供了远程用户可以采取的一些安全措施。

- 远程用户安全清单
- 个人计算机访问远程网络

远程访问和攻击

对于移动员工而言，有很多种远程访问的解决方案。SSl VPN 是一种基于 Web 的 VPN 设备。还有不同类型的 Webmail，以及 Outlook Web Access。Citrix 等较大的功能还有安全网关。经典的 IPsec VPN，以及各种不同类型的入口、企业内网和外延网也可以用于移动计算。

不管用什么方法，所有的远程反问共有的特性是它是端点计算机，而且和互联网上的其他任何系统一样容易受到攻击。在有些情况下，他们是管理计算机——公司发布的由企业 IT 部门管理的资产。而这些企业 IT 部门拥有提供安全项目的所有企业安全。

企业的资源可以从任何位置访问，而这些位置中的大部分都不足以信任。这里存在的危险非常严重，因为任意位置的移动计算环境可以在任何位置和不受管理的系统上。厂商了解这种安全威胁，而且他们也越来越推荐配置不同类型的安全和扫描技术。问题是大部分的安全技术都不能简单地配置。杀毒软件是个很大的应用，所以让每个远程登录的人下载这样的软件，然后再他们访问电子邮件之前先进行半个小时的扫描，这样做不现实。“不受管理的空间”的杀毒类型的技术必须是行动的、小型的、快速而可处理的。有一些正出现在市场上。

然而，这种移动通信模式上的漏洞是很明显的。除了恶意代码的一般危胁，这些计算机没有任何物理访问限制。任何人都可以上传他们向要上传的内容（无论有没有连接网络，击键的风险都很大）。一个人可以在使用之前可能需要漫游五分钟，而在使用后也需要五分钟，而且可以捕捉在这两个时间点之间在计算机上所作的一切。

恶意代码的威胁在这种不受管理的计算机上的威胁更大。有时，使用 IPsec VPN 的人会觉得安全，因为这种技术可以阻止隧道分离（当 VPN 正在连接时，两个或者更多的应用同时进行的功能）。阻止隧道分离只能产生假想的安全。

反连接的特洛伊木马在这种环境中的功能和它在企业环境中的共嫩一样，都是从里到外的顺序开始的。所以，如果用户可以看到互联网，那么也可以看到恶意代码。甚至没有互联网访问，恶意代码可以被写入，进而当在任何时候它可以重新在线时，进行窃取或者完成动作。无论周围环境的防御如何，恶意代码可以在任何环境中获得成功。所有环境中的防御可以做的是减少攻击的类型，而不能阻止攻击。

(作者：Larstan Publishing 译者：Tina Guo 来源：TechTarget 中国)

安全远程访问的五点策略

管理安全远程访问是一项艰难的工作。因为远程系统可能直接和互联网连接，而不是通过企业防火墙，这就增加了你的网络环境的危险。病毒和间谍软件防御，以及通用 VPN 网络策略并不足以保护这些系统——和他们连接的网络——的安全。本文，TechTarget 中国的特约专家将介绍提供安全的远程访问的五个最佳的做法。

1．软件控制策略

创建可以确定远程访问系统上必须存在的准确的安全软件控制的策略。例如，你可能需要阐明杀毒软件、反间谍软件和桌面防火墙必须以某种特定的方式安装和配置最新的特征库，以及厂商可以接受的部分。最好的做法是把策略和连接设置或者对终端用户而言相似的指导分配在一起。通常零容忍政策对端点安全是最好的。在连接到网络之前，终端用户应该满足一套指导方针的要求。没有杀毒软件、反间谍软件和桌面防火墙吗？那么也不允许远程访问，这个策略还应该阐明这个系统上的哪些端口和服务应该公开。

2．端点安全管理

选择一个提供把综合端点安全管理和策略实施作为他们的 VPN 或者远程访问解决方案的厂商。最好给使用企业支持的 VPN 客户端的远程用户授权。这是你可以找到的真正的策略遵从以及确保端点安全状态的唯一方法。你选择的远程访问解决方案应该可以拒绝不满足策略遵从检查的对端点系统的连接。理想的情况是，这个解决方案应该改告知终端用户那一项不符合策略的要求，这样他们就可以跳在再次连接前进行调整。这可以减轻服务台的呼叫负担。

