信息化建设中网络安全防护的对策

白金明

水利部海河水利委员会引滦工程管理局 河北 唐山 064300

【摘 要】：随着信息时代的到来，人们对建立信息网络安全性的兴趣日益增加，计算机的使用正在逐渐发生变化。如今，有关人的信息存储在网络中，那么如何最好地构建信息网络安全性呢？自网络开始以来，网络安全一直是我们面临的尤其重要的问题。随着网络安全信息化的不断发展，人们越来越关注它，外部通信，电子商务，信息平台等与网络密不可分，在使用网络时，如何保护公司网络的安全性，以防止其信息和数据被盗或泄漏是当今社会信息安全的主要领域之一。

【关键词】：信息化；网络安全；

引言

在最初出现时，计算机技术非常零散，在数据处理和网络方面相对较差。但是，随着时间的推移，网络技术也发生了显著发展。在这种环境下，计算机的功能变得更加多样化，计算机信息处理的复杂性也大大提高。此外，随着互联网时代的到来，已经收集了异构和独立的信息，并且还构建了非常大规模的数据信息系统。人们经常使用信息来促进我们的国家信息化发展过程。但是，在信息网络不断发展的过程中，信息和数据安全问题变得越来越重要。在各种开放网络和电子商务平台环境中，一些非法员工也可能入侵并最终影响整个网络的安全性。因此，即使在信息网络时代的环境中，如何成功地建立信息网络的安全性也已成为重要的问题，为了为信息网络的安全性建设做出贡献，我们提出了适当的保护技术和措施。在当今的社交环境中，计算机通过不断发展和优化逐渐提高其数据处理能力。建立网络后，它将构建一个巨大的信息数据平台，该平台可以集成和管理所有看似独立的信息，不仅可以确保信息的准确性，还可以加快操作速度。信息网络平台的泛滥为许多罪犯提供了机会。他们的非法活动不仅导致数据和信息的丢失，而且给人们造成了严重的问题。因此，在信息网络的基础上，加强安全管理和安全防护工作在实践中非常重要。

1、计算机安全概念

根据国际标准协会（ISO）对“计算机安全”的定义，计算机安全基本上是数据处理系统的创建，技术的应用和管理以及计算机软件和硬件的保护的一系列的保护措施。防止信息被故意毁坏，被盗，遗失或被篡改。计算机安全的内容从两个方面描述了计算机安全性的有效性：物理安全性和逻辑安全性。逻辑安全是我们通常所说的信息安全，科学合理的规划方案可确保信息和数据的准确性，可行性和可靠性。基于适当的保护，它彻底调查了信息和数据的安全性，并在网络安全管理中发挥了作用。网络安全也可以说是确保信息和数据严格，准确和实际地工作。

2、影响网络安全的主要因素

2.1 网络系统本身存在的问题

这主要体现在以下几个方面：稳定性和可伸缩性；未经调整的网络设备配置；缺乏安全策略。另外，许多 Web 应用程序站点在不知不觉中扩展并忽略了防火墙配置权限，精明的人可以滥用您的许可，访问控制的配置太复杂，容易出现配置错误，使其他人可以使用它们[1]。

2.2 来自内部网的安全威胁

许多事实证明，我们企业内部的日常安全威胁远大于外部的威胁。由于缺乏用户的安全意识，许多应用程序服务系统没有密切注意访问控制和安全通信。另外，如果系统配置不正确，则容易丢失数据。由于管理系统不完善，网络日常管理和维护中的人为安全漏洞可以说是对整个公司网络的最大隐藏安全威胁。同时，网络管理员和网络用户具有相应的特权，使用这些特权破坏网络存在安全风险。如果工作密码泄露，则硬盘上的机密信息将会被他人使用，并且盗窃回收站中没有及时清除或删除的临时文件夹和文件，给别人窃取信息的机会。禁用与网络安全性相关的安全性机制对公司 Intranet 用户没有用，特别是在某些安装了防火墙的网络系统上[2]。

2.3 缺乏网络系统安全性的评估和有效的监管手段及硬件设备的正确使用

安全评估和网络分析要求您检查网络的整体安全性，以发现可能被黑客和故意攻击者利用的漏洞。通过评估和分析网络系统的安全状态，可以为已发现的问题提供解决方案和建议，并提高网络系统的安全性和稳定性。因此，用于评估和分析网络安全性的技术是一种相对有效的安全性技术。

