金融行业

1 月报
2020 年

安全月报

年度盘点 | 政策解读 | 行业研究 | 漏洞聚焦

绿盟科技金融事业部出品

年度盘点

年度盘点:2019年金融安全大事记

政策解读

等级保护2.0之安全管理中心要求和建设方案浅谈

金融科技网络信息安全监管环境分析

浅谈金融行业云计算服务安全评估的必要性与方法

恶意软件可让 ATM机按需吐出所有现金

韩国加密货币交易所遭到黑客攻击

NSFOCUS

从边界防护
到数据交互
再到安全部署
数据安全高枕无忧

IATF行为域
全面覆盖边界接入
网络基础设施
计算环境及支撑性设施域

从风险评估
到渗透测试
再到代码审计
合规绿灯一路狂飙

从现场运维，
到后台服务，
再到管理体系
业务连续顺风顺水

贴身服务 加油干

绿盟科技城商行信息安全解决方案

无缝衔接 —— 密切配合

THE EXPERT
BEHIND GIANTS
巨人背后的专家

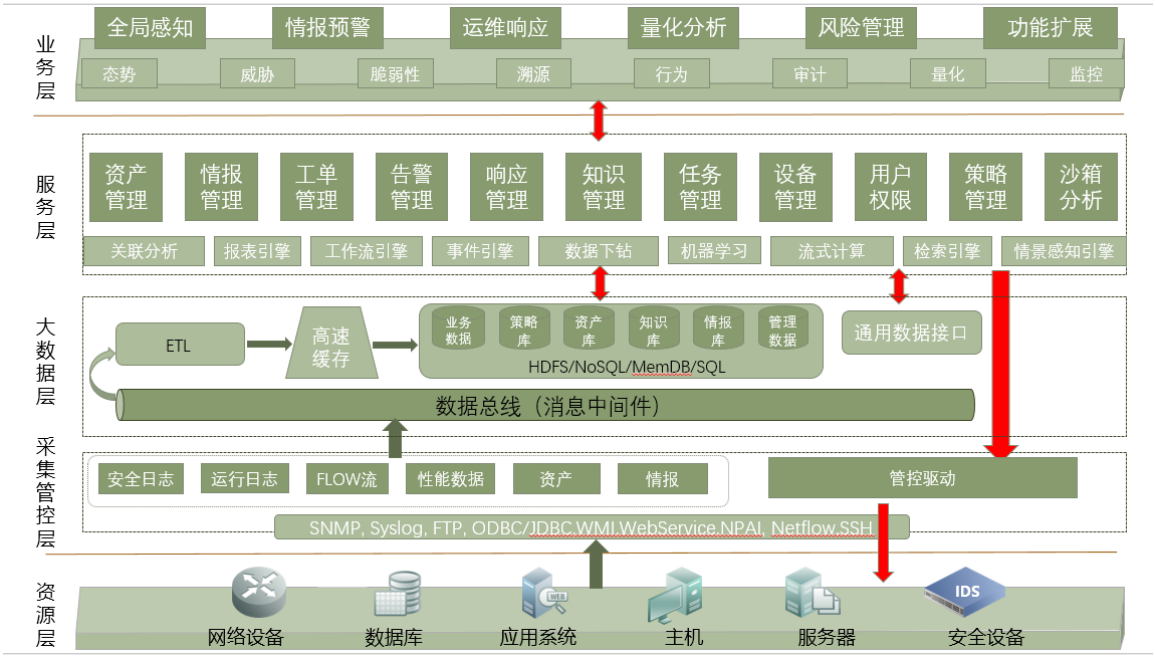
多年以来，绿盟科技致力于安全攻防的研究，为金融、政府、运营商、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS绿盟科技

本|期|看|点

P04 年度盘点：2019 年金融安全大事记

P16 多视角下的金融机构安全规划建设参考



安全月报

2020年第1期

绿盟科技金融事业部

目录 CONTENTS

年度盘点

政策解读

行业研究

漏洞聚焦

安全月报在线阅读

绿盟科技官方微信

NSFOCUS

年度盘点

年度盘点：2019 年金融安全大事记

金融事业部　张龙飞

时光荏苒，白驹过隙，随着“长征五号”运载火箭一飞冲天，中国航天开启新的征程，也为2019年画上了圆满的句号。回顾金融行业过去这一年，一方面，股市全面飘红、科创板横空出世、人民币汇率破“7”、中美贸易战、P2P加速出清、数据行业洗牌……一系列热点事件不断。另一方面，传统金融机构在金融科技方面的布局明显加速，纷纷成立金融科技公司，数字化转型与智慧银行变成各家银行战略热点。而网络漏洞、邮件勒索、DDOS攻击、信息泄露等安全事件有增无减，整个行业安全形势不容乐观。

本文结合2019年热点事件和安全态势从以下8个方面来总结金融行业面临的行业现状、监管要求、安全风险等，也给金融行业的2020年信息安全建设给出可落地的参考建议。

等保新规大升级　**IPv6**　成标配
红蓝对抗是热点　**安全竞赛**大练兵
国庆重保真实力　**数据安全**严监管
开发安全新趋势　**智能运营**领潮流

1. 等保新规大升级

2019年5月10日，网络安全等级保护制度2.0国家标准正式发布。相比等保1.0，等保2.0进行了全面的升级，保护措施进一步完善，将风险评估、安全监测、预警通报、应急演练、自主可控、供应链安全等重点措施纳入要求；监管对象也更加广泛，将重要网络基础设施、重要信息系统、云计算平台、物联网、工控系统、大数据平台、公众服务平台等全部纳入等级保护监管，并将互联网企业纳入等级保护管理；监管要求更加科学，也更加严格。

安全建议：等级保护的各个阶段有着不同的工作重点，绿盟科技将凭借着深厚的技术实力和丰富的安全服务项目经验，针对等级保护各个阶段的工作重点，在定级、备案、建设整改、等级测评、监督检查阶段，提供专业的等保咨询服务、安全防护产品、安全技术服务和安全运营服务。

推荐阅读：

【公众号2019-05-22文章】等保2.0解读“范文”来了，你跑偏了没?

【公众号2019-07-15文章】等保合规怎么破？教你一招KO!

【安全月刊2019 11月刊】等保 2.0 的变化在哪里?

2. IPv6成标配

2019年11月26号，世界上最后一个ipv4地址被用完，而金融行业IPv6的部署推进工作早已提上日程，2018年12月，人行/银保监会/证监会 联合发文 关于金融行业贯彻《推进互联网协议第六版（IPv6）规模部署行动计划》的实施意见（银发[2018]343号），针对金融行业IPv6规模部署提出了具体要求，2019年底之前要求金融服务机构门户网站支持IPv6连接访问，且具备不低于现有IPv4网络同等防护能力的安全防护体系。

安全建议：基于IPv6协议的下一代互联网的大规模部署与应用是互联网演进升级的必然趋势，是技术产业创新发展的重大契机，也是网络安全能力强化的迫切需要，绿盟科技响应国家号召，大力推进产品对IPv6协议的兼容性支持，积极协助用户构建高速率、广普及、全覆盖、智能化的下一代互联网。目前，绿盟科技全线产品已经支持IPv6环境。

推荐阅读：

【公众号2019-01-04文章】助力下一代网络建设，绿盟科技全线产品现已支持IPV6协议

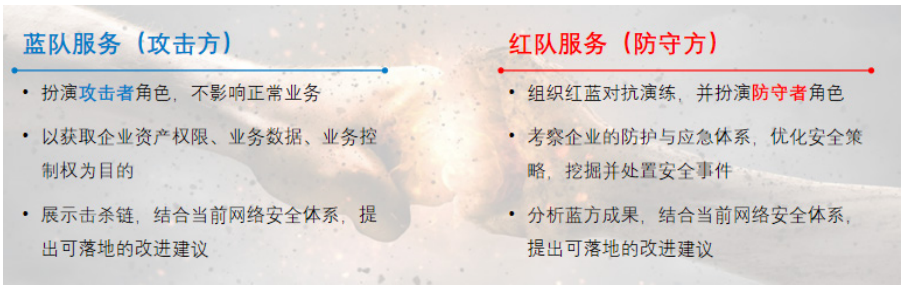
【安全月刊2019 08月刊】《IPv6 环境下的网络安全观察》报告- 上

【安全月刊2019 09月刊】《IPv6 环境下的网络安全观察》报告- 下

3. 红蓝对抗是热点

2019年，红蓝对抗这种高仿真的网络实战攻防演习成为检验重要信息系统真实安全性的有效方法。从国家层面、省市单位到企业机构都积极开展了网络实战攻防演习，以演练代检查，通过“背靠背”实战演习发现企业安全风险；以演练促整改，提升企业安全团队应急响应能力；以演练促安全，提高企业的安全防护能力。

安全建议：绿盟科技作为安全领域的领军企业，深耕专业领域，依托攻防实战对抗的技术积累，推出红蓝对抗服务方案，以实际网络和业务环境为战场，真实模拟黑客攻击行为，防守方通过企业中多部门协同作战，实践大规模攻击情况下的防护流程及运营状态，提升应急处置效率和实战能力，有效帮助企业提升整体安全防护能力。



推荐阅读：

【公众号2019-06-05文章】2019攻防演练指南

【安全月刊2019 06月刊】红蓝对抗如何开展，绿盟科技来助力

【安全月刊2019 11月刊】红蓝对抗演练落地指导方案

4. 安全竞赛大练兵

2019年，安全竞赛延续了2018年的发展势头，全国各地金融机构以及监管单位都积极参与和举办网络安全攻防比赛，以赛促学，帮助金融机构发现和培养网络安全专业人才，加强金融业网络安全人才队伍建设，从而提高金融行业网络安全防御能力和水平。

安全建议：随着我国信息化迅猛发展，信息安全问题越发凸显，但是信息安全人才持续短缺，国家也接连出台政策，鼓励信息安全人才的培养，而金融行业对信息安全人才的专业性要求更高，绿盟科技基于金融行业信息安全专业人才需求，推出定制化安全培训服务体系，可帮助企业培养信息安全专业人才，从容应对各类信息安全威胁。

推荐阅读：

【公众号2019-09-04文章】介绍下，这才是真正的CTF

【安全月刊2019 11月刊】知己知彼，百战不殆

5. 国庆重保真实力

随着综合国力与国际地位的不断提升，我国在世界舞台中的地位日益重要。奥运会、世博会、G20峰会、十九大、七十周年大庆等重大活动接连在我国举行。但每当重要时期来临，境外反动势力总是蠢蠢欲动，妄图通过网络攻击在世界人民面前抹黑我国国际形象，外部安全形势日益严峻。重要时期安全保障已经成为安全工作的重要内容。

安全建议：绿盟科技在过去的历次重大活动中，以技术支撑单位的角色帮助众多用户顺利完成了安全保障工作，通过实战的不断磨砺，培养出了一批具备丰富经验与过硬技能的安全工程师，总结出了完善的工作方法论。绿盟科技将把这

