电力企业网络安全威胁情报管理体系的研究与实践

陈伟雄[1]，杨晓晨[2]，春增军[1]，李若兰[3]，张华[1]
（1. 中广核智能科技（深圳）有限责任公司，广东 深圳 518026;
2. 上海中广核工程科技有限公司，上海 200241;
3. 中国广核集团有限公司，广东 深圳 518026）

摘　要：网络安全是国家安全的重要组成部分，网络安全威胁情报工作成为网络安全防护工作重要内容，针对电力企业开展网络安全威胁情报来源多、种类多、范围广、漏洞风险多、涉及部门和人员多等问题，提出了电力企业网络安全威胁情报工作方案，方案包括情报来源、情报研判、情报处置、情报平台、情报绩效 5 个方面，设计了网络安全漏洞评估方法、情报标准化处理流程、情报绩效评价方法。初步应用结果表明该方案对提升电力企业网络安全情报应急处置能力、网络安全防护能力水平具有重要参考价值。

关键词：网络安全；威胁情报；漏洞评估；绩效评价
中图分类号：TP393.08
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2022133

Research and practice of network security threat intelligence management system for power enterprise

CHEN Weixiong[1], YANG Xiaochen[2], CHUN Zengjun[1], LI Ruolan[3], ZHANG Hua[1]
1. CGN Intellgent Technology Co., Ltd., Shenzhen 518026, China
2. Shanghai Engineering Science & Technology Co., Ltd., Shanghai 200241, China
3. China General Nuclear Power Corporation, Shenzhen 518026, China

Abstract: Network security is an important part of the national security, and network security threat intelligence work has become an important part of the network security protection. Aiming at the problems of power enterprise carrying out network security threat intelligence, such as many sources, many types, wide range, many vulnerability risks, many subordinate departments and personnel, the network security threat intelligence work plan of power enterprise was put forward. The scheme includes five aspects: information source, information research and judgment, information disposal, information platform and information performance. The evaluation method of network security vulnerabilities, information emergency disposal process and information performance evaluation method were puts forward. The preliminary application results show that the proposed scheme has important reference value for power enterprise to improve the emergency response ability of network security information and the level of network security protection ability.

Key words: network security, threat intelligence, vulnerability assessment, performance evaluation

收稿日期：2021−11−24；修回日期：2022−03−14

0　引言

网络安全是国家安全的重要组成部分，是国家安全的基础。近年来，党中央高度重视网络安全工作，并对网络安全工作提出明确要求，采取措施，监测、防御、处置境内外的网络安全风险和威胁，加强网络安全信息统筹机制、手段、平台建设，建立健全网络安全保障体系，全方位提升网络安全防护能力。

所谓网络安全威胁情报，是指对企业产生潜在与非潜在危害的网络安全信息的集合，它主要利用互联网资源、网络安全机构或人员，预测企业潜在的网络安全威胁。电力企业开展网络安全威胁情报的工作目标：为电力企业建立一个网络安全预警机制，在网络安全攻击到达前，减少或消除网络安全漏洞等风险；为电力企业提供更完善的网络安全事件应急响应方案；通过 0day/*N*day 漏洞补丁更新，提升电力企业部署网络安全设备资产的安全能力，避免成为攻击利用突破口；加强攻击 IP 地址、恶意程序/网站、网络钓鱼、勒索病毒的情报收集，建立电力企业的快速响应与标准化工作机制；基于网络安全“以攻促防”理念，反推攻击者攻击思路与攻击链路，针对性防护关键网络节点。

目前网络安全威胁情报工作存在如下问题。

（1）情报来源多、范围广

目前网络安全情报来源国家、省、市网络安全主管机构，也有国内主流网络安全技术机构，还有电力企业网络安全同行，更多来自互联网（技术论坛、微信公众号等）。网络安全情报信息来源不同、范围广、非结构化，增加了网络安全情报人员人工收集和分析成本，也增加了网络安全快速响应时间，对于情报信息收集标准化、规范化工作和提升快速响应水平存在一定障碍。

