## ****内容介绍****

本篇是系列文章的第六篇，分享一下自己对基础IT设施安全的理解。

## ****基础安全是什么****

基础安全的保护对象，是公司的基础IT设施，类型有IT资产或IT服务。比如资产有服务器、域名、ip等，服务有网络、数据库、云服务等。黑客可通过应用间接攻击或互联网直接攻击公司的基础IT资源或基础服务，基础IT资产受到攻击，可导致应用安全，业务安全，数据安全等多方面的安全问题，因此需要进行基础安全建设。

当基础IT中没有自建设施，完全采用的云服务，没有云主机，就连数据库、消息队列等都是使用的云服务时，那么基础安全=云原生安全。当存在云主机时，那么就是传统的基础IT安全+云安全。

## ****基础安全需求来源与演变****

自从计算机出现后，企业就对计算机的安全有需求，其对应着主机安全。

后来伴随着互联网，IP，域名，基础服务组件（MySQL）等出现，它们共同构成了IT基础设施，任何的应用系统都跑在这上面，对应的，企业也需要基础设施具备安全性。

再后来，出现了托管IDC，出现了虚拟化技术，出现了云（公有/私有），出现了K8S，是基础IT设施的技术栈及服务演化，越来越灵活，也解决了好多的企业痛点，这些方式也越来越受企业欢迎。

其对应的安全需求也逐渐出现，只是企业用了更直接的名字，比如云安全。

笔者认为，从安全角度来讲，这些都对应着基础IT设施安全，所谓主机安全，网络安全，云安全等都是基础IT设施安全的一部分。

基础安全建设中公有云及私有云的异同分别是

异：公有云存在资源过期问题，私有云不存在过期问题。公有云在硬件层没有实现隔离，私有云在硬件层面实现了隔离。私有云可在硬件层面实现安全加固，公有云硬件层面安全是统一的。公有云使用的主机是虚拟化后的主机，网络隔离为逻辑隔离，私有云主机为物理机，需自行建设虚拟化，网络隔离可实现物理隔离及逻辑隔离。

同：在技术体系及管理体系可进行的安全建设都是相同的。如监控，如HIDS，如操作审计，如权限管理。

## ****基础安全理念演变****

基础安全这个词，在业内并没有很明确的定义。各人理解都不同，导致企业招聘的JD也不同。

然后因为定义都不统一，一开始是没有针对整个基础IT设施的安全理念的。

直到K8S与云生态出现之后，科技前沿企业，抛弃了主机/云主机，所有基础IT设施直接全部采用了云服务，才有了云原生安全这个安全理念。而且云原生安全，其理念内容，与应用安全的SDL有很多的重合。

后来，零信任理念出现，提出了微隔离。微隔离才是真正对应基础安全的理念，它对应着网络安全这一块，是网络隔离划分的更细化的进阶版。

下面是笔者自己对于基础安全的理念：

基础IT设施安全，可以围绕着资产生命周期，从管理、技术、运营三个方面展开。对于一般公司来说，基础安全更多的是管理及运营上的工作，技术方面的工作较简单。下面排列一下不同IT资产，在安全技术上的内容，详细说明一下为什么。

服务器安全：越权，安全补丁，HIDS等。研究系统漏洞，对于一般公司来说，没有这个必要。

网络安全：隔离划分，AD域，零信任建设，HTTPS等。这些东西也是没门槛的，照着文档做就行了。一般公司也没必要，去自行开发一套这样的东西。

IP及域名：只有管理及运营问题，没有技术问题。渗透及扫描，实际上对应着的是应用安全及服务组件安全。

组件安全：安全使用及安全配置。一般公司也没条件去做高深的技术上的安全工作。举几个有实际漏洞的例子：

Phpstudy，xcodeghost，这两个软件，都被种过病毒，但是其发现都是企业通过日志、审计等间接发现的，并不是直接发现。因为直接发现，就涉及到破解/二进制等技术内容，不是一般公司能玩的。

Redis漏洞，这个漏洞对应的是安全使用。

Fastjson等，这种漏洞都是乙方安全研究人员发现的，一般企业根本没有这个人力去模糊测试或审计代码。

组件安全在甲方的工作内容，基本就是管理，排查，修复，运营。排查的是已出过安全通告的组件，使用的是公开脚本或弱口令爆破。而且，具备组件安全研究能力的人，其职业选择可能更喜欢在国家队、安全乙方、科技型大集团中选择。

云安全：云服务商都采用安全共担模型，云安全的基础安全是云服务商负责的，企业负责的是其安全管理及安全使用。

综上所述，基础IT设施安全中，需要的技术上的东西都比较简单，甚至都有详细的文档，直接照着做就行了。而真实的涉及安全技术的高深的东西，一般企业没有这个需求，而且人选也不会选择企业。至于SEIM，SOC，日志中心，SBOM系统，情报系统等，则更偏向于开发方向，非安全行业的开发就能实现。

## ****基础安全的建设落地****

步骤：

应急跟需求：处理应急跟公司需求

资产梳理：梳理所有的资产，评估各种类的高优先级内容。建设资产发现机制跟能力。

基础资产其本身的优先级是一样的，因为任何出现问题，都会导致业务问题。所以优先级评定可从侧面评定。根据业务优先级，数据优先级，暴露性，脆弱性等方面来间接评定优先级。

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：结合调研结果，结合公司整体的建设方案，以生命周期，以管理，技术，运营三个方面为指导思想，来决定工作内容，内容顺序，落地方案。

整体基础安全方面的建设，可以从管理，技术，运营三个方面来做。

整体公司的基础资产管理要做好，最好有统一管理。消除资产黑洞，归属的黑洞。要建设基础的发现能力。

技术体系上，基础有什么类型，它们对应的安全威胁，安全防护是怎样的，各种类型基础的安全重点分别是什么。

运营体系上，怎么统一运营，怎么自动化数据化运营。

具体到某基础资产类型，各自有其对应的内容。会另外开篇谈一下。

思路也就是围绕生命周期，管理、技术、运营三个方面，攻防两个角度。估计会放在系列文章的最后。

## ****基础安全与其他安全方面的耦合****

应用安全：

木马，网马，内存马等问题

命令执行等漏洞

应用运行权限问题

办公安全：

资产申请，资产权限，安全使用，公器私用等问题

办公网准入问题

办公终端初始化及行为动态审核问题

数据安全：

数据管理关系管理

行为审计，日志记录。

业务安全：

单点问题

高可用问题

一致性问题

## ****总结****

基础IT安全是围绕基础IT设施的

各公司通常基础IT设施架构等都是不一样的

云安全正在成为潮流趋势

基础安全定义不同，要穿透词语，去看其真实的工作内容

基础IT安全，对技术深度要求有限，对广度及体系化要求较高

落地要灵活要适配，不要本本主义

## ****QA****

弟弟失业中，目前在上海，正在找工作。各位大佬如果对我感兴趣的话欢迎加我VX：qinbingjie1101