些经验在未来的重大时期安全保障工作中与用户分享，共同构筑重大时期的坚固防线。

推荐阅读：

【公众号2019-09-05文章】新长征路上细粒度重保服务指南

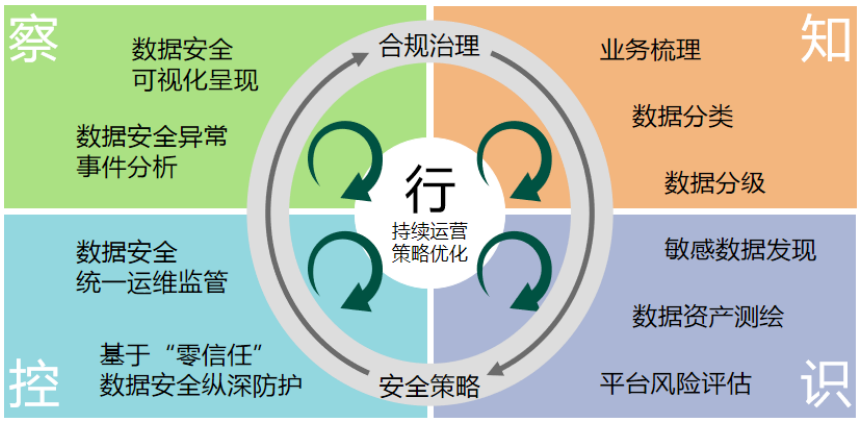
【安全月刊2019 11月刊】金融机构重要时期安全保障思路

【安全月刊2019 10月刊】山雨欲来，严阵以待

6. 数据安全严监管

在大数据时代，数据安全与隐私问题显得越来越严峻。我国也接连发布《中华人民共和国网络安全法》、《数据安全管理办法》（征求意见稿）等，并计划制定《个人信息保护法》、《数据安全法》等，而数据安全建设是一个庞大的体系化工程，对于掌握大量用户数据和隐私信息的金融行业来说，数据安全合规建设亟需尽快提上日程。

安全建议：绿盟科技基于对数据安全的研究理解推出数据安全解决方案，将数据安全治理方法“知”、“识”、“控”、“察”、“行”应用于实际项目中，利用咨询服务发现数据风险，通过产品落地实现对数据的可视化监控、风险点排除，及时预警、及时阻止非法的数据使用行为，最后对数据进行持续运营服务，让数据始终处于被监控的安全状态。



推荐阅读：

【安全月刊2019 04月刊】新品发布·绿盟科技 IDR 敏感数据发现与风险评估系统

【安全月刊2019 05月刊】新品发布.绿盟科技数据安全解决方案

【安全月刊2019 11月刊】拨开云雾见天日——数据安全治理体系

7. 开发安全新趋势

近年来，金融行业数字化转型加快进度，互联网应用系统如雨后春笋般开发上线，版本迭代也相当频繁，但层出不穷的安全漏洞成为了业务上线的“拦路虎”，因此，部分金融机构开始尝试建立覆盖信息系统全生命周期的安全管理体系，从根源梳理安全需求，建立设计安全开发基线，规范开发人员编码，加强安全测试，从而改进应用系统整体安全性。

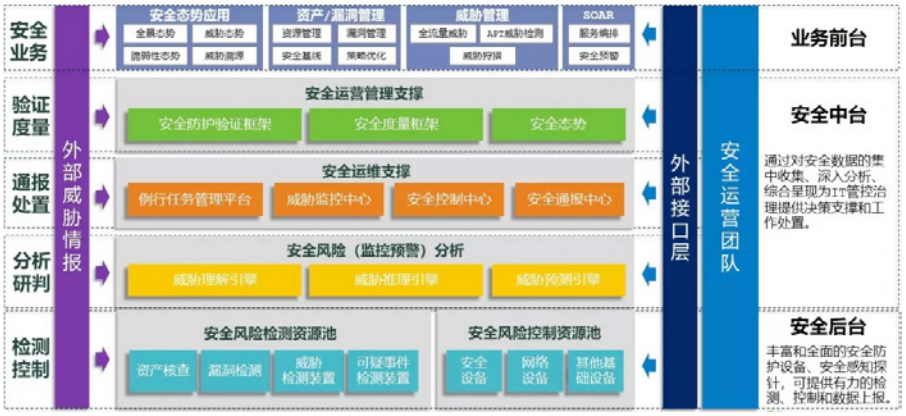
安全建议：绿盟科技应用安全开发生命周期（ADSL）以生命周期和深度防御的理念为基础，在重视威胁和脆弱性管理的基础上，改进系统的安全开发及交付过程。通过管理以及技术规范的方式，持续提升应用系统的安全质量，降低企业在软件开发中的不必要投入。

8. 智能运营领潮流

随着等保2.0时代的到来，网络安全的要求越发严格。为了应对日益严峻的安全形势，同时满足国家和行业监管要求，金融机构亟需建立一个全数据、集中管理的安全运营管理平台，做到事前预警、事中监控、事后分析，全面提升信息安全管理与防护水平。

安全建议：绿盟智能安全运营平台（iSOP）基于对金融行业安全需求的深入

理解及绿盟智慧安全2.0理念，以大数据为基础，结合威胁情报系统，通过对攻防场景的机器学习、威胁建模、场景关联分析、异常行为分析及安全编排自动化、可视化呈现等技术，实现安全态势全面监控、安全威胁实时预警、资产及漏洞全生命周期管理、安全事故紧急响应。



推荐阅读：

【公众号2019-11-20文章】从管控到运营，绿盟科技的金融行业安全防护之道

【安全月刊2019 07月刊】安全成本节约的选择

【安全月刊2019 12月刊】迈向安全运营之路的建设思考

面对日益复杂的网络安全威胁，绿盟科技将以前沿的攻防技术研究、创新的安全解决方案和全方位的安全服务满足客户的安全需求，以“智慧安全2.0”战略为指导，贯彻落实《网络安全法》及等级保护相关要求，以保障用户安全、行业安全为己任，紧跟国家网络安全发展战略蓝图，为助力构建网络安全空间治理体系，推动数字经济安全稳定高效发展，为我国金融行业网络安全和国家网络安全建设提供有力支撑。

NSFOCUS

政策解读

等级保护 2.0 之安全管理中心要求和建设方案浅谈

金融事业部　王志辉

早在2008年由公安部牵头组织编写的，国家标准化委员会发布的《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求 》及其配套政策文件和标准，标志着等级保护政策的正式实施，我们也称之为等级保护1.0时代。等保1.0在经历了多年的试点、推广、行业标准制定、落实工作后，由于由于新技术、新应用、新业务形态的大量出现，尤其是云计算、移动互联网、物联网、大数据、工业互联网、人工智能等领域快速发展，原来发布的标准已经不再适用于当前安全要求环境。从2015年开始，公安三所开始牵头逐步制定2.0标准，包括5个部分（最终发布稿）：安全通用要求、云计算安全扩展要求、移动互联安全扩展要求、物联网安全扩展要求、工业控制安全扩展要求，丰富了防护内容和要求，全面容纳了当今企事业单位的信息系统运行环境。通用要求中精简了多余或者不适用的内容，并首次强调了“一个中心，三重防护”的安全建设思路，并加入可信计算技术的使用要求。通过建设“一个中心”管理下的“安全通信网络、安全区域边界、安全计算环境”，为行业单位构建网络安全纵深防御体系。

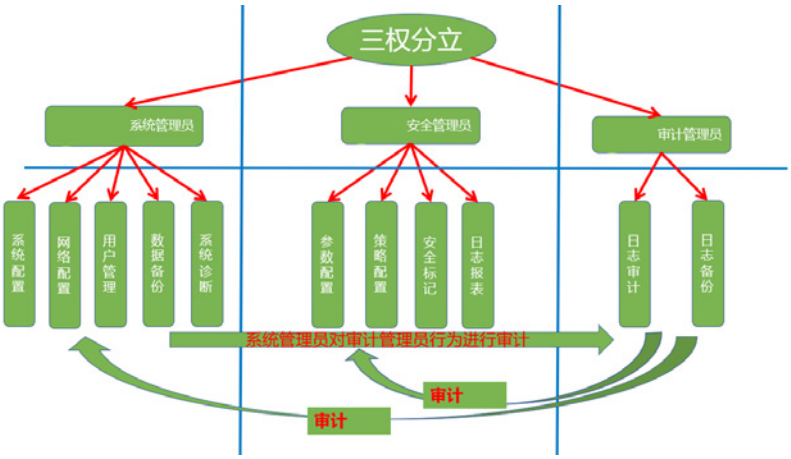
以等级保护基本要求四级为例，安全管理中心层面包含4个控制点，分别为系统管理、审计管理、安全管理、集中管控。系统管理控制点强调了系统管理员身份鉴定、权限控制、操作行为审计、系统管理员对系统的资源和运行拥有的权限和职责。审计管理控制点强调了对审计管理员进行身份鉴定、权限控制、操作行为审计、审计管理员的职责以及对审计记录的处理方式。安全管理控制点强调了对安全管理员的身份鉴定、权限控制、操作行为审计、安全管理员的职责以及配置可信验证策略。集中管控控制点强调了为安全设备在网络中单独划分带外管理区域，对网络安全设备管理需要通过安全

的网络传输方式或采用加密方式进行，建立审计日志集中存储和分析中心并满足网络安全法6个月的存放要求，对网络安全策略、病毒库、操作系统补丁进行集中监控、软件升级、策略下发，保证系统内信息资产及各种硬件设备时间唯一，对网络安全事件能够进行及时判断、告警、展示分析统计结果。

对于“一个中心”即安全管理中心所涵盖的控制可以归为两类，一个是以“三权分立”的方式对系统账户进行权限划分和操作行为审计，一个是通过集中管理平台的方式对安全设备进行集中管理和策略部署，把攻击事件可视化、对安全日志集中收集进行关联分析和分类统计、协助安全人员进行判断、提高安全事件的处理效率。

一、系统管理、审计管理、安全管理

建立“三权分立”的系统账户管理方式，默认出厂就取消超级管理员“admin”，审计管理员需要对系统管理员和安全管理员的操作进行审计，但同时审计管理员的操作也需要被系统管理员审计到，三个角色的功能没有任何交集，同时三者的行为都在被监管范围内。



