SearchSecurity.com.cn

技术手册

PDF安全使用策略

- ☆ 如何确保PDF和文档文件的安全？
- ☆ 企业如何预防PDF攻击？
- ☆ 采用pdf附件的电子邮件安全性就高吗？
- ☆ 如何借助修订策略来使用PDF修订工具
- ☆ 加密的Word文件通过互联网传输时是否没有PDF文件安全？

TechTarget
TT中国

PDF 安全使用策略指导手册

目录

如何确保 PDF 和文档文件的安全？

问：用什么方法能确保文档和 PDF 文件中没有被植入恶意内容呢？

答：这个问题可以有两种理解方式。一、如何确保你所接收或使用的文件不含恶意内容？二、怎样预防自己的文件中被植入恶意内容？对这两种理解，下文都会涉及，这样就能确保该问题能得到回答。

确保收到的文件中没有被植入恶意内容，需要做到以下几点：

1、你的操作系统和所有应用程序安装了最新的补丁。

2、要安装反病毒软件、反间谍软件和防火墙程序，及时更新，并确信其在运行。

3、文件在打开前都要扫描，禁止打开来源不明或不请自来的文件和链接。

4、在网络上要安装一些防网路钓鱼服务。

前三项建议都是标准的安全实践。许多攻击利用新发现的漏洞在文件中植入或执行恶意插件。因此，保证系统安装各种补丁，保持恶意软件工具的时刻更新，能够大大降低用户的机器遭受攻击的概率。 另外，文件打开前一定要扫描。对 Word 和 Excel 等应用程序还要进行如下设置：在没有你明确同意的情况下，嵌入在文件中的宏不能运行。

虽然第四层防护措施应用得还不普遍，不过它将变得越来越重要。供应商和 AV 产品生产者在发布产品补丁和病毒签名更新之前，零日（Zero-day）攻击是致命的。黑客要想发起类似攻击，首先需要引导受害者到一个特定的网站。这种引诱利用的是“网络钓鱼”技术，例如发一封带有诱惑性链接的电子邮件，该链接会连到某个恶意网站上。反钓鱼服务（比如由 OpenDNS 免费提供的服务），可以禁止对存在恶意性质的网站进行访问。这项保护服务还可以保护那些坚持将电脑链接到未知或不可信赖资源链接的用户。

供应商和 AV 产品生产者在发布产品补丁和病毒签名更新之前，零日（Zero-day）攻击是致命的。

问题二，如何确保自己的 pdf 文件或普通文件没有被恶意软件感染，这需要利用数据和文件生命周期管理系统。该系统保护静止的文件、传输中的文件，并且对处于访问、共享和发行状态的文件进行保护。除了加密和执行严格的访问控制外，你还可以在文件中寻求进行安全设置的地方，使文件在企业内外流通的生命周期中更加安全。或许，实现这种保护措施最常用的方法是采用 Adobe PDF 文件。PDF 文件具有内置控制，可以限制打开或者打印它的对象，以及收件人能够访问它多长时间。另外，PDF 文件还包括跟踪功能，能够了解文件被谁接收，以及文件是否处于打开状态。

即使采用了版权管理方案，如果你通过含有第三方广告，或允许用户输入信息的网站共享文件，仍然有可能将自己置于其他恶意攻击的危险之下。假如网站没有全面地对用户的输入信息（如，评论格式的信息）进行验证，那么黑客则可以使用跨站脚本攻击将恶意代码直接注入到你的网页上。

黑客还可以利用在网站上展示的广告来注入恶意内容，或将用户吸引到恶意的网站。谷歌的 Adwords（关键字广告）服务一直被用来展示文字广告，但这些文字广告却可以用来感染防护意识淡薄的网站浏览者，将他们吸引到中间的恶意网站。如果你没必要在自己的网站上展示第三方的内容或者广告的话，那就不要做，因为这样你能很快消除来自这方面攻击的危险。

