就安装具有防勒索功能的正版防护系统；入网后第一时间修复系统漏洞并升级病毒库，开启防护系统监控并进行全盘查杀。

（2）要谨慎上网。不点击可疑的链接，不下载、不打开可疑附件；通过官方渠道获取应用程序及升级包，警惕伪装为应用程序及升级包的勒索病毒。

（3）要及时备份重要数据，可以采用本地备份+脱机隔离备份+云端备份的三重备份方式。

5.2 局域网防御措施

局域网一般通过防火墙网闸等隔离设备与互联网隔离或者直接物理隔离，人们普遍存在物理隔离会带来绝对安全的错误认识，因此多数局域网并未采取充分的安全防御措施。然而目前勒索病毒已实现在局域网内传播。一旦勒索病毒攻破局域网内一台计算机，在防御能力不足的情况下，网内其他计算机将很快被攻破，对局域网数据安全造成毁灭性打击。

5.2.1 系统漏洞攻击防御措施

及时更新局域网内系统漏洞，防止攻击者通过漏洞入侵系统。在不影响正常业务的情况下修改容易被利用的端口号，可以使用私有端口代替 139、445 等公认端口；对于未使用的高危端口可以直接关闭，降低局域网被攻破的风险。

5.2.2 远程访问攻击防御措施

实现远程访问攻击的关键步骤之一就是实施弱口令攻击，可以使用复杂度高的密码增加攻破难度，避免使用 admin、user、root 等常用的用户名。此外还可以使用其他私有端口号代替默认的远程访问 3389 端口、使用其他加密登录软件代替系统默认远程登录工具等来防御远程访问攻击。

5.2.3 Web 服务防御措施

如果局域网中配置了 Web 服务器，应该及时更新 Web 服务器组件并安装软件补丁；同样 Web 服务也要避免使用弱口令。

5.2.4 数据库漏洞防御措施

采取及时更新数据库管理软件补丁，制定访问策略来限制访问数据库，及时备份数据库数据，拒绝使用弱口令等措施。

6　结束语

目前的病毒防护软件还是基于已经发现的网络攻击，新产生的勒索病毒只要穿透现有防御措施就会大面积迅速传播。未来勒索病毒还将会进一步与其他网络攻击方法相结合，攻击方法将更隐蔽、传播速度更迅速，这意味着安全防护将面临更大压力。运维人员及管理人员要在平时就要注重加强系统防护能力的建设，采取多种防御手段相结合的方法来加固系统，绝不能抱有侥幸心理，以防在新一轮的勒索病毒攻击中遭遇“灭顶之灾”。

参考文献：

[1]北京瑞星网安技术有限公司.瑞星 2021 年中国网络安全报告[R].北京.北京瑞星网安技术有限公司官网，2021.

[2]中国产业互联网发展联盟.2022 产业互联网安全是大趋势[R].人民邮电报，2022.

[3]詹洋.云存储系统中基于可信第三方的数据保护机制的研究[D].江苏：江苏大学，2018.

[4]蔡皖东.网络信息安全技术[M].北京：清华大学出版社，2015：29，40-41.

[5]于雪.互联网“生化危机”正在上演[J].中国经济报告，2017（6）：115-117.

数字企业网络安全评估体系设计

◆钟伟杰[1]　刘瑛[1]　陈静[2]

（1.海南电网有限责任公司　海南　571199；2.海南电网有限责任公司电力科学研究院　海南　571199）

摘要：在企业数字化建设过程中，网络安全评估是企业数字化环境安全保护中的一项重要工作。企业数字化资源在运行进程中，会由于遭到攻击者、病毒等各种因素的影响，进而产生不同的安全性问题，从而影响数字化系统使用的安全性。这时候也就需要通对企业的数字化环境进行安全评价，为企业的网络安全保护提供合理决策。传统线性的评估方式在目前网络安全评价中评测准确度较低，也因此使得评估结果不佳。笔者在日常工作中，采用了神经网络的网络安全评价体系，可以适应当前企业在数字化转型过程中网络安全保障的需要，并获得了广泛应用。因此本篇将着重解析在神经网络下的网络安全评估体系的设计。

关键词：网络安全评价；数字化；神经网络

当前，网络安全对于数字化技术发展是十分重要的，通过建设完整的安全防护系统保障数字化环境的稳定运行，是当今众多企业数字化建设过程中的核心。而对数字化环境的网络安全指标评估对于对数字化环境安全体系的管理以及技术升级也是十分有效的，能够保证数字化环境网络进行最严格的防护和更高效的发展。而研发自动化的评估系统，不但可以保证了数字化环境网络高效工作，同时也提高了网络的效率，因此在数字化企业中，加强针对数字化资源安全评估体系全面研究是十分有必要的。

