白皮书

未锁上的门

研究显示，目前打印机极易遭受网络攻击。

在 IT 团队侧重于其他终端的同时，企业打印机的安全防护往往显得滞后。

打印机极易成为攻击者的目标：因为有太多联网的打印机无任何限制措施，也未经安全锁定。

但上述安全威胁是切实存在的，不应被忽略。企业级打印机现已发展成功能强劲、可通过网络相互连接的设备；但这些设备和您的其他网络终端一样，都存在着相同的漏洞。这些未经安全防护的入口点可能招致网络攻击；他人也可由此获取公司的财务及私密数据，造成严重的商业后果。

即便如此，Spiceworks 调查了 300 多名企业 IT 决策者，其中仅有 16% 的受访者认为打印机正处于安全威胁/入侵的高风险状态，较之台式电脑/笔记本电脑和移动设备，这一数值要低得多。[1] 此调查结果表明 IT 工作人员对于网络安全的掌握情况仍不理想。每五家企业仅有三家左右为打印机采取了安全措施，这一比例远低于其他终端设备——当使用简单方法对这一特殊入口进行防护时就会留下打印机易受攻击的隐患。

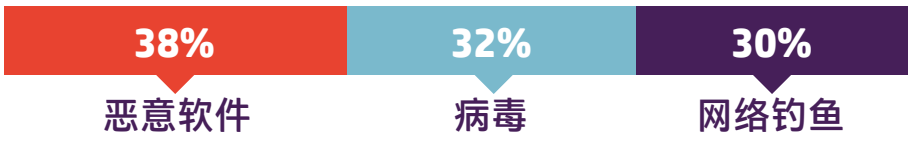
本白皮书提供了与打印机安全防护相关的数据，所依据的内容包括：Spiceworks 调查、安全入侵影响，以及现代内置打印机一些用于抵御网络攻击的安全功能。

仅有 16% 的受访者认为打印机正处于安全威胁/入侵的高风险状态。[1]

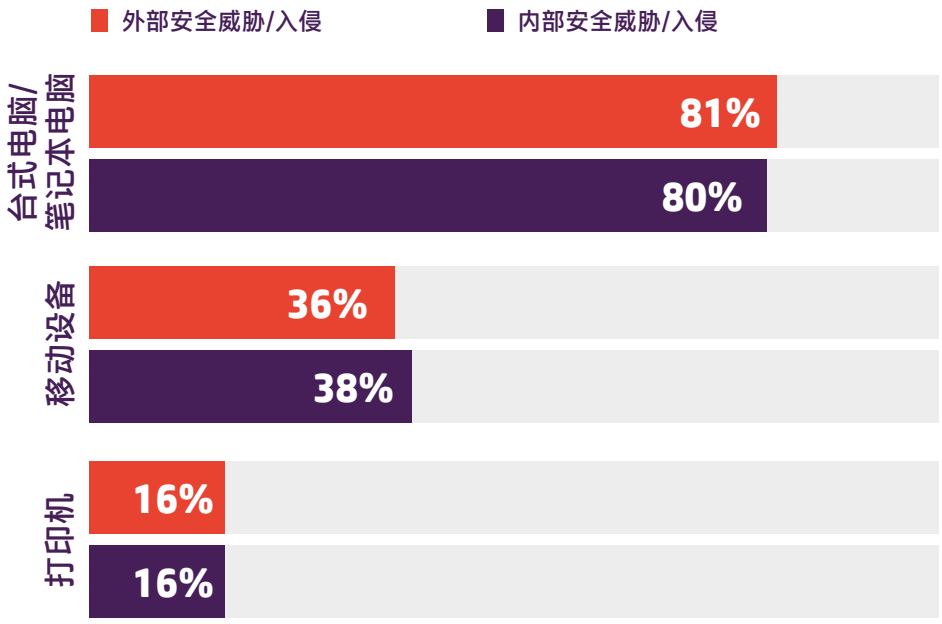
可供攻击的入口

在 Spiceworks 调查中，74% 的受访者（净人数）表示，其公司在去年至少发生过一次来自外部的 IT 安全威胁或入侵。同时，有 70% 的人（净人数）遭遇了一次来自内部的 IT 安全威胁或入侵，其中的大多数源自于用户错误、将个人设备用于工作目的，或员工将家用或共用网络用于工作目的等。[1]

最主要的外部 IT 安全威胁/入侵



主要威胁大多借助台电脑机和笔记本电脑进行藏匿，其余也会通过移动设备及打印机出现。[1]（来自打印机的威胁占到 16%，远超其在 2014 年 Spiceworks 调查中的数值 ——4%。）来自打印机的攻击次数还可能受到了低估，因为人们不会像监视个人电脑和移动设备那样对打印机也采取密切监视。



