DBAPPSecurity 安恒信息

西湖论剑

京洲市政务云安全事件分析与建议

安恒信息——郑赸JOJO

事件现象：

气象局门户网站被入侵，并被篡改了首页...

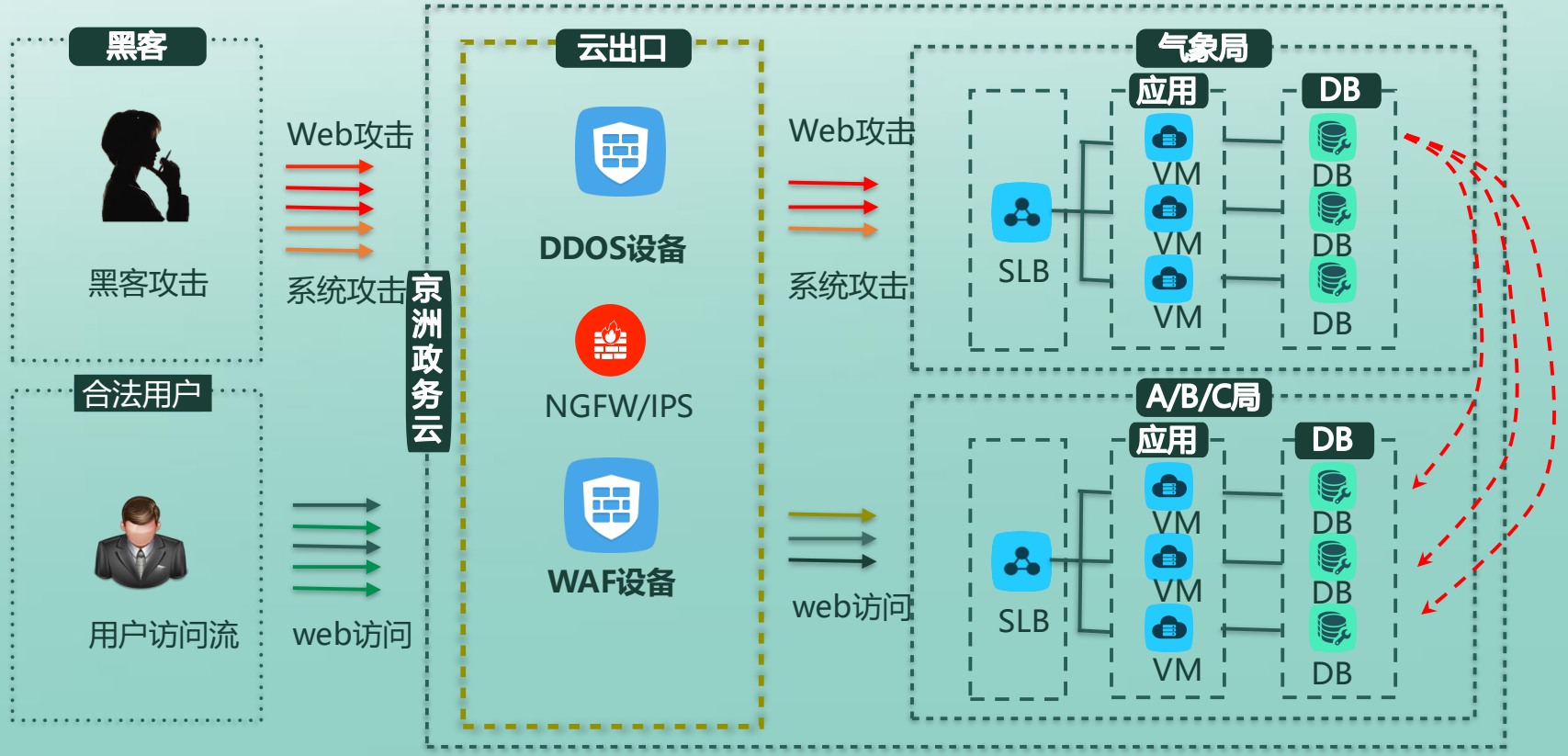
B局、C局、D局信息系统也发生数据泄露...

事件回放

1、黑客发起多种攻击

2、出口安全设备阻断了部分攻击，没挡住struts2

3、直接进入到气象局系统，入侵成功



4、通过气象局主机进行内网扫描

5、发现很多有漏洞的系统和主机

6、进一步入侵A/B/C/D局...

事件原因分析（技术）

『气象局』门户网站存在Struts S2-045漏洞...

云租户之间的东西向隔离不太完善...

多个租户的web系统、Db存在漏洞...

『云平台』安全设备策略比较简单...

事件原因分析（综合）

『云租户』信任云平台安全...

『云服务商』急于推广，轻视了安全...

『业务上云流程』缺乏安全评估...

对政务云的安全监管不足...

