



★ 本期焦点

运营商：我帮客户做规划

金融：证券类金融企业网络安全建设方法与思路

政府：探索“互联网+政务服务”安全保障体系

互联网：互联网企业的等级保护建设之路

绿盟科技官方微信



### 本期看点 HEADLINES

31 我帮客户做规划

42 证券类金融企业网络安全建设方法与思路

48 探索“互联网+政务服务”安全保障体系

59 互联网企业的等级保护建设之路



主办：绿盟科技  
策划：绿盟内刊编委会  
地址：北京市海淀区北洼路4号益泰大厦三层  
邮编：100089  
电话：(010)6843 8880-8667  
传真：(010)6872 8708  
网址：www.nsfocus.com


欢迎您扫描封面左下角的二维码，关注绿盟科技官方微信，  
分享您的建议和评论，或者来信 [nsmagazine@nsfocus.com](mailto:nsmagazine@nsfocus.com)  
与我们交流。  
[Nsmagazine@nsfocus.com](mailto:Nsmagazine@nsfocus.com)

# 2017/02 总第 034

## 安全+ SECURITY

© 2017 绿盟科技

本刊图片与文字未经相关版权所有人书面批准，  
一概不得以任何形式、方法转载或使用。本刊保留所有版权。

SECURITY  是绿盟科技的注册商标。

需要获取更多信息，请访问 [WWW.NSFOCUS.COM](http://WWW.NSFOCUS.COM)

<b>安全形势</b>	<b>2-26</b>
绿盟科技智慧防护方案，多次完成重大活动安保	2
绿盟科技金融行业脆弱性管理平台荣获“2016 企业优秀解决方案奖”	6
绿盟科技 ADS 获得国测网络安全产品最高级别安全证书“EAL3+”	8
安全意识培养浅谈	周博 10
互联网安全威胁月报 201612	陈颐欢 15
关于安全服务模型的一些思考	江国龙 刘文懋 21
<b>封面故事</b>	<b>27-30</b>
攻守“军备竞赛” 2017 如何布局	赵粮 27
<b>行业热点</b>	<b>31-53</b>
我帮客户做规划	曹晖 31
走进中移动 回忆合规平台规范编写的那几天	赵粤征 38
证券类金融企业网络安全建设方法与思路	俞琛 42
探索“互联网 + 政务服务”安全保障体系	何财发 48
物联网安全技术	张星 52
互联网企业的等级保护建设之路	孟凡勇 59
<b>智慧安全 2.0</b>	<b>65-84</b>
Android Intent 攻击分析与防范	周振 65
大数据安全平台威胁分析	吴天昊 吴子建 施岭 72
暗黑时代，APT 威胁阴影下的防御姿势	刘弘利 79

# 绿盟科技智慧防护方案 多次完成重大活动安保

近年来随着互联网时代的到来，数字化浪潮席卷全球，安全行业也随之发生着翻天覆地的变革，攻防差距逐间拉大，这意味着单一的安全产品已然无力招架突如其来的安全威胁。绿盟科技为确保服务客户业务顺畅运行，决定应势而变及时转型，智慧安全 2.0 战略及其相应的防御体系应运而生，“云地人机”核心理念成为保护客户网络安全的一方基石。

## 从智慧安全 2.0 到云地人机防护方案

绿盟科技已经充分搭建了“云 - 地 - 人 - 机”为核心理念的智慧安全 2.0 战略防御体系，这个体系在战术层面可以这样理解：

### “云”

代表绿盟科技云端安全能力，通过云端预警，7×24 小时云监测等服务，可对监测站点进行平稳度、敏感内容、篡改情况、网速、关键字的监测，并通过结合运营商云平台抗 DDoS 集群组对来自互联网大流量的攻击进行牵引清洗。

### “地”

代表绿盟科技独有的攻防平台，结合企业安全中心 ESPC 和大数数据态势感知平台 BSA，对各种资源进行态势感知和信息采集，综合分析用户即时的网络安全态势。

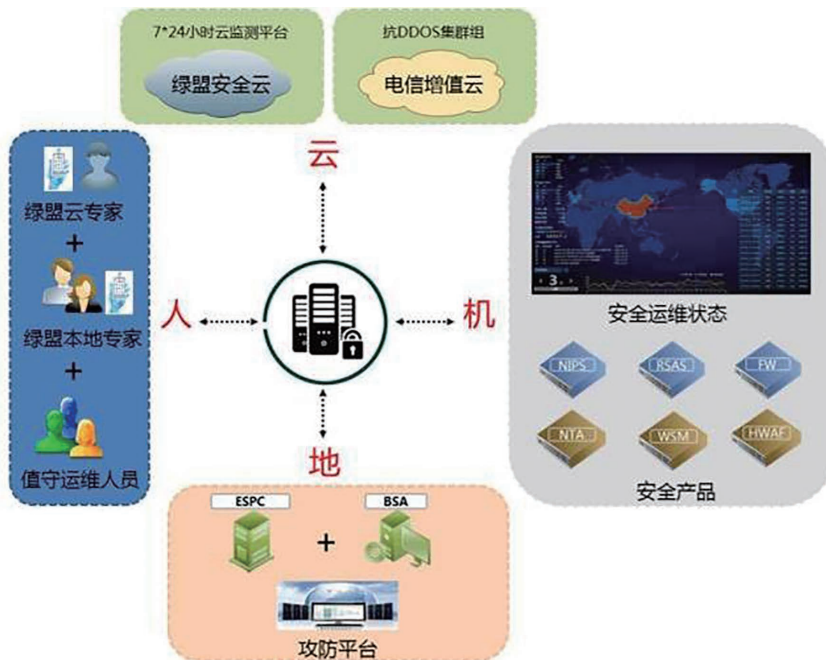
## 安全形势

### “人”

代表绿盟科技专业技术服务团队，绿盟科技通过绿盟云专家、绿盟本地专家及值守运维人员的专业服务，对网站运行情况及设备的运维情况进行实时的监控，并在网站上线前，对网站进行了充分的渗透测试。

### “机”

代表客户部署的安全设备，主要负责防护网站的安全，充分保障客户网站的正常运行。



绿盟科技“云-地-人-机”的全方位网络安全防御体系

同时，在这个安全防护体系中，安全设备的部署已经属于最基础的安全防护，安全监测体系及应急响应占据了防护体系更大的比重，特别是应急响应部分，更是重中之重。



绿盟科技网络安全防御等级

网络安全终归是人与人的智慧对抗，在互联网时代，新的攻击方式层出不穷，如何建立“即时、快速、有效”的应急响应体系，是当下乃至将来，网络安全服务的核心工作。

### 在 2016 年杭州 G20 峰会期间建功卓著

举世瞩目的二十国集团峰会成功举办，绿盟科技按照 G20 峰会网络安全保卫工作组的总体部署，从 10 多个部门抽调 118 位精兵强将，高质高效地完成了技术检测、24 小时监测、应急处置支持等各项工作任务，使用智慧安全 2.0 战略及其安全防护体系，有效保障了重点单位的网络安全，在 G20 峰会网络安全保卫工作中发挥出重要作用，做出重要贡献。

### 二十国集团 (G20) 峰会 网络安全保卫组

#### 感谢信

北京神州绿盟信息安全科技股份有限公司：

举世瞩目的二十国集团峰会（以下简称“G20 峰会”）成功举办，作为 G20 峰会网络安全保卫工作的技术支持单位，你单位站在维护国家网络安全的高度，充分认识到此次网络安全保卫工作的极端重要性，按照 G20 峰会网络安全保卫工作组总体部署，保质高效地完成了技术检测、24 小时实时监测、应急处置支持各项工作任务，有效保障了重点单位的网络安全，在 G20 峰会网络安全保卫工作中发挥了重要作用，做出了重要贡献。

在此，谨对贵单位一直以来对公安机关网络安全保卫工作的高度重视和全力支持，在 G20 峰会网络安全保卫工作中做出的重要贡献表示衷心感谢！

G20 峰会网络安全保卫组  
(公安福州第一局代印)  
2016 年 9 月 29 日

公安部致绿盟科技团队感谢信



第四十届亚洲艺术节开幕式，近 40 个国家受邀前来

### 在第十四届亚洲艺术节上忠于职守

2015 年 11 月 15 日，第十四届亚洲艺术节在福建泉州成功举办。泉州晚报作为活动的网络宣传平台，对此次活动的宣传工作给予了高度的重视。为充分保障活动期间网站的稳定运行，最终选择绿盟科技智慧安全 2.0 网络安全防护方案作为此次网络运维的保障方案。

在强大的防护体系支持之下，此次保障

绿盟科技仅投入 4 名技术人员，就实现与省电信公司人员及增值服务平台的顺利对接，一旦发生大流量攻击，随时将流量牵引至省干的 ADS 进行清洗。同时，绿盟北京云监测平台也将泉州晚报亚艺节 WAF 纳入监控范围，并定期形成监控报告。

活动前期对客户的服务器进行一天两次的巡检服务，同时对网站进行渗透测试，并对服务器进行安全加固。当网站进入访问的高峰期，监测频率甚至缩短至每小时一次，夜间直播时，更是进一步将监控频率缩短到每 10 分钟一次。

在绿盟科技的辛勤值守下，活动圆满落幕，绿盟科技作为此次活动唯一的网络安全防护工作组，也顺利完成了 9 天的网站安全护航工作。

2015 年 11 月 16 日，泉州晚报发来感谢信，对绿盟科技的全方位的网络安全服务给予

## 安全形势

### 感谢信

北京神州绿盟科技有限公司：  
第十四届亚洲艺术节暨第二届海上丝绸之路国际艺术节于2015年11月7日开幕并于11月15日正式落幕，历时9天。在此对贵公司技术人员在活动期间给予泉州网和亚艺术节官网网络亚艺术节的大力支持深表感谢。  
本次活动级别高、任务重，贵公司提供的网页代码和系统漏洞安全检查、流量监控和抗DDOS攻击、安全监控与入侵防护、应用系统渗透性测试以及7\*24小时值守等服务，确保了本次活动的圆满完成，充分保障了泉州网和亚艺术节官网的稳定与安全运行。  
贵公司为保障艺术节所做出的努力是有目共睹的，活动的顺利完成与贵公司为我方提供的各项安全服务是密不可分的，期望在日后的工作中能与贵公司有更广阔的合作空间。  
在此再次感谢贵公司技术人员在本次艺术节期间为我们提供的安全保障服务。  
此致  
敬礼

泉州晚报社信息技术部  
2015年11月16日

11月16日泉州晚报发来感谢信

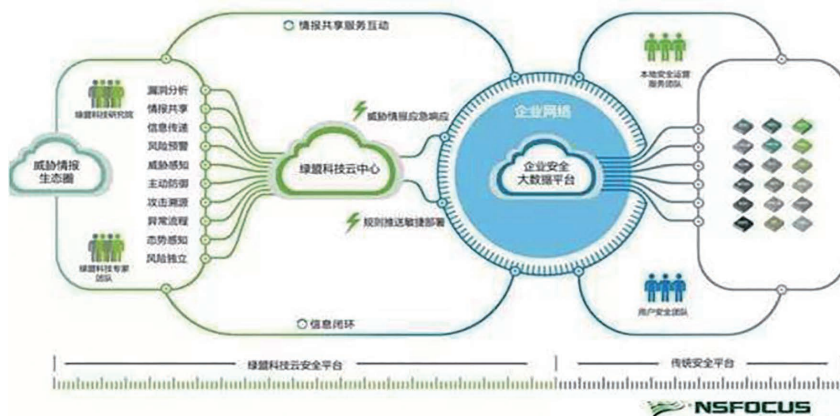
了高度的肯定。

### 关于绿盟科技 P2SO

2014年底绿盟科技提出转型的战略构想，并组建研讨小组针对国际国内的安全技术动向和安全态势进行激烈分析和讨论，提出了公司需从主要提供盒子产品，转变为为客户提供解决方案和安全运营服务。

这个构想经过管理层审议，确定为公司的转型战略，并将其命名为 P2SO。P 即指

产品，S 是 Solution，O 是 Operation。在新的战略下，P 仍是企业安全体系的关键节点，是采集安全数据和执行安全策略的主体。S（解决方案）是指要理解客户的业务场景，针对场景设计相应的能力组合。O（运营）是指在动态的安全生命周期内，建立持续运营体系以改进企业安全态势，并通过协同的方式将绿盟科技的安全能力快速交付给客户。



绿盟科技 P2SO 战略图

绿盟科技提出的 P2SO 战略转型，经过近两年的沉淀，现阶段已经进入落地阶段，P2SO 是以“快速响应”为核心目标建立起来的全方位网络安全防护体系，它并非绿盟安全产品的简单衍生，而是从云端到终端建立起来的 360 度的安全防护战略架构，它将为“互联网+”时代的网络安全提供全方位的保障。

绿盟科技，作为国内安全领域的领导者，16 年来一次又一次为国内及国际的重大活动进行网络安全的护航工作，经过不断的改进和积累，绿盟科技已经打造了从云端到终端的全方位安全防护体系，这也使得客户对绿盟科技的网络安全防御工作愈加信赖。

# 绿盟科技金融行业脆弱性管理平台荣获“2016企业优秀解决方案奖”

12月15日，第七届中国金融业信息化发展论坛暨2016年度金融科技及服务优秀奖颁奖典礼在北京隆重举行。经技术组委会层层选拔，严格根据评选要求审核，在众多优秀企业中，绿盟科技凭借过硬的技术、持续的创新和在金融行业的骄人战绩，以《金融行业脆弱性管理综合解决方案》一举摘得“2016企业优秀解决方案奖”。

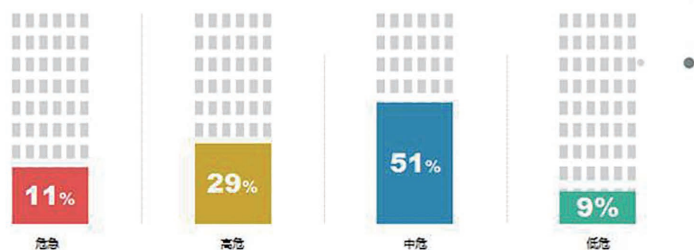
据了解，本次大奖由中国金融学会金融

信息化专业委员会指导，《金融电子化》杂志颁发。会上，绿盟科技安全专家还就该解决方案做了主题演讲，希望可以为更多的行业用户解决漏洞修复难以实现真正闭环的难题。

互联网+时代的到来，人们充分享受新时代科技创新成果便利的同时，万物互联带来的信息安全风险也日渐提高，信息安全事件层出不穷，在资金体系庞大、用户信息集中、安全事件影响深远的金融领域，所面临的安全问题尤为凸显。我们真切的感知到，原有的金融服务模式被颠覆，移动支付、第三方支付、互联网金融等新兴模式异军突起，攻击者的攻击手法和组织方式也更加专业化和更具破坏性，借助互联网上的威胁信息攻击者可以轻易突破企业安全防护手段，直逼用户核心数据，互联网的新兴技术发展向传统的信息防御体系提出了更高的要求。



## 2016年1-11月漏洞情况



CNNVD 信息安全漏洞数据显示，截至2016年11月，2016年的漏洞总数达到了5737个，其中危急漏洞和高危漏洞数量总和为2282个，占比达到40%，安全漏洞形势不容乐观。

新形势下的金融信息安全已经成为目前的重中之重，面对这一迫切需求，信息安全行业专家绿盟科技积极应对，帮助银行、保险等各类企业实现变革，助力金融智能安全运营防线



## 安全形势

的构建，绿盟科技针对金融行业推出的“金融行业脆弱性管理综合解决方案”可以很好的解决这一难题，而且也受到客户、行业的高度认可。

云计算、大数据、区块链等新技术为金融行业的发展注入了新的技术动力，金融行业在运用新技术快速发展的同时，不得不面对一个最直接的安全运维难题，那就是脆弱性管理。从风险管理的角度来看，脆弱性问题是导致风险的内在因素，消除脆弱性是降低风险最直接有效也是最难的手段。

绿盟科技在金融行业安全服务实践中意识到，企业在脆弱性管理中存在以下问题，

### 脆弱性管理现状



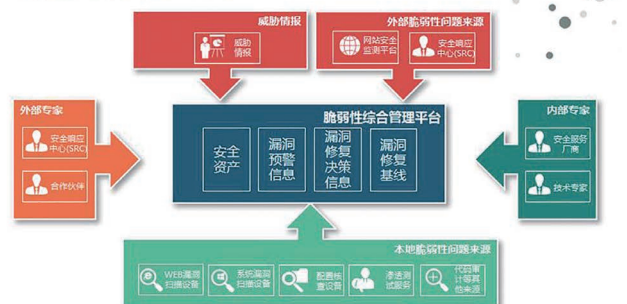
一是重发现、轻修复，无法形成有效的漏洞闭环管理；

二是系统和软件补丁、配置缺陷、应用系统问题、业务逻辑缺陷等脆弱性问题被割裂处理，没有从脆弱性管理的高度进行集中管理；

三是脆弱性问题处置经验未进行总结和积累，安全运维能力提升举步维艰。

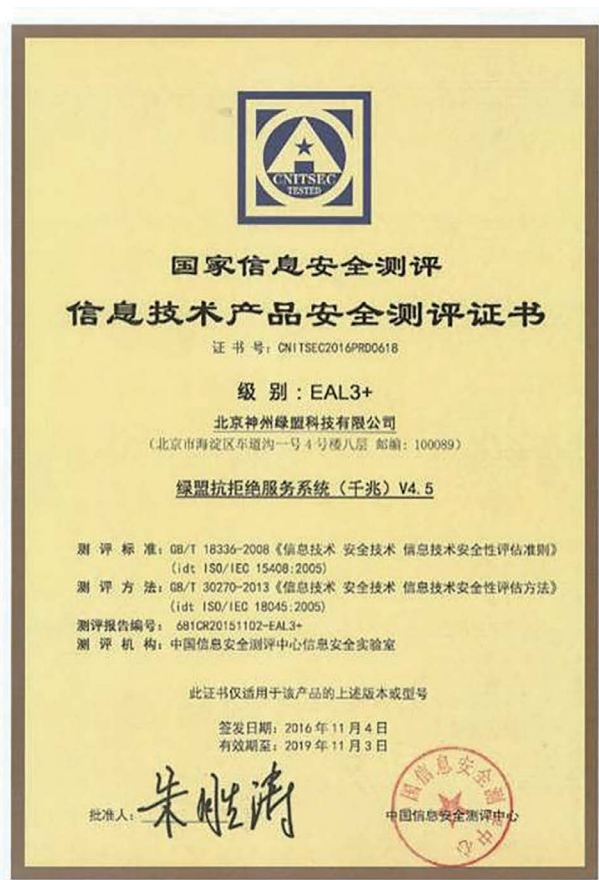
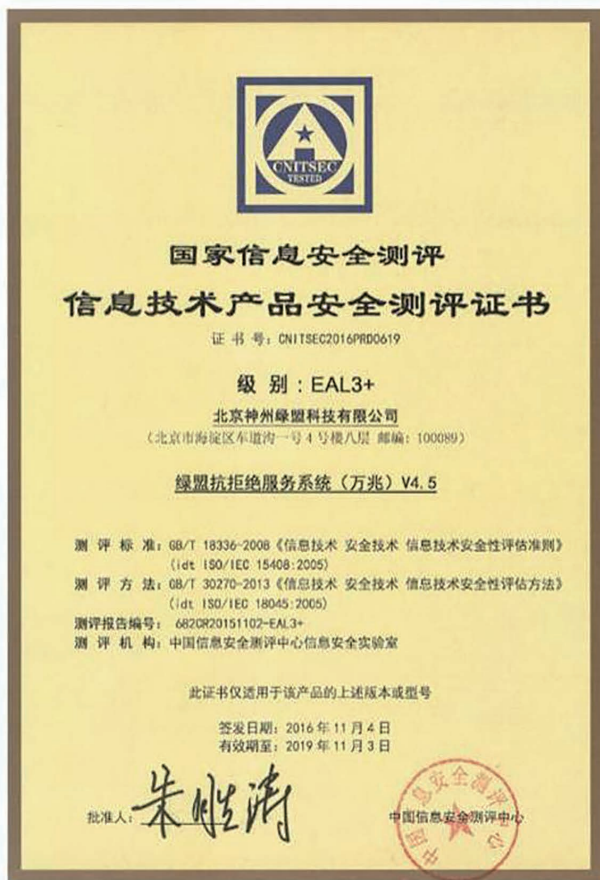
正是基于上述问题，绿盟科技提出从安全的视角重新审视资产，根据业务特性和系统架构等要素建立安全资产信息，借助威胁情报中精确的漏洞预警信息，结合资产的安全特性，为漏洞修复提供决策依据；同时通过脆弱性管理平台，依靠内部专家和外部 SRC 白帽子，对本地 WEB 和系统漏洞信息、渗透测试结果、配置检查结果以及其他相关信息和远程监测漏洞信息进行综合判断，实现漏洞综合、闭环管理，最后通过脆弱性管理知识库的建立，为企业安全基线管理、安全开发管理等运维过程提供参考依据，实现由脆弱性管理带动安全运维能力全面提升的效果，真正解决企业安全运维的实际难题。

### 脆弱性综合管理平台



绿盟科技作为安全领域的领军企业，深耕专注于专业领域，目前已与超过千余家金融机构建立商业合作，为其提供专业的安全产品、服务与解决方案。未来，绿盟科技将继续专注研究，实现技术突破和创新，在网络安全防护、保护关键信息基础设施安全等方面持续发力。

# 【荣誉】绿盟科技ADS获得 国测网络安全产品最高级别 安全证书 “EAL3+”



## 安全形势

近日，绿盟科技拒绝服务系统 ADS 通过中国信息安全测评中心分级评估 EAL3+ 级安全评测和专家验收，并获得《国家信息安全测评 信息技术产品安全测评证书，级别：EAL3+》。

信息安全产品分级评估是指依据国家标准 GB/T18336，综合考虑产品的预期应用环境，通过对信息安全产品的整个生命周期，包括技术、开发、管理、交付等部分进行全面的安全性评估和测试，验证产品的保密性、完整性和可用性程度，确定产品对其预期应用而言是否足够安全，以及在使用中隐含的安全风险是否可以容忍，产品是否满足相应评估保证级的要求。目前，中国信息安全测评中心颁发的网络安全产品分级评估证书的最高级别是 EAL3+。

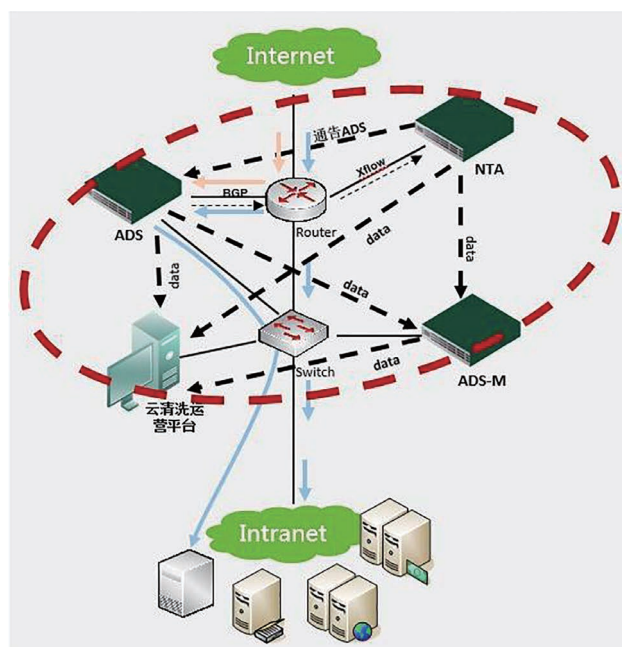
EAL3+ 相比 EAL3，主要是在保障要求上进行了增强：

- 在针对攻击面分析方面，考虑了更多因素，对抗的风险等级由中低风险提升到了中等至中偏高风险；
- 在产品渗透性测试方面，考虑了产品在预期环境下所面临的更多的风险及脆弱性，测试范围及测试深度得到了加强。

现在，信息安全问题日益突出，安全事件屡屡发生。信息安全问题已经成为事关国家政治、经济、社会和国防安全的重大问题。绿盟科技拒绝服务系统（简称 ADS）利用自身先进的攻击检测算法及时发现背景流量中的攻击行为，迅速对攻击流量进行过滤，确保正常业务的可用性。

此外，绿盟拒绝服务系统 ADS 还可以与管理中心 ADS-M、检测设备 NTA 形成三位一体的抗 DDOS 解决方案，帮助客户对 DDOS 攻击事件进行完整追踪，实现高效清洗、简化运维的完整抗

DDOS 解决方案。



此次评估过程针对绿盟 ADS 的安全目标、功能规范、高层设计、配置管理、交付和运行、生命周期支持、脆弱性分析、指导性文档、产品自测文档、独立性测试结果以及穿透性测试结果几个方面进行评估，最终测试结果确认绿盟 ADS 已实现了预期所有的安全功能和产品安全性能等，并满足国测网络安全产品最高级别 EAL3+ 的所有要求。

# 安全意识培养浅谈

总裁办 周博

关键词：员工信息安全意识 网络安全意识 安全意识培养

摘要：笔者长年从事内部安全管理，这几年也做了不少安全意识培养的工作，从中总结了相关工作容易产生的误区及需要关注的重要点，特别是安全意识培养的 6 种常见方法，值得借鉴。正好大家也都在做 2017 年规划，我们也应该思考安全意识培养这方面的工作。

---

## 安全技能、安全意识与安全规定 三个方面不划等号

---

度娘说安全意识就是人们在生产活动中各种各样有可能对自己或他人造成伤害的外在环境条件的一种戒备和警觉的心理状态。当然这句话中所讲的安全意识是广义的安全，可能包括生产安全、交通安全等等，其实用在信息安全意识上也很恰当。

人们在日常工作、生活中可能会遇到各种各样对自己或所在公司

的信息的安全性造成破坏的外部威胁（如附件带勒索病毒的恶意邮件、弱口令等），人们对这种威胁的戒备和警觉的心理状态就是信息安全意识。

安全意识的重要性不言而喻，各种社会工程学攻击、APT 攻击的攻击者们，往往都是利用攻击目标相关人员薄弱的安全意识所导致的漏洞入手，这在安全界好像已经成为共识。具体案例在此就不多讲了，毕竟本文不是安全意识培训文章。

## ▶▶ 安全形势

安全意识与安全技能是有区别的。上面的定义说明了安全意识是一种心理状态，比如收到一封陌生人的邮件，或者莫名其妙的邮件，你如果觉得只觉得很好奇、很紧张、很想打开附件或点击链接看，那你是没有安全意识的，如果你马上警惕起来，想到这可能是一封恶意邮件，想到附件可能有病毒，想到链接后面可能也有病毒或者钓鱼页面，想到你得问问安全管理员，那么说明你是具有安全意识的。

安全技能则是指一些具体的增强安全性的操作，比如基础一些的，设置复杂的密码，配置做无线路由器的安全配置，或者更高深的做渗透测试、代码安全审计。安全意识强的不一定有很强的安全技能，这个很好理解。但安全技能很强的，也不一定有很强的安全意识，这种情况多出现在刚入安全圈的技术新人，技术新人刚开始只在某一方面做深入研究，比如 web 安全，在那一方面一两年后可以达到比较强的境界，但安全意识可不只局限在 web 安全，安全意识涉及到日常工作、生活的各个方面，如移动端、物理安全、邮件安全、WiFi 安全等，职场新人无法

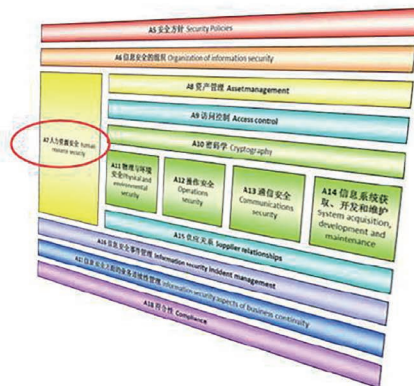
短时间掌握所有方面。安全界大牛就是另一个存在，这里就不涉及了。

安全意识与安全规定有什么关系？这里所谓的安全规定是指公司在信息安全方面制定的规章制度、操作规范。安全意识与安全规定不是可互相替代，而是相辅相成的关系。安全意识足够，就可以理解公司为什么制定相应的安全规定，就能更有主动性去执行安全规定。这就能解释在一个新公司推行安全制度前为何要先进行各种安全意识宣贯培养了，因为如果不这样做，安全制度的推行落地肯定处处碰壁，最后束之高阁。而仅仅具有有安全意识，只能是让大家具有警惕性，有警惕性后该怎么做才安全呢？依据安全规定、利用安全技能去做才安全。

