大数据时代背景下的计算机网络安全体系构建分析

◆何成宝

（齐鲁理工学院网络信息中心　山东省济南市　250200）

摘要：现阶段，计算机网络已经得以普及，不仅提高了工作效率，而且还促进了信息数据的传播。但同时，随着大数据时代的到来，网络的开放性也为一些别有用心人士提供了机会，计算机网络安全问题愈加突出，严重威胁了计算机网络以及个人信息的安全。本文对现阶段计算机网络安全问题进行了分析，并探讨了大数据时代背景下的计算机网络安全体系的构建，希望能够为加强计算机网络安全工作提供借鉴。

关键词：计算机网络安全；大数据；安全问题

0.引言

计算机网络的快速发展为各行各业工作提供了便利，对加快行业改革、促进地方经济建设发挥着重要的作用。计算机网络在为人们带来便利的同时，也带来了一些新的问题。外部人员通过恶意攻击计算机网络窃取信息、破坏程序，给个人、企业造成了严重的损失，甚至可能威胁国家安全。因此，在大数据时代下，构建计算机网络安全体系迫在眉睫。如何建立计算机网络安全体系提高信息传输、存储的安全性，如何提高计算机网络安全体系的和理性与实用性是本文重点研究的问题。在大数据时代背景下研究计算机网络安全体系是引导计算机技术良性发展的重要保障。

1.大数据时代背景下的计算机网络安全问题

第一，计算机系统漏洞。现阶段，大部分主流计算机操作系统都或多或少存在一些系统漏洞。用户在使用计算机过程中，由于未对下载、安装的软件与硬件加以筛选，导致系统产生漏洞。计算机系统漏洞是难以避免的，虽然用户可以利用计算机安全软件修复漏洞，但是在后续使用过程中又会产生新的漏洞。这些系统漏洞让黑客等有了可乘之机，通过漏洞窃取重要信息。

第二，人为因素产生的安全问题。一方面，网络黑客等不法分子通过编制的一些恶意程序或者植入软件入侵用户计算机网络，对计算机内信息进行非法的修改或窃取。部分违法人员甚至将这些信息违法转卖给他人，牟取不法所得，严重侵害了计算机网络安全。另一方面，计算机用户安全防范意识薄弱。一些用户为了方便或者是容易记住信息，网站、程序的账号以及密码设置过于简单，没有前往官方网站或者经过认证的网站下载程序，增加了用户隐私信息泄露的风险。而大数据、云计算技术的出现更是降低了用户对信息的控制程度，用户网页分享的位置信息、上网痕迹等都可能被外人窃取与利用[1]。

第三，特殊因素导致的安全问题。在计算机网络运行过程中，因电力故障等不可预见性因素对信息处理造成影响，一些网络信息在传输过程中可能会出现问题，进而引发计算机网络安全问题。

2.大数据时代背景下的计算机网络安全体系的构建

2.1 加强网络病毒的防控

对于防控网络病毒，应用最为广泛地便是防火墙技术。防火墙技术主要是为了防止外部网络用户的擅自访问，避免外部的非法入侵。因此，计算机用户需要重视防火墙技术的应用，在应用过程中要及时记录防火墙有关信息，通过日志文件发现系统漏洞，采取措施修复漏洞[2]。与此同时，除了可以利用防火墙抵御网络病毒之外，还可以利用其它的防病毒技术降低计算机网络安全风险。计算机网络病毒的预防重点是避免病毒进入磁盘等硬件进行相应的操作，计算机用户在使用过程中可以安装腾讯电脑管家等应用程序，利用程序中的病毒查杀功能检测计算机内是否存在病毒，减少计算机网络病毒传播的情况，降低网络病毒入侵的可能性。值得注意的是，用户应该避免安装两个及以上数量的杀毒软件，要优先选择病毒库数据更为全面的软件，提高网络病毒防控效果。

