金融行业安全月刊

安全月刊

08

2017 年

技术版

绿盟科技金融事业部安全月刊 专家观点 / 行业研究 / 漏洞聚焦 / 产品动态

企业网络安全观给高管们的网络安全建议

浅析商业银行数据安全保护体系建设思路

在阿里云上应用系统的安全防护解决思路

2017 年上半年重大黑客事件盘点

韩国最大比特币交易所 Bithumb 遭入侵用户损失数十亿韩元

多家企业感染 MBR 勒索病毒威胁预警通告

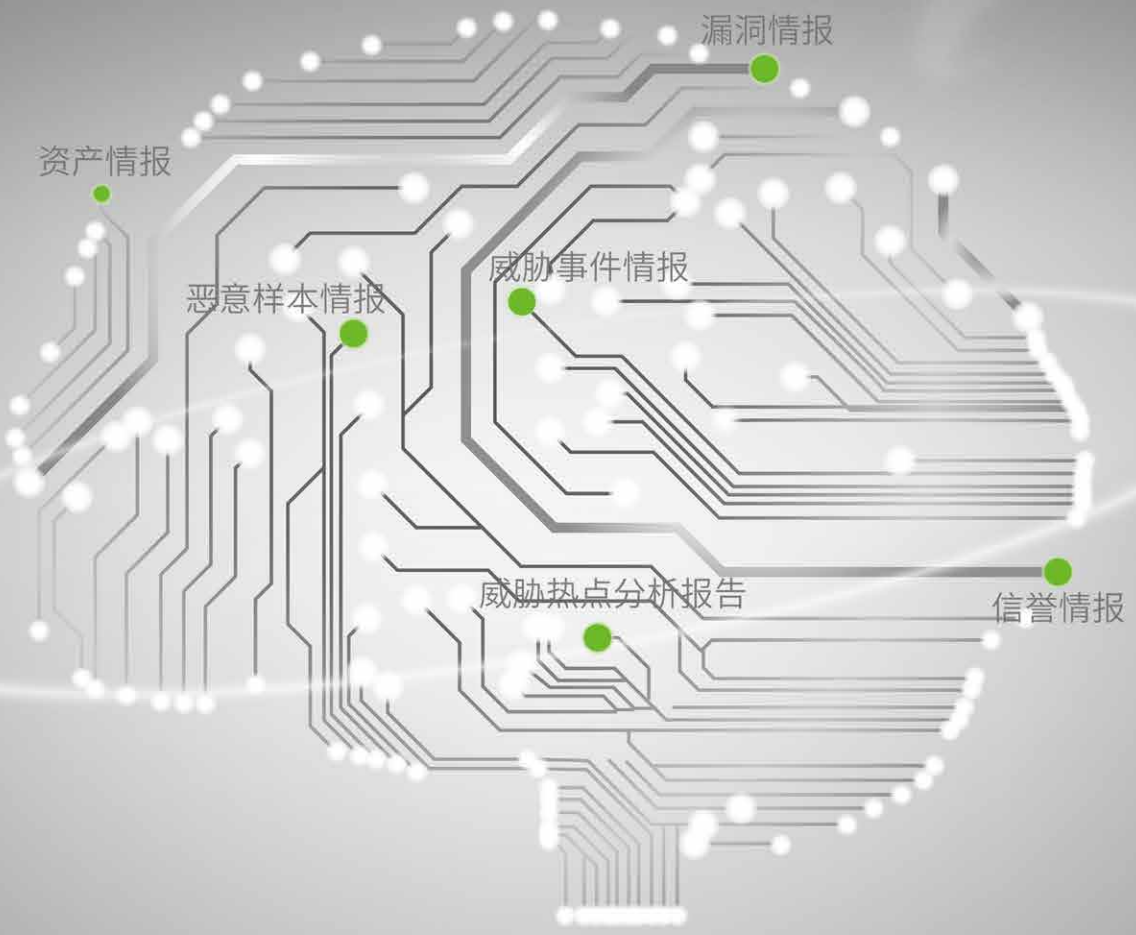
NSFOCUS

绿盟科技威胁情报平台NTI

智慧的大脑

智能 敏捷

Hot products at RSA 2017



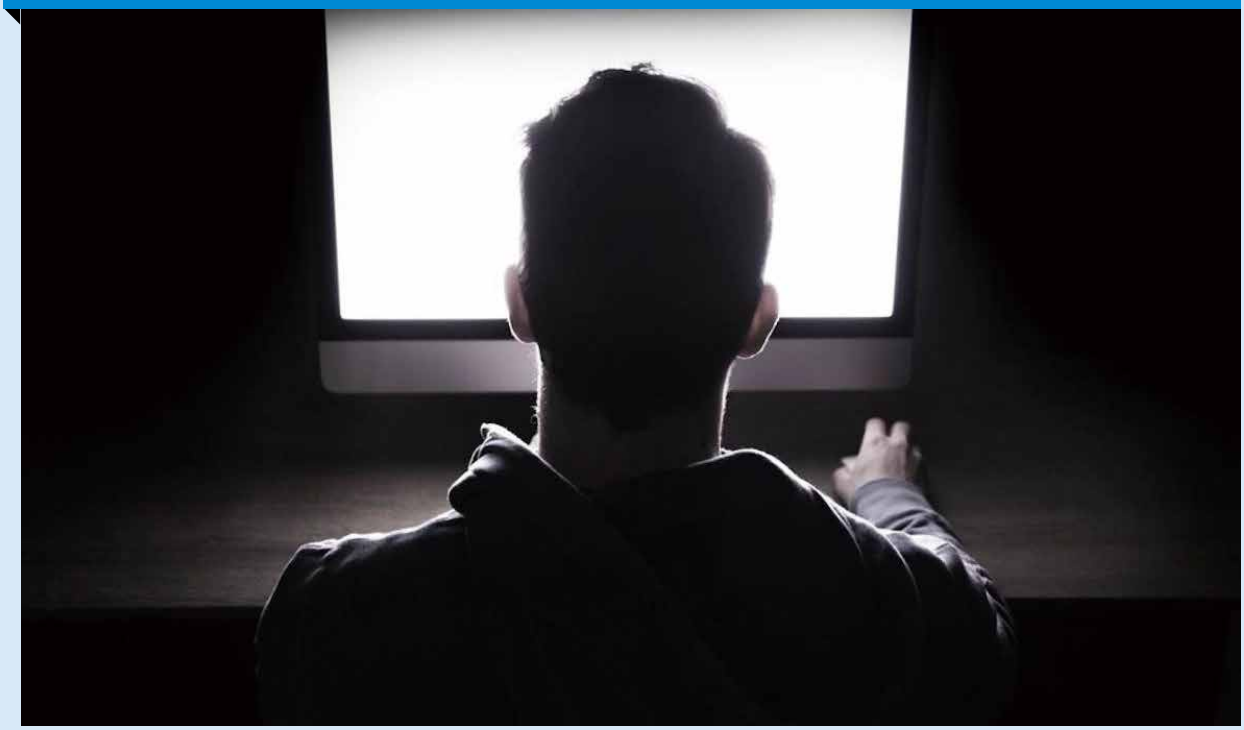
情报能力

强大的威胁捕获能力、精准的威胁预警能力、全面的威胁防御能力

洞察威胁知己知彼，助力安全运营提升

NSFOCUS绿盟科技

本|期|看|点



安全月刊

2017年第8期

绿盟科技金融事业部

目录 CONTENTS

专家观点

行业研究

漏洞聚焦

产品动态

绿盟科技官方微信

绿盟科技金融事业部

NSFOCUS

专家观点

企业网络安全观
给高管们的网络安全建议

金融事业部 傅戈

一、前言

随着国家安全战略的建立、《中华人民共和国网络安全法》等法律法规的颁布和实施、监管机构的推动、企业机构自身业务的发展，相信几乎所有的C Level级别的高管都认同网络安全的重要性和关键性。在这些新的形势下，很多机构的高管们都在思索和探讨如何持续改进和完善机构的网络安全治理，本文将根从企业网络安全的视角尝试提出以下六个建议供机构的高管们做参考。

二、建议

2.1 高管们的安全观决定企业安全建设的成效

通过研读多家机构针对网络安全发起对全球高管们的调查报告，我们可以看到一些值得思考的现象。

1. 高管们普遍都认同网络安全的重要性，同时也都认同网络安全是他们必须面对和解决的问题。但不少高管并不清楚和能说出安全风险来自什么地方，什么样的安全因素将带来最大风险，这种认知和理解上的不足表现在高管们心中的安全风险和现实中的安全风险的比例没有呈现一致性。例如，根据现状来看，数据泄露的威

胁中，55%的数据泄露事件来自内部人员，但调查显示仅有32% 的高管将目前/前雇员选入最主要的三大威胁 [1]。

2. 高管们对自己机构网络安全现状的情况以及安全防护能力的自信心有所不同。CIO（CSO）由于职能情况，对网络安全现状最为了解同时拥有最高的安全防护自信心。CEO的了解程度和自信心次于CIO（CSO），CFO和CMO在了解程度和自信心上是最低的。这方面的原因在于CEO、CFO和CMO是机构中职员、财务和客户信息数据的拥有者，因对安全状况的不了解程度降低了他们的信心。

3. 高管们和下层管理层以及具体工作的安全职员之间存在着对网络安全认知不一致性。这种不一致性体现在对机构整体安全性的认可程度以及对安全工作的重视程度。例如澳大利亚国立大学的研究表明只有58％的网络安全专业人员认为他们的董事会对网络风险有足够的了解。不到一半（46％）的网络安全专业人员表示，公司董事会很少或从来没有讨论过网络安全问题。几乎三分之一的网络安全专业人员（30％）甚至表示，他们的董事会没有收到关于网络安全威胁的报告[2]。

这些现象提示我们，机构的高管群需要改进他们的安全观，改变网络安全停留在口头重视的情况，需要切实深入的了解机构的网络安全现状、了解新的网络安全风险，只有这样，作为机构的最终决策者和负责人才能肩负好网络安全的责任。

2.2 良好的工作机制是机构中网络安全工作的关键之一

今天，关于网络安全应该是全员参与的企业安全理念早已被企业机构普遍所认同。但是高管们还需认真考虑如何将网络安全与机构的运营工作机制进行有机的融合，使其成为一个鲜活，立体的工作内容，而不只是停留在企业制度文档上苍白的文字。就目前而言，一些机构存在着以下工作机制方面的问题。

