计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(12):232−237 [doi: 10.15888/j.cnki.csa.007204]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

高校自建邮件系统的账户安全管理优化研究①

王露阳, 罗国富

(南京农业大学 图书与信息中心, 南京 210095)

摘　要: 电子邮件安全问题中, 账户被盗用是比较常见且突出的问题. 文章针对南京农业大学自建邮件系统的账户安全管理进行了系统的研究, 具体从邮件账户安全涉及的风险、原因、对策等方面展开分析与讨论. 最后, 文中给出整体优化方案, 着重关注邮箱账户被盗事件的发现与处理, 提出一种基于自动化脚本进行日志分析的账户状态监控方法. 实践证明, 整体优化方案的实施, 显著提高了被盗事件的发现率和处理效率, 账户信息失窃和外发垃圾邮件的情况有了较大改善, 同时节约了人力, 提升了用户体验, 为高校自建邮件系统的管理提供了思路.

关键词: 自建邮件系统; 账户安全; 自动化脚本; 日志分析; 管理优化

引用格式: 王露阳,罗国富.高校自建邮件系统的账户安全管理优化研究.计算机系统应用,2019,28(12):232–237. http://www.c-s-a.org.cn/1003-3254/7204.html

Optimization of Account Security Management of Campus Self-Built E-Mail System

WANG Lu-Yang, LUO Guo-Fu

(Information and Data Center, Nanjing Agricultural University, Nanjing 210095, China)

Abstract: As a popular data carrier, E-mail is an important tool in campus daily work and study, and account stolen issues are typical threats to the E-mail security. Firstly, a systematic study on the optimal security management of Nanjing Agricultural University self-built E-mail system is carried out in this study, then potential risks, courses, and strategies are discussed. Finally, the comprehensive optimization scheme is given, especially on the discovery and handling of account stolen issues, and a novel account status monitoring method based on automated scripts is proposed in this study. Implementation indicates that the proposed scheme significantly increases both the discovery rate and handling efficiency of account stolen issues, particularly stolen cases and spam mails from domain users are explicitly reduced, meanwhile, the manpower of management is saved and the user experience is improved. It also has a certain reference value in college E-mail system management applications.

Key words: self-built mail system; account security; automated script; log analysis; management optimization

电子邮件作为一项重要的信息载体, 是高校师生进行教学互动、学术交流等的重要途径. 随着电子邮件服务应用的日益广泛和数据价值的增加, 电子邮件账户和数据的安全管理成效, 已成为体现电子邮件服务质量的重要方面. 目前大部分高校都有属于自己高校的自建邮件系统, 因其具有提高办公效率、增强数据安全、提升单位形象、应用及管理灵活、可进行个性化定制等优点[1]. 但高校自建的邮件系统在维护管理上仍存在不可忽视的问题, 其所有的安全管理都需要使用单位自行完成, 系统提供的安全保障服务有限, 同时与厂商服务的耦合度较高, 包括软件设备的升级等. 因此系统维护对运维人员得要求较高, 需投入的工作量也较大. 此外, 垃圾邮件泛滥、账户被盗频繁等问题也比较突出.

① 收稿时间: 2019-05-16; 修改时间: 2019-06-21; 采用时间: 2019-06-28; csa 在线出版时间: 2019-12-10

© 中国科学院软件研究所 http://www.c-s-a.org.cn

1 常见的电子邮件安全问题

当一封电子邮件被发送时, 信息被一个服务器接一个服务器地传递, 一直传到收件人的电子邮件服务器. 从发送到接收的过程, 可以描述为图 1[2].

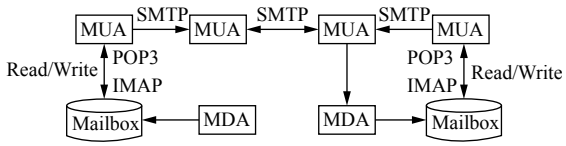

图 1 Internet 邮件传输示意图

信息先被发送到 MTA (即邮件传输代理), 经过若干 MTA 后, 最终到达收件人的 MTA. 接下来收件人的 MTA 会将电子邮件投递给 MDA (即邮件投递代理), MDA 存储邮件并等待收件人检查信箱[3]. 在这个过程中, 邮件可能受到的安全威胁大体可以总结为以下几点[4]:

1) 电子邮件数据安全: 包括电子邮件数据、账户信息、通讯录等. 不法分子通常采用口令攻击、零日漏洞攻击[5]、社会工程学等方式来获取这些数据, 获得权限.

