文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

计算机信息技术在网络安全中的运用研究

苏锋　高玉章
海军航空大学青岛校区
DOI:10.12238/acair.v2i4.10315

[摘　要] 伴随着网络的迅猛发展以及信息科技的飞速更迭,网络安全问题愈加明显且复杂。各种恶性攻击、数据泄露、网络病毒等潜在风险层出不穷,给信息安全带来了巨大的危害。面临此种情况,计算机信息技术的崛起给网络安全行业注入了新的可能性与考验。首先,我们要探讨一下计算机信息技术与网络安全之间的联系,然后深入探讨计算机信息技术如何被运用到网络安全的各个环节。其次,我们将对由计算机信息技术引发的网络安全问题以及相应的解决策略进行深入的剖析。
[关键词] 计算机信息技术；网络安全；威胁情报分析
中图分类号：TN915.08　文献标识码：A

Research on the Application of Computer Information Technology in Network Security

Feng Su　Yuzhang Gao
Naval Aviation University Qingdao Campus

[Abstract] With the rapid development of network and the rapid change of information technology, the problem of network security becomes more and more obvious and complicated. All kinds of potential risks, such as vicious attacks, data leakage and network viruses, emerge one after another, which have brought great harm to information security. Faced with this situation, the rise of big data technology has injected new possibilities and tests into the network security industry. First of all, we should discuss the relationship between big data and network security, and then discuss in depth how big data is applied to all aspects of network security. Then, we will deeply analyze the network security problems caused by big data and the corresponding solutions, and also predict the future research trends.
[Key words] computer information technology; Network security; Threat intelligence analysis

引言

随着计算机信息科技的广泛使用,它不仅增强了我们的职业能力,同样也给社会经济的进步带来了新的推动力。在这个数字化的年代,计算机科学技术已深深地融入到我们的日常生活,并且变得越来越关键。随着人们越来越深入地认识到计算机科技的价值,他们也增强了对计算机科技运用的研究与挖掘。然而,因为他们在利用计算机科技的过程中,往往忽视了保护自身的重要性,从而引起了网络安全问题的频繁发生。因此,有必要加强网络安全监管,以便提升网络安全的管理能力,并帮助更多的人明白网络安全的危害,从而增强他们的保护意识。

1 我国网络安全现状

目前,我国计算机网络安全的运行模式正在持续优化与提升。受益于计算机科技的驱使,我国计算机网络安全领域已经实现了某种程度的进展。近些年,尽管我国的相关机构已经非常注重网络安全监控,然而,由于财政、科技等各种原因的影响,有关部门在这个领域的投入却不多。此外,一些专家并未充分了解到计算机信息科学在网络安全控制上的价值,这使得他们在实际运用时遇到了一些困难,比如遭受到计算机病毒侵袭、黑客入侵等情况[1]。

2 计算机信息技术与网络安全的关系

2.1网络安全的重要性和挑战

网络安全的定义为维护互联网系统、数据以及交流不被恶意破坏、非法访问或者破坏的各种策略与行动。伴随着互联网的广泛应用以及人类对其的日益依赖,网络安全的问题愈发突出。在这个过程中,我们正在遭遇来自各个角落的严峻考验。首要的是,随着互联网攻击的日益复杂化,恶意分子利用最新的科技与方法发起攻击,这导致了对于即刻发现并防范攻击的挑战越发严峻。接下来,互联网环境的不稳定因素也在逐渐提升,网络安全的风险源头众多,攻击方法繁多且各异,涵盖了黑客入侵、病毒感染、恶意软件攻击等。[2]终究,由于大量的数据收集与储备,个体的隐私安全以及数据的防护已经变得至关重要。

2.2计算机信息技术在网络安全中的作用和优势

在网络保护领域,计算机信息技术科技扮演着关键角色,同时也展示出许多独特的优点。最初,它可以为我们提供更为详尽的安全信息,借助收集与剖析众多的互联网信息,可以对互联网危险的起因、方式以及属性有所理解,识别出可能存在的危险,并实行适当的预防策略。[3]接下来,利用计算机信息技术,能够立即识别出不正当的活动或者恶意的攻击,然后立即执行适当的策略,从而增强网络安全的处理效果。计算机信息技术也能够实现对个体的身份认定与访问监督,透过研究用户的行动方式、访问历史及个人资料,能够更加精确的辨认和核实个体的身份,同时也能够对其访问权限进行有效的管理,避免未经许可的访问及数据的外泄。

