构建人社电子信息工程安全通信防护策略

高建玲
山东省菏泽市曹县人力资源和社会保障局　山东菏泽　274400

【摘　要】当今社会随着信息技术的飞速发展，人社电子信息工程项目也已经成为现代生活中的重要部分，在保护好个人信息、劳动保障等各类数据安全方面发挥着至关重要的作用。建立安全的通讯防护系统，有效保护信息电子工程的信息安全显得非常重要和必要，本文主要从人社电子信息工程起因分析入手，分析了目前所面临的主要网络安全问题，并提出了相应的安全防护对策与措施，运用安全防护框架、数据加密保护及隐私保护措施、网络入侵检测体系等诸多方法对人社信息系统进行有效的防护，从而提高人社信息工程的安全保护能力。

【关键词】人社电子信息工程；安全通信防护；网络安全；数据加密；隐私保护

Construct the security communication protection strategy of social electronic information engineering

Gao Jianling
Human Resources and Social Security Bureau of Cao County，Heze City，
Shandong Province Cao County，Heze City，Shandong Province　274400

【Abstract】With the rapid development of information technology，human resources and social electronic information engineering projects have become an important part of modern life，playing a vital role in protecting personal information，labor security and other data security.Establish security communication protection system，effective protection of information electronic engineering information security is very important and necessary，this paper mainly from the social electronic information engineering cause analysis，analyzes the main network security problems，and puts forward the corresponding security protection countermeasures and measures，using the security protection framework，data encryption protection and privacy protection measures，network intrusion detection system，and many other methods to effectively protection of social information system，so as to improve the ability of social information engineering security protection.

【Key words】social electronic information engineering；security communication protection；network security；data encryption；privacy protection

引言：

电子信息工程随着信息化时代的进步逐渐应用于社会各个环节，如今，电子信息工程在人力资源和社会保障领域中应用范围不断扩大，这同时也对人力资源和社会保障信息系统的安全性提出更严峻的考验。由于人社电子信息工程中的信息包含敏感信息，其复杂网间交互对系统本身的安全性通信防护更具有保障意义，本文结合实际情况对其安全通信保护面临的挑战进行全面的研究，并提出相对应的防护对策，为具体实践应用提供指导参考。

1.人社电子信息工程安全通信防护概述

1.1 人社电子信息工程的背景意义

人社电子信息工程在现代生活中发挥着重要作用，尤其是关系到政府、企业单位及个人之间的社会保障管理工作和人力资源工作管理。伴随着信息技术迅猛发展，人类社会资源在人社领域里的一些工作逐渐实现了电子信息化、网络化、自动化，从而便于相关的信息管理工作，但是与此同时信息化过程也会导致参与人力资源和社会保障管理的各类数据，包括社保、养老金、医疗保险等诸多环节所涉及的信息数据的交换与存储之间存在更高程度的安全威胁，因此如何落实人社电子信息化的安全措施，尤其体现在数据的传递与存储数据的过程环节，在于维护社会资源稳定、维护个人权益发挥了关键作用。

1.2 安全通信防护的基本概念需求

安全通信防护主要是指信息在进行传送过程中，采取各种措施进行数据保密、保证完整性、可靠性。杜绝信息在传送过程中的泄露、损坏和伪造。对于一个信息系统而言，信息安全防护不是技术问题，它是系统和信息系统能否顺利开

展工作的必要条件。随着信息系统信息的交换频率和类型不断增加，其防护安全措施越来越完善。无论个人数据还是法律，都需要有完善的防护，为了防止系统的不稳定因素和人为因素，可以利用有效的保护措施来防止外部的攻击、内部的分配错误、人为干扰的风险，从而保证系统正常、安全的运行。

2.人社电子信息工程安全通信防护的挑战

2.1 网络安全威胁攻击类型

由于信息技术的发展，在人社电子信息工程建设过程中会产生一些复杂的网络安全威胁问题，其中外部攻击是常见的网络安全威胁之一。在外部攻击中常见的攻击形式有拒绝服务攻击（DDoS）、恶意软件攻击、钓鱼攻击、数据窃取和数据破坏等。拒绝服务攻击主要包括系统收到的恶意请求过多而造成服务不可用的情况；恶意软件攻击主要包括病毒、木马等软件侵入系统，窃取或破坏用户的信息与系统；钓鱼攻击指的是将假网站或邮件等方式来诱骗用户以提供其个人信息；数据窃取攻击与数据破坏攻击也是比较常见的，在黑客入侵防护系统后获取部分或全部敏感数据，从而侵犯了信息系统完整性和保密性，并对数据泄露进行了攻击。