### 安全意识培养的重要方面

通过各种方式使员工具有安全意识的过程就是安全意识培养。安全意识培养在 ISO27001 信息安全管理体系标准中也占据一个独立的控制项，是在附录 A 参考控制目标和控制项 -A7 人力资源安全 -A7.2 任用中 -A7.2.2 信息安全意识教育和培训，足以说明他

- A.5 安全方针
- A.6 信息安全组织
- A.7 人力资源安全
- A.8 资产管理
- A.9 访问控制
- A.10 密码学
- A.11 物理与环境安全
- A.12 操作安全
- A.13 通信安全
- A.14 信息系统获取、开发和维护
- A.15 供应关系
- A.16 信息安全事件管理
- A.17 信息安全方面的业务连续性管理
- A.18 符合性



图一：ISO 27001:2013 附录 A 控制领域结构

的重要程度。

具体的控制要求是这样描述的：组织内所有员工、相关合同人员及第三方人员应接受适当的意识培训，并定期更新与他们工作相关的组织策略及程序。从这个控制要求中，我们可以获取两个重要信息：

1. 不只是内部。安全意识培养的目标不仅是公司内员工，还包括与公司签订服务合同的人员以及与公司业务相关的第三方人员，比如外包的工程服务人员、保洁、供货商等，这些角色也同样可能接触到一些公司敏感信息或拥有一些特殊权限。我们在做安全意识培养时经常只关注公司内员工，后两者可能会遗漏，那么在做安全规划时可以着重考虑。

2. 规范要培训。定期更新与他们工作相关的组织策略及程序，就是指工作相关的安全规定、规范也要定期培训。虽然上面说安全意识与安全规定是不同的东西，但这两者都需要员工掌握，所以可以合并在一起进行培养。

### 为什么说“培养”而不是“培训”

这是因为安全意识不是简单一次两次培训就能提升的，它需要一个较长的时期适当利用各种方式来提升，所以用“培养”更为贴切些。

安全意识培养的几种方式：

#### 培训

虽然培训的效果往往不能达到预期，但仍然是一种重要的培养



图二：安全意识培养方式

手段，特别是对于新员工来讲，培训起到了一种师傅领进门、提纲挈领的效果。安全意识培训可以有如下几种：

A. 一批新员工集中入职时的集中培训：时长在 30-60 分钟，让新员工快速了解到基本的安全意识以及哪些方面可能会有风险，或者哪些方面公司可能会有要求，我在哪里可以找到一些学习资料，有不懂得可以向谁询问等。

B. 部门、业务线、事业部季度例会时的安全宣讲：时长 15 分钟左右，主要讲近期的一些安全事件、态势，以及公司安全制度的更新、安全管理情况的报告等。

#### 自学、考试及等级管理

这三种方式本可以分开，这里放在一起讲说明它们不可分割。只要求考试而未要求自学并给出自学资料，则是犯了舍本逐末的错误。我们的目标还是要求员工通过自学掌握相关内容。只给出自学资料要

求自学，而不设置考试，则无法调动员工学习的意愿。而考试后如果没有根据考试分数设定不同的管理措施，让没有认真学习的员工感受到不同的待遇，则无法真正调动员工学习的积极性。具体方式建议如下：

A. 考试：每年一次全员统考，每月一次新员工及重定级考试。题库是从之前各种文章、通告、安全规定中提取，题型为客观题，且至少每年更新一部分。至于开卷 / 闭卷、纸质 / 在线则各有各的优点，可以根据具体情况选择。

B. 自学：每次考试前一个月邮件通知本次考试对象，并发送考试大纲以及学习资料。一个月的时间足够员工合理安排学习时间，且不至于压力太大产生抵触情绪。

C. 等级管理：根据不同的分数划定不同等级，进而实施不同的措施。措施以提高安全意识为目的，比如必须参加一次培训、必须写指定主题的安全意识文章等，如果不执行则通报批评。员工可以继续学习并参加两个月后的重定级考试来提升等级。

### 文章推送

安全意识涉及内容具有范围广、更新快、

难度低的特点。前两个特点决定了仅用一次培训和自学肯定无法达到理想的效果。难度低则使我们利用一小段文字讲明白一个意识点成为可能。因此，日常频率比较高的安全意识短文推送方式能够适应这三个特点。具体方式建议如下：

A. 文章内容：每次一个安全意识点，最好以安全事件引入，然后进行事件分析，最后给出切实可行易行的安全操作建议。最忌讳仅给出“一定要谨慎、小心”之类建议，一方面有水文嫌疑，影响今后阅读量，另一方面对读者也起不到实际的帮助。

B. 文章来源：从网上直接抓取可以，但一方面有可信度和时效性的问题，另一方面网上这类文章更新速度不足以支撑我们的推送频率。最好是安全管理相关人员根据公司特点以及近期安全态势自己写。

C. 推送平台及频率：邮件、内部即时通讯、微信企业号等可以直达员工阅读终端的都可以作为平台。频率在每周一次左右为宜，过多容易造成反感。可以根据后台统计的阅读量来调整频率或内容。实际的经验是跟现在朋友圈转发一样，文章标题对阅读量提升

很重要，但标题党一定要适当使用，安全管理还是要务实。

### 实时通告

文章推送不能过于频繁的原因还有一个，就是要给我们的安全意识培养杀手锏之一 - 实时通告流出档期和关注度。实时通告是指利用正式的公司内部通告方式（比如全员邮件），对近日内部发生的安全事件，或者外界已经发生且很可能在内部发生的安全案例进行通告，提醒全员注意，并提示一些预防措施。实际操作过程中，这类通告发出后会收到不少员工反馈或询问，说明这种方式员工关注度很高。不过这种方式需要适当、谨慎利用，一个季度 2 次左右即可。

### 安全意识测试

如同对 WEB 的渗透测试是模拟真实攻击方式来发现 WEB 漏洞，安全意识测试则是模拟真实的攻击方式来发现安全意识方面的薄弱环节。测试方式有很多种，以下举几个例子来开阔一下思路：

A. 请一个刚入职的新员工不拿工卡和门禁卡，尝试从公司外进入其他楼层办公区，看能否成功进入且拿走一些员工办公桌上的

文件。

B. 模拟公司邮箱管理员给某些员工发一封邮件，提示你的外网邮箱在异地登录，请立刻提供原密码并重置密码。

这种测试的结果在告知当事员工后能够对其留下极其深刻的印象，进而带动提高其周围人员的安全意识，所以这种安全意识测试的方式也可以作为安全意识培养的杀手锏之一。如果将这种测试作为定期或不定期的例行抽测，测试结果纳入员工或部门考核，就可以对员工日常的安全警惕性起到一定的加强作用。

### 其他培养方式

绿盟科技每两年会组织相关资源做一次安全意识漫画，以台历或手册的形式发给大家，最近正在做《安全意识漫谈》手册，其中涵盖了6个板块30多个漫画形式的案例，每个都配有案例解析和安全建议，并总结了7个安全意识口诀，目的是希望通过简单、轻松的方式让员工从案例中学习。

另外还有一些方式虽然主要目的不在安全意识，但也能对安全意识培养起到一定作用，比如检查员工电脑合规性的安全检查，检查的过程也是讲解相应风险点、提高安全意识的过程。有的公司每年举办安全意识宣传周，利用讲座、知识竞赛等方式来培养公司安全文化、提升员工安全意识和安全技能。

### 安全意识培养体系建设思路

安全意识培养体系是随着公司整个安全管理体系的建设而同步发展的。安全管理体系不在本文讨论范围之内，下面简单整理了一

个安全意识培养体系建设的阶段，或者说是一个成熟度模型吧，希望对甲方安全管理人员的信息安全规划有所帮助：



图三：安全意识培养体系成熟度模型

1. 原始阶段：以实时通告为主。没有安全管理体系，出现安全事件就通告全员，依次引起大家重视。
2. 起步阶段：开始各种安全培训。开始建立安全管理体系，有了安全意识和安全规定的培训。
3. 运营阶段：建立以自学、考试和分级管理为基础的安全等级管理体系。随着安全管理体系的不断发展和完善，安全意识培养工作也逐步规范化和量化并开始运营。
4. 改进阶段：以定期安全意识测试和安全文章推送为代表。安全管理者开始对安全意识培养工作查漏补缺，开始寻求新的方式来测量和增强员工的安全意识。

经验有限，仅供参考，欢迎交流！



# 网络安全威胁月报 201612

威胁情报与网络安全实验室 陈颐欢



关键词：高危漏洞 DDoS 攻击事件 安全会议 绿盟科技漏洞库 绿盟科技博客

摘要：绿盟科技网络安全威胁周报及月报系列，旨在简单而快速有效的传递安全威胁态势，呈现重点安全漏洞、安全事件、安全技术。获取最新的威胁月报，请访问绿盟科技博客 <http://blog.nsfocus.net/>

## 一、2016年12月数据统计

### 1.1 高危漏洞发展趋势

2016年12月绿盟科技安全漏洞库共收录159个漏洞，其中高危漏洞107个。相比11月份的高危漏洞数量基本持平。

### 1.2 互联网安全漏洞

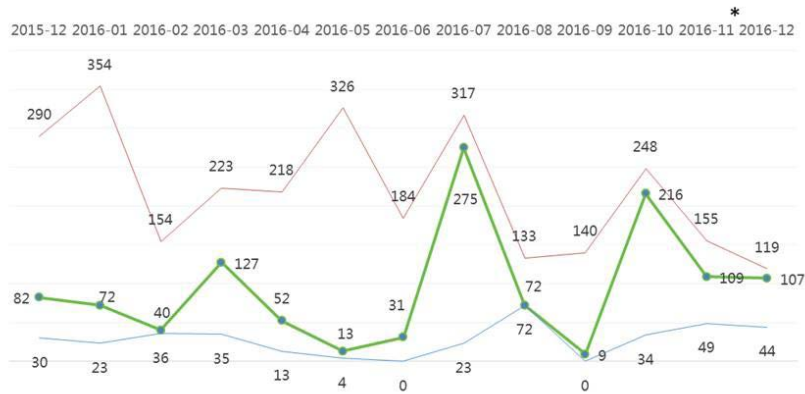
#### OpenSSH 远程代码执行漏洞

来源：<http://blog.nsfocus.net/openssh-remote-code-execution-vul/>

简述：2016年12月19日，OpenSSH官网发布了一个OpenSSH的版本更新，在新版本中修复了编号为CVE-2016-10009

绿盟科技漏洞库公布高危漏洞统计 2016.12

下图展示了2016年12月及过往12个月的高危漏洞公布情况对比



\* 数据来源：绿盟科技威胁情报与网络安全实验室，本表数据截止到2016.12.26

的漏洞。该漏洞允许攻击者在运行 ssh-agent(该程序通常运行在客户端)的机器上加载一个恶意模块 PKCS#11 从而使攻击者有机会执行远程代码。相关链接地址如下：<http://www.openssh.com/txt/release-7.4>

### Firefox 跨域设置 cookie 漏洞

---

来源：<http://blog.nsfocus.net/firefox-cross-domain-settings-cookie-vulnerability/>

简述：2016 年 12 月 6 日，insert-script.blogspot.gr 网站发布了一条关于 Firefox 跨域设置 cookie 的消息，该漏洞的成因是火狐浏览器允许元标签对浏览器 cookie 进行设置。成功利用该漏洞会使得目标用户在跳转到恶意站点之后，对用户浏览器中的 cookie 进行设置。相关链接地址如下：<https://insert-script.blogspot.gr/2016/12/firefox-svg-cross-domain-cookie.html>。

### Firefox 远程代码执行漏洞

---

来源：<http://blog.nsfocus.net/analysis-protection-firefox-vulnerability/>

简述：火狐浏览器上暴露出一个 JavaScript 0Day 漏洞 CVE-2016-9079，而且已经被用于攻击 Tor 用户。

### Roundcube 命令执行漏洞

---

来源：<http://blog.nsfocus.net/roundcube-command-execution-vulnerability/>

简述：2016 年 12 月 6 日(当地时间)，blog.ripstech.com 网站发布了一条关于 Roundcube 远程命令执行漏洞的消息。在

Roundcube1.2.2 及其以前的版本中，deliver\_message() 函数在调用 PHP 内建函数 mail() 时的第 5 个参数可由用户控制且未经恰当过滤，mail() 函数被调用后会使得 PHP 执行 sendmail 程序，而未经过滤的第 5 个参数允许对 sendmail 程序进行配置，从而使得 sendmail 程序将邮件流量保存在文件中，攻击者可以利用这个机制通过发送邮件将恶意 PHP 文件写入 webroot 目录。

### Apache HTTPD 拒绝服务漏洞

---

来源：<http://blog.nsfocus.net/apache-httpd-denial-service-vulnerability-notification/>

简述：2016 年 12 月 5 日(当地时间)，seclists.org 网站发布了一条关于 Apache 网页服务器拒绝服务漏洞的消息，漏洞编号为 CNNVD-201612-069。该漏洞存在于 mod\_http2 模块中，这是从 Apache HTTPD 2.4.17 版本开始引入的关于 HTTP/2 协议的模块。然而该模块在默认情况下不被编译，且默认不启用，该漏洞只影响使用 HTTP/2 协议的用户。在使用 HTTP/2 协议的服务器上，攻击者可以通过发送精心构造的请求，导致服务器内存耗尽，造成拒绝服务。

### ImageMagick 压缩 TIFF 图片远程代码执行漏洞

---

来源：<http://blog.nsfocus.net/imagemagick-remote-code-vulnerability/>

简述：2016 年 12 月 3 日，talosintelligence.com 网站发布了一条关于 ImageMagick 远程代码执行漏洞的消息，漏洞编号为 CVE-2016-8707。ImageMagick 在压缩 TIFF 图片时存在可利用

## ▶▶ 安全形势

的内存越界写入问题，在特别情况下该问题会造成远程代码执行。相关链接地址如下：<http://www.talosintelligence.com/reports/TALOS-2016-0216/>。

Crane 恶意代码样本

来源：<http://blog.nsfocus.net/analysis-protection-scheme-crane-code-samples/>

简述：2016年11月出现了一个针对俄罗斯工业部门的恶意代码Crane。该Windows木马被安全公司命名为BackDoor.Crane.1。其主要功能包括获取受害者计算机内的文件列表并窃取文件；通过连接远程服务器下载并执行恶意代码；实施文件上传、配置文件更新、命令执行等操作。

(来源：绿盟科技威胁情报与网络安全实验室)

### 1.3 绿盟科技漏洞库十大漏洞

NSFOCUS 2016年12之十大安全漏洞

声明：本十大安全漏洞由NSFOCUS(绿盟科技)安全小组<[security@nsfocus.com](mailto:security@nsfocus.com)>根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。

[http://www.nsfocus.net/index.php?act=sec\\_bug&do=top\\_ten](http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten)

1. 2016-12-02 Mozilla Firefox 释放后重用远程代码执行漏洞 (CVE-2016-9079)

NSFOCUS ID: 35513

链接：<http://www.nsfocus.net/vulndb/35513>

综述：Mozilla Firefox是一个开源网页浏览器，使用Gecko引擎。Firefox在实现上存在SVG Animation 模块释放后重用(UAF)漏洞。

危害：远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞，从而控制受害者系统

2. 2016-12-14 Microsoft Windows Graphics 组件远程代码执行漏洞 (CVE-2016-7273)(MS16-146)

NSFOCUS ID: 35581

链接：<http://www.nsfocus.net/vulndb/35581>

综述：Microsoft Windows是流行的计算机操作系统。Windows Graphics 组件处理内存对象方式中存在远程代码执行漏洞，可使攻击者控制受影响系统。

危害：本地攻击者可以利用此漏洞来提升权限，对系统进行非授权的访问

3. 2016-12-16 Adobe Flash Player 远程代码执行漏洞 (CVE-2016-7872)(APSB16-39)

NSFOCUS ID: 35622

链接：<http://www.nsfocus.net/vulndb/35622>

综述：Flash Player是多媒体程序播放器。Adobe Flash Player在MovieClip类中存在释放后重用漏洞。

危害：攻击者可以通过诱使受害者打开恶意swf文件来利用此漏洞，从而控制受害者系统

4. 2016-12-14 Microsoft Edge 远程内存破坏漏洞 (CVE-2016-7296)(MS16-145)

NSFOCUS ID: 35575

链接 :<http://www.nsfocus.net/vulndb/35575>

综述 :Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。Edge 处理内存对象时脚本引擎呈现方式中存在多个远程代码执行漏洞。

危害 : 远程攻击者可以通过诱使受害者打开恶意网页来利用此漏洞, 从而控制受害者系统

5. 2016-12-09 Roundcube steps/mail/sendmail.inc 任意代码执行漏洞 (CVE-2016-9920)

NSFOCUS ID: 35551

链接 :<http://www.nsfocus.net/vulndb/35551>

综述 :RoundCube Webmail 是一个基于浏览器的 IMAP 客户端。Roundcube 未配置 SMTP 服务器且启用 sendmail 程序后, steps/mail/sendmail.inc 未正确

使用 sendmail 命令行上的自定义发件人地址, 可使远程用户通过修改的 HTTP 请求, 执行任意代码。

危害 : 远程攻击者可以利用这些漏洞修改的 HTTP 请求, 执行任意代码

6. 2016-12-12 phpMyAdmin BBCode 注入漏洞 (CVE-2016-9862)

NSFOCUS ID: 35558

链接 :<http://www.nsfocus.net/vulndb/35558>

综述 :phpmyadmin 是 MySQL 数据库的在线管理工具。phpMyAdmin 4.6.x 版本存在安全漏洞。可使攻击者通过构造的登录请求, 在登录页注入 BBCode。

危害 : 攻击者可以利用此漏洞获取敏感信息, 劫持用户会话

7. 2016-11-28 NTP 拒绝服务漏洞 (CVE-2016-9312)

NSFOCUS ID: 35472

链接 :<http://www.nsfocus.net/vulndb/35472>

综述 :Network Time Protocol (NTP) 是用来使计算机时间同步化的一种协议。Windows 平台上, ntp-4.2.8p9 之前版本在接收过大的 UDP 数据包时会停止工作, 导致拒绝服务。

危害 : 远程攻击者可以通过向服务器发送恶意请求来利用此漏洞, 导致拒绝服务

8. 2016-12-07 Tesla Gateway ECU 命令注入漏洞 (CVE-2016-9337)

NSFOCUS ID: 35544

链接 :<http://www.nsfocus.net/vulndb/35544>

综述 :Tesla Gateway ECU 是汽车软件及驾驶功能管理固件。Tesla Gateway ECU 存在命令注入漏洞, 可使攻击者发送消息到车辆 CAN 总线系统。

危害 : 远程攻击者可以利用这些漏洞控制受害者系统

9. 2016-12-09 Linux kernel 权限提升漏洞 (CVE-2015-8967)

NSFOCUS ID: 35549

链接 :<http://www.nsfocus.net/vulndb/35549>

## 安全形势

综述:Linux Kernel是Linux操作系统的内核。Linux kernel < 4.0 版本 arch/arm64/kernel/sys.c 存在安全漏洞。

危害:攻击者可以绕过 "strict page permissions" 保护机制,修改系统调用表,获取提升的权限

10. 2016-12-01 OpenSSL Montgomery 乘法运算错误漏洞 (CVE-2016-7055)

NSFOCUS ID: 35512

链接 :<http://www.nsfocus.net/vulndb/35512>

综述:OpenSSL是一种开放源码的SSL实现,用来实现网络通信的高强度加密。OpenSSL 1.1.0 版本, Broadwell-specificMontgomery 乘法运算在处理可整除的、大于256位的输

入长度时存在运载传播 bug, 导致结果错误。

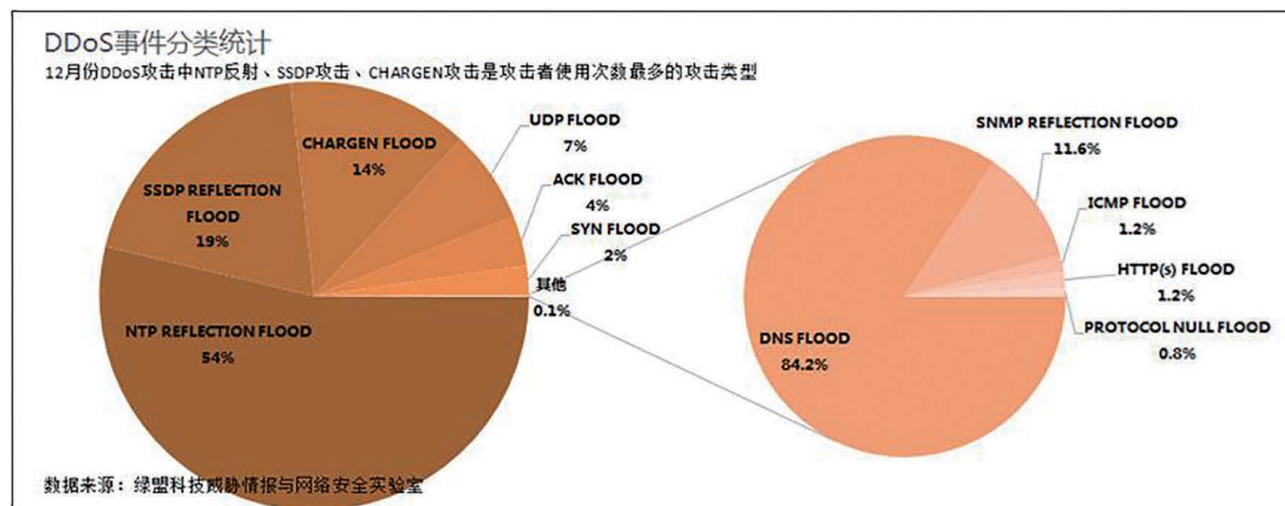
危害:攻击者可以利用此漏洞来导致拒绝服务。

(来源:绿盟科技威胁情报与网络安全实验室)

### 1.4 DDoS 攻击类型

12月份绿盟科技科技威胁情报及网络安全实验室收集及梳理了超过10.1万次攻击,与11月份相比,攻击次数有所下降,在这个月的攻击类型中,最常见的类型仍然是,SSDP,NTP,CHARGEN,UDP,ACK,SYN这几种,但比例有所变化,其中CHARGEN和SSDP攻击的比例明显上升。另外观测到少量的SNMP反射攻击。

小提示



•Chargen Flood: Chargen 字符发生器协议(Character Generator Protocol) 是一种简单网络协议, 设计的目的是用来调试 TCP 或 UDP 协议程序、测量连接的带宽或进行 QoS 的微调等。但这个协议并没有严格的访问控制和流量控制机制。流量放大程度在不同的操作系统上有所不同。有记录称, 这种攻击类型最大放大倍数是 358.8 倍。

•NTP Flood: 又称 NTP Reply Flood Attack, 是一种利用网络中时间服务器的脆弱性(无认证, 不等价数据交换, UDP 协议), 来进行 DDoS 行为的攻击类型。有记录称, 这种攻击类型最大放大倍数是 556.9 倍。

•SSDP Flood: 智能设备普遍采用 UPnP (即插即用) 协议作为网络通讯协议, 而 UPnP 设备的相互发现及感知是通过 SSDP 协议(简单服务发现协议)进行的。

攻击者伪造了发现请求, 伪装受害者 IP 地址向互联网上大量的智能设备发起 SSDP 请求, 结果受害者就收到了大量智能设备返回的数据, 被攻击了。有记录称, 这种攻击类型最大放大倍数是 30.8 倍。

更多相关信息, 请关注绿盟科技 DDoS 威胁报告。

---

## 二. 博客精选

---

### 物联网安全综述白皮书

---

这份白皮书展开描述了物联网安全的三个细分领域, 工业控制、智能汽车、智能家居, 列出了六点需要重点关注的方面, 包括物联网安全网关、应用层的物联网安全服务、漏洞挖掘研究、物联网僵尸

网络研究、区块链技术、物联网设备安全设计, 并深入探讨了物联网安全需求及对策, 物联网安全相关技术, 物联网安全公司及产品介绍等内容。

<http://blog.nsfocus.net/white-paper-security/>

### 看见到洞见之引子

---

《看见到洞见》系列文章汇聚、分享的是绿盟科技创新中心对于数据分析在安全领域应用的技战术思考与经验, 力求由浅入深层次递进, 实战到方法论双线剖析。此文为系列文章之引子第二篇, 深入浅出的对常用的数据分析和机器学习的算法进行介绍。

<http://blog.nsfocus.net/machine-learning-algorithm1/>

<http://blog.nsfocus.net/machine-learning-algorithm2/>

### 2016 年第三季度 DDoS 态势报告

---

据绿盟科技全球 DDoS 态势感知平台监控数据分析显示, Q3 发生 DDoS 攻击次数增加, 小流量攻击占比增加, 攻击手段呈现复杂化, 总体攻击态势依然严峻。

<http://blog.nsfocus.net/nsfocus-2016-q3-ddos-situation-report/>

### 2016 年上半年中国网站安全报告

---

2016 年 11 月 16 日, 中国电信股份有限公司北京研究院(以下简称“中国电信北研院”)联合绿盟科技等, 在北京发布“2016 年上半年网站安全报告”, 本文对报告内容进行生动解读, 大家可以当段子看。报告全文下载见文末。《2016 年上半年网站安全报告》主要内容。

# 关于安全服务模型的一些思考

创新中心 江国龙 刘文懋

关键词：云计算 安全交付服务 SECaaS

摘要：本文从为人们所熟知的云计算出发，类比云计算服务模式所带来的种种好处，提出一些安全服务提供方式的思路。希望能够借鉴云计算模式的优势，使安全防护能够更方便、更有效的为用户提供服务。

## 1. 概述

云计算的发展，可以说是信息技术领域的一次革命。以计算、存储、网络虚拟化等技术为依托，将所有的 IT 资源虚拟化，形成资源池，通过云计算管理平台，统一为用户提供所需的服务。这样用户在使用相应的服务时，可以像使用传统的水、电、燃气一样，按需购买，按需付费，而避免了复杂的配置、管理和运维。

云计算的主要模式就是把各种资源以服务的方式提供给客户，它的服务模型形成了“xxx-as-a-Service”的范式，通常包含三种具体的模型：基础设施即服务 (Infrastructure as a Service,

IaaS)、平台即服务 (Platform-as-a-Service, PaaS)、软件即服务 (Software-as-a-Service, SaaS)。其中 IaaS 模式为云用户提供所需的计算、存储等基础设施服务，PaaS 模式基于底层的基础设施资源，为用户提供应用程序的可运行环境，SaaS 则是基于底层的基础设施资源和程序执行环境，为用户提供云应用软件。

从云计算的定义和其服务模式来看，云计算有着以下特点：

**按需自助服务**：用户可以根据自己的实际需求，获取相应的服务资源。

**广泛的网络访问**：云平台通过网络连接为用户提供服务，用户可

以通过 PC 客户端、移动客户端等多种方式进行接入管理。

**资源池化**：云服务商依托虚拟化技术，将各种的 IT 资源汇聚到资源池内，采用多租户的模式，按照不同的用户需求将资源池内相应的 IT 资源分配给对应用户进行使用。

**快速弹性化**：云计算平台能够根据用户对资源的需求情况，快速的进行资源的动态划分，使用户的资源能够做到弹性的扩容和收缩，保障用户业务的高效、稳定运行。

**可度量**：云计算之所以能够按需提供服务，其主要依赖于所提供服务能够进行有效度量，用户可以根据自身使用量进行付费。

从云计算的上述特点我们可以总结出云计算所带来的好处：

**快速提供服务**：对于像 IaaS 这类服务，用户在云平台浏览、购买云主机等相应资源，只需轻松几步，便可以将基础设施平台搭建完毕，避免了传统的服务器采购、服务器组装、系统安装、机房建设、网络规划等，成本大大缩减。对于像 SaaS、IaaS 这类的服务，更是购买完成后，可直接使用，无论是从成本和复杂度来看，均有着不小的诱惑。

**弹性扩容**：一方面，从用户的角度来看，用户所拥有的资源可以进行弹性的申请和释放，资源操作更加的方便灵活。另一方面，从云服务商角度来看，云计算的这种资源池化的方式，可以方便的进行资源的扩容与收缩，保证用户的服务质量。

**成本低廉**：一方面，资源按需购买、随买随用，使资源利用率实现了最大化。另一方面，人力成本大大缩减，减少了复杂了购买流程、硬件安装部署流程以及硬件运维成本。

**高可用**：依托于虚拟化等技术的优势，通过云计算平台对虚拟机进行监控，并且可以提供多种服务高可用保障。

**可移植**：虚拟机迁移、虚拟机复制等均可以做到业务的服务高效、快速移植。

那么回到安全的主题，在安全领域，我们传统的防火墙、IDS、IPS、WAF 等通过在用户数据中心的部署，为用户机房内的业务提供访问控制、入侵检测、入侵防御等安全服务。从上述云计算所带来的种种好处中，我们惊喜的发现，这些好处同样是安全防护中所迫切需要的。比如：