3．实施企业策略遵从

告知终端用户，当他们连接到企业网络时，企业安全策略就会扩展到他们的远程桌面。例如，在连接到企业网络时，不能共享文件，也不能允许其他使用。

4．报告功能

终端用户的策略遵从非常关键。上面提到的大部分的解决方案都提供了报告功能，可以保持管理总是更新到连接端点的状态。根据你必须管理的用户数量，当一台很明显不遵从法规的计算机试图连接的时候，设置邮件管理警报是很明智的做法。在有些情况下，管理干预可能是很合理的——特别是当存在其他网络访问方式的时候。

5.定期查看策略和报告

每隔几个月，查看一下策略和保护，确定违反策略的访问的趋势和方式。这对于确保策略和技术控制可以解决你的远程访问安全需求是很重要的。如果你发现了违反策略的访问，就可以相应地增加或者修改策略。

（作者：George Wrenn 译者：Tina Guo 来源：TechTarget 中国）

远程访问与便携设备数据保护策略的制定

问：区分远程访问策略和便携设备数据保护策略的最好方法是什么？

答：远程访问与便携设备的数据保护这两个策略有着非常不同的侧重：

远程访问策略重点在于强调一下的几点概念：

针对以下对象，使远程链接标准化：

* 任何类型的系统，不论是企业型的还是针对个人用户，PDAs, smart 电话, 笔记本电脑, Blackberries 等等

* 用户类型(雇员，销售商，承包人，合伙人，股东，等等)

* 链接类型：dial-in 调制解调, 帧中继, ISDN, DSL, VPN, SSH,以及 缆线调制解调

远程访问仅仅能够执行基于企业的功能：

* 减少未经授权的对于公司资源的运用

* 连接以及加密的要求

* VPN, SSL, SSH 以及对于敏感数据的加密

雇员还要保证：

* 其家庭成员不能干涉公司制度

* 防病毒软件，补丁等定期升级

* 安置个人防火墙，并受到合理监控

* 个人验证信息不能够分享使用

* 系统不能够与非本公司或本公司员工的网络进行连接

* 不得使用非本公司的电子邮件系统

* 不得使用未经核准的硬件设备

* 密码，一次性密码，个人锁匙等

而一个便携式数据保护策略则是指以下的概念：

针对以下对象，使远程链接标准化：

* 笔记本电脑，Tablet PCs, Palm Pilots, Microsoft Pocket PCs (使用的是 Windows CE), text pagers, smart 电话, FireWire 设备, USB 驱动器

* 用户类型(雇员，销售商，承包人，合伙人，股东，等等)

* 链接类型：远程网络，LAN, WAN, 无限网等等

使用许可

* 有摄像头的 Smart 电话在一些情况下被禁止性用

* 分类的数据必须在传输过程中被加密

* 可以使用可移动设备的人员：

* 只有主管人员才能够使用并且在系统上连接 Blackberry 设备

* 不同的设备需要不同的安全软件

* 附加的安全软件应当被合理地安装

资产管理

* 公司所有的可移动设备必须被标记并且登记
* 用户在进行设备连接之前必须进行登记
* 可移动设备不得随意放置
* 公共网络只得允许从 Internet 进入可移动设备
* 当设备易主之前，必须删除设备内所有敏感数据。
* 减少未经授权的用户使用公司资源

连接以及加密要求：

要对敏感数据实施 VPN, SSL, SSH 和加密

员工必须做到：

* 防病毒软件，补丁等定期升级
* 安装个人防火墙，并适时监控
* 个人验证信息不能共享
* 系统不能够与非本公司或本公司员工的网络进行连接
* 不得使用非本公司的电子邮件系统
* 不得使用未经核准的硬件设备

* 密码，一次性密码，个人锁匙等

（作者：Shon Harris　来源：TechTarget 中国）

控制网络访问的五个步骤

在第一部分中，我解释了处理网络消除边界的关键之处并非取消网络外围，但是不得承认，网络外围存在诸多漏洞，你必须采取措施，以保护数据的安全，防止恶意信息流通过网络外围。在第二部分中涵盖了强化 Windows 的几个步骤，此外，这里，我们将关注确保网络基础设施安全的步骤。

一个普遍存在的安全错误是将网络和应用程序视为从来都不会互相作用的不同实体。你可能会让不同的人来维护、使用不同的安全策略、不同的程序等等。在保护这些服务器上数据的完整性方面，强化 Windows 服务器会大有帮助，但是你也必须要强化网络基础设施本身。首先采取如下五个步骤。