2) 电子邮件的应用安全: 正常的电子邮件业务应保证畅通传 用的方法即建立电子邮件网关、设置电子邮件出入站抵挡电子邮件和病毒邮件的侵扰.

3) 支持电子邮件应用的服务和协议层面的安全: 确保邮件传输和收取过程的安全.

4) 电子邮件安全基础设施: 如防火墙、电子邮件网关等支撑电子邮件运行的设施[6].

针对邮件系统面临的不同维度的潜在威胁, 近年来一直有学者致力于探索和构建更安全实用的邮件系统的方法, 如 Balakrishnan S 等提出了一种基于无证书密码机制的安全邮件系统实施方案[7], 柏宗超等提出了基于 DANE 的安全邮件系统架构的研究进展[8].

在诸多安全问题中, 账户安全背后隐含的问题不仅仅是数据和隐私的泄露, 还存在账户失窃后沦为垃圾邮件中转站的副作用. 垃圾邮件是邮件系统面临的最常见也最老生常谈的问题之一, 得益于机器学习和自然语言处理相关理论与技术的迅猛发展, 其在垃圾邮件分类和检测领域的应用日渐深入, 目前也有了较多进展.学者们基于相关理论提出了如基于花朵授粉寻优算法进行特征提取的垃圾邮件检测方法[9]、基于多级神经网络的垃圾邮件过滤方法[10], 基于 word-order preserving CNN 网络模型的垃圾邮件检测方法[11]等.

本文着重针对自建邮件系统邮件数据安全中的账户安全管理展开研究, 在自建邮件系统自身具备的安全管理与反垃圾能力之外, 积极从运维与管理角度挖掘可优化的环节与辅助手段.

2 我校电子邮件安全管理的现状

我校电子邮件安全问题中, 最突出的是账户被盗问题. 当邮件帐户被不法分子盗用时, 信息和隐私即面临失窃风险, 账户还会沦为垃圾邮件中转站, 严重时则导致系统发信 IP 被反垃圾组织列黑, 发信受阻的同时, 学校形象也受损害. 因此, 完善的安全保障策略和及时捕捉并控制异常行为的能力是账户安全管理的关键.

南京农业大学采用的是 Coremail XT v5.0 自建邮箱系统, 其 webadmin 后台管理系统针对电子邮件的安全管理主要涉及以下方面[12]:

1) 用户登录行为安全防护: 多层次密码策略功能、Web 端异常 IP 登录提醒.

2) 邮件收发安全管控: 反垃圾反病毒防护、邮件监控和审核功能、邮件加密功能等.

3) 邮件数据传输安全防护: 即通过 CMTP 私有协议对邮件内容进行加密和重新编码.

4) 邮件信息管理: 采用管理员、邮件审计员和安全监察员分权操作的业务管理模式, 部门间各司其职, 邮件归档系统可真正安全的应用起来.

虽然上述安全策略相对完善, 但在运维工作的辅助决策和管理功能上, 后台管理系统仍存在以下不足:

1) webadmin 上大量统计数据无法可视化, 例如账户被异常登陆的记录、退信量排名等信息无法以直观形式呈现;

2) 各类投递日志可供查询的记录总数仅限匹配条件后的最新 500 条, 在需要时, 无法完整详尽地供管理员查阅;

3) 异常事件出现时没有告警信息, 不具备主动监控能力和自处理能力.

综合上述问题, 自建电子邮件系统的管理, 目前在依靠人工管理和干预之外, 仍缺乏高效的辅助手段来提升运维效率, 尤其在发生账户被盗、大量退信、投递延时增大等影响收发信业务的异常情形时, 无法辅助运维人员做出及时的响应. 同时随着用户数和数据量的不断增加, 单靠人工已经无法满足管理上的要求, 因此, 运维自动化作为一种高效的管理手段得到了日

© 中国科学院软件研究所 http://www.c-s-a.org.cn

渐广泛的研究和应用, 本文借鉴运维自动化的思路, 在账户安全管理的优化上做了相应的探索和实践.

