文章编号：2096-1472(2018)-01-21-03
DOI:10.19644/j.cnki.issn2096-1472.2018.01.006

安全应急响应中心平台的设计与实现

游林飞，林 章，岳凌锋，鲍忠秀，潘钟强
(福州外语外贸学院信息系，福建 福州 350202)

摘 要：随着网络技术的迅速发展和普及，网络安全已经成为企业必不可少的环节。本文通对现有企业网络安全的调查和分析，结合企业网络安全的要求与平台功能需求，采用B/S结构模块化设计的基本思路，设计实现了一个基于PHP的网络安全应急响应中心，为企业实现漏洞收集和披露计划。因此，建立适合中小企业的网络安全应急响应中心平台具有十分重要的现实意义。

关键词：网络安全；漏洞收集；披露计划；应急响应平台
中图分类号：TP311 **文献标识码**：A

Design and Implementation of the Security Emergency Response Center Platform

YOU Linfei,LIN Zhang,YUE Lingfeng,BAO Zhongxiu,PAN Zhongqiang
(*Department of Information Technology,Fuzhou University of International Studies and Trade,Fuzhou* 350202,*China*)

Abstract: With the rapid development and popularization of network technology,network security has become an indispensable part of enterprises.This paper investigates and analyzes the network security of existing enterprises,and combines the requirements of enterprise network security and the functional requirements of the platform,the basic idea of modular design of B/S structure is adopted.The design realizes the network security emergency response center based on PHP and realizes the enterprise's vulnerability collection and disclosure plan.Therefore,it is of great practical significance to establish a network security emergency response center platform suitable for small and medium-sized enterprises.

Keywords:network security;vulnerability collection;disclosure plan;security response center

1 引言(Introduction)

近年来，黑客攻击越来越频繁，企业网络安全也变得极其重要。企业安全应急响应中心，一般起着对外发布企业突发安全事件处理动态，作为企业与热心用户和白帽黑客沟通反馈的平台，以及对外发布企业信息安全团队研究成果的重要作用，为互联网用户能够直接访问到企业网络安全保护体系提供途径，同时也是协调企业各部门及时响应安全事件的工作重点。实现属于中小企业的安全应急响应中心平台，有助于其完善网络安全保护体系[1]。

2 安全应急响应中心的基本含义(Basic concept of the security emergency response center)

安全应急响应中心是企业用于对外接收来自用户发现并报告的产品缺陷的站点。目前主要有两种实现方式。

2.1 漏洞报告平台

漏洞报告平台是指由独立的第三方公司或机构成立综合性的“安全应急响应中心”。国内补天平台、漏洞盒子平台，以及据此衍生的Sobug众测平台等均属于该模式。外部报告者注册对应漏洞报告平台选择对应的厂商进行报送，接着该第三方机构会发送邮件提示相关厂商确认处理。这种方法的缺陷十分明显。厂商的历史漏洞信息完全暴露给第三方机构，报告中涉及的企业内部大量敏感信息因此外泄，丧失私密性[2]。

2.2 xSRC模式

xSRC模式是指：企业自己分配工程师开发属于自身的安全应急响应中心，制定自己的漏洞收集和披露计划。目前包括Google、Microsoft、腾讯、阿里巴巴和百度等，均成立了自己的安全应急响应中心，对外收集并处理安全研究员报送的漏洞报告。使用这种模式，企业在漏洞的收集和披露过程中完全掌控了主动性，拥有良好的私密性和可定制性[3]。

3 建立安全应急响应中心的重要性和必要性(The importance and necessity of establishing the security emergency response center)

近年来黑客攻击频发，企业信息安全已经愈来愈受到重视。大型企业的业务模式多，涉及的产品也多，特别是互联网业务讲究小步快跑敏捷迭代，往往忽视了安全检查或者来不及进行细致的安全检查，同时安全系统本身是程序，也会存在各种遗漏。因为互联网业务的在线特性，使得使用互联网的人都能够接触到。相对于传统业务，被攻击面扩大，所

基金项目：2016年度国家级大学生创新创业训练计划项目(201613762012).