安全加固建议

- 理清安全责任边界，制定业务上云流程和安全规范；
- 构建全局监控能力，总览政务云安全；
- 构建三级等保安全资源池，为租户提供自服务安全能力；
- 保障云平台通过等级保护三级测评；

天池

云安全运营平台

- 云平台安全视图
- 云租户安全视图
- 用户管理
- 权限管理
- 统一认证
- 安全市场
- 订单与计费
- 大数据安全分析

云监测

- 应用监测
- 系统监测
- DB监测
- 安全事件监测
- 可用性监测
- 知识库

云防御

- VFW 抗DDOS VPN
- 防病毒 EDR
- WAF 防篡改
- 云堡垒
- 网络层
- 主机层
- 应用层
- 管理层

云审计

- DB审计
- web审计
- SOC
- 运维审计

云服务

- 渗透测试
- 安全加固
- 云上合规

API接口

监测预警

防御

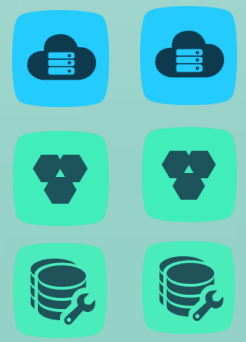
日志采集

加固

云控制平台

- 云资源调度
- 云平台管理

云资源平台



- 自助开通
- 租户隔离
- 统一管理
- 智能引流

全局感知京洲政务云安全态势

云平台自身防御动态

云租户安全威胁总览

云上合规符合性分析

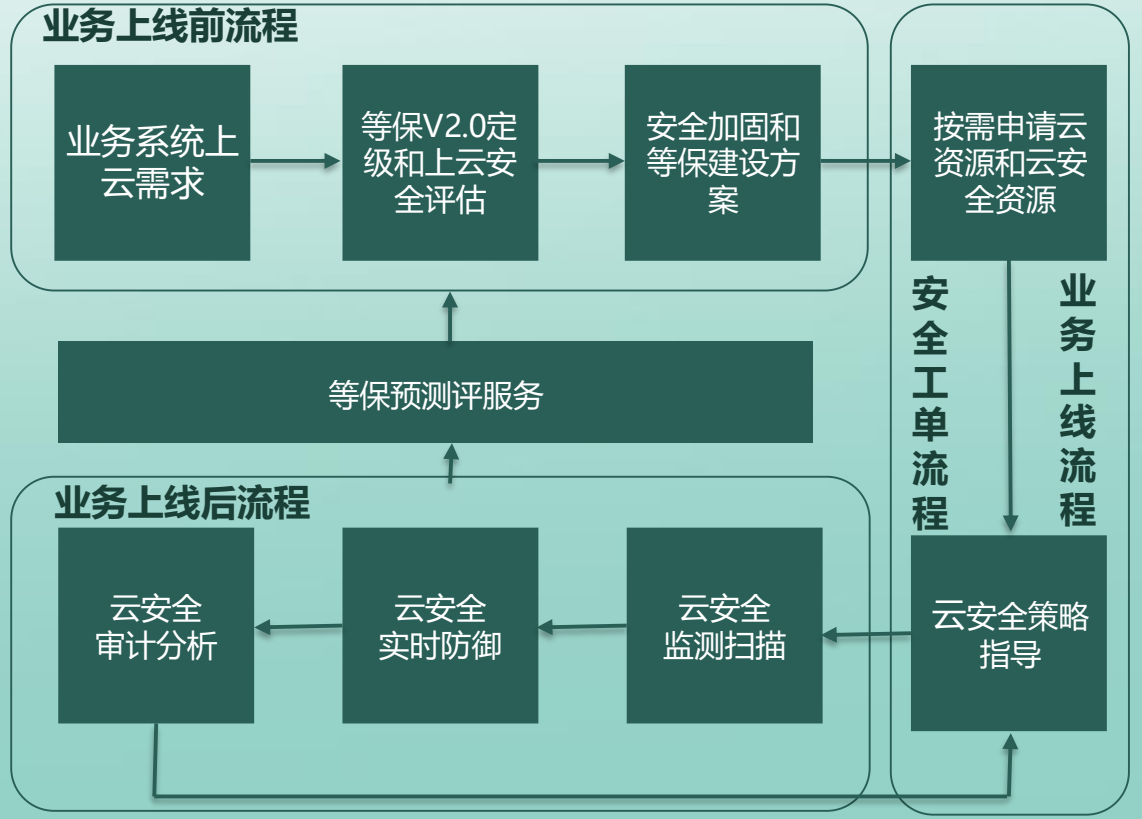
为京洲政务云构建三级等保安全资源池

云租户按需自助选用

为京洲政务云提供业务上云全生命周期服务

评估系统原有漏洞
提供安全加固建议
构建安全拓扑架构

实时扫描监测
动态防御阻断
及时审计分析



落实安全架构，定制安全策略，协助业务上线

天池已经成功对接：

阿里云

Dt Dream 数梦工场

HUAWEI

品高云 BingoCloud

openstack

DBAPP Security 安恒信息

西湖论剑

感谢您的聆听

祝您有个美好的一天

安恒官微　安恒通　E安全

电话：400-6059-110

网址：http://www.dbappsecurity.com.cn/