1．执行访问控制列表（ACLs）

如果有些人可以进入你网络的内部，那么他们就可以获得你的 Windows 系统的访问权。你需要在你的网络设备上执行严格的访问控制列表，并且只对那些需要的用户授予访问权。比如，休斯顿的用户是否需要访问纽约的系统呢？如果不需要，这些系统之间通过信息流的可能性对于业务来说并不是必要的。

2．执行基于网络的访问控制（NBAC）

将系统连接到网络过去常常是件麻烦事：你必须构建网络驱动程序、分配地址、并在物理上连接各个系统，进而使得它们可以对话。尽管这使得未经授权的系统要想容易地连接到网络变得极其困难，但是它却导致了过多的管理费用。然后，像星型连环状网络和动态主机配置协议（DHCP）等技术使得将系统连接到网络变得尤其简单。起初我很高兴。但现在，我意识到任何人都可以连接到网络上。实际上，我所访问过的大约 90%的客户都配备有活动的网络插孔，我很容易就可以插入，并获得网络访问权，如果他们有一些书面的策略，表明未经授权的连接是不允许的。

NBAC 旨在提供一个执行机制来支持这些书面的策略。有了 NBAC，你就可以界定什么是授权用户，并且确保所连接的系统正在运行合适的补丁和软件版本。如果没有运行合适的补丁和软件，就会将其安置在检疫状态，直到系统经过了修补和升级。

3．限制远程连接

执行 VPN 是一个冒险的尝试。它允许用户和病毒都可以访问网络。不要允许 VPN 访问你的整个网络，而要执行网络访问控制列表，限制仅使远程用户可以访问服务器和他们所需要的资源。比如，使用 VPN 来连接到 Citrix 或者终端服务器机房，以确保唯一允许通过 VPN 的信息流是通往 Citrix 服务器的 Citrix 信息流；如果某个远程客户的系统受到感染，它将不会感染你的网络。

4．限制并保护无线连接

如果在你的放火墙后面执行访问控制，无线局域网连接给你的网络外围带来了一个特别大的、敞开的漏洞。因此，创建你的无线局域网连接应当像任何其它远程连接一样：在放火墙外部终止它们，并在访问内部资源和受保护资源时，要求 VPN 连接。

5．执行 IPsec

在你的网络上执行 IPsec 是保护数据在传输过程中不受到威胁的一种不错的方式。但是它也并非灵丹妙药。比如，如果某个计算机受到了 Slammer 的感染，那么在信息传输之前，IPsec 仅能确保 Slammer 信息流是经过加密的。然而，当与其它强化方法一起使用时，IPsec 可以作为保护你的内部流量免于受到窥探的有效方法。

结论

由于网络消除了边界，你就不能再完全依靠网络外围来保护系统和数据。全部去除网络边界并不是解决方法，只强化外围也不行。你必须同时强化你的 Windows 系统和网络基础设施，网络边界不能起到保护作用，或者被规避绕开时，保护数据。

(作者：Wes Noonan 译者：李娜娜 来源：TechTarget 中国)

预防恶意软件危及远程用户

你认为你的恶意软件防御已经很正常了，对吗？有了邮件网关的杀毒工具了？检查一下吧。公司拥有的桌面电脑和笔记本电脑都配置杀毒软件了？检查一下。对于在笔记本、家用电脑上，甚至是手持设备上使用 VPN 的受感染的远程电脑有了全面的恶意软件防御了吗?

令人伤心的是，现在很多机构都没有适当地解决通过远程电脑感染恶意代码的潜在威胁。通常，家庭用户感染了互联网病毒，然后和公司网络建立 VPN 连接，受到感染的家庭系统就成为内部网络的扩散源——散步恶意代码以及绕过你的边界防御，包括互联网防火墙。在你的环境中，如何避免这种烦恼呢？这种解决方案需要策略，也需要技术。

确保要详细说明策略，要求家庭用户更新他们系统上安装的杀毒工具，不管计算机的所有者是用户还是公司。在现在每天都有新蠕虫的环境中，要求杀毒工具配置成每天自动下载新的特征，并且明确关闭杀毒工具时的详细后果，以及它的更新功能。

