敏行产品安全白皮书

发布日期：2014 年 9 月

版本：V3.0

目　　录

1 前言

敏行是新的互联网时代的企业社交网络工作平台，帮助企业利用移动设备构建企业内的沟通，分享，协作的工作环境。用户不但可以利用企业内网络进行信息的发布、分享，还可以使用移动终端，随时随地的获取团队的工作数据，与同事进行实时的协作。敏行将移动互联网的最新技术带入企业，为企业提供云的平台和服务，这些都来自于敏行团队多年在互联网和企业应用领域的技术积累。

在安全方面，敏行也拥有多位从事的设计、开发、运维经验的专家，还同多家安全领域的公司达成合作协议，为企业用户提供完整的安全解决方案。本白皮书介绍了敏行团队在安全方面使用的方法和采用的策略，涵盖了组织安全、软件开发、编程安全、访问控制、人员安全、环境基础安全、运行维护管理、灾难恢复和业务连续性的七个方面的主题。在本文描述的策略以本手册的发布时间为准。随着时间的推移，本手册的细节可能会因为创新有所变化。

2 概述

应用系统的安全往往涉及非常多的环节，从网络，到系统，到开发都会涉及。敏行团队为了保证用户的业务数据安全，遵循从系统开发、系统部署、运行维护到数据备份，数据销毁都有相应的安全管控。这些安全管控包含在下列几个方面：

- 组织安全
- 软件开发和编程安全
- 访问控制
- 人员安全
- 环境基础安全
- 运行维护管理
- 灾难恢复和业务连续性

3 组织安全

敏行的安全团队由三部分构成，内部信息安全专家、第三方合作厂商、安全测试团队。

敏行团队在安全方面有专职的安全专家对系统的设计、运行进行评估，同时敏行也定期邀请一些共开的安全团体对系统的安全进行评估。为了满足用户更高的安全需求，敏行也同业界领先的安全科技公司建立良好的合作关系，将这些安全公司的一部分安全技术增强到敏行的系统中。敏行平台每次发布新版本时，测试团队都会在安全方面进行针对性的测试，并使用常用的漏洞扫瞄工具检查系统内可能存在的安全隐患。

4 系统软件开发和编程安全

敏行平台的开发尊续敏捷的开发方法，软件的设计、开发、测试、发布有严格的作业规范和质量控制标准。为了最终系统可以安全运行，敏行团队从最初的设计就排除掉那些可以快速实现，但存在安全隐患的设计方案。保证软件从最初的设计开始，就考虑到用户的安全需求。

在测试方面，敏行团队有两套测试过程：在开发中就引入自动回归测试，确保送测试部门的版本不会引入重大缺陷，导致平台的稳定性有重大的波动。测试团队会在软件最终发布前做完整的测试工作，包括对安全防护内容的测试。

在开发过程中，敏行开发团队也非常注重编程的安全性，确保在开发过程中不会引入安全漏洞。在应用开发中，常见的漏洞有：

- sql 脚本注入
- script 注入
- 跨站点攻击

这三种攻击方式都跟不良的程序代码编写有关系，敏行团队使用了 Ruby on Rails 作为后台的开发框架，Rails 本身作为一个 Web 的编程框架，提供了很多

安全编程的指引。因此在编写开发代码上，充分利用框架自身的安全编程设计，减少程序员因为个人编码的问题引入安全漏洞。

5 访问控制

为了保护敏行系统内的数据，敏行系统在设计上采用了多种措施防止未经授权的访问。

5.1 认证机制

敏行系统采用多种策略保护用户的认证安全：

- 敏行系统对用户的密码采用高强度 512 位的 Hash 进行加密处理，同时加入盐值防止对密码进行彩虹表的攻击。
- 系统还可以强制设定密码长度，复杂程度的密码策略，对非法暴力尝试密码的行为可以及时将帐户锁定，阻断帐户泄露信息。
- 系统可以进一步加强用户的认证能力，可以对接企业内部的统一认证服务，动态口令系统。另外，敏行还与第三方的安全厂商合作，提供多种软硬件的认证设备。
- 对于失效的帐户，管理员可以及时注销或者禁用该帐户，则该帐户从浏览器或移动设备均无法再登陆。

5.2 帐户授权

敏行系统在设计的最初就严格限定业务管理和业务运行的权限，管理员的权限仅限于对人员和系统的配置工作，无法更改系统内部数据，并且这些配置工作受到系统内部的审计系统监控。审计系统拥有单独权限，审计信息的提取和查询需要单独的审计帐户，这种设计可以有效的控制系统内部作案的问题。

目前系统内的访问控制如下：

	系统管理员	审计员	社区管理员	普通用户
社区	创建社区、指		注册社区用户	

	定社区管理员			
工作圈			创建工作圈、设置工作圈管理员，设置工作圈成员	创建个人工作圈，邀请成员
消息				在工作圈中发消息
文件				在工作圈上传文件
群聊				创建群聊，发送群聊消息，离开群聊

