使你的家庭网络安全的最佳实践

Best Practices for Keeping Your Home Network Secure

翻译 樊山

正如在工作中需要访问敏感的企业或政府信息的用户，你的家里存在风险。通常想要获得的信息都存储在受保护的办公网络中，网络对手可能把你不安全的家庭网络作为目标进行操作。

不要成为受害者。遵循一些常识的指引并在您的家庭网络上实现一些简单的控制，你可以帮助保护你自己，你的家人和你的组织。

二〇一五年二月 广州

目录

个人计算机设备的建议

个人计算机设备包括台式计算机，膝上型计算机，智能电话和平板电脑。因为大部分的信息是通过这些设备存储和访问，你需要特别注意确保他们安全。

1. 迁移到一个现代操作系统和硬件平台

任何操作系统（OS）的最新版本不可避免地包含以前版本中没有发现的安全功能。其中许多安全功能在默认情况下启用，并有助于防止常见的攻击向量。另外，在64位硬件平台使用64位操作系统，大大提高了防止对手获得您的计算机上访问特权的努力。

2. 安装综合安全套件

安装提供分层防御的全面安全套件，通过防病毒，防网络钓鱼等安全功能。此外，一些安全套件，例如来自McAfee®[1]，Norton®[2]，Symantec®[3]，利于企业恶意代码知识库和历史记录提供基于云的信誉服务。请务必启用套件的自动更新服务，以保持签名是最新的。

3. 限制使用管理员帐户

在您的操作系统，通常使用高权限的管理员（或root）帐户的权利来访问系统。因此，Web或电子邮件发送的恶意软件因为你是管理员身份登录执行从而可以更有效地破坏系统。创建一个非特权“用户”执行大部分活动，包括网页浏览、电子邮件访问和文档创建/编辑。仅使用特权安装/升级软件。

4. 使用 Web 浏览器沙箱功能

访问被攻陷或恶意的Web服务器是一种常见的攻击向量。考虑使用提供了沙盒功能的几个当前可用的web浏览器之一（例如Chrome TM[4]，Safari®[5]）。包含恶意软件的执行在沙箱中运行，从而隔绝底层操作系统不被利用。

5. 使用 PDF 阅读器沙箱功能

PDF文件是一种提供恶意软件流行机制。使用多种商业或开源PDF阅读器（如Adobe®[6]，Foxit®[7]）提供的沙箱功能和内部文件嵌入恶意网址（网站链接）块的执行。

6. 更新应用软件

攻击者往往会利用未打补丁的计算机设备，运行过时软件应用的漏洞。启用应用程序提供的自动更新功能选项，并及时安装提示的可用更新。由于许多应用程序没有自动更新功能，使用一个来自第三方的产品，如来自Secunia公司和eEye Digital Security®[8]，它可以迅速探测已安装的软件并报告哪些应用程序已经过期或需要补丁或更新。

7. 实施笔记本电脑全磁盘加密（FDE）

通过实施FDE防止万一笔记本电脑丢失或被盗引起的数据泄露。大多数现代的操作系统提供了一个内置的FDE能力，例如微软的BitLocker®[9]，苹果Filevault®[10]或Linux的LIKS。如果您的操作系统不提供FDE，使用第三方产品。

8. 仅从可信的来源下载软件

为了尽量减少无意中下载恶意软件的风险，仅从可信来源下载软件和移动设备的应用程序。在移动设备上，仅授予应用服务需要功能的权限，并在不需要时关闭定位服务。

9. 保护移动设备

因为它们便于使用和携带，对于移动设备如笔记本电脑，智能电话，和平板电脑应该额外关注。为了防止设备或设备上的信息被盗窃，保持物理控制，可能的话，启用自动锁定屏幕在闲置一段时间后使用一个难以猜测的密码或 PIN。如果一台笔记本电脑，在旅途中必须留在酒店房间时应断开电源，并使用如 FDE

所述的方法保护。

网络推荐方案

家庭网络设备包括调制解调器/路由器，无线接入点（WAP）。这些设备控制信息进出网络的流量，并应仔细保护。

1. 配置灵活的家庭网络

作为服务合同的一部分您的 Internet 服务提供商（ISP）可能提供调制解调器/路由器。为了最大限度管理控制您家庭网络的路由和无线产品，使用个人拥有的路由设备连接到 ISP 提供的调制解调器/路由器。图 1 给出了提供给所述家庭用户使用支持多个系统以及无线网络和 IP 电话服务网络的典型小型办公室/家庭办公室（SOHO）网络配置。