3 计算机信息技术在网络安全中的应用

3.1网络安全策略制定与实施

3.1.1访问控制策略

网络安全的第一道屏障就是访问管理策略,它能够通过适当的访问管理来限制用户或者系统的网络资源使用权,进一步维护信息系统的秘密与完备。在设计这种管理策略的初始阶段,我们必须依照商业需求以及风险分析,来决定用户与系统的使用权限等级。这种方式能够借助如角色导向的访问管理(RBAC)和访问管理列表(ACL)等科学手段来达成。RBAC具备把用户划分成各类的功能,并赋予他们独一无二的权利;相反,ACL设立了针对某一特定资源的访问准则,明确指出哪些用户或者系统应该执行什么样的任务,精确的访问监控方案能够有力地避免未经许可的访问及其潜在的风险。

3.1.2数据加密策略

加密策略的实施,就是在互联网的流通与保留环节,为了避免敏感资料的外泄或者被篡改。当制定这样的加密策略的时候,我们必须依据资料的关键性和危险性,挑选出最恰当的加密技术及密码控制策略。为了保障数据的安全,我们采用了如传输层安全协议(TLS)和IPsec这样的协议来进行数据的加密传输。我们能够通过实施整体加密或者是文件级别的加密来确保数据在存储环境中的稳固。另一方面,针对如移动设备这类的终端,我们也需要实施移动设备管理(MDM)的策略,以便让设备内的数据也能得到有力的加密防护。利用科技化的加密方法,就算是数据遭到盗用,黑客也很难找到具备价值的信息。

3.1.3防火墙配置策略

作为网络保护的关键元素,防火墙的设计能够有力地抵御恶性攻击与网络侵袭。当进行防火墙的设置时,必须对企业的运营需求及其网络布局进行深度研究,并以此来设立相应的访问管理规章。这涵盖了接受或否决某一IP地址、接入点、协议的访问,同时设立了相应的安全策略与网络服务条例。适当的防火墙方案可以有效筛选出不良的流量,从而减少网络的危害。另一方面,对于防火墙记录的跟踪与解读同样至关重要,借助于实时追踪网络流量与攻击记录,可以适时修改防火墙方案,从而增强网络的保护力度。

3.2网络安全监控与检测

3.2.1入侵检测系统

IDS,一种被广泛认可的网络安全监控及检查手段,位于计算机信息系统的管理领域。它的核心任务就是对网络的流量以及系统的运作进行即时的跟踪,并能够发现并反馈可能存在的安全风险以及攻击性的行为。IDS的种类包括两种：NIDS,以及HIDS。NIDS的工作原理是,它能够收集并分析互联网的数据,从而识别出不寻常的网络活动。此类侦察方法既能依赖签名,也能依赖行为分析,借助学习到的正常网络活动,来找出不寻常的状态。[3]NIDS有能力利用协议解读、异常侦察及数据分析等手段寻找隐藏的威胁。与此对比,HIDS更倾向于安装在个人计算机中,对其内部的运作进行观察。它有能力识别出计算机中存在的不良操作,例如非正常的文档更新、系统访问等。HIDS可以利用其监控主机的记录和系统的调度,并配合基线分析,迅速辨认出异常的活动,甚至是可能的攻击。在具体的运作场景下,IDS一般会选择混合配置,也就是说,它会同时运作NIDS和HIDS,这样可以完整地进行网络与主机的安全检查,从而及早察觉并处理网络攻击。

3.2.2安全事件管理系统

SIEM(安全事件处置)系统在网络安全的监督和侦查方向上占有关键地位。该系统利用整合并解读多个与安全有关的数据源的资料,以此实现对所有安全事件的综合处置及反馈功能。SIEM系统的主要职责是搜集、解读、反馈以及上报。

首要的是,siem具备整合从防火墙、IDS、操作系统、应用程序日志等各种数据源获取的安全事件资料的功能。接着,借助于其高效的分析工具,SIEM可以对所有的安全事件做出即时且自主的解读。[4]多种技术方法如基于规则的侦查、行为研究、异常侦查等被用来寻找可能存在的危险。当SIEM系统察觉到任何不正常或者可能的危险,它会依照事先设置的准则和战略做出即刻反馈,其中涵盖了自动报警、防御攻击、产出任务清单等。SIEM不仅具备制作完整的安全报告的功能,也适应后续的审核以及合规性的评估。在SIEM的系统里,对于大量的数据处理以及即时的效率有着严格的需求。所以,它一般会选择使用分散且易于扩充的结构,并且能够迅速地搜索和解读大型的安全事故信息。