在访问控制矩阵中显示，敏行内的业务人员自己设置权限组，自己控制组内的访问权限。管理人员无法接触到工作圈和群聊内的数据。

5.3 审计

敏行系统提供完善的审计机制，管理员对系统内的权限变更和敏感信息的提取都会被记录到审计日志中，敏行系统设置了分离的审计帐户，只有审计帐户可以对审计信息进行查看和提取内容。这样设计有效防范管理员从内部进行违规的提权操作，并对系统的修改形成防抵赖机制。审计日志的信息可以与企业内的安全扫瞄和入侵监测的系统对接，及时发现帐户中的异常活动。

6 人员安全

在入职前，敏行团队会严格考察员工各方面的能力，包括责任心、工作技能、敬业态度和社会背景，以确定该人员能符合公司的行为准则、保密规定、商业道德信、信息安全准则。

在入职后，所有的员工必须签署保密协议，确认收到并遵守安全政策和保密要求，而在这些安全政策和保密要求中关于客户信息和数据的机密性要求将在每一位新员工入职培训过程中被重点强调。

除去针对新员工信息安全课程的培训，公司定期会邀请其他安全厂商的技术专家来公司进行技术交流，帮助员工了解最新的安全趋势，增强员工的安全意识。同时，公司经常贯彻企业内部的价值观，培养员工正确的商业道德观。

另外，敏行内部保留有匿名监督机制，任何违反安全政策和商业道德的事情都可以通过这个渠道进行反馈。

7 环境基础安全

为了提高敏行平台被设计在虚拟化的环境中运行，为了保证自身系统的安全可靠，敏行使用了下列最新的软件产品来提供运行服务。

操作系统 Debain Linux 6.0.10 版本
Web 服务器 Nginx 1.4.7
数据库 MariaDB 5.5.37
Redis 2.6.16
Memcached 1.4.5
Rails 3.2.19

敏行平台保证在发布给用户的各个软件服务都是最新的版本，不包含软件的漏洞，并且保证，后续都可以升级到最新的版本。

运行敏行平台的操作系统为 Debain Linux 6.0.10，系统为了安全运行已经做了安全加固

- 系统安装了最新的安全补丁
- 系统的 root 帐户已经被禁用，不允许登陆系统
- 系统进程都要求以非 root 用户身份进行

- 系统默认的网络防火墙都开启，默认屏蔽外部不安全的访问请求
- 用户存储的文件以加密的方式在系统内存储

为了保持用户数据在传送过程中的安全，敏行平台默认开启了全站的 HTTPS 的加密，在推送服务器上也开启了 SSL 的加密，为了防范中间人的 SSL 攻击，敏行开启了证书的校验。

发放给客户的移动端代码，都经过了数字签名处理，并增加了防逆向工程的保护，防止黑客利用客户端取得的信息对系统进行攻击。同时在客户端保存的数据，敏行都开启了加密策略，利用客户设定的手势密码加密客户的个人数据。客户端丢失之后，通过从服务器注销设备，还会执行客户机的数据擦除工作。

8 运行维护管理

敏行平台最初就将平台设计在虚拟化平台中运行，未来可以充分利用私有云或者共有云的环境进行快速扩展。因此，敏行团队非常重视在云环境下的系统安全。

敏行的运维团队会及时跟踪使用的软件的最新安全事件，当发生重大安全漏洞时，敏行团队会及时将漏洞信息和修补办法提交给客户，并在 24 小时内协助客户完成软件的修补工作。

系统在运行部署时，对会进行对各个软件进行安全配置，除去无用的帐户，关闭无用的权限，删除掉系统中多余的软件，维护一个运行的最小权限环境。

敏行平台运行时在网络层可以增强攻击防范，为系统部署防范 DDOS 的攻击的监控服务，可以为系统减缓 DDOS 的攻击效果。系统的 API 调用可以限制每个用户发送的次数，可以有效的阻断异常帐户的攻击和试探。敏行系统运行时会产生用户访问日志和系统权限变更的审计日志，配合入侵监测系统可以及时发现用户帐户的异常行为，例如：异地登陆、异常的帐户提权、异常时段下载数据、异常流量下载等入侵行为。

9 灾难恢复和业务连续性

敏行平台为了减少由于硬件故障，自然灾害为系统带来的服务中断，在系统设计的最初就让系统支持多机器，分布式运行，并且针对系统的持续运行采用了数据的冗余和实时复制的方案。

- 系统采用文件系统快照和数据库实时复制的手段为系统数据进行备份，可以做到因为故障引起的数据丢失降低到最小范围。
- 针对单独服务器的故障，系统使用 HA 软件进行自动维护，将失效的主机转移到其他可用的主机上。
- 敏行系统在部署上还可以为客户提供地理位置的数据分布，大幅降低用户因为数据中心故障带来的数据丢失风险。
- 敏行还可以为客户提供自动化的运维部署和恢复工具，大大缩短用户升级，数据恢复的时间。

10 结论

如白皮书上述内容的阐述，敏行平台运用多种的安全措施保护用户数据的安全，为了让用户的业务安全稳定的在云的平台运行，敏行团队在安全方面还会持续的改进和创新下去。