|  |
| --- |
| **成绩** |
|  |



**本科生课程论文**

**论文题目：**《我国网络安全的现实需要与保障体系研究》

**课程名称：** 信息安全原理与应用

**任课教师：** 赖祥伟

**专 业：** 软件工程（中外合作办学）

**班　　级：** 2022级01 班

**学　　号：** 222022321062009

**姓　　名：** 吴孜远

2024年 5月26日

我国网络安全的现实需要与保障体系研究

1. 信息安全的重要性

在当今数字化时代，我们每个人的生活生产都与互联网密切相关，特别是随着大数据、AI等技术的快速发展，信息安全问题形势严峻。保证信息安全对于维护国家安全、社会稳定、企业和团体利益以及个人安全至关重要。

一个国家的军事通信系统如果遭受网络攻击，可能会导致军事行动泄露或失败，从而危害国家安全；如果一个城市的交通控制系统遭受网络攻击，可能会导致交通混乱，甚至引发交通事故；一家零售商的顾客数据库如果被黑客窃取，会导致客户信息泄露，造成巨大的经济损失；个人银行账户信息如果因为安全漏洞被不法分子获取，可能会导致账户被盗，个人财产遭受损失。这些在我们看来好像并不常见，这是当前信息系统安全保障工作的功劳，但这些事故并非完全被避免，信息安全仍需增强。

我们接下来根据一个案例来理解信息安全保障发挥的重要作用，只是一个小案例，但与我们的专业甚至以后的工作息息相关。2023年10月，经浙江省网信办查实，杭州某科技公司旗下某生活类APP相关数据库服务端口直接在公网中开放，未按要求履行数据安全保护义务，违反《数据安全法》第二十七条，浙江省网信办对该公司作出罚款5万元的行政处罚。

这个案件的脆弱点很明显，就是暴露在公网中的数据库端口。威胁包括被黑客攻击导致数据泄露，或者注入恶意代码。为什么我选择这个案例呢？**首先是因为老师上课刚好讲了此类问题的一种解决方法**，就是在公网和数据库之间建立缓冲区，防火墙较为宽松，公网连接缓冲区中的应用程序接口；数据库被藏在最底层，被最严格的防火墙保护，公网无法直接访问。还有个原因是前段时间刷到了一个帖子说老板想将数据库开放在公网，分配一个公网IP，供出差人员使用，跟这个案件很像，这当然是很危险的，需要做好防护，所以这个帖子的评论区异常热闹。

1. 我国信息安全保障体系

要进行信息安全系统设计工作，首先要明确法律法规、技术标准和产业政策。接下来我们研究一下这些法律政策和标准。

**法律法规**目前仍在不断完善，几乎每年都有新的法规出台。目前最主要的法规有这四个：《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《网络数据安全管理条例（征求意见稿）》。接下来我分别总结一下这四部法律的关键内容：

《中华人民共和国网络安全法》保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民合法权益。

《中华人民共和国数据安全法》规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。企业必须建立完善数据安全管理制度和技术保护机制（本文提到的案例就是因为违反本法规）。数据处理者发现其使用或者提供的网络产品和服务存在安全缺陷、漏洞，或者威胁国家安全、危害公共利益等风险时，应当立即采取补救措施。

《中华人民共和国个人信息保护法》保护个人信息权益，规范个人信息处理活动，促进合理利用个人信息。

《网络数据安全管理条例（征求意见稿）》该条例结合《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规，对实现我国数字经济健康发展、依法保障数据安全等方面具有重要意义。国家应对个人信息和重要数据进行重点保护，对核心数据实行严格保护。

**技术标准**也是在经过不断地修改后形成了比较完整的一系列标准。我这里选出了四个使用最为广泛的标准：

《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）：这个标准提供了一套评估信息安全风险的方法论，为组织提供了一套系统的风险管理流程，包括风险识别、风险分析、风险评价和风险处理等步骤。

《信息技术 安全技术 信息安全管理体系 要求》（GB/T 22080-2016）：为组织建立和维护信息安全管理体系提供了一套要求。它涵盖了从风险评估到风险管理的全过程，帮助组织保护其信息资产。