（2）情报价值与漏洞风险评价

在电力企业实际工作过程中，经常遇到很多网络安全威胁情报（如操作系统漏洞、网络安全产品漏洞、中间件漏洞等），如何根据目前各种情报，快速筛选威胁情报价值高、网络安全风险比较高进行优先处置，这需要考虑情报价值评估方法。

（3）网络安全情报快速处置

电力企业经常遇到网络安全情报多、漏洞风险多、下属部门人员多，如何快速有效地进行网络安全漏洞排查，建立高效的漏洞情报排查跟踪机制，也是网络安全情报工作体系的工作要求。

目前有关网络安全威胁情报已有一些研究。王长杰等[1]提出一种针对恶意软件家族的威胁情报生成方法；陈剑锋等[2]提出了一种面向网络空间安全的威胁情报本体化共享方法；陈明等[3]提出网络空间安全战略情报保障能力是由情报保障工作主体、情报信息、情报手段、目标追求，以及时空条件等要素体系化运作后表现出的一种体系能力；徐锐等[4]提出从网络防御的视角介绍安全威胁情报的作用和工作流程，设计安全威胁情报即服务（threat intelligence as a service，TIaaS）的体系架构；徐留杰等[5]提出一种多源网络安全威胁情报采集与封装技术。以上网络安全威胁情报研究方法对当前网络安全威胁情报具有一定参考价值，但是在网络安全实践中，需要进一步验证。

1　网络安全威胁情报管理体系构建

综合当前网络安全情报主要问题，本文提出建立电力企业网络安全威胁情报管理工作体系，包括情报来源、情报研判、情报处置、情报平台、情报绩效 5 个方面内容，网络安全威胁情报管理体系的架构如图 1 所示。

图 1　网络安全威胁情报管理体系的架构

1.1 情报来源——建立网络安全威胁情报主动收集机制

网络安全情报包括漏洞风险、APT（advanced persistent threat）攻击、恶意 IP 地址、钓鱼攻击等信息，有来自国家漏洞中心、应急响应中心、国内主流网络安全机构的信息，也有来自非公开情报机构等的信息，情报格式有漏洞报告、邮件预警、微信共享、威胁通报等不同格式，为此，利用情报管理平台，统一网络安全情报格式信息：情报编号、情报类别、风险级别、情报来源、排查类别、收集日期、相关单位、评估状态，统一通过情报管理平台进行收集工作。网络安全威胁情报收集流程如图 2 所示。

1.2 情报研判——根据不同漏洞类型评估紧急程度

网络安全情报根据不同漏洞类型进行技术研判，主要包括 Web 漏洞（SQL 注入、XSS 漏洞、上传漏洞、Struts2 远程命令执行、敏感信息泄露等）、系统漏洞（Windows 操作系统、Linux 系统、Exchange Server 等）、服务漏洞（FTP 服务漏洞、SSH 服务、Windows 远程连接漏洞、DHCP 服务等）、协议漏洞（ARP 漏洞、DNS 协议漏洞、FTP 漏洞等）。根据网络安全情报确定超高危、高危、中危、低危漏洞，并根据情报评估规则，判定紧急程度（高、中、低）及其对应优先级别。网络安全威胁情报研判评估流程如图 3 所示。

1.3 情报处置——建立网络安全威胁情报标准化处置流程

建立了网络安全威胁情报标准化处理流程（standard operation procedure，SOP），如图 4 所示，包括情报收集、分类处理、处置反馈、通报考核 4 个方面。

- 情报收集方面，充分利用各同行、各地区网络安全情报分享、专业化网络安全保障机构等各方面来源及时收集汇总。
- 分类处理方面，加强网络安全威胁情报分类收集和处理，由专业技术研判人员判断排查对象，确定需要网络安全排查范围和排查紧急程度。
- 处置反馈方面，通过网络安全情报跟踪平台下发排查整改通知，邮件或微信提醒，如发现相关问题，要求及时整改；若未找到相关解决方法，需做临时下线处理，持续追踪。
- 通报考核方面，加强网络安全威胁情报排