**快速提供服务**。在安全防护方面，“快”绝对是用户永恒的追求，各大公司在安全应急响应上均有着很大的一笔支出进行支持。一般的大规模安全事件或者高危的安全漏洞爆出后，通常需要安全防护能够快速地进行响应，将恶意的攻击进行有效的防护。此时分分秒秒就能够影响到巨大的经济利益。

然而现有的安全产品交付过程，需要经过销售、售前的沟通，确定部署方案、产品规格、配置，然后下单生产，数周或数月收到货之后，安全厂商安排工程实施人员进行部署、调试，完成安全服务的交付。这个交付周期对于快速响应、快速防御来说，通常是很难接受的。

**弹性扩容**。随着互联网尤其是电子商务的发展，高并发、突发的访问流量逐渐成为了一种常态。例如每年的双十一，每分钟几百万甚至上千万的并发访问，其正常流量无异于一次拒绝服务攻击，如果在这些正常流量中再掺杂着各种各样的攻击流量，那么如何保证在



用户访问流量骤增的情形下，安全防护仍然能够有效的进行，安全防护能力不会因为大规模的并发流量而有所削减，成为了用户对安全产品服务的重要要求。

在安全防护设备中，有着很大一部分是属于网关类的设备，通常是单台串接或者旁路部署在用户业务流量中，一旦流量剧增，将会直接影响安全设备的性能，甚至安全设备会直接成为故障点，造成网络中断。如果购买大量的硬件安全设备，来抵御双十一这种突发的大流量安全防护，那么双十一结束之后，将会有很多的设备被闲置，造成了成本的巨大浪费。因此如何保证安全服务的提供能够做到按需服务，弹性扩容和收缩，也是安全用户所希望的。

**成本低廉。**任何用户在考虑购买产品或服务时，都会想要花最少的钱，获取质量最高的产品。当然这个成本不单单是指产品标注的价格，还包括用户在使用过程中所投入的人力成本。

传统的硬件安全设备，其价格成本通常都不低，而且其部署、维护、使用又需要有一定的安全背景的专门安全运维人员进行操作。安全厂商还要对设备进行故障维护、系统升级等，各种成本累积起来会发现，开销是一个不小的数字。

**高可用。**对于串联到用户业务网络内的防护服务，其高可用是最基本的需求，不能因为安全设备的引入，而成为业务网络的一个新的故障点。当前的网关类安全设备，通常都是单机串联的部署方式，对于上文弹性扩容中提及的问题以及设备故障，都会影响用户的业务网络。

由此可见，云计算所带来的种种优势，恰恰也同样是安全服务

领域里所需要的，那么可否参考云计算的模式，来为用户提供相应的安全服务呢。

## 2. 安全服务交付新模式—SECaaS

云计算的服务模式形成了“xxx-as-a-Service”的范式，在安全领域同样可以采用这样的范式来提供服务，保证安全服务也具有上述提及的种种好处。因此我们可以将安全资源进行云化，形成安全云，安全云为用户提供各种各样的安全服务，通常我们将其称作SECaaS (SECurity as a Service)。

类比企业部署云计算的模式，企业部署安全云同样也可以有三大类：**公有安全云、私有安全云和混合安全云。**

公有安全云即安全厂商提供的公众安全服务平台，理论上任何注册用户都可以接入该平台，获取相应的安全服务；

私有安全云即安全厂商在企业内部建设的专有安全云，由于其部署位置的优势，通常这种部署方式性能会更好，当然成本也更高；

混合安全云就是同时提供公有安全云和私有安全云两种服务类型的安全云建设方式，比如某大型企业，为了保证其自身安全防护的质量，在其自己的数据中心建设了私有安全云，同时将其中的部分安全服务对外提供给其它中小用户。由于混合安全云中集成了公有安全云和私有安全云的特性，因此也就不再针对这种部署模式进行赘述。

在用户获取安全服务层面看，SECaaS 具体也可以分为三种形态：**SaaS 化的安全服务、PaaS 化的安全服务和 IaaS 化的安全服务。**

## 2.1. SaaS 化的安全服务

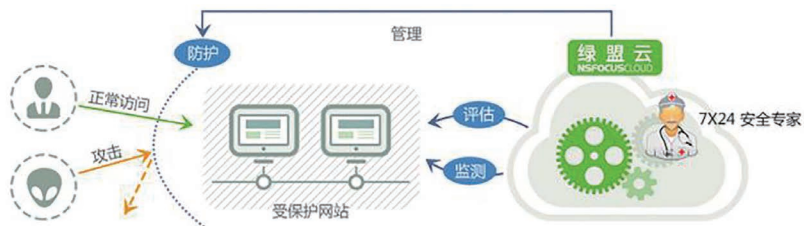
SaaS 化的安全服务是指用户可以直接从云端获取相应的安全服务，而无需安装部署任何设备。就像用户可以直接使用云端的邮件服务、文档管理服务一样，用户也可以直接使用云上的安全服务。

从安全云的部署形态来看，SaaS 化的安全服务又可以分为公有安全云的 SaaS 服务和私有安全云的 SaaS 服务两类。由于安全服务在流量上的特殊性，这两种 SaaS 安全服务之间还是有一定的区别的。

### 公有安全云 SaaS 服务

通常公有安全云的 SaaS 服务主要以非网关类的安全服务居多，比如网站安全评估、网站安全监测、文档安全服务等。因为对于公有安全云，所有提供服务的安全设备均部署在安全厂商的云端，那么网关类的安全服务就需要所有的访问流量都先进入云端设备，云端对其进行清洗后，再将其发往正常的目的地址，这通常对安全云端的带宽等有较高的要求。

如下图所示的绿盟云网站安全 SaaS 解决方案，通过绿盟云提供的 7\*24 小时安全服务，



全面的扫描受保护网站的主机漏洞和 Web 漏洞，以及各种的网页挂马检测、篡改检测以及敏感内容检测。一旦发现问题，将第一时间向用户进行通知确认，并且云端安全专家还会提

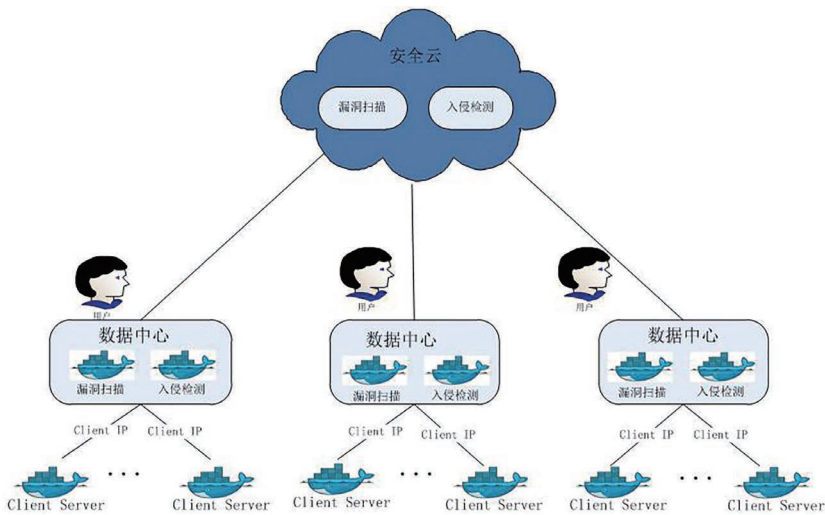
供更深入精准的咨询服务。

那么如果采用公有安全云的方式，是否其流量问题就是不可解决的呢？答案当然是否定的。从上文描述可以看出，上文所述的公有安全云服务的所有服务实施体均在安全厂商的安全云上，安全云与用户的业务网络之间跨越了广域网，所以才会产生所谓的流量带宽的问题。那么如果公有安全云提供的安全服务，其具体实施体在用户侧，这样的带宽问题就不存在了。

参考移动客户端的各种应用提供方式，我们的安全云 SaaS 服务也可以采用类似的方式，比如云端提供各种安全服务的应用商店，而非直接的安全服务，用户购买应用后，云端会将该应用与其对应的服务实体下载到用户数据中心本地，所有的安全防护服务均在业务网络本地进行实施，而云端仅仅是提供服务、购买服务的功能。其示意图如下图所示。

### 私有安全云 SaaS 服务

私有安全云由于其部署运行在用户侧的数据中心，因此理论上可以提供所有类型的 SaaS 安全服务。通常其方案架构如下图

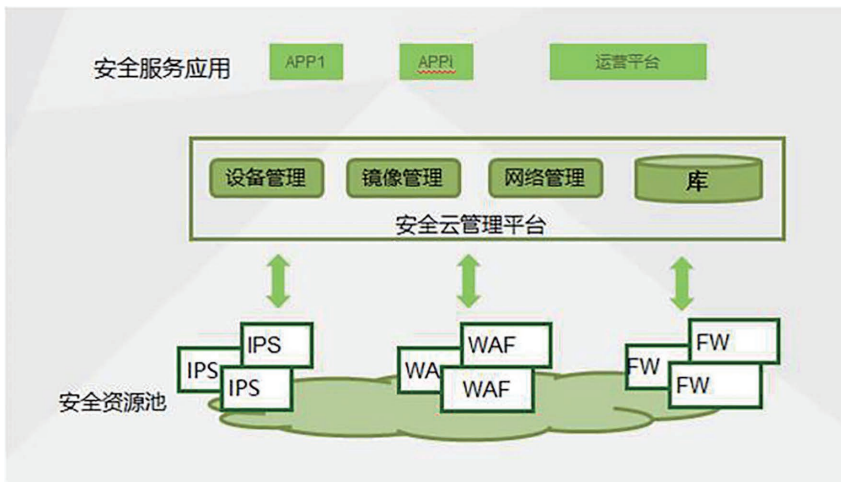


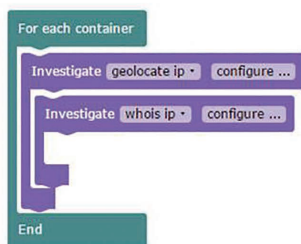
所示，该私有安全云主要由安全资源池、安全云管理平台和安全管理应用三大部分组成。用户通过安全应用获取对应的安全服务。该种服务模式的细节，可以参见《Security Fabric：软件定义的弹性安全云》一文。

这里安全服务应用的获取方式，既可以是安全云厂商提供的标准应用，也可以是用户自己根据云安全管理平台提供的接口设计编写的应用，还可以参照上文中提到安全应用商店，在私有安全云中进行部署，以实现安全服务的获取方式。

## 2.2、PaaS 化的安全服务

PaaS 化的安全服务和云计算的 PaaS 模型在概念上略有不同，通常意义上云计算的 PaaS 是指为用户提供编程环境。安全云的 PaaS 服务应该是指，云端可以为用户提供多种安全服务自动化编排的环境，用户在购买了 PaaS 化的安全服务后，云端会提供相应的编程模型、编程接口以及相关的安全服务能力，用户根据自身的需求，采用最简洁的脚本形式，形成安全服务的自动化编排，以应对复杂多变的攻击方式。比如 RSA2016 创新沙盒产品 Phantom，就可以





```
1 import phantom.rules as phantom
2 import json
3
4 def geolocate_ip_cb(action, success, container, results, handle):
5
6     if not success:
7         return
8
9     destinationAddress = set(phantom.collect(container,
10         'artifact.*.cef.destinationAddress'))
11
12     parameters = []
13
14     for ip in destinationAddress:
15         parameters.append({'ip': ip,})
16
17     phantom.act('whois ip', parameters=parameters, assets=['whois'])
18
19     return
20
21 def on_start(container):
22
23     destinationAddress = set(phantom.collect(container,
24         'artifact.*.cef.destinationAddress'))
25
26     parameters = []
27
28     for ip in destinationAddress:
29         parameters.append({'ip': ip,})
30
31     phantom.act('geolocate ip', parameters=parameters, assets=['maxmind'],
32         callback=geolocate_ip_cb)
33
34     return
35
36 def on_finish(container, summary):
37
38     return
```

这种 IaaS 化的安全服务提供方式，用户可操作、可控制的权限非常大，因此所能实现的安全防护场景也更多。当然这样的操作对于安全运维人员的相关积累和技术要求也越高。

### 3. 总结

本文从云计算出发，结合云计算的优点，分析了云化的各种安全服务提供方式的特点和优势，总体来看 SaaS、PaaS、IaaS 三种安全服务提供方式对用户来讲，其使用的门槛和难易度是逐级递加的，三种服务提供方式对用户的专业程度要求也是逐级递加的，其防护的灵活度、安全防护的效果当然也是逐级递加的。

据笔者的个人了解，从当前安全云的建设来看，主要的安全服务提供方式还是以 SaaS 类的安全服务居多，无论是公有安全云还是私有安全云。而像 PaaS 这种用户可自动化编排的安全防护模式将会给安全云带来更多的亮点。

希望通过本文的介绍，能够让大家在获取安全服务时提供更多的思路，如对本文观点持有疑问，欢迎互相交流。

是云端 PaaS 服务的一种典型例子。

如下图所示，是安全云提供的用户自动化服务编排环境，所有的安全服务均抽象为一种种的安全服务能力操作，比如隔离设备、拦截 URL，用户通过脚本编写自己的安全服务场景，实现更智能、敏捷、自动化的高级安全防护。

对于 PaaS 化的安全服务，在公有安全云和私有安全云上的区别，和 SaaS 化的安全服务类似，主要还是源自于流量方面的影响，在服务提供的原理上，二者基本是一致的。

### 2.3. IaaS 化的安全服务

IaaS 化的安全服务主要是指安全云为用户提供安全设备基础设施，这种基础设施既可以用来防护用户的业务云环境，也可以用来防护用户的传统物理网络。通常 IaaS 化的安全服务主要体现在安全私有云上。

用户根据自身需求，自助的通过安全云平台申请所需要的安全设备种类、安全设备配置、安全设备部署方式、安全设备工作模式等，然后与其业务网络之间进行互通性的配置，完成完全自主、可控的安全云管理。

# 攻守“军备竞赛” 2017 如何布局

决策委员会 赵粮

关键词：网络安全 攻防态势 灰色产业 威胁情报 机器学习

摘要：本文从四个角度分析威胁将会出现新特点，然后阐述在网络安全防御方面最值得谋篇布局的四个技术领域和安全能力。

有朋友说，2016 是“突飞猛进”的一年。的确，一方面，网络攻击事件的规模 and 影响产生了一系列新的记录。数据泄露单事件丢失的记录数量创出新高；绿盟科技在 2016 年 8 月观察到拒绝服务攻击峰值流量达到前所未有的 3.7Tbps。

另一方面，网络安全防御方面也取得了一系列重要突破和创新。威胁情报、机器学习、云地协同等新技术和防护体系进入生产实践，系列创新公司雨后春笋般建立起来。

本文结构如下图，从四个角度分析威胁将会出现新特点，然后阐述在网络安全防御方面最值得谋篇布局的四个技术领域和安全能力。

这些新特点看起来都很“潮”，到底是啥意思？看后面，笔者为你——道来。

攻	防
攻击无极限，各种攻击元素出租 将会继续推陈出新	关注威胁情报，依托生态伙伴 洞察攻防前沿，避免成为水果，令人垂涎
没有银弹 攻防进入机器学习对抗时代	攻防进入机器学习对抗时代 没有机器学习是万万不能的
广谱和定向融合， 相互利用，“精细化运营”	不对称防守 在维度上做扩展
战场无极限 各种 Tings 都上网	防守无死角 S（社交）M（移动）T（物联网）都要思考

### 攻守双方的“军备竞赛”正在加剧

攻 1：攻击无极限，各种攻击元素出租等“业务模式”创新将会继续

灰色市场已经进入更为精细化的“专业分工”，从漏洞、利用、工具开发、僵尸出租、社工库、以及各种专门服务都已经多次见诸各种安全报告。某勒索软件要求受害者在一个星期内支付赎金或查找两个新的受害者。如果事件中另外两名“下线”受害者支付了赎金要求，原始的受害者可以免费获得解密密钥。不管这种类“传销模式”最终是否会带来更大的杀伤力，但灰产挖掘人性弱点并在运作模式中充分利用的尝试得以充分展现。

另外，臭名昭著的 DDoS 攻击者在直接敲诈和烟幕服务等之外，提供非常低廉 DDoS as a Service (DDoS 即服务)，5 美元起卖和分销。

守 1：关注威胁情报，依托生态伙伴，洞察攻防前沿，避免成为水果，让人垂涎欲滴

战场的无限扩大使得防护目标所涉及的技术和不断产生的漏洞成为几乎“防无可防”的窘境。跟踪云物大移时代信息系统的所有环节的漏洞和攻防细节，并实时做出准确的判断，对于数十人规模的专业安全团队都是极度困难的。依托威胁情报系统和“生态伙伴”成为一种必然的选择。

威胁情报是一个非常大的概念。针对自身安全防护体系的“短板”，正确选择所需的威胁情报类型和提供方，与所使用的安全平台、

设备、运维流程进行有机的对接，接受并能利用”局部失败”，敏捷运营，动态防御。

攻 2：没有银弹，攻防进入机器学习对抗时代

机器学习 (ML) 在网络安全实践中应用在 2016 年获得了长足的进步。各种机器学习和人工智能算法和工具被引入安全产品和系统。但是，机器学习只是一个数学工具，攻守双方都可以使用。通过对抗性图像攻击可以欺骗机器学习模型，在下面的图像识别例子中，识别引擎给出了公共汽车车窗的误判。以此类推，如果攻击者面对机器学习的安全产品及系统，同样有可能利用这样的误判，发起致命的攻击。

机器学习作为一种数学工具，其输出的“智能”并不是真正的“智能”，而是由其设计和运作过程中所使用的攻防模型、机器学习算法以及训练样本所决定的“计算”。这样，如果攻击者通过某种手段可以获取这些信息，并进行针对性模仿、甚至“注入”，就可以达到“免杀”和“误导”的效果。

守 2：机器学习不是万能的，没有机器学习是万万不能的

威胁方将会利用机器学习等先进技术来优化“攻击”，并不意味着机器学习之于网络安全没有用处，恰恰相反，不掌握机器学习技术的安全防御方将会处于类似冷兵器对热兵器的“劣势”局面。绿盟科技在 2016 年发布了基于机器学习引擎的新版 WAF 和 NIPS，相对于研究员手工创建规则的检测防护方式，新引擎在检测准确度和性能方面都获得了大幅度的提升。

洞察网络系统中的各种用户和设备行为，寻找源自合法用户、合法供应链组件等的可能攻击和滥用，针对安全事件的溯源和追踪，对全局安全态势的感知和研判等等，需要大量的安全数据分析、可见性、威胁情报等能力的联合运用，都需要机器学习为代表的新一代计算工具的支撑。

### 攻 3：广谱和定向融合 - 相互利用，“精细化运营”

定向攻击 (TA) 和高级持续威胁 (APT) 通常被认为是高级的技术对抗，而广谱的、也就是非定向的攻击被认为是一般的的技术对抗。进一步考察，如下图，广谱攻不区分行业和目标属性，单次收益低，强调海量重复和自动化。这样，针对性的，广谱的防守主要考虑减弱攻方的自动化和重复能力，避免自己成为最容易捕获的“目标”，这样攻方处于成本考虑，将会转移到其它目标。

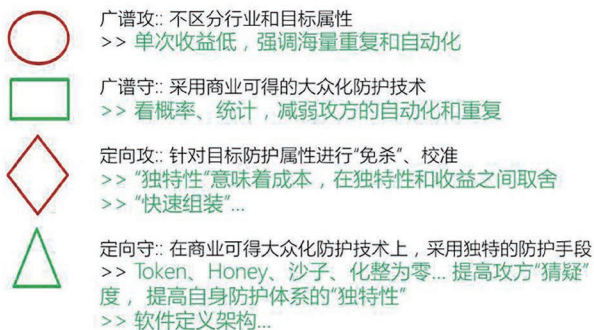


图 5. 四方博弈图像下的新视角, 2014

定向攻击者针对防护目标进行“免杀”校准，此时防守方所采用

的已被攻击者掌握的一般商业化防护措施已经失效。此时的防守成功要求攻方所不掌握的“独特性”。这种“独特性”对于攻方来说意味着成本和“风险”。

“广谱”发现精细化运营和“特种”服务可以带来更高的利润时，会主动设计并推广“画像”分析、数据标签分类、虚拟通道等高级定向服务。而“定向”考虑到风险、投入产出等因素，会尝试优先通过“广谱”手段达成目标或提供烟雾掩护。

### 守 3：不对称防守，在维度上做扩展

传统安全防护设备和体系在定向攻击面前无能为力，即使是基于机器学习引擎的防护手段，如果三个要素可以被攻击者了解或测试，攻击方就存在欺骗绕过的可能性。在动态纵深防御模型下，局部的“失败”并不可怕，但需要防守方能够及时的检查到“失败”并调整防护手段，保证掌控或重新夺回战场优势。

实现这种目标的一种途径就是攻击者所无法预测、侦查的“维度”的存在。“维度”可以是很庞大、很昂贵的系统，也可以是某种非常轻量级的对抗措施。

### 攻 4：战场无极限 - 各种 THINGS 都上网

物联网 (Internet of Things) 被利用来发起大规模拒绝服务攻击是 2016 年的一个热点事件，尤其 Mirai 和 DYN 攻击事件中大众传播达到一个新的高度。一个相对保守的预计是在 2020 年将会有 200 亿以上的物联网设备上网。如下图，大量低防护水平的目标涌入互联网，如同原来院子里玩耍的孩子们突然跑到车水马龙的大街上，必然对灰色产业和攻防态势产生深刻的影响。

灰色产业是逐利的，如下图简单的算式驱动下，物联网将会成为一个新的“主力”战场，并且不仅在消费领域展开，企业网也将遭受多种通过 Thing 的攻击。从而使得贯穿人和物的综合行为分析更为重要。

$$M = N \times (B - C)$$

潜在灰色收入      潜在节点规模      单节点收益      单节点成本

守 4：防护无死角，S（社交）M（移动）T（物联网）都需要考虑

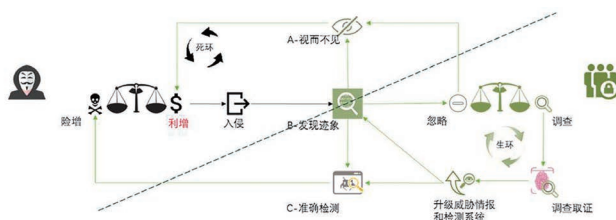
近年来，“云物大移”带来的安全威胁已经有很多的研究探讨。但就智能设备进入企业所带来的威胁以及相应的防护手段尚没有得到足够的研究和重视。Gartner 在 2016 年特别强调了 UEBA (User Entity Behavior Analytics) 的重要性，认为 UEBA 可以帮助更有效地对抗社交、移动、物联网等带来的新威胁。

攻防双方的“军备竞赛”需要高效的战略制衡

攻防双方的“军备竞赛”正在不断升级，威胁情报和机器学习是防御方当下的重要武器，而维度上的扩展是对抗定向和高级持续威胁的必要手段。短视或者犹豫不决，会让低水平防护者在“军备竞赛”中显露出来，成为僵尸军团的成员，进而在供应链、社交网络等信任体系中，成为攻击者高效的渗透跳板。

为了应对这个挑战，笔者曾经提出过生环死环模型，显然，“低

水平防护者”在网络中所占的比例较高，“生环”将会进入“死环”，其中的高水平防护者也很难作为安全孤岛而独善其身，这就要求“低水平防护者”尽快建立自己的防护体系，提升进入“生环”的几率，



而高水平防护者应该与各方携手，在整个行业中发挥更大的作用。

显然国家不会忽略国家安全战略问题，《网络安全法》于 2016 年 11 月 7 日正式发布，将于 2017 年 6 月 1 日施行。并且在 2016 年 12 月 27 日，国家互联网信息办公室发布了《国家网络空间安全战略》。笔者希望相关立法将会推动事故披露和案例分析制度、取证分析和威胁情报分享制度、安全责任体系等基础性体系的建立和提高，提升整体生态的安全防护水平。

网络安全已经变得前所未有的宽阔，也具有前所未有的纵深。对于绝大多数的防御方来说，依靠传统作业方式的、进行全面阵地防御已经不再现实。前面两年，相信读者大都或多或少地参与或了解了围绕新的纵深防御模型、从城防到塔防、基于失效的设计等的讨论，本文不再赘述。笔者认为，在大家布局 2017 年的网络安全技术能力时，威胁情报、机器学习、维度对抗、物联网等方面值得提到更高的优先级。



# 我帮客户做规划

运营商技术部 曹晖

关键词：运营商信息安全 运营商网络安全 应用安全  
数据安全 移动安全 云计算安全

摘要：在运营商行业，日益严峻的安全威胁迫使各个职能部门不得不加强对网络系统的安全防护，不断追求多层次、立体化的安全防御体系。然而，现有网络安全防御体系还是形成了一个个安全“孤岛”。在未来的一段时间，有限的安全管理人员面对这些数量巨大而相互孤立的安全信息，必须在思想上高度重视，从基础安全、应用安全、数据安全、移动安全、云计算安全等方面做好信息安全规划，指导信息安全体系建设，强化落实各项工作，切实提高信息安全整体水平。

## 1. 构建安保体系是信息安全规划的基础

当前，信息安全建设正在由关注单点安全向多点防护转变，由注重功能性能向关联防护转变，由“救火队长”式的应急防护和事后补救，到“先知”式的关联分析和提前预警转变，通过对信息安全建设进行合理有效规划，立足现状，理清当下需要解决的问题。

日益严峻的网络安全形势，正在迫使运营商各个职能部门对其网络系统安全防护工作，进行多层次、立体化的安全防御强化。然而，在

阶段化的发展过程中，现有网络安全防御体系还是以孤立的单点防御为主，彼此间缺乏有效的协作，从而形成了一个安全“孤岛”，有限的安全管理人员面对这些数量巨大、彼此割裂的安全信息，难以发现真正的安全隐患。因此必须在思想上高度重视，做好信息安全规划，指导信息安全体系建设，强化落实各项工作，切实提高信息安全整体水平。

信息安全规划的总体设计思路是以全面落实国家主管部门、

集团公司和上级单位的信息安全管理要求，实现信息安全管理体  
系化、标准化、平台化，为业务安全提供可靠的安全防护。通过对各  
项安全领域进行梳理、整合，制定涵盖管理体系、执行体系和支撑  
体系的信息安全保障体系总体架构。采用模块化方式逐层细化各项  
工作内容，形成实施框架，有效指引信息安全工作。

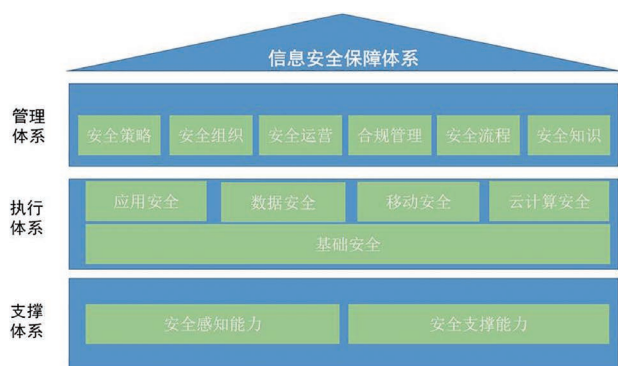


图 1 信息安全保障体系框架示意图

## 2. 安全规划思路

### 2.1、管理体系规划

管理系统的规划主要是从已有的管理体系入手，查找不足，查  
漏补缺。例如推进应用安全三同步工作，加强安全策略可落地性等。  
因此在管理体系规划过程中，要紧紧围绕安全防护体系、安全标准  
体系、安全组织体系、安全运维体系等方面的具体工作，实现业务  
网安全能力、支撑队伍、制度策略、执行流程的持续性提升。

按照国内外信息安全管理标准，行业安全标准要求，完善  
业务网的各项安全管理制度，持续构建在安全事件、安全合规检  
、合作伙伴等安全管理方面的制度和流程，确保安全策略的实时同步  
和更新，推动安全管理制度的落地实施。

强化安全合规管理工作，加强安全合规检查能力，提高合规工  
作标准化程度，细化安全合规要求，落实“安全工作矩阵”，提高安  
全基线与漏洞检查自动化程度，加强标准化执行支撑能力，提升安  
全合规管理效率。

完善安全组织架构，强化安全岗位配置、加快专业人才培养，  
优化激励和考评机制。针对提供安全服务的合作厂商的服务质量进  
行规范化管理，推动全网安全合作伙伴服务水平的定期评价及上报，  
以期全面提升安全服务质量。

### 2.2、执行体系规划

#### 2.2.1、基础安全

基础安全一般包括物理环境安全、网络安全、设备安全、系统  
安全和终端安全。各大运营商经过多年的基础安全建设，基础安全  
防护能力已经达到了相对完善的程度，具备了较为完善的满足合规要  
求的、体系化的基础安全防护措施。在未来规划方面，应重点考虑  
加强基础安全管控措施的自动化执行和流程化处置，力争做到安全  
管控自动化，操作执行流程化，进而构建更为完整和健全的基础安  
全防护保障体系。

