基于信息安全管理体系的技术脆弱性管理探讨

魏为民[1]，张运琴[1]，翟亚红[2]
（1.上海电力大学 计算机科学与技术学院，上海 200090；
2.中国网络安全审查技术与认证中心，北京 100020）

摘 要： 脆弱性是可能被一个或多个威胁利用的资产或控制的弱点。脆弱性识别是组织实施风险评估活动中最重要的一个环节，可从管理和技术两个方面进行识别。探讨了技术方面脆弱性的管理和软件安装限制两方面的最佳实践。提供一个关于技术方面脆弱性的实际审核案例，描述了主要的审核发现、沟通过程、受审核组织主要的改进方法等。

关键词： 信息安全管理体系；脆弱性；威胁；脆弱性管理；风险评估
中图分类号： TP399　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2096-5133.2020.12.004
引用格式： 魏为民，张运琴，翟亚红. 基于信息安全管理体系的技术脆弱性管理探讨[J].信息技术与网络安全，2020，39(12)：19-24.

Discussion on technical vulnerability management based on information security management system

Wei Weimin[1], Zhang Yunqin[1], Zhai Yahong[2]
(1.School of Computer Science and Technology, Shanghai University of Electric Power, Shanghai 200090, China;
2.China Cybersecurity Review Technology and Certification Center, Beijing 100020, China)

Abstract: Vulnerability is a weakness of an asset or control that can be exploited by one or more threats. Vulnerability identification is the most important activity of the organization's risk assessment, and it can be identified from both manager and technical aspects. This paper explores the best practices for management of technical vulnerabilities and restrictions on software installation, provides a practical audit case of technical vulnerability, describes the main audit findings and communication process and the main improvement methods of the audited organization, etc.

Key words: information security management system; vulnerability; threat; vulnerability management; risk assessment

0 引言

2013 年 10 月，国际标准化组织(International Organization for Standardization，ISO) 正式发布了 ISO/IEC 27001：2013《Information technology—Security techniques—Information security management systems—Requirements》，取代使用了 8 年之久的 ISO/IEC 27001：2005。2016 年 8 月，国家质量监督检验检疫总局与国家标准化管理委员会联合发布了 GB/T 22080-2016/ISO/IEC 27001:2013《信息技术 安全技术 信息安全管理体系 要求》，该标准使用翻译法等同采用 ISO/IEC 27001：2013，其中附录 A 包括 14 个控制域、35 个控制目标、114 项控制措施，并增加了资料性附录 NA 和 NB[1]。按惯例，ISO 每 5 年左右会对标准进行一次升级，2019 年 6 月，经评审和确认，ISO/IEC 27001：2013 标准维持现状[2]。上述标准中信息安全管理体系(Information Security Management Systems，ISMS)是指“基于业务风险方法，建立、实施、运行、监视、评审、保持和改进信息安全的体系，是一个组织整个管理体系的一部分[3]”。本文将重点讨论信息安全管理体系标准 GB/T 22080-2016 附录 A 中的“A.12.6 技术方面的脆弱性管理(Technical vulnerability management)”，包含“A.12.6.1 技术方面脆弱性的管理(Management of technical vulnerabilities)”和“A.12.6.2 软件安装限制(Restrictions on software installation)”两

项控制措施，其目标是“防止对技术脆弱性的利用(To prevent exploitation of technical vulnerabilities)”。

所谓脆弱性(vulnerability)，又称弱点或漏洞，ISO/IEC 27000：2016 中将脆弱性定义为“可能被一个或多个威胁利用的资产或控制的弱点[3]”，而威胁是“可能对系统或组织造成危害的不期望事件的潜在原由[3]”。在 GB/T 20984－2007 中的定义是“脆弱性是可能被威胁所利用的资产或若干资产的薄弱环节[4]”。由此可见，脆弱性是资产或系统本身固有的，如果没有被威胁所利用，仅仅脆弱性本身是不会对资产或系统造成损害的[4]。风险评估(risk assessment)是信息安全管理体系实施过程中最重要的一个活动，脆弱性识别(vulnerability identification)是风险评估中最重要的一个环节。而有些资产或系统的脆弱性只能在满足一定的条件和特定的环境下才能显现，这正是脆弱性识别困难之所在[5]。