（作者：Michael Cobb　译者：Sean ）

企业如何预防 PDF 攻击？

由于 Adobe 系统公司 Adobe Reader（以前称为 Acrobat Reader）的广泛应用，黑客常常瞄准这一软件及其使用的 PDF 文档来发起攻击，这一点已不足为奇。

尽管如此，真正值得关注的是攻击者发现的漏洞数量以及利用漏洞进行攻击的成功率。据 McAfee 公司 Avert 实验室 2010 年第一季度报告，目前恶意的异常 PDF 文档与 28%的恶意软件都有关系，而这些恶意软件又直接与漏洞利用程序（exploits）相关。

那么，如何使你的公司免遭来自 PDF 的攻击呢？难道要彻底限制 PDF 的使用吗？这就是本文要重点讨论的问题。

我们先说第二个问题。利用 PDF 文档作为信息交流的一种手段是非常普遍的，对于大多数公司而言，如果想有效的制止 PDF 文档在内部的使用，需要在内部应用程序、政策和规程方面进行重大的改革。由于其他大多数公司会继续使用 PDF 文档，所以在可预见的将来，你的公司将面临与第三方如何发布和共享信息的问题。实际上，因为它们是必不可少的正常业务活动，所以使用 PDF 文档必然会有风险。这便意味着，企业需要找到处理 PDF 文档的最佳措施。

要做到这一点，首先需要制订一个可接受的使用指南，其中应明确规定，在任何情况下均不允许打开来源不明的 PDF 文件。基于 PDF 的攻击通过使受害者打开受病毒感染的 PDF 格式文件进行的，因此禁止打开附在垃圾邮件或意外邮件上的 PDF 文件，将大大降低受病毒感染的风险。在安全意识培训课程上，上述措施应该被提到，这些培训课程的重点也应该放在你的安全和可接受的使用政策上，包括电子邮件和电子邮件附件。即使是为了防止那些受感染附件的潜在危险，在公司墙壁上贴几张海报，也没什么不妥。

但是，如果电子邮件看上去像是来自一个同事呢？你的政策应当说明，如果收到意外的附件，在打开之前，收件人应与发件人核实其真实性。这个过程可能显得有些繁琐，但发件人可以通知收件人：他们在发送 PDF 文件之前会发送一条短消息。

为了确保用户在自己的浏览器打开 PDF 之前就收到警告，你应该要求用户设置 PDF 文件的处理方式。

另一个 PDF 攻击方法是引诱用户访问恶意网站，然后调用 Adobe Reader 打开受感染的 PDF 文件。如果顺利的话，你所制订的可接受的使用政策和安全意识培训应该阻止员工点击主动发送的电子邮件中的 Web 链接，而你的杀毒软件应当

提供某种形式的 URL 过滤，以提醒用户不要浏览一个已知的恶意网站。不过，他们在日常工作中依然有可能会意外地访问到恶意网站。

为了确保用户在自己的浏览器打开 PDF 之前就收到警告，你应该要求用户设置 PDF 文件的处理方式。例如，对于 Firefox，可以通过在“工具>选项>应用程序”选项卡中设置为“总是询问”来改变。

有人质疑是否有必要在 PDF 文件（或者任何与此相关的文档类型）中嵌入可执行代码。但实际操作起来，如果这个功能被禁用，许多用户也并不会过于在乎。因为在不用 JavaScript 的情况下，他依然可以阅读 PDF 文件。如果你觉得你的公司离不开 PDF 的话，可以在 Adobe 阅读器中禁用 JavaScript，这将有助于防御一些较常见的攻击。

和其他类型的攻击一样，通过确保用户不会以不必要的高权限登录系统，这种 PDF 攻击可以被成功的避免。典型的企业用户几乎不需要对自己的电脑具有管理员权限。这使得很多攻击者很难完全控制、或很难通过 PDF 文件进行攻击。

显然，必须通过定期修补和更新杀毒软件、反恶意软件以及 URL 和垃圾邮件过滤器来加强这些安全措施，它们应当有助于阻止除了零日攻击以外的其他所有攻击。Adobe 已经改变了自己对软件安全的做法，现在它正在模仿微软的安全开发生命周期以开发自己的安全产品生命周期模型。它也在考虑为 Reader 和 Acrobat