针对运营商较为普遍存在的资产信息不全，与安全管控措施缺  
乏有效联动机制，漏洞管理和处置能力不足的问题，应将资产的梳

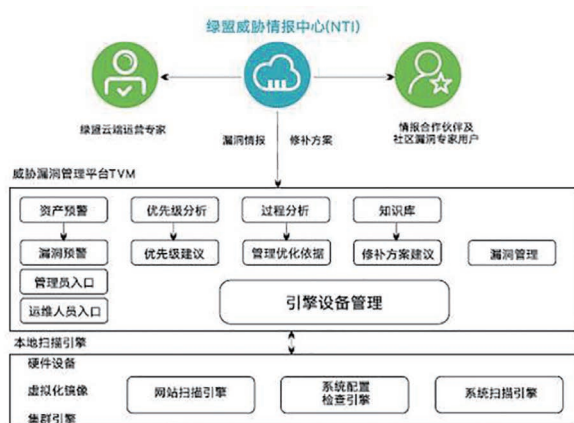


图2 威胁漏洞管理平台示意图

理监控和漏洞的跟踪处置进行有机整合，实现资产威胁和漏洞处置的一体化管控，进而实现资产高危漏洞的全生命周期闭环管理。

以此思路构建威胁和漏洞集中管控机制，由威胁情报系统(NTI)、威胁漏洞管理平台(TVM)和本地扫描引擎相互关联实现对资产威胁和漏洞的动态闭环管控。通过结合运营商漏洞管理现状，引入云端专业漏洞情报和互联网资产暴露稽核能力，激活传统企业漏扫产品，形成专家级的资产和漏洞管理能力。

该平台一方面解决了资产快速发现、精细管理的需求，一方面对资产相关的漏洞进行全过程跟踪分析，结合精确的资产信息分析漏洞对业务的影响程度，并跟踪漏洞发现、分析、修补和审核过程，为漏洞管理全过程制定可量化的基准要求，达到持续优化的目的。

## 2.2.2、应用安全

应用安全方面，在已有的安全管控措施上，应从应用代码审计管控、应用系统开发流程和应用开发人员安全意识等方面完善和提高。

**首先，要规范安全测试操作步骤，提升工作效率。**

按照应用安全“三同步”的标准规范流程，建立明确的安全测试管理规范，细化安全测试技术方法体系。主要包括：定期组织代码审核，挖掘应用系统漏洞，及时进行漏洞修复。建设应用系统漏洞库，实现应用系统研发人员发布信息产品的漏洞收集、漏洞发布、漏洞修复的联动管理，实现对漏洞的查询分析、预警督办功能。

对于外来渠道反馈的漏洞，第一时间分析核实入库备案，信息系统研发人员立即开展修复工作。对于第三方组件，项目研发人员要及时更新版本，项目运维人员要及时协调，督促项目开发及时更新版本或升级补丁。

**其次，要大力推广自动化白盒测试工具的使用，扩大测试范围，提高测试频率，降低测试成本。**

随着时间推移，大量漏洞已被黑盒扫描方式发现，修复后，可直接通过黑盒扫描工具发现的漏洞逐渐减少，而隐藏较深的安全漏洞却难以发现。相对于黑盒扫描，白盒代码扫描可以从代码层面发现隐藏较深的安全漏洞，不仅具备自动化的特点，而且发现问题的准确率较高。省去了黑盒测试时大量的人工验证工作，可大幅度的提交审计工作的效率及质量。

**再次，要加强研发过程安全培训，提高编码安全。**

通过对应用系统研发人员的信息安全开发技能培训，提高开发技术人员的安全编码能力和应用漏洞修复能力。同时，培训研发人员了解应用漏洞的相关知识以及安全测试软件的使用方法，使他们在研发过程中，能够及时自查并完成问题修复，从而降低应用代码中的漏洞数量，提高应用代码的安全性。培训内容可包括安全工具原理、安全工具使用方法、安全工具结果分析、安全编码规范、攻击技术原理、流行漏洞分析等。

最后，要建立软件生命周期安全管理流程，提升软件整体安全质量。

以应用安全“三同步”为指导，在应用软件生命周期各阶段引入安全建设步骤。

- 在需求阶段，针对功能可能涉及到的安全缺陷，进行全面的风险评估；
- 在设计阶段，针对风险评估结果提出完善的安全解决方案；
- 在研发阶段，监督和配合安全解决方案的落地，针对可能出现的漏洞，及时从代码层面进行检测和修复；
- 在测试阶段，需要验证对安全解决方案的有效性，同时需要审核研发人员是否遵

循安全编码规范；

- 在运维阶段，确保应用程序部署过程中的操作安全、环境安全并针对部署和运行中可能出现的风险，提供风险防护方案。

### 2.2.3、数据安全

在数据安全的保护方面，现有的措施比较单一。一般是通过制定数据安全规范，对数据的流通、操作和保存等环节规定安全的操作方式，再辅以数据加密方式，确保数据在传输、存储过程中的机密性和完整性。但是由于企业数据是保护的重点之一，也是黑客攻击入侵的主要目标，因此现有的措施已经无法有效保障数据安全，需要更为精准，覆盖面更广的自动化监控管理系统，能够实时的保障数据安全。

针对数据安全保护需求，可以通过采用数据防泄漏系统 (DLP)，基于内容识别技术，达到防止数据资产非法扩散的目的。该系统根据数据在存储、传输和使用中的特性，可细分

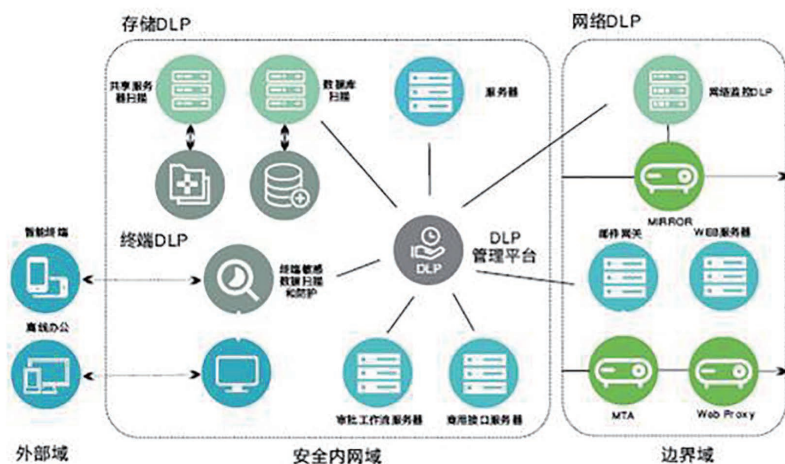


图3 数据防泄漏系统示意图

## ▶▶ 行业热点

为终端 DLP、网络 DLP 和存储 DLP，对关键数据进行针对性的防护。

- 终端 DLP 实现对企业终端敏感数据进行识别、监控，组织敏感数据非法外泄；

- 网络 DLP 以旁路方式部署，对网络中的流量数据进行还原、分析和识别，对传输中的敏感数据进行识别和监控。

- 存储 DLP 对存储位置的数据对象进行扫描识别，及时发现违规存放或生成的敏感数据

### 2.2.4、移动安全

随着近几年移动智能终端的兴起，移动应用火速发展，但随之而来的安全问题给运营商业应用带来了不小的安全隐患，因此立足于移动安全实际需求，从移动安全管理出发，规范移动 APP 安全扫描、渗透测试工作内容，建立问题处置跟踪机制，有利于保障移动应用业务安全。进一步完善移动安全保障措施，建议从以下三方面入手。

1. 加强终端接入控制，降低终端接入风险。在传统认证方式的基础上，采用移动终端硬件认证绑定的手段，加强终端接入安全。

2. 加强对数据安全的保护，提高数据的

隐秘性。通过加密手段提高数据通道的传输安全，保证数据的隐秘性，防止数据被恶意嗅探和篡改。

3. 加强终端生命周期管理，控制移动终端各阶段的安全风险。在移动终端的获取、部署、运行及回收的四个生命周期环节提供完善的策略和手段，确保每个环节都能顺畅、安全地实施和开展。

### 2.2.5、云计算安全

云计算技术给传统的 IT 基础设施、应用、数据以及运营管理带来了革命性的变革，对于安全管理来说，既是挑战，也是机遇。

云计算引入的新的威胁和风险打破了传统的信息安全保障体系设计、实现方法和运维管理体系；云计算的资源弹性、按需调配、高可靠性等间接增强或有利于安全防护，同时也给安全措施改进和升级、安全应用设计和实现带来了问题和挑战。

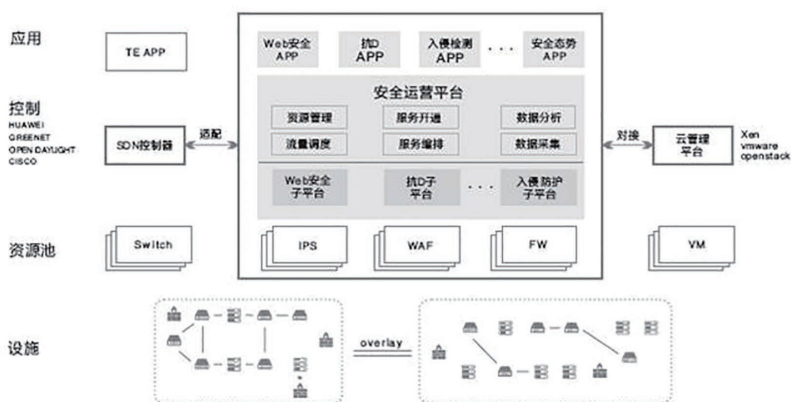


图 4 云计算安全保障示意图

但毫无疑问，如果云计算安全防护可以与业务环境进行有效结合，以业务为中心，风险为导向，基于安全域进行纵深主动防护，综合考虑云平台安全威胁、需求特点和相关要求，对安全防护体系架构、内容、实现机制及相关产品组件进行优化设计，那么云计算技术将为业务发展插上腾飞的翅膀。

正是考虑到云计算技术的挑战和机遇，绿盟科技设计了由安全资源池、安全运营平台、应用 APP 等组成的云计算安全方案。

- 安全资源池支持物理安全设备、虚拟化安全设备、安全类 SaaS 服务等各种安全资源，接受各安全子平台的管理，对外提供相应的安全能力。

- 安全运营平台与安全子平台配合，提供安全产品开通、调度、服务编排，以及安全运维功能，并实现与云管理平台、SDN 控制器的对接。安全运营平台包含了云安全运营的一些共性功能模块和一些提供特定安全能力的子平台。

- 安全子平台负责管理安全资源，提供安全策略管理、配置管理、安全能力管理、安全日志管理等与特定安全应用密切相关的功能。根据应用场景的不同，可灵活配置和扩展。

- 安全应用基于安全子平台提供的安全能力，提供管理、控制、分析、呈现功能的组件。用户可根据需要灵活选配。

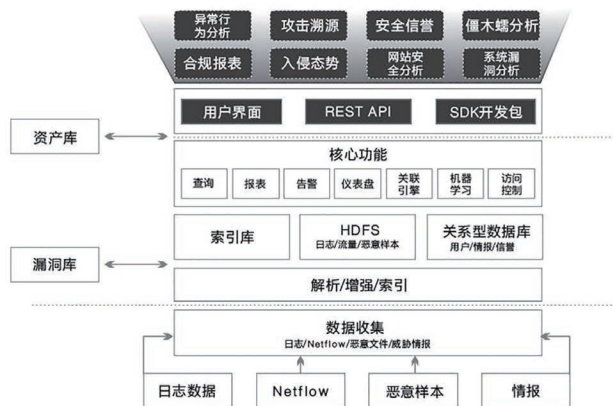
### 2.3、支撑体系规划

#### 2.3.1、安全态势感知能力

安全态势感知能力是要解决普遍存在的安全设备多，关联能力弱，无法及时了解全网安全态势和威胁情况的现状。以全面监测、

提前预警、及时处置、有效控制为目标，在大数据平台基础上，建立安全态势感知体系，建立全网安全数据关联分析和协同防御能力，准确、高效地感知整个网络的安全状态以及变化趋势，从而对外部的攻击与危害行为可以及时的发现，并采取相应的响应措施，保障信息系统安全。

安全大数据分析解决方案依托专业的安全分析模型和大数据管理工具，结合威胁情报的安全分析理念，利用事件理解模型实现多元数据关联分析，基于攻击链模型实现事件的正反双向推理，结合



态势感知能力图

威胁情报模型实现威胁验证及预警，最终借助风险评估模型为安全防护决策提供有力支撑。

安全大数据分析解决方案构建的态势感知平台，囊括了网络入侵态势、系统漏洞态势、网站安全态势、异常流量态势和僵尸蠕虫态势，

实时感知各类攻击事件和资产威胁情况，做到知己知彼，为企业提供全方位的、全天候的安全态势感知能力。



图 5 安全态势感知能力

### 2.3.2、安全支撑能力

安全支撑能力主要着眼于 4A 管控能力和全网的信息化综合管控能力。云计算、大数据、能力开放、掌上办公等新技术、新业务、新模式的出现，传统的 4A 平台系统在接入范围、管理能力方面面临挑战。应以“拓展平台能力、安全便捷运维”为目标，从“优化提升”和“能力开放”两方面进行规划。

1. 适应新技术、新业务，强化管控能力。加强 4A 平台针对大数据、移动 APP 在帐号权限合规、统一访问认证、操作访问可控以及

安全事件审计方面的能力。

2. 进一步强化审计能力，有效支撑日常工作。通过操作日志标准化策略精细化，进一步提升待审数据的准确性、完整性；通过审计分析专题化、场景化与报表制作灵活化，有效提升审计能力的可扩展性与适用性。

3. 建设帐号权限管理中心，实现联邦身份管理。基于 4A 平台现有帐号权限管理模块，构建统一的帐号权限管理中心，制定统一的帐号权限标准、提供统一的管理接口，并以服务方式提供给外围系统调用，进一步降低系统间接口的耦合度，减少应用接入 4A 的工作量。

4. 建设业支统一访问门户，实现应用访问无缝切换：打破应用系统边界，集中在 4A 门户展现所有应用操作界面，操作人员登录统一认证门户，不再需要跳转到其他业务系统即可完成业务支撑系统所有业务操作。

### 3. 信息安全规划肩负着对未来的预判

信息安全建设如逆水行舟，不进则退。随着新技术爆发式增长，移动互联应用的广泛使用，新模式的不断创新和落地，越来越多的信息安全薄弱点会不断暴露，给业务应用带来安全威胁和隐患。信息安全规划就显得尤为重要，一方面通过信息安全规划理清思路，找到主线，分清主次，才能够有条不紊地开展信息安全建设，另一方面，信息安全规划肩负着对未来几年内信息安全发展趋势的预判，准确引领安全建设方向，做到技术创新和安全保障两手抓，相互促进，协调发展。

# 走进中移动 回忆合规平台规范编写的那几天

系统架构部 赵粤征

关键词：中移动 合规平台规范 网络攻防 流动管理

摘要：2016 年底，笔者走进了中移动合规平台规范的封闭现场，一时间各路英豪云集，大家携手开始了合规平台规范的编写之旅。这期间，有争论有碰撞，但却激发出我们对安全行业及绿盟科技未来的思考。

---

## 规范的编写 热烈又严谨

---

由于前期我们是作为设备厂商进入编写组的，所以我们的主要工作目标是在设备方面，部分延展至平台等方面。在前期规划阶段的两三天时间里，我们首先梳理合规平台和扫描器之间的接口，同步考虑

平台、绿盟科技与友商之间的接口及协同；然后是关于合规平台编写的任务分派，最终由于绿盟科技在网络攻防方面的多年积累，漏洞管理的 8 个章节，由我们与另一个在 SOC 领域有深厚积淀的厂家合作完成，但这个过程并非一帆风顺。



在和平台总体负责厂商的初期沟通中，平台规划的各个章节模板还在进一步定义，某些章节的功能点展开方面还在进一步细化，考虑到业务环境的复杂性，简单拷贝原来 SMP4.0 的模式，就具体的功能写功能，这种方式肯定是存在问题的。

我们的基本看法是，所谓规范，它所回答的问题就是 5W1H 中的为什么要做、做什么和怎么做（部分回答）这三个范畴。基于这样一个框架，而合规平台更主要是要通过平台实现管理范畴，技术实现其实不是难点，因此，和同事讨论之后，我们提出的一个写作思路是实现一个映射，一个从业务管理流到用户场景再到功能架构的映射，然后再整体考虑一二级平台间的接口规范，这样就基本能回答 Why/What/How 的问题了。

按照这个思路，大家花了大概 4 天时间，经过反复讨论及沟通，完成了业务管理流 / 用户场景 / 功能架构及功能描述，文档进入了初步内部评审。但出于意料的是，评审过程还有不少的争执。争论过程中，大家各自提出自己的理由和观点，且我们的团队成员在人数上并不占优。但绿盟科技的架构及描述，以其清晰的逻辑及完整性，最终胜出。中移动业支领导给出的评价是，绿盟科技完成的章节贴合业务及最终用户场景，且功能架构描述清晰，建议其他章节各部分参考编写。客户领导的决定，统一了整个规范的架构体系，即按照业务场景 - 用户场景 - 功能描述的架构来展开平台规范。

在编写阶段的合规管理部分，SMP 平台上由几个友商主导实现，大家也都在之前的基础上强化了业务场景及逻辑严谨性。在漏洞管理部分，友商提出漏洞爬虫管理技术，并纳入到了平台中并作为一

个独立的章节。但我们认为，爬虫仅仅是获取漏洞信息的一种技术，而且并不是唯一的技术，并不适合作为独立章节展开。这一章节应该是站在更高的维度，利用爬虫、订阅等一系列的技术手段，我们要能获取到漏洞信息，实际上应该定义为漏洞情报，我们不仅要能获取情报，还要能管理情报，对情报进行关联分析，并生成预警，所以这一章节应该定义为漏洞情报管理。我们的这个想法得到众多友商和客户的支持，最终经过与客户的沟通，由绿盟科技完成漏洞情报管理部分。

虽然，笔者和同事们不是第一次参与安全方面的规范编写，但在与客户及各个友商的讨论及思维碰撞过程中，很多新的思路和想法也不断涌现出来，这些闪光点需要随时记录下来，并不断完善我们后续编写规范的流程。从这次中移动合规平台规范的编写过程中，我们总结了几点，希望能对后续相关人员能有所启发：

- 1、规范的模板应该在编写之前需要确定下来，在各个大的章节确定后，章节的内容建议按照业务范畴 用户范畴 功能架构 功能描述 接口等几个维度推导展开，若某一章节涉及到有技术难点或者技术关键点，可以放在功能架构中展开。这样写作的好处，就是作为使用者主体，可以知道当前的功能处于业务的哪一个环节，并从用户的视角知道该怎么用。

- 2、无论初期客户是怎么定义我们的身份（设备厂商还是平台厂商），我们都应该从客户的角度出发，从帮助客户业务发展的角度出发，去积极解决问题，将我们各个平台及产品的优势在规范中体现出来。

- 3、在规范写作及评审中，一味做老好人，追求小改动，反而会

给客户后续的工作埋下隐患，对业务有帮助的、新的观点及方法还是要提出来，通过与客户及友商的反复沟通及讨论，尽可能实现较为优化的规范。

4、当业支的领导在业务发展方面的规划及想法，还是需要保持和客户的交流顺畅，根据客户的想法随时调整编写思路，尤其是在新业务新形势下的创新，还需要多结合最终用户的应用场景来考虑，这样才能输出高质量的规范。

---

### 友商们也很关注客户体验

---

工作之余，同住一个房间的同事和另外一家友商的小伙伴们聊起了整个网络安全的行业现状。

有 H 公司是从系统集成进入安全领域的，他们以现有的产品冲击安全市场，面对客户的诉求，通过已有的产品的网络能力迅速复制相应的网络安全能力，并通过市场策略，迅速抢占同质化的市场份额，在拉低网络安全领域利润的同时，不断推动提高整体的市场进入门槛，这将会进一步挤压小型安全公司的生存空间；与此同时，在技术方面，以多年积累的网络设备能力及综合软件能力，构建面向客户体验的软件服务能力，提升其差异化的竞争能力。

S 公司，从进入安全领域之初，就带着 H 公司的血统，能冲，敢打，公司内以 996 为其工作模式，继承了 H 公司以客户需求至上为其开发理念，这个理念，深刻的影响着他们对几乎每一个问题的看待角度乃至处理方法。除了努力研发好用的产品，他们更注重对客户的快速响应，不断根据用户反馈的问题改进完善产品。

---

### 发挥绿盟的优势

---

那绿盟科技的优势在什么地方？市场积淀、业界影响力、技术实现能力等方面的优势如何发挥出来呢？从友商们的做法中不难看出，就是需要真正的建立以客户为中心的开发理念和服务理念。

在这一次规范写作中，看到有些友商几个前场经理的情况，由于缺少来自后方的支援，一些应该体现出来的实力及优势没有发挥出来，团队的协同能力建设及以客户为中心的工作模式等方面，还有进一步提升的空间。绿盟科技团队通过内部组建的合规平台协作群获得了有效的能力支撑，在整个编写过程中，始终能得到来自最贴近代码的开发的支援，这里不得不给后方团队的同事们点个赞！正是他们的密切配合与支持，帮忙我们反复的翻看代码、确认接口、评审文档，让我们最终获得了中移动领导的肯定。在后续类似工作中，我们还有空间，将这些后方协作平台与体系进一步完善与提升，并最终保证我们每一次的客户交流、达标等的活动获得超越预期的效果。

以客户为中心，就是我们在体系中的每一个角色职责，在面向下游交付时，这个下游就是你的客户，你要交付的是一个满足这个客户要求的 quality product。SE 提交的就是可以直接面向售前客户的解决方案文档；面向开发的设计体系文档；面向测试的同源测试文档；面向客服的支撑文档，当面向我们的任意层级的客户，能做到想的清楚，写的清楚，讲的清楚，做的清楚。开发提交的不仅仅是代码，而是包含着别人的信任和期待的质量体系。测试就是我们质量缺陷

的发现者和质量体系的守护者，我们要能做到，测试完成交付，就是一个质量完备的可以真正面向客户发布的产品。这一切需要我们不仅仅只是做一个只知道砌墙的建筑工，而是我们心中要有自己的教堂，自己的梦想。

以客户为中心，就是在业务实现中体现技术和客户诉求的完美融合。技术人员常常有某种偏执，就是我做的东西就是最好，不允许在功能上、架构上有任何的瑕疵。我常常能遇到面对客户直接的诉求的时候，我们总是强调，这样做不符合技术的方向，但很多时候我们从客户的角度出发，做的还不够多，我们还需要进一步减少客户的操作流程，进一步能提升客户的体验，从而降低客户的管理成本。实际上，当我们内心真的心存客户的时候，我们最终的架构都是技术和应用上的一个妥协，它未必是技术上呈现最完美的，但一定是面向客户最柔性和最实用的体系。

以客户为中心，就是在业务交付上，我们能够根据市场诉求，快速跟进并切入市场，这就要求我们能打造出很多支能够在任何时候实现快速交付的研发团队，这样的团队，有创新力，有激情，有打死也不服输的劲头，记得我以前曾经接触过的一支友商的测试团队，他们的座右铭就是：死了都要测，往死了测，这就是他们的精神。

---

### 绿盟科技的未来

---

关于未来绿盟的市场机会点，我和我的同事，聊得最多的是关于未来国际市场的开拓。在国内市场，网络安全的发展，国家作为十三五 100 项重大工程的第 5 项给予了我们持续发展的机遇；国

外企业由于政治安全上的考虑原因，无法瓜分中国市场。而对于国际市场，由于国家一带一路的大战略推进，存在一大批和我们国家政治上互信的国家 and 政府，做国际市场的网络安全，只有政治上的互信，别人才会用我们的产品。因此，对于欧美日等国家的市场进入，目前我们存在两个重大问题是没办法应对的，第一，政治上互信程度还不足支持我们在这些市场上能大的斩获；第二我们的安全服务的精细化程度尚不足以支持我们能满足这些国家的要求。基于以上考虑，我们国际市场的主攻方向应该是跟随国家的一带一路战略，先在巴基斯坦、伊朗、中亚 5 国、俄罗斯等国家落地生根，逐渐向其他亚非拉其他国家辐射。我们也许可以称之为“绿盟科技的网络安全丝绸之路”

之前，有人常常说，我们做项目，得靠关系，有关系，才能做成大单，但我想说的是，通过友商公司开拓海外市场之路，我们可以看到，任何的关系，都是靠我们坚守的力量，相信的力量获得的。利益面前，别人来了，我们也来了，我们可能没有收获；困难面前，别人走了，我们选择坚守，我们收获到满满的信任，这就是我们关系的基石。但这一切，知易行难，没有一件事是容易的事儿，没有一件事儿不花精力时间就能解决的，看看全是问题，靠什么继续走下去？唯有坚持，唯有坚信，一直到转机的时候，这个过程有自我否定自我怀疑，还有多少次的艰难，事实上，只要开始了，就必须走下去再难也要走下去，到最后，靠什么支撑？唯有信仰，唯有相信的力量！

绿盟科技网络安全的未来，我看好，我坚信，我期待……

所以，让我们来共同坚守！

# 证券类金融企业 网络安全建设方法与思路

金融技术部 俞琛

关键词：金融业网络安全规划 金融网络安全建设方案  
网络安全系统建设方案

摘要：本文梳理网络架构分析、拒绝服务攻击防护、网络入侵防护、APT 攻击行为识别等方法，以企业信息安全管理视角，提出适合证券类金融企业网络安全建设思路和内容。文中介绍的方法和建设内容相互对应，读者可以在工作规划中按需参考。

金融企业是指执行业务需要取得金融监管部门授予的金融业务许可证的企业。其中，执业需取得证券业务许可证的证券公司、期货公司和基金管理公司等，与银行类一样，同属于国家重要信息系统范围。相较于银行类金融企业网络安全工作，证券类金融企业在网络安全的整体建设方面存在一些差异。首先，时间维度来看，证券类存在明显的交易时间段与非交易时间段，交易时间段的网络、系统可用性要求很高。系统维度来看，证券类相对较集中，对外服务的重要系统以交易 WEB 平台和交易 APP 为主。归结到安全威胁维度，由于存在交易时段和资金交易，证券类面对拒绝服务攻击、网络入侵、和数据窃取威胁，如具有 APT（高级持续性威胁）特性的“基金幽灵”威胁。

因而，证券类金融企业网络安全建设思路是首先优化网络结构，减少网络安全高危漏洞或缺陷数量，通过部署抗拒拒绝服务攻击、网

络入侵防护和恶意程序防护措施提高基础安全水平，采取网络流量分析技术、安全意识培训、监测与防护措施等，应对高级别攻击。

## 一、安全建设方法

### 1.1 网络架构分析方法

网络架构分析是对用户评估范围内网络建设规范性、网络边界安全性、网络通信安全、整体网络架构合理性，及网络安全管理等方面进行现状分析，采用的分析方法包括资料收集、人员访谈、网络流量采集、防火墙策略分析、网络设备自身配置参数检查等。由于前几种属于通用方法，不作赘述，如下重点介绍后两项方法。

#### 1.1.1 防火墙策略分析

防火墙策略分析需安全工程师对已导出的防火墙策略进行阅读，通过与网络管理员、防火墙厂商工程师交流，理解策略含义。之后，通过与网络拓扑结合分析，找出存在安全风险的配置策略并提出整

改建议。分析过程遵循如下原则：

- 防火墙策略设置应遵循“最小化”原则，根据系统内外部互连的实际需求，建立细化到源 / 目的 IP、端口、承载信息、信息敏感性等内容在内的网络连接信息表，并据此配置防火墙策略，禁止出现非业务需要的大段 IP、连续端口开放的策略。

- 原则上不允许提交策略的业务服务占用小于 1024 的常用端口；所有没有明确允许的访问都应该禁止。

- 在不影响防火墙策略执行效果的情况下，应将针对所有用户（源为 any）的策略设置为较高优先级；将匹配度更高的策略优先级次之；将拒绝的策略设置为比允许的策略更高的优先级。

- 原则上防火墙策略中不应出现允许远程登录及数据库管理的相关策略。对于特殊需求的，可设置点对点访问控制策略。

- 原则上互联网用户只能访问外联 DMZ 区域的设备，不允许存在互联网用户直接能访问到内部核心服务器区域的访问权限。

- 防火墙策略的最后应有一条拒绝所有 (deny all) 的策略。对于需要自行配置 deny all 的策略的防火墙，在最后添加 deny TCP any any。