3 账号安全管理优化方案的提出与实现

针对我校邮件系统存在的账户安全管理问题, 本文拟遵循一套系统的方案进行整体优化, 重点提出一种基于自动化脚本的账户状态监控方法, 旨在从以下几个方面改善账户安全问题: (1) 从预防角度降低账户被盗风险; (2) 从状态监测角度及时发现账户被盗事件并作自动处理; (3) 从事件分析角度来指导安全防护策略的完善.

3.1 账户安全管理的整体思路

(1) 密码策略和登陆行为控制

密码是确保账户安全最直观的一道防线, 具体根据以下几个角度来完善用户密码的管理:

① 密码强度: 提升密码复杂度, 收集完整的弱密码字典导入禁用列表, 定期采用弱密码检查工具[7], 进行用户排查并通知整改;

② 密码有效期: 通过设置密码有效期强制用户定期修改密码;

③ 防暴力破解策略: 暴力破解[13]的原理就是使用攻击者构建的用户名和密码字典进行枚举, 尝试是否能够登录. 理论上来说, 只要字典足够庞大, 枚举总是能够成功的. 目前来说, 暴力破解方法的适用性有位数限制, 合理的密码策略能有效地防范暴力破解. 由于暴力破解攻击通常会被写成一个脚本, 启用 IP 登陆限制和图形验证码保护一定程度可拉长攻击间隔, 降低被爆破的概率.

(2) 基于自动化脚本进行日志分析的账户状态监控方法

账户信息失窃是目前我校邮件系统存在的最典型且突出的安全问题, 通常账户被盗时存在以下典型信号:

① 用户收到大量退信, 但发信却不是该用户本人所为;

② 正常邮件延时很大, 远程队列堵塞了大量邮件;

③ 投递日志中出现大量主题及大小都一样的邮件投递记录 (正常群发邮件除外).

基于上述特征, 本文提出一种基于自动化脚本进行日志分析的账户状态监控方法, 通过提取日志文件中符合上述特征的信息, 来实现账户状态监控, 具体在 3.2 节中进行介绍.

(3) 长期未登录账号的定期自动清理

对于高校来说, 用户角色主要是教职工和学生, 因此每年都存在一定数量的学生毕业离校以及教职工离职或退休的情况, 因此, 离校人员的账户管理, 也是确保电子邮件账户安全的重要一环. 为避免这些账户因长期未登录而成为暴力破解攻击的脆弱对象, 需对其进行定期清理. 目前 webadmin 管理后台上可根据未登录截止时间进行相关用户统计, 但是最多可查询 500 条记录, 为实现相关账户的完整统计, 本文借助 coremail 邮件服务器上提供的用户管理工具/home/coremail/bin/userutil, 调用其中--get-user-attr 和--set-user-attr 命令, 通过指定 user、lastdate (用户末次登陆时间)、user_status (用户状态) 等关键字的值过滤出符合条件的所有记录. 这里 user_status 有 0、1、4 三种值, 分别代表当前帐户状态为正常、停用、锁定. 比如要过滤出末次登陆时间截至 2016-08 的账户, 可使用如下命令:

/home/coremail/bin/userutil--get-user-attr @ lastdate= |grep-v '=$'|grep-v "lastdate=2018"|grep-v "lastdate= 2017"|grep-v "lastdate=2016-12" |grep-v "lastdate=2016-11" |grep-v "lastdate=2016-10"|grep-v "lastdate=2016-09"

将过滤出的账户导入临时列表, 借助--set-user-attr 命令, 对列表中账户的 user_status 值进行重写, 即锁定或停用相关账户. 这里, 将末次登陆时间作为可配置项写入配置文件便于读取, 上述其他操作写成定时执行的 bash shell 脚本, 完成自动定期清理.