2.2 建立健全网络安全管理机制

在大数据时代背景下，要想提高计算机网络的安全性就必须在制度层面强调计算机网络安全的重要性。第一，国家工信部等部门可以联合立法机关一同加强对计算机网络安全、个人信息保护等方面法律研究，不断完善网络管理条例，对于恶意传播病毒、攻击他人计算机网络安全的不法分子严惩不贷。同时，工信部等部门还需要加强网络监管力度，建立网络安全问题举报平台，发动社会力量进行监督，要做到及时处理、严厉惩处、及时反馈，在全社会形成网络安全防护合力。第二，企业要加强网络安全管理制度建设。企业要坚定不移地落实国家关于网络安全管理等方面的条例，要结合企业的实际情况完善企业网络安全管理制度，提高企业信息化建设质量。同时，企业要将计算机网络安全管理制度纳入日常管理制度中，要在制度中明确网络安全负责人员的职责；要明确各个部门人员应用计算机尤其似乎企业内部信息库的权限、流程等；完善企业信息发布、审核制度；安排信息技术部门人员或邀请专业人士定期对企业计算机网络系统进行检测，做好全面筛查。除此之外，还要对全体员工进行网络安全培训，使员工在工作中可以自觉践行制度，不随意下载软件、不随意将自己的账号借给他人使用，提高企业计算机网络安全管理水平。第三，个人用户也要与政府一同加强监督，对于网络黑客要善用举报制度，保护计算机网络安全。

2.3 实行严格的身份认证

身份认证是较为常见的安全保护方式，主要是对当前计算机操作者的身份进行确认，身份无误后才可以进入系统。相比于简单口令认证，即传统账号密码形式，动态口令身份认证可以减少因用户网站、程序的账号以及密码设置过于简单带来的风险问题，更为安全。即计算机用户在操作前需要将系统发送至手机等设备上的动态密码，结合系统账号确认身份。因为每次系统发送给计算机用户的密码是不同的，而且有些动态口令还有时间限制，因此黑客即使截获了密码也难以通过这一动态口令通过身份认证，有效地保护了计算机网络的安全。另一种身份认证技术是通过 SD 卡等智能卡进行的。当计算机用户面临身份认证时，用户端会向系统发送身份验证请求，系统在接受指令后会随机生成一串数字并将数字发送给用户端。之后，用户端再将这串数字传送至智能卡，而智能卡则将这串数字与自身密钥结合后将该数据发送给认证服务器，而服务器在进行相同计算后得出的结果一致，则认定操作者为合法计算机用户[3]。动态口令身份认证技术与智能卡身份认证技术使用方便、可靠性较强，结合实际需求应用身份认证技术可以提高计算机网络的安全性。

2.4 建立信息应急处理机制

前文所述，一些不可预见、不可抗力因素也可能诱发计算机网络安全问题，因此需要尽快建立网络信息应急处理机制。计算机用户应该做好数据的存储、备份，要定期确认所存储的信息。在一些突发事件中，要尽量使用户在解决后尽可能地找回数据。

3.结语

综上所述，在大数据时代背景下，计算机网络面临着更为复杂、更多样的攻击、入侵形势，国家要加强网络安全法律制度建设，企业与个人也要加强计算机网络安全防范意识，建立健全网络安全管理机制，实行严格的身份认证，保护计算机网络安全。计算机网络安全体系的构建是维护网络秩序、促进经济发展的重要保障，在大数据时代下我们需要以更谨慎的态度对待计算机网络体系。

参考文献：

[1]苏智华. 试谈大数据时代的计算机网络安全及防范措施[J]. 网络安全技术与应用, 2018(3):22-24.

[2]匡博, 王颖. 大数据时代的计算机网络安全及防范措施研究[J]. 电脑知识与技术, 2018, v.14(17):37-38.

[3]张森. 大数据时代的计算机网络安全及防范措施探析[J]. 网络安全技术与应用, 2018(1):55-55.

作者简介：何成宝（1982 年 8 月–），男，汉族，山东省泰安市，山东经济学院，信息与计算科学专业，本科学士，齐鲁理工学院，高级实验师，计算机网络方向或学校教育信息化方向。