计算机网络信息安全及其防护对策

柴桦

西部战区陆军参谋部，甘肃兰州，730000；

摘要：随着计算机网络技术的普及，信息传递与存储的效率大幅提升，各类数据资源的交互愈发频繁，与此同时，计算机网络信息安全问题也随之凸显，对信息的完整性、保密性与可用性造成威胁，影响个人信息权益与社会信息环境稳定。本文从计算机网络信息安全的核心内涵与主要威胁入手，分析威胁产生的关键原因，进而提出针对性的防护对策，旨在为构建安全、可靠的计算机网络信息环境提供思路，保障网络信息在传输与存储过程中的安全。

关键词：计算机网络；信息安全；安全威胁；防护对策

DOI：10.69979/3041-0673.26.03.025

引言

现在数字化发展越来越快，计算机网络已经走进生活、工作和生产的方方面面，成了大家交换信息、共享资源的主要工具。有了计算机网络，信息不用再受时间和地点的限制，能快速传递，不仅让整个社会运转得更快，也让每个人的生活更方便。但网络本身是开放的，还能和其他网络连在一起，这也给安全风险创造了条件，让原本信息存储和传递的安全边界变得不再牢固。要是网络里的信息被偷偷泄露、故意改掉，或是恶意破坏，造成的影响会扩散到很多方面。对个人来说，隐私可能会被曝光，进而被人冒用身份、偷走钱财；对公司或单位来说，核心的经营数据、关键技术资料可能会泄露，打乱正常的工作流程，让自身的竞争力变弱；对公共领域来说，如果涉及公共服务、社会管理的信息出了安全问题，还会影响公共信息的安全秩序，甚至冲击社会稳定。所以，弄清楚计算机网络信息安全到底包含哪些内容，把藏在网络里的安全威胁和背后的原因都理明白，再制定出科学、管用、能落地的防护办法，就成了现在保障网络信息安全、避开数字化发展风险、让数字化好好发展的重要事，这对保护个人权益、稳住单位运行、筑牢公共信息安全防线都很重要。

1 计算机网络信息安全的核心内涵

计算机网络信息安全不是只做某一方面的防护，而是围绕信息从产生、传递、保存，到使用、销毁的整个过程，搭建的一套全面的安全保障体系。它最核心的目标和要求，就是保证网络里的信息，在传递、保存、使用这几个关键环节，一直都具备完整性、保密性和可用性这三个核心特点。

1.1 完整性：计算机网络信息安全的基础

完整性是计算机网络信息安全的基础特点，它的核心意思是：网络里的各种信息，在整个传递和保存的过程中，不会被没经过允许的人、单位，或是非法程序，进行修改、删除，或是偷偷添加内容，始终保持信息刚产生时的原始样子和真实属性，不会出现任何没经过允许的内容改动或形式调整。从信息的实际价值来看，不管是个人平时聊天的文字、视频、语音，还是公司、事业单位在运转中产生的核心业务数据、管理数据，这些信息要发挥作用，都得建立在信息完整、真实的基础上。一旦信息的完整性被破坏，信息本身的价值会大幅降低，甚至完全没用。更严重的是，被改过后的信息可能会传递错误的内容，进而导致后面做决策出错、做事方向走偏等一系列连锁问题。比如，在网络传递数据的时候，如果涉及业务订单、交易凭证这些关键数据被恶意修改，可能会直接让业务流程断了，引发交易纠纷，造成经济损失；在保存信息的时候，如果公司的核心规划文件、过去的业务档案这些重要文件被偷偷删掉，又没有做好备份，可能会造成再也找不回来的信息损失，对公司长远发展带来不好的影响。由此可见，完整性是保证网络信息能被有效使用、避免信息被滥用的首要前提，也是搭建计算机网络信息安全体系的基础。

1.2 保密性：计算机网络信息安全的关键

保密性是计算机网络信息安全的关键特点，它的核心意思是：网络里那些比较敏感的信息，只对经过合法允许的特定的人或单位开放访问权限，任何没经过允许的人或单位，都没法通过任何方式获取、查看、复制，或是泄露这些信息的具体内容，确保敏感信息的传播范

