计算机网络安全防范技术的研究和应用

王东升
超越科技股份有限公司

[摘　要]计算机的出现为人们的生活带来了极大的便利，有效的提高了人们的生活质量。尽管如此所存在的安全性问题也依旧不能忽视，如何做好计算机的安全防控对于今后的使用有着重要的意义。为此本文选择针对计算机网络安全防范技术的具体使用情况进行研究，找到有效的防控措施，才能做好计算机网络完全工作，避免因安全隐患带来不必要的损失。

[关键词]计算机；安全防范技术；研究和应用
【DOI】10.12252/j.issn.2096-6288.2021.12.527

前言

在频繁的运用计算机的过程中，各种安全问题也随之而来，特别是衍生出很多不法分子，利用自身对于计算机技术的掌握，找到所存在的漏洞大量的获取用户信息，满足自己的私利。继而为了更好的确保个人隐私安全，国家信息安全，其管理人员需要重视起来，找到计算机存在的风险漏洞，同时提高安全防范技术，满足现阶段广大用户对于计算机网络系统的应用。

1 计算机网络安全面临的威胁

1.1病毒攻击

现阶段通过针对计算机网络进行分析可知，在计算机使用的过程中，常常会因为存在各种各样的病毒造成其网络安全受到威胁。同时计算机中的病毒类型较为繁琐，虽然目的都是为了窃取各种各样的数据，但是应对这些病毒的方式或者是手段却不尽相同，甚至还会有部分病毒直接造成计算机网络瘫痪，造成相关数据的丢失。随着计算机的出现，各种病毒也随之产生，计算的更新换代也是病毒种类的更新换代。简单分析，计算机中存在的病毒通常都是以代码的形式出现，这种代码与传统的软件存在着一定的差异，会在用户下载常用软件的过程中直接植入到用户的计算机中，随着用户对于软件的打开和应用，最终对于计算机中的数据下手，复制大量的内存数据，并且通过各种途径来感染其他用户的计算机系统，只要其他的系统被感染后，这些病毒会造成计算机系统的延迟和运行缓慢，造成数据损失。

1.2黑客入侵

用户在需要注意病毒攻击的同时，也需要注意到计算机中的另一大安全威胁，那就是黑客，黑客常常会通过用户使用计算机的过程中未经过用户的允许直接利用网络技术侵入到用户的计算机中，针对计算机中的大数据进行窃取，或者是将现有数据进行整改，这对于用户而言，自身利益会大大的受到影响。同时黑客入侵电脑的手段是多样性的，很难令用户有所察觉，更加无法进行防范，甚至在黑客入侵到用户的计算机中，用户的计算机黑客在实施入侵以后，用户的计算机网络还会产生很大漏洞，而这也会使用户在对计算机网络进行修复时存在极大难度，某些漏洞甚至无法进行修复。可以说，对于计算机网络安全防范工作必须要将黑客入侵作为网络安全问题的防范重点。

2.3系统漏洞

针对计算机系统进行深入分析的过程中可以发现，尽管计算机的出现是人类文明的产物，但是其中存在的各种问题也是需要深入分析和重视的，在计算机使用和运行过程里，常常存在着各种系统的漏洞，这些漏洞的存在，无疑为黑客的入侵提供了便利的条件，同时也是计算机病毒入侵的重要渠道。黑客一旦确定了想要攻击的计算机后，便会在计算机的系统上进行查找，选择通过各种各样的方式对于计算机进行进攻，此种方式的出现，必然会对于计算机系统中的各种数据造成损失，数据可能会都是也可能会被改动。为此在计算机网络安全防范技术研究中，必须要将系统漏洞作为重要的防范重点，确保黑客及计算机病毒不会利用系统漏洞入侵用户计算机系统。

2 计算机网络安全防范技术的研究和应用

2.1防火墙技术

在计算机网络安全防范技术中比较常见的一种是防火墙技术，这种技术可以简单的理解为一种墙体的存在，正是因为这种墙体，使得将计算机系统的内网和外网之间充分隔离，减少外网中的安全风险问题冲破到内网中，对于计算机造成损失。简单分析，防火墙的组成是分为两个部分，分别是计算机的软件设备和计算机的硬件设备，用户在计算机中设置防火墙之后，将其内部和外部进行有效的隔绝，把计算机分成两个部分，分别是计算机的专用网络和公用网络。再者防火墙技术的使用也是需要经过严格的检查，检查后直接应用到计算机网络中，防火墙技术的应用可以有效的针对现有用户进行审核，审核后达到标准的用户可以使用计算机，具体的审核信息也会上传到计算机的数据库中作为保存，并不会直接被其他用户所浏览和使用。

2.2加密技术

在计算机网络运行过程中，需要进行信息传递，这也使信息在传递过程中可能会造成信息发生泄露。因此，为了确保信息的传输安全，就必须在计算机网络系统中充分运用数据加密技术，以此保障信息传输的安全性。在将数据加密技术应用到计算机网络过程中，其具体的技术层次包括三个：分别是链路加密、端至端加密和节点加密。其中，链路加密能够将所有的链路数据按照特定的形式进行加密转换，这样链路信息在网络各个节点中的安全性便得到了极大保障。对于节点加密来说，其节点加密段涵盖了原节点至目的地节点，在这两个节点之间的传输链路能够有效保障其信息安全。而对于端至端加密来说，则是通过特定的加密方式使信息能够从云端用户向着目的端用户进行传输，以此确保数据在传输过程中得到保护。

2.3漏洞修复技术

在计算机网络安全防范技术中，对于漏洞修复技术来说，需要通过相应的工具对传输数据进行扫描检测，以便于对计算机系统中可能存在的系统漏洞进行查找。当发现计算机系统中存在可能会产生安全风险的漏洞时，便会通过该技术来对系统漏洞进行及时修复，以此防止黑客或不法分子利用该系统漏洞实施网络攻击，这样才能使计算机网络安全得到可靠保证。在漏洞修复过程中，用户可以自行选择通过手动方式进行修复，或是由系统进行自动修复，以此保证网络系统中的漏洞在修复以后不会成为黑客和不法分子的攻击途径。

3 结语

综上，想要更加有效的针对计算机网络安全问题进行了解和掌控，就必须针对现有计算机网络安全防范技术开展深入研究，在研究的过程中将研究成果直接应用到实践中，从而更好的确保计算机网络数据安全问题。

参考文献

[1]王华.关于计算机网络安全防范技术的研究和应用[J].信息记录材料，2021，22（01）：153-154.

[2]袁源.浅谈计算机网络信息安全技术及防护[J].山西警察学院学报，2021，29（04）：109-111.

[3]田扬畅.计算机网络安全防范技术的研究和应用[J].普洱学院学报，2021，37（06）：31-33.