以更容易被善意的、恶意的或者无意的人发现漏洞。如果漏洞被利用或者在黑市交易，对企业和用户是极大危害的[3]。

纵观国内外，Google、微软、阿里巴巴、腾讯、小米、网易等知名互联网公司都已经建立各自的应急响应中心，并在推出以后取得了良好的效果，对企业安全有了巨大的协调和推动作用[1]。可以把安全应急响应中心看成一种安全能力或者产品。由一个安全应急响应中心服务商来为没有资源建设安全应急响应中心的企业整合资源，提供安全应急响应中心平台，这就是云安全应急响应中心了。

4 安全应急响应中心平台的需求分析(Requirements analysis of the security emergency response center platform)

需求分析(Requirements Analysis)是系统分析员和软件工程师在创建新的系统时，确定顾客的需要，包含基本需求、整体框架、设计目标、设计原则、系统功能、可行性分析等。需求分析是一系列活动的组成，包含需要解决问题的具体方法及确定系统实施方法必须采取的行动等。

4.1 总体需求

由于“漏洞报告平台”模式在实现过程中操作运营的规范问题，外加越来越多的鱼龙混杂的第三方企业和机构的介入，甚至出现了漏洞报告平台泄漏企业敏感信息，从而导致企业因此被攻击的案例。另一方面，出于私密性和可定制性的考虑，大多数互联网企业均倾向于选择“xSRC”模式。作为互联网企业安全防护体系中用户所能直接接触到的门面，同时也作为协调企业各部门对安全事件做出及时积极响应的工作中心，企业制定长远的战略性规划，建立安全应急响应中心能够更直观地了解到企业网络安全情况[3]。

企业对安全应急响应中心平台的总体需求是：①漏洞提交与管理；②安全公告管理；③研究博客管理；④贡献管理；⑤用户管理；⑥平台设置。

基于以上原因，本文开发安全应急响应中心平台，提供企业常用的网络安全应急响应功能，建立属于中小企业的安全应急中心平台[4]。

4.2 平台实现的原则

4.2.1 可操作

该平台主要面向中小企业。因此，在平台的操作上尽可能简单明了，没有复杂的操作，同时保证平台的稳定运行。

4.2.2 安全

该平台是通过浏览器访问互联网使用，因此系统在设计上全面考虑用户权限设置，并配备必要的网络安全设备确保平台安全[5]。

4.2.3 高效

虽然该平台的流量不多，但是通过网络来访问用户存在不确定性，因此应该具备较好的网络服务器性能并配置高性能的Web服务。

4.2.4 可扩展

虽然中小企业网络安全是大体相同的，但不同企业的需求必然有其特殊的地方，因此平台应该具有二次开发的功能，更好地进行平台升级优化。

5 安全应急响应中心平台数据库设计(Database design of the security emergency response center platform)

通过对上述平台要求的分析，给出了数据库设计、平台数据库关键的信息表，如图1所示。

图1 平台数据库关键信息表

Fig.1 Key information table of platform database

平台管理员信息表中主要字段有管理者ID、用户名、邮箱、密码、防护token、登录IP、创建时间、上次登录时间。

平台用户信息表中主要字段有用户ID、个人资料ID、用户名、真实名字、团队、邮箱、密码、防护token、用户头像、地址、个人简介等。

平台漏洞信息表中主要字段有编号、会话控制、标题、内容、状态、日期、时间、提交编号、提交者、分类、操作等。

平台公告信息表中主要字段有公告ID、标题、名称、作者、内容、发布时间。

平台博客信息表中主要字段有博客ID、标题、名称、作者、内容、发布时间。

平台奖品信息表中主要字段有奖品ID、标题、图片、价格、分类。

平台设置信息表中主要字段有设置ID、设置内容、设置数据1、设置数据2、设置数据3等。

6 安全应急响应中心平台的模块设计(Module design of the security emergency response center platform)

本平台主要由两部分组成，分别是前台模块、后台模块。前台模块结构如图2所示。

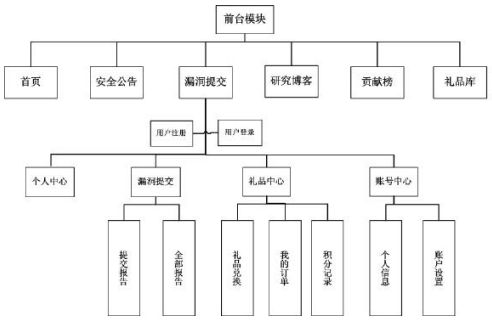

图2 前台模块结构

Fig.2 Foreground module structure

后台模块结构如图3所示。

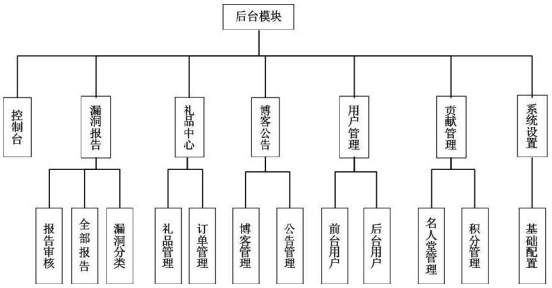

图3 后台模块结构

Fig.3 Backend module structure

7 安全应急响应中心平台的运行环境(The operating environment of the security emergency response center platform)