还有，策略要详细说明公司有权利搜索网络的任何 VPN 用户，也是不管计算机的所有者是用户还是公司。使用提示框，在 VPN 登录的时候，要求用户点击“确定”，了解当事故发生时，他们的个人系统可以被远程搜索到。从系统的所有者——员工那里获得许可，允许你的事故回应组合法的进行分析，进而解决问题。没有这个策略和提示框，你就不能搜索员工所有的计算机。此外，你也可以创建这样的策略：只允许企业拥有的电脑访问 VPN。当然，你的公司需要为所有的远程用户购买计算机，所以要确定预算可以支持你选的这条路。

幸运的是，很多 VPN 网关现在提供了向客户端询问，进而确定主机系统在运行每天更新病毒库的活跃杀毒工具和个人防火墙。如果你的基础架构支持，就可以激活这些功能；想要访问公司工作区的用户首先必须证明他们没有感染其他病毒。还有，确保你的 VPN 网

关把所有流量都通过执行全面过滤的防火墙——只允许访问完全需要的服务，以及每个单独的远程用户需要的服务器。此外，考虑配置网络监控工具，包括基于网络的入侵检测和入侵防御系统，配置在和 VPN 以及过滤设备连接的网段上——这样你就可以及早检测并避开攻击。

（作者：Ed Skoudis 译者：Tina Guo 来源：TechTarget 中国）

使用远程接入工具访问系统是否安全?

问：使用远程接入控制工具对 Windows 文件许可或共享有什么影响?可以通过远程接入工具登录服务器为用户提供与通过物理登陆的用户相同的权限或许可吗?服务器上的文件能被修改吗?

答：远程接入工具对于 Windows 文件许可和共享没有任何影响。用户将有同样的权限或许可，就像他们真正在服务器前一样。因此，服务器上的文件也是可以被修改。

有两种类型的远程接入工具：软件工具和托管服务。软件工具要求主机和远程计算机都安装这个应用程序。这些软件工具包括赛门铁克公司的 pcAnywhere、开源软件的 RealVNC 和 Windows 远程桌面。

另一方面，托管服务是基于订购的。在注册主机之后，用户可以从任何地方使用任何浏览器登录到服务网站访问他们的主机计算机。由于托管服务是基于网络的，他们不需要在远程计算机安装软件。托管的解决方案包括 GoToMyPC 和 LogMeIn。

无论是软件的还是基于网络的，这些工具的主要目的是提供从多个地方访问系统的全部功能。对于安全来说，托管服务使用 SSL。软件工具使用各种身份识别方案防止未经过授权的访问。

除此之外，最好的忠告是使用与你物理访问服务器相同的 Windows 文件和共享的保护措施。在本地把关于文件权限和许可设置在你要求的水平，仅允许获得批准的组或者个人访问。

(作者：Joel Dubin 来源：TechTarget 中国)

远程用户安全清单

在有些时候，你可能需要有远程用户连接到你的网络上。远程计算在生产力和环境上有些得到证明的优势，但是并不是没有缺点——大部分的时候以信息安全风险的形式出现。如果远程用户的电脑感染了病毒或者他们在不安全对的无线连接上传送敏感的电子邮件和即时消息时， 会发生什么事儿呢？当没有受到练好保护的系统连接到你的网络上会怎么样呢？这些网络可以为任何想要恶意进入或者试图进入的人提供直接的入站连接。

可以证明可能发生很多恶劣的事情。会发生对信息的未授权访问、信息泄露、并且总是可能恶意软件深入到你的网络边界中。

在你创建新的策略或者锁定你的远程系统前，决定目前你的系统中存在什么远程访问漏洞。这样做不仅可以发现还没有打的补丁，而且更进一步发现错误的配置、不必须的共享、空余的连接和其他你不容易发现的攻击漏洞。我建议你使用一个漏洞评估工具，例如 Tenable Network Security 的 NeWT、GFI Software Ltd。的 LANguard Network Security Scanner (我最喜欢的低成本扫描器)、 Qualys Inc。的 QualysGuard (我最喜欢的全面扫描器)。

在笔记本或者桌面电脑上的内部支持的图像上，使用这些中的一个（或多个）工具，如果有意义，也要测试你的用户用户的远程系统。如果后者不是政治或者资源限制的原因的选择，你就可以把这些指导存储起来，这样你的远程用户就可以自己做了。考虑在他们的系统上安装他们，并运行微软基线安全分析器（Microsoft Baseline Security Analyzer ，MBSA），并且把报告和你共享。 你甚至可以通过 Windows 上的登录脚本和/或组策略使这一过程自动化。记住，有很多原因必须保护公司的资产。