围一直能控制得住。因为网络信息的所属者和类型不一样，不同信息需要保密的程度和等级也有本质区别，得根据不同情况制定不一样的保密办法。从个人层面来说，需要保密的敏感信息主要有身份证号、家庭住址、手机号、银行卡号、收支记录等，这些都和个人隐私、财产安全有关；从公司或单位层面来说，需要保密的敏感信息包括企业的经营数据、财务报表、核心技术资料、产品研发方案，还有事业单位的管理流程、专项工作方案等，这些都和单位的核心利益、竞争力有关。这类敏感信息一旦泄露，会给信息所属者带来直接且严重的伤害。对个人来说，可能会面临隐私曝光、身份被冒用、钱财被偷等风险；对公司或单位来说，可能会导致竞争力下降、经营策略被竞争对手知道、业务发展陷入被动，甚至引发法律纠纷，造成经济损失。所以，做好保密性保障，核心是建立一套严格、准确的“授权访问”规则，通过技术手段，比如加密、身份验证，再加上管理规定，比如权限管理制度、信息保密守则，一起发挥作用，严格控制谁能访问信息，从源头挡住非法获取和传播信息的渠道，保证敏感信息的安全。

1.3 可用性：计算机网络信息安全的保障

可用性是计算机网络信息安全的保障特点，它的核心意思是：当经过合法允许的人或单位需要使用网络信息时，能在需要的时候，顺畅、高效地拿到想要的信息，而且用来保存和传递信息的网络系统、存储设备，比如服务器、硬盘、云存储平台，要一直保持正常运行，不会因为各种安全问题，比如恶意攻击、病毒感染、设备坏了，导致信息没法访问、没法读取，或是网络系统、存储设备瘫痪、没法用。可用性直接决定了网络信息的实际价值能不能真正发挥出来，是连接信息安全和信息使用的关键。就算网络信息的完整性和保密性都做得很好，但如果因为没法使用，导致经过允许的人或单位拿不到、用不了这些信息，那信息本身的价值就没法变成实际用处，甚至会变成“没用的信息”。比如，要是企业的业务系统被黑客攻击，导致网络瘫痪，就算系统里存的客户数据、订单信息都完整，也没被泄露，员工也没法正常登录系统、处理业务，会直接导致企业业务中断，影响客户体验，让企业少赚钱；要是保存单位核心数据的硬盘坏了，又没及时修好，会导致数据没法读取，就算数据本身没被破坏，也没法给单位做决策、推进业务提供帮助，进而影响工作和业务的正常进度。由此可见，可用性是让计算机网络信息安全的价值落地、保证信息能正常使用的重要支撑，也是搭建网络信息安全体系时，不能少的核心环节。

2 计算机网络信息安全面临的主要威胁及成因

2.1 主要安全威胁

计算机网络信息安全的威胁有很多种，还会随着网络技术发展不断变化，核心能归为三类，分别影响信息的完整性、保密性和可用性，破坏网络信息安全稳定。一是信息泄露威胁，主要针对信息保密。指敏感信息被没经过允许的人或单位获取，分主动偷和被动漏两种。有的是用技术手段偷偷突破网络防护，拿到存在设备里或正在传输的信息；有的是因为防护做得不到位，信息在使用时不小心暴露。这种威胁会直接让个人隐私和单位核心信息泄露，引发后续安全问题。二是信息篡改威胁，主要破坏信息完整。指没经过允许的人或单位，修改、替换或删除网络里的信息，改变信息原本的内容和属性。改信息的行为可能发生在信息传输时，也可能发生在信息保存时，而且改完后很难一下子发现。如果用这些被改过的信息干活、做决定，会造成很多不好的结果是系统破坏威胁，主要影响信息使用。指通过恶意攻击、病毒感染等方式，搞坏网络系统的正常运行，或让存储设备出故障，导致经过允许的人或单位没法访问信息。这种威胁不仅让信息用不了，还可能让网络系统瘫痪，造成业务停摆、数据丢失，严重影响网络安全和日常运行。

2.2 威胁产生的成因

计算机网络信息安全出现威胁，不是某一个原因造成的，而是技术、管理和人的行为一起作用的结果，这三方面相互影响，让安全风险变得更严重。从技术来看，一方面，网络开放方便信息交换，却也留下安全漏洞，有的设备和软件在设计时没考虑好安全，自带技术缺陷，这些漏洞成了威胁突破防护的入口；另一方面，网络技术更新快，新的攻击手段和病毒不断出现，但有的防护技术更新慢，跟不上攻击技术的速度，形成安全短板。从管理来看，主要是没完善的安全制度。有的单位和个人没定好网络使用、信息管理的规矩，对谁能访问信息、信息存在哪、怎么传都没说清楚，导致使用时很随意；同时，没定期检查、维护网络，发现不了隐患，就算发现了，也没好的应急办法，没法及时处理，让风险变大。从人的行为来看，分不小心做错和故意做坏两种。不小心做错多是因为安全意识差，比如乱点不明链接、用简单密码、随便传敏感信息，虽没恶意，却给威胁留了机