3.3网络安全应急响应与处置

3.3.1安全事件报告与处置流程

在网络保护的范畴内,制定和执行安全事故的通知和处理步骤,是打造紧急反馈机制的关键。此步骤既能够对网络危险进行灵敏的反应,又能够快速而高效地做出反馈。在制定安全事故通知步骤时,最重要的职责就是进行辨认。此阶段的运作需要依靠有效的IDS与SIEM。IDS能够实时追踪网络流量以及系统的运作,从而及早察觉出任何不正当的行为。[5]SIEM则是将众多来源的数据融合,以便精确地辨认出可能的危险。只要被察觉出有可能存在的危险,就会马上切换至报告的步骤。通过使用自动化的报警系统,我们能够实现信息的即时发送,并且能够启动全面的

紧急反馈流程。确定阶段构成了整体报告流程的核心部分。在此阶段，网络安全的专家需要检查报告的精确度，核查事件的真伪，并搜集有效的证据来协助接下来的应对措施。此一过程可能会运用到更为深度的网络流量研究、系统记录的审查以及漏洞的检测等科学方法，从而保障对于安全事件的完备把握。对于安全问题的应对步骤涵盖了隔离和限制、研究和解读、修补和重建、观察和回应以及概述和优化等环节。在具体执行过程中，快速阻止并控制被感染的设备，并停止对其产生的影响，这是防止危险扩散的主要工作。接下来，需要进行详尽的研究和解读，以明确攻击方式、损害区域及可能的缺陷。在修复和重建的过程中，根据研究成果，涵盖了修复设备的缺陷、删除不良代码、重新启动被破坏的设备等。在全流程里，我们始终密切跟踪并及时回应，以便对事态做出有利的管理，并为涉及的各方提供即时的信息。终究，归纳和优化是一项必须重视的步骤，我们会对处理过程中的缺陷进行剖析，并据此设立优化策略，以此来增强紧急响应的速度和精度。

3.3.2应急响应计划与演练

网络安全应急响应计划被视作企业应对危机与侵害的策略导向。这个计划给予企业清晰的操作流程与步骤，帮助企业快速且高效地应对所有的安全问题。在应急响应计划中，企业必须首先清晰地界定其计划的设立过程，这其中涵盖了企业的架构、沟通路径、职责划分、应急处理流程、所用的工具及技术援助等诸多元素。我们需要全面考虑并评估网络安全的所有可能性，以便设立具体且多变的解决方案。此外，加强培训和增强认知也是我们设立这些方案的重要组成部分。尽管已经制定出详尽的策略，但若相关工作者未掌握其实质及操作方式，他们依旧无法在突发状况时快速且有效地处理。我们的教育目的就是让这些工作者深入理解并掌握应急反应策略，明白他们在这个策略里的作用与任务。另外，我们也会努力增加团队成员的网络安全认知，让他们能够立刻发现潜在的安全威胁，从而更好地加固我们的安全屏障。

4 结束语

综上所述，为确保网络信息的安全，我们必须在构筑网络信息安全防御系统的过程中运用诸如加密和防火墙这样的计算机科学技术，从而确保系统内的网络信息的安全。另外，借助这些计算机科学技术，我们也能提升信息数据的传递安全和稳定，从而预防信息被盗，或者由于关键信息的泄漏引发的严重问题。随着时间的推移，借助计算机网络科技来搭建起网络信息的保护框架，从而有效地增强了网络信息的保护能力，这将对未来的计算机产业的保护任务产生重要的科学依据。

[参考文献]

[1]刘洋.“大数据”背景下计算机信息技术在网络安全中的运用[J].信息记录材料,2023,24(4):113-115.

[2]毛军强.计算机信息管理技术在网络安全中的应用探讨[J].信息与计算机(理论版)2023,35(15):99-102.

[3]夏泽暄.计算机信息管理技术在网络安全中的应用[J].信息记录材料2023,24(6):98-100.

[4]齐雪.浅谈计算机信息管理技术在网络安全中的应用[J].中国新通信2023,25(1):91-93.

[5]柳少华.计算机信息管理技术在网络安全中的实施与应用[J].造纸装备及材料2022,51(8):126-128.

作者简介：

苏锋(1983--),男,汉族,四川广安人,本科,工程师,研究方向：计算机管理。