《信息安全技术 网络安全等级保护基本要求》（**GB/T 22239-2019**）：该标准规定了不同安全保护等级的对象应具备的安全保护能力，并提出了相应的安全通用要求和安全扩展要求

《信息安全技术 关键信息基础设施安全保护要求》（GB/T 39204-2022）：此标准专注于关键信息基础设施的保护，明确了保护这些基础设施所需的安全措施和要求。它的目标是确保这些对国家安全至关重要的信息系统的安全性和稳定性。值得一提的是它重点对于身份安全鉴别与授权提出明确的要求。

至于产业政策，它可以说是基于法律法规和技术标准，给出国家的或者地方的政策支持或者限制等。比如《“十四五”国家信息化规划》做出整体安排。这里我认为前面都已经提到，所以并不做详细介绍。

以上就是我国的信息安全保障体系，学习下来感觉很完善，也很贴合时代，看得出来是一次次案件堆起来的。提出的标准和要求很严格，很考验从业人员的能力啊。不过有标准总比大家纯发挥想象力要科学的多，安全的多

1. 政策、法律、技术对信息系统的影响

政策、法律和技术对信息系统的影响是贯穿于整个生命周期的，从**设计、建设到运维**，每个阶段都需要遵循相应的规范和标准，以确保信息系统的安全性、合规性和高效运行。

在信息系统的设计阶段，遵循相关法律法规和技术标准是确保系统安全性和合规性的基石（不遵守法规谈何合规嘛）。必须要遵守如《网络安全法》、《数据安全法》和《个人信息保护法》等法律对数据保护、用户隐私等方面的规定。这就不得不提到我们上文中讨论的将数据库服务端端口暴露在公网的案例，它显然就没考虑对数据的保护，违反《数据安全法》。另外，设计团队需要依据国家和国际上认可的技术标准，来指导系统架构、数据存储、传输安全等方面的设计。符合技术标准的技术或协议才是可靠安全的。这些都都是项目负责人必须熟知和考虑到的问题，否则就是在破坏整个数字化社会的安全。

建设阶段是将设计蓝图转化为实际运行系统的阶段，此阶段的安全措施至关重要。光设计得好还不够，得选择合适的技术实现系统，符合预期没有漏洞才行。比如最重要的是需要实施数据加密和数据备份等具体的措施，确保存储和传输的数据安全。构建访问控制机制，如基于角色的访问控制(RBAC)，确保只有授权用户才能访问敏感数据和资源。部署网络安全设备和软件，如防火墙，以防御外部攻击和内部威胁。最后进行系统测试，包括安全测试和渗透测试，以发现并修复潜在的安全漏洞。简单地说，这些技术虽然实现在各个层次，但都是为了保护数据的安全。

运维阶段是信息系统生命周期中持续时间最长的阶段，系统上线之后也应该提供持续的安全维护。执行持续的安全监控措施，利用入侵检测系统(IDS)和安全事件管理系统等工具，实时监测可疑行为并及时作出反应。制定详尽的安全事件响应计划并不断更新，确保相关人员了解并能够迅速有效地执行，以应对任何安全事件。随着新安全漏洞的发现和技术的迭代，也要定期对操作系统、数据库管理程序和应用程序等进行更新和添加补丁，保证这些技术的兼容性和安全性。运维阶段就是在不断更新系统，提升其安全性，同时也要时刻检查系统是否符合我国的相关法律法规，不能因为一次不合理的更新酿成大祸。

参考文献：

[1]郑平亮.(2024).数据隐私保护与个人信息安全的法律规制研究. 法制博览(12),33-35

[2]姜盼盼.(2019).大数据时代个人信息保护研究综述. 图书情报工作(15),140-148. doi:10.13266/j.issn.0252-3116.2019.15.016.

[3](2022).《信息安全技术关键信息基础设施安全保护要求》国家标准发布.信息网络安全(12),96.

[4]朱琳 & 陆明.(2020).信息系统建设者视角下生命周期安全管理研究.信息安全研究(12),1139-1144.

[5] 山石网科.（2022）. [知乎回答]. 在 知乎专栏. (请问国内有哪些与信息安全相关的政策法规？) 知乎. 2024年5月26日，https://www.zhihu.com/question/458842343