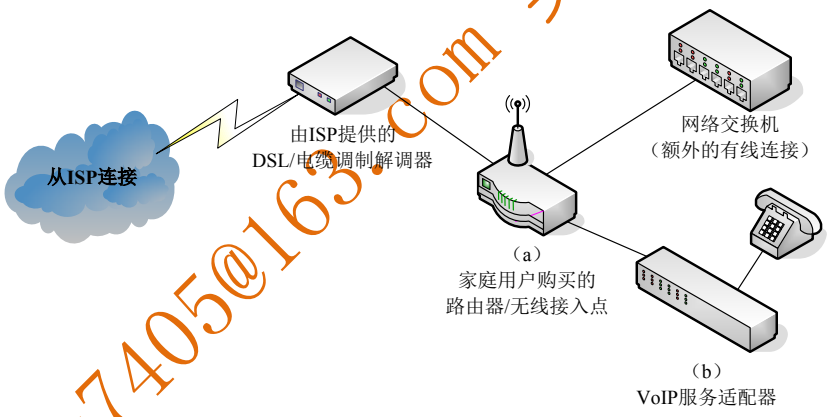

图 1: 典型的 SOHO 配置

2. 禁用 Internet 协议版本 6（IPv6）隧道

IPv6 和它的前身 IPv4 二者用于在互联网上传输的通讯。大多数现代操作系统默认使用 IPv6。如果设备上启用了 IPv6，但当你的通信不支持其他系统/网络时，有些操作系统将尝试使用隧道功能通过在 IPv4 封装 IPv6 流量如 Teredo，6TO4 或 ISATAP（站内自动隧道寻址协议）。因为攻击者可以利用这些隧道建立隐藏的通信通道进出你的系统，你应该禁用隧道机制。在 Windows 中，您可以通过设备管理器禁用这些（一定要选择在视图菜单下的“查看隐藏的设备”）。

3. 提供防火墙功能

为了防止攻击者扫描您的网络，确保您个人拥有的路由设备支持网络地址转换（NAT）以防止内部系统能够被直接从互联网上被访问。无线接入点（WAP）一般不提供这些功能，因此它可能需要购买一个无线路由器或附加在WAP有线路由器。如果您的ISP支持IPv6，应该确保您的路由器同样支持。

4. 采用 WPA2 无线网络

为了让您的无线通信保密，确保你的个人或者ISP提供的WAP使用保护无线电脑网络安全系统升级版本 (WPA2)而不是更弱的容易被破坏的保护无线电脑网络安全系统WPA，更改默认的密码使其成为复杂并难猜测的密码。需要注意的是较旧的客户端系统和接入点可能不支持WPA2，将需要升级软件或硬件。当确定一个合适的替代品时，确保设备支持WPA2的个人认证。

5. 限制管理内部网络

关闭允许攻击者访问和更改您的网络，您的网络设备的漏洞，禁止从您的内部网络实现远程/外部变更的能力。

6. 实施一个备用 DNS 提供商

域名系统（DNS）关联域名（如www.example.com）与他们的数字IP地址。ISP的DNS提供商可能并不提供增强的安全性服务，如危险网站的阻断和黑名单。可以考虑选择使用开源或商业DNS提供商提升网页浏览的安全性。

7. 对所有网络设备实施强密码

除了对你的WAP使用强大复杂的密码，任何可以通过Web界面，包括路由器和打印机等进行管理的网络设备使用强密码。例如，目前市场上的许多网络打印机可以通过Web界面管理如电子邮件警报和日志的功能。没有密码或弱密码、默认密码都会使攻击者可以利用这些设备来获得你的其他内部系统的访问。

家庭娱乐设备的建议

家庭娱乐设备，如能够通过无线或有线连接访问互联网的蓝光播放器，机顶盒视频播放器（如苹果TV®[11]）以及视频游戏控制器。尽管连接这些类型的设备到家庭网络通常会带来较低安全风险，您也需要实施安全措施以确保这些不会成为您网络中的一个薄弱环节。

1. 保护网络内的设备

保护它免受来自Internet不受限制的访问。在支持无线设备的情况下，按照本文档中的无线局域网安全性指导。

2. 服务账户使用强密码

大多数的家庭娱乐设备，需要您注册其他服务(如Playstation®[12] Network, Xbox Live®[13]®[14]，Amazon Prime®[15]，iTunes®[16]）。按照本文档中密码指导创建和维护服务帐户。

3. 不使用时断开链接

为了防止攻击者经由家庭娱乐设备探测网络，如果可能的话，在不使用因特网时断开这些系统。一些ISP调制解调器/路由器有一个待机按钮，你可以用它来禁用Internet连接。