每月发布一次补丁。这些都是积极的发展，希望这些变化所带来的好处可以使 Adobe 的软件在未来更安全，但同时你需要采取如上所述的 PDF 安全最佳措施，以减少由于使用 PDF 文件而带来的潜在危险。

（作者：Michael Cobb　译者：Sean）

采用 pdf 附件的电子邮件安全性就高吗？

问：用电子邮件发送包含敏感信息的 pdf 附件安全吗？

答：首先，我们必须明确，单纯发送一封电子邮件或者发送带 pdf 格式附件的电子邮件并不会感染病毒或者恶意软件，但我想这并不是你真正想问的问题。通过电子邮件或者附件的方式发送敏感信息都是不安全的，并且，鉴于您所在企业的安全政策，这可能使你陷入很多麻烦之中。原因如下。

发送一封电子邮件就好像发送一张明信片：每个处理这封电子邮件的人或者系统都可以阅读和记录邮件的内容。当然，如果内容无利可图或者一点也不重要，这倒没有什么问题，然而，如果内容包含银行资料、网络密码或者其他类型的敏感数

仅仅将敏感信息转换为 pdf 格式的文件来替代邮件正文并不能保护信息，除非使用 Adobe 的加密选项。

据，这将是一个很大的问题，包含明确禁止的反动言论也是一样。如果您通过电子邮件发送包含公司安全策略明文禁止的数据或者内容，你会因此招致麻烦。绝大多数具备安全意识的公司都会有涵盖敏感信息传输的政策和准则：哪些数据可以通过电子邮件发送，哪些必须被加密，等等。为了不冒犯这些政策，您应该与 IT 部门确认如何区分发送不同敏感等级的信息。

仅仅将敏感信息转换为 pdf 格式的文件来替代邮件正文并不能保护信息，除非使用 Adobe 的加密选项。文件必须签署数字标识并应用安全证书。Adobe Acrobat 允许创建自我签名的数字标识，在大多数情况下就足够安全了。

最安全的发送信息和附件的方式是在发送前将它们加密。除了在传输过程中保护附件，而且不管是存储在 PC 上，还是它通过的任意邮件服务器，或者最终到达收件者的机器上，文件加密都将为存储提供保护。在为他人提供可读的 pdf 文件之前，应考虑移除显示文档历史或者包含个人信息的内容，如将您的姓名列为作者的元数据。

另外，我建议在加密重要文件的同时对这些文件进行签名，这样收件人可以确信文件是由您发出的。如果收件人也有数字证书，您可以签署和加密信息，确保它

不能被预期收件人以外的人更改或者阅读。作为一个良好的习惯做法，我总是将电子邮件写成明信片而不是信的格式，在电子邮件的正文添加致敬、数据和时间确保电子邮件的内容明确。发送出去的电子邮件或者附件可能被有意或无意的转发给许多其他人阅读。即使加密了电子邮件的内容或者 pdf 文档属性禁止打印或复印，但是没有什么可以阻止人们对内容显示屏拍照。

最近 pdf 文档中出现不少安全漏洞，因此如果你需要交流 pdf 文档，请确保计算机保持最新的补丁更新。确保计算机上安装、更新和运行了防病毒和反间谍软件，在打开电子邮件和文档前扫描它们。

（作者：Michael Cobb　译者：Lily ）

如何借助修订策略来使用 PDF 修订工具

我常常收到来自读者的问题，这些读者关注各种微软 Office 产品中“允许快速保存”选项的安全问题。“快速保存”背后的观念就是通过仅保存所做更改并将更改添加到原始文档，从而加速保存文档或展示的过程。这意味着，保存的文档可能包含元数据，如注释和被删除的文本。任何人只要使用文本编辑器或 Word 的“恢复文本”功能就可以查看“被删除的”文本。此外，在这些文档被转换为另一种文件格式时，如转换为 HTML，“被删除的”文本通常都包括在新的文档中。