1. 一方面，高层间缺乏专门的网络安全联席会议机制同时也较少将网络安全列入联席会议议题。而另一方面，CFO，CMO们也往往较少参与此类专门的网络安全联席会议，这使得他们对安全信息了解不畅并让他们对机构的网络安全计划抱有怀疑，认为这些计划不完善或者无法正确实施。因此，高管们存在着对网络安全意见的不一致情况并将有可能对机构的网络安全建设产生消极影响

2. 有一些机构其各部门之间的安全工作开展缺乏联动协调机制，致使安全工作集中于IT部门，将本是全员参与的工作畸变为IT部门，甚至是机构安全小组的工作。在这种情况下，安全部门/人员和业务部门常存在安全职责不清、相互推诿、处理及反应滞后的情况。

3. 不少机构虽然已建立内部的OA系统，但尚未将网络安全运维流程和OA系统进行集成以实现机构安全管理工作的电子化、流程化和自动化。现代网络安全管理要求强调安全快速响应与处置以及安全闭环管理以对付日趋复杂的安全威胁。显然那种依靠人工方式进行工作协调和沟通的处置方式无疑是落后的，亟需进行改变。

2.3 安全态势感知与情报分享将显著改变原有被动防御的局面

绝大部分网络攻击很少是孤立事件。攻击者在发动攻击时需要提前做很多的工作，例如寻找漏洞、制作工具、甚至对真实目标进行攻击前会对其它目标进行测试攻击。根据美国执法机构的调查研究表明在2014年一次针对摩根大通公司的攻击中，执法机构调查发现至少另有10家金融服务机构成为同一黑客组织的目标。又如，近期勒索病毒的猖獗就和黑客团体泄露并利用美国NSA的网络战武器有直接关系。因此，如果机构能够迅速获取到执法部门、安全企业发布的关于安全威胁和攻击的

安全态势信息，则可以迅速的提升警戒程度，制定相应的预防和处置措施，减小受影响和受攻击的可能性。

除了外部的安全态势感知外，机构也有必要建立内部的安全态势感知。这种感知是建立在对内部安全信息的集中、整合、过滤、挖掘及分析之上。这样可以帮助机构时时知晓内部网络安全的运行动态并识别潜在的安全风险活动，并根据这些态势及时调整内部安全策略和展开相关的安全处置。

现实中，黑客们往往在地下通过诸如暗网（dark web）这种地下资讯和交易网络进行黑产协作以提高攻击成功的可能性并获取最大的经济利益。然而，机构们之间对安全共享和协作却保持相当谨慎的态度。据调查，68%的CEO们表示不愿意对外共享发生在己方内部的安全事故。诚然，处在一个市场竞争如此激烈的时代，CEO们的顾虑无可厚非。但是，反过来说，我们是否可以多分享在网络安全方面的建设经验呢？高管们可以商议并建立企业之间的分享和学习机制，通过这种方式了解和学习彼此之间优秀的网络安全建设经验，提升己方安全管理水平。此外，高管们还可尝试在机构内部建立部门之间的分享和汇报机制，通过引入集体智慧，形成更优的安全解决思路和解决方案。

2.4 持续和理性的安全建设是保障机构网络安全有效性的重要基础

在一些机构中，高管们常依据自己对特定网络风险的认知来决定安全建设的方向、建设重点和投入成本。但由于他们的安全威胁认知存在一定的局限性、滞后性和偏差性。因此在开展网络安全的建设过程中，常出现以下多种现象：

1. 安全建设满足合规要求就好。一些高管们认为机构安全仅需要遵从合规要求就够了，并不愿意在安全上进行过多的投入。在实践中，合规要求是帮助机构建立良好的网络安全基线并解决已知的漏洞。但合规要求没有能充分解决和应对新的、动态的安全威胁或对复杂的攻击对手。正确的做法应该是使用基于风险评估的方法来应用最新的网络安全标准和业界最佳实践，这样比仅遵从合规能更全面和更有效地管理网络风险[3]。

2. 过于轻信己方的安全防护能力。事实上，这些年来发生的诸多攻击事件表明，机构的网络安全防护并不是想象中的钢铁长城，在外部APT攻击以及恶意内部人员的面前，机构的网络处于巨大的威胁中。幸运的是，很多企业CISO们认为威胁形势其实十分严峻，国外公司的研究报告表明83% 的 CISO 表示，过去三年外部威胁带来的挑战不断攀升，42% 的表示外部威胁显著增加； 59% 的 CISO 强烈赞同，攻击者的水平超过了企业的防御水平[1]。因此建议通过定期和全面的安全评估来检查真实的安全防护能力。

3. 不觉得己方将遭受到攻击，认为攻击的几率和可能性非常低。这种考虑有些基于国情的考虑，认为国内处罚严厉，黑客不敢发起攻击。有些则认为己方属于小型机构或非关键基础信息设施行业，不会引起黑客的注意。但是，最近发生的勒索病毒事件以及国外机构对境内金融机构进行DDOS攻击并进行勒索的事件证明了上诉观点的错误。

4. 期望通过某种解决方案解决绝大部分的安全问题。网络安全是一个内容涵盖非常广泛的领域，因此在网络安全建设中，不存在银子弹的解决方案，每一种方案都只能提供一定范围和一定程度上的安全防护。在这其中尤其要注意两种错误的观念，一个是认为只要有完善的外网安全防护，内网就安全；另一个是认为业务生产网和其它网络已实现物理或逻辑隔离，因此业务网是安全的。实践中，因持有这两种观点而遭遇惨重损失的企业机构案例非常之多，值得高管们警惕。

5. 重视技术层面的投入而忽略对人员的投入。战争

中，决定战争胜负的是人的因素，网络安全建设也遵循同样的道理。内部人员的安全技能、对设备工具的使用熟悉情况、人员的数量、工作的积极性和主动性都将直接影响安全工作的质量和执行效率。因此高管们应该考虑进行安全人力资源的评估、招募或引进足够的安全人员数量（包括安全外包）、开展定期的安全培训以提升人员技能、优化KPI绩效考核以提升人员工作积极性。

2.5 基础的安全管理和防护手段发挥着最大的功效

目前，高管们在度量己方机构内部网络安全建设的时候，往往会受到互联网新技术新业务的应用和开展，黑客攻击技术和手段日益先进和复杂，以及安全厂家不断推出的新产品这三个因素的影响，将资源投入到这类热点领域而忽视了企业机构最为基础的安全管理和防护。事实上，在安全领域，最为基础的安全管理防护措施发挥着最为重要的作用，国外咨询机构的研究报告中就显示超过75%的安全漏洞可以通过基础的控制措施进行防护[4]，因此高管们应该把如何做好基础的控制措施放在首要和优先的位置 （在机构有更多资源的情况下可进一步扩充和提升全面安全防护能力）。一般来说，这些基础控制措施包括

1. 有效和更新的管理制度和流程机制
2. 有效的网络边界隔离与防护
3. 定期/不定期的安全评估
4. 严格的权限账户管控
5. 配置操作规范和安全审计
6. 安全漏洞的发现与修补
7. 桌面终端安全防护
8. 持续的内部人员安全培训
9. 第三方服务及供应链的安全管控
10. 安全应急预案编制与应急演练

网络安全中的基础防护犹如建筑中承担抗震关键的柱子和房梁。做好基础防护则意味着企业机构达到了应有的安全基线，同时也获得了最大程度的安全投入回报。

2.6 积极的应对和恰当的改进可帮助建立更为有效的网络安全

正如网络攻击者不断的寻找漏洞，不断的改进其攻击手段以提高攻击成功率一样，企业机构也需要针对网络风险的变化及时的进行调整。在这种情况下，高管们应该主动开展和进行一些有利的变革改进以适应新的合规、新的法律框架、以及新的风险应对要求。这些变革改进包括组织架构、企业安全策略、安全管理机制、安全技术等层面，下面给出一些变革的方向和内容以供高管们参考。

1. 改变并提升对网络安全的支持程度。网络安全的问题会威胁到企业的各个层面，并带来商业和声誉的双重损失，因此，企业机构的网络安全不再只是 IT 部门的问题，仅有CSO或CISO的支持是不够的。高管们均有责参与到企业安全管理中。离开了高管决策层领导的集体支持，则难以建立一个有效的网络安全防护。调查表明自2013年起，有31%—32%的受访者称，管理层意识和支持的缺乏对网络安全的有效性产生了不利影响[5]。

2. 提升安全管理层的发言权重。一些机构并没有设立CSO或CISO的职位，或者CSO和CISO并没有能够进入到公司的决策层（或董事会）（国外著名咨询机构的研究报告表明约有75%的受访者表示其负责网络安全的人没有进入董事会[5]）。这样将导致网络安全的问题和建议没有能够被决策层给予足够的重视，从而没有获得对网络安全应有的建设支持。

3. 改进管理层汇报报告的质量和内容。研究表明在给决策层呈报的报告中，存在着两个突出的问题。一个

是网络安全的内容偏低，约25%的报告会阐述提及威胁等级；另一个问题是网络安全的内容没有能够以决策层能看懂的业务语言来进行描述。因此导致决策层不能完全了解和理解当前机构所面临的风险，进而对网络安全建设产生了不利影响。

4. 提升应对危机的处置能力。现在绝大多数的企业机构普遍均建立了基于技术层面的网络安全应急预案。然而，很多机构缺乏以下三种应急预案。第一种是对于发生事件之后如何邀请执法机构介入的应急预案，第二种是如何配合监管和执法机构进行事件调查与处置的应急预案，第三种是如何在媒体上发布应对消息以缓解或消除造成的社会影响及公众质疑的应急预案。建议高管们考虑增加以上应急处置内容和程序，确保企业机构更加有效地应对安全危机。

5. 提升对客户信息的保护水平。随着国家《网络安全法》的颁布实施，国家在法规层面显著提升了对个人信息的保护要求。高管们需要重新认真审视己方机构内对此类数据的安全防护水平。建议通过加强管理和技术两个层面的安全内控，降低内部人员恶意窃取或无意泄露客户信息的几率。建议通过加强第三方管控，减少经由第三方人员和机构泄露客户信息而给企业机构带来的直接和间接损失。

参考文献：

[1] http://www-03.ibm.com/security/cn/zh/ciso/index.html

[2] http://nsc.anu.edu.au/news-events/news-20161102

[3] https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

[4] KPMG《Cyber security: a failure of imagination by CEOs》, https://assets.kpmg.com/bh/en/home/insights/2016/04/cyber-security-ceo-cyber-outlook-study.html。