1　数字企业网络安全评价体系

企业的数字化环境复杂度较大，涉及数字化技术的网络安全因素也较多，数字化安全评估系统的科学合理性设计，可以合理且充分发挥其网络安全评估的功能和作用。而在具体评估系统使用时，由于评价的差异，其评估取值准则亦存在不同，之中包含了定量评估技术指标和定性评价指标。而关于定性评价指标，则必须根据评估网络的实际状况决定取值范围，而另外一些定性指标则能够采用专家评估方法加以判断，根据数字化环境网络在评估时的实际状况提出适当的评估标准。针对不同的技术指标，也可以从不同视角判断数字化环境网络的稳定性，但技术指标间的取值范围往往缺乏可比性。而确立的评估指标系统，需要充分考虑到对神经网络训练的收敛情况，则必须是通过技术指标的规范性进行处理。而关于定性指标，则通过度量单位间的差别，规范性处理过程后得出取值范围，一般在 0~1 左右；对于定性指标，需要采用专门的评分方法来证明定量标准。总体而言，评价结果可分为：

非常安全：网络安全保障全面，在数字化资源运行和使用稳定性较好；

基本安全：网络安全保障初步具备，在数字化资源运行和使用也能够保证基本安全性；

不安全：网络安全保障措施很薄弱，在数字化资源运行和使用产生了一定的安全隐患；

很不安全：网络安全保护措施很差，在数字化资源运行和使用的安全隐患也很大。

2　对神经网络和数字化环境安全的评价综述

2.1 神经网络的起源与发展

网络神经利用数学模型模拟数据的处理和传输，这一概念引起了社会各领域学者的广泛关注。例如特斯拉马斯克：要实现自动驾驶，就要先实现 AI，现在的公路网是为神经网络的设计也就是我们的大

脑，直观的就是视觉、听觉。如果需要数字资源去处理这些，那么就要先在现实世界解决 AI 和视觉。我们需要用摄像头和硅神经网络，来处理我们的眼睛和生物神经网络。

数字化专业方向需要继续深度学习，随着神经网络的应用趋势，在计算需求的状态下使得数字化计算的发展速度得到了提高。像以往的信息系统应用中，用的是程序代码的图形计算，一个精细的角色有几十几百个关节，这些关节位置组合起来再加上其他输入，而且每一个物种的运动特征是不同的，两脚的生物运动模型显然不能用于四脚或者鱼的运动模拟。要用代码精确描述一个生物的运动规则，需要结合运动工程学，物理学，生物学，数字化环境图形学等等的专业知识，难度可想而知。那有没有不通过这些运动学的相关专业知识也能找到运动的规律呢？和所有从已知数据里寻找规律的方法一样——可以用人工神经网络代替。

2.2 数字化环境网络安全评价体系特点

为了保证数字化环境网络安全，数字企业利用信息技术，体系化地评估数字化环境与资源的风险因素。该评价方法逐步建立，成为较为完整的数字化网络安全评价体系。此后，神经网络技术的创新发展，通过对神经网络模型的详细研究，明确认识到神经网络的非线性结构特征。这为神经网络应用于数字化环境网络安全评估奠定了基础，提出了一种新的发展思路。

3　神经网络在数字化网络安全研究中的运用

3.1 建立评价指标集

数字化企业的信息系统设计非常复杂，需要的数字化资源、基础网络也种类、数量多，影响安全的因素很多。为此在设置评价指标的过程中需要考虑综合因素，使各个评价指标发挥完整的作用。

3.2 建立神经网络的数字化安全评价模式

这个模型的设置必须分三个部分执行。第一部分是设计输入层，将神经元节点数与所选评价指标数进行匹配。如果第一级参数结构中存在多个第二级指标，则必须将两个输入层神经元节点设置为两个兼容性。第二部分是重新设计隐藏层。在设计 BP 神经网络时，通常采用单个隐层。如果节点数量太大，学习时间太长，学习效率会降低。如果节点数量过少，会对网络的非线性映射和缺陷电阻产生负面影响。

一些研究人员利用神经网络进行数字化环境中，网络安全状态识别判断等方面的研究，他们使用数据初步判断，使得误差显著降低，获取数据是为了提高工作效率。在国内，将神经网络应用于网络入侵测试的工作很广泛，研究人员基于网络检测方法，提出了一种基于主机的网络入侵检测方案，达到了提取和检测各种网络攻击特征的目的。人类大脑依赖于预计算其分析并存储它们以供将来参考，之前一直默认在训练神经网络模型中的矩阵运算仅局限于数字化环境中的数字计算，没想到还能用模拟电路进行，实现了更高的效率。在效率和通用性不可兼得的情况下，两条路线都有其各自独特的价值。

3.3 神经网络的学习过程

由于神经网络是一个大尺度的复杂网络系统，为实际时间处理提供了重要条件。一般情况下，通过学习获得的知识作为互联网上需要研究的数据，分布在以全网系数的连接上，可以通过其他学习方法和内容，从各种网络获得各种应用。因此，它可以解决传统人工智能中的知识获取、知识表达等问题。此外，神经网络在处理输入数据失真方面具有很强的灵活性。人脑在于可以用其类似于黑箱的神经网络去模拟冯诺依曼数字化环境 CPU 的操作。人类文明建立于这种逻辑推理能力之上。然而对于真实的日常生活，人与人之间的相处，亲情友情爱情，这种 CPU 推理更多依赖的是外界输入的论点论据，而不是人们内心真正想要的或者真实的感受。实际上，当人和人相处的时候，根本不需要动用逻辑推理，直接黑箱神经网络借助于无数人类祖先训练好的模型就可以有很准确的答案了。尽管有时候人们不知道这个答案是怎么来的，正如人们不知道这个网络的形状和运行原理，但它就是高效且准确的。

