Proposal for Mitigating Malicious Database Deletion

工程师 Proposal

作为企业工程师，本提案将侧重于技术解决方案，运用技术让公司财政数据库平稳运行，规避风险。基于公司数据量及经费预算，本提案针对恶意删库行为，设置 4 线 3 库解决方案。

一、物理安全防线

以目前公司数据量，可以将数据库服务器设置在 10 平米的封闭机房内。在做好控温防雷防受潮静电粉尘以外，可以考虑如下配置：

以下系统可以很好地防止攻击人员接触数据库。

P0 设置门禁系统，控制物理访问，记录进出人员。5000 元

P0 配置 24 小时 CCTV 与报警系统，录像修改权在 CTO 中。3000-5000 元

以下措施将在前两套系统被突破后对数据库进行物理防护。

P2 购置防爆机柜，隐蔽通信线缆；配备气体消防系统，及时扑灭恶意纵火。6000 元

P1 为服务器及各安全系统配置 UPS 电源。6000-10000 元

二、网络安全防线

以下措施成本低效益高，可以有效阻止攻击人员获得攻击入口。

P0 配置防火墙，数据库访问仅限公司内网，外网连接需配置 VPN；禁用多余服务。3000 元

P0 做好账号控制，对部分人员发放堡垒机账号及密码；及时清除带有隐患的账号；控制账号权限，在网络层禁止普通账号发出删除数据库及系统等危险命令；控制账号会话时间。

以下系统需要一定时间和成本用于建设与完善，可用于防御网络攻击。

P4 配置 IDS、IPS 入侵检测与防御系统，实时侦测、中断、调整、隔离不正常或具有伤害性的行为如 DDoS 攻击、SQL 注入、XSS 攻击并报警。**25 万元**

三、主机安全防线

P0 做好访问控制，建设堡垒机；堡垒机上禁用 rm-rf 等删除命令；用户只能执行相应的封装方法访问与修改数据库。执行高危命令可触发阻断、二次审批等操作。访问全程的传输加密。

P0 进行身份鉴别，双因素认证核实用户身份。超级用户设置为公司老板。

P1 做好资源监视，检测主机任务、处理器是否正常，设置心跳监听模块；

四、数据库安全防线

P0 使用 Revoke 语句撤销用户对删库删表的权限。

P0 事务跟踪，所有对数据库的修改都将被记录，方便后续追踪与回滚。

P2 使用 Trigger 检测更新或删除数据的合法性。对重要数据库表格设置敏感标记。

数据库备份策略

P0 做好备份。定期将数据备份至另一个数据库，该数据库平时不可直接访问，应对容灾。

P1 购买配置云服务器，将数据加密上云作异地备份，做公私混合云，是目前小企业很好的备份数据库的选择。一个安全且高性能的云数据库一年成本仅在 2000 到 7000 元。

P4 异地多活，将数据同时存在另一个机房中，平时可同时访问，修改时将进行同步。

数据库物理安全建设参考：广州莱安智能化系统开发有限公司 东莞英视特电子有限公司

网络、主机安全建设参考：《网上银行系统信息安全通用规范》《银行信息安全技术与管理体系》

CTO Proposal

做为企业首席技术官，在技术提案之外，本提案将侧重公司长期发展对商业数据的保护需求，从团队和战略的层面让公司财政数据库不丢失不泄露。

1、人是企业信息安全中最重要的一环。想防止删库跑路的根源办法，就是把员工关怀放在最先。同时，培养员工的安全意识，熟练掌握数据库操作，减少误删除可能性。另外，向员工普及删库跑路的法律后果，讲解刑法【破坏计算机信息系统罪】和删库跑路案件如【（2019）浙 0122 刑初 143 号】。

2、建立完善的容灾方案和管理条例。面对数据库入侵与删库，有相应的完整流程，进行定期的容灾应急演练。制定访问数据库和进入机房的管理条例，使得对数据库的更改在条例下运行。

3、做好数据库的扩展性应对方案。虽然以目前公司的规模不需要大型的数据库。但是随着公司发展，数据迁移，方案扩大是不可避免的。为此必须在购置物理设备的时候做可扩展性的考虑，防止在数据库在防删库考虑时投入的资产无法随着数据库增大而留存。同时防止在迁移时安全性下降过大，遭到恶意删库。

4、可以考虑云服务器存储。使用高弹性、高性能的服务器，加之高安全性的秘钥，可以在低成本的前提下管理公司数据，将防删库任务交给云厂商处理。当然在此之中应调查好竞争对手等外部安全隐患。

5、备份一定要全量备份、增量备份、异地备份，做到可监控，可灰度，可回滚。可结合云存储做好备份，这样数据不会轻易丢失，就算一个数据库被删库也可做到回滚。核心数据可做更多的备份。

6、建设完备的多层安全模型，随着企业发展逐渐完成从物理层到数据层的保护。同时逐步完善 WPDRRC 模型的建设，做好预防、保护、检测、相应、恢复和反击各动作准备。

7、学习各企业数据库建设案例及教训。如商业银行数据库建设案例。而教训有最近语雀的 P0 级事故，阿里淘宝崩溃的事故等。

Reference

[1]商业银行私有云设计与实现 金磐石.戴蕾.侯铮 机械工业出版社 2016-2

[2]银行信息安全技术与管理体系 洪崎.林云山.牛新庄 机械工业出版社 2016-1

[3]法律评论||员工恶意删除企业数据库的法律责任及企业的权利救济 知乎 (zhihu.com)

[4]关于语雀 23 日故障的公告

[5] 张林. 化工企业实时数据库系统应用及安全策略[J]. 化工管理, 2023(04):72-74. DOI:10.19900/j.cnki.ISSN1008-4800.2023.04.021.

[6]广州莱安智能化系统开发有限公司 机房建设解决方案