### 1.1.2 网络设备自身配置参数检查

从整体网络安全的角度对现有的网络安全策略进行全局性的评估，主要包括：

- 对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。应强制对只支持 telnet 的设备进行淘汰，在支持 SSH 设备上运行版本升级，如 OPENSSSH 组件建议升级到

v7.0。同时，禁用已证实弱算法组合，如停用基于 MD5 的 HMAC 算法、blowfish-cbc、cast128-cbc 等。

- 定期对网络设备的配置文件进行备份。

- 对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

- 应对网络设备的管理员登录地址进行限制。

- 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

- 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、注入式攻击、IP 碎片攻击和网络蠕虫攻击等。

### 1.2 拒绝服务攻击防护方法 1.2 拒绝服务攻击防护方法

拒绝服务攻击，即 DDOS，是在众多网络攻击中一种简单有效并且具有很大危害性的攻击方式，通过各种手段消耗网络带宽和系统资源，直至不能对正常用户进行服务。

DDoS 攻击形式更趋复杂，存在大小流量两极分化。据绿盟科技全球 DDoS 态势感知平台监控数据分析显示，2016 年 Q2 较 Q1 发生 DDoS 攻击事件有所下降，平均攻击峰值也有所降低，但攻击手段呈现复杂化，因此总体攻击态势依然严峻。我们观测到很多利用几种流量混合发起的攻击，这类攻击相比单类型攻击，对攻击目标网络破坏能力更强。从攻击总流量占比看，利用混合攻击手段发起的攻击流量占总类型分布的 33.7%。其中，最常见攻击混合类型为

SYN Flood 和 UDP Flood 攻击混合，占全部混合类型的 36.1%。另外，发现较多使用反射攻击流量混合的情况。

Q2 季度仍然是峰值在 10Gbps 以下的小流量攻击最多，占比达 50%，相比 Q1 季度的 40% 其所占比例继续上升，可见攻击者越来越多地使用小流量攻击方式，只是攻击手段更加复杂。NTP Reflection Flood 攻击流量占比最多，为 36.1%，其次是 DNS Reflection Flood 攻击，攻击流量占比为 24.8%。小流量攻击有着特殊的目的，与大流量（百 G 以上）及超大流量（500G 或更高）相比，1 这些攻击因为其流量小，不会引起业界的关注，2 这些小流量隐藏在大流量之中，难以辨识；3 更有些小流量攻击时长小到防护设备难以捕获，很难完整呈现其攻击过程，这些特点决定了小流量攻击不仅不会被攻击者抛弃，而且将其充分贴近业务特性，形成 DDoS 脉冲攻击（Hit-and-run DDoS）。因此，采取能够应对大流量和小流量攻击类型的多个维度防护方法，应对 DDoS 攻击行为。主要防护方法是运营商清洗和本地防护平台，建议采取双机制措施部署，其中一项失效时，互为备份措施。

### 1.2.1 运营商流量清洗

国内各运营商陆续提供网内 DDoS 流量清洗增值服务，可有效应对大流量 DDoS 类型攻击。如广东电信流量清洗系统利用旁路部署技术，集中部署在省干网，并结合攻击检测系统，及时发现背景流量中各种类型的攻击流量，迅速对攻击流量进行过滤或旁路，保证正常流量的通过，有效地提供 DDoS 检测防护服务。

### 1.2.2 本地防护平台

通过在企业网络互联网边界部署 DDoS 专用防护系统，可有效应对小流量 DDoS 类型攻击。在未达到攻击规模之前，可以对流量进行分析，并统计背景流量状态，事前调整防护策略提高准确性，提升攻击事件发生时的防护水平。

同时，作为运营商流量清洗的备份措施。

## 1.3 网络入侵防护方法

网络入侵防护是应对非授权人员从网络边界入侵企业重要信息系统和相关网络设备。防护方法有网络入侵检测、入侵阻断、威胁风险分析。如下对入侵检测和威胁风险分析方法做介绍。

### 1.3.1 入侵防护检测

#### • 基于特征分析的专家系统

特征分析主要检测各类已知攻击，在全盘了解攻击特征后，制作出相应的攻击特征过滤器，对网络中传输的数据包进行高速匹配，确保能够准确、快速地检测到此类攻击。

#### • 协议异常检测

协议异常最为重要的作用是检测特定应用执行缺陷（如：应用缓冲区溢出异常），或者违反特定协议规定的异常（如：RFC 异常），从而发现未知的溢出攻击、零日攻击以及拒绝服务攻击。

#### • 流量异常检测

流量异常检测主要通过学习和调整特定网络环境下的“正常流量”值，来发现非预期的异常流量。如果实际网络流量统计结果与

基准达到一定的偏离，则产生警报。

### 1.3.2 威胁风险分析

威胁情报，是资产威胁或危害的基于证据的知识，包括上下文、机制，指标，意义和应对建议，可为主体提供如何响应威胁或危害的决策。

证券类金融企业对外服务的重要系统以交易 WEB 平台和交易 APP 为主，通过收集威胁情报，掌握国内外已发生的特定信息安全事件所利用的已知漏洞是否与企业交易 WEB 平台存在的漏洞或交易 APP 某项业务流程缺陷有关联，从而提出漏洞缺陷修补优先级。威胁风险分析过程需要将信息资产、存在漏洞信息、威胁信息综合分析，得出风险高低结果，提供安全团队决策。

绿盟科技提供威胁情报平台 NTI，可以从绿盟云推送相关威胁情报至企业本地，支撑企业威胁风险分析。

## 1.4 APT 攻击行为识别方法

绿盟科技在多家基金机构陆续发现具有 APT 特征的恶意样本，即木马 Backdoor.David。该木马除具备传统木马功能外，同时还具有被捕获后告警、驱动级自保护、多级代理控制、数据通信加密等功能，经过充分分析此木马在本次攻击事件中的行为特征以及 rootkit 功能，再结合该样本定向攻击、潜伏期长、攻击模式隐蔽且形式多样等特点，我们将该事件性质定义为 APT 攻击。

识别此类木马的方法是定期在企业的网络边界和内部网络进行网络入侵防护基础上，采取网络流量威胁分析，提高 APT 攻击行为

的识别率。如下对网络流量威胁分析技术做介绍。

### 1.4.1 多种应用层及文件层解码

从高级可持续威胁的攻击路径上分析，绝大多数的攻击来自与 Web 冲浪，钓鱼邮件以及文件共享，基于此监测系统提供以上相关的应用协议的解码还原能力，具体包括：HTTP、SMTP、POP3、IMAP、FTP。

为了更精确的检测威胁，监控系统考虑到高级可持续威胁的攻击特点，对关键文件类型进行完整的文件还原解析，系统支持了以下的文件解码：

Office 类：Word、Excel、PowerPoint...

Adobe 类：.swf、.pdf...

不同的压缩格式：.zip、.rar、.gz、.tar、.7z、.bz...

### 1.4.2 智能 ShellCode 检测

恶意攻击软件中具体的攻击功能实现是一段攻击者精心构造的可执行代码，即 ShellCode。一般是开启 Shell、下载并执行攻击程序、添加系统账户等。由于通常攻击程序中一定会包含 ShellCode，所以可以检测是否存在 ShellCode 作为监测恶意软件的依据。这种检测技术不依赖与特定的攻击样本或者漏洞利用方式，可以有效的检测已知、未知威胁。

需要注意的是由于传统的 ShellCode 检测已经被业界一些厂商使用，因此攻击者在构造 ShellCode 时，往往会使用一些变形技术来规避。主要手段就是对相应的功能字段进行编码，达到攻击客户

端时，解码字段首先运行，对编码后的功能字段进行解码，然后跳到解码后的功能字段执行。这样的情况下，简单的匹配相关的攻击功能字段就无法发现相关威胁了。

系统在传统 ShellCode 检测基础上，增加了文件解码功能，通过对不同文件格式的解码，还原出攻击功能字段，从而在新的情势下，依然可以检测出已知、未知威胁。在系统中，此方式作为沙箱检测的有益补充，使系统具备更强的检测能力，提升攻击检测率。

### 1.4.3 动态沙箱检测

动态沙箱检测，也称虚拟执行检测，它通过虚拟机技术建立多个不同的应用环境，观察程序在其中的行为，来判断是否存在攻击。这种方式可以检测已知和未知威胁，并且因为分析的是真实应用环境下的真实行为，因此可以做到极低的误报率，而较高的检测率。



检测系统具备指令级的代码分析能力，可以跟踪分析指令特征以及行为特征。系统发现恶意软件后，会持续观察其进一步的行为，包括网络、文件、进程、注册表等等，作为报警内容的一部分输出给安全管理员，方便追查和审计。而其中恶意软件连接 C&C 服务器

(命令与控制服务器)的网络特征也可以进一步被用来发现、跟踪 botnet 网络。

## 二. 安全建设内容

### 2.1 网络架构分析

网络架构分析是通过用户对用户评估范围内网络建设规范性、网络边界安全性、网络通信安全、整体网络架构合理性，及网络安全管理等方面进行现状分析，差缺补漏，并提出网络改造方案。

网络架构分析主要工作内容说明如下：

- 1) 网络建设的规范性：网络安全规划、设备命名规范性、网络架构安全性；
- 2) 网络的可靠性：网络设备和链路冗余、设备选型及可扩展性；
- 3) 网络边界安全：防火墙策略、网络设备的 ACL、VLAN (二层 ACL) 等；
- 4) 网络协议分析：路由、交换、组播、IPv4 等协议；
- 5) 网络通信安全：通信监控、通信加密、VPN 分析等；
- 6) 设备自身安全：口令、设备版本、系统漏洞、服务、端口等；
- 7) 网络安全管理：客户端远程登陆协议、日志审计、设备身份验证等。

### 2.2 拒绝服务攻击防护

证券类金融企业购买运营商的流量清洗服务，在运营商网间解决大流量的 DDoS 攻击。在互联网出口处部署绿盟抗拒绝服务系统，解决运营商服务无法处置的多重复杂的 DDoS 脉冲攻击，并在运营



商服务失效时，提供防护备份措施。

同时，通过本地部署防护系统，在未达到攻击规模之前，可以对流量进行分析，并统计背景流量状态，事前调整防护策略提高准确性，提升攻击事件发生时的防护水平。

### 2.3 网络入侵防护

在互联网出口位置部署具备检测和实施阻断能力的防护设备如 IPS，对网络流量特征进行实时检测和阻断。同时，由安全团队组织开展威胁风险分析，针对已部署网络入侵防护设备的日志、告警信息，开展日志分析，提供整体信息安全形势综合分析报告，初期以人工分析为主，随着安全建设深入，逐步提升自动化分析比例和人机学习技术的应用，提升防护效率，提高网络入侵防护水平。

### 2.4 APT 识别与防护

笔者建议开展针对 APT 攻击行为的安全检测、监控与防护、安全意识培训三项内容。

#### 安全检测

使用具备检测此类特定攻击能力的安全扫描设备对全网 IT 网资产（主要是服务器和 PC 终端）进行全网安全风险和漏洞扫描。考虑到攻击者主要针对证券行业进行定向攻击，不排除重新感染的可能性。因此，建议用户持续对发现的后门相关的扫描结果进行关注，定期更新扫描设备插件并执行扫描作业。

#### 监控与防护

- 在业务网段部署安全审计设备，对数据库查询、FTP 传输、

网络登录等网络行为进行安全审计，及时发现恶意查询、匿名登录等网络异常行为；

- 考虑到该后门以及类似攻击变种多样，建议部署具备流量还原能力的威胁分析系统，并对主要通讯协议和主要文件类型进行检测覆盖。

- 安全意识培训

面向全员/特定岗位/管理层进行持续的安全培训，告知其日常安全注意事项、操作规范、安全事件预警原则等必要信息，改善工作习惯，提升安全意识，持续增强企业安全防护能力。

## 三. 结语

我国信息安全态势显示“针对我国重要信息系统的高强度有组织攻击威胁形势严峻”，“仍有众多 APT 攻击事件尚未被识别”这一观点已是业内共识。证券类金融企业网络安全建设应根据企业现状进行网络架构优化、部署网络方面的检测防御类和安全评估类产品，利用大数据、人机学习等新技术实现态势感知、关联分析等安全建设目标。

本文梳理了网络安全建设思路方法和内容，从架构分析、DDoS 防护、入侵防护逐步深入，从无到有，对于 APT 识别与防护水平高低的关键是企业需要组建自有安全团队，且信息安全经理必须认识安全产品的安全价值，独立于厂商给予产品的名称标签，赋予安全产品在企业自身环境中的专属功能定位和名称标签，从而发挥超出单一安全产品的防护功能，实现整体安全防护价值。

# 探索“互联网+政务服务”安全保障体系

政府技术部 何财发

关键词：互联网+政务服务 安全保障体系 应急响应预案

摘要：“互联网+政务服务”安全保障体系，这个概念来自于国务院印发《关于加快推进“互联网+政务服务”工作的指导意见》。意见要求对加快推进“互联网+政务服务”工作作出总体部署；其中（五）加强网络和信息安全保护；按照国家信息安全等级保护制度要求，加强各级政府网站信息安全建设，健全“互联网+政务服务”安全保障体系。本文结合国家要求、等级保护、新型安全威胁及新的安全建设思路及措施，与大家一同探索“互联网+政务服务”安全保障体系。

## “互联网+政务服务”安全保障体系建设背景

“互联网+政务服务”安全保障体系，这个概念来自于国务院印发《关于加快推进“互联网+政务服务”工作的指导意见》。新华社北京9月29日电 经李克强总理签批，国务院日前印发《关于加快推

进“互联网+政务服务”工作的指导意见》，对加快推进“互联网+政务服务”工作作出总体部署。其中（五）加强网络和信息安全保护。按照国家信息安全等级保护制度要求，加强各级政府网站信息安全建设，健全“互联网+政务服务”安全保障体系。明确政务服务各

平台、各系统的安全责任，开展等级保护定级备案、等级测评等工作，建立各方协同配合的信息安全防范、监测、通报、响应和处置机制。加强对电子证照、统一身份认证、网上支付等重要系统和关键环节的安全监控。提高各平台、各系统的安全防护能力，查补安全漏洞，做好容灾备份。建立健全保密审查制度，加大对涉及国家秘密、商业秘密、个人隐私等重要数据的保护力度，提升信息安全支撑保障水平和风险防范能力。

中央政府将推进“互联网+政务服务”，“应上尽上、全程在线”彰显了国务院利用互联网技术提高政府效率和透明度，降低制度性交易成本的决心。《意见》提出，到2017年底前，各省（区、市）人民政府、国务院有关部门建成一体化网上政务服务平台，全面公开政务服务事项，政务服务标准化、网络化水平显著提升。2020年底前，建成覆盖全国的整体联动、部门协同、省级统筹、一网办理的“互联网+政务服务”体系，大幅提升政务服务智慧化水平，让政府服务更聪明，让企业和群众办事更方便、更快捷、更有效率。

---

### 政务上网，必然要面临着互联网的安全威胁

---

随着“互联网+政务服务”的全面推进，信息技术在国家政务服务中的应用也越来越广泛，然而新型的网络安全威胁也更加突出，传统以“防护”为主的安全体系将面临极大挑战，互联网安全也成为国家安全、社会稳定、经济持续发展的必要条件。近年来，以互联网为媒介或直接以互联网上的资产为目标的安全事件也在不断滋生，来自于敌对势力、恐怖份子、邪教势力、各类犯罪份子也在不

断利用互联网从事破坏、间谍、犯罪、传播邪教与恐怖主义的行为，互联网安全已经成为影响到我国国家安全和国计民生，需要加强网上治理，“互联网+政务服务”安全保障体系建设势在必行。

---

### “互联网+政务服务”安全保障体系建设

---

依据信息安全等级保护相关要求，需要先对“互联网+政务服务”业务系统进行定级，然后结合“互联网+政务服务”实际安全建设情况，从技术和管理两个方面综合评估后，依照“一个中心，三重防护”的设计思想，建设“互联网+政务服务”安全保障体系，制定既有可操作性又符合国家推行的信息安全等级保护制度的“互联网+政务服务”安全管理制度、应急响应预案等安全体系文件。未来“互联网+政务服务”网络安全保障体系将侧重于建设线上线下闭环敏捷响应的安全体系，更加注重网络安全的监测和响应能力，充分利用网络态势感知、大数据分析及预测技术，大幅提高安全事件监测预警和快速响应能力，应对大量未知安全威胁。

“互联网+政务服务”安全技术服务内容：

#### 1、“互联网+政务服务”系统应用防护

“互联网+政务服务”的目标是建成覆盖全国的整体联动、部门协同、省级统筹、一网办理的“互联网+政务服务”体系，需要在“互联网+政务服务”一体化网上政务服务平台前端部署专业的应用系统防护WAF，WAF系统是采用串联的方式部署在网络中，并支持透明代理的部署方式，作为Web客户端和服务器端的中间人，避免政务服务平台Web服务器直接暴露于互联网上，监控HTTP/HTTPS

双向流量，对网络层、Web Server/Application 层双向数据实施检测和保护，可以降低“互联网 + 政务服务”系统 Web 站点安全风险。

## 2、“互联网 + 政务服务”系统数据库安全防护

“互联网 + 政务服务”系统中需要在线部署专业的数据库防火墙系统 (DAS-FW)，加大对涉及国家秘密、商业秘密、个人隐私等重要数据的保护力度；通过虚拟补丁技术捕获和阻断漏洞攻击行为，通过 SQL 注入特征库捕获和阻断 SQL 注入行为，防止外部黑客攻击“互联网 + 政务服务”系统中的数据库系统；通过限定更新和删除影响行、限定无 Where 的更新和删除操作、限定 drop、truncate 等高危操作，防止内部系统维护人员、外包人员、开发人员等的数据库运维高危操作；限定数据查询和下载数量、限定敏感数据访问的用户、地点和时间，防止政务敏感数据泄漏；在部署实现上，支持透明网桥模式，在网络上物理串联接入数据库防火墙系统 (DAS-FW)，所有用户访问的网络流量都串联流经设备，通过透明网桥技术，客户端看到的数据库地址不变。

## 3、“互联网 + 政务服务”系统安全漏洞扫描服务

系统安全漏洞扫描服务，针对系统、设备、应用的脆弱性进行自动化检测，帮助“互联网 + 政务服务”业务系统来侦测、扫描和改善其信息系统面临的风险隐患；检测某个政务特定设备的系统配置、系统结构和属性；执行安全评估和漏洞检测；提供漏洞修补建议，是“互联网 + 政务服务”系统进行信息系统合规度量和审计的一种基础技术手段。

随着 IT 规模的不断增大，在网络安全建设中面临千变万化的攻击手法，单纯采取被动防御的技术手段越发显得力不从心，更多的政府用户开始关注风险的管理与度量，侧重在“事前”尽量降低甚至规避风险。“探测与发现”漏洞全面性，同时增强了帮助用户“管理漏洞”侧重“修复”的能力，实现真正意义上的漏洞修复闭环，应对日益变化的安全漏洞形势；漏洞扫描是确定安全漏洞修补方案的最佳手段，及时查补“互联网 + 政务服务”系统安全漏洞，可以有效提高“互联网 + 政务服务”各平台、各系统的安全防护能力。

## 4、“互联网 + 政务服务”系统运维安全审计

“互联网 + 政务服务”系统涉及大量的网络设备、服务器、数据库等关键基础设施，需要在系统中部署安全审计堡垒机技术规范运维操作行为。通过在堡垒机上对运维人员的账户、运维操作进行统一的策略配置和过程审计，将原本无序的运维操作进行统一的规范管理。实现对运维人员的单点登录、权限控制、动作记录及违规告警。在部署实现上，将堡垒机与汇聚交换机相连的接口配置为工作口，并且配置内网 IP。核心应用服务器及数据库服务器上均设置防火墙控制规则，只允许堡垒机 IP 地址访问 3389 等运维服务端口，实现非授权用户的访问阻断。

## 5、“互联网 + 政务服务”系统安全态势感知系统建设

“互联网 + 政务服务”安全态势感知系统对骨干网络出口和重要网络节点，包括电子证照、统一身份认证、网上支付等系统进行严密监控，及时预警大规模网络攻击和病毒传播，保障重要系统的信息

系统的网络安全。宏观层面，安全态势感知平台严密监控、切实防范大规模病毒攻击和网络攻击；微观层面，安全态势感知平台监控保障重点信息系统的网络安全，实现安全事件的预警、检测、响应、取证。按照“统一规划、分级部署、协同共享”的原则，建设形成多级互联互通的通报平台，构建覆盖全网的网络安全态势感知、安全监测和通报预警体系，建立“互联网+政务服务”各方协同配合的信息安全防范、监测、通报、响应和处置机制。

## 6、“互联网+政务服务”系统安全服务

### (1)、“互联网+政务服务”系统安全监测服务

绿盟科技针对“互联网+政务服务”安全需求，提供7×24小时远程网站监测服务，通过不间断的远程专家值守，为客户“互联网+政务服务”业务系统提供远程安全监测、安全检查、实时响应和人工分析服务，是构建完善的“互联网+政务服务”安全体系的最好补充。“互联网+政务服务”安全监测内容包括远程网页挂马监测、网页敏感内容监测、网页篡改监测检测。

### (2)、新“互联网+政务服务”系统上线前评估

针对新上线的“互联网+政务服务”进行系统漏洞扫描、WEB应用漏洞扫描、安全基线核查与渗透测试。

利用相关安全设备和工具进行系统漏洞扫描、WEB应用漏洞扫描、安全基线核查，针对应用层的漏洞进行发现，并针对存在的漏洞提供合理的解决方案。渗透测试(Penetration Testing)是由具备高技能和高素质的安全服务人员发起、并模拟常见黑客所使用的攻

击手段对目标系统进行模拟入侵。渗透测试服务的目的在于充分挖掘和暴露“互联网+政务服务”系统的弱点，从而让管理人员了解其系统所面临的威胁。

### (3)、“互联网+政务服务”应用层防护设备巡检

针对WEB应用防护系统(WAF)、数据库防火墙系统(DAS-FW)、网络入侵保护系统(NIPS)、网络入侵检测系统(NIDS)等安全设备进行日志分析、规则库升级、设备状态查看等巡检、远程代维工作。

绿盟科技提供手机安全管家服务，该服务允许用户通过手机APP随时随地查看其安全设备运行状况，做好对安全问题的快速感知与应对。

### (4)、安全人才培养

“互联网+政务服务”总体战略部署，需要重视网络安全人才培养，针对“互联网+政务服务”的安全需求，开发专门的安全培训课程，提升“互联网+政务服务”网络安全人才的安全意识、安全知识和技能，组织安全攻防竞赛强化动手实践能力，选拔安全人才，进行安全人才队伍梯队建设。

## 结束语

“互联网+政务服务”安全保障体系，在国务院文件“意见”指导下，参考等保，结合当下的安全风险和威胁，进行有针对性的建设和改进，并持续循环提升安全能力，保障“互联网+政务服务”业务开展；笔者根据自己的经验及见识进行书写，或有不全之处，欢迎各位读者来信一同探讨。

# 物联网安全技术

创新中心 张星

关键词：物联网安全技术 物联网应用技术介绍  
异常行为检测 访问控制 区块链

摘要：本文将分别从已有技术在物联网环境中的应用、新技术的探索和物联网相关设备、平台、系统的漏洞挖掘和安全设计三个方面介绍物联网安全技术研究的一些思路。

本文是物联网安全系列文章的第二篇，通过上期物联网安全的需求与对策分析之后，我们总结出需要重点关注的《物联网安全技术》

## 一. 引言

物联网安全产品的核心在于技术，由于物联网的安全是互联网安全的延伸，那么我们可以利用互联网已有的安全技术，结合物联网安全问题的实际需要，改进已有技术，将改进后的技术应用到物联网中，从而解决物联网的安全问题。如：互联网环境中的防火墙技术，主要是对 TCP/IP 协议数据包进行解析，而在物联网环境中，防火墙还需要对物联网中的特定协议进行解析，如工控环境中的 Modbus、PROFIBUS 等协议。此外物联网还有其独特性，如终端

设备众多，设备之间缺乏信任的问题，互联网中现有的技术难以解决此类问题，所以我们还需要探索一些新的技术来解决物联网中特有的新问题。此外，由于物联网将许多原本与网络隔离的设备连接到网络中，大大增加了设备遭受攻击的风险。同时物联网中的设备资源受限，很多设备在设计时较少考虑安全问题。还有物联网中协议众多，没有统一标准等等这些安全隐患都可能被黑客利用，造成极大的安全问题，所以我们需要利用一些漏洞挖掘技术对物联网中的服务平台、协议、嵌入式操作系统进行漏洞挖掘，先于攻击者发现

并及时修补漏洞，有效减少来自黑客的威胁，提升系统的安全性。因此主动发掘并分析系统安全漏洞，对物联网安全具有重要的意义。

通过对物联网安全需求和对策的分析，我们总结出以下需要重点关注的技术。本章将分别从已有技术在物联网环境中的应用、新技术的探索和物联网相关设备、平台、系统的漏洞挖掘和安全设计三个方面介绍物联网安全技术研究的一些思路。

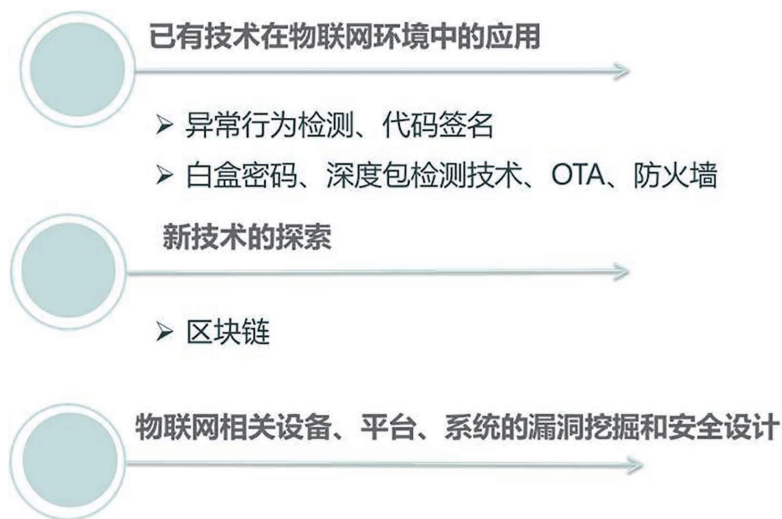


图 3.1 物联网安全相关技术

## 二、已有技术在物联网环境中的应用

### 2.1 异常行为检测

异常行为检测对应的物联网安全需求为攻击检测和防御、日志和审计。

文章前面已经提到过，异常行为检测的方法通常有两个：一个是建立正常行为的基线，

从而发现异常行为，另一种是对日志文件进行总结分析，发现异常行为。

物联网与互联网的异常行为检测技术也有一些区别，如利用大数据分析技术，对全流量进行分析，进行异常行为检测，在互联网环境中，这种方法主要是对 TCP/IP 协议的流量进行检测和分析，而在物联网环境中，还需要对其它的协议流量进行分析，如工控环境中的 Modbus、PROFIBUS 等协议流量。此外，物联网的异常行为检测也会应用到新的应用领域中，如在车联网环境中对汽车进行异常行为检测。360 研究员李均利用机器学习的方法，为汽车的不同数据之间的相关性建立了一个模型，这个模型包含了诸多规则。依靠对行为模式、数据相关性和数据的协调性的分析对黑客入侵进行检测。

### 2.2 代码签名

对应的物联网安全需求：设备保护和资产管理、攻击检测和防御。

通过代码签名可以保护设备不受攻击，保证所有运行的代码都是被授权的，保证恶意代码在一个正常代码被加载之后不会覆盖正常代码，保证代码在签名之后不会被篡改。

相较于互联网，物联网中的代码签名技术不仅可以应用在应用级别，还可以应用在固件级别，所有的重要设备，包括传感器、交换机等都要保证所有在上面运行的代码都经过签名，没有被签名的代码不能运行。

由于物联网中的一些嵌入式设备资源受限，其处理器能力，通信能力，存储空间有限，所以需要建立一套适合物联网自身特点的、综合考虑安全性、效率和性能的代码签名机制。

### 2.3 白盒密码

对应的物联网安全需求：设备保护和资产管理。

物联网感知设备的系统安全、数据访问和信息通信通常都需要加密保护。但由于感知设备常常散布在无人区域或者不安全的物理环境中，这些节点很可能会遭到物理上的破坏或者俘获。如果攻击者俘获了一个节点设备，就可以对设备进行白盒攻击。传统的密码算法在白盒攻击环境中不能安全使用，甚至显得极度脆弱，密钥成为任何使用密码技术实施保护系统的单一故障点。在当前的攻击手段中，很容易通过对二进制文件的反汇编、静态分析，对运行环境的控制结合使用控制 CPU 断点、观测寄存器、内存分析等来获取密码。在已有的案例中我们看到，在未受保护的软件中，密钥提取攻击通常可以在几个小时内成功提取以文字数据阵列方式存放的密钥代码。