二、集中管控

1. 管理区域

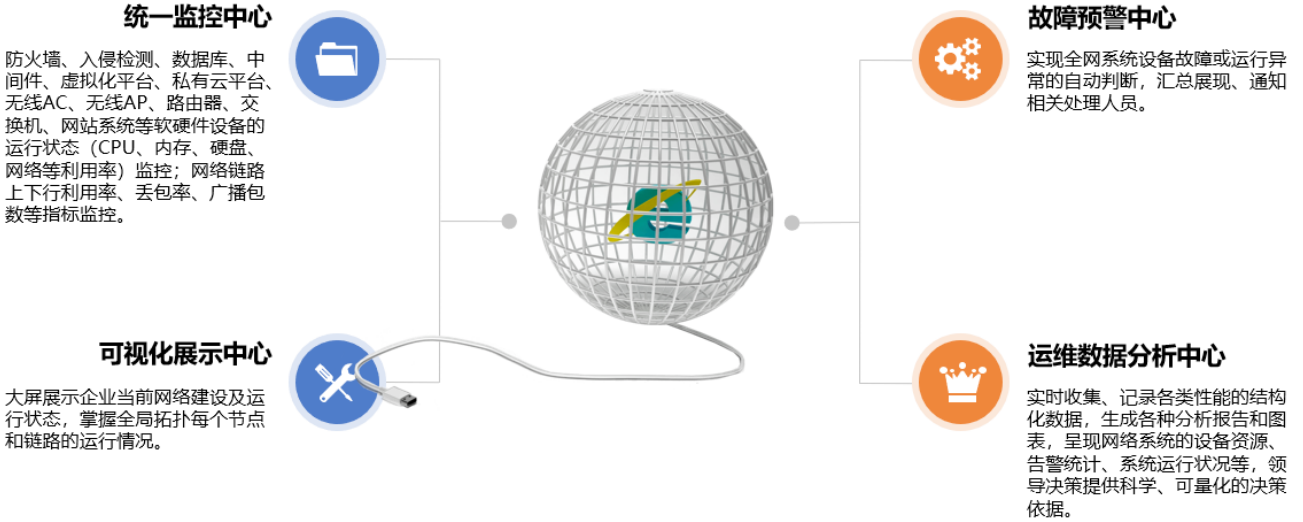
通过网络划分单独VLAN网段的方式，将网络安全设备例如入侵防护、负载均衡、网站防护、防火墙、上网行为管理、数据库审计、堡垒机等设备管理IP地址划入独立网段与其他区域网段区分开，同时也实现管理流量和业务流量分离的作用。

2. 安全传输路径

通过HTTPS协议去管理网络中的安全设备，实现加密传输数据包，防止信息泄密。是HTTP的安全版，本质上是在传输层（TCP）与应用层（HTTP）之间增加了一个SSL或TLS协议层。SSL/TLS协议提供了加解密的机制，所以它比HTTP协议更加安全。

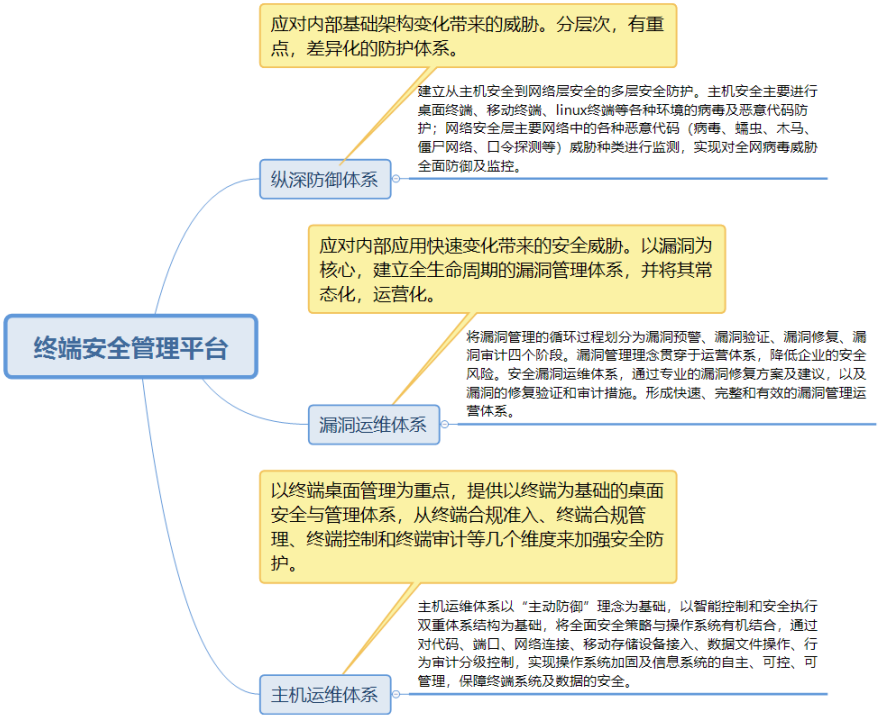
3. 状态监控

对企业信息资产的状态监控，需要以企业“业务系统资产”和“网络运维需求”为核心而建立一套综合性网络运维管理中心平台，容纳防火墙、服务器、交换机、数据库、中间件、虚拟化、web系统、机房动力环境等方方面面的设备运行信息统一采集，以业务系统拓扑结构为主线将数据关联分析从而迅速判断影响业务系统访问的故障原因。网络管理运维平台使得管理人员既可以对运维效率、质量有总体的掌控了解，也可以对运维个体进行数据分析，从而全面提高管理能力和水平，提升对运维体系全管理能力。



4. 集中管控

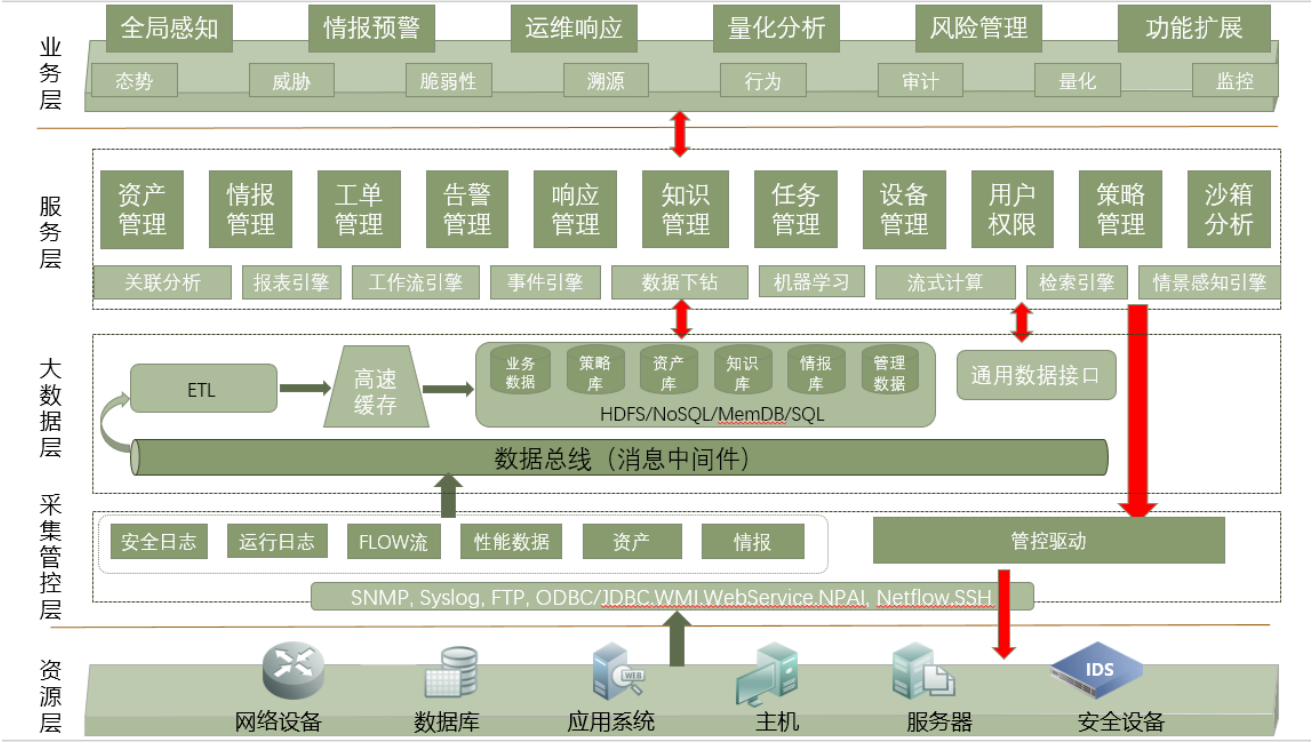
建立全面统一的终端安全管理平台，对内部PC终端、服务器、移动终端、进行全生命周期化管理，实现端到端的全面安全管理，提供恶意代码快速查杀、安全攻击实时防护、全方位桌面管理、丰富的运维支撑、灵活的漏洞补丁管理、细粒度的外设管控以及多维度的日志审计回溯等功能。同时要从异常检测、行为安全管控、安全加固、安全运维及安全事件回溯等维度实现终端整体安全防护，成为一套终端异常行为检测和防御综合管理系统。



5. 日志审计、事件预警、分析

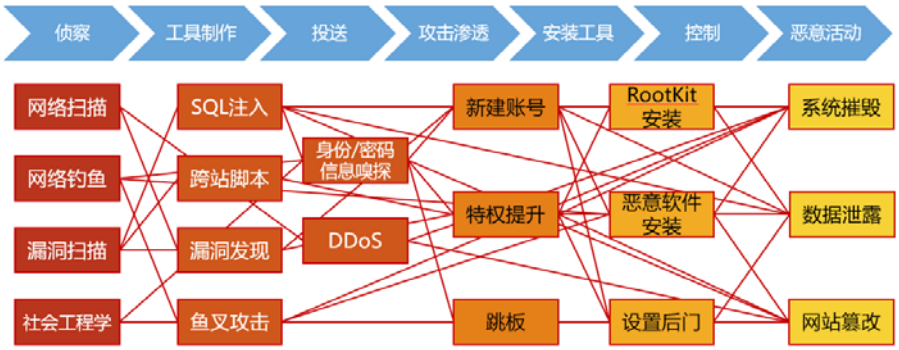
在安全运维工作中，安全运维人员面对不同类型并且部署于不同位置的安全设备，难以在全局上了解全网存在的脆弱性是如何分布的、面临的安全威胁有哪些，也难以判断第一时间应该优先对哪些脆弱性进行修补和控制，对哪些威胁进行诊断和分析。同时由于采集日志的多元性、异构性和海量性，还会包括对于网络流量的采集，因此平台所采集的数据量将是一个巨大的数字，并且涉及到今后对于数据的挖掘以及关联分析和历史查询分析。综上原因为满足等保2.0中规定的各类安全事件识别、分析、预警，需要通过安全态势感知平台进行实现。

态势感知平台（或是SOC平台）设计需要以大数据框架为基础，结合威胁情报系统，通过攻防场景模型的大数据分析及可视化展示等手段,协助客户建立和完善安全态势全面监控、安全威胁实时预警、安全事故紧急响应的能力。通过自适应的体系架构，高效地结合情境上下文分析，协助安全专家快速发现和分析安全问题，并能通过实际的运维手段实现安全闭环管理。态势感知平台建设应考虑包括6大核心：数据采集中心，情报预警中心，态势感知中心、安全分析中心，风险管理中心，IT运维中心。适用于企业海量日志管理、威胁分析、情报预警、风险管理、IT运维等多种安全运维场景。