2.2 系统漏洞安全隐患分析

系统漏洞是造成电子人社信息工程安全的因素之一。系统漏洞是指在软硬件配置、系统设计、实施维护中出现的漏洞，是攻击者或应用程序能够加以利用来破坏系统的信息安全。系统漏洞主要出现在系统安全性或强度上的不足，包括缺少安全认证机制、输入验证过少、访问权限管理过疏、无机密性或完整性等保护措施以及文件上传和下载防护的不足；另外，有些信息工程漏洞还包括信息安全程序及系统的错误，信息工程在技术上不可靠，从而使攻击者或入侵者可以趁虚而入；由于文件系统控制不严格，导致文件被截断，使得文件失去其本来的意义，关键信息被删除或文件无法使用。例如个人信息和社会保障信息等。除此之外，还存在着系统更新、补丁更新滞后的风险，系统更新滞后则可能会丧失漏洞防护能力，未修复的系统漏洞则可能成为攻击者的突破口[1]。系统设计人员需要加强系统安全隐患的排查和修复，定期开展系统漏洞扫描审计活动，保证信息系统的全程安全。

2.3 防护技术实施中的难点

安全通信防护在实施的过程中，技术的选用和运用势必会面对诸多问题。安全防护技术的复杂性需要相关的各方共同协作完成，这些需要网络技术安全、数据加解密、身份认证等多种技术支持，对技术人员的专业能力提出了较高的要求。在人社电子信息工程中，数据的传输量大，频率高，如何在保障系统高效率运行情况下实现数据的大范围加密和保护是其存在的一大问题。不同的防护技术之间存在兼容问题，在融合使用时，安全防护可能会留下缺口[2]。此外，安全防护技术更新迅速，攻击者的方式不断地转变，对于防护体系的即时应答能力是防护技术的必需品。这些问题都造成了防护技术操作的难度，所以在编制防护方案的时候，应统筹考虑防护的技术运用上的可行性以及防护效果。

3.构建人社电子信息工程安全通信防护策略

3.1 安全防护架构设计

在设计人社电子信息工程安全防护体系架构时，应该首先确定安全防护的目标，即保持系统的完整性、保密性和可用性的目标。为了保证系统应对所有网络攻击和泄密的风险，安全防护体系架构的构建应该从不同的层面进行全面的安全防御体系构建。人社电子信息工程一个安全防护体系架构的设计应该是由安全需求分析开始，通过识别系统的重要资源以及主要的安全数据，并识别和评估目前系统的安全风险。安全风险分析为下一步的安全防护设计提供了思路，首先是在网络层面上对整个网络安全进行控制，包括对外的网络控制以防止网络攻击，包括恶意流量以及恶意访问；使用防火墙、入侵检测及防御系统（IDS/IPS）能够有效防止外部攻击，以及屏蔽来自网外的恶意流量。其次是对于整个应用进行安全防护，主要是防止应用本身漏洞所带来的风险。应用层应该遵守安全编码原则以杜绝出现常见的 SQL 注入、XSS 等漏洞问题，也要加强对于用户输入内容的核查，同时需要对系统进行定期漏洞扫描和代码审计以发现各种潜在的漏洞问题并且及时修复。数据在传输及存储阶段的安全也很重要，数据加密是整个系统信息安全防护的重要策略，对于静态存储和动态传输的数据都应该进行强加密以防止被窃听、窃取或篡改；存储的敏感数据还应该加密，并控制该敏感数据的访问权限[3]。数据备份与灾难恢复，为了防止由于意外情况出现而导致数据丢失，需要定期进行备份与异地备份，备份的数据要加密存储，防止数据泄露。安全防护架构的设计要考虑可扩展性、灵活的变化，满足技术发展需求与需求的变化。架构要兼容应用新安全技术、对新安全威胁反应快速。总之，一个安全防护架构设计是全方位的、多层次的综合防护，包括网络防护、应用防护、数据防护、物理防护。

