第25卷第4期
2015年12月

陕西国防工业职业技术学院学报
Journal of Shaanxi Institute of Technology

Vol. 25 No. 4
Dec. 2015

计算机犯罪的防范及对策研究

梅雪莲
（鄂州三六五金典文化传播有限公司，湖北 鄂州 436000）

摘 要：计算机犯罪在金融、保险、银行等领域比较严重，这就需要我们加强对计算机犯罪的认识，并从加强立法，加大惩罚措施与力度、加强技术层面的防范等多方面防范计算机犯罪。

关键词：计算机；犯罪；对策
中图分类号：TP309 文献标识码：A 文章编号：94007－(2015)04－0036－03

计算机从最初的电子管式发展到今天的大规模集成电路式计算机，无论是功能还是应用程度上都得到了很大的提高。当前计算机在人们的生活中扮演者越来越重要的角色，对人类社会的发展做出了卓越的贡献。但是计算机在给人们带来便利的同时，也给人们带来了一些困境，例如计算机犯罪。有些人利用计算机网络的虚拟性、隐蔽性等特点，从事一些非法的活动，给人们的生命财产安全带来了较为严重的威胁。计算机犯罪当前在我国已经属于一种经常出现的犯罪方式，尤其是在金融、保险、银行等领域，计算机犯罪的情况更加严重。随着我国的不断发展，在不久的将来计算机必然会得到更为广泛的应用，这就需要我们加强对计算机犯罪的认识，找出防治计算机犯罪的对策。

1 计算机犯罪概述

计算机犯罪就是以计算机作为工具，或者以计算机资产作为对象而实施的犯罪活动。这里的工具不仅仅包括计算机的信息系统，也包括计算机技术的应用。计算机犯罪作为一种新型的犯罪状态，与普通的犯罪相比较，往往具有一些较新的特征。首先，计算机犯罪是通过高科技手段进行的，具有一定的智能化。当前随着计算机技术的不断发展进步，计算机往往都会有一定的防护措施，想要进行计算机犯罪，肯定要具备一定的专业知识及计算机操作技能。而计算机犯罪一般都是采用高科技手段，通过对计算机系统植入木马等方式来达成犯罪目的。其次，计算机犯罪都会有一定的隐蔽性。因为计算机犯罪都是通过计算机来完成的，所以犯罪分子一般都是通过远程对计算机漏洞进行攻击或者植入病毒等方式。而植入的病毒一般都会有一定的潜伏期，不会当时就被发现，只有在特定的场合或者被激活的状态下才会对用户的信息进行窃取，犯罪的过程很难被察觉。然后，计算机犯罪一般后果都比较严重。当前计算机犯罪基本都存在与金融行业，主要涉及到银行电子账户等等。一旦计算机犯罪得逞，造成的影响是非常严重的，往往都是属于数额较大或者数额巨大的犯罪。最后，计算机犯罪还有一定的地域性特征，这也是计算机犯罪区别于其他犯罪的一个重要因素。因为计算机网络的普及，其虚拟性在方便了大家的同时，也给信息安全带来一定的困扰。计算机犯罪多半都是跨地域性的。因为互联网拉近了人们之间的距离，同时也方便了计算机犯罪的进行。只要通过点击鼠标就可以实现对其他区域计算机的攻击行为[1]。

2 当前我国计算机犯罪的情况分析

我国当前的计算机犯罪呈几何增长的趋势上升，并且计算机犯罪在所有犯罪案件里面所占的比例也越来越高。

收稿日期：2015－09－20
作者简介：梅雪莲(1981－)，女，湖北鄂州人，主要从事职业教育培训研究工作。

2.1 利用计算机网络制作、传播、贩卖淫秽信息

随着计算机的不断普及,非法软件将黄色病毒迅速的传播起来。随着计算机技术的不断发展,有许多网站公然提供黄色淫秽宣传物的下载,大肆传播淫秽信息。

2.2 利用计算机网络实施财产性犯罪

我国当前每年因为计算机犯罪造成的经济损失将是一个不可估量的数字。1、犯罪分子利用计算机技术修改、伪造存款金额,来诈骗、盗窃金融部门的财产。2、犯罪分子利用计算机技术侵占他人财物或者倒卖他人物品。利用计算机进行敲诈勒索的案件数量也在不断的增加当中。

