## ****内容介绍****

本篇是系列文章的第八篇，分享一下自己对办公安全的理解。

## ****办公安全是什么****

办公安全的保护对象是公司的一切，不安全的办公行为，可能导致可能导致公司各方面的损失。比如“临时工使用公司账号发布不当言论”，“永恒之蓝大范围感染办公电脑”，“Xcodeghost病毒自动给APP安装后门”，“员工删库跑路”，“内鬼买卖客户信息”，“专利泄露”等等。

种种行为分别对应着办公网络安全，办公终端安全，办公系统安全、办公工作流安全、员工意识安全、行为安全、身份权限安全等。

办公安全聚焦于日常办公的工作流及公司员工。对日常办公的所有相关事务进行保护。

理论上任何公司都需要办公安全。

特别是高精尖高端制造业，如汽车、芯片等行业，办公安全的重要性应该是排在首位的。因为其业务不依赖互联网应用，应用安全的需求较弱。其核心价值就是自己的知识产权及对应产品。知识产权看重数据安全，但是前文，数据安全建设篇也提过，没有办公安全则数据安全无从谈起。对应产品的生产安全，应该是办公安全的一部分。

## ****办公安全需求来源与发展****

企业天然具有办公安全的需求，办公安全在企业最初期的明显体现是安全生产。

在IT化建设，互联网发展之后，企业随之产生了对员工行为管理的迫切需求，对应的出现了域控及各种上网行为管理的产品。

再然后，随着企业互联网边界的模糊，办公终端的多样化，对应出现了零信任这个办公安全的理念。

## ****办公安全理念演变****

零信任安全之前，有一个多层防御理念。多层防御理念的出现，是因为企业发现，围绕着企业网络边界的安全防御体系，一旦被突破边界，内部的网络安全防御为零。比如应用WAF，一旦WAF被绕过，其应用脆弱性一览无遗。比如网络防火墙，一旦有黑客通过社工等手段，在内网种下木马，黑客可轻易获取域控权限，成为域管理员，控制域内所有电脑。

与之对应的，出现了多层防御的理念，出现了单点登录的技术，网络多AP划分等。WAF，NIDS等产品，也随着攻防在发展。安全产品，也越来越多层次，不再都围绕着边界内卷。

但是随着远程办公、企业扩张、APT攻击发展，企业网络边界也越来越模糊，基于网络边界产生的安全措施不再符合新的态势。

零信任安全理念，正是基于企业网络边界模糊问题而产生的新一代办公安全理念。其理念有三个核心，IAM，SDP以及微隔离，借助三个核心实现“持续验证，永不信任”。企业本来对外部的信任就是零。所以零信任的革新与具体实现，表现出来就是对企业内部的变革，就是办公安全。

IAM解决的是授权验证。SDP解决的是动态边界。微隔离解决的是基础IT设施层面的最小权限访问。

## ****办公安全的建设落地****

办公安全可拆成以下7个方面进行落地。

### 办公网络安全

网络隔离划分，AD、AP、VLAN建设，SDP终端，NIDS

### 办公终端安全

EDR，DLP，软件控制等，安全培训

### 办公系统安全

应用安全，IAM，安全情报及安全态势感知，日志操作审计

### 办公流程安全

这个要详细跟进部门角色的办公流程，自行发现

### 员工安全意识

安全培训，安全演练，红蓝对抗，渗透服务

### 办公行为安全

权限控制及办公行为审批流

从办公日志中审计发现

未来或许会出现AI分析录像的产品，发现没有日志的不安全的办公行为

### 身份权限安全

IAM。

没预算的话，可以自己实现一个伪IAM。

各系统权限的申请，都建一个审批流。审批完成自动创建权限。过程中完成权限记录表。

每日使用审批流的权限记录表，跟实际系统的权限进行对比。

顺序步骤：

状态调研及评估：调研安全建设状态，评估建设完成度。

决策工作内容：结合办公安全调研结果，结合公司整体的建设方案，来决定工作内容，内容顺序，落地方案。

## ****办公安全与其他安全方面的耦合****

应用安全：xcodeghost病毒事件。

操作失误，比如误发版。

数据安全：

内鬼行为的审计及发现

基础IT设施安全：

不合理的使用，比如利用公司服务器挖矿

配置错误

权限分配管理混乱

业务安全：

职务侵占

以公谋私

贪腐

## ****总结****

办公安全跟内控内审有重合的部分。

办公安全的重要性根据企业不同有不同

办公安全产品都挺贵

办公安全可自行建设的内容也都挺复杂的，市场上的人也比较少

公司规模也决定办公安全的落地可行性

## ****QA****

VX：qinbingjie1101