[5]《安永第19届全球信息安全调查报告》，http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-cn/$FILE/ey-global-information-security-survey-2016-cn.pdf

结束语

网络安全对企业机构的高管们而言不是一个单纯管理或技术层面的战术问题，而是一个关系到企业生存的战略问题。网络安全需要高管们对其有清晰、正确和全面的认识，通过主动和积极方式将其作为组织治理、风险管理和业务连续性框架的必不可少的一部分。随着网络安全形势的日益严峻，国家和行业网络安全监管的日益严厉，建议企业机构的高管们加强对网络安全的工作协同、改善工作机制、保持持续有效的建设投入、以灵活和恰当的方式构建和形成具有弹性的企业网络安全治理。

NSFOCUS

行业研究

信息安全实验室在银行网络中的应用

金融事业部 徐贵敏

各行业用户对信息系统的依赖程度越来越高，建立持续、稳定、安全的网络是保障用户业务发展的前提。当《网络安全法》的正式发布，各行业更加认识到网络及信息安全的重要性，当前众多银行系统均已部署防火墙、加密、身份认证、访问控制，备份等保护手段来保护信息系统的安全。与此同时，安全问题日益严重，病毒、木马、黑客攻击、网络钓鱼、DDOS 等安全威胁层出不穷，而且技术越来越复杂，病毒、木马及黑客技术等融合造成了网络安全的巨大危机。为此，需要通过建立职位体验式实践的软环境，使实验室成为“安全技术高手”培养的前沿阵地，进而全方位提升技术人员的攻防技能并能够真正的实现由安全运维向安全运营转化。

构建信息安全实验室目的是能够使银行信息安全技术人员能够自行构建环境完成实验，其次可以对外购设备、系统进行验证性安全测试，再次可以利用竞技、实训平台完成攻防演练及攻防知识的学习。

一、实验室定位

本着全面培养安全从业人员的创新精神与实践技能、综合分析问题和解决问题的能力的宗旨，将实验环境打造成工作职位理解和工作能力提升的平台，通过搭建具体环境及引入行业应用平台（攻防学习平台、攻防竞技平台）的实验组件构建符合实际业务应用的网络信息系统，并且建立职位体验式实践的软环境，以培养银行信息安全从业人员的实践能力、创新能力为宗旨，以提升攻防技能为核心，以实验资源开放共享为基础，以完善的实验平台为保障，全面发挥实验室平台的可学习性。

二、实验室建设需求

2.1 新购设备防护效果验证

面对市场各类参差不齐的安全产品其实际防护效果如何，需要有专门的实验平台提供对第三方厂商提供的安全产品进行功能及性能的全方位测试，通过全面的测试验证，能够使银行技术人员能够彻底了解新购或即将新购的安全产品真正防护效果，为后续的安全建设提供有力的安全支撑。

2.2 安全防护体系需求

经过前期的信息安全发展与建设，大部分银行已建立了完善的信息安全体系，但在大的安全体系之下，仍然存在一些可提升点。为此需要建立专用的安全攻防实验室实现运维环境相结合的信息安全竞技及学习平台。

2.3 网络攻防演练需求

目前众多银行没有专门用于日常教学实训及攻防演练的环境，若需要临时进行攻防演练活动时，才进行演练环境的搭建。但由于演练的目地与人员能力不同，使得演练环境变得非专业（缺少专业人员建设与管理）与不健全（不贴近金融行业真实环境），使得实验室的建设效果达不到最佳的演练效果，影响攻防演练及攻防技能学习的效率与成效。且重复的演练投入可能出现设备与人员重复投入的现象，造成资源的重复投入。

当前攻防演练还处于人工阶段，由人工使用攻防工具一步一步的对演练目标进行渗透测试，对目标进行攻击。后期在由人工对攻防过程进行归纳整理，总结演练经验与报告。没有专业的、自动化的渗透测试平台来实现攻击渗透过程，效率相对低下，自动化程度不高。缺少一个自动化的可视化的专业化的平台。

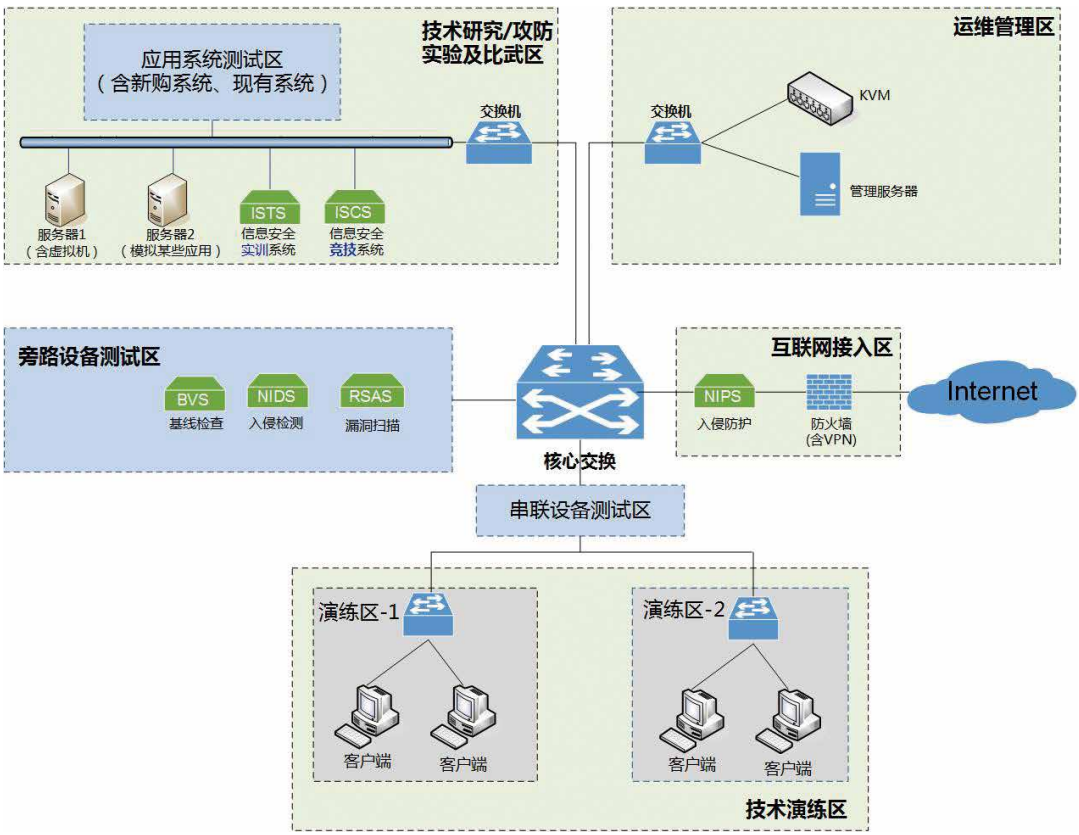
2.4 提升运维人员安全技能的需求

当前大多培训多是意识层面来提高人员对信息安全的理念认识对自身的攻防水平的提升并没有卓有成效的提高，无法做到针对性的提高人员的安全技能能力与动手能力，无法做到理论与实践相结合，缺少与实际环境相结合的信息安全学习与竞技平台。

三、实验室环境构建

3.1 平台结构搭建

信息安全实验室平台网络拓扑构建方式，如下：



3.2 平台区域划分说明

◆ 技术研究/攻防实验及比武区

技术研究/攻防实验及比武区由服务器、攻防竞技平台、攻防学习平台以及应用服务系统测试区组成，主要用来提供应用环境搭建以及供内部进行攻防比赛、攻防学习使用。

对新购的应用服务器系统可部署在应用服务系统测试区进行功能验证以及熟悉系统配置方法。

◆ 旁路设备测试区

旁路设备测试区用于部署旁路设备（IDS、漏洞扫描系统等），一方面可以在攻防学习、攻防比赛过程中使用，也可用于新购旁路设备的功能以及检测效果验证。

◆ 互联网接入区

互联网接入区为整个实验室网络总出口，当需要从Internet进行渗透测试或进行远程操作需利用该出口进行。

◆ 技术演练区

技术演练区分为演练区1和演练区2，演练区1和演练区2一方面可用于进行攻防对抗另外还可用于技术学习。同时演练区1和演练区2还可以利用技术研究/攻防实验及比武区的信息安全竞技系统进行进行单兵挑战及网络混战，以真正检验安全运维技术人员真实的技术实力。

◆ 运维管理区

运维管理区主要用于该网络中各网络设备、安全设备及应用系统的日志收集、策略调整、知识库管理以及各系统的集中管控。

3.3 信息安全实验室功能

3.3.1 基础功能

信息安全实验室基础功能主要由银行信息安全运维人员或由第三方专业安全厂商提供 “个性化”实验环境的构建。

同时，利用技术研究/攻防实验及比武区的信息安全实训系统开展信息安全意识、密码学与应用、信息系统安全、网络安全、数字内容安全、软件安全、信息安全工程、手机安全、协议分析与开发、数据库、程序设计、网站开发、操作系统应用、网络基础、路由交换等信息安全学习课程。基础功能具体描述如下。

3.3.1.1 提供安全测试环境

为业务系统提供安全方面的测试；为安全评估及加固服务提供技术环境测试；为信息安全设备入网提供专业性能和指标能力测试，以此形银行本身的技术支撑平台。

3.3.1.2 专业技术人员培训

银行信息安全岗位人员进行相关安全培训和实际操作试验环境，同时也作为和外部安全机构和组织的技术交流窗口。

3.3.1.3 新技术研究

为公司专职信息安全人员提供平台，进行信息安全前沿技术、SDN、各种攻防技术、业务系统和网元安全基线研究。

同时利用平台进行对新安全技术及新威胁场景进行研究，并根据具体场景实现虚拟化技术进行深入分析，为后续安全防护提供有针对性的防护建议。

3.3.2 专项竞技功能

攻防竞技功能主要利用技术研究/攻防实验及比武区的信息安全竞技系统实现，专业技能的培养，需要对纷繁复杂的知识体系进行细分，将网络攻防技术中常用到的技术进行分类，或者按照黑客攻击的步骤，将这些技术分类细化，具体描述如下。

