关于数据备份的 ISMS 审核案例

魏为民

摘要：在对某证券公司进行 ISMS 第二次监督审核时发现，技术部软件开发使用 SVN 管理源代码，其备份策略要求备份频率为每日全备份、备份数据验证周期为 1 年。但其实际仅保留前一天的数据备份，存在源代码不可恢复的极大风险，不符合 GB/T22080-2016/ISO/IEC27001:2013 条款“A.12.3.1 信息备份：应按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试”的要求。该不符合项的发现令受审核方非常感激并高度重视，经反复研讨测试改进方案，最终制定了一个比较完善的解决方案。

一、案例背景

推荐机构：中国信息安全认证中心

案例类型：信息安全管理体系（ISMS）

受审核方：某证券公司

审核类型：第二次监督审核

审核依据：GB/T22080-2016/ISO/IEC27001:2013，SOA 3.0

审 核 组： 组长：魏为民，组员：常琳

二、案例发生的主要过程

受审核方技术部有 8 个小组，各小组承担不同的项目开发、管理任务，源代码版本管理工具是 Subversion，备份管理员为王某。在与

王某的交流和对备份记录的抽样过程中发现，该公司的数据备份策略要求备份频率为每日全备，备份数据验证周期为 1 年，但审核发现王某仅保留前一天的数据备份。王某解释说，一方面每次全备要占用较大的磁盘空间，另一方面，SVN 全备份中有全部的历史版本，因此只需要保留前一天的备份即可。

三、主要的审核发现、沟通过程

Subversion 有三种备份方式：完全备份、增量备份和同步版本库，常规做法是在一个备份周期内，一次完全备份其余增量备份，这样兼顾了性能和磁盘容量要求。在备份时间充裕或特殊要求情况下，每次均采用全备份也是可行的。但如果仅保留前一天的数据备份，将具有极大的风险，一种可能的情况是当系统崩溃时，恰好前一天的备份也不可用，将导致所有的源代码永久不可恢复。

针对备份管理员王某的解释意见，审核员列举了多种可能的风险情况，与王某一一分析可能发生的概率，在分析的过程中王某逐渐意识到了可能存在的巨大风险，特别是考虑到公司的核心价值有极大一部分体现在软件代码中，王某心悦诚服的确认了审核组开具的如下不符合项：

不符合项描述：SVN 源代码备份，其数据备份策略要求备份频率为每日全备份，备份数据验证周期为 1 年。但审核发现仅保留前一天数据备份。涉及到的标准条款：A.12.3.1 信息备份：应按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试。

四、受审核组织主要的改进方法及其成效

许多时候我们认为一些极小概率的事件特别是一系列极小概率的事件不可能恰好同时发生，但最近 GitLab 误删 300G 数据的事故发生时（2017.1.31），预设的 5 种不同备份方案竟全部失效，导致损失惨重（参见：http://blog.jobbole.com/110171/）。

在 2017 年 2 月 14 日，GitLab 官方对删库事故的事后分析报告出来后，审核组组长第一时间通过邮件将该报告转发给受审核方联系人，GitLab 报告中出现的一种风险情况与审核组当初的分析几乎完全一致。

受审核方联系人在 2017.2.15 回复的邮件中表示感谢：“**我部门领导非常肯定‘SVN 源代码备份’的不符合项发现，之前确实没有深入分析源代码数据备份的机制，审核发现正好为我们提个醒。谢谢您的分享，期待 2017 年您和常老师的审核。**”

随后审核组一直跟进其整改过程，了解到受审核方高度重视该问题，组织相关方召开了 3 次专门会议，联合相关供应商进行多个方案的论证，最终制定了《SVN 应用数据备份策略》、《SVN 备份步骤》等比较完善的解决方案，有效预防可能的风险。

五、扩展

关于备份，还有一个比较容易忽略的问题是对备份管理系统自身的备份，如在某交易中心审核发现，未正确设置备份管理系统自身的备份策略，每周仅一次全备和六次增备，不满足“备份系统自身的数据库应每天进行一次全备，数据直接写入专用物理磁带”的体系要求。

在这个数据暴增的科技时代，数据安全的重要性是不言而喻的，

对于企业来说，数据备份系统在 IT 系统中具有非常重要的地位，数据丢失或损坏很可能造成企业的日常运作无法正常进行，甚至会给企业带来不可估量的损失，在一定程度上决定了企业的“生死”。总之，数据备份作为保证数据安全的最后一道防线，是可以把损失降到最低的行之有效的方式。