BP 神经网络、隐层、输入输出层必须包含所有初始接口权限。在设置神经网络的构建模式之前，必须先了解这一点，使偏差最小化。首先要收集相关数据，这些数据要包括数字化环境网络安全性。在设定预期之后，建立网络模型。当然时间的长短和效果的好坏与输入层设计节点的数量直接相关。正确设计节点数量，提高工作效率，使 BP 神经网络安全评估更接近客户期望。首先，初始化 BP 神经网络的滥用，建立多维参数。其次，比较 BP 神经网络的单位粒子分析，选择效果最好的最佳数据值。同时，采用最合适的粒子惯性值。

3.4 应用神经网络对数字化环境评价模型进行验证

BP 神经模型不仅要学习网络安全评估模块，而且要验证模型的有效性。测试过程中，可以选择仿真样例数据，对网络安全评估模块的性能进行测试。如果各类型样本的评估结果与预期一致，则可以使用该模型，因为之前设置的模式可以对数字化环境网络安全做出正确的决策。当评估的结果和预期有很大的差异时，则说明这种评估模式出现错误，必须对每一个进行再次测试，重新进行选择直到与期望值符合。BP 自然网络信息分析是一种抽象的模拟人脑工作的数字化环境科学、生物学等有关的内容。因此，在数据处理方面，BP 具有足够的网络信息处理功能和信息变化或网络信息传输过程。

4　神经网络在数字化安全评估中的主要意义

神经网络完全融合了生物学原理和数学模型，利用数学模型来模拟神经元和传递信息，并逐渐应用到各个方面。

神经网络就是所谓的数据结构，它是一种用于在数字化环境硬件内部组织思想的形状或格式。如果在工作中的 IT 支持系统中可能成为队列的数据结构，甚至可能也对这些结构进行了编程代码。

神经网络不仅仅是物理数据结构——它是结构和在人工智能中使用结构的加权编程方法的总称。数字化技术不像单纯的数学学科，理论并不深奥，甚至很多也不严谨，逻辑上没有漏洞，加上有正确的实现，应该离成功不远了。

作为一种具有优势的神经网络算法架构，在数字化环境视觉、强化学习、图神经网络等领域逐渐渗透，展现出人工智能多学科领域通用架构的可能性。辅助设计芯片成为新趋势，预训练模型对于信息检索挖掘领域产生深远影响，有望形成基于 Web 大模型的新型信息检索范式。

4.1 使整个评价体系具备更强的适应性

该神经网络能够以最快的速度适应各种环境，如果所有的数据都是输入输出计算，神经网络就可以自我控制。同时，神经网络可以控制整个数字化网络的运行过程，在整个评价过程中起着重要的作用。

神经网络范式试图模拟人类大脑中神经元的计算结构，每个模拟神经元都可以是模拟软件中神经元模型的简单计算机程序，也可以通过电子实现。随着时间的推移，神经网络组织起来，神经网络也可以学习其主题，可以模仿广泛的人类模式识别能力。今天使用的有多种自组织方法，它们是上面讨论的神经网络模型的数学表亲。其中一种技术被称为 Markov 模型，广泛应用于自动语音识别系统.

4.2 使整个评价体系的容错性更高

在网络安全评估过程中，神经网络比现有评估方法具有更高的效率。数字化系统在运行过程中产生大量不完整的信息。由于神经网络对这些不完全信息不敏感，因此评估结果是不理想的。神经网络对不完全信息的初始设置不正确，则神经网络无法响应。

4.3 神经网络能够实现在线应用

在对网络安全环境进行评估的过程中，神经网络的重复判断速度更快。在大多数情况下，可以在输入数据后快速做出决定。这种有效的评价过程，实现了信息系统的在线使用，提高了应用效果。

5　结束语

综上所述，基于神经网络的数字企业网络安全评估系统设计中，通过神经网络在系统发生变化时继续保证系统的安全。适应环境，并对系统工作环境中的检测、分析和计算问题有效完成，另外神经网络在使用时还包含自动处理功能，可以明显提升其效率，所以在数字化环境安全评价系统应用上可以进一步增强神经网络应用能力。

参考文献：

[1]王谢玮.计算机网络安全评价体系的设计及应用[J].通讯世界，2015（24）：51.

[2]闫驰.GABP 神经网络算法在计算机网络安全评价方面的实施分析[J].电脑知识与技术，2021，17（27）：70-71+74.

[3]张文沛，熊小杰.基于神经网络的计算机网络安全评价仿真模型研究[J].数码世界，2020（08）：263-264.

[4]张钊.神经网络在计算机网络安全评价中的应用[J].电子技术与软件工程，2019（03）：176.