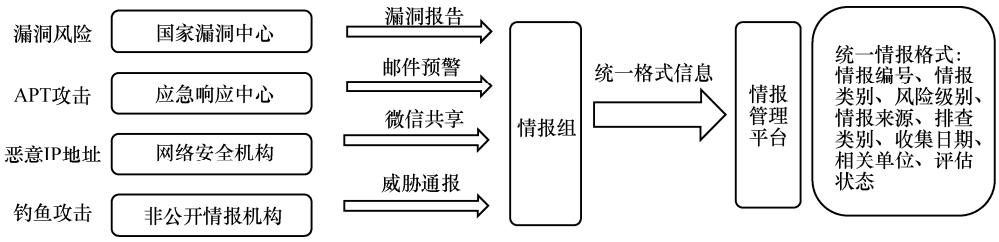

图 2 网络安全威胁情报收集流程

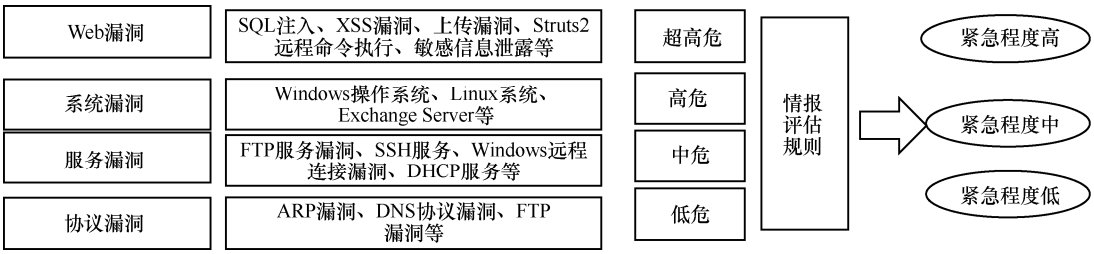

图 3 网络安全威胁情报研判评估流程

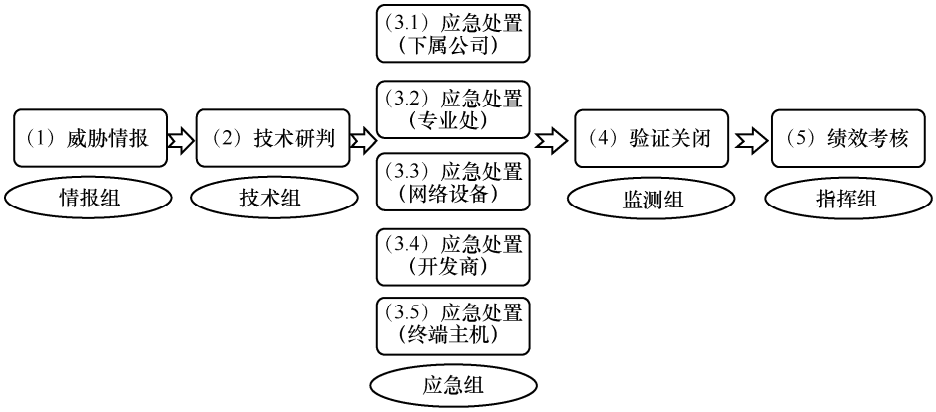

图 4　网络安全威胁情报标准化处理流程（SOP）

查管控，并在网络安全态势感知会议通报各单位网络安全考核结果。

1.4　情报平台——建立网络安全情报管理平台

网络安全威胁情报纳入电力企业网络安全管理平台专项跟踪，实现电子化管理，及时统计和提醒下属各单位网络安全漏洞排查整改情况，并通过邮件或手机短信等形式进行提醒。

1.5　绩效评估——加强各网络安全情报绩效评估工作

网络安全情报来源主要分为外部情报与内部威胁情报，外部威胁情报来自相关机构提供的情报信息。内部威胁情报基于自建的威胁挖掘团队，通过联合各大专业厂商，部署了如态势感知、下一代防火墙等监测及防护类设备，对日常访问的流量及日志进行统一收集，同时组织各厂商安排大量技术专家对收集的数据进行分析处理，输出威胁情报以供指挥部参考，及时调整防护策略及网络节点，同时还会反推产品升级，增强产品防护与监测能力。网络安全威胁情报绩效考核示意图如图 5 所示，网络安全威胁情报绩效考核包括如下内容。