1 脆弱性识别

1.1 脆弱性识别内容

资产或系统中脆弱性几乎是无处不在的。脆弱性产生的原因多种多样，其中主要的原因有计算机或网络系统在硬件、软件、协议设计和实现中存在缺陷或错误(包括设计错误、设置错误、网络协议自身的缺陷、输入验证错误、访问验证错误、意外情况处理错误、竞争条件、环境错误等)，采取的安全策略存在不足和缺陷，用户对系统的误用、误操作等。有时也把脆弱性称为漏洞，一般意义上的漏洞是系统设计和开发过程中存在的缺陷，非法用户能够在未经授权的情况下获得访问或提高其访问权限甚至破坏系统，由此可见漏洞是某种形式的脆弱性，但很多时候不加区分地使用脆弱性或者漏洞。

20 世纪 90 年代，美国国家标准协会根据漏洞发现时间、漏洞产生的原因和漏洞所处的位置对漏洞进行了分类。目前主要有 CVE(Common Vulnerability Exposures)、NVD(U.S. National Vulnerability Database)、SecurityFocus、OSVDB(Open Sourced Vulnerability Database)等几种针对漏洞的分类管理方式。其中 CVE 是由美国 MITRE 公司负责维护的全球公认安全漏洞索引标准[6]，其为每个确认的公开披露的安全漏洞，提供作为安全领域标识该漏洞的标准索引 CVE 编号，同时提供一段简单的漏洞描述信息。CVE 漏洞库定期发布，方便全球相关组织共享漏洞信息。

漏洞可能存在于物理环境、组织、过程、人员、管理、配置、硬件、软件和信息等各个方面。脆弱性一旦被威胁成功利用就可能对资产造成损害。脆弱性识别可从管理和技术两个方面进行，管理脆弱性包括与具体技术活动相关的技术管理脆弱性，如物理和环境、通信、运行、访问控制、系统获取、开发和维护、业务连续性等，以及与管理环境相关的组织管理脆弱性，如安全策略、信息安全组织、资产管理、人力资源、符合性等。技术脆弱性识别对象包括物理环境、网络结构、系统软件、应用中间件、应用系统等。可依据国际或国家安全标准、行业规范等进行脆弱性识别。例如，对物理环境和操作系统、数据库应分别按 GB/T 9361－2011 和 GB 17859－1999 中的技术指标进行脆弱性识别。对管理脆弱性识别可按照 GB/T 22081－2016 的要求对组织的安全管理制度及其执行情况进行核查[5]。以数据脆弱性识别为例，其识别示例如表 1 所示。

可以基于资产的损害程度、技术实现的难易等维度，并参考管理脆弱性的严重程度，采用等级方式对已识别的脆弱性严重程度进行赋值[2]。例如等级 1、2、3、4、5 分别表示，如果弱点被威胁利用将对资产造成可忽略的、较小的、一般的、重大的、完全的损害。此外还可以参考 CVE、CNNVD 等提供的漏洞分级作为脆弱性赋值参考。

1.2 脆弱性识别方法

用于脆弱性识别的方法主要有问卷调查、手工核查、文档查阅、工具检测、渗透性测试等，其数据来源应为资产或系统的所有者、使用者或者责任人，以及相关业务领域、软硬件开发维护方面的专业人员，应根据不同场景选择合适的方法。

工具检测(包含定制的脚本)的效率要明显高于手工核查，但是工具扫描可能会对被评估的生产系统造成可用性降低等不良影响。因此在执行扫描前应做好充分细致的计划和准备工作。扫描计划至少应包括：扫描对象或范围、工具选择和使用、扫描任务计划、风险规避措施等。

尽管工具检测有非常高的效率，但考虑到其风险性，对那些对可用性要求较高的重要系统还是采用手工核查方式进行脆弱性识别。在检查之前，需要事先准备好设备、系统或应用的检查列表。在进行具体的人工检查活动时，识别小组成员一般只负责记录结果，而检查所需的操作通常由相关管理员来完成。