(4) online RBL check and monitoring 服务的启用

RBL (Real-time Blackhole List) 是反垃圾邮件组织提供的检查垃圾邮件发送者地址的服务, 当邮箱账户失窃时, 通常也意味着该账户极大可能将沦为垃圾邮件中转站, 此时, 邮件系统发信 IP 将面临因信誉受损而被 RBL 组织列黑的风险. 针对该问题, 本文提出利用在线的第三方 IP 监控服务, 实时监控目标 IP 被 RBL 收录的情况并设置告警通知, 帮助管理员及时发现异常, 便于尽早进行申诉、解禁等处理, 以将系统收发信受影响的程度降至最低.

(5) 事件分析及防火墙策略的完善

邮件系统后端服务器上的/home/coremail/logs/udsvr.log 文件保存了用户数据和邮件索引等信息, 为完成被盗事件的分析与跟踪, 本文基于 user 信息分析该日志中的异常认证记录来定位可疑 ip, 并在邮件服务器上利用 iptables 工具对其增加访问控制规则, 配

© 中国科学院软件研究所 http://www.c-s-a.org.cn

合 hosts.allow 和 hosts.deny 实现简单的黑白名单管理. 此外, 还对邮件服务器设置 ssh 和 telnet 方式下的 IP 连接限制, 仅限于部分工作区 IP 和堡垒机 IP 访问. 对外部人员启用堡垒机访问模式, 便于进行运维安全审计, 提高并规范内部信息安全管理水平.

3.2 基于自动化脚本进行日志分析的账户状态监控方法

Coremail 邮件系统的 DA 模块负责邮件投递、邮件到达提醒、邮件退信处理等业务, 邮件系统前端服务器上的 deliveragent.log 文件会记录当天的所有投递日志, 每个账户的投递行为和结果都被详尽地记录在日志文件中. 前文已提到账户被盗时, 大量系统退信的产生是一个显著特征, 本文从日志分析的角度出发, 结合自动化脚本手段, 对校内帐户邮件投递的退信情况进行读取与分析, 实现账户状态监控. 以日志中某一条为例:

T:1647916800(01:20:58)[S:M012cxAAAHMCnVxEXJkA][da:Info] DAH8CgC3vhpzAp1ctlKaAA--.25117S3: from=<mail.oggdoavsactufpth@email.biotechniques.com>, to=<fangwp@njau.edu.cn>,channel=dummy,size=86289, delay=0,rcpttype=to,subject=Can memories be transferred with an injection?,state=bounced,id=2, User reject

可以看出, 投递记录通过若干字段记录了信件的投递信息, 其中, state 字段描述了邮件的投递状态, 是监控方法关注的重点, 字段含义具体如表 1 所示.

表 1 state 字段的含义

state 值	含 义
sent	发送成功
bounced	退信
ignore	丢弃
defer	投递失败尝试重新投递
dump	转发
discard	丢弃

注: state=bounced 即表示邮件的投递结果为产生“退信”.

监控脚本的基本设计思想为: 每日定时且多次地以对应时刻的校内用户即时退信量排名为依据, 定义多种参考阈值 (包含可疑值和警戒值), 以排名第一的退信量与参考阈值做对比, 超出不同的阈值时将关联相应的动作, 具体遵循以下流程进行编写:

1) 以 njau.edu.cn 域内账户为维度统计 state=bounced 的投递记录形成退信量排名, 将排序后的退信量和账户名称作为键值对记入临时列表 L;

2) 利用用户管理工具/home/coremail/bin/userutil 中的--get-user-attr $x user_status 命令获得 L 中账户状态. 退信量排名仅针对状态为“正常”的用户进行, 即根据 user_status 的值筛选出队列 L 中退信量排名前 N 名的账户, 并更新队列 L 的内容, 被锁定或停用的账户不参与筛选;

3) 设 L 中退信量排名第一位的账户为 account x, 对应的退信量为 value x. 对退信量设置阈值 $T1$, $T2$, 若 $T1$<value x<$T2$, 将 L 中的账户导入.monitoring.eml 文件, 利用群发邮件工具/home/coremail/bin/batchsend 将 eml 文件发送给管理员作账户疑似被盗的提醒; 若 value x >=$T2$, 则在邮件通知管理的基础上, 同时将账户 account x 的 user_status 值置为 4, 即对其自动锁定.