- 情报搜集及时性：评价是否及时收集到网络安全漏洞信息，尤其是 0day/*N*day 信息；
- 技术研判准确性：评价是否正确研判网络安全漏洞影响范围、风险大小并评价其优先程度合理性。

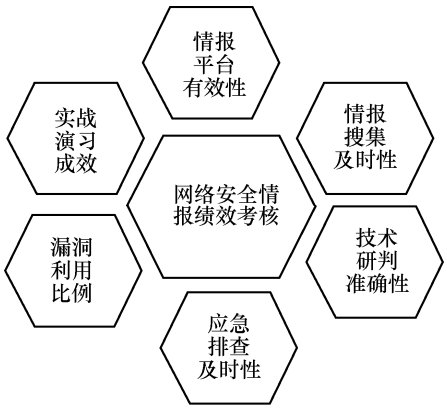

图 5　网络安全威胁情报绩效考核示意图

- 应急排查及时性：评价是否在规定时间组织相关下属单位或部门排查，是否存在指令不通畅情况。
- 漏洞利用比例：评价网络安全漏洞是否被成功利用数量比例。
- 实战演习成效：评价是否在实战演习下，网络安全情报组织体系是否有实际效果，收集情报数量，并是否可以成功处置 0day/*N*day 漏洞。
- 情报平台有效性：情报平台是否可以实现情报信息有效排查、跟踪、统计，并及时预警相关单位整改等。

2　网络安全漏洞评估方法

网络安全威胁情报来源多、种类多、范围广、漏洞风险多，根据某电力企业网络安全实际情况，

发现高危漏洞有时有 10～100 种漏洞需要紧急排查、整改、安装漏洞补丁，如何评估漏洞排查优先顺序，本文提出漏洞评估方法，漏洞规则库由漏洞影响范围和漏洞风险程度组成，影响范围包括全公司级、部门级、个人，风险程度分为高、中、低，依次安排计算因子，漏洞优先级=影响范围×风险程度，如果优先级分数 80 分以上，则优先安排整改（打漏洞补丁或其他网络安全风险排除措施）。网络安全威胁情报漏洞评估示意图如图 6 所示。

3 结束语

以上网络安全威胁情报管理平台已在某电力企业初步应用，并在网络安全实战演习期间及时发布安全漏洞情报排查通知，累积排查 33 000 多次漏洞且修复率高达 99.7%，弥补了网络安全管理薄弱节点，保障网络安全演习工作取得了预期成果。在后续网络安全工作中，作者将加强网络安全威胁情报工作方法论研究，积极向优秀网络安全单位学习经验，充分利用网络安全保障机构力量，利用“以攻促防”的理念，努力做好网络安全保障工作，快速提升电力企业网络安全防护能力，持续打赢电力企业网络安全保卫战。

参考文献：

[1] 王长杰, 李志华, 张叶. 一种针对恶意软件家族的威胁情报生成方法[J]. 信息网络安全, 2020, 20(12): 83-90.
WANG C J, LI Z H, ZHANG Y. A threat intelligence generation method for malware family[J]. Netinfo Security, 2020, 20(12): 83-90.

[2] 陈剑锋, 范航博. 面向网络空间安全的威胁情报本体化共享研究[J]. 通信技术, 2018, 51(1): 171-177.
CHEN J F, FAN H B. Ontological threat intelligence sharing in cyberspace security[J]. Communications Technology, 2018, 51(1): 171-177.

[3] 陈明, 王乔保, 汤文峤. 网络空间安全战略情报保障能力研究[J]. 情报杂志, 2020, 39(4): 127-131.
CHEN M, WANG Q B, TANG W Q. The capability of strategic intelligence supporting for cyberspace security[J]. Journal of Intelligence, 2020, 39(4): 127-131.

