# 基础安全落地

## 前言

大家好，这篇是系列分享第七篇。之前文章请移步个人主页。这篇来分享一下基础IT安全建设的落地实操。

## 落地准备

在进行实际的基础IT安全工作落地之前，有两方面的准备工作要做。一方面是思想准备，一方面是落地的逻辑方案准备。

### 思想准备

先说思想方面的准备。我们知道，网络安全的建设工作，不是安全部门自己能完全cover住的，安全部门发现问题，但是问题的整改，还是需要其他部门进行落地整改。不管是整体企业的网络安全建设，还是单一方面的基础IT安全建设，都是需要多部门协同配合的工作。

而多部门的协同配合，在任何项目，任何工作，任何公司，都是一件很麻烦的事情。为了解决其中的麻烦，国外最早出现了PMO这个角色，国内有些大公司也开设PMO岗位。但是对于一些中小公司，就没有专门的PMO了。

所以中小企业的安全部门，要自行去推动其他部门进行安全建设的配合与落地。

安全部门扮演了整体公司安全事务的领导者的角色，但是没有领导者的权限，也没有人去帮助安全部门推动其他部门进行协同落地。

这些事情都需要安全自己来做。

而落地这些事情，更多的是需要沟通能力、说服能力、耐心等等技术之外的能力。

基础IT安全的落地，牵涉到的其他部门角色，是所有安全事务里最少的一个了。它只牵涉到运维一种角色。

### 方案准备

另一个方面的准备，是落地的实操方案准备。

准备内容除了之前两篇文章讲的内容，还需要更细的实际落地的方法论。

即我们要知道，基础IT安全建设里边，更细节的基础IT生命周期里边的落地的工作内容有哪些。如安全部门能独立完成的部分是哪些，牵涉到其他部门的内容是哪些？生命周期的各阶段，什么部门需要做什么事？这些事，对于其他部门的价值是什么？他们为什么要配合？哪些东西是安全的底线，哪些东西是可以跟部门商量的，如何跟其他部门沟通配合，如何实操落地工作内容等等等等

## 落地实操举例

这里举例一个实操过程，欢迎大佬们指指点点。

### 应急及领导的需求调研处理

在整体企业建设方案制定的过程中，我们调研了公司层面是否需要安全应急，以及公司层面有没有什么迫切的安全需求。

安全事件应急，以及安全需求可能对应着基础IT安全这个方面。

这时候我们需要评估，这些事务是否是能够短时间内处理掉的东西。

如果是个短期能处理的东西，就先处理这个。如果是需要体系化建设才能处理，才能满足的需求事务，那么它就是一个长期的工作。那么就应该把具体的事务放到整体建设方案里。优先级调高。

### 熟悉人员

基础IT安全的落地建设，我们只需要认识运维的领导就够了。

可以请领导带着安全跟运维的领导认识一下，简单对齐一下信息。留一下联系方式，便于后期的沟通以及工作开展。

### 宣讲会

认识运维领导后，找时间把所有运维拉到一起开个会，讲一下公司要开始进行基础IT安全的建设了。

会议应该讲清楚为什么做基础IT安全，它的意义价值是什么。基础IT安全建设的方法论是什么，在基础IT生命周期的各个阶段分别牵涉的角色是什么，各阶段安全要干什么，运维要干什么。跟大家讲一下，计划里各个业务的优先级顺序是怎样的。

宣讲会的目的，是安全跟大家对齐一些信息，让大家心里有个谱，方便后续的配合协作。

### 调研梳理+校对信息

趁着已经把大家拉到一起了，可以趁机会，让大家跟安全这边，也对齐一下信息。

会议之前，安全部门自己可以使用技术手段，先梳理一下公司所有的基础IT资产。

这时候让大家校对一下基础IT信息对不对，全不全，有没有补充。

然后调研一下，各领导他们自己有没有什么需求，探讨一下基础IT优先级顺序。

优先级顺序的确定，可以以业务优先级，数据重要性，单点依赖程度，资产脆弱性，外部访问性等因素来辅助判断。

### 确定沟通协调机制

一个会议可能搞不定这些事，而且一些具体的工作事务，可能不需要每次都找领导。可以让领导们在自己部门里定一个安全的对接人，安全部门后续的会议，跟一些工作的对接，可以找这个对接人来做。

### 建设基础IT发现的能力

安全部门应该建设自己的基础IT发现的能力。

基础IT安全建设，安全部门必须要有要发现新资产的能力，这样才能实现对所有基础IT的覆盖。

能力建设可以通过管理方面，在工作流程上做一些建设，让运维在搭建新资产时及时通知安全。

也可以通过技术方面，进行一些监控建设，能实时监控，以发现资产变化。

### 具体基础IT方案的制定

在基础IT梳理完成，优先级确定好之后。

安全可以按优先级，针对具体业务的具体基础IT资产，制定细化的安全建设方案。确定其具体基础IT对应的安全建设的重点。不同基础IT资产，类型可能不同，重点等都可能不同。

### 具体方案讲解

可以跟这个基础IT的方案涉及的其他部门的工作实施人员，讲解一下这个方案。

讲好安全要做什么，技术这边的人要做什么。优先级是什么，时间预期是什么。这样方便实施人员事先了解，以进行工作安排。

### 落地执行

以服务器资产举例，单个主机的安全保护，有安全基线，HIDS，安全日志，操作日志，用户权限，应用运行权限，端口开放，访问限制，故障监控，日志审计等工作内容。

对于整体的基础IT安全，应该建设整体的安全管理与运营体系。比如整个基础IT的架构设计，比如如下系统：

统一的安全管理及运营系统，统一的基础IT资产备案系统，统一的资源及权限申请流程系统，统一的安全监控系统，统一的日志审计系统，统一的权限管理系统等等。

### 持续运营

要对基础IT安全进行持续运营，比如以上系统的运营，安全设备的运营，跟进漏洞修复等等

### 合理分配资源

基础IT安全建设要注意合理的分配资源。

在针对某类基础IT的安全建设到达一定水位后，最好将资源投入到其他类型资产中。

在整体基础IT安全建设到达一定水位后，最好将资源投入到其他方面的安全建设中去。

这样处理，能够最大发挥资源的性价比。

## 总结

基础IT安全是牵扯最少的一个安全方面

基础IT安全极度依赖自动化，人工方式会累死

注意投入产出比，灵活配置资源。

## QA

弟弟失业中，目前在上海，正在找工作。大佬们如果感觉我符合您的需求的话，欢迎联系我 VX：qinbingjie1101