网络安全在后疫情时代的变化

■ 厍浩文

如今，一些首席信息安全官表示，新型冠状病毒肺炎疫情正在破坏网络安全计划并改变其优先级。虽然没人知道疫情的影响何时会结束，但对于这种新常态需要有清醒的认识。以下是行业专家对网络安全在后疫情时代的 10 个变化预测。

在家工作成为默认模式

这是一个显而易见的假设，但可以提供数据来证明。根据 ESG 公司的研究，79 %的 IT 高管表示，在新型冠状病毒疫情结束之后，他们所在的组织将实施更加灵活的在家工作策略。此外，在家工作策略似乎运行良好，78 %在家远程工作的人员表示，在家工作更具生产力或生产力并没有减弱。在提高生产力和节省房地产成本方面，企业员工在家工作显然成为一个良好的选择，并且推动安全投资和优先事项出现更多的变化。

网络安全边界将会消亡

由多家金融服务机构 20 年前成立的一个名为 Jericho 的论坛提出了取消网络边界的理念。尽管大多数安全专家都认同这一想法，但网络边界的安全性仍然是一个挑战，因此网络边界仍然存在，并且随着时间的推移而缓慢变化。新型冠状病毒疫情可能最终打破网络安全边界。为了支持更分散的 IT 基础设施，安全控制措施将大量移至网络端点（用户、设备、应用程序及数据等）。好消息是，基于云计算的管理平台将使该架构比过去更易于扩展和操作。那么什么是新的边界？用户、设备和数据。

加强云安全

由于疫情的蔓延，很多企业加快将工作负载迁移到云平台，因为与运营内部部署数据中心服务器、网络和存储设备相比，更容易管理云计算基础设施。为了跟上发展的步伐，首席信息安全官必须加强云计算安全团队的招聘、培训和技能开发。很多人知道公共云是用于网络安全控制、整合 SD-WAN 和安全服务的基础设施。对于安全分析而言，数据和分析引擎快速迁移到云平台也是如此。最后，安全管理平台朝着多云方向前进。首席信息安全官将需要新技能来迁移数据和工具以及管理云计算订阅。

攻击面管理的主流化

随着用户和资产变得更加分散和远程，企业的首席信息安全官将需要更好的方式来收集、处理和分析数据，以进行网络风险管理。由于大多数员工不知道与网络连接的风险，并会定期发现诸如以前未知的设备、配置错误的服务器、默认密码以及合作伙伴连接之类的东西，而且这些事情可能很快发生。攻击面管理（ASM）将从员工管理发展到企业需求。像 BitSight，Bugcrowd，CyCognito，Randori 等供应商将从这一转变中受益。

在政策管理上加倍努力

在分发了所有内容之后，首席信息安全官需要与业务经理一起确定何人从何处执行操作，然后通过精细而动态的规则集加强安全策略。在确定政策之后，他们还将需要获得首席信息官的帮助，以构建用于政策实施和监控的基础设施。对于安全技术来说，这是一个巨大的机会，而那些没有构建直观、灵活和可扩展策略管理引擎的供应商将会被淘汰。

身份验证管理得到彻底改革

分布式安全控制和策略管理必须以现代的身份管理基础设施为基础，而不是过去 20 年来采用的安全措施拼凑而成。为了简化这种迁移，身份验证也会很快迁移到云平台中。对于 JumpCloud，Okta，Ping 来说，这是一个好消息，但相信像 AWS、Google、VMware 和微软这样的云计算服务提供商也会在这里发挥重要作用。

加强大规模的网络威胁情报

疫情对于网络攻击者来说是一个全球性的机遇，导致了一系列新的网络诈骗和攻击。为了应对这种趋势，企业需要能够以前所未有的规模实施、分析和寻找威胁。这将是威胁情报平台和调查工具（如 Anomali，King&Union，Palo Alto Networks，RecordedFuture，ThreatConnect，ThreatQuotient）在高端市场的增长机会。规模较小的企业可能会更深入地研究来自思科、FireEye、IBM 及 Secureworks 等公司的威胁情报服务。

人工智能和机器学习技术的应用

安全团队将需要同时了解更多资产、连接、移动和威胁。业务管理部门将推动建立永久性在家工作政策，这是一个必然趋势，而且全球没有一个安全团队能够在没有获得帮助的情况下跟上新的现实。目前，人们正在加速采用人工智能和机器学习技术，需要尽快跟上发展的速度。这是一个广泛的机会，像 Devo，Google（Chronicle），IBM，Microsoft，SAS，Splunk 这样的公司将会发挥重要作用。

进行认真的安全培训

展望未来，相信大多数组织员工都需要具备安全意识，因为他们的薪酬激励或惩罚与业绩相关。业务经理还将对员工的教育负责，并在团队因无知导致安全漏洞时受到处罚。在供应方面，供应商需要为企业员工设计更全面的课程，为基本的合规性培训提供补充。