[4] 徐锐, 陈剑锋, 刘方. 网络空间安全威胁情报及应用研究[J]. 通信技术, 2016, 49(6): 758-763.
XU R, CHEN J F, LIU F. Research on cyber threat intelligence and applications[J]. Communications Technology, 2016, 49(6): 758-763.

[5] 徐留杰, 翟江涛, 杨康, 等. 一种多源网络安全威胁情报采集与封装技术[J]. 网络安全技术与应用, 2018(10): 23-26.
XU L J, ZHAI J T, YANG K, et al. A multi-source network security threat intelligence collection and packaging technology[J]. Network Security Technology & Application, 2018(10): 23-26.

[6] 朱薏. 计算机网络安全分层评价防护体系的构建与应用研究[J]. 大众标准化, 2020(24): 50-51.
ZHU Y. Research on the construction and application of hierarchical evaluation and protection system for computer network security [J]. Popular Standardization, 2020(24): 50-51.

[7] 吴仲. 计算机网络安全风险评价及防范措施探析[J]. 电子技术与软件工程, 2015(19): 216.
WU Z. Computer network security risk assessment and analysis of preventive measures [J]. Electronic Technology & Software Engineering, 2015(19): 216.

[8] 黄欣. 计算机网络安全威胁与防范措施[J]. 产业与科技论坛, 2011, 10(5): 95-96.
HUANG X. Computer network security threats and precautions[J]. Industrial & Science Tribune, 2011, 10(5): 95-96.