表 1 数据脆弱性识别示例

类型	识别对象	识别内容
管理脆弱性	数据安全管理	数据管理总纲缺少数据安全相关内容，或没有成文的、经过专门的部门或人员制定、审核、发布的数据安全管理总纲；
		缺少数据安全管理制度或相关数据安全管理办法；
		缺少数据安全应急方案；
		缺少数据使用申请规范；
		缺少人员数据安全管理规范
	系统运维管理	未设立数据安全主管及数据安全各个方面的负责人岗位，并定义相关岗位职责；
		缺乏对个人进行数据安全意识教育、岗位技能培训，人员数据安全意识依然需要提高；
		未建立资产数据安全管理制度，规定资产管理的责任人员或责任部门，没有对个人介质进行控制和保护，并实行存储环境的专人管理；
		未建立数据审计制度，并定期对数据库日志和审计数据进行分析；
		未建立数据加密制度，并对核心数据结构化或非结构化数据进行加密；
		未建立数据防护管理办法，未清理数据请求规则及进行数据请求防护；
		未建立数据脱敏制度，未对敏感数据进行脱敏处理；
		没有根据数据重要性及其对业务系统运行的影响，制定数据的备份策略和恢复策略；
		没有关于安全响应和恢复方面的业务可持续性计划；
		未建立数据安全风险评估制度，并对数据资产进行风险评估及安全改进
技术脆弱性	数据库	数据库系统未安装最新的补丁程序；
		未删除对应的数据备份文件；
		数据库口令薄弱或长时间未进行修改；
		数据库鉴别机制简单
	数据应用	未进行数据分类分级；
		敏感数据存储时未进行加密；
		敏感数据使用、传输、共享交换时未进行脱敏处理；
		数据使用、传输、共享时未进行安全防护；
		敏感数据分布、数据流向不可视

渗透性测试(penetration test)是在确保被检测系统安全稳定运行的前提下，从攻击者的角度，通过模拟恶意攻击者的技术和攻击手法，主动利用安全漏洞，对目标网络、系统及应用的安全性进行深入透析，以发现系统的薄弱环节，评估计算机网络系统的安全程度。渗透测试方法有提供了背景和系统信息的白盒测试，和只提供基本信息或除公司名称外不提供任何信息的黑盒测试，以及提供与审计人员共享的目标有限知识的灰盒测试。渗透测试可以帮助组织发现系统安全漏洞、造成业务影响后果的攻击途径，并提出针对系统的薄弱环节进行修补与升级的技术方案。例如，作为 Web 应用程序渗透测试(Web Application Testing，WAPT)的场景有：跨站点脚本(Cross Site Scripting，CSS)、SQL 注入(SQL Injection)、破损的认证和会话管理(broken authentication and session management)、文件上载缺陷(file upload flaws)、缓存服务器攻击(caching servers attacks)、安全错误配置(security misconfigurations)、跨站点请求伪造(cross site request forgery)、密码破解(password cracking)等。

1.3 管理脆弱性核查

管理脆弱性的检测，一般采用问卷调查和管理记录查阅等现场调查方式，检测的内容主要有：

机构——安全管理机构的存在能够对管理制度制定和实施起到监督的作用，机构建设得不完全、不合理会给被评估系统的安全带来风险。

制度——明确、系统的安全管理规章制度可减轻系统的安全风险。

运行——网络正常运行、数据完整统一、业务连续运转。

人员——工作人员的管理和系统用户管理。

2 脆弱性管理实践指南

2016 年 8 月，国家质量监督检验检疫总局联合国家标准化管理委员会同步发布了 GB/T 22081－

2016 ISO/IEC 27002:2013《信息技术 安全技术 信息安全控制实践指南》[7],同样使用翻译法等同采用 ISO/IEC 27002:2013《Information technology—Security techniques—Code of practice for information security controls》及其相应的技术勘误(ISO/IEC27002:2013/COR1:2014),并增加了资料性附录 NA 和 NB。该标准可作为组织基于 GB/T 22080-2016/ISO/IEC 27001:2013 实现 ISMS 过程中选择控制时的参考,或作为组织在实现通用信息安全控制时的指南。本文重点讨论与 GB/T 22080-2016 中"A.12.6 技术方面的脆弱性管理"相对应的实践指南。

2.1 技术方面脆弱性的管理实践指南

ISO/IEC 27001 的"A.12.6.1 技术方面脆弱性的管理",其控制为"应及时获取在用的信息系统的技术方面的脆弱性信息,评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险[7]。即主要通过以下三个步骤进行脆弱性管理:

(1)及时发现漏洞。越早发现漏洞,并及时向厂商上报,就越有充足时间对其进行修复,留给攻击者利用漏洞的时间就越少。

(2)对组织的漏洞暴露情况进行评估。某个漏洞或一组漏洞对不同组织的影响可能不尽相同,需要进行风险评估,找出资产和业务的重要漏洞,并对其进行优先级排序。

(3)采取将相关风险考虑在内的适当措施。找出最严重的漏洞后,需考虑采取措施,然后分配资源处理漏洞,即制定风险处置计划。

ISO/IEC 27002 定义了实现脆弱性管理目标的支撑行动,提供实施上述安全措施时需考虑的最佳实践,建议采取以下行动:

(1)盘点资产。进行技术方面的脆弱性管理的先决条件是掌握当前完整的信息资产清单,包括软件厂商、软件版本、软件安装位置以及相关软件责任人。

(2)明确职责。脆弱性管理需进行多项不同活动(如监视、风险评估和纠正等),因此,需明确角色和责任,确保对资产进行合理追踪。

(3)明确参考资源。参考资料列表上应包含厂商站点、专业论坛和特别兴趣小组,从而了解漏洞与修复措施相关的新闻,并及时更新。

(4)按照制定的流程处理漏洞。按照漏洞优先级,根据变更管理或事件响应规程采取相应的措施,如打补丁或应用其他控制。

(5)记录并事后分析。记录所发生的事件以及事件处理过程,并定期评审,确保可尽快改进和修复漏洞。

另外,如果有可用的补丁,宜评估漏洞引起的风险和安装补丁带来的风险。补丁在安装之前,应进行测试和评价,确保是有效的且不会导致重大的负面影响。如果没有可用的补丁,就应考虑其他控制措施,如关闭有漏洞的服务、调整访问控制、加强监视、提高安全意识等。

总之,由于市场需要更快速的软件交付及更多特性,将会有更多漏洞出现[8]。因此,为确保组织的信息资产安全、维护企业形象以及保持竞争力,制定漏洞发现和处理计划非常重要。同时,应该充分利用威胁情报信息,深度解读漏洞利用细节、利用热度、利用难度等,为 IT 运维人员提供详实的漏洞细节,便于他们结合企业实际情况分析漏洞影响,为漏洞修复提供决策依据,真正实现漏洞管理的闭环操作。

2.2 软件安装限制实践指南

ISO/IEC 27001 的"A.12.6.2 软件安装限制",其控制为"应建立并实现控制用户安装软件的规则[7]。考虑到在计算机设备上安装不受控制的软件可能违反知识产权,甚至可能导致信息泄露、完整性损失或其他信息安全事件。ISO/IEC 27002 提供了如下实践指南:

(1)制定软件安装策略。基本原则是软件应该由专业人员或者 IT 运维人员来安装,普通员工应禁止从互联网下载软件。员工需要安装特定的软件应提出申请,IT 部门确认是否有该软件的授权,若有则为相关人员安装该软件;若没有授权,则应评估该软件及类似功能软件的必要性,如果是收费软件,还应进行相应的财务审批。

(2)最小授权原则。应根据用户所涉及的角色最小化授权,如果用户获得了某些特权,就有可能随意安装或删除特定的软件。组织宜建立软件安装白名单(允许安装的软件)和黑名单(禁止安装的软件)。以 Windows 10 为例,可通过组策略编辑器(gpedit.msc)设置软件安装限制策略。路径如下:计算机配置——Windows 设置——安全设置——软件限制策略。

2.3 漏洞管理趋势

大量数据和案例表明,虽然漏洞评估和管理工

具日新月异,但漏洞管理始终是企业网络安全的致命环节,近年来60%的企业数据泄露与安全漏洞未得到修补有关。基于合规性的要求,企业将不得不部署漏洞管理程序。漏洞管理重在“管理”,企业的漏洞管理或脆弱性风险相关管理依然存在很大的改进空间。与此同时,漏洞风险正随着攻击技术的快速升级而增加,例如攻击者在利用机器学习/人工智能技术方面已经超越了防御者,企业用于预防、检测、修补、记录和报告的漏洞管理工作平均成本正在不断上升。因为人员配备不足,或者担心补丁修补过程导致关键应用程序和系统停机,补丁修补过程经常被延迟。在软件中发现安全漏洞后,大多数企业都希望开发人员能够迅速采取行动来解决问题,管理层对补丁延误的容忍度在不断降低,在增加人手的同时,通过自动执行补丁管理流程来缩短补丁时间将是应对补丁挑战的重要方式。