加强安全性和 IT 运营合作

设置安全的端点、云计算工作负载或网络基础设施需要

网络安全管理在医院计算机应用

罗奕菲 河南省郑州市第三人民医院

1 引言

十八大以后，我国一直致力于完成改革事业，为打造现代化社会而努力。各种信息技术、计算机技术以及网络技术的出现，使我们获取信息资源的渠道拓宽了，工作速度和效率提高了，但同时，也给我们提出了一个更大的难题，那就是如何维护网络系统的安全运转。医疗事业是我国的重要事业之一，能够保障我国人民的生命安全。医院工作又是一项十分复杂的工作，在当代社会的发展背景下，应顺应时代变化，逐渐向自动化、智能化的方向发展，这对提高我国人民的幸福指数有着积极影响。而如何采取有效措施，实现医院计算机的网络安全管理，就成为医院能否实现现代化建设的决定性因素。本文从计算机网络安全管理的意义出发，对现阶段该管理方法在实施过程中，面临的主要问题及现状进行了分析，并提出了几点应用策略。

2 网络安全管理在医院计算机中的应用

医院现代化建设，是我国实现现代化强国的重要工作之一。随着各种科学技术的出现，使得医院各项工作的开展变得越来越智能化，这都要得益于我国计算机技术和网络技术的发展，为医院工作的开展提供了一个网络化的工作环境，而如何维护好这一网络系统高效、高质运转，就需要做好医院计算机网络安全管理工作。

2.1 网络管理协议

在新时期的发展背景下，计算机技术得到了广泛应用，其管理工作也应按照一定的协议，凸显出自己的特色和优势。

站在功能性的层面来说，网络管理协议能够总结出各网络间的通信规则，同时还能对相关变动信息进行整理和分析，这就能够为医院的发展提供一套合理的方案，以达到高效管理的目的。

2.2 网络管理系统

随着人们生活质量的提高，对于服务行业的要求也越来越高。医院可以借助各种科学技术，建立属于自己的数据库和服务平台，以此来优化患者的就医流程、提高患者的就医体验。但这需要建立在网络管理系统之上。

通常来说，网络管理系统需要借助网络平台及网管协议设备等完成构建，而各种软、硬件以及各种科学技术，在这一构建过程中起到了辅助作用，还可以对系统功能进行升级。

拿 CORBA 技术来说，该技术应用在网络管理系统中，能够为系统提供事物以及名字等服务，并与 CMIP 以及 SNMP 等相结合，共同构建了网络管理系统。

2.3 网络管理结构体系

在当代社会的发展背景下，计算机网络技术得到了快速发展，且已被应用在各个领域。医院要想借助这一发展优势来实现现代化建设和管理，就需要对医院内部的网络管理体系进行优化和升级。

对于医院的整个运行系统来说，结构特点决定了功能特点。一般来说，医院的网络管理结构分为 2 种，集中式和非集中式，而无论哪一种结构，都需要在网络管理体系下进行。其中，集中式管理结构运用较多，它以一个集中控制中心或平台，对整个系统的活动进行操控和管理。一直以来，,受到了广大医院的一致认可。

3 计算机网络安全管理对医院发展建设的重要意义

网络安全管理能够为医院办公建设提供一个无人化操作平台，代替人工执行部分工作，从而减轻工作人员的工作压力、提高工作效率、保证工作质量、促进医疗事业的长远发展，是实现医院办公自动化建设的需求。网络安全管理还能优化医院的服务流程，让患者获得更加优质的服务。同时，引入更加先进的管理理念，规范工作人员的行为、提高医院管理工作的质量，是实现医院现代化管理的必然要求。

4 结束语

综上所述，医疗事业是一项社会事业，对民生健康和社会经济的发展有着重要影响。在现代社会的发展背景下，应做好医院计算机网络安全管理工作，实现医院的办公自动化和智能化管理，促进我国现代化建设的进一步发展。但就目前情况来看，医院在计算机网络安全管理工作中，还存在一些问题亟需解决。为解决这些问题，医院需不断提高计算机的软、硬件设施，提高工作人员的网络安全管理意识，以此来保证医院计算机网络系统运行的安全性和可操作性。

增强安全性。此外，安全策略的实施和监视需要在各地进行协调。在以往，安全和 IT 运营团队具有不同的目标、指标和薪酬结构。考虑到这些，企业可能会根据共同的项目而不是分散的目标来评估这些团队。对于像 ExtraHop，Netscout，Service Now，Tanium 这些在这 2 个领域都有技术和经验的供应商来说，应该是一个好消息。

如果安全厂商想跟上步伐，他们将需要改善自己的 IT 运营能力。