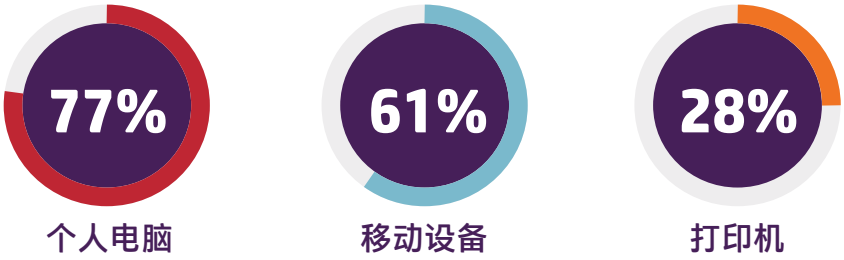
我们忽视了自己的打印机

不论调查情况如何，从 Spiceworks 调查中我们可以清楚地看到，人们往往不会去优先考虑打印机的安全问题。

企业只意识到网络、终端和数据安全的重要性。实际上，有超过 3/4 的受访者采用了网络安全防护、访问控制/管理、数据保护，或终端全防护保护等措施中的一项或多项。[1]

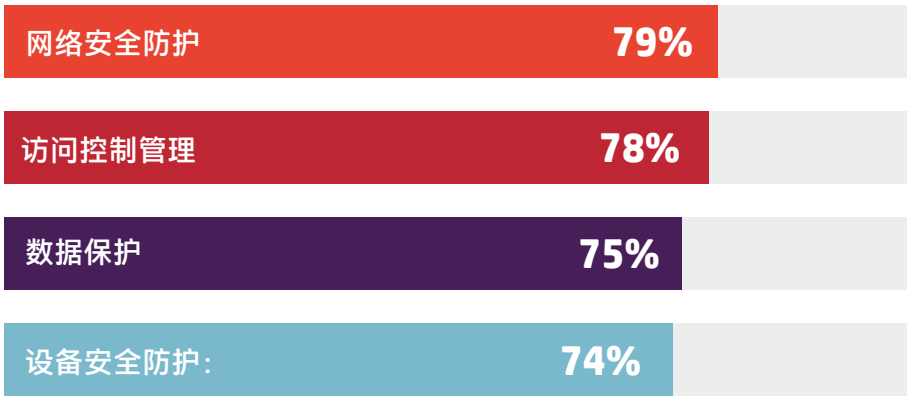
但在多数情况下，这些措施都未能部署到打印机上。与此同时，有 83% 的受访者对台式电脑/笔记本电脑采用了网络安全防护，也有 55% 的受访者对移动设备采用了网络安全防护，而对打印机采用了网络安全防护的仅有 14%。[1]

就终端安全防护而言，上述差距更为显著：



另外，仅有不到 1/3（28%）的受访者为打印机部署了安全认证，而对于个人电脑和移动设备而言，这一数值分别为 79% 和 54%。[1]

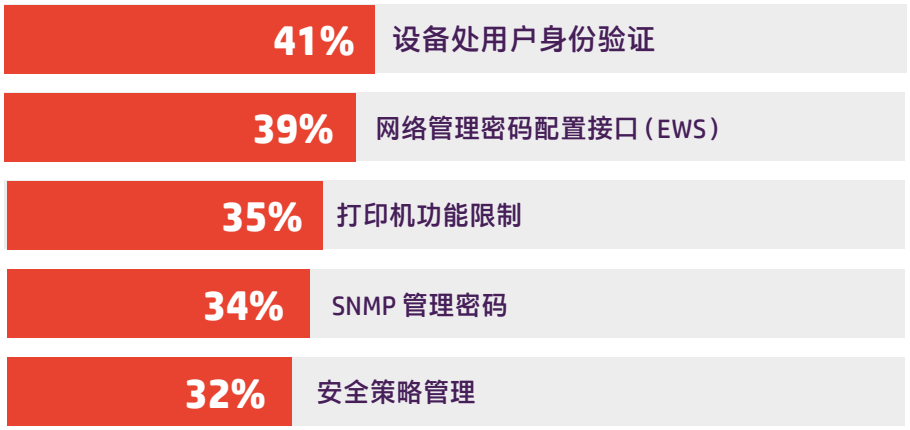
最主要的终端安全防护措施



在常见终端设备的保护措施中，针对打印机最为常用的要数文件安全防护、网络安全防护和访问控制，但仅有不足半数的受访者表示，其公司为打印机采用了上述措施。[1]

