十五个急需解决的典型信息安全问题 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E5_8D_81_E4_BA_94_E4_B8_AA_E6_c98_460922.htm 互联网和IT技术的普及，使得应用信息突破了时间和空间上的障碍，信息的价值在不断提高。但与此同时，网页篡改、计算机病毒、系统非法入侵、数据泄密、网站欺骗、服务瘫痪、漏洞非法利用等信息安全事件时有发生。据公安部公共信息网络安全监察局的调查结果显示，2005年5月至2006年5月间，有54%的被调查单位发生过信息网络安全事件，其中，感染计算机病毒、蠕虫和木马程序的安全事件为84%，遭到端口扫描或网络攻击的占36%，垃圾邮件占35%。未修补和防范软件漏洞仍然是导致安全事件发生的最突出原因，占发生安全事件总数的73%。 目前，许多企事业单位的业务依赖于信息系统安全运行，信息安全重要性日益凸显。信息已经成为各企事业单位中的重要资源，也是一种重要的“ 无形财富 ”，分析当前的信息安全问题，有十五个典型的信息安全问题急需解决。 1、网络共享与恶意代码防控 网络共享方便了不同用户、不同部门、不同单位等之间的信息交换，但是，恶意代码利用信息共享、网络环境扩散等漏洞，影响越来越大。如果对恶意信息交换不加限制，将导致网络的QoS下降，甚至系统瘫痪不可用。 2、信息化建设超速与安全规范不协调 网络安全建设缺乏规范操作，常常采取“ 亡羊补牢 ”之策，导致信息安全共享难度递增，也留下安全隐患。 3、信息产品国外引进与安全自主控制 国内信息化技术严重依赖国外，从硬件到软件都不同程度地受制于人。目前, 国外厂商的操作系统、数

据库、中间件、办公文字处理软件、浏览器等基础性软件都大量地部署在国内的关键信息系统中,但是这些软件或多或少存在一些安全漏洞，使得恶意攻击者有机可乘。目前，我们国家的大型网络信息系统许多关键信息产品长期依赖于国外，一旦出现特殊情况，后果就不堪设想。 4、IT产品单一性和大规模攻击问题 信息系统中软硬件产品单一性，如同一版本的操作系统、同一版本的数据库软件等，这样一来攻击者可以通过软件编程，实现攻击过程的自动化，从而常导致大规模网络安全事件的发生，例如网络蠕虫、计算机病毒、“ 零日 ”攻击等安全事件。 5、IT产品类型繁多和安全管理滞后矛盾 目前，信息系统部署了众多的IT产品，包括操作系统、数据库平台、应用系统。但是不同类型的信息产品之间缺乏协同,特别是不同厂商的产品,不仅产品之间安全管理数据缺乏共享,而且各种安全机制缺乏协同,各产品缺乏统一的服务接口,从而造成信息安全工程建设困难,系统中安全功能重复开发,安全产品难以管理,也给信息系统管理留下安全隐患。 6、IT系统复杂性和漏洞管理 多协议、多系统、多应用、多用户组成的网络环境，复杂性高，存在难以避免的安全漏洞。 据SecurityFocus公司的漏洞统计数据表明，绝大部分操作系统存在安全漏洞。由于管理、软件工程难度等问题，新的漏洞不断地引入到网络环境中，所有这些漏洞都将可能成为攻击切入点，攻击者可以利用这些漏洞入侵系统，窃取信息。1998年2月份，黑客利用Solar Sunrise漏洞入侵美国国防部网络，受害的计算机数超过500台，而攻击者只是采用了中等复杂工具。当前安全漏洞时刻威胁着网络信息系统的安全。 为了解决来自漏洞的攻击，一般通过打补丁的方式来增强系统

安全。但是，由于系统运行不可间断性及漏洞修补风险不可确定性，即使发现网络系统存在安全漏洞，系统管理员也不敢轻易地安装补丁。特别是，大型的信息系统，漏洞修补是一件极为困难的事。因为漏洞既要做到修补，又要能够保证在线系统正常运行。 7、网络攻击突发性和防范响应滞后 网络攻击者常常掌握主动权，而防守者被动应付。攻击者处于暗处，而攻击目标则处于明处。以漏洞的传播及利用为例，攻击者往往先发现系统中存在的漏洞，然后开发出漏洞攻击工具，最后才是防守者提出漏洞安全对策。 