浅析电子信息安全隐患的存在类型

张瑞　伍德章

（解放军 32022 部队）

摘要：复杂的网络业务平台、各种层次的云服务、无处不在的数据访问、多样化的通信网络环境等等，伴随着云计算、大数据、物联网、人工智能等一系列互联网科技的引入，提出了越来越多的信息安全需求。

关键字：电子信息；安全；加密

电子信息安全与我们每个人、每个企业都息息相关。但由于大多数人对于电子信息安全的知识了解甚少，因此很多时候，并不能真正地做好电子信息的防护，从而造成了极大的电子信息安全隐患。电子信息的安全隐患主要有以下几个方面：

第一：系统安全

一个安全的系统可以保护主机和所有运行于其上的软件和硬件。安全是操作系统的一个非常重要的设计目标，操作系统接触（内存、文件、硬件、设备驱动程序等）的每一个资源，都必须从安全的角度进行交互。在开始安装一个全新的系统之前，必须百分之百地确保系统里的软件都是可信的；通过访问控制列表，实现操作系统的基础安全功能；关闭不必要的服务来减少攻击系统的可能；安装安全软件，以及定期和快速地更新系统和基础软件的安全补丁；

强化身份验证的过程，以及限制管理员的数量和权限。

第二：数据安全

数据是核心的电子信息资产，也是绝大多数被攻击的最终目标。不过，对数据进行保护，不能仅仅保护存储在数据库中的静态数据，还要关注动态数据。最常用的方法就是使用加密；要实行身份访问控制，以限制对数据的读取；要对数据的导出尤其是批量导出进行严格的管控；要提供对数据进行操作的各种审计和日志记录；要注重各种非结构化数据的管理，例如网页、邮件、社交工具中被展示和传输的数据。

第三：管理安全

电子信息安全已经不能再靠单纯的防火墙，它需要一个全面的风险管理方法。随着越来越多的大量业务数据，电子信息安全必须得到更高一层的认可、思考、拥护和倡导。可以尝试在企业高层设置首席安全官；并要确保所有部门关键岗位的业务人员得到了与岗位匹配的充分的信息安全知识和技能培训；信息安全部门要了解公司的业务发展，并能够及时发现甚至预测新的信息安全问题；对于负责网络业务研发的部门，应该有专注于信息安全的架构师来测试和处理安全漏洞；要建立跨部门的安全事件响应团队，随时准备调动内外部资源，处理棘手的安全问题；可以适当地与外部信息安全公司合作，以从不同的以及更专业化的角度查找安全问题。

第四：物理安全

传统的观念认为，物理安全性一直与电子信息的安全隐患保持完全的隔离。但是随着技术不断取代纸张和手工操作，物理安全性正日益成为信息安全的重点。数据中心的站点如果建在有可能遭受洪水、地震、台风的地区，则会有显著的风险；锁不再只是为门而设计，任何有价值的东西，都应该在有锁的位置进行保护；物理入侵检测需要深谋远虑，而利用摄像头、警报器等安全设施时，需要经常确认其可用性；随着图像、视频、声纹识别的发展，需要充分认识到，信息的盗取未必一定通过网络。

结合实际生活，比如用手机来接入电脑，那么有可能就会造成资料的泄露，那如果我们的手机有漏洞，被一些黑客攻破，如果手机的端口连入电脑，那么就有可能会导致其他的设备相应的被攻破，即使不被攻破，也会造成一定的损失。针对电子信息保护，我们要时刻保持警惕，要加强电脑抵御，进行相应的防护。对公司资料进行加密，是相对直接的保护措施，有 4 种方法来防止信息泄露：

第一：端口管控

自动识别并限制各种移动存储设备的使用，包括 U 盘、移动硬盘、刻录机、MP3、相机、智能手机、蓝牙、红外、1394、光驱等。而对于 USB 键盘、鼠标、打印机等非存储类的设备则不管控。对于注册授权的移动存储设备，可以允许在指定的计算机上使用，且同一个 U 盘可针对不同的电脑设定不同的读写权限，灵活方便，更贴合管控需求。还可将 USB 存储设备设为加密盘，拷入 USB 存储设备中的数据进行加密，防止因 USB 存储设备丢失而导致数据泄密。

第二：数据加密

强制对计算机生成的文档图纸、源码、office 文档等数据自动透明加密，加密后仅在指定范围内进行数据交互；所有加密过程均为自动和透明，不影响原有工作习惯和管理流程；全生命周期、全流程保护。新建、修改、传递、存储、备份均加密；未授权同意，无论您通过何种途径外发出去，均无法打开。

第三：文件外发管控

严控使用权限，可对外发文件，设置指定的可查看次数、时间，设置是否允许修改、是否允许打印等；禁止拖拽、拷屏、另存为、剪贴板获得和另存等手段获得外发文档内容；超过打开时间或者打开次数外发文件自动销毁；支持所有的类型文件外发包括：CAD 图纸文件、源代码、财务数据报表、office 文件等；对信任的收件对象可设置邮件白名单，邮件发送至白名单中用户时自动解密，提高工作效率。

第四：日志审计和文件备份

提供完整的日志管理，可对所有加密文档的所有操作进行详尽的日志审计，并对审计日志提供查询、导出、备份及导出数据报表等支持。对日常办公中文档的复制、移动、重命名、删除等涉密操作过程做详尽记录，对便于监督检查和事后追溯。提供详细的加密文件备份功能，有效避免了文件因版本更新或者是意外破坏造成的风险，大大保护了企业机密数据的完整性和安全性。

电子信息的安全既独立，又与各个具体的行业领域密切相关。而随着各行各业加快互联网转型的步伐，随着各类关系民生的重要企业全面推进业务上云，随着信息安全产业上升至国家安全战略层面，未来的社会，将需要大量的信息安全方面的人才；未来的企业，也将需要在信息安全方面投入更多的重视。

参考文献：

1. 黑客攻防技术宝典 :Web 实战篇(第 2 版)[英]Marcus Pinto 著

2012 - 07 - 01 人民邮电出版社

2. Python 黑帽子 :黑客与渗透测试编程之道 Justin Seitz (贾斯汀 · 塞茨) 著，孙松柏 李聪 润秋 译 2015 - 08 - 01 电子工业出版社

3. 黑客大曝光：网络安全机密与解决方案（第 7 版）美）麦克克鲁尔，（美）斯坎布雷，（美）克茨著，赵军 等译 2013 - 10 - 01 清华大学出版社