上网行为建议

为了避免透露有关您的组织或个人生活中的敏感信息，遵循下列准则访问互联网。

1. 访问公共热点时，务必小心

许多场所，如咖啡馆，酒店和机场，为客户访问Internet提供无线热点或信息亭。由于这些底层基础设施是未知的，安全往往是脆弱的，这些热点很容易受到攻击活动。如果当你离开家时需要访问Internet，请遵循以下建议：

- 如果可能的话，使用蜂窝网络（也就是手机Wi-Fi，3G或4G服务）连接到互联网，而不是无线热点。此选项通常需要与蜂窝提供商服务计划配合。
- 建立一个加密隧道到可信虚拟专用网（VPN）服务提供商（例如，StrongSwan的Strong VPN）。这个选项可以保护监视。但是，使用VPN带有一些不便、开销，而且往往会带来成本的问题。
- 如果使用的热点是访问互联网的唯一选择，限制动态网页浏览。避免访问服务，如需要输入用户凭据或个人信息的银行网站。

2. 不交换家庭和工作内容

信息（如电子邮件，文件）不太安全的家庭系统和工作系统之间通过电子邮件或者可移动介质交换可能使工作系统受损害的风险增加。如果可能的话，家里开展各项工作业务使用组织提供的笔记本电脑。这些业务的交互请求应该是预期的，联系发送与工作有关的邮件应该使用工作邮箱账号而不是个人邮箱账号。

3. 要认识到的设备信任级别

家庭网络包括有线和无线设备和计算机的各种组合。建立一种信任关系不仅基于设备的安全功能还包括它的使用。例如，有关安全性儿童比成人通常缺乏头脑，并且可以更容易在其设备上安装恶意软件。避免使用缺乏头脑的用户电脑上进行网上银行，股票交易，家庭照片存储以及其他相关的功能。

4. 警惕互联网上存储的个人信息

个人信息从传统的本地计算设备上存储正在稳步向称作云计算的按需网络存储发展。信息在发布到基于云服务，问问自己谁将会有机会获得您的信息并且

你如何控制信息的存储和显示。此外，要注意定期通过使用互联网搜索引擎搜索网上公布的个人信息。

5. 社交网站上采取预防措施

在社交网站的分享与家人和朋友个人信息是一种便利方式。然而，这种便利同时也带来一定程度的风险。为了保护自己，请执行以下操作：

- 发布信息时三思而后行，如地址，电话号码，工作地点，以及可用来针对或骚扰您的其他个人信息。
- 如果可能，限制你的信息为“仅朋友”访问，并尝试通过电话或亲自验证任何新的共享请求。
- 从朋友处接收内容（如第三方应用程序）时，请注意由于最近许多攻击者利用普遍接受的社交网络的优势轻而易举地在内容中采取插入恶意软件的方法。
- 可从您的社交网络提供商定期复查安全策略和设置，以确定是否有新的功能可以保护您的个人信息。例如，一些社交网站目前允许您选择不暴露你的个人信息提供给互联网搜索引擎。
- 按照朋友的个人资料，看是否发布的信息对你可能存在问题。

6. 开启 SSL 加密应用

当登录基于Web应用，如Web邮件和社交网络网站时，通过应用加密（SSL或TLS）在互联网上建立传输。幸运的是，大多数Web浏览器默认启用SSL支持。

当在进行敏感的个人活动，如Web站点时使用SSL。大多数Web浏览器提供某种迹象表明启用了SSL，通常是锁符号或者网页旁边的URL或浏览器底部状态栏。此外，许多流行的网络应用如Facebook® [17]和Gmail®[18]选择强制所有通信默认使用SSL。

7. 遵守电子邮件的最佳实践

个人电子邮件帐户，无论是基于Web还是本地计算机都是常见的攻击目标。

下面的建议将有助于减少基于电子邮件暴露的威胁：

- 家庭和工作电子邮件地址使用不同的用户名。独特的用户名让某些针对您的工作帐户也可以通过访问您的个人账户更加困难。
- 为了防止密码泄露后的重复使用，为每个电子邮件帐户使用不同的密码。
- 不要设置不在办公室时使用个人邮件账号，因为您的邮件地址是合法的并可以提供有关你活动的信息给不知道的人而被确认为垃圾邮件发送者。
- 为了防止他人读取邮件，在你的电脑和邮件服务器之间传输时始终使用安全的电子邮件协议（IMAP安全或安全POP3），特别是如果使用无线网络时。
- 应考虑到未经请求的包含附件或链接的是可疑电子邮件。如果发送者的身份不能被验证，删除电子邮件而不是打开。对于那些电子邮件中的嵌入式链接，应该打开浏览器直接通过众所周知的Web地址在浏览器上访问或者使用互联网搜索引擎搜索这个网站。
- 警惕任何电子邮件请求的个人信息，如作为您目前进行的电子商务的任何Web服务相关密码或社会安全号码，它们应该已经有这些信息。