白盒密码算法是一种新的密码算法，它与传统密码算法的不同点是能够抵抗白盒攻击环境下的攻击。白盒密码使得密钥信息可充分隐藏、防止窥探，因此确保了在感知设备中安全地应用原有密码系统，极大提升了安全性。

白盒密码作为一个新兴的安全应用技术，能普遍应用在各个行业领域、应用在各个技术实现层面。例如，HCE 云支付、车联网，在端点（手机终端、车载终端）层面实现密钥与敏感数据的安全保护；在云计算上，可对云上的软件使用白盒密码，保证在云这个共享资源池上，进行加解密运算时用户需要保密的信息不会被泄露。

### 2.4 over-the air (OTA)

对应的物联网安全需求：设备保护和资产管理。

空中下载技术（over-the air, OTA），最初是运营商通过移动通信网络（GSM 或者 CDMA）的空中接口对 SIM 卡数据以及应用进行远程管理的技术，后来逐渐扩展到固件升级，软件安全等方面。

随着技术的发展，物联网设备中总会出现脆弱性，所以设备在销售之后，需要持续的打补丁。而物联网的设备往往数量巨大，如果花费人力去人工更新每个设备是不现实的，所以 OTA 技术在设备销售之前应该被植入到物联网设备之中。

### 2.5 深度包检测 (DPI) 技术

对应的物联网安全需求：攻击检测和防御。

互联网环境中通常使用防火墙来监视网络上的安全风险，但是这样的防火墙针对的是 TCP/IP 协议，而物联网环境中的网络协议通常不同于传统的 TCP/IP 协议，如工控中的 Modbus 协议等，这使得控制整个网络风险的能力大打折扣。因此，需要开发能够识别特定网络协议的防火墙，与之相对应的技术则为深度包检测技术。

深度包检测技术（deep packet inspection, DPI）是一种基于应用层的流量检测和控制技术，当 IP 数据包、TCP 或 UDP 数据流



## ▶▶ 行业热点

通过基于 DPI 技术的带宽管理系统时，该系统通过深入读取 IP 包载荷的内容来对 OSI 七层协议中的应用层信息进行重组，从而得到整个应用程序的内容，然后按照系统定义的管理策略对流量进行整形操作。

思科和罗克韦尔 自动化联手开发了一项符合工业安全应用规范的深度数据包检测 (DPI) 技术。采用 DPI 技术的工业防火墙有效扩展了车间网络情况的可见性。它支持通信模式的记录，可在一系列安全策略的保护之下提供决策制定所需的重要信息。用户可以记录任意网络连接或协议（比如 EtherNet/IP）中的数据，包括通信数据的来源、目标以及相关应用程序。

在全厂融合以太网 (CPwE) 架构中的工业区域和单元区域之间，采用 DPI 技术的车间应用程序能够指示防火墙拒绝某个控制器的固件下载。这样可防止滥用固件，有助于保护运营的完整性。只有授权用户才能执行下载操作。

### 2.6 防火墙

对应的物联网安全需求：攻击检测和防御。

物联网环境中，存在很小并且通常很关键的设备接入网络，这些设备由 8 位的 MCU 控制。由于资源受限，对于这些设备的安全实现非常有挑战。这些设备通常会实现 TCP/IP 协议栈，使用 Internet 来进行报告、配置和控制功能。由于资源和成本方面的考虑，除密码认证外，许多使用 8 位 MCU 的设备并不支持其他的安全功能。

Zilog 和 Icon Labs 联合推出了使用 8 位 MCU 的设备的的安全解决方案。Zilog 提供

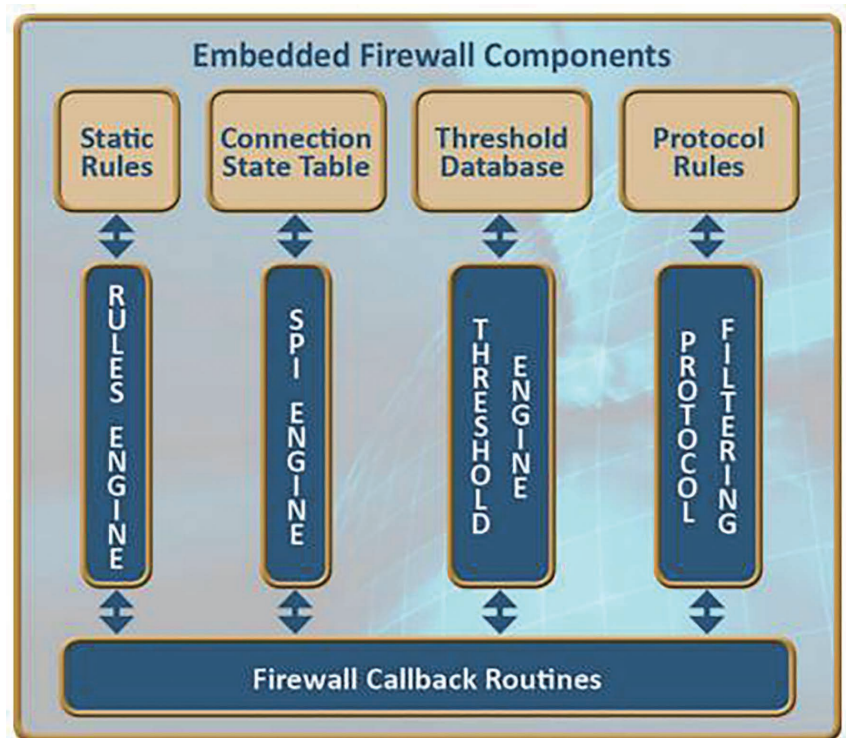


图 3.2 嵌入式防火墙

MCU, Icon Labs 将 Floodgate 防火墙 集成到 MCU 中, 提供基于规则的过滤, SPI (Stateful Packet Inspection) 和基于门限的过滤 (threshold-based filtering)。防火墙控制嵌入式系统处理的数据包, 锁定非法登录尝试、拒绝服务攻击、packet floods、端口扫描和其他常见的网络威胁。

## 2.7 访问控制

对应的物联网安全需求: 认证、访问控制管理

传统企业网络架构通过建立一个固定的边界使内部网络与外部世界分离, 这个边界包含一系列的防火墙策略来阻止外部用户的进入, 但是允许内部用户对外的访问。由于封锁了外部对于内部应用和设施的可见性和可访问性, 传统的固定边界确保了内部服务对于外部威胁的安全。企业网络架构中的固定的边界模型正在变得过时, BYOD 和钓鱼攻击提供了对于内部网络的不可信访问, 以及 SaaS 和 IaaS 正在改变边界的位置。

软件定义边界 (Software Defined Perimeter, SDP) 使得应用所有者部署的边界可以保持传统模型中对于外部用户的不可见性和不可访问性, 该边界可以部署在任意的位置, 如网络上、云中、托管中心中、私营企业网络上, 或者穿过这些位置的一些全部。

SDP 用应用所有者可控的逻辑组件取代了物理设备, 只有在设备证实和身份认证之后, SDP 才提供对于应用基础设施的访问。

大量设备连接到 Internet 中, 管理这些设备、从这些设备中提取信息的后端应用通常很关键, 扮演了隐私或敏感数据的监护人的角色。SDP 可以被用来隐藏服务器和服务器与设备的交互, 从而最

大化地保障安全和运行时间

## 三. 新技术的探索

### 3.1 区块链

对应的物联网安全需求: 认证

区块链 (Blockchain, BC) 是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案主要让参与系统中的任意多个节点, 通过一串使用密码学方法相关联产生的数据块 (block), 每个数据块中包含了一定时间内的系统全部信息交流数据, 并且生成数据指纹用于验证其信息的有效性和链接 (chain) 下一个数据库块。结合区块链的定义, 需要有这几个特征: 去中心化 (Decentralized)、去信任 (Trustless)、集体维护 (Collectively maintain)、可靠数据库 (Reliable Database)、开源性、匿名性。区块链解决的核心问题不是“数字货币”, 而是在信息不对称、不确定的环境下, 如何建立满足经济活动赖以发生、发展的“信任”生态体系。这在物联网上是一个道理, 所有日常家居物件都能自发、自动地与其它物件、或外界世界进行互动, 但是必须解决物联网设备之间的信任问题。

越来越多的侵犯用户隐私的报告说明第三方收集和大量的个人数据的模式需要被改变。IBM 认为物联网设备的运行环境应该是去中心化的, 它们彼此相连, 形成分布式云网络。而要打造这样一种分布式云网络, 就要解决节点信任问题——在传统的中心化系统中, 信任机制比较容易建立, 存在一个可信的第三方来管理所有

的设备身份信息。但是物联网环境中设备众多，可能会达到百亿级别，这会对可信第三方造成很大的压力。IBM 认为中本聪的比特币区块链技术可以完满地解决这个问题。

Guy Zyskind 等人提出一种分散式的个人数据管理系统，来实现用户数据的保护，确保用户可以拥有并管理自己的数据。实现了将区块链应用于自动访问控制管理而不需要可信第三方。与比特币不同，系统交易 (transaction) 不是严格的金融交易——他们被用于携带指令，比如存储、查询和共享数据的指令。

#### 四· 物联网相关设备、平台、系统的漏洞挖掘和安全设计

物联网相关设备、平台、系统的漏洞挖掘技术，有助于发现 0day 漏洞和未知威胁，从而提升 IDS、防火墙等安全产品的检测和防护能力。

将安全产品嵌入到设备之中，或者产品设计时采用物联网设备安全框架，在物联网设备生产之时就考虑安全问题，可以极大提升物联网设备的安全性。

##### 4.1 物联网平台漏洞挖掘

随着物联网的发展，将会出现越来越多的物联网平台。BAT 三家均已推出了智能硬件开放平台。国外免费的物联网云平台有 Temboo、Carriots、NearBus 和 Ubidots。不过，目前对于物联网平台的安全性的分析还不多，相信以后物联网平台的安全性将会越来越多地吸引到人们的关注。

Samsung SmartThings 是一个智能家庭编程平台，谷歌根

大学和微软研究院的研究人员对其上的 499 个应用和 132 个设备管理器 (device handlers) 进行了静态代码分析 (static code analysis)，论文发表在 S&P 2016 上。主要有两点发现，一是，虽然 SmartThings 实现了一个特权分离模型 (privilege separation model)，但是，有两个固有的设计缺陷 (intrinsic design flaws)，可导致 APP 越权；二是关于 SmartThings 的事件子系统，设备与 APP 之间通过其进行异步通信，该系统并未对包含敏感信息 (如 lock codes) 的事件提供足够的保护。研究人员利用框架设计漏洞实现了四个攻击的概念证明：修改门锁密码，窃取已有的门锁密码，禁用家庭的假期模式，触发一次虚假的火灾告警。

##### 4.2 物联网协议的 0Day 漏洞主动挖掘技术

在现代的汽车、工控等物联网行业，各种网络协议被广泛使用，这些网络协议带来了大量的安全问题。很多研究者开始针对工控等系统，特别是具有控制功能的网络协议的安全性展开研究。研究人员在 QCon2016 的议题中提到用网络协议 fuzzing 技术对 0Day 漏洞进行挖掘。

##### 4.3 物联网操作系统漏洞挖掘

物联网设备大多使用嵌入式操作系统，嵌入式系统通常内核较小，专用性强，系统精简，高实时性，安全在嵌入式系统中处于较低的位置，随着设备逐渐接入互联网，操作系统的安全性需要重点关注。

2015 年，44CON 伦敦峰会中，研究人员采用了 Fuzzing 框架 Sulley 对 VxWorks 系统的多个协议进行了 Fuzzing，挖掘到一些漏

洞，并结合 VxWorks 的 WDB RPC 实现了一个远程调试器，进行了相关调试分析

#### 4.4 嵌入式设备安全框架

嵌入式设备众多，而且大多在安全设计方面考虑不足。联网的设备往往存在极大的潜在威胁。作为设备制造商，应在嵌入式设备的设计过程中就将安全框架考虑进入，对嵌入式设备进行安全设计。

Icon Labs 是嵌入式设备安全厂商，提出 Floodgate 安全框架，用于构建安全的嵌入式设备。Floodgate 安全框架模块既可以作为单独的产品使用，也可以集成到已有的嵌入式 Linux 和任何 RTOS 中。

Floodgate Firewall，是一个嵌入式防火墙，提供状态包检测 (Stateful Packet Inspection, SPI)、基于规则的过滤和基于门限的过滤来保护嵌入式设备免受来自互联网的威胁。

Floodgate IDS 对嵌入式 Linux 和 RTOS 设备提供保护，其能检测出固件、配置信息和静态数据的改变。

Floodgate Secure Boot 确保只有从 OEM 认证的固件才允许在这台设备上运行。

Floodgate Agent 提供对于嵌入式和物联网设备的态势感知、安全事件报告、命令审计日志和安全策略管理，同时也提供与企业安全管理系统的集成。

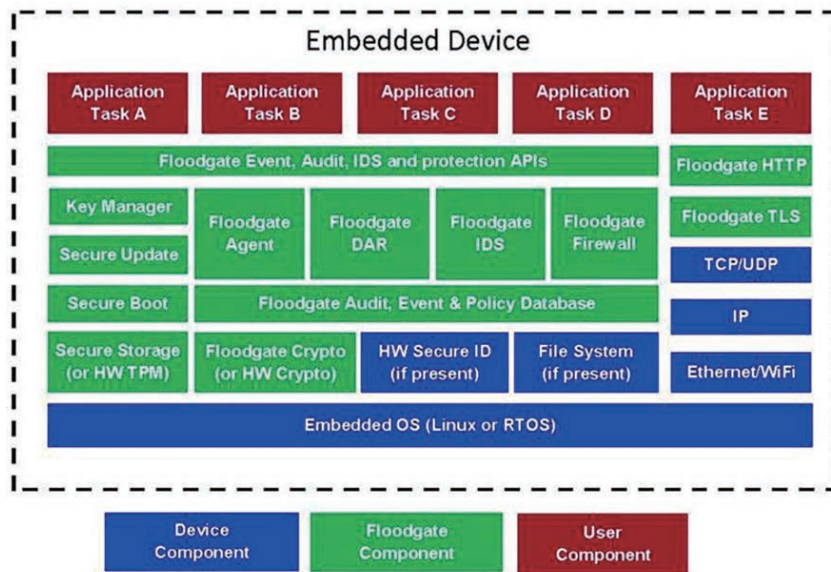


图 3.3 Floodgate 架构

## 五. 物联网安全公司及产品介绍

消费行业的市场处于物联网普及的开端，可穿戴设备、智能家庭产品、照明设备和其他的智能设备正在成为主流。全球的多个城市也正在采用物联网，依赖于从数以千计的按地理位置分布的不同类型的传感器捕获的数据，它们正在往智慧城市的道路上发展。

在下期本章中，笔者选取了五家公司，在介绍公司产品的同时，也会对其所关注的行业的需求进行一个介绍。

# 互联网企业的等级保护建设之路

能源企业技术部 孟凡勇

关键词：互联网 等级保护 网约车

摘要：随着互联网企业的迅猛发展，其自身核心业务安全性的不断提升和行业监管力度的不断加强，如何应对与日俱增的内部需求和外部驱动，本文分析了互联网企业面临的安全威胁及合规监管，以及业内现有的针对该行业的安全建设内容，然后提出了我们基于三级等保的互联网企业信息安全建设思路，从整体上发现并解决互联网行业的安全问题。

## 序 - 互联网企业的兴盛与隐患

1994年，中国通过一条64K的国际专线接入互联网。20年后，互联网带给整个中国经济模式的改变已经影响到了社会的方方面面。可以说，互联网极大地改变了中国，而这种改变仍在继续。

中国拥有庞大的网民数量，大量的需求被创造，给新的互联网行业形态出现奠定良好基础。其次，中国互联网行业的商业模式日渐成熟。网络广告、搜索引擎、电子商务、网络支付等业务日渐被人接受，各大互联网公司从各自核心领域优势向这几个方面渗透，形成有序竞争，带动互联网行业良性发展。再次，中国网络基础设施的建设、4G/5G互联网的发展、国家政策的扶持规划，均给整个互联网行业创造了一个非常好的前景。

中国的互联网企业发展迅速，目前已有多家跻身全球互联网公

司市值排行榜top10中，像大家熟知的阿里巴巴、京东、腾讯及百度均榜上有名。

相对于传统行业，互联网行业还显得很年轻，在一派欣欣向荣的快速发展背后，互联网行业同时隐藏着让人难以捉摸的巨大的安全风险，由于技术和监管的诸多问题，使得该行业已陷入危机四伏的困境中。

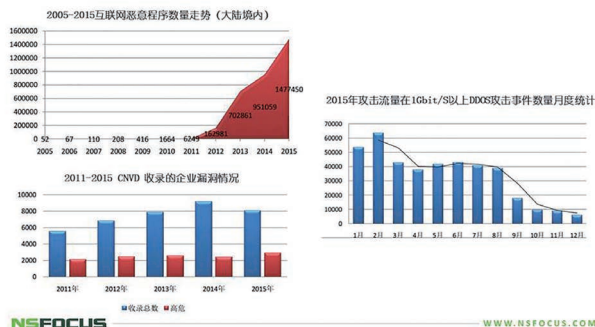
2016年4月3日，土耳其爆发重大数据泄露事件，近5000W土耳其公民个人信息被黑客打包放置网络上任人下载。为证明被盗数据的真实性，黑客还公布土耳其现任总统埃尔多安的个人信息以作示范。

2016年7月29日，越南两个机场被黑客攻击，这是越南遭受迄今最严重的黑客攻击事件。黑客通过攻陷机场电子显示屏及广播

系统，散发“南海是中国的固有领土”等信息，给机场候机的乘客带来视觉和听觉上的冲击，造成的混乱远超常见的攻击网页行为。

而在最近披露的一项报道中，俄罗斯黑客成功盗取了2.723亿个帐号，以俄罗斯最受欢迎的电子邮件服务 Mail.ru 用户为主，此外还有 Gmail 地址、雅虎以及微软电邮 Hotmail 用户。数以亿计的数

源系统，这些系统存在大量风险漏洞，安全性严重缺乏保障，企业数据安全岌岌可危。那么知名大企业又如何呢？随着互联网技术的发展，黑客技术也在升级，企业投入巨大财力和人力研发的系统，同样存在不可预知的问题。因此，也不可避免的遭受黑客的恶意攻击。近年来，知名大企业数据泄露事件频频发生，逐年增多。



据目前正在“俄罗斯的地下黑市”出售。

不只是境外企业，国内互联网企业也正在成为最大的受害者。2016上半年，全国互联网企业安全漏洞总量同比增长181.9%。相关人士表示，目前互联网行业存在很大的安全隐患，而且伴随着相当程度的数据泄露风险。

**起 - 黑客重点攻击的行业目标**

作为一种新生事物，互联网企业起步于民营企业，很多小平台风险意识淡薄，把关注重点放在扩大客户规模、赚取利润上。而技术防护则严重缺失，另外出于成本考虑，大多数企业采用廉价的开

据调查统计，黑客攻击互联网企业平台的目的主要为窃取数据，占比高达48%，其次为敲诈勒索和商业竞争。

通过攻陷大批互联网企业平台，引起系统瘫痪，黑客还能将数据恶意修改、洗劫一空。此外，黑客还可能通过申请账号、篡改数据、冒充投资人进行恶意提现甚至盗取资金。

企业数据泄露，造成的不只是业务的巨大损失，更为重要的是信誉上的丧失。互联网企业的门户网站作为信誉展示的首要平台，如果因为网站信息泄露、宕机、页面篡改等原因导致用户信任丧失，那么平台也就丢失了本身的信誉，成为无源之水。

因此，互联网企业如何有效保护信息安全，事关企业生死存亡。

### 转 - 国家信息安全的基本保障制度

互联网行业是需要依托互联网的，其核心业务需要 IT 系统的支撑，因此安全是首当其冲的。而等级保护是国家推行的在 Cyber 空间安全的强制保护制度，其最终目的是保护信息系统和基础信息网络不受到侵害，保护用户的业务数据和系统的服务功能。

等级保护发展历程



从 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》（147 号令）开始，到今年（2016 年）10 月份在昆明举办的由公安部网络安全保卫局、中央网信办网络安全协调局、工信部网络安全管理局、国家密码管理局、国家保密局、中国科学院办公厅为指导单位和由公安部第三研究所主办的第五届全国信息安全等级保护技术大会上提出的进入等级保护制度 2.0 时代为止，等级保护这一项国家政策已经走过逾 20 个年头，等级保护不仅是对信息安全产品或系统的检测、评估以及定级，更重要的，它是围绕信息安全保障全过程的一项基础性的国家管理制度，是一项基础性和制度性的工作。

如何帮助互联网企业有效的防范网络入侵、网络拒绝服务攻击以及网络非法监听等恶意网络行为，就有必要了解相应的合规要求。而国家等级保护标准中对于网络安全方面的要求，特别是对网络安全管理、访问控制、入侵防范、网络设备防护、安全审计的相关条款对于和网络密不可分的互联网企业来说，确实有着十分重要且重大的意义。

### 赋 - 等级保护之于互联网企业的意义

在互联网产业不断融合的态势下，互联网跨界融合竞争的趋势越发凸显，线上与线下问题不断交织，新现象、新问题不断涌现，政府的管理也面临前所未有的挑战。因此从 2015 年，工信部开始进一步加强和改进互联网行业管理，促进互联网企业良性有序发展。”

信息安全是永远不变的话题，工信部部长苗圩认为应该高度重视我们所面临的严峻安全形势，大力提升网络与信息安全的保障能力。“促进互联网融合发展，安全是基础，更是保障，必须处理好安全与发展的关系，做到协调一致。不断健全互联网行业网络和信息安全机制，持续推进信息安全和体制化建设，推动完善网络安全的法律法规、标准体系，严格落实互联网企业信息安全的责任，加强网络信息安全监管和网络环境的综合治理。”

除却自身发展面临的网络安全问题，国家有关部门对互联网行业网络安全方面的监管力度也逐年增加。在内部需求和外部监管的双重压力下，加快互联网企业信息安全等级保护建设显得迫在眉睫。

国家等级保护的核心思想：

- 全方位划分安全等级是实施信息安全等级保护的基本条件；
- 信息系统等级化安全设计是实施信息安全等级保护的基本方法。

- 信息安全技术和信息安全管理是实现信息系统安全的基础。

对信息安全技术和信息安全管理进行等级划分是信息系统安全等级保护的需要，也是对信息安全技术和信息安全管理进行规范化的需要。

企业必须根据安全建设目标将需求分析结果进行逐步细化，并转化为信息安全体系建设的总体安全策略，根据登记保护建设的具体要求，可以形成技术层面的安全管理和安全管理层面的安全策略并通过总体安全策略的落实构建安全技术体系和安全管理体系框架。

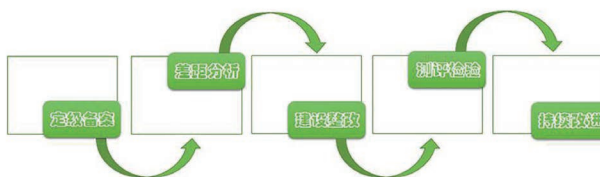
对抗能力和恢复能力已然构成了信息系统的安全保护能力。安全保护能力主要表现为信息系统应对威胁的能力，但当信息系统无法阻挡威胁对自身的破坏时，信息系统的恢复能力使系统在一定时间内恢复到原有状态，从而降低负面影响。

对于互联网企业来说，实施信息安全等级保护测评能够有效地提高企业信息系统安全建设的整体水平，有效控制企业信息安全管理成本；有利于明确国家、法人和其他组织、公民的信息安全责任，加强企业信息安全管理。

对于企业的信息系统来说，通过等级保护测评可及时发现信息系统安全状况并制定方案进行整改，当信息系统完全达到安全保护能力要求时，信息系统就基本可做到“进不来、拿不走、改不了、看不懂、跑不了、可审计、打不垮”。

### 比 - 互联网企业的等级保护解决方案

按照国家信息安全等级保护的相关标准，互联网企业一般通过第三方测评机构或安全厂商按照如下流程进行等级建设：



同时，按照等级保护中针对技术和管理的不同要求，应持续开展如下工作：

**【保障基础设施安全】**保障网络周边环境和物理特性引起的网络设备和线路的持续使用。

**【保障网络连接安全】**保障网络传输中的安全，尤其保障网络边界和外部接入中的安全。

**【保障计算环境的安全】**保障操作系统、数据库、服务器、用户终端及相关商用产品的安全。

**【保障应用系统安全】**保障应用程序层对网络信息的保密性、完整性和信源的真实的保护和鉴别，防止和抵御各种安全威胁和攻击手段，在一定程度上弥补和完善现有操作系统和网络信息系统的安全风险。

**【保障数据安全及备份恢复】**保障数据完整性、数据保密性、备份和恢复等。

**【安全管理体系保障】**根据国家有关信息安全等级保护方面的

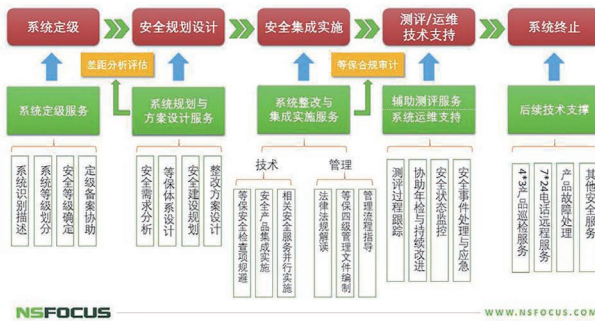


▶▶ 行业热点

标准和规范要求，建立一套切实可行的安全管理体系，加强安全管理机制。

兴 - 巨人背后的安全专家

针对互联网企业的信息安全等级保护建设，绿盟科技作为国内安全厂商当仁不让的领军品牌，基于对信息安全的深刻理解，以为互联网客户信息系统构建“等级化的安全体系”为等级保护工作的服务理念，旨在根据等级保护不同等级、不同阶段的业务特性、安全需求及安全应用重点，为互联网客户在等级保护的框架下构建一个



安全、可靠、灵活、可持续改进的信息安全体系。

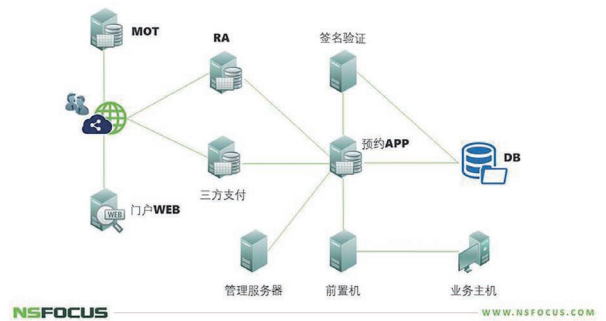
由于网约车新政的落地实施，交管局明令要求各大网约车平台尽可能快的进行线上业务系统的三级等级保护测评，因为最终测评通过与否关系着该平台营业执照的办理。

以下以易到租车为例，详细阐述绿盟科技针对互联网用户的信

息安全等级保护建设。

各网约车平台由于自身业务系统的差异，对预约系统应用架构会有不同的设计，但基本的技术构成是类似的，其各部分的功能也相似。

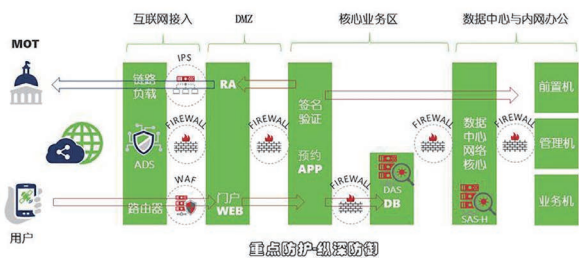
针对易到租车预约 APP 核心应用的等保三级安全建设，绿盟科技本着“重点防护，纵深防御”的原则，在各服务器区以防火墙作为区域安全边界，为提高预约业务的整体安全性，各区域边界防火墙采用功能与性能兼备的产品，由此在整体布局上形成了“多层异构防火墙”安全架构。从业务功能上考虑，把这种安全架构划分成四个