上述 3 个步骤通过 bash shell 脚本实现, 并用 crontab 命令配置为定时任务, 实现定时监控. $T1$, $T2$, N 的值可自行定义, 其中, $T1$ 的值大致定义了一个退信量的可疑值, $T2$ 则定义了退信量的警戒值, N 为选取的告警账户数量. 退信量仅达可疑值时, 系统给管理员发送告警之外, 被盗事件的真正确认还须人工核实; 而退信量的警戒值通常以一个几乎可以断定被盗事件发生的较高数值来定义. 这里, 监控脚本实现时仅以较严格的阈值 ($T1$、$T2$) 和排名第一的退信量做对比进行粗估, 一旦有账户“触线”即发送告警或锁定, 通常可快速“捕获”异常度最高的账户, 而排名靠后的账户也可较快得到管理员的关注, 以此发挥主动监控和辅助决策的作用.

3.3 案例与评价

南京农业大学使用 Coremail XT v5.0 版本的邮件系统, 其服务器采用的操作系统版本为 Linux version 2.6.32-431.el6.x86_64 (mockbuild@c6b8.bsys.dev.centos.org) (gcc version 4.4.7 20120313 (Red Hat 4.4.7-4) (GCC)). 实践中 bash shell 脚本的参数取值如下: N=10, $T1$=30, $T2$=150. 用 crontab 命令将脚本配置为定时任务, crontab 可自行安装, 脚本执行频率也可按需自定义. 本文以每小时一次的频率执行脚本, 配置如图 2 框线内容所示.

当有账户退信量达到设定阈值时, 管理员即可接收到主题为“Discover”的告警邮件, 邮件正文会注明是否存在被锁账户, 异常账户和锁定提示如图 3 框线内容所示.

管理员可基于告警邮件内容在 webadmin 上查询

© 中国科学院软件研究所 http://www.c-s-a.org.cn

投递日志详情进行核实. 以用户 zfpk@njau.edu.cn 为例, 投递日志部分截图如图 4 所示, 可见该用户确实因被盗而发送了较多主题类似的垃圾邮件.

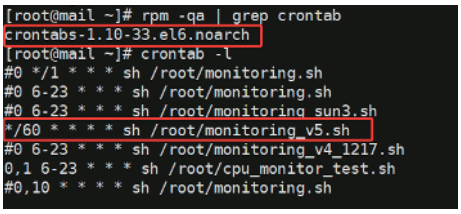

图 2 定时任务配置信息

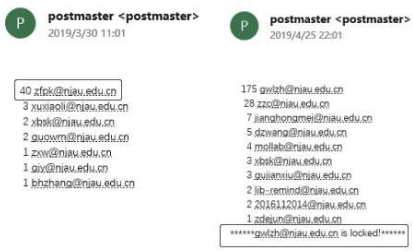

图 3 告警邮件样例

图 4 退信异常账号的投递记录

随后, 同样基于日志分析的思想, 管理员可通过“user password error”关键字及 user 信息, 从 udsvr.log 日志中定位出疑似暴力破解行为发生的问题 IP, 如图 5 框线内容所示.

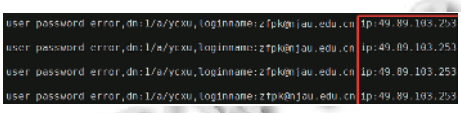

图 5 被盗账户登录认证时的错误信息

定位到问题 IP 后, 在防火墙策略中将其封停即可.

实践表明, 将自动化监控脚本引入管理后, 校内账户被盗事件如若发生, 第一时间即可得到管理员的关注, 产生较多退信的账户将被自动锁定, 实现了一定程度上的运维自动化. 配合前述多环节的管理优化, 校内弱密码账户已基本不复存在, 账户被盗事件的发生率显著降低, 由于被盗事件的发现率和处理效率的提升, 服务器发信 IP 被列黑的情况极少发生或也能及时申诉得到解禁; 而后续防火墙策略的完善, 则能较好地维护一个本地黑名单, 控制问题 IP 等对邮件系统的后续威胁, 形成类似“闭环”的管理体系. 方案整体上提升了用户体验, 将日常账户安全管理中大量的重复性工作, 如账户末次的登陆时间、退信量、登录记录等的查询与分析工作, 由过去的手工执行转为自动化操作, 有效弥补了自建邮件系统被动管理的缺陷.