3 脆弱性管理审核案例

3.1 审核案例背景

案例类型:信息安全管理体系(ISMS)

受审核方:XXXX信息有限公司

审核类型:第一次监督审核

审核依据:GB/T 22080-2016/ISO/IEC 27001:2013,SOA 3.0

3.2 案例发生的主要过程

受审核方是国内领先的互联网金融平台,基于业务角度出发,认识到信息安全的重要性,依据GB/T 22080-2016/ISO/IEC 27001:2013标准策划和建立了信息安全管理体系,希望能做到规范管理体系,切实完善安全管理制度,执行安全控制措施,不断提高信息安全风险管理水平。受审核方建立信息安全管理体系的总体方针“业务为核心;风险导向;持续改进;指导与参与;技术与管理并重;合规性”。该信息安全方针作为受审核方安全工作的总方向,为目标设定提供框架。《信息安全适用性声明》版本为V3.0,选择了标准附录A的所有控制措施。

2018年某日,审核组按照计划审核人事行政部,该部门主要职责为:负责公司人事、行政、总务等综合管理工作;负责打造符合公司战略的人力资源体系,确保公司团队升级、吸引和保留优秀人才,打造积极向上的企业文化。该部门人员基本稳定,所有入职员工签署保密协议,管理岗位和核心技术岗位员工有背景调查,员工离职按照《离职流程》撤销和复查相应的权限。审核发现该部门一台用于薪酬数据备份的笔记本电脑未设置屏保,自2018年1月19日该机启用以来从未安装Windows更新,未更新病毒和间谍防护软件。

3.3 主要的审核发现、沟通过程及改进方法

人事行政部的这台笔记本电脑配置为:Windows 7 Pro SP1;安装内存(RAM):4.0 GB;系统类型:64位操作系统。从控制面板查看Windows Update状态:

最近检查更新的时间:从未

安装更新的时间:从未

接收更新:仅适用于Windows产品和其他来自Microsoft Update的产品。

查看Windows Update:“C:\Windows\Windows-Update.log”更新日志文件,结果与上述状态一致。

该笔记本电脑貌似一台“孤岛”式的电脑,但由于该电脑除了主要用于薪酬数据备份外,偶尔还用于其他工作,存在数据之间的交换,因此极有可能感染计算机病毒,从而传染到工作网络,违反公司《信息系统使用安全制度》和《漏洞扫描管理流程》,据此开具不符合项,涉及的标准条款:

A.11.2.9 清理桌面和屏幕策略:应针对纸质和可移动存储介质,采取清理桌面策略;应针对信息处理设施,采用清理屏幕策略。

A.12.6.1 技术方面脆弱性的管理:应及时获取在用的信息系统的技术方面的脆弱性信息,评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险。

受审核方高度重视本次审核结果,对不符合项进行原因分析如下:薪酬电脑由于断网未在域控范围内,因此未同步域策略,也未对该关键电脑人工定期进行安全策略的配置和更新。

采取的纠正措施为:该电脑属于HR部门专用电脑,单机不加域,已经设置了自动锁屏及密码,采用手动更新防病毒软件的病毒库以及Windows关键更新,并每个季度检查更新一次。

4 结论

目前,随着工业互联网、智能制造的深入发展,企业采用的主机操作系统、通信协议、应用软件已大量采用通用技术,传统的互联网安全风险已可对企业生产端造成影响;工业企业打造工业互联网过程中,不断加强系统互联互通,对部分安全风险和威胁渗透扩散提供了有利环境。而很多企业存在以