3.3.2.1 攻防技能实训

信息安全竞技平台提供信息安全攻防技能实训功能，指导安全技术人员学习信息安全攻击技能与安全防护技能。攻防技能实训功能中包含密码学与应用、信息

系统安全、网络安全、数字内容安全、软件安全、信息安全工程、漏洞渗透、持续控制目标、渗透工具、手机安全、协议分析与开发、数据库、程序设计、计算机取证与司法鉴定、安全防护、安全基线评估等具体操作实践。

3.3.2.2 技能水平检验

信息安全竞技系统平台提供针对安全技术人员的技能考核功能，可以利用平台开展安全技术人员技能考试。平台考核功能支持在线的选择、判断、简答、实验操作考核几种方式，选择、判断、简答与纸面考核相似，实验操作考核为安全技术人员开启实验操作模式，教员进行在线监控安全技术人员操作动态，进行同步监控考试。在考试管理中，管理员可以进行相应的考题及题库的管理，对考试的管理，进行考卷批改、考试汇总和实验报告管理等。考题管理中包含试题的增删改查，类型丰富，可以为单选多选，判断简答。题库管理中可以对考题进行分类整合的集中管理。考试管理主要是对考试的时间设置，考试考生安排以及考试发布管理，考卷的批改和汇总管理可对用户的考试结果进行相应的审批和汇总。实验报告管理中可查看用户提交的实验报告并进行相应的评审操作。

平台且具备网络安全攻防演练或竞赛提供灵活多样的竞赛模式和赛题，在演练、竞赛过程中，根据需要可以启动基于不同操作系统平台的赛题，满足信息安全攻防竞赛的需求。信息安全攻防竞技平台能够提供了单兵在线CTF、网络混战、综合靶场三种竞赛模式和配套态势展示。

3.3.3 虚实结合业务真实环境模拟

利用实验室所配备的各类网络设备安全设备能够实现对各种安全设备和网络设备进行管理，通过平台提供的服务器实现虚拟化应用并模拟业务系统，使业务系统与实际工作中的真实网络设备相结合，虚实结合，真实还原业务系统工作环境。

总结

信息安全实验室的建立，可以提高验证银行应用系统中安全设计及安全工程建设的实际效果是否满足信息安全保障体系要求的能力。

信息安全实验室的构建可以给银行内信息安全技术人员提供安全实验环境，为银行信息安全技术培训提供培训环境，提高了银行各部门信息安全技术水平。

信息安全实验室是公司信息安全保障体系持续提高的一个重要支撑平台，为系统安全建设、改造，各种安全理念和技术手段提供直观的验证，为下一步的安全工作指明方向。

通过信息安全实验室的建立，可以加强与第三方安全厂商的合作与交流，建立持续对国际国内最新安全技术前沿的跟踪研究的基础，为建立最有效与最可靠的安全解决方案提供保障。

信息安全实验室可以提供一个对外展示的平台，可以向同行业进行安全事件及解决方案的展示，展示安全技术人员的技术水平和能力。

另外，为应对某些特殊攻击或事件，可以作为一个对互联网异常行为和其它威胁的监控平台，预先发现威胁的发生与蔓延的情况。信息安全实验室将逐步成为安全防御体系的一个必要组成部分。

浅析商业银行数据安全保护体系建设思路

金融事业部 张海仓

一、前言

近年来，随着商业银行信息化的发展，信息系统越来越多的使用于日常工作，成为不可或缺的工具和手段。银行通过信息化大大提高其生产效率，从传统的柜面银行与24小时自助银行，再到手机银行，微信银行。银行的业务受理无论在空间和时间上都得到了极大的拓展，依赖于信息系统的发展而运行发展并壮大；

但是当银行正在利用信息化技术高效率的进行跨地域、跨国家的信息交流时，海量的如客户资料、营销方案、财务报表、研发数据等关乎企业核心竞争力的机密数据也随之被传输。信息技术本身的双刃剑特性也在组织网络中不断显现：强大的开放性和互通性催生了商业泄密、网络间谍等众多灰色名词，“力拓案”、“维基泄密”等事件让信息安全事件迅速升温，信息防泄密成为商业银行越来越关注的焦点。

本文结合目前数据保护技术现状及绿盟科技数据保护建设经验，对商业银行数据保护建设思路进行梳理

二、商业银行数据保护的困境

2.1 数据存在形式多、访问人员多、存储分散、易传播

在商业银行内部，有海量电子数据，纸质数据，且一直处于动态增长状态，如用户基本信息，账户信息；应用系统源码，需求说明，设计说明文档：系统的用户名和密码;系统交付及规划资料：网络拓扑图、IP地址清单;安全设备的告警和自动生成的报告、日志;甚至于一些管理决策支撑信息：如银行经营状况分析报表、某分行业务经营报告、风险管理报告;市场推广活动情况、后督工作记录、拆借操作记录、贷款审批与发放记录、客户征信、董事会、股东会议等会议纪要等等。

这些数据大部分数据被分散存储在全行办公人员PC电脑中，移动存储介质中或个人邮箱中。这种分散的数据存储方式给商业银行数据保护工作带来很大的困扰，同时，人员办公又存在地域上的不集中，一旦发生数据泄露，会很快在全省及至全国范围内扩散。再者，每个机构对员工日常要求和管理的标准高低不一，人员安全意识不均衡，进一步增加了数据保护的难度。

2.2 数据泄露途径多

从数据存储侧泄露来看，这些数据被存放于办公PC，个人笔记本，个人邮箱，移动办公设备以及移动存

储设备中。尤其是可移动办公设备和移动存储设备，容易因丢失或失窃发生数据泄露。

从数据泄露手段角度看，互联网邮箱，公有云网盘，WEB类应用都会成为用户存储和传播企业数据的工具。如某银行为了防止内部数据外泄，将所有办公终端U口全部进行了禁用。但其有一个办公业务应用，是内外网互通的，允许用户上传文档。为了便于日常文件传输，很多用户将大量的数据上传到了此平台。结果，这台应用服务器被攻击，上面存储的大量敏感数据被下载。

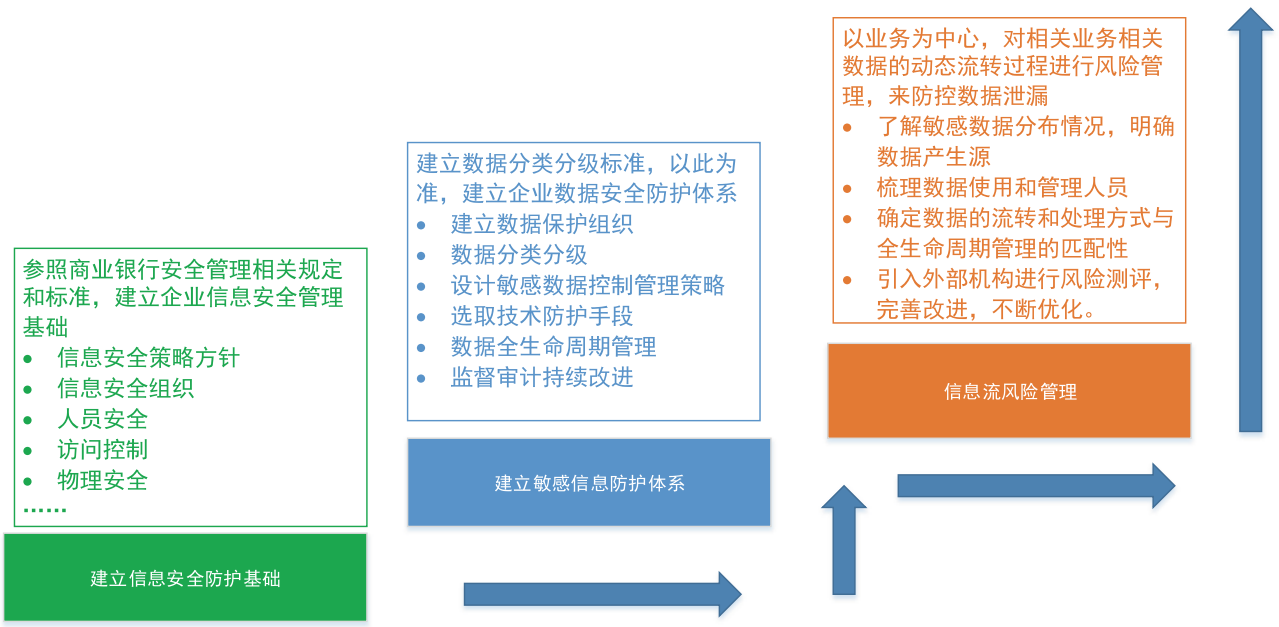
从数据泄露人员来看，商业银行内部办公人员，外部黑客，第三方外包人员以及合作单位或设备维护人员都有可能造成数据泄露。

2.3 数据价值定义不明确，保护工作重点不突出

在有些商业银行没有明确的数据价值定义标准，或者数据价值宣传教育不到位，致使工作人员对手里掌握和拥有的数据不能进行很好的估值，自然而然，对其泄露后产生的后果也就无从评估了。2016年，沈阳某银行在其装修期间将客户资料当废品进行处理，就是一期对客户资料价值错误评估的典型案例。设想，如果该行有明确的数据价值定义和评估标准，而工作人员对此标准又很熟悉，那么在对此类资料进行处理时，就有了处理的标准，而不是随心而为。

数据价值定义不明确的另外一个弊端就是数据保护人员的工作重心不突出，采用大而全的数据安全保护策略，不但自己的工作量大，成效低，不好开展，业务人员或其他部门人员的工作效率也因此而降低，数据保护工作得不到其他部门的认可，推进十分缓慢，甚至终止。

三、数据保护建设步骤



3.1 建立信息安全防护基础

商业银行数据保护建设是信息安全防护中的一部分。因此，在进行数据安全防护建设过程中，需要商业银行有良好的信息安全防护基础，例如机房物理安全，各安全域之间的访问控制，人员安全等。并已经建立完整的信息安全组织，和信息安全策略方针。目前来讲，国内大部分商业银行之部分建立已经基本完成，也就是说，大部分商业银行已经具备建立数据安全防护体系的基础条件。

3.2 建立数据安全防护体系

数据安全防护体系的建设是商业银行数据安全保护的必经之路，整体规划，分步建设，有助于商业银行在逐步提高数据安全保护水平的同时避免资源的浪费，降低数据保护成本和工作难度。一般包括数据保护组织的建立，数据分类分级，数据保护控制策略制定，数据保护技术手段选取，数据全生命周期管理，以及审计与持续改进等内容。