安全区域: 互联网接入区、DMZ 区 (接入 WEB 服务器、RA 服务器)、核心业务区 (接入 APP 服务器、DB 服务器)、数据中心内网区。

互联网接入区：

- 部署链路分担设备，提供多 ISP 的互联网接入。
- 部署流量清洗，防御 DDOS 攻击



NSFOCUS

WWW.NSFOCUS.COM

系统定级阶段	规划设计阶段	实施实现阶段	运行管理阶段
《等级保护培训课件（系列）》	《等级保护现状分析报告》	《等级保护总体设计方案》	《信息安全通告》（定期）
《等级保护现状分析报告》	《等级保护现状分析报告》 (含管理调研和技术调研结果)	《等级保护解决方案》	《等级保护自查报告》
《等级保护定级分析报告》	技术调研包括： 架构分析、 漏洞扫描、 人工检查、 渗透测试、 代码审计等	《等级保护整改方案》	《等级保护培训课件（系列）》
		《等级保护安全加固报告》	
		《等级保护安全管理文件（系列）》	
	《等级保护差异分析报告》	《等级保护培训课件（系列）》	
	《等级保护安全规划》		
	《等级保护整改方案》		
	《等级保护培训课件（系列）》		

NSFOCUS

WWW.NSFOCUS.COM

- 部署外网边界防火墙，实现互联网与 DMZ 区隔离

DMZ 区：

- 部署 WAF，为 WEB 服务器提供深层次的安全保护；
- 部署 WEB-APP 边界防火墙，实现 DMZ 与核心业务区的隔离；

核心业务区

- APP 服务器与 DB 服务器间可部署防火墙实现访问控制；
- 部署内网边界防火墙，实现核心业务区与数据中心服务器区

间的隔离；

- DB 服务器旁路接入 DAS，实现对数据库的监听与审计

数据中心内网区

采用“核心——边缘”分区模块化架构，各服务器区围绕网络核心区部署，

- 各服务器区与网络核心区之间通过防火墙做访问控制；
- 内网核心旁路接入 SAS-H，实现对 IP 可达的所有设备的单

点登录及运维审计

安全技术手段作为支撑，辅以绿盟科技等保咨询服务，为客户搭建信息安全管理与策略体系。如此双管齐下，既能满足国家信息安全等级保护相关政策与标准要求，又可为客户搭建等级化的安全保障体系，在全面防护中突出重点，帮助客户最终通过等保三级测评，不仅提升了安全防护能力，也间接增强了客户的核心竞争力。

### 终-NSFOCUS 伴您扬帆远航

互联网行业的三级安全等保技术要求，既有与其它行业要求的共性，又有其自己的特点。

三级等保对于互联网企业既是一次命题考试，又是一次切实提升企业安全能力的好机会。作为等保技术要求的主要部分——网络安全，因其分散、覆盖面广和难以管理，也是整个等保安全的难点。绿盟科技从网络与安全融合、终端与边界融合、集中与分级融合等多个维度，覆盖了包括结构安全、访问控制、安全审计、边界完整性、入侵防范、恶意代码入侵和设备防护在内的绝大多数技术要求，为互联网客户提供完整的三级等保解决方案方案。

# Android Intent 攻击概说

安全能力中心 周振

关键词：Android；Intent；Intent Spoofing；intent scheme URLs 攻击

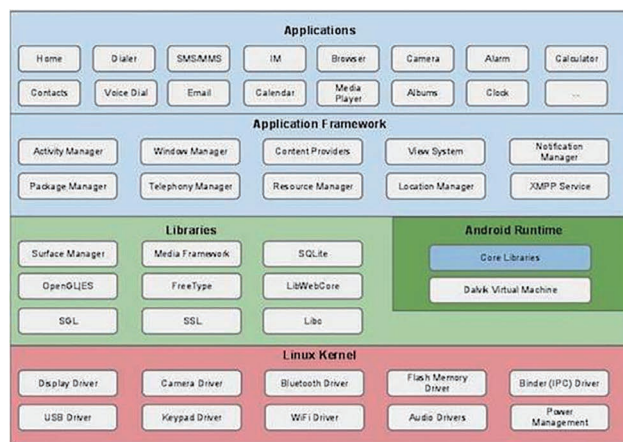
摘要：Intent 是一个将要执行的动作的抽象的描述，一般来说是作为参数来使用，由 Intent 来协助完成 android 各个组件之间的通讯。比如说调用 startActivity() 来启动一个 activity，或者由 broadcastIntent() 来传递给所有感兴趣的 BroadcastReceiver，再或者由 startService()/bindService() 来启动一个后台的 service。所以可以看出来，intent 主要是用来启动其他的 activity 或者 service，所以可以将 intent 理解成 activity 之间的粘合剂。

## 一、Android 的安全模型

Android 基于 Linux 操作系统开发，因此在安全的设计上借鉴了许多 Linux 的安全设计，比如利用了 UID、GID 的机制，但是 Google 根据手机操作系统的特点，对 Android 系统的安全体系重新进行设计和加强，本章将对 Android 的安全模型进行简要的介绍。

从大的角度来说，Android 本身属于分层设计，一共有 4 个大的层次，如下图所示：

所以显而易见的是，用户态的程序和内核态的程序之间是相互隔离的。内核态之上是 Android Runtime 和基础组件，再往上就到



了 Android Framework, Android Framework 就是 Google 提供的 SDK, 最上一层是各种 Application。从总体上看 Android 系统的安全模型由下面几部分 application sandbox、selinux、permissions 和 application signing。

### 1.1 Application sandbox

---

Android 系统在 app 安装时为每一个 app 分配一个唯一的 UID, app 运行时以此 UID 的身份启动进程, 此外 Android 系统还为每一个 app 分配一个指定的数据目录, 只有这个 app 才拥有对该目录的读写权限。所以每个 App 在进程级别和文件级别都是相互隔离的, 这就是 Android 系统的 application sandbox。

```
$ ps
u0_a37 16973 182 941052 60800 ffffffff 400d073c S com.
google.android.email
u0_a8 18788 182 925864 50236 ffffffff 400d073c S com.
google.android.dialer
u0_a29 23128 182 875972 35120 ffffffff 400d073c S com.
google.android.calendar
u0_a34 23264 182 868424 31980 ffffffff 400d073c S com.
google.android.deskclock

# ls -l /data/data/com.google.android.email
drwxrwx--x u0_a37 u0_a37 app_webview
drwxrwx--x u0_a37 u0_a37 cache
drwxrwx--x u0_a37 u0_a37 databases
```

```
drwxrwx--x u0_a37 u0_a37 files
```

### 1.2 Permissions

---

因为每个 App 都在一个独立的 application sandbox 里, app 的能力是非常受限的,

只对 UID 所拥有的进程和文件资源有权限, 为了实现功能更加丰富的 App, App 可以向 Android 系统申请权限。App 向 Android 系统申请的权限定义在 AndroidManifest.xml 中。在 App 安装时 Android 系统将向用户显示 App 所申请的权限, 只有用户授权 App 才能被安装到系统。App 并不能获得所有的权限, 有些权限只有 Android 系统自带的 app 才能获得。

### 1.3 Application signing

---

Android 系统中所有的 App 都必须签名, 以标识 app 开发者的身份。在更新 App 时

Android 系统检查更新的 App 的签名是否和系统中安装的 app 一致。系统应用则用 platform keys 签名, 许多权限只有使用 platform keys 签名的程序才能获得, 这样又进一步提高了 Android 系统的安全性。

### 1.4 SELinux

---

早期 Android 系统的安全模型主要依靠安装 app 时分配的 UID 和 GID。而 Linux 的默认的访问控制策略是 DAC (discretionary access control), 这意味着用户取得的权限是可以传递的, 一个用户获得了对某个资源的访问权限, 他可以将这种权限传递给其他用户。SELinux(security Enhanced Linux) 使用的则是 MAC 访问控

制策略，在 Android 4.3 被集成到 Android 的内核。MAC 定义了一系列系统范围的访问授权规则，只有系统管理员才能修改这些规则，其他用户无法覆盖和将其获得的对系统资源的访问权限传递给其他用户。在 Android 系统中，SELinux 主要用于隔离系统关键 daemon 进程和 App 的进程。

## 二 . Intent 介绍

正是因为 Application sandbox 的存在，App 进程之间是相互隔离的。有下面一个场景一个 App 需要调用 weixin 来分享内容，如何处理？这就需要用到 intent，告诉 Android 系统你的意图是什么，Android 系统将调用相应的处理程序来处理。

Intent 是一个将要执行的动作的抽象的描述，一般来说是作为参数来使用，由 Intent 来协助完成 android 各个组件之间的通讯。比如说调用 `startActivity()` 来启动一个 activity，或者由 `broadcastIntent()` 来传递给所有感兴趣的 `BroadcastReceiver`，再或者由 `startService()/bindService()` 来启动一个后台的 service。所以可以看出来，intent 主要是用

来启动其他的 activity 或者 service，所以可以将 intent 理解成 activity 之间的粘合剂。

Intent 有两种类型，Explicit Intent 和 Implicit Intent。下面将对者两种 Intent 进行说明。

### 2.1 Explicit Intent

明确指定 Intent 的名字（全类名），当你使用 Explicit Intent 启动 Activity 或者启动 Service，Android 系统会立即启动 Intent 对象所指定的 Component。

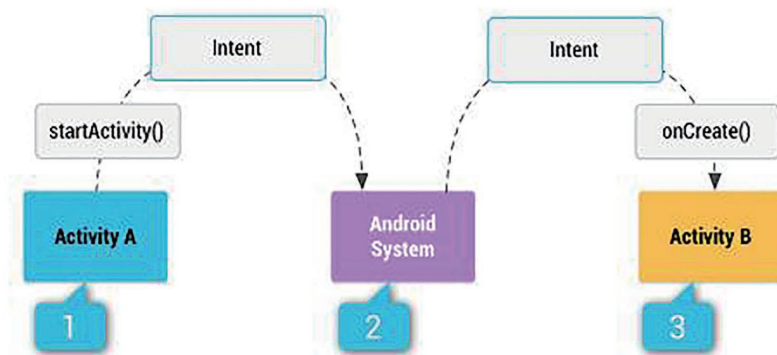
```
Intent downloadIntent = new  
Intent(this, DownloadService.class);
```

```
downloadIntent.setData(Uri.  
parse(fileUrl));
```

```
startService(downloadIntent);
```

### 2.2 Implicit Intent

指定 Intent 的 ACTION，当你使用 Implicit Intent，Android 系统将通过比较 App Manifest 文件中所定义的 Intent filter 来启动符合要求的 Component。如果只有一个 Intent filter 被匹配成功，系统将启动对应的 Component，并递送 Intent Object。如果有多个 intent filter 是兼容的，系统将显



示一个 dialog, 用户可以选择需要使用的 component.

```
Intent sendIntent = new Intent();
sendIntent.setAction(Intent.ACTION_SEND);
sendIntent.putExtra(Intent.EXTRA_TEXT, textMessage);
sendIntent.setType(HTTP.PLAIN_TEXT_TYPE); // "text/plain" MIME type

// Verify that the intent will resolve to an activity
if (sendIntent.resolveActivity(getPackageManager()) != null) {
    startActivity(sendIntent);
}
```

### 2.3 intent scheme URL

下面是一个使用了 Intent Scheme URL 的页面, 这个页面插入了一段 javascript 代码, 将页面重定向到一个 Intent scheme URL 链接。

```
<script>
location.href = "intent:mydata1#intent;action=myaction1;type=text/plain;end" ;
</script>
```

如果浏览器支持 Intent scheme URL, 加载页面时, 将根据 URL 自动生成 intent 对象, 并且调用对应的 activities。Google 的文档中对 Intent Scheme URL 是这么介绍的。

```
https://developer.chrome.com/multidevice/android/intents
A little known feature in Android lets you launch apps directly
```

from a web page via an Android Intent. One scenario is launching an app when the user lands on a page, which you can achieve by embedding an iframe in the page with a custom URI-scheme set as the src, as follows: <iframe src="paulsawesomeapp://page1"></iframe>. This works in the Chrome for Android browser, version 18 and earlier. It also works in the Android browser, of course.

The functionality has changed slightly in Chrome for Android, versions 25 and later. It is no longer possible to launch an Android app by setting an iframe's src attribute. For example, navigating an iframe to a URI with a custom scheme such as paulsawesomeapp:// will not work even if the user has the appropriate app installed. Instead, you should implement a user gesture to launch the app via a custom scheme, or use the "intent:" syntax described in this article.

从 Google 官方的介绍的文字中, 我们可以知道, Intent scheme URL 其实就是定义了一套语法, 使得 web 页面可以直接调用 Android 的 application。要使用 Intent scheme 必须遵循相应的语法规则, Google 的官方文档中有相应的说明:

```
intent:
HOST/URI-path // Optional host
#Intent;
package=[string];
action=[string];
```

```
category=[string];
component=[string];
scheme=[string];
end;
```

我们来尝试解析下面这个链接：

```
intent://foobar/#intent;action=myaction;type=text/plain;S.xyz=123end
```

按照上面的语法得到的解析结果：

```
intent:
//foobar/
#Intent;
action=myaction
type=text/plain
S.xyz = 123
end;
```

翻译成 java 代码，上面的 URL 等价于

```
Intent intent = new
Intent(“myaction”);
intent.setData(Uri.parse(“//
foobar/”));
intent.setType(“text/plain”);
intent.putExtra(“xyz”, “123”);
```

启动的组件必须在 AndroidManifest.

xml 中定义 intent-filter

```
<intent-filter>
<action android:name="android.intent.action.VIEW"/>
<category android:name="android.intent.category.DEFAULT"/>
<category android:name="android.intent.category.BROWSABLE"/>
<data android:scheme="zxing" android:host="scan" android:path="/">
</intent-filter>
```

为了加强安全性，Google 规定只有调用的组件的 Intent filter 的 category 为 android.

Browser	Intent Scheme Support	App Package Name	Version
Old Stock Browser	✓	com.android.browser	(for Android 4.2.2)
Chrome for Android	✓	com.android.chrome	30.0.1599.92
Opera browser for Android	✓	com.opera.browser	16.0.1212.64462
Samsung Browser	✓	com.sec.android.app.sbrowser	1.0 (on Galaxy S4)
Firefox for Android	—	org.mozilla.firefox	26.0

intent.category.BROWSABLE 才能被浏览器直接调用，对 Intent scheme 做了必要的限制，确保只有必要的组件才能被启动。

基本上主流的手机浏览器都支持 Intent Scheme URL，下表是一个概况。

### 三 . 和 Intent 相关的安全问题

#### 3.1 Intent Spoofing

Android Intent Spoofing 是一个比较常见的问题。如果 Android 组件

(component,service receiver) 是导出的话 (exported=true), 恶意程序可以使用 Explicit Intent 向这个组件 发送 Intent, Android 无法识别这个 Intent 是谁发送的, 将会正常的执行请求的操作。

### **android:exported**

<http://developer.android.com/guide/topics/manifest/receiver-element.html>

Whether or not the broadcast receiver can receive messages from sources outside

its application — "true" if it can, and "false" if not. If "false", the only messages

the broadcast receiver can receive are those sent by components of the same

application or applications with the same user ID.

The default value depends on whether the broadcast receiver contains intent filters.

The absence of any filters means that it can be invoked only by Intent objects

that specify its exact class name. This implies that the receiver is intended

only for application-internal use (since others would not normally know the class name).

So in this case, the default value is "false". On the other hand, the presence

of at least one filter implies that the broadcast receiver is intended to receive

intents broadcast by the system or other applications, so the default value is "true".

This attribute is not the only way to limit a broadcast receiver's external exposure.

You can also use a permission to limit the external entities that can send it

messages (see the permission attribute).

从上面的描述中可以发现, 关键是 component 要是导出的, 而 Android 的 component 的导出的默认值并不是固定的, 这点我们从 Google 提供的文档可以证实。

我们在 Android 系统下写了一个程序测试具体的情况。

### **AndroidManifest.xml**

```
<receiver
    android:name=".PhoneReceiver"
    android:enabled="true">
    <intent-filter>
        <action android:name="com.nsfocus.test" />
    </intent-filter>
</receiver>
```

测试程序注册了一个 Receiver, 这个 Receiver 处理 com.nsfocus.test Intent, 包含了一个 Intent Filter, 在 AndroidManifest.



xml 中没有明确声明这个 receiver 是导出的还是未导出的。

receiver 的代码为

```
public void onReceive(Context
context, Intent intent) {
    Toast.makeText(context, "Get it",
Toast.LENGTH_LONG).show();
}
}
```

使用 adb shell 中发送广播

```
adb shell am broadcast -a com.
nsfocus.test
```

可以看到 Get it 的提示信息，也就是说 component 处理 Implicit Intent 时默认是 exported=true 的，这就是问题的关键。

下面修改代码改成 exported=false，看看是什么情况。

#### AndroidManifest.xml

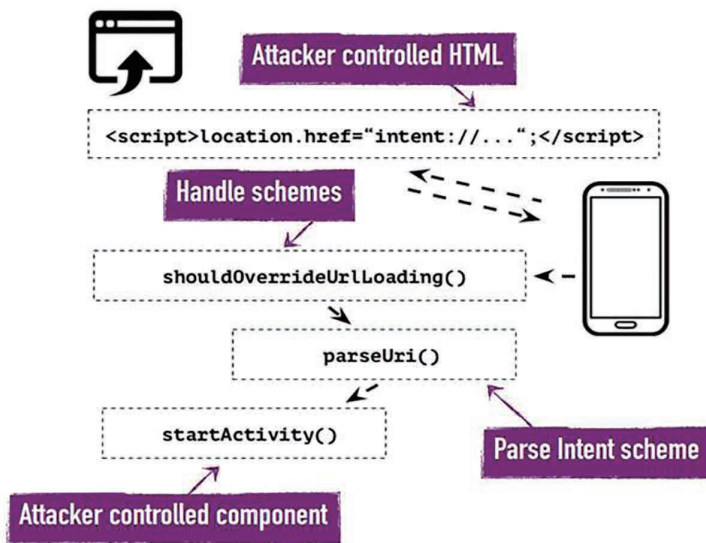
```
<receiver
    android:name=".PhoneReceiver"
    android:enabled="true"
    android:exported="false">
    <intent-filter>
```

```
<action android:name="com.nsfocus.test" />
</intent-filter>
</receiver>
```

receiver 照样可以收到，显示 "Get it"，所以在 receiver 里做校验是非常有必要的。因为无论 exported 如何设置，只要里面包含了 Intent Filter 就可以接受到消息。

### 3.2 intent scheme URLs 攻击

Intent scheme URL 可以被用来攻击浏览器 app，主要目标是未导出 (exported) 的 activities，这很可能导致信息泄漏等问题。Intent scheme URL 还可以被用来攻击其它 app，利用 app 程序原先的逻辑，精心构造 Intent 对象，将可能进行远程攻击，下图是一个可能的攻击路径。我们将在后续的漏洞实例章节进行详细地介绍。



# 大数据安全平台威胁分析

安全平台中心 吴天昊 创新中心 吴子建 合作产品部 施岭

关键词：大数据平台 安全威胁 数据泄露

摘要：大数据时代的到来，颠覆了各个领域的固有模式，在各行各业都引发了巨大的变革，“数据驱动业务”成为了新的全球趋势；同时也为信息安全行业带来了前所未有的挑战，系统架构的更新、业务模式的变革，使得大数据时代的安全形势与传统的安全形势相比变得更加复杂。

## 一. 引言

近年来，数据量呈爆炸式增长，截止到 2013 年，数据量已经从数据量已经从 TB 级别跃升到 PB、EB 乃至 ZB 级别。国际数据公司 (IDC) 的研究结果表明，2008 年全球产生的数据量为 0.49ZB，2011 年增长为 1.82ZB，2013 年数量更是高达 4.4ZB，2020 年将达到 44ZB。数据量年增长高达 58%。毫无疑问，我们已经进入了大数据时代。

大数据是一把“双刃剑”。大数据时代的到来，颠覆了各个领域的固有模式，在各行各业都引发了巨大的变革，“数据驱动业务”成为了新的全球趋势；同时，对于信息安全来说，大数据时代的到来，

也为信息安全行业带来了前所未有的挑战，系统架构的更新、业务模式的变革，使得大数据时代的安全形势与传统的安全形势相比变得更加复杂。

## 二. 大数据平台研究概述

### 2.1. 什么是大数据？

对于“大数据”(Big Data)，研究机构 Gartner 给出了这样的定义。大数据 (Big Data)，指的是那些超出正常处理范围和大小、无法使用传统流程或工具处理或分析的信息；是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产。

## 智慧安全 2.0

### 2.2. 大数据平台应该具备什么能力?

IBM 提出, 构建大数据平台具备五大核心能力, 如图 2.1 所示。

**Hadoop 系统 (Hadoop System):** 利用 Hadoop 平台提供完整的大数据解决方案。

**流计算 (Stream Computing):** 能够提供有效的实时数据分析能力。

**数据仓库 (Data Management & Warehouse):** 提供数据存储能力。

**内容管理 (Content Management):** 提供数据内容安全管理能力

**信息整合与治理 (Information Integration and Governance):** 提供数据整合、管理能力。

### 2.3. 大数据平台的组成

大数据平台通常由六部分组成, 分别是基础设施、数据集成、数据存储、数据处理、应用展示及运维管理, 如图 2.2 所示。下面分别具体介绍这六部分组成。

**基础设施:** 实现大数据平台建设的基础设施, 包括网络、服务器、安全设施等。大数据平台建设中, 基础设施建设尤其重要。面对海量的数据, 无论从网络传输、数据存储、数据管理等各个方面来看, 都是巨大的挑战, 提供良好的大数据平台基础设施, 是大数据平台稳定高效运行的基石。

**数据集成:** 实现将数据从外部设备收集到大数据平台的框架, 包括一些数据采集设备、数据缓存设备等。大数据平台的数据集成

与传统平台有所不同, 大数据平台数据集成面对着海量的数据。如何能够使用少量的设备对数据进行合理的采集并存储至大数据平台, 是数据集成层需要解决的问题。

**数据存储:** 实现大数据平台中大数据存储的框架, 包括文件形式存储及数据库形式存储。大数据平台以数据为中心, 因此数据能够稳定的存储、高效的读写就成了大数据平台建设中的核心问题所在。数据存储框架提供各种存储方式来应对海量种类繁多的数据存储。

**数据处理:** 实现将大数据平台中的数据进行处理分析, 挖掘其中价值的框架。数据处理是大数据平台的核心流程。利用合理的处理分析算法, 将大数据平台中存储的数据的价值挖掘出来, 就是数据处理框架的目的所在。

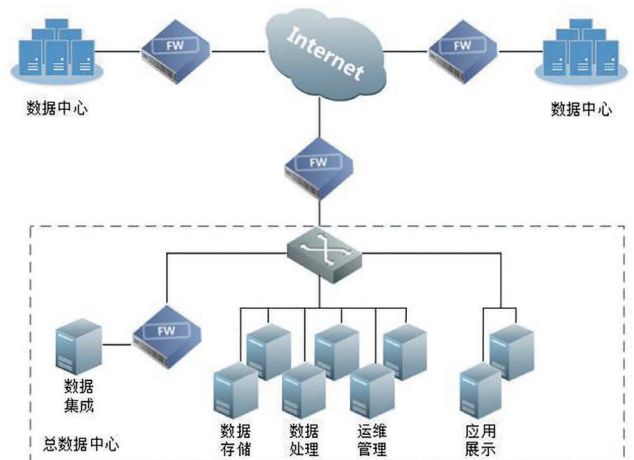


图 2.2 大数据平台主流框架架构

应用展示：实现基于大数据平台中的数据或分析结果向用户提供应用或者展示的框架。应用展示框架是将数据处理分析后的结果，以更加方便、易读的方式呈现给用户的框架。

运维管理：运维管理是大数据平台中的重要组成部分，依靠大数据平台的运维服务，来保证整个大数据平台的平稳运行。运维管理框架包括大数据平台的实时监控、大数据平台的运维管理工具等。

### 三. 大数据平台面临的威胁

#### 3.1. 大数据安全事件

2013年4月24日，美联社 Twitter 账号被盗，发布虚假信息称总统奥巴马遭受恐怖袭击受伤。虽然虚假信息很快就被修改，但是仍然引发了股市跳水。

2014年1月，Target 公司储存有 7000 万顾客姓名、地址、电话和邮件等信息的数据库遭黑客攻击，而 Target 在很早之前就开始了对孕妇商店或者其他数据进行大数据挖掘。

2014年5月，著名电商 eBay 要求要求近 1.28 亿活跃用户全部重新设置密码，此前这家零售网站透露黑客能从该网站获取密码、电话号码、地址及其他个人数据。

2014年9月，苹果“iCloud 艳照门”爆发，101 位好莱坞女演员陷入艳照门，起因就是因为黑客 8 月底对云盘的破解。

2015年5月，携程网瘫痪长达 12 小时，紧接着，艺龙网又遭受到了黑客攻击；携程网长达 12 小时的宕机，带来的经济损失达 1200 万美元。

2015年6月，阿里云香港节点出现权限宕机，业务中断超过 12 小时，甚至出现部分用户数据损毁。

随着大数据时代的来临，传统的存储架构无法解决高速的数据增长，越来越多的企业使用大数据平台存储数据。大数据平台大多是基于一些开源软件开发而成，其复杂的架构，模块的不稳定，数据的跨地域传输等特点，都会给大数据平台的安全带来极大的威胁。

绿盟科技的调研分析发现，大数据时代下的安全威胁具有几个相同点：

**波及范围广**，与传统威胁不同，大数据平台一旦受到攻击，波及范围会更加广泛，往往是跨地区甚至是跨国家的，这与大数据平台集中控制，高耦合性的特点是密不可分的。

**数据泄漏量大**，近年来，数据泄漏威胁的趋势呈现数据泄漏事件频率越来越高，数据泄漏量越来越大的特征。究其原因，就是因为大数据平台的应用。数据集中存储于大数据平台中，而大数据平台自身的安全性低。

**经济损失大**，大数据平台承载着大量的高价值数据，而且大数据平台是各大企业的业务根本。因此，每次大数据平台上的安全问题都会带来巨大的经济损失。

图 3.1 是一份 CSDN 提供的关于“大数据平台打造的主要挑战”的调查报告，图中可见，企业要打造大数据平台，需要企业克服诸多问题和挑战。而在这些问题中，最突出的就是安全性问题。

大数据平台作为大数据时代的信息载体、处理工具和应用平台，在大数据时代起着至关重要的作用，其必将成为黑客组织、各类敌

智慧安全 2.0

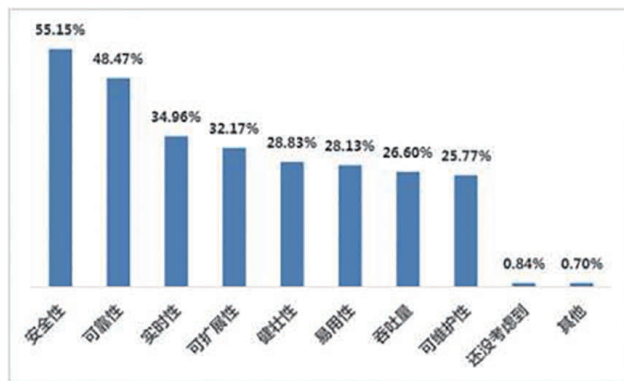


图 3.1 大数据平台打造的主要挑战

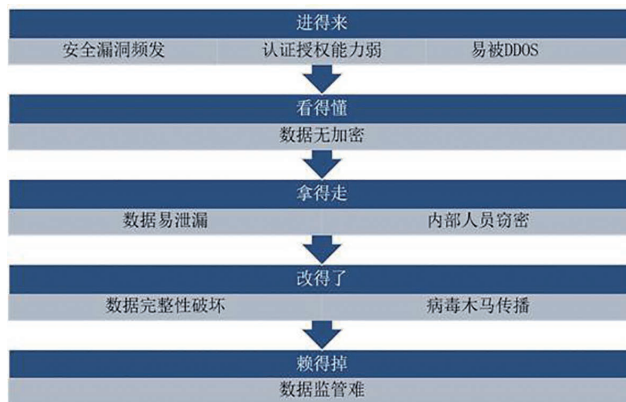


图 3.2 大数据平台安全威胁

对组织攻击的重要目标；因此，大数据平台的安全问题，就成了大数据平台建设的焦点所在。

### 3.2. 大数据平台的安全挑战

沈昌祥院士曾介绍过，安全平台建设的几个重点就是做到非法人员进不来、拿不走、看不懂、改不了、赖不掉。其具体内容如图 3.2 所示。但是，大数据平台建设中，在这些方面都存在威胁点，这些问题，就导致了大数据平台“进得来”、“看得懂”、“拿得走”、“改得了”、“赖得掉”。另外对大数据服务平台的拒绝服务攻击 (DDoS) 也会造成大数据服务平台的宕机，因此 DDoS 攻击也是大数据平台安全建设的一个重要部分。以下详细介绍大数据平台的安全挑战。