2.3 实施危害的计算机犯罪

实施危害的计算机犯罪主要模式就是黑客攻击计算机。金融机构等是黑客攻击的重点目标,在现实生活中也存在着许多通过计算机网络入侵网上银行从而实施犯罪的活动。其他机构像重点民生工程也是黑客攻击的重点。例如移动通信网络、互联网信息提供者等等,都是受攻击的对象。网络蠕虫、脚本病毒、木马程序、网页病毒这些都已经成为当前造成计算机病毒的主要危害。

2.4 计算机犯罪还有可能危害国家安全

主要有两个方面,首先就是一些邪教组织不断的利用互联网来反对社会主义事业的建设。通过互联网中的电子邮件、聊天工具等等来达到蛊惑人心的目的。甚至通过互联网来煽动民族冲突,破坏民族团结,严重的影响了国家的安全与稳定。其次,就是黑客对于国防安全网站的攻击,有可能使得国防相关机密泄露,容易给国家安全造成危害。之前就有过联邦德国的学生通过互联网黑入美国国防部网站并且窃取军事机密的案例,给美国的国防信息造成了严重的危害。在我们国家,我们也要防范这种事情的发生。

3 如何加强对计算机犯罪的防范及对策

3.1 加强立法,加大惩罚措施与力度

首先,是对计算机犯罪罪名的完善。我国刑法对计算机犯罪中的规定例如“非法入侵计算机信息系统罪”、“破坏计算机信息系统罪”等等都是突出了对计算机信息系统的保护,却忽略了对计算机硬件、相关配套设施的保护。计算机中保存的一些电子数据有可能会产生巨大的上商业价值,甚至可能涉及到国家安全等。这些财富虽然是无形的,但是这些财富又都是无价的。所以说,要加强立法,增设一些计算机犯罪的新罪名。例如新增“破坏计算机设施罪”、“妨害计算机系统信息正常运行罪”、“盗窃计算机服务罪”、“滥用计算机信息系统罪”、等等[2]。

其次,针对当前计算机犯罪年龄趋于小龄话,建议将12—16周岁的未成年人也纳入计算机犯罪的主体。随着计算机技术的不断发展,越来越多的未成年人开始熟练的掌握着计算机技巧,犯罪的主体年龄趋于降低。而我国现行刑法规定,不满14周岁不需要负刑事责任。这对于一些年纪较小的计算机犯罪者来讲,并没有约束力。

最后,要出台专门的《计算机犯罪法》,我国现有的关于计算机犯罪的法律法规基本都分布在刑法当中,并没有一部专门针对计算机犯罪的法律法规,对一些细节问题规定的不够细致,导致了许多事情没有具体法律法规可以依据。另外也还要借助行政法律的配合,因为现有的行政法规在许多方面已经对计算机犯罪做出了规定,所以在完善相关法律法规时,可以参照些许行政法规。

3.2 加强技术层面的防范

3.2.1 加强设备安全防范

加强设备的安全防范,首先要保证计算机的物理安全。在计算机管理系统中要安装专业的杀毒软件以及防火墙。在计算机机房管理中,要加强对电子密码的设置,对重点要害部位要进行指纹密码锁的设置。在技术上设置访问控制、安全传输机制等等,并且开启自动报告功能,当信息系统受到侵害之后,系统能够准确的提供受损情况,并且针对受损情况作出补救措施。其次,要重视一些数据保存媒介的安全,避免计算机因为接触到外接型数据储存设备而感染上病毒。当前许多病毒都是通过数据保存媒介来传播的,所以在使用外部数据保存媒介时,一定要重视对媒介病毒的查杀。

3.2.2 提高计算机数据加密保护

数据加密是计算机网络安全控制中最为基本的内容,网络加密数据可以通过算法和密匙的方法,并且数据加密可以在OSI协议模型的多个层次上面实现,主要包括链路加密以及端间加密。同时加强对计算机数据库的建设,防止因为数据库设计不够全面而造成信息的泄露。数据库可以选择基于Microsoft SQL Server(SQL Server2005& SQL Server CE3.5)为主要的数据库模型。选用SQL主要是因为其非过程化的语言,允许用户在更高层次上的数据结构工作,可操作记录。并且诶SQL的特性允许一个SQL语句的结果来作为另外一条SQL语句的