平台的推荐运行环境是Apache+MySQL+PHP[6](5.3及以上)，在安装和使用平台之前确保已经具备运行环境。若是Linux系统的服务器,在使用前确保为平台运行的环境目录分配了足够的读写权限[7]，保证ThinkPHP框架[8]文件正常加载或Runtime缓存目录正常生成,以上都是平台稳定运行的前提条件。

配置环境后，请将平台目录的源代码程序全部解压缩至网站目录下。

接着需要配置平台运行所需的数据库。登录到phpmyadmin，创建名为inet的数据库，确保\Application\Common\Conf\db.php中对应位置被正确配置：

```
'DB_HOST'=>'localhost', //Mysql服务器地址
'DB_NAME'=>'inet', //数据库名
'DB_USER'=>'root', //Mysql用户名
'DB_PWD'=>'flying', //Mysql密码
'DB_PORT'=>'3306', //Mysql端口
```

8 安全应急响应中心平台的实现运行(Implementation of the security emergency response center platform)

通过以上设计、实现急响应中心平台后，可进行本平台的运行。

8.1 平台的首页

当用户通过域名登录平台后，进入了安全应急响应中心平台的首页，如图4所示。

图4 安全应急响应中心平台的首页

Fig.4 The homepage of the security emergency response center platform

8.2 平台的贡献榜页面

实现用户提交漏洞之后，获得排名和积分。排名越前，实力越强。因此能帮助用户快速查看贡献，提高自己的实力。如图5所示。

图5 平台的贡献榜页面

Fig.5 Platform contribution page

8.3 平台的礼品库页面

用户通过自己的总积分，可在礼品库兑换相应等值的礼品，是平台的奖励机制，其页面如图6所示。

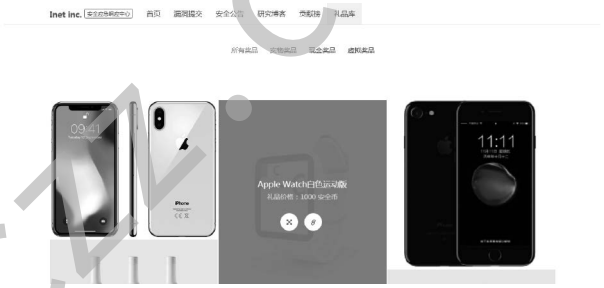

图6 平台的礼品库页面

Fig.6 The platform's gift library page

8.4 平台的后台主页面

后台管理页面提供的功能主要包括控制台、漏洞管理、礼品中心、博客公告、用户管理、贡献管理、系统设置，其页面如图7所示。

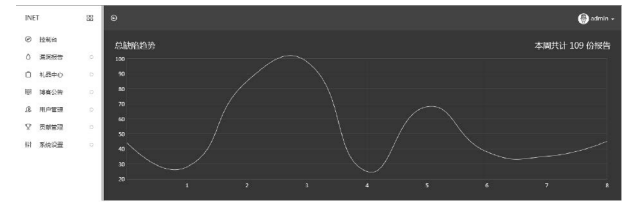

图7 平台的后台主页面

Fig.7 The backend home page of the platform

8.5 后台的特色功能页面

专门为方便企业安全事件管理设计的特色功能有外部漏洞报告导出、单个漏洞报告生成工单(导出为json格式)，其页面如图8所示。

图8 后台的特色功能页面

Fig.8 Backend feature page

9 结论(Conclusion)

本系统为中小企业的网络安全需求提供了一种捷径，使原来复杂的收集漏洞和披露计划简化，大幅度地降低了网络安全的成本，增加了积极主动地内部探测潜在的安全漏洞，减少网络安全的威胁，使企业网络系统给企业和用户带来稳定健康的服务，发挥了安全应急中心平台的预期效果。

虽然平台的实现如期获得了一些成果，但由于团队的实现时间的限制与技术水平的局限，在有些功能上还需要进一步的优化。首先，平台功能不够完善。该平台只实现了基本的相关功能，在功能上仍然有进步的空间。下一步将是根据具体的需求，进一步更新平台的功能。其次，平台代码仍需要进行简化。在平台设计中，针对共同的代码进行集成类，如数据库连接等，但仍在平台代码中存在冗余，代码在执行过程中占用较多的资源和时间，还需要做进一步的代码简化。

参考文献(References)

[1] 康玉婷,刘刚,张春柳.信息系统安全管理的问题和对策[J].电子技术与软件工程,2017(10):212-214.