3.3 对信息流进行风险管理

在商业银行数据安全防护体系建设完成后，为了更加精细的控制企业数据的流转并防止泄露，一般会建立以业务流为中心的敏感数据动态流转风险管理，进一步防止敏感数据外泄。其内容包括敏感数据分布状况调研；明确业务系统使用管理人员；确定数据流转和处理方式；并借助第三方安全机构进行数据流转各环节的风险评估，发现薄弱环节，进行加固和修复，长期持续改进等内容。

四、数据安全防护体系建设思路

4.1 完善数据保护组织架构

近年来，伴随着商业竞争的加剧，数据保护工作已经越来越得到企业的重视。随之在市场上已经产生了数据间谍这类职业，他们受雇于某个企业，对其竞争对手的数据进行针对性的窃取。在很多企业也产生了专门的部门或职位来进行单位数据保护工作，可以预见，在不久的将来，这一职位或部门将出现在越来越多的企业中。

数据保护工作涉及到商业银行各个部门及所有业务系统和全行工作人员，因此，数据保护组织的建立过程中应该充分考虑到数据保护工作的系统性，建立完备的组织架构。一般分为决策组织，管理组织，执行组织和审计组织。

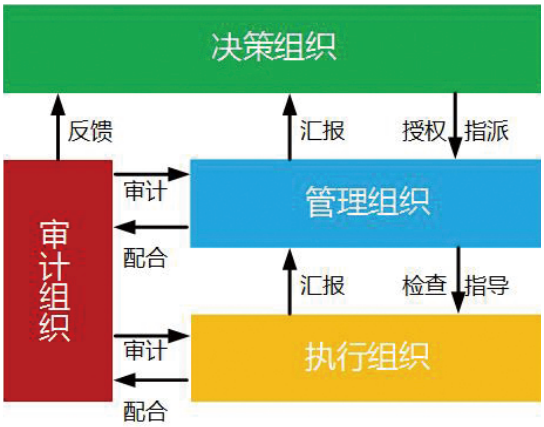
决策组织职责主要有根据公司发展战略，结合企业信息安全策略方针，制定符合企业业务发展的数据保护战略方针；并授权指派管理组织开展数据保护工作；对管理组织的工作进行指导和定期检查；对审计组织反馈的问题进行督导问责和解决。

管理组织职责主要有根据企业数据保护战略方针完善企业数据保护管理制度，规划数据保护建设项目；并向决策组织定期汇报数据保护管理工作情况；对执行组织数据保护工作进行检查和指导；配合审计组织的监督和检查。

执行组织负责具体的数据保护技术工作的实施和执行；并定期向管理组织汇报，接受和配合审计组织监督和检查。

审计组织职责主要是对管理组织和执行组织日常数据保护工作进行监督和检查，并将检查结果反馈给决策组织，跟踪审计问题的解决情况等。

各组织间的关系如下图所示：



4.2 对数据进行分类分级保护

数据保护和信息系统保护类似，应该分等级，分类别，进行重点保护。如果一味追求大而全，密而精，必然使得数据保护工作的效果难以达到预期。这种保护工作，也不可能得到业务人员或其他部门的支持与认可，自然也就无病而终，不能长期有效的开展下去。

因此，商业银行在开展数据保护工作之前，应当有明确的数据分类依据和数据重要程序分级依据。

4.2.1 识别现有数据

数据识别方法有调研了解，技术手段收集等，一般的，为了数据分级工作的准确性，还需要结访谈调研。步骤如下：

1、向各部门分发数据收集表，了解各部门日常工作中所涉及的敏感数据类型。

2、访谈各部门，调研了解敏感信息的重要性。

根据数据收集表的内容，进行各部门的针对性访谈，了解其对自己所在部门数据重要程序的分级情况，为后期数据分级定义工作做准备。

3、通过技术手段，按照数据类型进行敏感数据存储分布调研。

依据前两步调研结果，对通过技术手段，对全网的敏感数据进行收集，分析其存储分分布情况，为后期数据保护策略定义提供依据。

4.2.2 进行数据分类

根据数据识别的结果，依据商业银行自己业务特性或自身情况进行数据分类，一般的分类依据有：

1、根据国家标准和监管要求进行数据分类

这种分类方式简单明了，但存在与商业银行自身业务不匹配或不完全匹配的情况，可能全出现分类过大或过小，存在重合或遗漏的情况。

2、参考同行业进行数据分类；

由于行业的相通性，数据分类也有一定的共同性，参考同行业进行数据分类一种简便而又高效的数据分类方式。

3、根据业务部门和管理部门的经验分类

对于业务形式比较独特的商业银行，如涉及到跨国业务，由于不同国家对数据重要程程度的认识和定义上存在区别，需要业务部门和管理部门进行数据分类时也要考虑其特殊性。

数据分类方式没有统一的标准，各商业银行可以选择一种或多种分类方式进行数据分类。但建议在进行数据分类时遵循如下原则，以保护数据分类的合理性，为后期的数据分级工作提供良好的前提保证。

1、科学性原则

分类过程中应当充分考虑数据的业务属性，同时兼顾数据的敏感性级别

2、实用性原则

数据的类目设置应与商业银行现有的管理和分类相兼容，保证员工的数据分类习惯，降低分类和数据保护的难度。

3、稳定性原则

在进行数据分类过程中，应当充分考虑未来的拓展需求，使得分类保护兼容和稳定。

4.2.3 进行数据分级

数据分级是从数据的机密性角度出发，为了满足数据保护的要求。分级过程可以单独设计，如：

数据分级	敏感程度定义	定义标准
3	高敏感数据	涉及组织重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性影响，如果泄露会造成灾难性损失
2	中敏感数据	涉及组织的一般性秘密，其泄露会使组织的安全和利益受到损害
1	低敏感数据	涉及仅能在组织内某一部门或处室可以公开的信息，向外扩散可能对组织的利益造成轻微伤害

也可以结合保密规定等内容进行，如：

密级定义	数据分级	敏感程度定义
绝密	3	高敏感数据
机密	2	中敏感数据
秘密	1	低敏感数据

数据分级是为了合理的进行数据保护，防止矫枉过正，防护过度，造成防护资源的浪费以及给员工日常办公带来不便，以至于员工抵抗，保护工作无法继续。

4.3 制定数据保护控制策略

商业银行在数据保护过程中，应当根据企业文化，业务特点和敏感数据数据面临的风险情况，对不同环境下的敏感数据设计相应的控制策略，如：敏感性标识，授权审批，信息脱敏，安全隔离。

制定并推进敏感性标识策略

为了让员工在日常工作中，对所产生的数据和接触到数据的重要程度有清晰认知，制定数据敏感性标识策略，并在日常办公过程中推行。

数据敏感性标识可以根据分级重新定义标识标志，如：公开信息，内部使用，商业机密等，也可以直接按照密级进行标识。如果有多个分级定义，需要再进一步细化标识，如：公开信息，内部使用，商业机密A，商业机密AA，商业机密AAA等；

制定数据标识标志后，再依据不同类型的数据制定不同的标识策略，如：

文件，文档类：应当在封面或首页的明显位置标识其使用范围或密级以及期限；

非文件、文档类：例如源代码，数据库数据，应建立所在系统的敏感性标识台账，对所存储的数据进行标识；

信息载体：如光盘，U盘，移动硬盘等，应在介质明显位置进行标注或标签标示。

4.4 制定授权审批策略

由于内部办公的需要，数据不可避免的会在各部门或各工作人员之间进行流动，商业银行应根据企业组织特点，规范各级别敏感数据的授权审批流程。

4.5 制定敏感数据脱敏策略

商业银行应制定严格的数据脱敏策略。商业银行在内部办公，第三方数据交换，测试系统开发过程中，存在大量的数据交互，如果直接使用未脱敏的数据，极有可能造成数据泄露。为此，企业应建立完整的敏感数据脱敏策略来应对数据流转过程中的泄露风险。并结合授权审批策略，强制要求只有数据脱敏，杜绝未脱敏数据泄露。

- 制定安全隔离策略

根据数据分级，敏感性标识和密级定义对不同级别的数据进行分区分级别存储。对涉及敏感信息处理的网络、操作系统、中间件，数据库，甚至业务人员的办公电脑进行物理或逻辑上的安全隔离，保证数据处理环境的安全

◆ 制定第三方数据使用控制策略

在商业银行业务高速发展的今天，涉及到大量的第三方外包人员或第三方公司，银行应当设置专门的控制策略来控制这部分人员的数据使用。策略设置过程中应考虑如下因素：根据不同的级别，设置对应的第三方控制要求；根据所接触数据级别，提高第三方准入门槛，缩小数据接触范围；按照“必需知道”和“最小授权”双重原则进行访问授权。并通过服务合同或协议等，明确第三方在安全和数据保密方面的责任。定期通过安全检查，外部评估等方式对第三方公司策略执行情况进行检查，确保第三方控制策略的的效执行。

4.6 建立技术手段进行数据保护

技术手段是对管理和控制策略的有效补充，同时也是确保控制策略落地的有效支撑，企业应当根据其自身业务特性和控制策略，选择有效的技术手段，来封锁各种数据泄露途径，保证数据安全。好的技术手段应该可以在数据泄露事件发生前，发生时，发生后全过程进行控制。

◆ 事前预防

事前预防指通过技术手段的采用，可以预防数据泄露的发生或提高数据窃取成本，从数据CIA原则出发进行技术手段设计。常见的事前预防技术手段有透明加密，数据脱敏，终端安全，加密key，磁盘加密，移动介质管控等；

◆ 事中阻断

事中阻断是指当数据泄露发生时，其可以识别数据泄露行为并进行阻断。常见的技术手段有网络数据防泄露系统（网络DLP），邮件数据防泄露，终端数据防泄露等。其中终端数据防泄露可以有效防护移动介质拷贝，即时通讯工具传输，截屏，录屏等手段造成的数据泄露。

◆ 事后审计

事后审计是指当数据泄露事件发生后，提供可追溯审计的日志，帮助技术人员进行数据泄露源头或责任人定位。常见的技术手段有数据库审计，日志审计系统以及事中阻断技术手段产生的日志。

