央视网信息安全的前世与今生

黄 乐

2017-6

我们从一些尴尬的事开始

BEGIN

页面篡改不知情

页面篡改或发生未知故障感知能力有限

页面的问题总是由高层领导发现，运维人员毫不知情，尴尬的场面可想而知。

黑客入侵无感知

2012年至2016年
央视网发生了多起入侵事件

入侵事件造成部分敏感数据泄漏，并被黑客当成“肉鸡”对互联网发起攻击，也影响了央视网内部业务。

继续

漏洞永远补不完

最近一年Struts2漏洞频繁爆发

被反复爆发的Struts2漏洞折磨了整整一年，2017年3月再次爆发漏洞后的24小时内，国内某安全公司公有云拦截的攻击数量就超过6万次，其中90%来自国内。黑客利用漏洞的效率之高超乎想象。

设备升级无止境

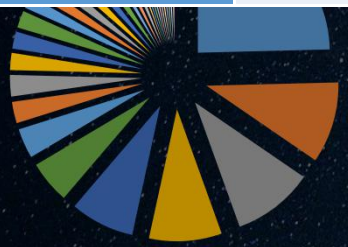
设备更新频繁，改造速度缓慢

业务严重的潮汐效应，导致安全设备频繁升级。对央视网本就不大的安全运维团队造成了很大的压力。

我们在做什么？

业务系统漏洞影响情况

控制域	控制目标	控制措施
安全方针	1	2
信息安全组织	2	11
资产管理	2	5
人力资源安全	3	9
物理和环境安全	2	13
通信和操作管理	10	32
访问控制	7	25
信息系统获取、开发和维护	6	16
信息安全事件管理	2	5
业务连续性管理	1	5
符合性	3	10
合计	39	133



- 后台弱口令漏洞
- 未授权的SQL查询执行漏洞
- 管理后台未授权访问漏洞

疑问

我们的安全工作做的是不是很差？？？

持续的入侵行为，大量的漏洞遗留，做不完的设备升级。我们做的是不是不够？

答案

其实...也做了很多...

网络安全部针对1480个域名和约20000个IP地址：

- 网络安全设备日常维护
- 漏洞挖掘
- 源码审核
- 安全管理

方法

重点业务重点保障

发布等重要系统（约500台主机）

- 漏洞检查周期减少到一周以内
- 执行更严格的安全防护方案

正常业务系统（约6000台主机）

- 漏洞检查周期为一个季度
- 执行基本符合要求的防护方案

对大量常规业务采用较为宽松的防护措施，以节约有限的资源，并将资源用于重点业务的严格管控

再看一遍

BEGIN

页面篡改不知情

黑客入侵无感知

主机安全监测

探针安全

机器学习

雾计算

异常检测

8000+主机支撑

页面篡改监控

页面比对

高效压缩

对接发布

内容过滤

第一安全需求

+

应急恢复

应急预案

快速执行

100%准确

权限管理

快速准确

继续

安全云

SDN

弹性伸缩

透明部署

底层优化

投资保护

+

安全态势感知

大数据

多维度

可视化分析

安全趋势判断

宏观态势掌控

漏洞永远补不完

漏洞全生命周期管理

漏洞评分

资产管理

综合排名

奖惩条例

基础工作

设备升级无止境

未来关注

NEXT

法律法规

等级保护2.0

网络安全法

等级保护2.0为我们提供了云环境下的安全标准，在云时代，我们至少要保证不落后于时代。

网络安全法在保护我们的同时，也给我们提出了更高的要求，合规合法的开展信息安全工作对网站至关重要。

安全态势感知平台增强

增强安全数据与安全情报的分析能力， 从更多维视角发现系统面临的安全威胁。

整合Agent数据、页面防篡改数据、应急恢复平台数据和其他来源数据，使态势感知真正具备辅助决策的能力！

未来关注

团队建设

安全工作最重要的还是人

在现有框架内最大限度的增加人力

- 安全开发
- 安全资产
- 管理&培训
- 漏洞挖掘

开放心态

改变从前闭门造车的状态

多学习，多交流，多思考，多.....

下一个开始

感谢观看!

央视网　黄乐