一旦你决定了你的弱点存在在哪里，并且解决了这个问题，使用下面的清单，包括常用以及不常用的安全保卫措施，并确定你的远程系统已经关闭了：

1. 确定安装了个人防火墙软件。（XP SP2+、 BlackICE 等中的 Windows 防火墙 ）以及提供至少的袋内保护——带外应用保护也很好，特别是如果你可以配置，这样你的用户就不会受到不断地带外连接请求的阻碍了。

2. 要求在每个系统上都有恶意软件防护（杀毒软件和反间谍软件），并且确保如果有更新就在实时采用了，可以防御不必要的感染。

3. 在远程硬盘上和其他存储设备上激活强大的文件和共享许可——特别是在默认允许每个人都全权访问的 Windows 2000 和 NT 系统上。

4. 为补丁管理准备写好的策略和存储的程序。例如，激活实时自动更新或者使用已有的补丁管理系统配置补丁

5. 切断不使用的连接，就像列出的一样，来防御远程系统的未授权的用户名、安全策略信息和更多信息的收集。

6. 实施 VPN（基于 Windows 的免费 PPTP 就是合适的选择）或者确保你云正在运行安全的备选连接，例如 Windows 远程桌面（Windows Remote Desktop）或者 Citrix。

7. 记住把远程用户、电脑和应用程序包括到你的安全事故回应计划和灾难恢复计划中。这些常见的错误在你的安全出现遗漏的时候就会刺激你的神经。

8. 你的用户将可能下载和安装 IM、P2P 和气他你不支持的应用，这样肯能回使你紧张，所以准备通过最小权限的用户

对于配置为使用基于 802。11 的无线网络（或者将来可能这样使用）的系统，不要忘了下面的安全措施：

1. 在最小程度上激活 WEP，因为比什么也没有要好得多，但是理想的情况是用户激活拥有强大（超过 20 个的任意字符）密码短语的 WPA2-PSK。

2. 要求你的用户使用方向天线——而不是把信息存储在所有接入点上的全向天线。

3. 激活 MAC 地址控制，它可以帮助非技术人员防火你的网络（技术人员知道改变 MAC 地址来绕开）

4. 如果可能，要求特定的供应商/接入点和无线 NIC 模式来确保他们已经根据你的标准作了持续加固，所以你可以和任何主要的安全警报、必要固件或者软件更新保持一致。

5. 记住用户可能通过公共热点连接你的网络，所以确保你和他们理解安全的含义，并且采取了适当的安全措施。

6. 激活安全信息，如果通过 POP3、SMTPs 不能获得 VPN 或者其他的热点保护，通过 HTTPS 和其他内置控件不能获得 Webmail。

7. 切断蓝牙，如果不需要。否则在默认状态下它很危险，所以把它关闭。

这些相对简单，而且大部分都是免费的远程访问安全措施，和适度的信息安全警告项目结合在一起在保护远离站点的电脑和保护那些你不能负担得起丢失责任的信息方面就有了很大的保证。

（作者：Kevin Beaver 译者：Tina Guo 来源：TechTarget 中国）

个人计算机访问远程网络

为了提供更广泛的远程访问性能，IT 经理正承受着日趋增加的压力。用户群体的范围从临时的“加班人员”，他们只需要从家里的个人计算机上访问其电子邮件和公司网络端口，到那些全职的远程办公者，他们使用核心应用程序和 IP 电话。由于他们依赖的是所有工作均为远程访问，所以通过为远程办公者提供公司的计算机、防火墙和 24x7 服务台访问，进而为全职的远程办公者提供高端解决方法，公司在这点上通常没有太多的困难。但是我们如何能够有效地（经济实惠地）支持其它用户的低端需求呢？

允许用户从其个人计算机和网络连接上进行访问的优点极具吸引力。通常，远程用户甚至都不需要一台公司的笔记本——带来带去不方便。除此之外，家庭系统很有可能更快捷（为孩子们设计，用于炸毁外星人的太空船）。然而，我们也需要考虑它的不足之处。

带来的风险与所提供的访问成正比

一些用户允许网络完全访问企业内部的局域网，这样会比那些仅使用电子邮件的用户造成更多的破坏。因此，你的战略第一步就是提供分层访问，以满足每个用户的需求。通过两层或者三层，低端的网络邮件、中端的文件和网络应用程序访问，高端的全部 VPN 连接，许多公司就可以获得访问权。