SOC平台系统架构逻辑图

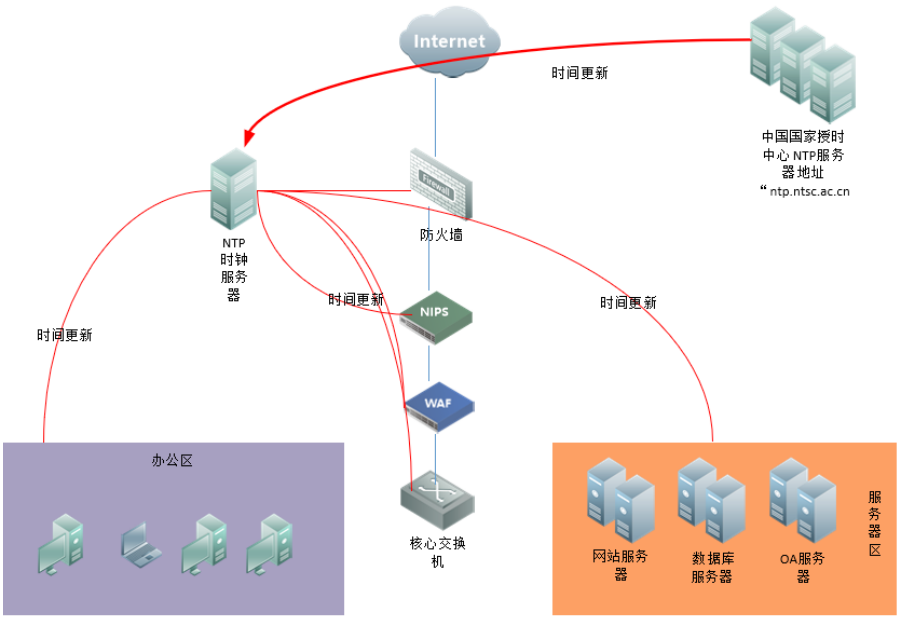
为了简化人工对设备的操作流程，提高运维人员对攻击流程的直观感受，适用新常态下威胁感知变化；需要对传统NIPS、WAF规则的划分维度做全新调整，结合完整的解决方案，彻底摆脱传统安全设备显示给客户的单一事件单一告警的无状态统计局面。通过对规则库重新按照事件的攻击链划分，结合数据处理中心对规则新分类告警的日志分析，利用智能化的势态分析模块从大数据分析的角度分阶段的（侦查、工具制作、投送、攻击渗透、安装工具、控制、恶意活动7个阶段）给客户呈现出攻击的整个过程。通过态势感知平台的数据仓库，可以对多有与该事件相关的数据进行记录，并重新构建攻击的逐步过程，安全分析人员可以清晰的了解和查询，攻击时间和位置，提权以及安装特征等，安全分析师可以快速地构建恶意攻击的概要信息，并通过链条式分析将注入路径衔接起来，识别出第一感染源头和其他被感染者，或下一步预判，使安全团队提前发现威胁，能够快速不久损害，将损失降到最低。



取证调查和威胁分析

6. 统一时间

采用NTP服务器（NTP协议用来使计算机时间同步化的一种协议），它可以使终端、服务器、网络设备、网络安全设备、业务系统等对其服务器或时钟源做同步化，它可以提供高精准度的时间校正（局域网标准间差小于1毫秒），同时内部NTP服务器还可以与互联网时间服务器进行时间校对，从而保证时间的准确性。



NSFOCUS

行业研究

金融科技网络信息安全监管环境分析

金融事业部　温福城

我国网络信息安全的立法是伴随着信息技术发展而逐步开展的，在信息技术发展初期，由于信息技术应用范围的限制，仅就特定的信息技术应用场景和行为进行原则性的约束，主要表现为在《中华人民共和国宪法》《中华人民共和国保守国家秘密法》《中华人民共和国标准法》《中华人民共和国商标法》《中华人民共和国专利法》《中华人民共和国著作权法》《中华人民共和国民法》《中华人民共和国刑法》《中华人民共和国治安管理处罚法》等法律中的部分条款和原则。针对网络信息安全和网络行为而制定的法律，主要是1994年发布的《中华人民共和国计算机信息系统安全保护条例》和2000年发布的《关于维护互联网安全的决定》。这一时期，国家层面已经注意到信息技术对国民生活的重要性，以及信息技术在应用过程中所存在的网络信息安全问题，由于缺乏广泛的应用，网络信息安全问题存在一定的技术门槛，法律条款不能逐一规范具体行为，仅在个人权利、违法行为和指导原则方面进行表述。另外，为了鼓励我国电子商务行业的发展，2004年国家发布的《中华人民共和国电子签名法》，主要目的在于认可电子商务过程中的民事行为，但也在很大程度上促进了网络信息安全的发展。

随着信息技术的发展与广泛应用，网络信息安全的问题逐渐显露，国务院及各部委局发布一些条例和规章，应时处理和规范时下热点网络信息安全问题，填补立法空隙，例如《计算机病毒防治管理办法》《互联网新闻信息服务管理规定》《电子出版物管理规定》《中国互联网络域名管理办法》等等。这一阶段，国务院及各部位局均对网络和信息安全均提出了管理要求，导致存在多头管理、管理不严、依据标准不一等问题。与此同时，国际网络空间安全环境险象环生，存在诸多不确定因素，我国网络空间安全战略提上了日程。

为进一步加强对网络空间安全的保障，规范网络信息安全的管理，2016年我国先后发布了《中华人民共和国网络安全法》《国家网络空间安全战略》，阐明了我国关于网络空间发展和安全的立场，指导网络安全工作，维护国家在网络空间的安全、安全和发展利益。

经过多年的发展，我国金融行业信息安全监管框架已经基本形成，并且具有明显的特征，一是监管主体向网信办协同各部位的“1+N”多维化转变，二是监管制度趋于严格化，三是监管内容越来越精细化，四是监管科技手段增加，监管方式也从原有事后审计调查向事中事前转变，五是由于各地区地域所处经济发展现状有所差异，地域化的监管特征也已经初步显现。

一、监管主体多维化

目前我国金融行业网络信息安全主要受网信办、公安部、银行保险监督管理委员会等部门多个维度的监督管理。

金融机构作为国家重要基础设施，国家法律对金融机构信息安全具有监管要求。《网络安全法》规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作，国务院电信主管部门、公安部门和其他有关机关依法在各自职责范围内负责网络安全保护和监督管理工作。这种“1+N”的监管体制，符合当前互联网与现实社会全面融合的特点和我国监管需要，也满足了国家对网络安全重点保护、预防为主、责任明确、严格管理的原则。

我国公安机关行使计算机网络信息安全保护监督管理工作，其对金融机构的信息安全具有管理要求。1994年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》赋予公安机关行使对计算机信息系统安全保护工作偶的监督管理职权，同时规定由公安机关牵头落实信息系统安全等级保护制度。1995年全国人大发布的《中华人民共和国人民警察法》，明确了公安机关具有监督管理计算机信息系统的安全的职责。1997年执行的《计算机信息网络国际联网安全保护管理办法》将公安机关的监督职权扩大到信息网络国际联网领域。2017年实施的《网络安全法》强调在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护，明确关键信息基础设施的运营者负有更多的安全保护义务，并配以国家安全审查、重要数据强制本地存储等法律措施，确保关键信息基础设施的运行安全。这不但强化了公安机关在网络信息安全监督管理方面的主导地位，同时将网络安全等级保护制度作为国家监管、保护国家重要基础设施网络安全的有力抓手。

中国人民银行是我国金融领域的行政主管单位，其对金融机构的信息安全管理也有直接管辖要求。第一，在全国金融风险管理方面，央行需要对金融机构、金融资金流向的信息安全全面掌握，例如《关于进一步加强银行业金融机构信息安全保障工作的指导意见》《国库资金风险管理办法》《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》《金融机构大额交易和可疑交易报告管理办法》等制度文件，要求各金融机构需要保障金融系统和数据的可用性和完整性。第二，央行在管理金融交易、结算清算等方面的管理要求，需要保障经济信息、全国交易信息的信息安全风向，例如《关于加强条码支付安全管理的通知》《关于强化银行卡磁条交易安全管理的通知》《关于开展支付安全风险专项排查

工作的通知》等。第三，央行在统筹规划、建设和使用国家基础数据过程中要保障数据的安全性，例如《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》《个人信用信息基础数据库管理暂行办法》《企业信用信息基础数据库管理暂行办法（征求意见稿）》《关于进一步加强征信信息安全管理的通知》等管理办法。

银行保险监督管理委员会（下称“银保监会”）是我国银行、保险机构网络信息安全工作的直接监管部门。早在2006年，银监会为有效控制电子银行业务风险，完善电子银行业务的监管规章体系，发布的《电子银行业务管理办法》《电子银行安全评估指引》对开展电子银行业务的金融机构提出信息安全相关的制度要求。同时，银监会发布的《商业银行信息科技风险管理指引》，对银行明确提出了风险管理的要求，该指引涵盖了信息科技风险管理的各个领域，进一步加强了商业银行信息科技风险管理。此外，针对银行业金融机构在业务连续性和信息科技外包等重点信息安全风险领域，银监会也分别出台了《商业银行业务连续性监管指引》和《银行业金融机构信息科技外包风险监管指引》等管理指引，强化上述重点领域的风险管理。

银行业金融机构在业务快速发展过程中，积累了用户数据、交易数据、外部数据等海量数据，数据已经成为银行的重要资产和核心竞争力，加之社会大众对个人信息保护意识的提升，银监会在《银行业金融机构数据治理指引》中，要求金融机构加强数据治理保障数据安全的同时，按照《信息安全技术个人信息安全规范》的国家标准加强对个人信息安全的保护。

证券监督管理委员会（下称“证监会”）同样是我国金融行业主要的监管单位，主要针对证券、期货、基金及相关服务机构等进行监管。2012年证监会发布《证券期货业信息安全保障管理办法》，该办法系统地规范了证券期货业信息安全管理等监管制度,确立了行业信息安全监管的体制,明确了行业监管部门、自律组织和市场主体的信息安全责任,提出了信息安全工作的要求。将于2019年6月1日起实施的《证券基金经营机构信息技术管理办法》，全面覆盖了各类主体，强化信息技术的主体责任，按照“谁运行，谁负责”的原则，明确信息安全监管安排，同时了明确治理、安全、合规三条主线，要求经营机构设立信息技术治理委员会，进一步加强了证监会对行业机构信息安全领域的监管力度。