4.7 建立覆盖数据全生命周期的制度与技术手段

商业银行在设计和制定数据保护管理制度以及技术措施时，应融入和覆盖数据全生命周期的各个环节。

一般来讲，数据全生命周期包括如下几个环节：

◆ 创建

在数据被创建时，应当通过管理制度和技术手段强制要求数据创建者确定数据安全级别，并进行有效的安全性标识；

◆ 存储

在数据存储过程中，应当根据不同级别的数据采用不同的技术手段进行数据存储，敏感数据应当分环境，加密存储

◆ 使用

数据在流转和使用过程中，应当有明确的应用审批和记录流程，第三方人员的使用应当严格管控。

◆ 传输

需要异地使用数据或传输使用的，应对数据加密后进行传输，并采用加密协议，甚至专人专网进行传输，保证数据在传输过程中不被截取或窃听。

◆ 销毁

在数据使用完毕后，确保完善的技术和管理手段监控数据销毁过程，防止数据被恢复或有备份没有销毁，造成数据的泄露。

◆ 建立有效的审计与持续改进举措

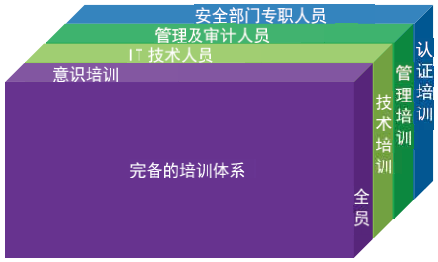
良好的数据保护工作是一个不断改进优化，持续改

进的过程。通过安全检查，审计跟踪，发现问题和解决问题，优化旧的管理制度，使用与新的数据安全形势相匹配的管理制度与技术手段，不断提高敏感信息防护水平。

4.8 建立数据保护安全培训体系

再好的管理策略，多么完美的技术手段，如果不能得到执行者的拥护和执行，一切都将是空谈和摆设。因此，为了保证商业银行数据保护工作的有效落地，降低公司当前所面临的数据泄露风险，商业银行应当建立完备的安全培训体系，提升其安全管控水平。

完备的安全培训体系应当覆盖全员，又重点突出，既包含管理策略，又涉及技术手段；并且针对不同的人群有不同的要求和标准；



总结

商业银行数据保护是一个系统工程，需要多方面的协调与配合，既涉及到组织架构的调整，也有技术手段的增加，管理策略补充，更需要长期的进行人员教育与培训。数据保护整体架构可概况如下：

在阿里云上应用系统的安全防护解决思路

金融事业部 俞 琛

目前公有云的建设发展成为互联网时代的风向标，如阿里云、亚马逊等建立的公有云规模增长迅速。在移动互联网发展推波助澜之下，依托移动互联网开展P2P网贷、线上理财、消费金融、三方支付业务的企业为了享受公有云提供的快捷、弹性架构，从而纷纷将应用系统部署到云上。

首先，合规要求方面，《信息系统安全等级保护基本要求云计算分册》（以下简称“《云等保》”）定义云计算服务带来了“云主机”等虚拟计算资源，将传统IT环境中信息系统运营、使用单位的单一安全责任转变为云租户和云服务商双方“各自分担”的安全责任。这点明确了企业作为云租户，其应用系统都需要定级且符合对应等级安全控制措施要求。2016年12月银监会发布了188号文，《中国银监会办公厅关于加强非银行金融机构信息科技建设和管理的指导意见》（以下简称“《指导意见》”），对信托公司和金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司等非银行金融机构信息科技建设、信息科技风险防范提出了要求。《指导意见》第五章节指出“加强网络区域划分和隔离；通过部署防病毒、防攻击、防篡改、防泄密、防抵赖等措施提升系统抵御内外部攻击破坏的能力；”。对于云上应用系统的安全防护明确提出了安全建设要求。

其次，参考“安全牛”对于2002年至2017年3月之间公开报道的敏感信息泄露案例的数据分析发现：

◆ 敏感信息泄露呈现上升趋势，泄露手段从以黑客入侵等技术手段为主向技术手段与收买内部员工、内部管理不善等非技术手段结合并用发展，特别是对非技术手段的运用，近几年呈现出较快速的增长。企业对可能的应用系统攻击行为没有安全检测防护措施。

◆ 敏感信息泄露涉及行业广泛，但重点集中在互联网、制造业、政府机构及金融行业。

◆ 基于IP的审计，难以准确定位责任人，难以将IP地址与具体人员身份准确关联，导致发生安全事故后，追查责任人成为新的难题。

◆ 互联网行业信息泄露事件呈现高速增长趋势，需要引起警惕。

由此，安全威胁与应用安全风险与企业业务经营如影随形，应用系统部署到云上的企业需要考虑在公有云上应用系统的安全防护解决思路。

作者建议从满足合规要求作为起点，业务在“云上”的企业都需要符合《云等保》要求，非银行金融机构都受到国家对应主管单位的合规监管，未持牌开展业务或违规经营将会后果严重。紧接着，为了达到正常业务开展需要的安全防护水平，安全服务也应纳入，解决应用系统安全检测和安全监测需要。

1. 合规要求

依据《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》，明确定义了云租户侧的等级保护对象也应作为单独的定级对象定级。云计算系统的定级对象在原有定级对象基础上进行了扩展，原有定级对象主要是信息系统和相关基础网络，而云计算将定级对象扩展为云服务商的云平台和云租户的应用系统。云计算系统定级时，云服务商的云平台和云租户的应用系统应分别定级，云平台等级应不低于应用系统的安全保护等级。这点明确了企业作为云租户，其应用系统都需要定级且符合对应等级安全控制措施要求。

对照等保二级要求，应至少部署防火墙、堡垒机达到控制措施要求；对照等保三级要求，应至少部署入侵防护、防火墙、堡垒机、数据库审计达到控制措施要求。在阿里云云市场中当然也有对应的安全防护服务可供选择。对有线下服务需求的企业，如专家版服务，可以直接与绿盟联系，订购线上线下服务套装组合。

《指导意见》第五章节中提出“……加强系统安全漏洞和补丁信息的监测、收集和评估，确保及时发现和处置重大安全隐患。……”漏洞管理工作应该是信息安全工作的重中之重，漏洞生命周期管理不仅仅涉及漏洞自身的发现、评估和修复，同时还牵涉漏洞情报信息的获取，组织漏洞管理基线的建立和应急处置工作。改变传统的以IP信息为视角的资产管理方法，从安全的角度重新审视资产信息，从资产的业务功能、服务对象、版本信息、安全防范措施等方面建立安全资产信息，从安全的角度管理资产脆弱性。当出现安全漏洞时，不仅需要考虑漏洞的风险等级，还需要结合资产安全信息，不同资产相同漏洞区别对待，体现业务对漏洞的差异性，真正实现差异化漏洞管理策略，从而实现漏洞管理能力的提高。

《指导意见》第五章节中提出“……开展应用系统安全检测，对官方网站等通过互联网提供服务的系统，在上线及重大投产变更前进行渗透测试，杜绝系统“带病”上线。……”应用系统在上线后由于存在类似SQL注入、密码明文传输、安全功能缺失等漏洞而遭受攻击，会直接影响正常业务运行，甚至造成经济和名誉的损失。因此，需要在系统上线前对系统安全状况进行检验，从信息安全的角度对应用系统、集成环境等内容的安全状况进行评估，对发现的问题进行妥善处理，避免将影响系统安全的问题遗留到系统上线后，成为系统安全的隐患。

为了满足《云等保》和等保三级要求，部署了阿里云上应用系统的企业应至少选择防火墙云服务（支持入侵防御）、网站安全防护服务(vWAF)、堡垒机云服务和数据库监控与审计服务。

非银行金融机构需要同时满足《指导意见》要求，其阿里云上应用系统应选择安全检测服务和安全监测服务。

2. 安全保障需求

先回顾近期某互联网公司发生的信息安全案例，公司内部员工对公司200余台服务器植入木马，该木马具备远程控制和对外DDoS攻击功能。这意味着外部人员可远程控制这些服务器做流量攻击，进而导致被攻击的服务器瘫痪。目前，此事已在法院宣判。至案发时，内部员工获利2万余元，但对于企业的经济和名誉损失就相当巨大。不少互联网企业都发生过类似案件，但没有安全检测和安全监测手段，无法及时发现漏洞和安全问题。有的企业虽能锁定具体账户，但无法锁定到具体个人，加之留存的证据不多，事情就不了了之。

信息安全CIA三要素（机密、完整、可用）应当在定义安全保障需求时统一考虑，对开展理财、支付、保险等金融业务的企业更应关注金融资料的保护，如银行账户信息、扣款账号、保险数据，避免信息被篡改或外泄。

因而，为了达到正常业务开展需要的安全防护水平，需要定期开展安全检测和持续有效安全监测服务，云上应用系统更应被纳入，解决应用系统安全需要。部署了阿里云上应用系统的企业可以选择云清洗服务，电子签章服务，安全可视化服务等增值安全服务，提升安全保障水平。

3. 云上安全防护措施

◆ 防火墙云服务

以虚拟化形态部署防火墙，适用于多种虚拟化平台，使管理员可以快速高效地调配和扩展防火墙。企业所要选择的服务需要支持应用识别、入侵防御、内容过滤、URL过滤、VPN等，且这些增值功能授权费用应该一并考虑，如IPSEC VPN 、SSL VPN的授权并发连接数量是否满足企业日常需求。包含必要增值功能的防火墙才是有效的安全服务。

◆ 网站安全防护服务(vWAF)

以虚拟化Web应用防火墙(Virtual Web Application Firewall， 简称 vWAF)为核心的安全服务，企业客户可以在公有云等环境中快速部署上线，从而能全面抵御OWASP Top 10等各类Web安全威胁免遭当前和未来的安全威胁。企业所要选择的服务必须同时支持HTTP协议和HTTPS协议，且可以支持vWAF托管服务的服务提供商更佳。

◆ 云清洗服务

基于DNS智能牵引技术，主要解决10G及以上大流量DDoS攻击防护，同时可防御电信、联通和BGP三条链路大流量攻击，而运营商提供的云清洗服务仅能清洗本网内的攻击流量。由于DDoS攻击可能在相同行业内同时发生，存在带宽和防护资源冲突情况，因而企业选择服务时需留意服务提供商的清洗能力是否充足。同时，建议选择提供云清洗配套线下本地防护混合的服务，以获得更完善的防护保障。

◆ 堡垒机云服务

以虚拟化形态部署堡垒机，提供账号管理和资产管理，实现运维审计。基于唯一身份标识，通过对用户从登录到退出的全程操作行为进行审计，监控用户对目标设备的所有敏感操作，聚焦关键事件，实现对安全事件的实时发现与预警。企业所要选择服务需满足等保标准对用户身份鉴别、访问控制、安全审计等条款的要求，且支持准确定位用户身份，追溯安全事件责任，满足合规要求且日常使用方便的服务才是正确选择。