#### 3.2.1 拒绝服务攻击

数据采集节点在运行过程中往往是在高负载运行的状态。攻击者常常会在正常数据流中混入大量的垃圾数据，导致数据采集节点

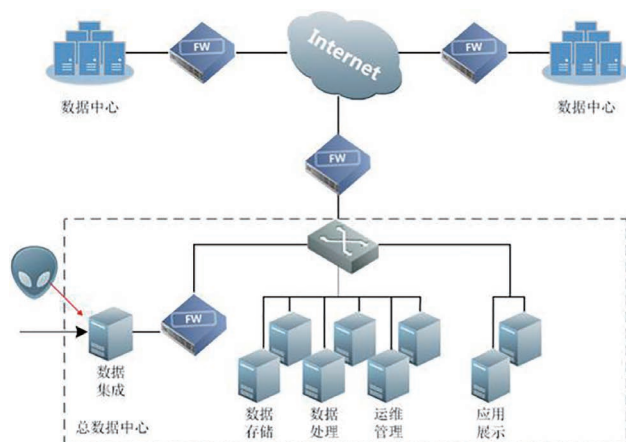


图 3.3 拒绝服务攻击 (DDoS)

响应迟缓,影响正常数据的接入,如图 3.10 所示。此外,对于应用展示方面,大数据平台由于其业务的特殊性,在可靠性方面会受到挑战。针对大数据平台的拒绝服务攻击需要受到绝对的重视。

### 3.2.2 安全漏洞频发

近年来大数据平台漏洞频发,且暴露出来的漏洞级别都较高。攻击者借助这些漏洞对平台进行入侵、渗透,给企业带来巨大损失。以搜索引擎为例,大数据平台中搜索引擎是必不可少的组件,根据 CSDN 的调查结果,在大数据平台中主流的搜索引擎共三种: Splunk、Solr 及 Elasticsearch,如图 3.3 所示。

这三款主流的数据检索框架都存在大量的安全漏洞问题:

**Elasticsearch:** 远程代码执行漏洞 (CVE-2014-3120), 远程代码执行漏洞 (CVE-2015-1427), 任意文件读取漏洞 (CVE-2015-3337) 等;

**Solr:** XML 外部实体注入漏洞 (CVE-2013-6408), 跨站点脚本漏洞 (CVE-2014-4638) 等;

**Splunk:** 命令注入漏洞 (CVE-2013-7394), Web 跨站脚本漏洞 (CVE-2015-7604) 等。

### 3.2.3 认证授权能力弱

大数据平台的存储框架主要是使用开源框架组成。开源框架在初期往往是对功能、性能非常重视,而对安全问题重视较轻。以分布式文件系统 (HDFS) 为例,一旦攻击者知道了 HDFS 的超级用户名,就可以轻易的伪装成超级用户,对数据进行窃取。分布式数据库也类似,虽然会有层级保护,但是攻击者一旦知道了管理员或

其他用户的用户名,就可以轻易获得数据库中的数据,完全不需要进行任何密码验证,如图 3.4 所示。

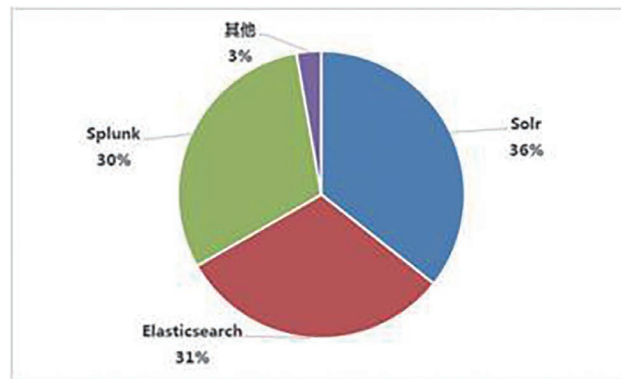


图 3.4 大数据平台查询检索工具分布

在系统授权安全方面,分布式文件系统也做的不尽人意。分布式文件系统中的文件是存在授权的。但是由于系统设计问题,通过存储系统中的数据块名 (blockID),攻击者可以轻易绕过授权获取数据。

### 3.2.4 数据无加密

数据加密是为了保证数据在泄漏之后,无法被非法人员利用。由于大数据技术刚刚兴起不久,大数据平台的各个框架又基本都是使用开源软件来构成,对于安全方面意识不够。因此数据在大数据平台中,无论是存储还是传输方面,都是使用明文。一旦数据泄漏,将为用户带来极大的损失。

## 智慧安全 2.0

## 3.2.5 数据泄漏威胁

如果要选出大数据平台面临的最大挑战，那非数据泄漏莫属，如图 3.5 所示。企业往往将大量有价值的历史数据存储在大数据库平台上。一旦发生数据泄露，将会对企业造成巨大的损失。近年来，数据泄漏呈发生频率越来越高、泄漏数据越来越多的趋势，这与大数据平台的广泛应用是分不开的。

## 3.2.6 内部人员窃密

大数据平台中，内部权限认证机制及授权机制都是存在缺陷的。对于能够轻易接触到系统底层的内部人员来说，获取数据就变得轻而易举。赛门铁克曾经做过调查，数据泄漏发生的原因大部分为内部人员人为泄漏，占比高达 63%。如图 3.6 所示。如果没有一套完整的运维监控管理手段，大数据平台安全就无从谈起。

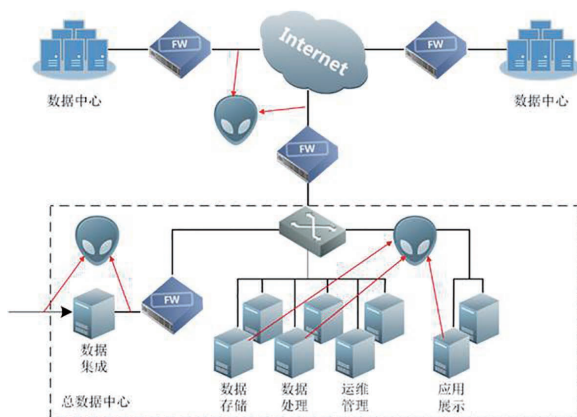


图 3.6 数据泄漏威胁

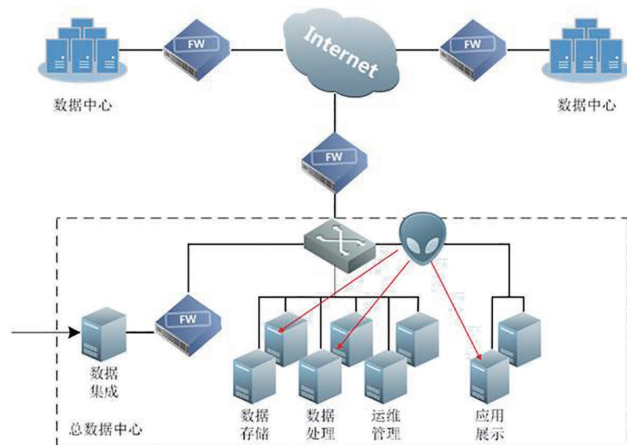


图 3.5 认证授权能力弱

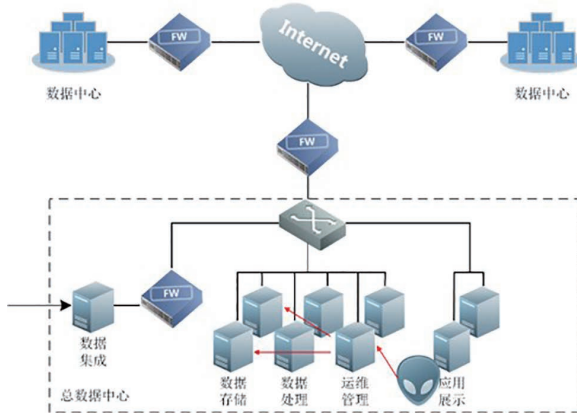


图 3.7 内部人员窃密

### 3.2.7 数据完整性损坏

数据完整性一旦被破坏，带来的损失将是不可估量的。如图 3.7 所示，大数据平台具有跨地域部署的特点，即多地域共享数据或数据多地域共存。这就对网络基础设施建设提出了很高的要求。一旦网络基础设施建设出现漏洞，攻击者就很容易对数据进行篡改。在数据收集过程中也可能遇到数据完整性被破坏：攻击者可以将恶意数据混杂在正常数据中，最终导致数据分析结果错误。

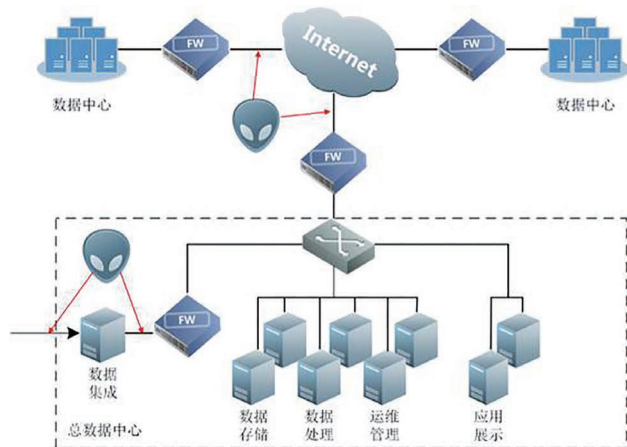


图 3.8 数据完整性破坏

### 3.2.8 病毒木马传播

传统平台中各个系统之间会存在大量的边界。传统网络安全思想可以在这些边界之间大做文章，做成一个一个隔离的、封闭的空间。

而大数据不同，大数据内部会有大量的数据交互，各模块之间的关联性也非常强。因此，大数据内部的边界可能就不那么明显。攻击者就是利用这一特性在入侵集群中某个节点后，便能够快速、大量的传播病毒或木马，如图 3.8 所示。

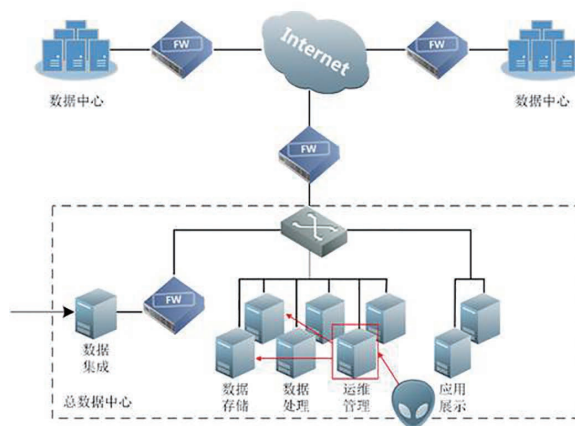


图 3.9 病毒木马传播

### 3.2.9 事后追责难

大数据平台中实时数据流量都非常大。无论在输入、输出阶段都会包含大量复杂的数据。这就使得数据监管非常困难。这种情况下，由于少量的泄漏数据混杂在大量的正常数据中，出现数据泄漏情况会变得极难发现；此外，大数据平台时时刻刻都会产生大量的日志，因此即使出现了数据丢失，取证也非常困难；最后，攻击者通常还会在攻击行为结束后删除日志，擦掉尾巴，让企业无法追责。



# 暗黑时代，APT威胁阴影下的 防御姿势

ESD产品管理团队 刘弘利

关键词：APT 鱼叉攻击 威胁评估

摘要：安全是一个对抗的过程，攻防双方此消彼长。攻击在暗处，防护在明处；攻击只需一个点，防护需要一个面。暗黑时代，企业需要从战略和战术两个层面，对抗高级持续性威胁。

## 一、网络攻击造成巨大损失

网络攻击造成多大的损失？每次攻击规模不同，所受损失也不同，从过往发生的攻击事件，可以窥见受到攻击的受害者所造成的损失。

网络攻击造成数据泄漏，金钱上损失惊人。2016年9月，美国电信运营商 Verizon 收购雅虎，在谈判的关键期间，雅虎被爆出5亿账号信息泄漏的事件。账号泄漏导致 Verizon 压价10亿美金。对于受害者雅虎来说，这个数目，可以说是此次攻击造成的损失。

对重大基础设施发起的网络攻击影响广泛。2015年圣诞节期间，

乌克兰电网遭到攻击，导致西部地区大规模停电。这次攻击，是继伊朗核设施受攻击后，又一次针对工业控制系统发起的攻击。可以想见，失去电力供应，人们的生产生活受到何等影响，损失何等巨大。

网络攻击还会产生致命的严重后果。2016年11月，轰动一时的高考考生徐金玉遭诈骗致死案，有了最新进展。最高检披露，涉案的32名诈骗团伙成员，全部落网。案件查明，考生信息泄漏的源头，系犯罪嫌疑人杜某，利用技术手段攻击了“山东省2016高考网上报名信息系统”，盗取了包括受害女生在内的大量考生信息。这些包含

考生姓名、家庭、联系方式的敏感信息，几经倒手转卖，到了诈骗团伙手中。他们组织严密，利用手中的信息取得受害者信任，一步步精心诈骗，导致女生最终死亡。

《2015 年全球网络犯罪成本研究》报告显示，针对 7 个国家（美国、英国、德国、澳大利亚、日本、俄罗斯、巴西）252 家公司的调查，应对安全攻击年化平均总成本为 770 万美金。

## 二、安全面临挑战

网络安全面临诸多挑战。一方面，潜在的攻击者虎视眈眈，磨刀霍霍；而另一方面，企业还没有意识到兵临城下，危机四伏。

### 2.1 攻方屡有斩获

网络攻击无时不在，攻击的技术手段越来越高级。高级持续性威胁（Advanced Persistent Threat，以下简称 APT 威胁），因其攻击技术高级隐蔽，攻击时间长，影响范围广，最近几年持续受到关注。过往的 APT 攻击，更多的发生在国家之间网络安全战略对抗中，入侵政府机构，国有企业，基础设施，进行战略威慑。随着黑客在网络安全地下产业的发展，越来越多的企业，面临着 APT 威胁的风险。

勒索软件让许多企业受到困扰。勒索软件中招后，文档和资料被粗暴的加密，需要支付赎金才能解密。很多企业的主机，中了勒索软件，业务系统不能正常工作，导致业务停摆。除了支付赎金，没有其他办法进行恢复。攻击者屡试不爽，尝到甜头，大有越演愈烈之势，2016 年出现多个勒索软件，也是未来几年企业重点防范的攻击方式。

勒索软件有复杂而精巧的攻击步骤。“鱼叉攻击”是勒索软件的

普遍传播形式，用“三段式”的攻击步骤，实施攻击。第一步，诱骗用户打开邮件中的文档，安装“Downloader”或者“Launcher”，为下一步攻击做准备；第二步，关闭防病毒软件或者隐藏自身，上传受害主机识别码，下载加密程序和加密密钥；第三步，遍历受害主机所有文档，进行加密处理，完成攻击，在桌面上留下提示信息进行勒索。

勒索软件与 APT 攻击目标不同，但其攻击手法类似。感染了勒索

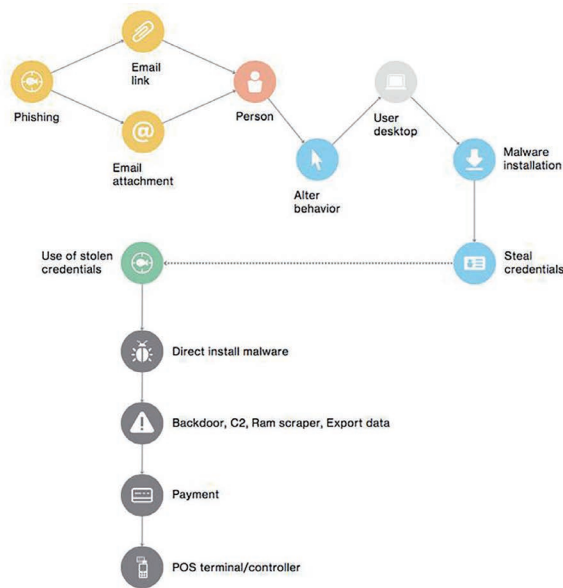


图 1：典型勒索软件的攻击步骤

勒索软件的企业，虽然清除起来麻烦，甚至有金钱上的损失。从另外一个角度，应该感到庆幸。想想看，倘若勒索软件不提醒进行勒索，而是一个 RAT 木马，就会长期驻留在企业网络中，监视着企业的一举一动。

## 2.2 守方还未做好准备

新技术采用给企业带来更多风险。云计算业务，BYOD，社交网络，企业越来越多的采用新技术，企业的网络边界越来越模糊。新技术的采用，无疑为企业提高了效率，减少成本，同时也增加了风险。企业利用云计算，不可避免的，一部分敏感数据保存在云端。不管是企业自行建设的云平台，还是使用第三方的云平台，这一部分数据，都存在安全风险。微信、微博等社交工具，在企业营销，员工办公提供便利，同时增加了企业敏感信息的暴露。微博中，官方账号与企业员工的互动而形成的关系链，恰恰是别有用心攻击者千方百计所寻找的。

**企业在新型威胁则投资不足。**企业认识到网络安全的重要性，对传统的网络、内容、和端点安全不遗余力的进行部署。但是对待 APT 这种新型威胁，大部分企业，还没有深刻意识。在新技术的评估和采用上，也偏向保守。

**员工的安全意识教育不够。**根据 MediaPro 《2016 年安全隐私和安全意识报告》，超过 80% 的员工缺少安全意识的教育培训。APT 攻击者，善于利用人性弱点，精心构造钓鱼邮件，引诱缺少安全意识的员工就范。

## 2.3 恶意软件技术在安全对抗中占据优势

传统安全系统不能有效监测未知威胁。基于“签名”技术检测方式，比如防病毒软件和入侵检测系统，已经过时。2016 年 11 月，在新西兰举办的安全大会上，谷歌的安全专家断言，“杀毒软件其实没什么用，安全行业应该把工作的重心放在其他真正有用的方面，像是白名单这一类的应用”。这样的观点虽然有些偏颇，不过从侧面证实，对高级恶意软件的检测，防病毒系统力不从心。

攻击者采用多种技术绕过检测。根据最新的 NSS Lab 实验室的研究，二进制逃逸，虚拟环境检测，沙箱逃逸，HTML 混淆，SSL 加密是高级恶意软件的主要逃逸方式。这是恶意软件如检测手段的“猫鼠游戏”。现实情况，每发现一种逃逸方式，安全厂商需要增加一种检测方式，处在被动追赶的尴尬位置。

基于 0Day 漏洞的威胁危害更大。很多重大的 APT 事件与 0Day 漏洞有关。系统存在 0Day 漏洞，只有攻击者知道这个漏洞，厂家没有发布补丁，弥补漏洞无从说起。0Day 漏洞一旦公布，虽然厂家立刻修复此漏洞，还是留存一个时间窗口。其他攻击者利用这一短暂时间，更新自己的黑软工具进行攻击。这也说明，及时更新补丁程序非常重要。

## 三、安全防御战略

“没有网络安全就没有国家安全”，网络安全的重要性，毋庸置疑。APT 为主的高级威胁，形势紧迫。检测和防御 APT 威胁，需要“战略上重视，战术上也要重视”。网络安全的建设和维护，离不开 PPT

(People, Process, Technology) 三个要素。PPT 的组合，在 APT 威胁时代，如何发挥和协作，才能更好的检测和防御 APT 威胁呢？

### 3.1 人思想和行动需要转变

---

APT 威胁的检测和防御，人是整个建设过程中的决定性因素。首当其中，企业最高领导，有网络安全重要性的深刻认识，支持企业对高级威胁防御的建设。只有这样，后续的安全建设才能落实。好的开始是成功的一般。其次，主管 IT 和网络安全的中层领导，对于新形势下的安全建设，要制定安全检测的规划，评估安全风险，寻找适合的技术方案，制定评估流程和应急策略，抓好安全意思教育等。最后，公司全体员工，要遵守安全规则，提高防范警惕意识。

### 3.2 APT 威胁评估与持续响应

---

APT 威胁的安全流程，着重考虑评估和应急响应流程。安全运维过程中，风险评估，在原有的基础上，增加 APT 威胁弱点评估。常见的 APT 威胁手法，“水坑攻击”和“鱼叉攻击”是最主要的两种方式，评估过程中，找出这两种攻击手段对应的弱点，评估安全风险，提出应对方案。

APT 威胁中，应急响应也是重要一环。Gartner 建议，企业要转变“应急响应”为“持续响应”。其实，这个思维的转变，是替企业安全管理人员回答一个问题，即企业一旦发生了 APT 攻击，企业有没有能力进行恢复、调查、溯源？

这让笔者想起一个案例，日本最大的旅游公司，JTB 在线网站发生的 APT 攻击，造成数据泄漏事件。2016 年 6 月，日本最大的在线旅游网站 JTB，向公众披露发生数据泄漏事件，近 800 万人

信息泄漏。让人惊奇的是，JTB 能够立刻意识到入侵，并且邀请外部专业安全公司同步调查。根据 Mandiant 的 APT 威胁趋势报告，APT 攻击被发现的平均时间为 205 天。2016 年初，绿盟科技发现某客户的一起 APT 案例，木马存留 10 年之久。所以看到，日本 JBT 的应急响应做得已经很出色，即便如此，依然发生了严重数据泄漏事件。

悲观的讲，被攻击被入侵是大概率事件，持续响应才能及时发现入侵痕迹。比如业务系统运行不正常，外网发进来的可疑邮件，公网上出现公司的敏感资料（源代码，内部财务消息）。循着这些蛛丝马迹，才有及时发现入侵的可能。另外，对于高级威胁的样本分析，事件调查，影响评估，攻击溯源，必要时需要专业安全公司辅助分析。

### 3.3 评估和选择 APT 防御技术

---

安全厂商应对 APT 威胁挑战，有多种技术可以选择。企业应该在风险评估的基础上，选择合适的技术方案，部署在薄弱风险点。

在基于“签名”的防病毒软件，无法有效检测高级恶意样本。在这样的背景下，沙箱技术应运而生。沙箱技术是防病毒软件，入侵防御系统的补充。

大数据技术出现后，应用在海量的网络流量上，希望在大规模的数据中找出不正常的行为。建立分析模型和算法，找出僵尸网络，隐秘通道，异常网络访问行为等。

白名单技术基于程序“信任”锁定方式，不允许白名单意外的程序安装和运行。杜绝了恶意软件在主机上安装的可能。白名单技术

技术	说明	部署	适用场景
沙箱	采用仿真或者虚拟机的方式，运行进入企业的外来文件（如 web 下载，邮件附件），纪录文件所有行为（注册表，文件，内存网络），根据规则判断文件是否为恶意代码的方式	网络部署	水坑攻击和鱼叉攻击的网络上对威胁进行检测
网络流量分析	网络流量分析是指捕捉网络中流动的数据包，并通过查看包内部数据以及进行相关的协议、流量分析、统计等来发现网络运行过程中出现的安全相关问题	网络部署	适用于检测内网存在僵尸木马主机
白名单	主机上安装白名单应用，除了白名单内的程序外，不允许安装和运行其他程序，主机处于锁定状态，用这种方式防御恶意软件的感染	主机安装	不经常进行软件变更的服务器，银行 ATM 机，POS 机等
虚拟桌面	Virtual desktop infrastructure (VDI)，虚拟桌面环境，隔离操作系统进行上网，收发邮件	网络部署	对整个操作系统的安全要求严格，对外网访问完全隔离
远程应用隔离	对应用实现类似 VDI 形式的隔离，浏览器访问资源，远端实现应用的执行，本地看到应用执行后的视图	网络部署	对应用（如浏览器）安全要求严格，访问外网的应用进行安全隔离

表 1: APT 检测和防御技术

适合不经常变更的系统，比如服务器，银行的 ATM 机，POS 机等。

虚拟桌面和远程应用隔离的机制类似，把威胁隔离在外。虚拟桌面其实并不是 APT 威胁检测技术，用虚拟桌面完成危险度高的工作，需要连接互联网的 web 访问，邮件下载等。更极端的，连接互

联网使用另外一台电脑。远程应用隔离，这种技术还比较新颖，类似代理机制，把 web 的对象执行放在代理，本地浏览器只是看到最后的视图，也避免了类似 Flash，JS 脚本攻击。当然这种方式，也有许多不方便，需要在安全性和易用性中取得平衡。

#### 四、绿盟在 APT 威胁防御实践

绿盟在安全攻防领域有近 20 年积累，面对 APT 高级威胁的挑战，在安全技术产品、方案、服务等方面做了研究和实践，推出针对 APT 威胁检测和防御的下一代威胁防御解决方案 (Next Generation Threat Protection，以下简称 NGTP)，NTI 全球威胁情报系统，虚拟安全响应中心服务。

##### 4.1 绿盟下一代安全防御 NGTP 解决方案

NGTP 解决方案，由沙箱引擎 TAC，大数据分析引擎，威胁防御模块 IPS，金山防病毒套件，以及邮件安全网关 SEG 组成。

NGTP 解决方案的工作原理，以沙箱引擎和大数据分析引擎为核心，以安全信誉为纽带，通过安全协同，关联 IPS 进行网络和 Web 防护；关联金山防病毒进行终端防护；关联 SEG 进行邮件防护。

首先，沙箱引擎对进入企业的高级恶意软件进行分析，大数据分析引擎对藏匿在内网的特种木马进行检测，并且自动生成本地安全信誉；

其次，NIPS，金山防病毒套件，SEG 分别对网络、终端、邮件进行安全防护，并接收来自沙箱引擎和大数据分析引擎的安全信誉；

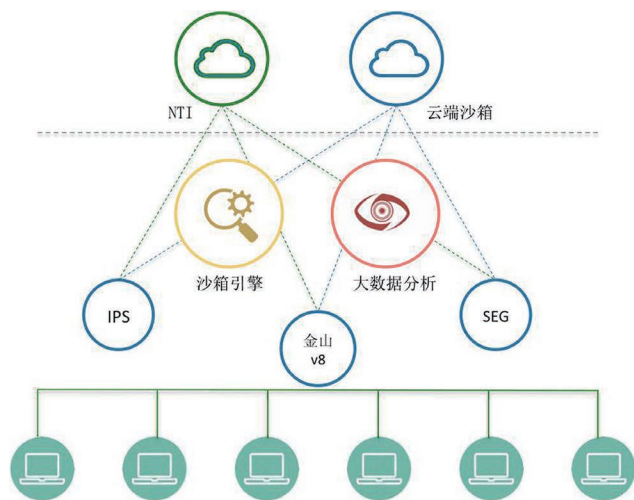


图 2:NGTP 解决方案示意图

最后，IPS、金山防病毒套件、SEG 根据接收到信誉的等级和策略，进行安全阻断，隔离，删除等操作。

绿盟下一代威胁解决方案，全面的 APT 威胁检测和防御。无论是网络、Web 上网、邮件收发，终端操作，都是 APT 威胁可能利用的通道，NGTP 解决方案，不仅在网络边界进行检测和防御，还在企业内网，邮件服务器，终端等多个层面进行检测和防御。

绿盟下一代威胁解决方案，利用本地沙箱引擎和云端安全信誉，大数据分析引擎，准确地对 APT 威胁检测和防御。本地沙箱提供了恶意软件静态检测和虚拟执行手段，检查恶意软件 Shellcode，并且模拟真实的 PC 环境进行验证；大数据分析引擎，对网络流量，

DNS 查询数据进行建模分析。此外，绿盟云端信誉 NTI 提供另外一层保护，及时和准确的威胁情报信息，进一步提高 NGTP 方案对 APT 威胁检测的准确性。

#### 4.2 绿盟应急响应中心安全服务

虽然部署有针对性的技术方案。即便如此，也有可能发生数据泄漏，APT 攻击等安全事件。这就需要自己的应急响应团队（Computer Security Incident Response Team, CSIRT）来执行应急任务。

绿盟应急响应中心，是企业安全响应团队的扩展。高级恶意样本分析和攻击溯源，APT 攻击调查等，需要足够专业的知识和技能，这正是绿盟安全应急响应团队所擅长的。绿盟应急响应中心，是由多位资深安全专家组成，专注在恶意软件的研究领域，深入分析恶意软件的行为和攻击特征，帮助客户进行 APT 攻击事件调查。

## 五、结语

安全是一个对抗的过程，攻防双方此消彼长。攻击在暗处，防护在明处；攻击只需一个点，防护需要一个面。暗黑时代，企业需要从战略和战术两个层面，对抗高级持续性威胁。

应对 APT 威胁，绿盟科技已经做好准备。NGTP 解决方案，在时间上，兼顾传统威胁和新型威胁；在空间上，兼顾网络边界与企业内网；在运营上，兼顾技术方案与应急服务。以多层次、主动安全，安全组件通过信誉共享机制进行协作，提供“威胁进不来”，“扩散藏不住”，“数据带不走”的保障效果。



# THE EXPERT BEHIND GIANTS

## 巨人背后的专家



# 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，为政府、运营商、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。

# 知所未知 运筹帷幄

海量数据治理 / 安全态势感知 / 威胁情报预警 / 风险管理度量 / 安全应用响应

## 一站式综合运营平台

您优选的企业安全治理解决方案

- 海量数据快速查询和分析
- 安全态势可视、可控
- 风险度量及过程监督



**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，为政府、运营商、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。