金融机构的网络信息安全工作同时接受工业与信息化部（下称“工信部”）的监管。金融机构在使用信息网络资源时，需要遵循工业与信息化部在基础信息网络方面的相关规定。例如《互联网域名管理办法》（工信部〔2017〕43号）规定金融机构在注册互联网域名需要提供真实准确的信息，在运营和使用互联网域名时禁止提供的服务内容等要求；《规范互联网信息服务市场秩序若干规定》（工信部〔2017〕20号）规定金融机构在提供信息时不得实施侵犯其他互联网信息服务提供者合法权益的行为，收集用户信息时应征得用户的同意，同时应当加强系统安全防护等要求。

工信部下设网络安全管理局，承担电信网络和互联网基础环境的安全及信息安全工作。网络安全管理局拟订并组织实施电信网、互联网网络信息安全防护政策，同时承担电信和互联网行业网络安全审查相关工作。另外，网络安全管理局会承担电信网、互联网网络数据和用户信息安全保护管理工作。2019年1月25日，网信办、工信部、公安部、市场监管总局等四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，决定在全国范围组织开展App违法违规收集使用个人信息专项治理。

金融机构互联网应用系统中发布的内容信息应接受国家互联网信息办公室的监管。金融机构在其发布互联网应用系统上往往增加一些额外的信息服务，如公众账号、财经新闻、

微博、即时通讯等功能，而这些功能和其中流转的内容信息均应满足国家互联网信息办公室出台的相关规定。《互联网新闻信息服务管理规定》（国家互联网信息办公室令〔2017〕1号）规定金融机构在申请、运行信息服务时因遵循的相关规定，其中包括信息安全管理和技术措施，以及相关知识产权的保障要求；而金融机构在发布相关内容服务时如果采用了新技术新应用，则应按照《互联网新闻信息服务新技术新应用安全评估管理规定》相关要求，开展自评估并接受评估机构评估，审查信息安全管理制度和技术保障措施是否配套健全;金融机构在发布移动互联网应用程序（APP）时，应遵照《移动互联网应用程序信息服务管理规定》执行，包括要求App提供者对注册用户的实名制、建立健全用户信息安全保护机制、建立健全信息内容审核管理机制、尊重用户合法权益，以及记录并保存用户日志六十日等要求。

二、监管制度严格化

随着我国信息科技的发展，我国在监管层面的制度不断发展和强化，逐步形成了严格的网络信息安全保障制度，例如，金融机构在建设、使用和运维信息系统时，应按照网络安全等级保护制度要求，对信息系统进行定级、备案、测评和整改；在使用安全设备或产品时，应选用通过信息安全检测和评估认证的安全产品；金融机构在使用密码算法时应遵循商用密码管理制度；在使用互联网开展业务前，应按互联网信息服务安全管理制度要求进行备案。此外还有，安全专用产品销售许可证制度、计算机案件强行报案制度、计算机信息系统使用单位安全负责制度、计算机病毒专管制度、计算机信息系统国际联网备案制度、电信安全管理制度、计算机信息媒体进出境申报制度等制度要求。

金融机构在采用信息科技开展特定业务时，不但要遵循上述制度要求，同时还要遵循监管单位的特殊要求，例如银行业如需要开展电子银行业务，则应按照《电子银行安全评估指引》的规范要求，定期开展覆盖机构各个部门和层面的风险评估，以保障网络信息安全。在2019年1月25日中央网信办、工业和信息化部、公安部、市场监管总局决定，自2019年1月至12月，在全国范围组织开展App违法违规收集使用个人信息专项治理。为了更好地满足监管要求，金融机构建设使用的移动App，可以按照市场监管总局和中央网信办发布的《移动互联网应用程序（App）安全认证实施规则》的要求对应用程序进行安全认证。

三、监管内容精细化

我国网络信息安全的监管，从原有的原则性监管正逐步向精细化监管迈进。20世纪90年代更多的关注破坏计算机系统的犯罪，进入21世纪逐步关注金融行业系统可用性和安全风险的识别。时至今日，除了已经颁布的《网络安全法》和和国家标准《个人信息安全规范》，全国人大和学术界正在紧锣密鼓地加紧拟定我国数据安全保护和个人隐私保护的相关法律。网络信息安全的监管正从基础设施和系统的安全性向数据和隐私方向演进。

我国个人信息保护，是从个人邮件信息安全逐步向个人信息保护转变的。在1979年的刑法中对隐匿、毁弃或者非法开拆他人信件，侵犯公民通信自由权利进行保护；在1997年的刑法中，除对上述信息保密性保护以外，对邮政人员职务犯罪进行规定。2009年在刑法修正案七中，规定了特定人员出售、非法提供公民个人信息，一般人员非法获取公民个人信息都是犯罪，增加规定了单位犯罪。2015年的刑法修正案九，又在刑法修正案七的基础上，增加规定从重情节，使得内容更详细、完备，有层次感。

个人信息定义的范围也是逐步扩大和明确的。2003年发布的《中华人民共和国身份证法》和2006年发布的《中华人民共和国护照法》规定个人信息主要是指公民的姓名、年龄、住址、身份证号码、血型、婚姻状况、职业等身份识别信息。而在2005年中国人民银行发布的《个人信用信息基础数据库管理暂行办法》中，将个人信息分为基本信息、信贷信息和信用信息。扩大了个人信息的定义。2016年颁布的《中华人民共和国网络安全法》，其中第76条规定：“个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。” 2017年《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条明确规定了公民个人信息的范围：“指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。”结合以上法律条文的概括和列举，个人信息的范围逐步扩大，定义也逐步明确。

近年随着欧盟《通用数据保护条例》（GDPR，General Data Protection Regulation）的发布，欧盟实施了长臂管辖的政策，在网络空间中占领先机，我国也出台了相应的技术标准《个人信息安全规范》，在个人信息定义、个人信息的收集、保存、使用、披露和安全保护措施等方面提供技术性标准建议，进一步加强了个人信息的保护。

在数字化时代里，所有社会生活和个人信息都可以通过数字进行定义和标识，数据本身就是源源不断的资源，而国家监管正在逐步精细到每一个数据处理过程，以保障数据资源规范地流动并创造价值。银保监会在2018年发布的《银行业金融机构数据治理指引》要求各银行业金融机构加强数据治理，提高数据质量，充分发挥数据价值，提升经营管理水平，由高速增长向高质量发展转变。

四、监管手段科技化

金融科技的核心是运用新技术提高效率，以更好地解决信息不对称难题。科技的快速发展催生了个体网络借贷（P2P网贷）、互联网众筹、互联网保险等业务的同时，也带来了洗钱、金融诈骗和网络信息安全问题。为了应对由于科技发展所带来的新问题，监管部门正在充分运用人工智能、大数据和云计算等新技术，着力解决好监管过程中的信息不对称难题，以切实提高合规管理的能力和水平。

监管部门通过人工智能和大数据等科技化监管手段的应用，一方面可以在业务层面对金融诈骗、洗钱、个人信息泄露等行为特征进行识别和追溯，提高了分析和处理效率，强化了对金融机构业务操作层面的监管水平。另一方面，通过搭建统一的数据集中化存储和分析平台，可以对金融机构信息系统运行状况、网络信息安全风险情况进行精准化的规则匹配，发现潜在风险，并以事件和问责的形式，推动金融机构快速响应和处置整改，形成完整而高效的工作机制。如果金融机构没能在网络信息安全风险管理方面采用科技化的手段和机制，必然会在应对监管问责时处于被动地位。

五、监管政策地域化

另外一个不可忽视的现状是，我国各地区信息技术发展不均衡，信息产业结构也并不相同，因此各地区政府对网络信息安全监管的要求也存在侧重。北京、上海、重庆、杭州、贵阳、大连等城市近几年分别发布网络信息安全规范和要求，有的促进大数据发展，有的促进数据共享，有的关注个人信息保护等等。在2019年2月18日发布的《粤港澳大湾区发展规划纲要》中要求大湾区内城市建立健全网络与信息安全信息通报预警机制，加强实时监测、通报预警、应急处置工作，构建网络安全综合防御体系。相信在未来，这种网络安全监管政策地域化的趋势也将更为明显

浅谈金融行业云计算服务安全评估的必要性与方法

金融事业部　安全顾问　郭嘉祺

引言

近年来，随着“云大物移”相关技术的日趋成熟，Fintech进一步促进了金融行业云计算服务的发展。以云计算服务为依托，借助大数据和AI技术，金融机构的业务应用开始逐渐融入到云化的IT架构当中，从而也开始改变了金融行业的服务模式和行业格局。

一、云计算金融行业应用状况

在银行领域，云计算目前主要应用于IT运营管理和开放型底层平台等方面。云计算平台通过借助API接入的方式，构建全面的金融服务生态圈，为最终用户提供如生活缴费、资讯查询、网上购物等各类“互联网+”的金融服务，优化金融服务与生活的场景，提升了金融账户的价值。

在证券基金领域，云计算目前主要应用于客户端行情查询和交易量峰值分析等方面。通过部分非关键业务系统上云，在数据库分库、分表的部署模式下，可实现相当于上千套清算系统和实时交易系统的并行运算。

在保险领域，云计算目前主要应用于个性化定价和产品上线销售等业务服务。定制化云软件实现了快速分析客户实时数据，提供个性化定价，还能够通过社交媒体为目标客户提供专门的一对一保险服务。

二、云计算在金融行业应用的主要问题

如上所述，当前能够真正把核心交易系统上云的金融机构依然有限，大部分的金融机构对云计算的应用尚处于尝试阶段，只愿意把非关键业务系统部署在私有云或者行业云上，没有真正发挥云计算的生产效率。在我国金融机构对云计算服务的大规模应用，主要担心以下几个方面：

业务中断：在云计算框架下，希望能够通过冗余备份的方式能实现系统资源的充分利用，但金融机构核心系统不适合采用多副本备份，当云平台因为容灾备份技术不到位而发生服务器宕机时，有可能造成业务连续性问题。

技术外包：对于行业云、公有云这些主要由CSP（云服务供应商）提供服务的第三方服务商来说，有可能存在的操作行为不当、安全防护漏洞、数据混淆储存等风险，最终会导致托管的金融机构在业务、网络和数据等各层面的安全受到威胁，甚至有可能演化成金融系统性风险；而私有云对于身份、凭证和访问管理不足，技术能力没跟上，或者内部人员导致的信息数据泄露等风险问题，也延缓了金融机构重要业务系统部署上云的步伐。

新老系统不兼容：传统金融机构IT系统普遍建立时间较早、耦合性较

高，与分布式云计算系统融合存在一定的困难。另外，部分金融机构同时采用私有云和公有云部署不同业务系统，对混合云的管理尚缺乏能够参考的成熟安全体系。

监管制度不明确：虽然金融行业相关监管机构已经有明确的政策鼓励金融机构IT系统能够运行在云计算架构之上，如人行印发的《中国金融业信息技术“十三五”发展规划》，但具体落地的实施监管要求并没有明确，应用了云计算架构的金融机构都面临这如何满足相关合规要求的挑战。