[2] 白嘎力.安全应急响应中心(SRC)是如何运作的?[J].中国信息安全,2016(07):61-62.

[3] Martin Zhou.企业安全应急响应系统[DB/OL].https://github.com/martinzhou2015/SRCMS,2017-09-09.

[4] 赵粮.网络安全应急响应的新常态[J].中国信息安全,2015(07):94-97.

[5] 张睿,李欣.基于PHP技术的自助建站系统的设计与实现[J].科技创新导报,2008(04):42-43.

[6] MicheleE.Davis,JonA.Phillips.学习PHP和MySQL[M].北京:机械工业出版社,2008:179-190.

[7] Evi Nemeth Garth Snyder Trent R.Hein.Linux系统管理技术手册(第2版英文版)[M].北京:人民邮电出版社,2007:9-15.

[8] 王俊芳,李隐峰,王池.基于MVC模式的ThinkPHP框架研究[J].电子科技,2014,27(04):151-153;158.

作者简介：

游林飞(1994-)，男，本科生.研究领域：软件开发，信息系统.

林　章(1996-)，男，本科生.研究领域：网络安全.

岳凌锋(1996-)，男，本科生.研究领域：信息系统.

鲍忠秀(1995-)，男，本科生.研究领域：数据挖掘.

潘钟强(1996-)，男，本科生.研究领域：数据分析与处理.

(上接第27页)

分功能，如图2所示。

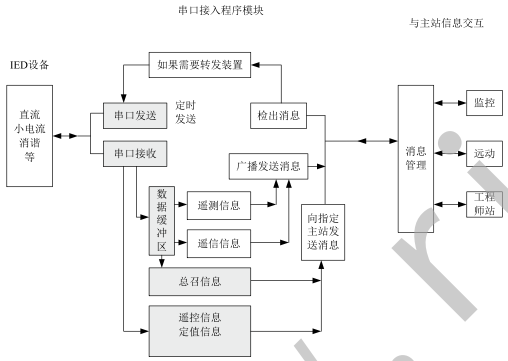

图2 串口设备接入流程图

Fig.2 Flowchart for access of serial devices

对常用的串口规约来说，只需要对黄色标注部分的模块需要修改。在主循环中定时发送串口问询命令，根据接收数据进行各种处理。需要修改的部分主要在串口数据的发送和接收处理部分。

对于问答式规约，定时下发问询命令，然后开始检查串口是否有接收到数据。如果接收到数据，判断数据格式是否正确，如果正确则解析，按遥测和遥信处理。如果未接收到数据或接收数据不正确则返回。同时增加错误计数，用于判断通讯中断。

4 结论(Conclusion)

本文提出了一种可广泛适用于电力供配电环境下不同类型IED通信接入及转出的通用型通信管理装置的软硬件设计方案。本技术成果具有很强的应用灵活性，在不同的应用场景下，可承担不同类型的设备角色，如变电站的远动通信装置、站内的保护信息管理机装置、前置单元装置、通信总控单元装置等。随着智能电网的建设重点向配用电端侧重的趋势，越来越多的配用电设备具有通信接入、互联互通的需求，本技术成果将在这些领域发挥巨大作用。

参考文献(References)

[1] 王平,叶福兰,陈章斌.嵌入式远程控制系统的设计与实现[J].软件工程,2016,19(3):55-57.

[2] 陈杰,杜伟春,王振岳,等.基于嵌入式技术的工业通信管理机的开发及应用[J].电力系统保护与控制,2010,38(11):113-117.

[3] 刘姜涛,邓其军,聂明媚,等.基于ARM的智能配电房通信管理机设计[J].自动化与仪表,2014(01):34-37.

[4] 陈雄.配电自动化终端中通信管理机的设计与实现［D］.合肥:合肥工业大学,2010:14-18.

[5] 丁俊杰.地铁变电所自动化系统通信管理机的研制［D］.成都:西南交通大学,2016:12-16.

[6] 谭方勇,王昂,刘子宁.基于ZigBee与MQTT的物联网网关通信框架的设计与实现[J].软件工程,2017,20(4):43-45.

作者简介：

魏　勇(1973-)，男，硕士生.研究领域：电力系统自动化监控软件开发.

史宏光(1976-)，男，硕士.研究领域：嵌入式系统软硬件驱动软件开发.

刘　星(1972-)，男，硕士，高级工程师.研究领域：电力自动装置嵌入式系统开发.

李俊刚(1981-)，男，博士，高级工程师.研究领域：电力自动装置嵌入式系统开发.

张　义(1984-)，男，本科，工程师.研究领域：电力自动装置嵌入式系统开发.