训练

对于成功的远程访问项目而言，每个用户的安全教育是必要的。这对你正在进行的安全教育项目有突出的影响。你可以在公司的企业内部互联网中使用在线项目。确保跟踪完成，并且需要定期进修培训。尝试从那些参加课程培训的人中挑选出一部分进行奖励认证，以给用户积极的激励，使其完成其强制训练。全部课程应该包括积极活动带来的危险方面的信息，包括病毒、蠕虫和间谍软件。需要指出的一点是，这个指令将有助于保护其

自己的数据，以及公司的数据。也包括密码护理方面的信息，以及一旦发现可疑事件正在发生时应该做些什么。不要忘记还包括访问公司信息的必要条件。

认证

在允许他们访问任何服务，包括网络邮件之前，你必须知道这些人是谁。通常情况下，我们使用用户名和密码来提供身份验证，这很容易被拦截，并且受到威胁。教育用户要进行密码护理，在传输过程中使用加密的方法保护密码，这在过去来说就足够了，但是今天有了间谍软件和按键嗅探器，实际上，所有远程用户都必须强制使用带有硬件令牌的双因素认证技术，即使是那些低端优先权的用户也必须使用。

如果你选择继续应用用户名和密码，确保你没有将自己设为服务拒绝攻击。你是否使用你的内部域认证资源进行远程访问，并且在一定数量的登录企图失败以后自动锁定账户呢？如果要求管理员进行人工干预，储存一个自动锁定的账户，你的系统就很容易受到攻击。一个不满的雇员坐在网吧中，打开公司的目录，为列表中的每个用户名输入弱密码，并锁定整个公司的内部互联网和外部互联网。为外部服务使用分离的认证资源，或者在短期内仅锁定账户，这是个更好的方法。即使锁定的时间仅为五分钟，也可以保护你免于受到字典式攻击。

授权

合理地访问内部资源是关键。如果你有一个现有数据的盘存和授权模式，这将会获得回报。如果没有的话，你需要确定你的信息资源，以及它们是如何分类的。虽然最佳的SSL VPN和网关产品具有丰富的访问控制模型，但是如果你不知道哪个用户应该访问哪些数据以及这些数据存储在哪里的话，这些产品对你不会有任何好处。如果你没有对你的数据进行分类，这为你开始对数据进行分类提供了很好的动机。

现行内容控制

病毒是这十年来的灾祸，并且与所有有效的安全程序一样，病毒也可以分层，在网络边缘启动。当然每台计算机都应当已经安装了防病毒软件，并及时维护。这是你可以激励良好安全做法的另一个地方：考虑为你的终端用户免费或者打折提供防病毒软件。你可能不想使用用于内部配置的企业版，因为这会增加你的维护负担，但是你也可以为加班人员提供消费版。当然你希望确保用户每年都更新其订购，因此在你的计划中要考虑到更新问题。同时不要忘了保护全职远程办公者所使用的系统。

个人防火墙

个人防火墙在完全 VPN 环境中是非常普遍的，并且即使对于那些使用网络电子邮件的加班人员也是非常有用的。因为个人防火墙可以帮助阻止间谍软件返回到信道中。你可以选择与讨论过的防病毒软件类似的方式来资助使用个人防火墙。

信息泄露

每次浏览器载入一个明确的文本网页，浏览器的缓冲存储器中就复制了该网页。同样地，浏览器的历史功能也可以捕捉到路径和其它参数。此外，终端用户通常下载电子邮件信息和附件，以及他们有可能获得的文件。显而易见，这是一个严重的问题。所有的信息并没有丢失，然而，浏览器不能在 SSL 连接中正常地缓存所下载的数据。一些 SSL VPN 远程访问产品具有特殊的性能，可以在马虎的软件和健忘的用户使用后进行清理缓冲存储器。如果信息泄露带来的风险对你的公司很重要，那么你就需要研究一下这些性能。

如果你不能控制，那么进行监测

你不一定有必要的资源来执行技术控制，以补偿每一种威胁。这是底线。然而，你不应该放弃。如果你不能进行控制，通常你可以进行监测。监测技术包括网络入侵检测和基于主机的入侵检测、系统审计以及日志分析——这些都是在路径上阻止问题发生的强有力的技术。

你的公司可以允许雇员使用他们的家庭计算机。虽然这不是免费的，并且不可能包括一些用户需要的所有服务，但是可以安全地执行许多服务。

(作者：Mark Mellis 译者：李娜娜　来源：TechTarget 中国)