4 结论

本文针对南京农业大学自建电子邮件系统的账户安全管理优化进行了系统的研究和讨论, 重点将基于日志分析的自动化监控脚本引入管理实践. 管理方法经过整体的优化调整后, 账户安全性得到提升, 账户失窃和由其引发的大量外发垃圾邮件的情况得到极大改善. 但在账户监控方法部分, 对触发告警邮件和账户自锁定的门限参数不具备自适应选取的能力, 目前需要根据实际情况手动调整, 具有一定的主观性; 同时由于该方法严格依赖于退信的产生, 因此在退信存在时延的情况下, 该方法也无法及时检出被盗账户, 这些缺陷需在后续研究工作中继续完善. 总体上, 本文提出并实践的整体优化方案, 有效弥补人工干预手段在及时性和主动性方面的欠缺, 节省人力成本并提升用户体验, 这在高校电子邮件系统的管理应用中也具有一定的参考价值和意义.

参考文献

1 罗辉琼, 李瑞维. 高校电子邮件系统的优化管理. 计算机系统应用, 2015, 24(5): 232–236.
2 王涛, 卢显良. Fast & Safe 邮件系统的设计. 计算机应用研究, 2004, 21(10): 238–240, 243. [doi: 10.3969/j.issn.1001-3695.2004.10.085]
3 徐伟平, 董秀成. 安全、可靠的电子邮件服务器系统的实现. 计算机应用, 2003, 23(5): 120–122.
4 陈建奇, 张玉清, 李学农, 等. 安全电子邮件的研究与实现. 计算机工程, 2002, 28(6): 121–122, 134. [doi: 10.3969/j.issn.1000-3428.2002.06.047]
5 杨豪璞, 邱辉, 王坤. 面向多步攻击的网络安全态势评估方法. 通信学报, 2017, 38(1): 187–198. [doi: 10.11959/j.issn.1000-436x.2017021]
6 Wu Y, Li ZJ, Luo P, *et al*. A new anti-Spam filter based on data mining and analysis of email security. Proceedings of SPIE 5098, Data Mining and Knowledge Discovery: Theory, Tools, and Technology V. Orlando, FL, USA, 2003: 147–154. [doi: 10.1117/12.484894]

© 中国科学院软件研究所 http://www.c-s-a.org.cn

7 Balakrishnan SK, Raj VPJ. Practical implementation of a secure email system using certificateless cryptography and domain name system. International Journal of Network Security, 2016, 18(1): 99–107.

8 柏宗超, 姚健康, 孔宁. 基于 DANE 的电子邮件安全研究. 计算机系统应用, 2018, 27(7): 71–77. [doi: 10.15888/j.cnki.csa.006427]

9 Rajamohana SP, Umamaheswari K, Abirami B. Adaptive binary flower pollination algorithm for feature selection in review spam detection. 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT). Coimbatore, India. 2017. 1–4.

10 Alkaht IJ, Al Khatib B. Filtering SPAM using several stages neural networks. International Review on Computers and Software, 2016, 11(2): 123.

11 Zhao SY, Xu ZW, Liu LM, *et al*. Towards accurate deceptive opinions detection based on word order-preserving CNN. Mathematical Problems in Engineering, 2018, 2018: 2410206.

12 邓楚燕. 如何确保邮件信息安全. 信息安全与技术, 2014, 5(1): 53–54.

13 尹芷仪, 江伟玉, 沈嘉荟. 一种针对暴力破解的安全口令保管库方案. 计算机应用与软件, 2017, 34(7): 319–324. [doi: 10.3969/j.issn.1000-386x.2017.07.059]

www.c-s-a.org.cn

www.c-s-a.org.cn

© 中国科学院软件研究所 http://www.c-s-a.org.cn