录入。SQL 不强制要求用户对于数据的存放方式，这样会让用户能够集中精力得到想要的结果。并且 SQL 可以为许多任务提供命令语句。可以查询、插入修改删除数据、控制数据的存取与读取、保证数据库的一致性。数据库的核心是数据库管理系统，并且当前基本上主要的数据库管理系统都支持 SQL 语言。要采用分布式数据库系统，可以有效的实现数据共享，并且可以采用局域或者互联网连接的模式，实现各模块之间的协同工作[3]。

3.2.3 加强硬件设施及系统网络设计

首先，要加强对系统网络结构的设计。服务器放置在特种设备数据中心，通过 internet 与数据中心进行数据的交换、审查。随着网络化进程的加速，数据起到了越来越重要的作用，一但出现被黑客攻击，数据丢失，将会给电脑维护带来极大的困难。这就要求对数据进行有效地备份。在设备运行的过程中，由于数据量较大，产生数据丢失的现象是在所难免的。这就要求系统能够及时的对数据进行备份，以确保即使系统运行不畅，也能保证基础信息。所以在系统网络结构设计上，采用 windows 操作系统，10M 的 VPN 链路，通过 SQL 数据库，实现每天一次的数据备份，并且将备份数据进行集中管理，保存于独立于特种设备之外的其他计算机设备上。其次，要加强 UTT 网关的设置。为了保障网络数据的安全，采用 UTT 网关来实现对数据的保护。首先，要有安全交换机，实现内网交换。VLAN、IP/MAC 端口绑定等可以帮助实现防止大部分的内网可能存在的问题。采取管理员、执行员、浏览这三个等级的权限，确保能够提供对每个 nat session 的监控，包括目的地址、端口等等。再次，可以在内部网络之间使用 VPN 系统，减少与公共网络的接触。VPN(Virtual Private Network)，是虚拟专用网络，利用公共网络建立起来的一个安全却又临时的连接。通过加密协议实现在不同地域之间的安全连接。VPN 的核心内容就是建立企业内部的虚拟网络。最后，要保障硬件设备的完善。对于防止计算机犯罪，需要较为完善的系统硬件设施配置。要有数据库服务器、应用服务器、UPS 电源等等。这一系列的硬件设施才能更好的保证整个安全防护系统的有效运行。

3.3 安全防护系统的有效性

3.3.1 先进性

整个关系系统采用了 Microsoft. NET Framework 2.0 系统框架，能够充分的发挥 Web 的优势特点，并且能够更好地利用当前的发达的网络资源与计算机技术。SQL Server2005 数据库保证了数据的有效性与安全性。

3.3.2 完整性

整个系统通过虚拟网络实现连接，可以将各个部门项目联系在一起，在不必要的时候可以避免与外部计算机网络的互联，减少攻击行为的发生。并且在必要时还可以通过 internet 与外部实现信息的共享，保证了整个网络系统的完整性。还在一定程度上减少了计算机犯罪的威胁。

3.3.3 经济实用性

安全防护系统一般都充分的考虑到造价问题，可以充分的利用现有资源进行整合，实现更高的性价比。

Computer Crime Prevention and Countermeasures against It

MEIXue-lian

(365 Cultural Diffusion Limited Company of EZHOU EZHOU Hubei 436000)

Abstract: Computer crime is very serious in the financial, insurance, banking and other fields, which we need to strengthen the awareness of computer crime, and to strengthen legislation, increase punitive measures and efforts to strengthen the prevention of the technical aspects of many ways to prevent computer crime.

Key Words: Computer; Crime ;People

参 考 文 献

[1] 朱兆坦. 计算机犯罪在刑法上的概念及其完善[J]. 信息网络安全，2011(2)18.

[2] 宋冰. 计算机犯罪特点及防范[J]. 法制与社会，2012(3)19.

[3] 文建. 计算机犯罪的技术防范对策[J]. 云南警官学院学报，2010(1)15.