下误区：一是工业尤其是工控系统信息相对安全，缺乏推进工作的主动性；二是认为隔离的工业网络就绝对安全，其内部网络、主机和设备基本不作安全防范，一旦网络隔离被突破将造成严重影响；三是工业主机、工控系统等的操作系统、软件应用版本老旧，且认为进行补丁升级操作将带来生产安全风险或无法得到生产厂商维保服务，而几乎不作补丁升级，存在安全隐患；四是认为部署持续性的在线安全监测手段不必要，使得应对突发性的漏洞、病毒等事件不及时，应急措施严重缺乏。

建议企业注重发展过程中的信息安全风险，按照《中华人民共和国网络安全法》要求，落实网络安全主体责任和等级保护等基本安全制度；对照《工业控制系统信息安全防护指南》等的有关要求，对工业互联网中的安全薄弱环节，重点加强工业网络、主机、控制设备的安全软件部署和安全配置，软件补丁升级管理，生产网、办公网等网络隔离，互联网远程访问控制，以及外连设备安全连入管理等有关工作。

参考文献

[1] GB/T 22080-2016/ISO/IEC27001：2013 信息技术 安全技术 信息安全管理体系 要求[S].2016.

[2] ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT[EB/OL].[2020-09-01].https://www.iso.org/isoiec-27001-information-security.html.

[3] GB/T 29246-2017/ISO/IEC 27000：2016 信息技术 安全技术 信息安全管理体系 概述和词汇[S].2017.

[4] GB/T 20984-2007 信息安全技术 信息安全风险评估规范[S].2007.

[5] 邢栩嘉，林闯，蒋屹新.计算机系统脆弱性评估研究[J].计算机学报，2004(1)：1-11.

[6] Common Vulnerability and Exposures[EB/OL].[2020-09-01].http://cve.mitre.org/.

[7] GB/T 22081-2016/ISO/IEC27002:2013 信息技术 安全技术 信息安全控制实践指南[S].2016.

[8] 韦正现，宋敏，童鹏鹏，等.一种基于信息熵的体系流程脆弱性分析方法[J].科技导报，2019，37(13)：40-46.

(收稿日期：2020-09-28)

作者简介：

魏为民(1970-)，男，博士，副教授，主要研究方向：信息安全、图像处理、数字取证和信息隐藏。

张运琴(1996-)，男，硕士研究生，主要研究方向：信息安全、图像处理。

翟亚红(1974-)，女，本科，高级工程师，主要研究方向：网络安全与认证认可。

(上接第 18 页)

[9] 顾欣，徐淑珍.区块链技术的安全问题研究综述[J].信息安全研究，2018，4(11)：997-1001.

[10] 王静，蒋国平.一种超混沌图像加密算法的安全性分析及其改进[J].物理学报，2011(6)：89-99.

[11] 呼阳，陈亮.基于区块链的生产线数据共享方案研究[J].国外电子测量技术，2019(5)：123-127.

[12] 谢向军.大数据环境下物流企业的数据信息安全保障对策分析[J].信息通信，2017(6)：34-36.

[13] 严霄蕙.区块链技术驱动下的新零售业态变化与发展路径[J].技术经济与管理研究，2019，27(1)：13-18.

[14] 罗杏玲.区块链技术在物流领域中的应用探索[J].中国商论，2017(24)：7-8.

[15] 彭长根，田有亮，刘海，等.密码学与博弈论的交叉研究综述[J].密码学报，2017，4(1)：1-15.

[16] 吴腾，黄锴，周琳琳，等.具有状态合法性验证的区块链一致性算法研究[J].计算机工程，2018，44(1)：160-164.

[17] GERVAIS A，KARAME G O，WÜST K，et al.On the security and performance of proof of work blockchains[C].ACM Sigsac Conference on Computer & Communications Security.ACM，2016.

[18] PASS R，SEEMAN L，SHELAT A.Analysis of the blockchain protocol in asynchronous networks[C].Annual International Conference on the Theory and Applications of Cryptographic Techniques.Paris，France，2017.

(收稿日期：2020-09-09)

作者简介：

龙萍(1995-)，女，硕士研究生，主要研究方向：区块链、数据安全与隐私保护。

邢镔(1962-)，通信作者，男，博士，教授级高级工程师，主要研究方向：智能制造、数据处理和工业数字仿真。E-mail：xingbin@casic.com.cn。

胡小林(1984-)，男，硕士，研究员，主要研究方向：智慧物流、智能仓储。

版权声明