◆ 安全检测服务

服务提供对各种Web应用系统漏洞和操作系统漏洞安全检测，可按需定制检测扫描频率，用于网站安全评估的云服务。企业选择服务时需了解服务包含的漏洞库种类、是否维护更新，且对于识别的漏洞是否提供漏洞验证服务，降低误报概率。

◆ 安全监测服务

服务符合网信办、公安部等国家主管机关关于网站安全建设的合规要求，为客户提供网站漏洞扫描及漏洞验证、网页挂马监测、钓鱼网站监测、网页篡改监测、网页敏感内容监测以及网站可用性监测服务。通常本服务包含安全检测服务内容。企业应留意监测服务是否在重要时期支持发送平安短信以及安全日报，是否能够协助关停发现的钓鱼网站，这点值得关注。

◆ 电子签章服务

依据《电子签名法》获得权威数字认证，采用第三方授时技术，防篡改技术多项核心技术实现流程规范，保障电子文件/电子合同与纸质合同具有同等法律效力。企业可留意选择所有交互环节都通过接口实现，不干涉平台业务逻辑，完全满足业务全流程需要。

◆ 安全可视化服务

依托云端技术和大数据安全分析能力，以可视化方式为用户快速构建多层次联动纵深防御体系，基于数据驱动及时发现隐患从而加强安全防御能力。企业所要选择的服务应自建威胁分析模型，而且提出可行的规避建议。

◆ 数据库监控与审计服务

通过对数据库访问行为的精确解析，完成性能监控、事中审计、事后追溯、风险告警等一系列动作，全面洞察数据库安全状况，并提供事后追溯依据。企业所要选择的服务是否全面考虑数据库存储、使用管控，监控告警记录本地是否加密防护，这一点很重要。

4. 云上服务优势

◆ 便捷快速

依托公有云提供的快速部署、实时开通的能力，客户可以随时在公有云上按需选购，同时也避免了硬件设备的生产、货运和上架环节，最短时间内就能获取到对应的安全能力。

◆ 恶意行为发现

基于实时的信誉机制，结合企业级和全球信誉库，可有效检测恶意URI、僵尸网络，快速识别、定位出恶意的攻击行为或恶意资源。

◆ 通过云安全服务提供应急响应

凭借云安全服务的支撑（MSSWAF），可以实现与云安全中心对接和同步，由安全专家团队协助用户对网站安全隐患和遭受的攻击威胁进行7*24小时全天候监控，并定期优化安全策略，提供安全日志分析报告。

◆ 深度对接公有云特性

通过与公有云的API进行对接，辅助堡垒机云服务实现托管资产信息自动录入，减轻运维人员工作难度，提高效率。

◆ SaaS安全管家

在获得用户授权后，云上服务自动把运营数据上传给云中心，用户在手机上实时查看运行状态以及异常告警，并且一键寻求安全专家与技术支持团队，第一时间解决安全问题。

总结

本文期望达到安全普惠效果，为企业提供应用系统线上安全防护解决思路。

参考文献

安全牛公众号《国内外敏感信息泄露案例汇总分析》

2017 年上半年重大黑客事件盘点

在过去的 2016 年，发生了许多大规模和令人震惊的网络攻击事件。正如我们所预料的，2017 年我们将面对更严峻的安全挑战！下面让我们共同回顾下截至当前，网络上所发生的重大的安全事件。

1. 加拿大贝尔公司190万客户信息泄漏

加拿大贝尔公司（Bell Canada），约190万个活跃电邮地址，约1,700个客户姓名以及在用电话号码遭到匿名黑客的非法入侵。由于该公司拒绝支付黑客的赎金要求，而导致部分客户数据被在线泄漏。

2. Edmodo教育平台超7700万信息泄漏

黑客入侵教育平台Edmodo，窃取超7千万教师、学生和家长账户信息。通过对盈利性漏洞通知网站LeakBase提供的200多万个用户记录的样本进行验证发现，这些泄漏数据包括用户名、电子邮箱地址以及散列的（hashed）密码等信息。

目前，一个化名为“nclay”的供应商正在暗网市场Hansa上以1000多美元的价格出售这些Edmodo用户数据。此外，根据LeakBase 所言，Nclay还声称自己手中掌握着7700万个用户账户信息，其中4000万个账户中含有电子邮箱地址信息。

Mac视频编码器HandBrake感染恶意软件在HandBrake（Mac的视频编码器）被感染恶意软件之后，数以千计的机会在五月初被感染了远程访问木马。那些被感染的人有盗窃窃取OS X Keychain登录证书的风险。

3. Proton木马入侵HandBrake服务器

HandBrake用于下载的镜像服务器（download.handbrake.fr）遭到未知黑客的入侵，并将HandBrake客户端的Mac版本（HandBrake-1.0.7.dmg）替换为感染了Proton新变种的恶意版本。一旦用户下载了包含该恶意程序的Mac版本，攻击者将获取目标苹果的Root访问权限。

9. 美国中央情报局数千份机密文档泄漏

中情局数千份机密文档泄露，这些文件不仅暴露了CIA全球窃听计划的方向和规模，还包括一个庞大的黑客工具库，网络攻击入侵活动对象包括微软、安卓、苹果iOS、OS X和Linux等操作系统和三星智能电视，甚至是车载智能系统和路由器等网络节点单元和智能设备。许多文件还被分类或标记为“最高机密”。在加上此前的NSA事件，可谓是情报界的一大尴尬。

6. WannaCry勒索病毒席卷全球

5月12日晚，一款名为Wannacry的蠕虫勒索软件袭击全球网络，这被认为是迄今为止最巨大的勒索交费活动，影响到近百个国家上千家企业及公共组织。之所以能产生如此大的影响力，还得‘归功于’NSA泄漏的0day黑客工具的加持。在该事件爆发不久后，美国国会便提出了一项法案，以阻止政府存储网络武器的行为。

5. 英国发薪日贷款机构Wonga违约，影响27万账户

英国发薪日贷款机构Wonga四月发布声明称，该公司部分客户信息可能遭到非法和未经授权的访问。数十万账户的个人详情可能被非法访问，有报告显示这一数字可能多达27万。Wonga表示曝光的信息可能包括客户的姓名、电子邮件地址、家庭住址、电话号码、一张卡号、银行账号、以及排序代码的最后四位数字。

就在信息泄漏事件发生数月后，黑客便窃取了特易购银行9000名在线客户总计250万英镑的巨款。该事件被归咎于“系统、复杂的网络攻击”，目前仍在该国犯罪机构和国家网络安全中心的调查之下。

8. 暗网托管商Freedom Hosting II被黑

Freedom Hosting II 代管暗网上 20% 的网站，可说是最大的暗网托管服务。但就在二月份，一个匿名的黑客由于看不惯其为儿童色情网站提供托管服务，而黑入了Freedom Hosting II导致其所有托管网站下线。

该名黑客称，他已经发布了 Freedom Hosting II 的系统档案，但是不含使用者资料，因为有敏感的儿童色情资料。同时他也表示他会将这些资讯交给与执法机构合作的信息安全研究人员做进一步处理。

4．知名内部沟通软件HipChat数据库泄露

黑客通过第三方扩展中的漏洞攻击了HipChat服务器，并导致数据库泄露，泄露的数据库中包含了用户的姓名、用户账户以及哈希密码等，好在没有证据表明用户信用卡信息遭到泄露。

7. 手机破解专家Cellebrite公司被黑，900GB数据泄露

世界上最臭名昭着的iPhone和设备破解公司Cellebrite，在1月份遭到了黑客入侵，并导致数百GB的企业敏感文件遭到泄漏。据悉，这些数据中包含了大量Cellebrite的用户资料（包括登录信息），技术细节，遭到破解的手机数据和公司设备日志。其中部分资料显示该公司曾向阿联酋，土耳其和俄罗斯等政府提供手机破解设备。

11. 字体共享网站DaFont网站被黑，69.9万用户信息泄漏

字体共享网站DaFont 五月份遭到黑客攻击，699000个用户账号信息被盗，其中包括用户名、电子邮件地址和散列密码等。由于用户设置的密码过于简单，结果导致超过98%的用户密码被成功破解。

12. 俄罗斯黑客攻击60多所大学和美国政府机构系统

俄罗斯黑客Rasputin在今年二月份，黑掉了60多所大学和美国政府机构的系统。据了解，Rasputin主要使用一些由自己开发的SQL注入工具，来完成入侵任务。

被Rasputin黑掉的受害者有：10所英国大学、20多所美国大学、大量美国政府机构（包括邮政管理委员会、联邦医疗资源和服务管理局、美国住房及城市发展部、美国国家海洋和大气管理局）。

10. 著名网络服务商CloudFlare泄露海量用户信息

著名的网络服务商CloudFlare又曝出“云出血”漏洞，导致用户信息在互联网上泄露长达数月时间。据谷歌安全工程师Tavis Ormandy披露，CloudFlare把大量用户数据泄露在谷歌搜索引擎的缓存页面中，包括完整的https请求、客户端IP地址、完整的响应、cookie、密码、密钥以及各种数据。

经过分析，CloudFlare漏洞是一个HTML解析器惹的祸。由于程序员把>= 错误地写成了 ==，导致出现内存泄露的情况。就像OpenSSL心脏出血一样，CloudFlare的网站客户也大面积遭殃，包括优步(Uber)、密码管理软件1password、运动手环公司FitBit等多家企业用户隐私信息在网上泄露。

13. 黑客向苹果要7.5万美元赎金，否则抹掉2亿个iCloud账号

今年三月份，一个自称为“土耳其罪犯家族”的黑客组织，声称已经破解了超过3亿个苹果电邮账户，并向苹果索要7.5万美元的赎金，要求苹果以比特币或以太坊（Ethereum，另一种电子货币）的形式进行支付，否则将抹掉数亿个iCloud账户的数据。

不过，这个黑客组织说话有些前言不搭后语，此前一位代表称他们破解了3亿个账户，但后来这个数字又变成了5.59亿，而现在他们则发推文称要抹掉2亿个账户。

对于此事，苹果发言人并未给予置评。只是表示：苹果系统没有受到任何袭击，包括iCloud或Apple ID账号。所谓的电子邮件地址和密码名单似乎是黑客通过第三方服务获得的。