这个问题和 Word 的“修定”功能多年来已经产生了一些令人不快的安全漏洞，敏感和秘密信息被不知不觉地泄露给未被许可看到此信息的人。例如，用 Word 发表的文档就曾泄露了英国政府对有争议的拘留恐怖份子嫌疑人员的计划的怀疑，还有一份 Word 文档泄露了政治捐款人名单的私密注解。

Adobe Acrobat Pro 8 和 9 中有一个内置的 PDF 修订工具，如果你的企业经常以 PDF 格式发布文档，工作人员就应当学会如何使用这种工具。

不适当修订的类似问题——用于发布的文本的审核和准备——如今在 PDF 文档中很常见。去年年底，由于未能妥善修订他们在网上公布的文件，HSBC Bank USA N.A.泄露了包含美国客户电子申请破产程序的详情。该年早些时候，关于 Facebook/ConnectU 和解的保密听证会正式

文本确实修订了对和解的金融条件的所有引用，但是，修订得并不恰当，敏感信息仅仅用“白盒”（其内部结构可以直接观测）掩盖起来。简单的复制和粘贴就能泄露 ConnectU 的创始人收到 650 万美元的赔偿这一信息。

可以看出，如果不正确地准备就公开发布电子文档，可能会导致数据安全方面的严重损害。这是敏感数据从企业网络中泄露的一种明显但却很常见的方式。不仅企业的信息安全过程应当包含修订文档策略，而且工作人员还需要知道如何正确地完成修订。正确的电子修订就是从电子文档中完全清除内容，使其不能复原，且难以查看、打印、搜索或复制。修订要求恰当的工具和培训，这样修订才会长期有效。

具有讽刺意味的是，美国加州北区的联邦法院已经制定了一个很好的修订步骤指南，正是这家法院披露了我之前提到的 Facebook 的正式文本。

Adobe Acrobat Pro 8 和 9 中有一个内置的 PDF 修订工具，如果你的企业经常以 PDF 格式发布文档，工作人员就应当学会如何使用这种工具。Adobe 建议从“视图”菜单中选择“修订”，然后选择“工具栏”菜单。如果要设置修订标记的外观，请单击“修订属性”。下一步，选择“标记修订”工具，并通过双击来选择一个单词或图片，或在你选择一行、一个文本块、一个对象或区域时按下 Ctrl 键，为你想清除的项目作出标记。为了修订所标记的项目，单击修订工具栏上的“应用修订”。 在任何时候，都要用“检查文档”功能来搜索并清除可能隐藏的信息。

如果不保存文档，这些项目就不会被永久性的从文档中删除。在保存文档时，起一个新的文件名并将其新的分类等级加入到文档属性中是很明智的。

有一些第三方修订产品可作为升级到 Adobe 专业版本的另一种选择。Appligent Document Solutions 发布了 Adobe Acrobat 的 Redax 插件，它是第一家提供 PDF 文档修订工具的公司。Informative Graphics 公司提供了著名的 Redact-It，在其网站上有一系列免费的关于如何修订文档的白皮书。还有一个针对 Microsoft SharePoint 的 Redact-It 企业版，它能自动清除由 SharePoint 所发布的敏感内容及私密信息，同时又不改变源文档。

如果你没有预算购买额外的修订软件，Adobe 有一个有用的文档，称为电子文档中机密信息的修订，这份文档解释了在不使用 Adobe Acrobat 专业版的情况下，如何修订 PDF 文档。

对于仍在使用具有“允许快速保存”功能的 Microsoft Office 早期版本的用户来说，可通过单击“工具”/“选项”/“保存”，然后取消选择“允许快速保存”。在完成一篇文档时，你还应当在你与其它人共享文档之前，执行一次完整的保存，并将文档的文本迁移到其它程序，或将文档转换为一种不同的文件格式。