三、云计算服务安全评估的必要性

在云计算架构下开放的网络、模糊的边界、海量的数据和共享业务场景复杂多变，安全挑战比传统IT架构更为严峻，需要关注的安全点包括了：

- 软件定义基础服务的健壮性和对外部攻击的防御能力；
- 底层的安全漏洞对上层用户数据的威胁；
- 资源的弹性供给而带来的服务响应延迟；
- 分布式架构数据备份和恢复方案设计等等；

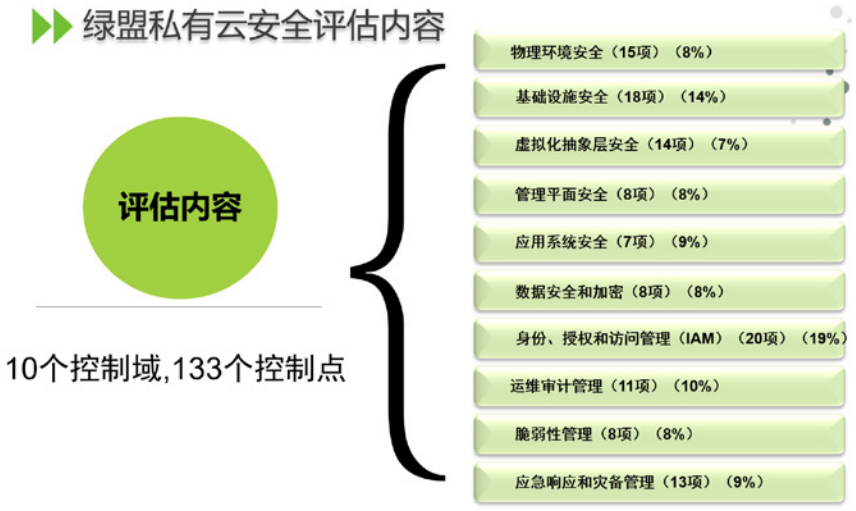
另外，目前云平台架构还没有形成如传统IT服务架构下相对成熟的安全体系。因此，在云平台架构下保障信息系统保密性、完整性、可用性为目标的云计算服务安全风险评估尤为重要。

近日国家网信办等四部门联合发布了《云计算服务安全评估办法》。该办法指出对面向党政机关、关键信息基础设施提供的云计算服务的云平台进行安全评估，评估的重点内容包括云平台技术、产品和服务供应链安全情况，以及云服务商安全管理能力和云平台安全防护情况等。而《关键信息基础设施保护条例》也有望在年内出台，金融行业的关键信息基础设施必涉及

其中。

四、云计算服务安全评估方法

笔者根据金融行业的相关合规要求，基于即将实施的《信息安全技术网络安全等级保护基本要求 第2部分：云计算安全扩展要求》、GB/T31168-2014《信息安全技术云计算服务安全能力要求》、CSA开发的《云安全控制矩阵3.0》，以及OpenStack安全指南等云服务建设方面的安全指导和实施要求，结合金融行业客户对云计算的理解和风险偏好，优化整理针对金融行业的云计算服务安全评估方法。具体的评估内容包括：物理机房环境安全、物理基础设施安全、虚拟化抽象层安全、管理平面层安全，还有上层的业务应用系统安全、数据存储安全，在运维管理方面的还包括了IAM管理、审计管理、脆弱性管理，以及应急响应和业务连续性管理。总共归纳出10个控制域（每个控制域根据重要性赋予不同的权重比例），133个控制点进行安全评估，如下图所示：



由于篇幅有限，这里以虚拟化抽象层安全评估为例。本控制域权重比例为7%，主要针对虚拟化平台、虚拟主机/容器安全、虚拟网络安全、虚拟存储方面进行检查：

1）虚拟化平台安全

梳理云平台提供的API接口列表，并且对API接口的访问进行检查，评估API

生命周期的安全问题，例如对API的认证和授权、安全监控（调用次数、延迟、错误率等的监控）、日志的审计、传输的安全等；另外，还可以检查云平台软件版本和物理机安全基线等；

2）虚拟主机/容器安全

检查虚拟机之间、虚拟机与资源管理器之间、虚拟机与外部网络之间的访问控制；扫描虚拟机（VM）镜像或者容器镜像当中封装的软件或者中间件是否存在已知的CVE漏洞；检查虚拟机或者容器版本的安全基线；检查镜像库的存储和访问控制是否安全等。

3）虚拟网络安全

检查是否采用VLAN/VXLAN/VPC/安全组等对多租户的虚拟网络资源进行隔离；检查虚拟网络的冗余设计情况，第三方安全产品的接入；检查是否配置Qos实现多租户流量管理等；

4）虚拟存储安全

检查是否使用数据隔离和访问控制技术，对不同安全等级的业务应用系统所产生的数据，独立存储在不同的物理磁盘中；检查数据存储的可靠性机制，例如是否采用冗余模式和完整性校验。

另外对残余信息的保护，确保在虚拟化环境下的数据存储安全，例如检查存储资源回收时，是否已经对逻辑卷进行“位”格式化；检查是否使用数据隔离，访问控制，数据可靠性和残余信息保护来保障虚拟化环境下的数据存储安全等。

结束语

因此，通过云计算服务的安全评估，利用差距分析方法，能够为金融机构在制定云平台安全技术框架时提供基础参考依据，同时能够促进将来监管机构对金融机构云计算平台的建设、推广、运行，以及外购产品和服务采购等各项工作的合规要求。此外，还能够有效降低和应对各类内/外部威胁对云上系统和数据带来的安全风险，同时能够利用云计算领域技术与服务提升安全防御工作的精准性、有效性和实施能力。

GozNym 恶意软件窃取近 1 亿美元 幕后黑客被判刑

美国司法部发布报告：美国企业及金融机构盗窃案告破，其中三名犯罪分子已被监禁判刑。

该案件发生在2015至2016年间，犯罪分子主要是利用 GozNym banking Trojan病毒入侵全球的4000多台计算机来进行网络欺诈，最终盗取近1亿美元，美国和欧洲损失最为严重。而Goznym病毒的本质是一个银行木马，它由两大部分组成，分别是2012年首次出现的银行木马Gozi ISFB 以及类似勒索软件的木马下载器Nymaim。

今年五月，欧洲刑警组织捣毁这一犯罪网络，美国对该犯罪组织10名成员提出指控，5名成员当场被捕，包括开发者在内的另外五名成员潜逃。

周五，在匹兹堡的一家联邦法院，事件中担任财务的Krasimir Nikolov以网络欺诈罪名被联邦政府指控。Nikolov于2016年9月被保加利亚当局逮捕，并于2016年12月被引渡到保加利亚。而在格鲁吉亚被逮捕起诉并判刑的另外两名成员Alexander Konovolov及Marat Kazandjian也分别被判监禁7年和5年。

该恶意软件运行流程为：先利用大规模恶意软件来攻击受害者的电脑，然后进行病毒传播，在受害者将他们的银行密码输入浏览器后，通过恶意软件来捕获账户密码，继而登录银行账户进行资金转移。

对于该案件的告破，美国检察官Scott W. Brady说到：“这是全球各执法伙伴共同合作的功劳。”

原文转自： HackerNews.cc

原文链接：http://hackernews.cc/archives/28947

专家点评

文中提到的“犯罪分子首先通过恶意软件大规模入侵受害者，在入侵成功完成病毒传播，窃取受害者的个人银行信息”这种攻击方式也是很常见的木马攻击行为；因此针对此类木马攻击的防范建议：

❶ 应该避免在公用电脑上登录个人金融账号信息，同时个人电脑应该安装杀毒软件并保持病毒库的最新状态；

❷个人用户在访问金融网站进行交易时，需要注意网站页面及域名的真实性，检查浏览器地址栏的SSL证书是否可信；

❸ 不随便打开来路不明的电子邮件与附件程序。

在万物互联的时代，每个人均需有防范网络诈骗的意识，建设安全的网络空间还需要各方的努力；对于网络欺诈行为，全球任何一个国家都将严厉打击。

恶意软件可让 ATM 机按需吐出所有现金

近日某个上午，德国弗莱堡市的一位银行职员发现，某台 ATM 机似乎出现了问题。其控制面板上收到了一条奇怪的消息 —— “Ho！”可惜的是，这位员工没有立即意识到，黑客已经将恶意软件植入了自动柜员机中 —— 这也是所谓的“劫持”攻击的一部分。最终结果是，正如大家在许多影视作品中所见到的那样 —— 这台 ATM 吐出了一堆现金，直至钞箱被彻底清空。

资料图（来自：Wincor Nixdorf，via BGR）

通过 Motherboard 与一家德国新闻媒体联合进行的调查，可知黑客是如何逐步对运行过时软件、安全性较低的计算机进行攻击的。

有关部门显然不希望在事情经过上着墨太多，但多个消息来源证实，这

种类型的 ATM 攻击，正在全世界范围内（包括美国地区）呈现上升趋势。这意味着银行的安防系统脆弱不堪，且基本没准备对此进行处理。

通常情况下，攻击者会先从 ATM 机上的访问点（如 USB 接口）下手，以安装恶意软件。相关攻击代码的成本竟然也十分低廉 —— 仅需 1000 美元，即可买到在欧洲各地进行肆意攻击的俄罗斯软件。

软件截图（来自：@CRYPTOINSANE / Twitter）

尽管好莱坞影视作品中经常出现让 ATM 机吐出大量现金的场景，但不幸的是，现实情况也是如此。

有消息人士向参与调查的记者透露，某些不良行为者在出售代码，使得任何人只要肯出钱购买，基本上都有攻破 ATM 机的可能。

网络安全专家 David Sancho 认为，这件事不会局限于世界的某个特定角落，而是在全球范围内都有可能发生。

原文转自：cnbeta

原文链接：https://www.cnbeta.com/articles/tech/899627.htm

专家点评

自从2010年安全研究专家、传奇白帽黑客巴纳比·杰克（Barnaby Jack）在国际信息安全会议BlackHat大会上演示ATM“吐钱”的案例之后，让ATM机“吐钱”的新闻就开始频繁见诸报端，针对ATM机的恶意软件也不断升级，攻击案例在全球范围内呈现不断增长的态势，一方面，由于ATM机网络大多使用内部专用网络，因此一般没有杀毒软件等安全防护措施；另一方面，由于ATM机使用了过时的操作系统和软件，这些都为攻击者提供了有利条件。建议金融机构针对ATM机网络加强安全防护措施，及时更新ATM机的操作系统和软件，定期进行安全检查并排查安全隐患。

韩国加密货币交易所遭到黑客攻击

黑客攻击总部位于韩国的加密货币交易所Bithumb，成功窃取了价值近1900万美元的加密货币。Bithumb在此前就遭受过严重的黑客攻击，此事一出，引起了相关人士的强烈不满。