2.4 不断更新的黑客手段

在大多数情况下，人们需要带头发现以前未知的安全问题。这些条件的存在太慢，无法响应新的安全问题[3]。当安全工具发现一个安全问题并尝试更新该安全问题的某些方面时，其他安全问题再次发生。诸如消防员之类的防护工具不断地精疲力尽，并成为安全问题的追随者。

3、保证网络安全的有效措施

网络安全问题现在是我们最紧迫的问题之一，从当前网络发展的角度来看，不可能保证绝对的网络安全，但仍然是可控的。可以在技术水平上对其进行控制，在一个稳定的区域中，网络安全实际上是理想安全措施和实际实施之间的平衡。建立网络安全性是一项复杂而乏味的任务。由于涵盖了广泛的内容，因此它不仅包括技术问题，还包括管理研究。因此，在构建网络安全性时，人员素质、专业技术可以作为起点，这两个方面旨在提高网络的安全性。

1）根据有关规定和网络安全措施，不仅要完善网络安全管理体系，还应加强安全实施和培训以及人员培训。

2）改进的网络病毒防护。由于病毒的传播媒介是网络，因此独立产品的防病毒软件越来越无法满足病毒清除的需求，因此需要安装防病毒软件以检测网络病毒并终止其功能。特别是这些地区中的不同公司，机构，政府机构和学校使用两种形式：本地网络和全球网络。因此，在规划网络安全性时，需要基于原始服务器创建一个更完整的总部。为了全面提高整个网络中计算机的安全性以及用于检查和销毁服务器上病毒的软件系统，应该为下一个子服务器开发相应的防病毒软件。更新防病毒软件不仅可以管理和阻止特定病毒，还可以使监视区域更全面和更立体，从而提高网络的安全性。

3）防火墙是网络安全的最重要障碍，也是监视网络安全的主要障碍。使用正确的设置，可以正确地监视访问人员，事件和说明。只有批准的步骤才能继续进行下一步。运行时，可以直接隔离有害程序，确保系统不受恶意软件篡改，并确保网络安全。

4）选择正确的入侵检测系统。现在，入侵是窃取企业中重要文件或破坏网络的最常见方法，网络安全的主要目标是主动检测并检测入侵。因此，选择正确的入侵检测系统，防火墙和防病毒软件是确保企业信息安全和减少相关损失的最有效方法之一。

5）网络系统可以通过配置网络安全墙，监视 Eamil 邮件和审核 FTP 数据来有效控制 Web 应用程序，Internet 访问和系统漏洞[4]。同时，安装和配置类似软件也可以提高漏洞扫描的速度和准确性。扫描完成后，程序将自动生成针对扫描过程中出现的问题的解决方案，以帮助系统完成最终修复并随后修复网络安全漏洞。

6）通过将 IP 地址绑定到计算机网卡的 MAC 地址，可以改善 IP 地址被盗的问题。当 IP 地址通过中央交换机访问地址或 Internet 时，中央交换机检查以查看请求的 IP 地址是否与绑定的 MAC 地址匹配，如果不匹配，则拒绝通过并发送 IP 广播警报信号。

结束语

简而言之，网络安全是一个复杂的主题，包括技术，管理，使用等，包括物理和逻辑技术措施以及信息系统本身的安全性，一种技术只能解决一个问题，这不是万能药。唯有开发和实施一个相对完整的网络安全系统，并采用一种将管理和技术相结合的集成方法来主动检测，预防和控制网络安全事件，并防止网络安全事件的发生。这只能通过进一步增强主动预防功能来实现。它有效地维护了网络安全性，并提高了业务系统的整体计算机化水平以及网络系统的安全性。

参考文献：

[1] Stallings.W.网络安全基础应用与标准.

[2] WilliamStallings.原理与实践（原书第 3 版).机械工业出版社，2016.

[3] 姚淑萍,彭武,吴丹.网络安全预警防御技术，2015.

[4] Chris，Sanders，Jason，Smith.网络安全监控：收集、检测和分析.机械工业出版社，2015.