为了防止将仍包含修订或注解的 Word 2003 或更早版本的文档发送出去，应选择“工具”/“选项”/“安全性”，选择“打印、保存或发送包含修订或批注的文件之前给出警告”。你也许需要考虑微软的清除隐藏数据工具，此工具可以从 Word、Excel、 PowerPoint 2003/XP 等文件中清除隐藏的和关联的数据，如修订和注解。不过，还要阅读一一篇题为“清除隐藏数据工具的已知问题”的知识库文章，以避免代价高昂的错误。对于使用 office 早期版本的人来说，可查看 http://www.codeplex.com/redaction 上的 Word 2007 Redaction Tool 这个开源工具。

不管你的单位选择了什么工具，你都必须为员工提供恰当的培训。将一些修订很差的文档包含在培训中来强调危险性，这是一个不错的主意。没有什么比现实生活中的例子更有说服力。此外，培训应当包含如何修订不同类型文档的详细步骤。这些说明可从你所使用工具的手册中获得，也可参考 Adobe 及微软提供的建议。

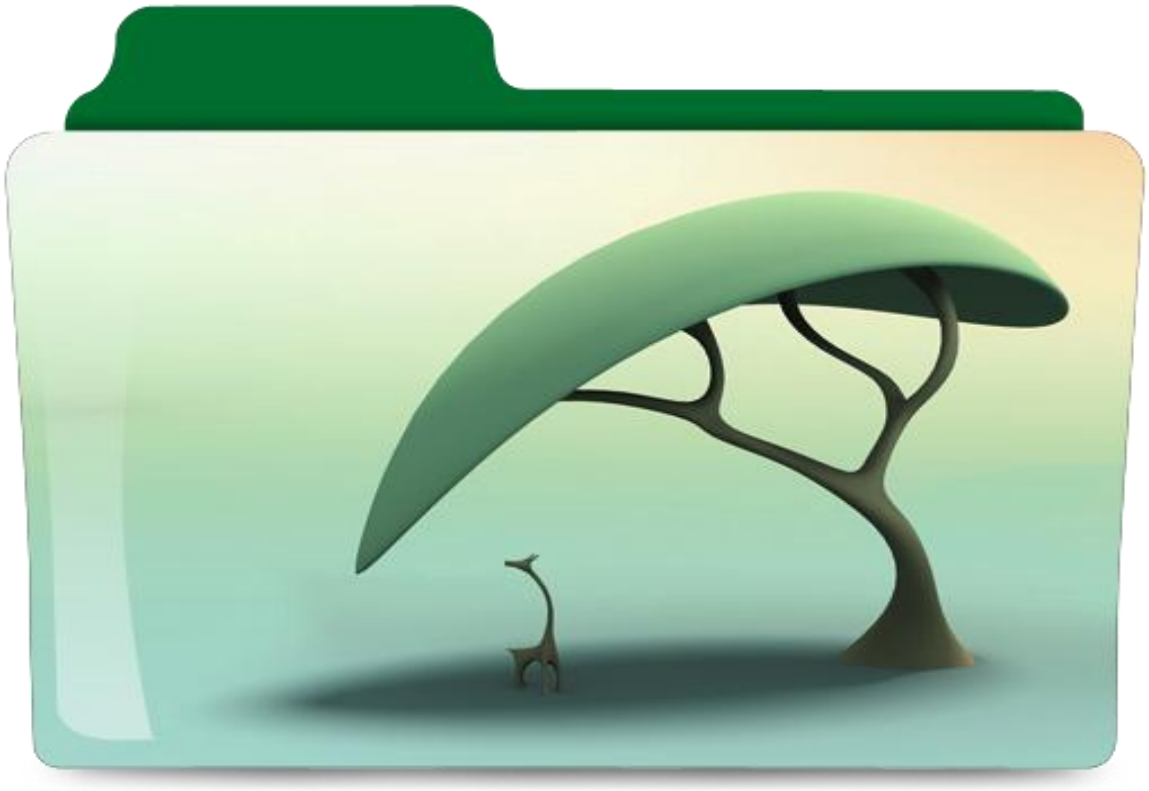
正确修订的文档必须清晰地显示出原始文本的位置，从而醒目地显示其清除内容。

正确修订的文档必须清晰地显示出原始文本的位置，从而醒目地显示其清除内容。修订的目的是为了留下清晰的删除证据，而不会给读者这样的印象：清除的文

本可在任何地方，其长度也是任意的。很明显，在确信已经清除了元数据和修订信息后，这是没有必要的。

修订有助于保护知识产权以及被认为是敏感或私密的数据，对于任何处理机密、敏感或私密信息的组织而言，这是一个重要的安全过程。糟糕的修订可能要付出高昂的代价。

（作者：Michael Cobb　　译者：Charlie）



加密的 Word 文件通过互联网传输时是否没有 PDF 文件安全？

问：当从一个安全性不强的客户端发送到一个 HTTPS 网站，然后继续传到另一个安全性不强的客户端时，在互联网的传输中， 微软的 Word 文件是不是没有 PDF 文件那么安全？（我没有假设任何一种文件类型是完全安全的。）

答：你描述的这种情况相对而言一开始就是不安全的，这一点你也意识到了。人们往往容易忽视 HTTPS 所提供的保护，它在一般的 HTTP 增加一个认证和加密层，同时受到端点 Session 的限制。服务器给客户端提供一个证书，但客户端并不需要出示证书给服务器。换句话说，一个客户端的身份证明是很容易伪造的，这可能你提到的“安全性不强的客户端”。