据外媒报道，总部位于韩国的加密货币交易所Bithumb承认，黑客于3月29日从Bithumb窃取了价值近1900万美元的加密货币。

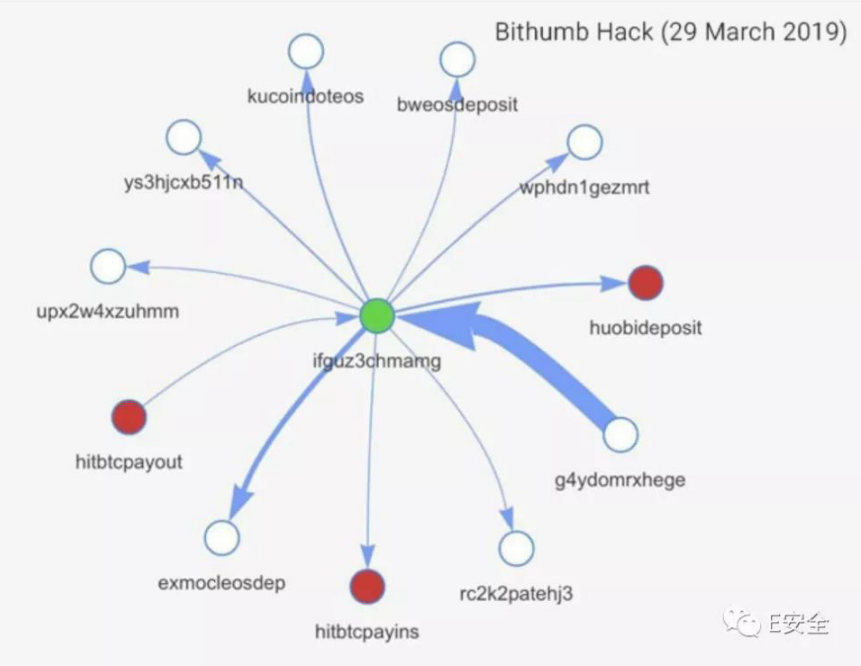
据称，黑客成功侵入了Bithumb的一些热门EOS和XRP钱包，并将大约300万EOS（约1300万美元）和2000万XRP（约600万美元）转移到了新创建的账户中。

然后，黑客通过ChangeNow（一个不需要KYC/account的非托管密码交换平台）将所盗的资产分散转移到他在其他加密货币交易所（包括Huobi、HitBTC、WB和EXmo）上创建的不同账户。

Bithumb在过去就已经被黑多次。这家流行的加密货币交易所Bithumb上次遭到黑客攻击是在2018年6月，那次黑客窃取了3100万美元。2017年7月，黑客从许多用户的钱包中窃取了价值100万美元的EOS。

相关人士在推特上称，这是Bithumb第二次遭遇重大黑客攻击，在第一次黑客攻击之后，它居然仍然能够从韩国获得正式许可，WTF?

Bithumb的EOS热钱包账户的私钥被盗（地址g4ydomrxhege），黑客可以将资金转移到他的地址“ifguz3chmamg”。



黑客资金分配图

下面是黑客如何在不同的交易所将所盗资金的分配和转移：

EXMO： 662,600

Huobi：263,605

Changelly：143,511

KuCoin：96,270

CoinSwitch：38,725

目前Bithumb仍在调查此次黑客攻击，并已向韩国互联网安全机构（KISA）和网络警察报告了此次攻击事件。Bithumb加密货币存取款服务已延迟推出。

Bithumb公司表示，经过检查，公司至今还未发现外部入侵路径，因此判断该事件是内部人员参与。

公司正在与主要加密货币交易所和基金会合作，希望可以挽回损失。去年，该交易所遭到黑客攻击，损失3000万美元时，Bithumb设法追回了一半的被盗资金。

原文转自：E安全

原文链接：https://www.easyaq.com

专家点评

很多金融企业与Bithumb公司相似，边界安全比较完善，针对外部攻击检测和防护的能力较强，但针对内部威胁的防护与审计薄弱，导致内部威胁的暴露时间长、补救成本高昂。根据Ponemon Institute公布的《2018年全球组织内部威胁成本》显示，在3269起事件中，有64%都是由员工或承包商的疏忽导致的;而犯罪分子和内鬼造成的泄漏事件则为23%。建议通过下述几方面提升针对内部威胁的安全防护能力：1、对员工进行安全意识和技能培训；2、分配权限时遵守最小特权原则，只在必要的时候进行权限升级；3、通过设置复杂口令、多因素身份认证等方式保护账户安全；4、增强内部重要数据和信息系统的安全审计。

NSFOCUS

漏洞聚焦

VMware ESXi 远程代码执行漏洞 (CVE-2019-5544) 安全威胁通告

发布时间：2019 年 12 月 6 日

综述

当地时间12月5号，VMware 官方发布安全通告公布了一个存在于 VMware ESXi 和 Horizon DaaS 中的远程代码执行漏洞（CVE-2019-5544）。漏洞来源于ESXi和Horizon DaaS设备中使用的OpenSLP存在堆覆盖问题，能够通过网络访问ESXi宿主机上 427 端口或任何Horizon DaaS平台的恶意用户可能会通过覆盖OpenSLP服务的堆，最终导致远程代码执行。

VMware已评估了此问题，并定级为严重，CVSSv3 评分 9.8。该漏洞由360Vulcan团队和“天府杯”组织者合作上报给官方。

参考链接：

https://www.vmware.com/security/advisories/VMSA-2019-0022.html

受影响产品及修复情况

产品	受影响版本	修复补丁
ESXi	6.7	ESXi670-201912001
ESXi	6.5	ESXi650-201912001
ESXi	6.0	ESXi600-201912001
Horizon DaaS	8.x	补丁制作中

安全建议

官方已为 ESXi 提供了修复该漏洞的补丁及缓解措施，请受影响用户尽快前往对应页面下载更新防范风险，Horizon DaaS的补丁还在制作中，请密切关注官网更新。

- ESXi 6.7 补丁 ESXi670-201912001

  https://my.vmware.com/group/vmware/patch

  https://docs.vmware.com/en/VMware-vSphere/6.7/rn/esxi670-201912001.html

- ESXi 6.5 补丁 ESXi650-201912001

  https://my.vmware.com/group/vmware/patch

  https://docs.vmware.com/en/VMware-vSphere/6.5/rn/esxi650-201912001.html

- ESXi 6.0 补丁 ESXi600-201912001

  https://my.vmware.com/group/vmware/patch

  https://docs.vmware.com/en/VMware-vSphere/6.0/rn/esxi600-201912001.html

- 缓解措施：

  ESXi 6.x https://kb.vmware.com/s/article/76372

声明

Drupal 修复多个漏洞安全威胁通告

发布时间：2019 年 12 月 20 日

综述

当地时间12月18号，Drupal官方发布安全通告公布其核心产品中存在的多个漏洞。其中包括一个严重漏洞和三个中危漏洞。

◆ 严重的符号链接漏洞

Drupal使用的第三方库 Archive_Tar 中存在漏洞，该库被用于创建、提取和添加tar文件。在Archive_Tar解压带有符号链接文档的过程中存在问题，一旦被成功利用，攻击者便可通过上传恶意的tar文件来覆盖目标服务器上的敏感文件。

据Drupal开发人员称，已经存在针对此漏洞的概念验证代码。

◆ 中危访问绕过漏洞

Drupal默认媒体库模块中存在一个安全漏洞，可允许低权限用户访问敏感信息。

◆ 中危安全限制绕过漏洞

Drupal 8中的file_save_upload()功能不会从文件名中去除前导和结尾处的（'.'），能够上传具有任何扩展名和贡献模块的用户，可以使用它来覆盖任意系统文件，例如.htaccess，以绕过安全性保护。

◆ 中危拒绝服务漏洞

Drupal 8使用的install.php文件中包含一个漏洞，未经身份验证的远程攻击者可以利用该漏洞破坏网站缓存数据，最终造成拒绝服务。

官方通告参考链接：

https://www.drupal.org/sa-core-2019-012
https://www.drupal.org/sa-core-2019-011
https://www.drupal.org/sa-core-2019-010
https://www.drupal.org/sa-core-2019-009

受影响产品及修复情况

漏洞	受影响版本	修复版本
严重的符号链接漏洞	Drupal 7.x < 7.69 Drupal 8.7.x< 8.7.11 Drupal 8.8.x< 8.8.1	Drupal 7.69 Drupal 8.7.11 Drupal 8.8.1
中危访问绕过漏洞 中危安全限制绕过漏洞 中危拒绝服务漏洞	Drupal 8.7.x< 8.7.11 Drupal 8.8.x< 8.8.1	Drupal 8.7.11 Drupal 8.8.1

安全建议

官方已为受影响产品提供了修复漏洞的最新版本。请相关用户尽快前往官网下载更新防范风险。

另，官方为部分漏洞也提供了缓解措施：

◆ 中危访问绕过漏洞

可以通过取消选中/admin/config/media/media-library 上“启用高级用户界面”复选框来缓解此漏洞。（此缓解措施在8.7.x中不适用）

◆ 中危拒绝服务漏洞

如果不需要，可以禁止对install.php的访问。

参考链接

Drupal 7.69 下载地址：https://www.drupal.org/project/drupal/releases/7.69

Drupal 8.7.11下载地址：

https://www.drupal.org/project/drupal/releases/8.7.11

Drupal 8.8.1下载地址：

https://www.drupal.org/project/drupal/releases/8.8.1

声明

Harbor 多个漏洞安全威胁通告

发布时间：2019 年 12 月 4 日

综述

今日在 Harbor 官方仓库公布了 5 个漏洞，其中包括 2 个官方定级为严重的漏洞（CVE-2019-19025、CVE-2019-19023），2个高危级别漏洞（CVE-2019-19029、CVE-2019-19026），1个中等级别漏洞（CVE-2019-3990）。

Harbor是一个开源镜像管理项目，通过添加一些用户常用的功能特性，例如安全、标识和管理等，扩展了开源Docker Distribution。

◆ CVE-2019-19025：缺少CSRF 保护漏洞，Harbor Web界面未实现针对跨站点请求伪造（CSRF）的保护机制。通过把经过身份验证的用户吸引到事先准备好的第三方网站，可导致第三方代表经过身份验证的用户或管理员在平台上执行任意操作。

◆ CVE-2019-19023：特权提升漏洞，该漏洞使普通用户可以通过API调用来修改特定用户的电子邮件地址，从而获得管理员帐户特权。漏洞源于Harbor API没有对修改电子邮件地址的API请求进行适当的权限限制。

◆ CVE-2019-19029：通过用户组进行SQL注入，具有项目管理功能的用户可以利用SQL注入来从底层数据库读取机密信息或进行权限提升。

◆ CVE-2019-19026：通过项目quotas进行SQL注入，Harbor API的quotas部分存在一个SQL注入漏洞。经过身份验证的管理员可以通过GET参数发送特制的SQL有效负载，从而从数据库中提取敏感信息。