8. 保护密码

确保密码和挑战应答得到妥善的保护，因为它们可以访问个人信息。

- 密码应该强壮，每个账号是唯一的并且难以猜测。请考虑使用一个自己容易记住但是在足够长的时间内破解存在难度的密码
- 禁用允许Web站点或程序记住密码的功能。
- 许多在线网站使用密码恢复或挑战提问。你这些问题的答案应该是，没有人能知道，或从网上搜索或公共记录中不能找到。为了防止攻击者利用你的个人信息来回答问题的挑战，考虑提供一个基于事实的问题和一个虚假的答案，承担应答是唯一的并令人难忘。
- 可以在访问网络邮件，社交网络和其他帐户时使用双因素身份验证。双因素身份验证的例子包括发送到您的手机上的一次性密码验证码，或同时使用密码和基于可信设备的鉴别登录。

9. 避免张贴 GPS 坐标照片

许多手机和新的傻瓜相机嵌入了GPS定位坐标，当照片对你生活和当前所在位置形成习惯/形态时。限制这些照片在互联网上曝光并且仅由受信任的观众可以观看或在使用第三方工具上传到互联网之前时去除坐标。有些服务如Facebook会自动去掉了GPS，以保护其用户的隐私坐标。

更多的指导

社交网络

http://www.nsa.gov/ia/_files/factsheets/i73021R-2009.pdf

星期一缓解–针对恶意电子邮件附件的防御：

http://www.nsa.gov/ia/_files/factsheets/ MitigationMonday.pdf

星期一缓解 #2 – 防御通过驱动下载

http://www.nsa.gov/ia/_files/factsheets/i733-011R-2009.pdf

强化技巧

Mac OSX10.6强化技巧：

http://www.nsa.gov/ia/_files/factsheets/macosx_10_6_hardeningtips.pdf

执行无互联网或E-mail的特权帐户：

http://www.nsa.gov/ia/_files/factsheets/Final_49635NonInternetsheet91.pdf

Red Hat Enterprise Linux 5默认安装强化技巧：

http://www.nsa.gov/ia/_files/factsheets/pamphlet-i731.pdf

Internet Protocol Version 6（IPv6）：

http://www.nsa.gov/ia/_files/factsheets/IPv6.pdf

个人管理Apple的iPhone和iPad的安全性提示：

http://www.nsa.gov/ia/_files/factsheets/image.pdf

Windows 7中的安全性亮点：

http://www.nsa.gov/ia/_files/factsheets/highlights.pdf

免责条款

商品名称，商标，制造商或其他服务，并不一定构成或暗示为其代言、推荐或有利于美国政府。上述美国政府的看法和意见，不得用于广告或产品代言目的。

参考文献

[1] McAfee® is a registered trademark of McAfee, Inc.

[2] Norton® is a registered trademark of Symantec

[3] Symantec® is a registered trademark of Symantec

[4] ChromeTM is a trademark of Google

[5] Safari® is a registered trademark of Apple

[6] Adobe® is a registered trademark of Adobe Systems, Inc.

[7] Foxit® is a registered trademark of Foxit Corp.

[8] eEye Digital Security® is a registered trademark of eEye, Inc.

[9] BitLocker® is a registered trademark of Microsoft

[10] Filevault® is a registered trademark of Apple

[11] Apple TV® is a registered trademark of Apple

[12] Playstation® is a registered trademark of Sony

[13] Xbox Live® is a registered trademark of Microsoft

[14] Netflix® is a registered trademark of Netflix.com, Inc.

[15] Amazon Prime® is a registered trademark of Amazon Technologies, Inc.

[16] iTunes® is a registered trademark of Apple

[17] Facebook® is a registered trademark of Facebook

[18] Gmail® is a registered trademark of Google

联系信息

行业咨询: 410-854-6091 **bao@nsa.gov**

USG/IC客户建议: 410-854-4790

DoD/军事/COCOM 客户建议: 410-854-4200

一般咨询: NSA信息安全保障

服务中心 **niasc@nsa.gov**