3.2 数据加密隐私保护技术

数据加密在信息技术的信息化时代显得越来越重要，而且在信息加密过程中，所保护的对象都是用户的重要隐私，

对信息化时代的人社电子信息工程来说，更要运用数据加密技术。数据加密技术主要是确保在信息在存储或者传输过程中，在信息被截获的情况下，保证攻击者无法解密。目前，加密技术主要采用对称加密技术和非对称加密技术进行数据加密，其中对称加密技术是在加密以及解密时使用相同的密钥，适合比较大的信息进行加密；而非对称加密技术主要使用公钥和私钥，这被运用在信息传输过程中对信息进行加密。虽然数据加密是必不可少的隐私保护技术，但在隐私保护技术中还存在着数据匿名化和去标识化[4]。在对个人的数据保护中，数据的去标识化采用的是脱敏技术，主要是通过脱敏手段对个体数据的敏感性信息脱敏或者对数据信息进行一定的处理，不能直接暴露给其他用户，从而确保用户身份信息的隐私安全。而数据的匿名化则是需要对信息数据进行匿名化，那么就可以避免通过数据信息的某些特征将个体与其关联起来，进一步做好个体隐私的保护。

3.3 网络入侵检测防护技术

IDS/IPS 作为信息安全防护的一种方式之一，在信息安全防护中发挥着关键作用。人社电子信息工程系统面临的威胁不仅仅包括外部侵入，还包括内部人员进行恶意破坏，而 IDS（入侵检测系统）作为信息安全防护的一种手段，能够实时监控系统中的网络流量，并通过监控数据包、流量状态以及协议动作等判断是否有恶意行动或攻击行为，当发现行为异常，可以发送警报提醒安全管理员进行相应的防护操作[5]，而 IPS（入侵防御系统）则是在 IDS 的基础上实现自动化防护，在监测到攻击或异常时，会发出警报并进行实时的防御，及时阻断恶意流或攻击路径，从而降低系统的损失。例如通过 IPS 检测到并阻断对 DDoS 攻击、SQL 注入攻击等。为了能够更加准确地检测和防御，IDS/IPS 还需要与防火墙、数据包过滤技术、行为分析技术等相结合，进行多层面的防护，同时还需要 IDS/IPS 保持更新的数据库来应对新型的攻击和漏洞威胁。

3.4 多层次安全防护方案的实施

多层安全防护机制是针对复杂安全威胁的有效技术方法，即在不同的层次采用防护手段来保证系统能抵御来自不同层面的攻击。针对人社电子信息工程的防护策略除了常见的网络层的防护措施，也包括应用层、数据层等防护。网络层面是安全防护的基础层次，也是典型的防护技术，例如在工程中采用部署防火墙、IDS/IPS、反病毒等网络安全防御手段，使得攻击流量在进入内部系统前得不到有效处理。而对于工程中可能涉及的用户请求处理、数据处理等行为，应用层则显得更为重要，防止被外部攻击者利用以入侵信息系统。因此，在开发阶段可以对于应用的代码进行代码审计、漏洞扫描及修复等方式来进行应用安全的防护。而在数据层面，采用常见的对数据的加密保护以外，需通过采用对数据的访问控制等手段来保证数据的安全。例如在数据存储时采用数据库的加密保护、存储加密以及数据库的备份策略等[6]。此外，多层安全防护机制还涉及物理安全的防护。即使在网络及应用层面防护措施都较完善，也依然能够有攻击者通过物理层面来攻击系统本身，例如针对数据中心等重点建筑物的安防措施。因此在保证物理环境安全层面，对重要机房、服务器等采用严格的访问控制等防护措施，例如门禁系统和监控设备等。通过多个层次的安全防护机制，可使工程能够对于每个防护层面，能够起到较好的安全防护，极大增强信息系统的抗攻击能力。

结束语：

综上所述，技术在不断进步，人社电子信息工程项目的安全防护通信所面对的安全威胁与挑战也在随之变革和演变，在做好技术防护的同时，对政策和法规的进一步完善也是保障信息安全不可缺少的重要构成部分，文中提出的多级安防防护策略不仅可以很好的解决当前面临的安全威胁问题，还为未来信息系统的安全发展保驾护航，文中研究内容希望对人社电子信息工程的安全防护通信给予更多实践上的参考。

参考文献

[1]王磊，李晓东.信息安全与隐私保护技术研究[J].网络安全技术与应用，2022，21（05）：45-47.
[2]张涛，刘海波.网络安全防护技术的应用与发展[J].计算机安全，2020，36（09）：13-15.
[3]李鹏飞.网络入侵检测与防护技术研究[J].信息系统工程，2021，19（03）：60-63.
[4]陈建华，王志强.数据加密技术在信息安全中的应用[J].信息与电脑，2021，33（04）：78-80.
[5]郑伟，王莹.信息系统安全防护架构的设计与实现[J].计算机与信息技术，2020，28（06）：92-94.
[6]刘丹，张鸿.网络安全防护措施与技术分析[J].现代计算机，2022，41（12）：49-52.