简单易用的目标管理工具

源目标企业版安全白皮书

v1.0

目 录

1.前言

「源目标」OKR 依据 PDCA 理论，为企业提供 OKR 目标管理以及落地执行的一站式解决方案，帮助团队明确目标，量化目标，自下而上对齐目标。公开透明的目标及任务，让团队即时分享工作、集中资源、提高沟通与协作效率，并激发员工的内在动机，实现从“要我做”到“我要做”，是新时代背景下企业管理的刚需。

作为一款企业级 SAAS 产品，「源目标」 始终坚信企业数据安全是重中之重，本白皮书将会从数据安全，账号安全和运维安全几方面详细介绍「源目标」 是如何保护企业数据安全的。

2.数据安全

「源目标」 通过以下各种方式，全力保护企业数据的保密性，完整性，不会丢失以及不会被第三方应用非法爬取。

2.1 核心数据保护机制

「源目标」 对于企业的数据采用分级保护机制，敏感的、重要的数据采用加密存储方式。对于用户密码的处理，大部分软件的处理方式是只在服务端对密码进行哈希存储，「源目标」 进行了两次哈希处理，在用户密码提交到服务端

之前，在客户端首先进行一次哈希，在服务端再次进行哈希，好处是用户的密码在所有的环节中始终只是哈希值，密码并不会在网络上明文传输。

2.2 异地多机房数据备

「源目标」 对于企业数据进行了多点灾难备份，备份会分布在不同的服务器，不同的地区，不同的机房。这样可以在不可抗力产生的灾难出现时，依旧保障用户数据的安全性，并及时从备份中恢复出来。

2.3 SSL/TLS 全程加密

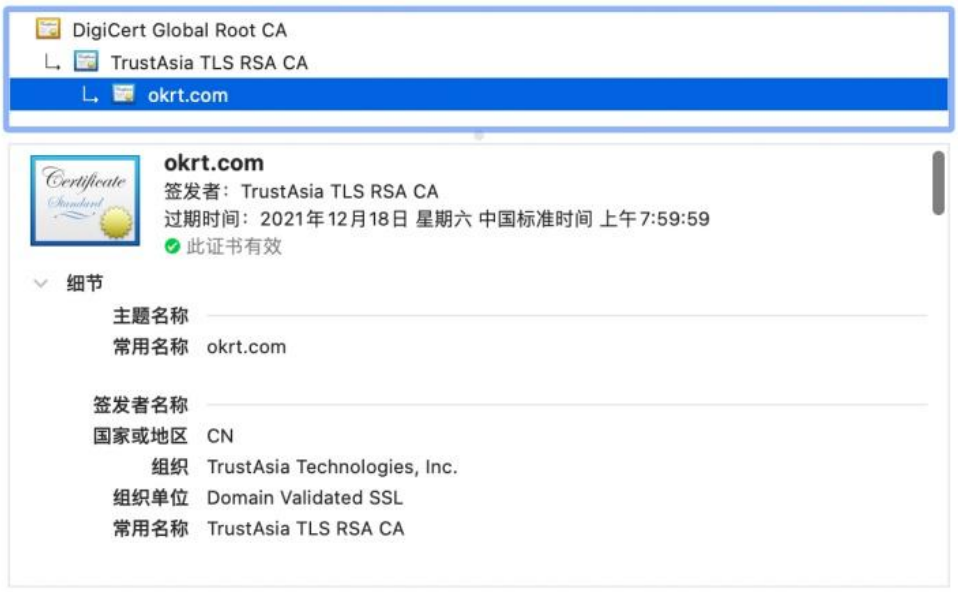
「源目标」 数据传输过程中全程使用 SSL/TLS（Secure Sockets Layer，详情请参考 RFC5246 及 RFC6176），在不采用 SSL/TLS 前数据存在传输存在以下风险：

1. 窃听风险（eavesdropping）：第三方可以获知通信内容
2. 篡改风险（tampering）：第三方可以修改通信内容
3. 冒充风险（pretending）：第三方可以冒充他人身份参与通信

