入侵检测技术在计算机网络安全维护中的应用探析

永胜

内蒙古警察职业学院公安管理系　内蒙古　010051

摘要：本文着手于入侵检测技术的概念探究，结合我国计算机网络安全维护情况进行分析，总结出入侵检测技术在计算机网络安全维护中的实际应用措施，为我国今后的计算机网络安全维护工作提供合理化参考。

关键词：入侵检测技术；计算机网络安全维护；应用探究

0.引言

随着我国计算机网络技术的快速发展，计算机技术已经逐步应用到我国的各个行业领域当中，为我国提供了现代化的科学技术支持，极大的推动了我国整体经济建设。在我国众多企业的运营与发展过程中，实现优质化的计算机网络安全维护与管理工作，具有显著的现实意义，能够极大提升我国计算机服务行业的网络管理质量，充分发挥我国人力资源优势，促进我国信息化技术的整体发展。

1.入侵检测技术概论及应用情况

（1）常见的几种入侵检测分析手段包括，模式匹配、异常发现与完整性分析，这三种分析手段在实践应用过程中都可以发挥出高效的入侵检测效用，帮助计算机系统实现安全维护的工作状态。模式匹配具体指的是计算机入侵检测系统会对每一个数据包进行检查，挑选出其中带有攻击特征的类似数据进行比对。异常发现具体指的是入侵检测系统会自动检测系统操作过程中的一段数据，通过对该段历史数据进行分析与验证，结合系统正常运作情况下的数据进行比较，从而判断出网络故障的原因。完整性分析是入侵检测系统对网络文件内容进行检测与验证的一种手段，通过寻找发生改变的网络文件内容，确认计算机入侵者的身份，组织入侵者的非法意图[1]。

（2）入侵检测技术在国内应用的时间尚短，在计算机网络中往往只能进行系统文件、系统数据的收集与整理工作，在处理更为细致化的实践操作时，难免会暴露出不足与缺失的地方。在计算机系统中，入侵检测主要用来防测违反安全策略的行为，通过多种数据分析手段，入侵检测技术在计算机系统遭受非法入侵时，可以发挥出较为高效的作用，切实保障计算机系统的完整性与安全性，保证计算机内部数据与软件不会被非法人员利用入侵系统所盗取。在我国今后的计算机网络运营与发展过程中，入侵检测技术应在原有基础上不断优化与创新，为我国今后的入侵检测技术营造良好的发展环境[2]。

2.入侵检测技术在计算机网络安全维护中的实际应用情况探究

2.1信息收集工作

入侵检测技术在实践环节首先需要完成信息收集工作，所需收集的数据源通常情况下有4个，分别包括，系统与网络日志中所包含的数据源、文件中发生改变的数据、应用程序在执行程序时产生的数据、主要以物理形式侵入的数据信息，这4个数据源中所包含的信息数据，是入侵检测技术在端口调试过程中需要收集的内容。为切实保证用户计算机系统的安全性，入侵检测技术在实践应用过程中会对检测对象的来源进行反复确认，确保信息数据中所包含的异常信息在网络中不会经常出现，对存在异常情况及问题信息数据进行挖掘与处理[3]。

2.2信息分析与处理

入侵检测系统在收集完所需信息数据以后，就需要开展信息的分析与处理工作，在实践环节主要采取模式匹配与异常情况分析这两种模式，通过这两种应用模式，对存在问题或者安全隐患的信息数据进行处理和识别，将处理后的结果传达给信息管理器，由管理器进行统一分析。因此，信息分析与处理手段在实践应用过程中具有规范化与标准化的特点，能够妥善处理计算机系统中所存在的安全隐患问题，使机器能够自行分析问题，将问题信息传达给控制器，实现智能化、专业化的入侵检测技术，充分保障了用户计算机系统及其数据信息的安全性。同时，在处理问题信息数据的过程中，一般网络系统都只会单一性质的对信号进行读取与解析，而在入侵检测技术中的信号处理环节，问题信息数据在系统中将会被及时告知，处于实时监控下的问题信息，会被以日志的形式进行记录，直到计算机系统中的问题信息被入侵检测系统所处理或者问题隐患得到排除。

2.3信息响应与防火墙系统的应用

信息响应具体指的是入侵检测系统对问题信息的攻击行为做出合理化的反应，根据信息的实时状态，查看事实会话记录，顺利将信息通报给控制台，实现异常状态的信息处理优化模式；防火墙技术是我国计算机系统中主要应用的一种应用层与网络层控制技术，通过防火墙应用，用户电脑系统中的数据资源得到了有效保护，一般的网络入侵所带有的攻击行为往往都会被防火墙所阻挡，然而，随着科学技术的创新与发展，入侵技术不断升级，传统的单一化防火墙应用已经逐渐无法满足用户的实际需要，在我国今后的入侵检测技术实践应用过程中，应将入侵检测技术与防火墙应用实践结合，取长补短，发挥防火墙的过滤机制，同时，利用入侵检测技术将带有攻击性的数据进行清除，以此充分保障用户计算机数据信息的安全性。

3.结语

综上所述，入侵检测技术在计算机网络安全维护工作中具有极其重要的实际意义，能够极大的促进我国信息化网络的安全运营，提高我国计算机技术的利用效率，为我国市场经济的提升与发展注入了极大的动力。

参考文献

[1]刘进出.新时期下的入侵检测技术应用探究[J].信息技术教育，2013，12(09):23-24.

[2]杨剑锋.传统计算机网络维护工作中存在的问题[J].西北科技大学院报，2012，23(07):23-25.

[3]何伟.入侵检测工作中的问题分析[J].湖南科技大学院报，2012，12(07):33-25.