又或者，你也许是指另一个事实，就是客户端是在不安全的地点（如咖啡馆）或者有一个不太负责任的操作员（:执行备份和设备维护工作的人）。举个例子，比如 Acme Widget 的销售人员 Bob，在某互联网咖啡馆会见了客户 Alice。Bob 用 Word 写下一个报价，并且用 Acme Widget 网站上一种特殊 HTTPS 页面上传申请批准。报价被批准后，Alice 用她的电脑从另一个不同的 HTTPS 页面下载批准的文件。想一下，这份文件的完整程度有多少？对于一个恶意的用户，或者可能是竞争对手来说，发现文件的内容有多大的难度（假定其中包括了专有的定价和规格数据）？

我们应该清楚，答案是“不太难”。因为该文件并不是很完整，而且发现它的内容也不难。咖啡馆提供免费的–无线上网，没有加密。这个文件可能在传送过程中被发现，或甚至可以直接从 Bob 的硬盘中读取该文件，如果者他的手提电脑没有正确配置防火墙。同样的漏洞存在于服务器和 Alice 的硬盘。即使我们假设 Bob

和 Alice 是在各自的办公室，利用他们公司网络的电脑，如果客户端没有得到很好的保护和适当的验证，那么文件可以会被未经授权进行访问和修改。如果一旦对文件中所述条款产生争议，其中一方声称另外一个不同的版本才是原版，在这种情况下，可能较难找到一位专家，去证明哪一个版本才是真正的原版。

你可能知道，对微软的 Word 文件和 Adobe 的 Acrobat 文件都可以进行加密。用其中任何一种方法都可以使文件在任何时候都多少安全一点（在传送和没有传送时）。然而，问这些产品中哪一个提供最好的加密技术，是一个很复杂的问题（这很难回答）。Word 和 Acrobat 的早期版本在加密上相对较弱，其解密应用相当广泛。后来的版本不断加强，但是仍容易受到强制攻击，这也就是说，把一份敏感的 Word 文档转换成为一个有密码保护的 PDF 格式具有几个安全方面的优点。其中一个就是，清除潜在有害的或内部的元数据和隐藏的数据，例如删除只是隐蔽的文本，事实上没有真正删除。Acrobat 同时也提供多种文档签名和控制的功能。

当然，你可以更进一步使用额外的、与 Word 或 Acrobat 无关的安全产品，例如文件加密。有很多这样的加密产品，而且都使用了强大的 Blowfish 算法。

（作者：Michael Cobb　　译者：周甜）