会；故意做坏是有人为了赚钱或达到其他目的，主动攻击网络、偷信息、改信息，这种行为针对性强、破坏大，直接威胁网络安全。

3 计算机网络信息安全的防护对策

3.1 强化技术防护，筑牢安全屏障

技术防护是保障网络信息安全的核心办法，要围绕信息传输、存储和系统运行三个关键环节，用对应的技术，建好“防泄露、防篡改、防破坏”的技术防护墙。信息传输时，用加密技术保护信息不泄露，通过对称或非对称加密，把传输的信息变成密文，就算信息被偷看到，没解密权限也读不懂；同时，用身份认证技术，传输前先核实双方身份，确保只有经过允许的人才能收发信息，防止信息被偷转、偷看。信息存储时，用存储加密和备份技术，一方面给存储设备里的敏感信息加密，就算设备被盗或被偷偷访问，信息也不会泄露；另一方面定期备份重要信息，既在本地备份，也在其他地方备份，就算存储设备坏了，或信息被改、被删，也能通过备份快速恢复，保证信息完整、能用。系统运行时，装防火墙和杀毒软件，防火墙能挡住没经过允许的访问请求，过滤有害数据，不让外部攻击闯进网络；杀毒软件实时检查网络系统和存储设备，及时找到并清除病毒、有害程序，防止系统被破坏、信息被改，还要定期更新杀毒软件的病毒库，应对新出现的病毒和攻击手段，保证系统正常运行。

3.2 完善管理规范，强化安全保障

完善的管理规则是网络信息安全防护的重要支撑，要建立覆盖“日常管理、隐患排查、应急处理”的全流程管理制度，通过规范操作和流程管控，降低安全风险。建日常管理制度，明确网络使用和信息管理的具体规矩，包括谁能访问哪些信息、密码怎么设、敏感信息怎么传和存等，让每个用网络的人都清楚自己该做什么、不能做什么，避免操作随便引发问题；同时，统一管理网络设备和软件，定期更新设备固件和软件版本，修复已知的安全漏洞，防止漏洞被利用。建隐患排查制度，定期检查网络信息安全，检查范围包括网络设备、存储系统、软件程序和信息使用情况，及时发现设备故障、软件漏洞、操作不规范等隐患；把发现的隐患分类记录，明确谁来整改、什么时候整改完，确保隐患及时处理，不扩大风险。建应急处理制度，制定网络安全事件的应对预案，明确信息泄露、系统瘫痪、病毒感染等不同事件的处理步骤和负责人；一旦发生安全事件，能快速启动预案，采取切断攻击源、恢复系统、补救信息等措施，尽量减少损失，事后还要分析原因，完善防护办法，避免再发生同类事件。

3.3 提升安全意识，减少人为风险

人的行为是引发网络信息安全威胁的重要原因，提高使用网络的人的安全意识，规范他们的操作，是减少风险的关键，要通过宣传和培训，强化个人和单位的安全认知。加强安全宣传，通过多种渠道普及网络安全知识，包括信息泄露、病毒攻击的危害，以及规范操作的重要性，让大家明白网络安全和自己的权益、单位的利益有关，改掉“安全和自己无关”的想法，主动做好防护，避免危险操作。开展针对性培训，根据不同人的需求，做不一样的安全培训。对个人用户，教日常网络安全操作，比如正确设密码、识别不明链接和诈骗信息、规范用公共网络；对单位员工，尤其是接触敏感信息的人，还要教信息管理规矩、应急处理步骤，提高他们规范操作和应对风险的能力，避免因意识差、操作错引发安全问题。

4 结语

计算机网络信息安全是数字化发展过程中不可忽视的重要课题，其核心在于保障信息的完整性、保密性与可用性，应对信息泄露、篡改与系统破坏等威胁。因此，需结合技术、管理与意识三个维度，构建全方位防护体系，通过强化技术防护筑牢安全屏障、完善管理规范强化保障、提升安全意识减少人为风险，形成“技术防、管理控、意识守”的协同防护格局，才能有效降低安全风险，保障网络信息安全，为数字化健康发展提供稳定、可靠的网络环境。

参考文献

[1]姜念云.从计算机发展历史看高技术及其产业发展机理[J].科技智囊,2023,(03):12-16.
[2]国勇.网络环境下计算机硬件安全保障及维护策略分析[J].网络安全技术与应用,2021,(10):176-177.
[3]彭求明.计算机网络安全与防火墙技术分析[J].科技资讯,2021,19(22):22-24.