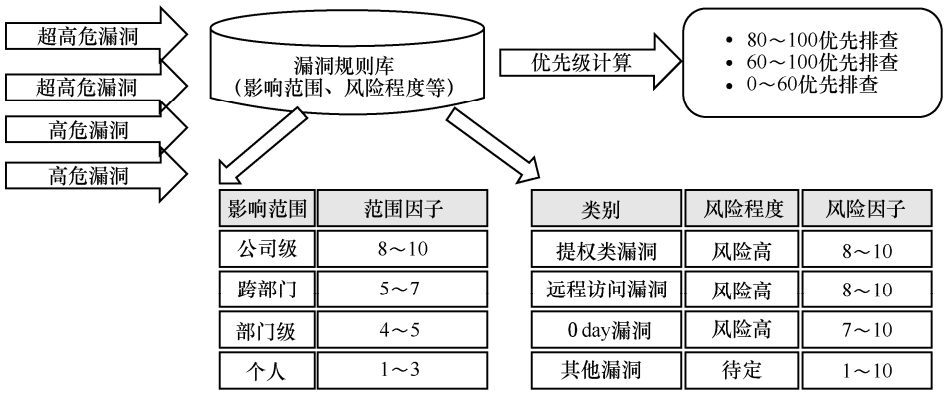

图 6 网络安全威胁情报漏洞评估示意图

[9] 林晨希, 薛丽敏, 韩松. 浅析网络安全威胁情报的发展与应用[J]. 网络安全技术与应用, 2016(6): 12-13, 15.
LIN C X, XUE L M, HAN S. A brief analysis of the development and application of cybersecurity threat intelligence [J]. Network Security Technology & Application, 2016(6): 12-13, 15.
[10] 王晓周, 乔喆, 李雨昂, 等. 基础电信企业网络安全威胁情报工作思路探讨[J]. 电信工程技术与标准化, 2018, 31(12): 7-12.
WANG X Z, QIAO Z, LI Y A, et al. Discussion on cyber security threat intelligence work of telecom operators[J]. Telecom Engineering Technics and Standardization, 2018, 31(12): 7-12.
[11] 刘俊博, 马博克. 网络安全模糊风险评价方法与应用[J]. 网络安全技术与应用, 2020(5): 3-4.
LIU J B, MA B K. Network security fuzzy risk assessment method and application [J]. Network Security Technology & Application, 2020(5): 3-4.
[12] 董聪, 姜波, 卢志刚, 等. 面向网络空间安全情报的知识图谱综述[J]. 信息安全学报, 2020, 5(5): 56-76.
DONG C, JIANG B, LU Z G, et al. Knowledge graph for cyberspace security intelligence: a survey[J]. Journal of Cyber Security, 2020, 5(5): 56-76.
[13] 林玥, 刘鹏, 王鹤, 等. 网络安全威胁情报共享与交换研究综述[J]. 计算机研究与发展, 2020, 57(10): 2052-2065.
LIN Y, LIU P, WANG H, et al. Overview of threat intelligence sharing and exchange in cybersecurity[J]. Journal of Computer Research and Development, 2020, 57(10): 2052-2065.
[14] 黄克振, 连一峰, 冯登国, 等. 基于区块链的网络安全威胁情报共享模型[J]. 计算机研究与发展, 2020, 57(4): 836-846.
HUANG K Z, LIAN Y F, FENG D G, et al. Cyber security threat intelligence sharing model based on blockchain[J]. Journal of Computer Research and Development, 2020, 57(4): 836-846.
[15] 尹立君. 基于大数据下的网络安全威胁感知决策指挥系统设计[J]. 邯郸职业技术学院学报, 2020, 33(1): 63-66, 90.
YIN L J. Design of network security threat perception decision command system based on big data[J]. Journal of Handan Polytechnic College, 2020, 33(1): 63-66, 90.
[16] 肖俊芳. 网络安全威胁情报概述[J]. 保密科学技术, 2016(6): 12-15.
XIAO J F. Cybersecurity threat intelligence overview [J]. Secrecy Science and Technology, 2016(6): 12-15.

[作者简介]

陈伟雄（1974− ），男，中广核智能科技（深圳）有限责任公司高级工程师，主要从事网络安全情报、网络安全态势感知研究等工作。

杨晓晨（1963− ），男，上海中广核工程科技有限公司高级工程师、副总工程师，主要从事网络安全与数字化转型规划、网络安全演习技术研究工作。

春增军（1973− ），男，博士，中广核智能科技（深圳）有限责任公司研究员级高级工程师，主要从事网络安全架构与网络安全技术研究工作。

李若兰（1982− ），女，中国广核集团有限公司高级工程师，主要从事网络安全等保测评、应急演练等工作。

张华（1980− ），女，中广核智能科技（深圳）有限责任公司工程师，主要从事网络安全管理、网络安全管理平台设计开发等工作。

《电信科学》第六届编辑委员会

收录声明

本刊已被中国核心期刊遴选数据库(万方)、中国学术期刊数据库(知网)全文收录,被本刊录用的文稿,将一律由编辑部统一纳入中国核心期刊遴选数据库(万方)、中国学术期刊数据库(知网)。若作者不同意被收录,将在来稿时向本刊说明,本刊将做适当处理。若无特别声明,视同将录用文稿的电子网络版、汇编或合订本的使用权授予本期刊社,本刊支付的稿费中已包含上述费用。

The articles of *Telecommunications Science* have been embodied by WANFANG DATA and CNKI. The accepted articles will be unified into WANFANG DATA and CNKI. If the author does not agree to his or her article to be included, the author must illustrate when the article is submitted. The editorial department will properly handle. If the authors do not give a special announcement, the editorial department believes that the authors have granted the right of their articles to *Telecommunications Science*. The expenses have been included in the fee paid by editorial department.

道德声明

本刊发表的文稿是作者独立取得的原创性研究成果,无一稿多投;文稿内容不涉及国家机密;未曾以任何形式用任何文种在国内外公开发表过;文稿内容不侵犯他人著作权和其他权利。若发生一稿多投、侵权、泄密等问题,文稿作者将承担全部责任。

The authors of *Telecommunications Science* guarantee that their submitted articles are original and contain nothing confidential. The said article is only submitted to *Telecommunications Science*. The said article has not been published before and has not been submitted elsewhere for print or electronic publication consideration. The said article is in no way whatever a violation or an infringement of any existing copyright or license from the third party. Otherwise, the authors of the said article shall take the blame for the violation or infringement of the related copyright and the leakage of secrets.

电信科学

Telecommunications Science

ISSN 1000-0801

邮发代号：2-397　国外代号：M841　定价：68.00元