ManageEngine 卓豪

PAM360

突破安全孤岛

- Ian Aitchison

身份、安全、自动化和服务管理的突破性组合如何能够提高业务生产力，以及同时改变您的安全游戏规则

近年来，IT安全行业的快速增长带来了令人振奋的创新、新概念和新厂商技术，应对IT领导者面临的日新月异的威胁形势。这种增长使IT安全成为一个成熟且资金实力雄厚的行业，为IT安全专业人员提供了一条更强的职业道路，挑战高薪。

然而，与任何其它在企业部署的IT系统一样，若将IT安全置于“功能孤岛”下，可能衍生新的风险。孤立的IT安全方法可能阻碍业务的成功，“孤岛”式的服务常常会导致延迟、断联和错位，也可能表明内部的治理政策不健康。

所以，下一级的IT安全成熟度要求更为广泛的功能集成以及有意识的消除“孤岛”。

这里我们阐述打破IT安全孤岛的三种方法：

1.将安全融入IT服务管理流程

IT服务管理（ITSM）通过任务管理将业务的目的和IT的价值结合在一起。安全信息、知识以及动作可以增强IT流程，使企业业务从IT获得价值以及安全性。这里有一些例子：

- 在可能产生风险的服务、应用或访问权限申请服务请求中，直接纳入安全审核流程；
- 将安全指导及建议作为IT知识库一部分，确保机构中的所有人都可以通过自动门户查阅；
- 与其单独发布安全门户和IT服务门户，不如将两者结合起来。在您的IT自助服务门户中发布安全新闻、培训计划和其它建议；
- 在ITSM数据中开始记录雇佣员工的安全状态标识，确保IT支持团队可以查看和了解所有用户的安全状态，如果新员工尚未完成安全培训，则可能对组织构成高的风险，IT团队应做出响应；
- 不在单独的系统中管理安全事件；扩展ITSM流程，在一个统一位置管理所有类型的安全事件

• 不在单独的系统中管理安全事件；扩展ITSM流程，在一个统一位置管理所有类型的安全事件

尽管上述所有内容都严重依赖ITSM工具，但您的安全团队在其间应发挥主导作用。这不是在撤销安全，而是将安全融入IT所做的所有工作。定位非常关键！

2.利用自动化实现更快、更主动的安全响应

一旦您的ITSM工具集开始支持管理与安全相关的工作流，无论它涉及故障、事件、请求或知识，接下来就是增加自动化。这里应当由一个明确的、良好定义的策略来自动化工作流，作为对特定操作、事件或安全流程的响应。这里以例子描述：

• 如果侦测到未知设备访问到了您的网络，应自动并立即将设备从网络移除。同时自动创建相关安全事件工单，来检查究竟是谁进行了连接以及为何连接。
• 如果员工的公司邮箱或者登录信息被发现泄露在了一个外部数据集中，自动通知这些员工并立即强制重置密码；
• 时刻确保补丁的正确性，确保它们是经过测试的。通过自动化将补丁分阶段部署到目的系统；
• 是否存在员工经常执行关闭防火墙的操作？不要仅仅自动将它重置回来，通过配置自动·的用户调查，引导用户完成调查问卷，了解他们为何需要将防火墙关闭。这可以确保网络环境的安全，同时也不会让您的员工感到沮丧；
• 是否有人需要临时特权来采取特定的动作？不必让他们等待，建立自动化的特权提升自助服务流程，在特定的时间内为他们提供相关权限，并在到期时或不需要时收回。

许多独立的安全工具都能够提供这些方法，而对于您则可专注于通过集成、自动化来实现这些功能，规避单独使用、管理独立安全工具所可能引发的风险。

3.通过更好的角色和权限管理支持更高的生产力

除了检测和应对安全威胁之外，还有一个维护安全业务的领域可以立即从集成方法中受益，即访问、特权与权限的持续管理与维护。在整个过程中，正确维护安全权限和特权访问权限至关重要。

在服务管理流程中整合入职和离职流程，以及自动化修改访问及权限，您可以确保所有身份（具有高风险、标准或特权访问）在任何时间都可以遵循易于理解、便于审计，以及自动化的安全生命周期。

自动化HR系统的角色更新，可以使您即时且自动修改角色及对应的访问权限，并自动发起ITSM工作流完成进一步的安全审批以及非自动化的操作。

总结上述思路

把这三种集成思路放在一起，您可以走的更远。

1.当新入职的IT安全管理员开始他们第一天的工作，他们可以自动获取工作所需的所有基础权限、访问和特权；
2.在第一天，IT自助服务门户也会显示给员工他们需要参与的安全培训以及需要阅读的安全文档；
3.当他们完成培训，并在任职期间充分展示出了他们的能力水平，他们就会被授予更高级别的访问权限，并收到变更的通知；
4.当他们具有更高的权限后，一旦机构出现高风险安全事件后，他们可立即收到自动化的通知，并通过自助服务门户进行报告；
5.在他们报告了安全事件后，流程及自动化可以确保需要的补丁能够及时部署，最大程度的减少风险的影响。
通过主动寻求将安全控制构建到更广泛的工作流和自动化策略中，您可以消除孤立的安全管理带来的运营效率底下以及风险，提高生产率，确保业务始终处于更好、更安全的状态。

www.manageengine.cn/privileged-access-management/

ManageEngine 卓豪

PAM360