信息安全室 (/)

网络打印机安全最佳做法

多功能打印机（MFP）面临身份危机：IT管理员并不总是将它们视为真正的成熟网络计算机。但是攻击者确实如此-并且他们发现它们越来越具有吸引力！

这些打印机被推到办公室的角落，悄悄地进行复印，打印，传真和扫描的业务，似乎并没有构成任何真正的安全风险。但是，就像任何联网设备一样，如果管理不当，它们可能会将敏感的园区数据暴露给未经授权的访问和滥用。

为了保护您的打印机免遭未经授权的访问，更改打印配置，窃听和设备损坏，请遵循以下打印机安全最佳实践：

管理打印机访问

校园打印机不应暴露于公共互联网

采取以下适当的措施以确保仅将打印机配置为仅允许来自批准的网络和设备的访问：

- 校园部门应考虑使用RFC1918专用IP地址空间来限制仅对校园主机的打印机访问，从而使打印机无法从Internet访问
    - **注意：** RFC 1918专用IP地址空间由IST Network Operations and Services提供 (https://technology.berkeley.edu/services/network-voice-and-connectivity/data-networking-services) 可以从《伯克利电信目录》中 (http://telcat.berkeley.edu/)订购 (http://telcat.berkeley.edu/)
- 使用IST网络防火墙限制访问，校园部门可以免费使用
    - **注意：** IST网络防火墙服务由 IST网络运营和服务提供 (https://technology.berkeley.edu/services/network-voice-and-connectivity/data-networking-services) 可以从《伯克利电信目录》中 (http://telcat.berkeley.edu/)订购 (http://telcat.berkeley.edu/)
- 配置打印机的访问控制列表（ACL）以限制子网或设备的访问
- 删除IP配置中的默认网关以禁用Internet路由，从而仅在您的本地网段上进行打印
- 使用低成本硬件防火墙阻止对打印机的公共Internet访问
- 将另一台机器配置为具有适当访问控制的专用打印服务器

将默认密码更改为管理控制面板网页

现在做！如果未正确配置打印机的管理面板，则攻击者可能会：

- 更改打印机的网络地址并重新路由打印作业
- 进行拒绝服务（DOS）攻击并使设备无法运行
- 使用打印机作为攻击网络上其他系统的平台

具有未授权访问权限的攻击者也可以在打印机上安装恶意软件，从而允许远程后门访问。

访问打印机管理控制面板时使用加密的连接

例如，当通过Web浏览器访问打印机界面时，请使用“ https：//”地址（使用SSL加密），而不要使用常规的“ http：//”地址。如果需要命令行访问，请使用SSH而不是Telnet来防止窃听。

不要运行不必要的服务

默认情况下，许多打印机启用了不安全和不必要的协议（例如Telnet，HTTP，FTP）。启用这些服务可使攻击者能够直接访问打印机数据。尽管对打印机工作语言（PJL）知识了解有限的实用小丑可能只能通过Telnet来将“就绪”消息更改为可爱的东西（“插入硬币”），但更具恶意的攻击者可能会浏览打印机的硬盘驱动器并查看所有数据存储在那里。

禁用这些服务将禁止您的打印机被用于非预期目的，例如托管色情内容，或用作受版权保护的音乐和电影的FTP服务器。

更新和修补

就像计算机一样，打印机和多功能设备也需要更新和补丁。作为常规补丁程序管理计划的一部分，请检查所有打印机和网络设备上的固件更新。更新可以添加新的或改进的安全功能，修补已知的安全漏洞并修复其他问题。

确保您的多功能打印机不会造成巨大的安全漏洞，并将敏感的园区数据暴露给未经授权的访问和滥用。

选择合适的打印机

家用和小型办公室打印机通常不适合连接UC Berkeley的高速，开放网络。这些低成本打印机通常不满足园区网络设备的最低安全标准 (https://security.berkeley.edu/minimum-security-standards-networked-devices-mssnd)（MSSND）。如果使用打印机处理敏感信息，则家用或小型办公室打印机更不可能具有满足敏感数据更严格的MSSND要求所必需的安全功能。

对于共享的部门打印，请确保选择业务工作组打印机。这些打印机将打印作业，密码和其他信息存储在其硬盘驱动器上，并提供磁盘加密以保护存储在设备上的敏感数据。他们还可以在打印作业运行后擦除数据。

请记住，所有打印，复印，传真或扫描的内容都存储在打印机硬盘驱动器上-并确保在取消预置打印机或将打印机送出现场进行维修时，擦除了所有存储的数据。

在UCSF打印管理程序 (http://campuslifeservices.ucsf.edu/documentsmedia/services/print_management) 可作为加州大学伯克利分校校园部门的一项完整的打印机/复印机管理服务。

不需要的打印输出

如果您发现部门中发生不必要的打印输出（垃圾邮件，骚扰或令人反感的材料），请联系IT客户服务（提交在线票证） (https://berkeley.service-now.com/ess/) 或发送电子邮件 至 itcsshelp@berkeley.edu (mailto:itcsshelp@berkeley.edu)），以尽快帮助保护您的打印机并向 信息安全和政策小组报告安全问题 (https://security.berkeley.edu/i-want/report-security-incident)。

回到顶部