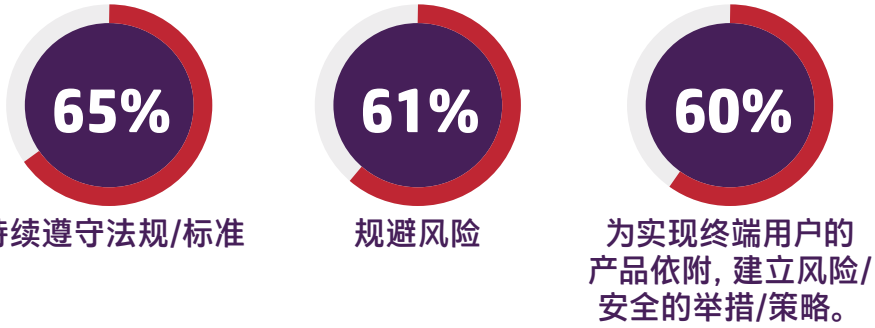
一些公司的确拥有打印机专用的安全措施，但即便如此，这些措施也存在着相当大的差异。仅有 40% 多的企业部署了用户认证，而为网络配置界面采用了管理员密码的企业不足 40%。[1] 为了确保强大的防御效果，各个企业都应对以上措施——乃至其他有效措施——进行搭配使用。

最主要的打印机专用安全措施



就终端合规和审计实务而言，打印机的安全控制几乎滞后于其他所有终端设备。近 90% 的企业都部署有信息安全策略，但这些策略通常都未能延及打印机。例如，57% 的受访者表示其为公司个人电脑部署了恶意软件防御系统，而为打印机部署的，仅有 17%。[1]

近九成的 IT 专家表示其公司实施有信息安全策略，原因如下：



显而易见的是，企业对于打印机并未引起足够的重视——但这真的很有必要。

“许多打印机仍在使用默认密码，或者干脆没有密码，或者有十台机器在用着相同的密码。”惠普首席安全顾问 Michael Howard 在 6 月份对《计算机世界》杂志如此说道。“对于黑客而言，没有密码保护的打印机就好比一座金矿。常见的入侵攻击中，有一种被称作“中间人”的攻击，黑客会控制打印机，并在我们打印资料前将“入侵文件”转移到笔记本电脑中。这样一来，黑客就能掌握 CEO 所打印的情报信息了。[2]

打印机入侵的潜在影响

据 Bogdan Botezatu 比特凡德杀毒软件的一名资深电子威胁分析师表示，打印机呈现出了相当大的安全漏洞隐患。“我们在漏洞评估实验室中进行了大量的遥感勘测。路由器已经不再是最糟糕的互联网设备了。现在这个头衔归打印机所有。[3]

打印机漏洞能给企业带来十分严重的影响。如果单台打印机未进行安全防护，那么您的整套联网设备都将极易受到攻击。黑客能够借此窥视您的联网设备——并且破坏整个网络的安全。

1. 增加帮助台呼叫与支持时间

2. 降低生产率/效率

3. 增加系统停工时间

4. 增加支持呼叫用时

5. 增加终端用户策略实施

对于安全入侵的影响，我们都有了解。在 Spiceworks 调查中，受访者表示，安全入侵最主要的五种影响包括：[1]

打印机入侵所能造成的影响可能比安全入侵更为严重，尤其是当您使用多功能打印机电子存储打印数据的时候。黑客可能通过存放在打印机存储器中的打印任务获取敏感的个人或商业信息。

更严重的是，黑客还可能利用未经安全防护的打印机进一步访问公司网络，窃取诸如社保编号、财务信息或内部备忘录及文件等资料。遭窃的信息不仅会给员工个人造成影响，还会被用于企业竞争，或对公司声誉造成严重损害。

简单的解决方案：内置安全功能

显而易见的是，即使是打印机，公司也需要想办法解决其安全问题。如今，一些现代企业级打印机具备便于使用且内置的安全防护功能，能够有效抵御针对打印机的威胁。其中包括：

- **针对攻击实施自动检测、防护和恢复**
- **追踪使用状况，以防出现非法使用**
- **采用简单标志选项，如 PIN 或智能卡等**
- **采用感应读卡器，便于用户快速验证，并通过身份标记实现打印机的安全打印。**
- **对敏感文档进行加密打印**

如果您又打算购买打印机，无论是桌面型或是多功能式，请务必详细了解其安全防护功能——并确保这些功能都处于激活状态。通过上述简易的打印机专用功能，您的打印机将不再脆弱不堪；毕竟，随着物联网的发展，有太多其他的接入点需要担心——而您的打印机不会成为它们中的一个。

查看更多关于打印机保护的信息？
了解更多信息 ›

信息来源：

[1] Spiceworks 调查，共计 309 名身处北美、EMEA、APAC 等地的 IT 决策者参与调查，调查代表惠普利益，开展于 2016 年 11 月。

[2] “打印机安全：您的公司数据真的安全吗？”《计算机世界》，2016 年 6 月 1 日。
http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] “打印机：当前互联网上安全程度最低的设备”，《*The Register*》，2016 年 9 月 8 日。
http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/