◆ CVE-2019-3990：用户枚举漏洞，该漏洞存在于 "/users" api 中，这个功能应该仅限于管理员使用，可是该限制可被绕过，非管理员用户（例如通过自我注册创建的用户）可以通过向 /api/users/search发送 GET请求来列出所有用户名和用户ID、确认与用户名关联的电子邮件地址等。

受影响及已修复版本

编号	受影响版本	修复版本
CVE-2019-19025	1.7.*, 1.8.*, 1.9.*	1.8.6, 1.9.3
CVE-2019-19023	1.7.*, 1.8.*, 1.9.*	1.8.6, 1.9.3
CVE-2019-19029	1.7.*, 1.8.*, 1.9.*	1.8.6, 1.9.3
CVE-2019-19026	1.7.*, 1.8.*, 1.9.*	1.8.6, 1.9.3
CVE-2019-3990	1.7.*, 1.8.*, 1.9.0, 1.9.1	1.8.6, 1.9.3

安全建议

官方已提供修复了以上漏洞的最新版本，请受影响用户尽快下载更新防范风险。

参考链接：

https://github.com/goharbor/harbor/security/advisories/GHSA-gcqm-v682-ccw6

https://github.com/goharbor/harbor/security/advisories/GHSA-3868-7c5x-4827

https://github.com/goharbor/harbor/security/advisories/GHSA-qcfv-8v29-469w

https://github.com/goharbor/harbor/security/advisories/GHSA-rh89-vvrg-fg64

https://github.com/goharbor/harbor/security/advisories/GHSA-6qj9-33j4-rvhg

下载链接：

https://github.com/goharbor/harbor/releases

声明

Adobe 12 月安全更新安全威胁通告

发布时间：2019 年 12 月 11 日

综述

当地时间12月11日，Adobe官方发布了12月安全更新，修复了Adobe 多款产品的多个漏洞，包括Adobe Photoshop CC、Adobe Acrobat and Reader、Brackets以及Adobe ColdFusion等。

官方通告地址：

https://helpx.adobe.com/security.html

漏洞概述：

Adobe Photoshop CC

Adobe已发布Adobe Photoshop CC 安全更新，修复了2个安全漏洞。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
内存损坏	任意代码执行	Critical	CVE-2019-8253
内存损坏	任意代码执行	Critical	CVE-2019-8254

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：

https://helpx.adobe.com/security/products/photoshop/apsb19-56.html

Brackets

Adobe已发布Brackets安全更新，修复了1个安全漏洞。

漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
命令注入	任意代码执行	Critical	CVE-2019-8255

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：
https://helpx.adobe.com/security/products/brackets/apsb19-57.html

Adobe ColdFusion

Adobe已发布Adobe ColdFusion安全更新，修复了1个安全漏洞。
漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
默认安装路径	权限提升	Important	CVE-2019-8256

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：
https://helpx.adobe.com/security/products/coldfusion/apsb19-58.html

Adobe Acrobat and Reader

Adobe已发布Adobe Acrobat and Reader安全更新，修复了21个安全漏洞。
漏洞概括如下：

漏洞类别	漏洞影响	严重程度	CVE 编号
越界读取	信息泄露	Important	CVE-2019-16449 CVE-2019-16456 CVE-2019-16457 CVE-2019-16458 CVE-2019-16461 CVE-2019-16465
越界写入	任意代码执行	Critical	CVE-2019-16450 CVE-2019-16454
释放后重利用	任意代码执行	Critical	CVE-2019-16445 CVE-2019-16448 CVE-2019-16452 CVE-2019-16459 CVE-2019-16464

漏洞类别	漏洞影响	严重程度	CVE 编号
堆溢出	任意代码执行	Critical	CVE-2019-16451
缓冲区错误	任意代码执行	Critical	CVE-2019-16462
不信任的指针错误	任意代码执行	Critical	CVE-2019-16446 CVE-2019-16455 CVE-2019-16460 CVE-2019-16463
目录权限提升	权限提升	Important	CVE-2019-16444
安全绕过	任意代码执行	Critical	CVE-2019-16453

关于漏洞的具体影响版本及修复情况，请参考Adobe官方安全通告：
https://helpx.adobe.com/security/products/acrobat/apsb19-55.html

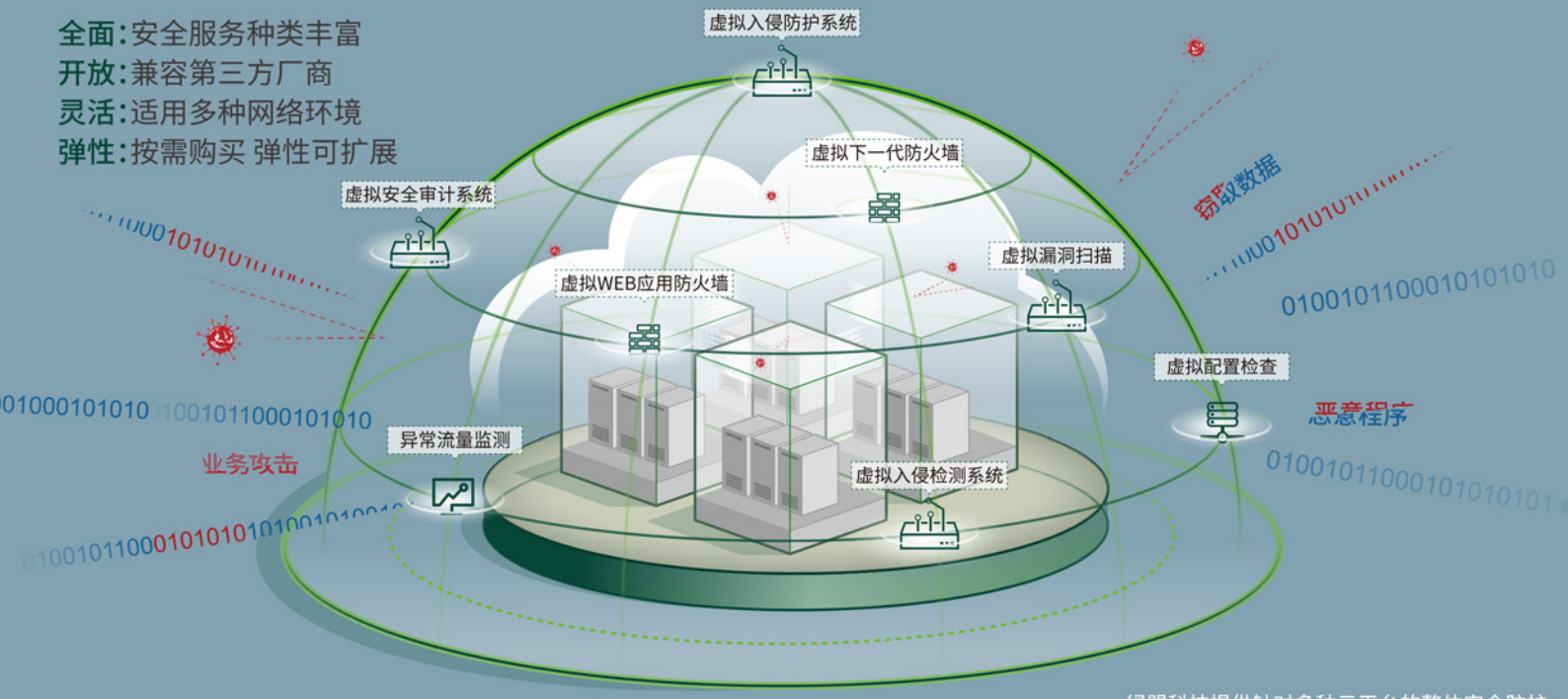
解决方案

Adobe官方已经发布新版本修复了上述漏洞，用户应及时升级进行防护。

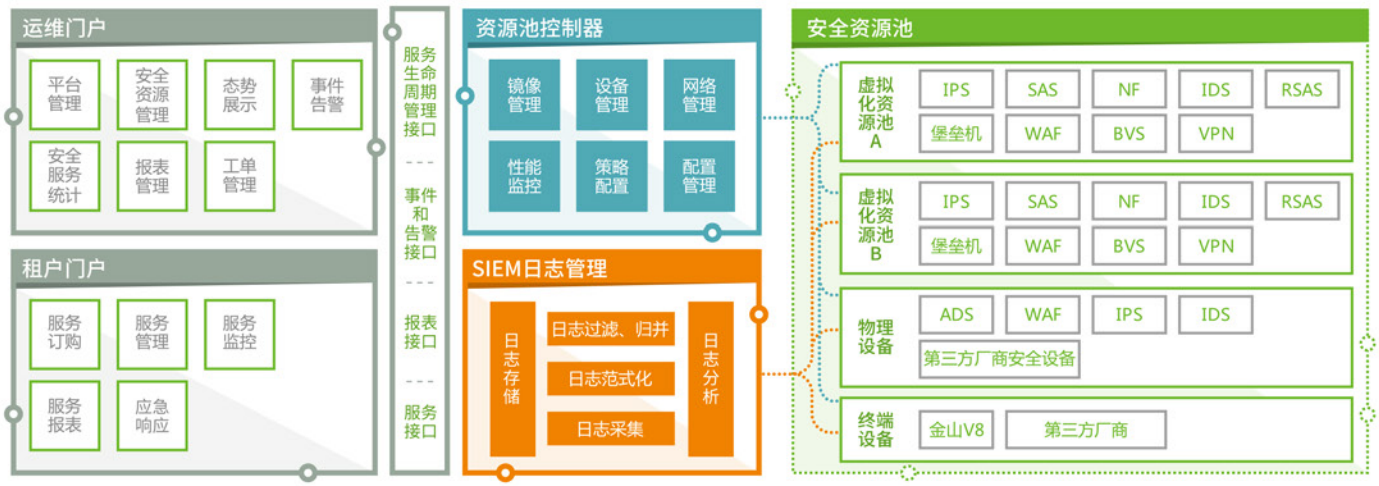
详细信息及操作可参考各产品漏洞部分的官方通告链接。

绿盟科技
云计算安全解决方案

全面:安全服务种类丰富
开放:兼容第三方厂商
灵活:适用多种网络环境
弹性:按需购买 弹性可扩展



绿盟科技提供针对多种云平台的整体安全防护



THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

安全月报

绿盟科技金融事业部出品

主办/ 绿盟科技金融事业部
地址/ 北京市海淀区北洼路4号益泰大厦3层
邮编/ 100089
电话/ 010-59610688-1159
传真/ 010-59610689
网站/ www.nsfocus.com
客户支持热线/ 400-818-6868
股票代码/ 300369
月报电子版下载/ http://www.nsfocus.com.cn/research/list_145_145.html

NSFOCUS