而采用 SSL/TLS 后，这些风险都可以规避：

1. 所有信息都是加密传播，第三方无法窃听
2. 具有校验机制，一旦被篡改，通信双方会立刻发现
3. 配备身份证书，防止身份被冒充

「源目标」 的 SSL/TLS 证书见图 1：



见图 1

2.4 爬虫协议处理

Robots 协议（也称为爬虫协议、机器人协议等）的全称是“网络爬虫排除标准”（Robots Exclusion Protocol），网站通过 Robots 协议告诉搜索引擎哪些页面可以抓取，哪些页面不能抓取。「源目标」 中只允许搜索引擎抓取博客上由运营人员产品的文章，用户相关的数据都不允许抓取。

3.账号安全

3.1 账号加密算法

「源目标」 使用了自研的加密算法，对我们用户的密码进行加密，用户的密码信息存在 「源目标」 数据库中的将不是明文的而是通过自研算法加密过后

的数据，用户的密码信息将不会遭到泄露。

3.2 密码解锁

在 「源目标」 的 iPhone、Andorid 客户端中，登录成员可以开启登录密码或指纹解锁，在每次进入应用的时候，都需要输入正确的密码或指纹才能进入应用，如图 2 、图 3 所示

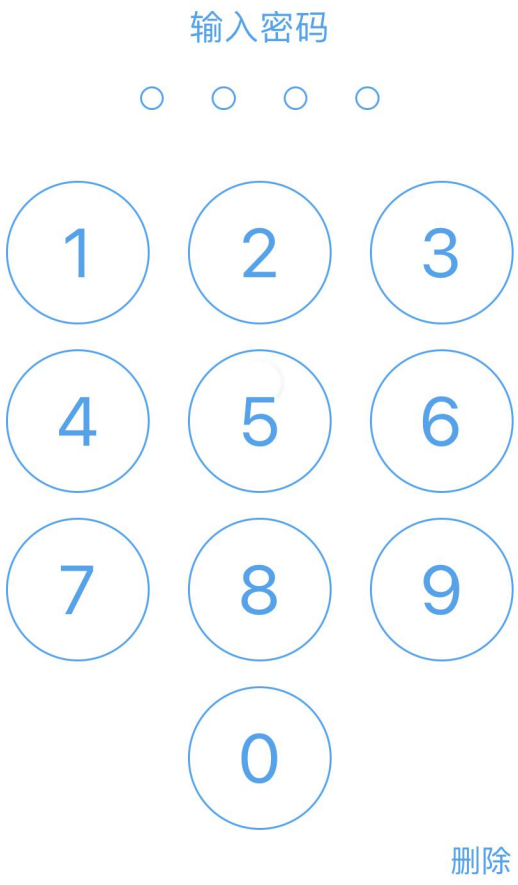


图 2

图 3

4.运维安全

「源目标」 从成立以来一直把运维安全放在最重要的位置，经过几年的改进和完善，在运维管理上已经总结出了一套切实可行的运维流程以及应急灾难处理机制。

4.1 服务器登录授

「源目标」 所有生产环境服务器都采用密钥对登录，无法使用密码登录，密钥对采用公有密钥密码术加密和解密登录信息(基于 2048-bit SSH-2RSA)，只有用户密钥对文件.pem 的人员才可以连接服务器。这种登录授权方式，使得恶意攻击无法通过猜测服务器的用户名和密码来连接服务器。

4.2 分级运维制度

所有能够接触到生产环境服务器的人员，都进行了严格的分级，对于数据中心只有极少数的人员得到授权时才可以访问。「源目标」 团队在运维管理上提出了“结对运维”的制度，只要操作生产环境服务器，就需要至少两人同时在场，同时做好每一次操作生产环境服务器的日志。

4.3 网络访问控制

所有生产环境服务器按照逻辑分组之间，使用安全组（防火墙）进行隔离，每个安全组之间的互访都定义了严格的流入和流出规则。所有生产环境服务器都无法通过外部网络直接访问。

4.4 应急制度

「源目标」 内部有一支应急处理小组，在遇到问题的时候，我们的应急处理小组将会立刻响应并处理。