14. 美国达拉斯警报器遭黑客入侵，警笛声持续一小时

今年4月，达拉斯紧急警报器系统被黑客入侵。导致该城市的156个紧急警报器被激活，警笛声持续一个小时，引发市民恐慌。

在警报系统被黑之后，城市官员被迫基本上拔掉整个系统，完全停用警报系统。调查后，城市官员确认了系统存在的漏洞，并且进行了及时修补。

15. 纽约机场超750GB备份数据泄漏事件

今年2月，纽约斯图尔特国际机场750GB备份数据被暴露在互联网上，没有密码保护、无须任何身份验证。

泄露的数据包括来自机场内部的 107GB 个人电子邮件通信内容，以及来自美国国土安全局（DHS）和联邦机构运输安全管理局（TSA）的信件，还包括员工社会保障号（SSN）、工资记录。许多泄露的文件标有“仅供官方使用”、“未经授权公布将受到民事处罚”警告字样。此外，泄露的数据海安包括机场系统的密码列表，攻击者可不受限制地访问机场网络。

16. 美国执法论坛71万账户泄露，涉国家安全局、FBI等

今年2月，一个自称“Berkut”的黑客在暗网出售美国警察论坛PoliceOne.com的数据库，包含约71.5 万账户信息，涉及联邦调查局、美国国家安全局以及国土安全部等，泄漏信息包括用户名、电子邮件以及哈希密码等。

17.美国空军数千份高度机密文件泄漏

3月16日，一份没有设置密码验证的备份服务器暴露了数千份美国空军的文件，包括高级军官的高度敏感个人文件资料。

安全研究人员发现，任何人都可以访问数GB的文件，因为联网备份服务未设置密码保护。

据悉，这些文件包含一系列个人文件，例如4000多名军官的姓名、地址、职级和社保号。另一份文件罗列了数百名其它官员的背景调查（Security Clearance）等级，其中一些军官拥有能访问敏感信息和代号级别的“最高机密”许可。文件还包含数个电子表格，其中罗列了工作人员及其配偶的电话和联系信息等其它敏感个人信息。这个备份驱动还包含数GB的Outlook电子邮件文件，包含好几年的电子邮件。

专家点评

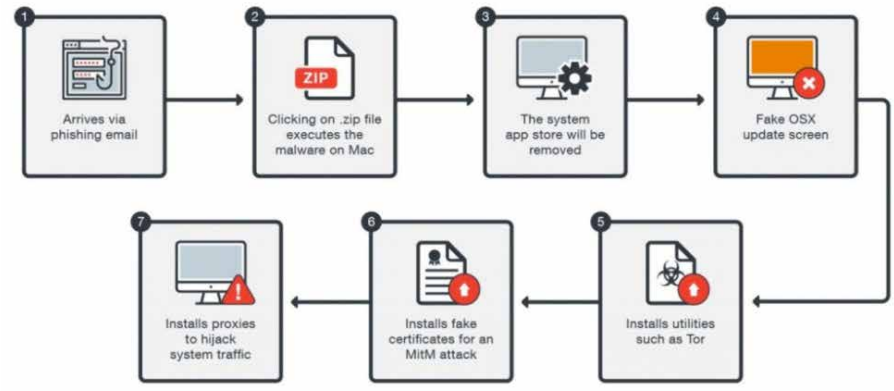
总结上半年的重大安全事件，基于政治和经济利益的攻击越来越多。而且在比特币的加持下，暗网成为黑产犯罪的温床， 而通过“勒索”来获利的方式，日渐变为网络犯罪的重头戏。通过暗网买漏洞、工具->攻击网站、拖裤->拿到信息再去暗网交易形成一个完整的产业链。面对这些威胁我们可以做的是：

1. 保持操作系统及软件的及时更新，尤其是重大的安全更新，及时修复已知漏洞。
2. 部署APT防御产品，重点在互联网出口和邮件服务器区域。
3. 完善web防护体系，要建立新业务上线安全评估制度，并部署web应用防火墙等设备。
4. 监控和审计系统要完善，尤其数据库审计是重点。
5. 加强内部安全防范，防止内鬼及内外勾结作案。
6. 经常性开展安全意识培训及分享，牢固树立安全观念。

参考来源：zdnet，FB小编 secist 编译，转FreeBuf；
原文链接：http://www.freebuf.com/news/135842.html

Operation Emmental 幕后黑手再度潜入瑞士银行系统

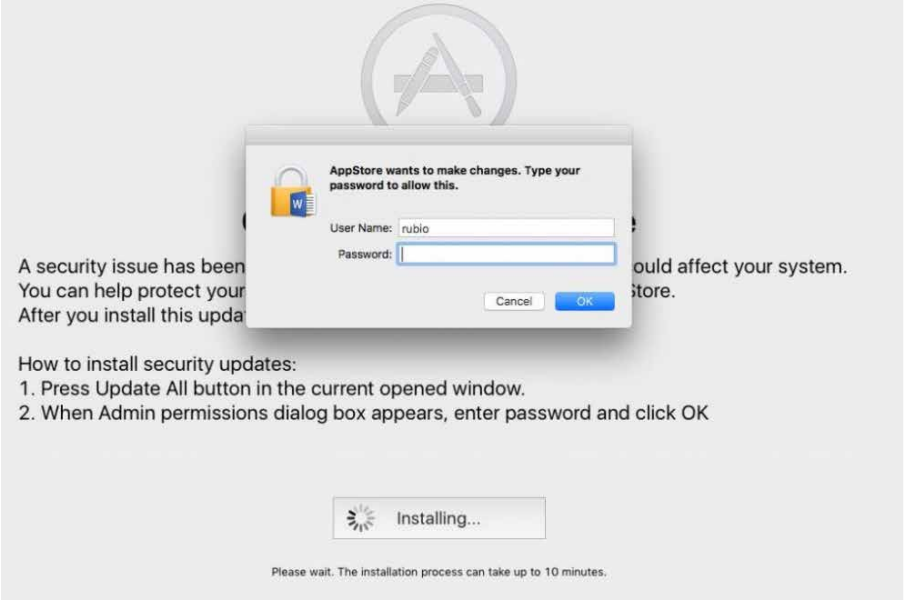
据外媒 7 月 10 日报道，趋势科技（ Trend Micro ）研究人员近期发现黑客活动 Operation Emmental 幕后黑手利用 OSX/DoK 恶意软件新变种 OSX_DOK.C 针对瑞士银行系统展开新一轮攻击活动。



2014 年 7 月，趋势科技研究人员发布一份关于黑客活动 Operation Emmental 报告，指出攻击者绕过金融机构双重身份验证入侵瑞士银行账户、窃取客户私人敏感信息。OSX/DoK 允许黑客通过拦截授权操作短信令牌、更改域名系统设置诱导受害者访问虚假银行网站。

近期，研究人员发现黑客更新代码并通过电子邮件传播恶意软件 OSX/DoK 新变种 OSX_DOK.C。据悉，后者一旦感染 Mac 系统后将窃取管理权限并安装新 root 证书，拦截包括 SSL 加密流量在内的全部通信记录。

调查显示，仅当受害者外部 IP 地址位于瑞士时，OSX_DOK.C 才会劫持用户流量。被感染系统将重定向至虚假金融机构登录页面。此外，OSX_DOK.C 还具备其他复杂功能，如滥用证书与安全软件漏洞、影响苹果系统设备正常使用等。目前，OSX_DOK.C 正利用可执行文件压缩软件（UPX）漏洞包装木马以规避安全软件检测。



原作者： Pierluigi Paganini， 译者：青楚，译审：游弋

本文由 HackerNews.cc 翻译整理，转自 HackerNews.cc，

原文链接: http://hackernews.cc/archives/12228。

专家点评

❶ 根据外媒的报道，无论是OSX/DoK 病毒或者是新变种 OSX_DOK.C病毒，其主要的传播途径都是通过邮件作为传播媒介。作为客户端用户，应该加强安全信息意识，对来历不明陌生的邮件不应该随便打开，通过安装防病毒软件加强个人终端防病毒入侵；作为邮箱的服务提供商，应该有义务对类似的具有威胁邮件通过邮件过滤安全系统过滤，如绿盟科技的邮件安全网关SEG，而不应该让这些邮件有机会扩散到客户的邮箱里。

❷ 对于感染了病毒的客户终端，黑客最终的目的是引导客户去访问预先设置的钓鱼网站或者虚假网站，欺骗客户的相关用户信息。因此，作为瑞士银行应该有义务保障银行客户的利益，实时监控在互联网上冒充瑞士银行的非法钓鱼网站存在，及时发现后并且举报。绿盟科技可以为银行金融客户提供类似的服务，可以为我们的客户提供全天候的网站安全监测服务（WebSafe Service），防止客户的钓鱼网站出现。

黑客再次入侵川普酒店：信用卡支付数据泄露

据《财富》网站北京时间7月13日报道，美国川普国际酒店管理公司（Trump International Hotels Management）当地时间周二晚间表示，由于一家服务提供商的系统遭到黑客入侵，旗下14处酒店的客户信用卡支付细节遭到外泄。

川普酒店网站上的一份通知显示，黑客攻击了川普酒店服务提供商——Sabre的中央预订系统处理，从而造成部分川普连锁酒店的客户预订信息泄露，这些被泄露的信息包括支付卡号以及卡安全密码。

此次攻击，是今年5月份所披露Sabre预订系统遭到网络攻击的一部分。全球范围内，Sabre公司的预订系统被近3.2万家酒店所使用。

川普酒店网站通知称，Saber公司在6月5日告知川普酒店，包括拉斯维加斯、芝加哥在内的多家等城市的川普连锁酒店的客户信息遭到外泄。通知还称，泄密仅仅发生在川普酒店所使用的预订服务系统Sabre Hospitality Solutions，但川普酒店的电脑系统本身并未受到影响。

另据《洛杉矶时报》网站的报道称，美国中间派智库“新美国基金会”高级研究员彼得·辛格（Peter Singer）对此表示，“为何黑客要攻击酒店？因为它们是很好的目标。然后你再看看川普的连锁酒店，很显然，它们更是一个具有高度象征意义的目标。”

辛格称，最近几个月来，这家连锁酒店可能对黑客更具有吸引力，因为它吸引了源源不断、希望与特朗普总统开展业务往来的共和党议员、行业游说人士和外国政要前来入住。

去年，川普酒店曾出现7万多张信用卡号码和300多个社安号外泄事件，因未立即通知客人，被纽约州罚款5万美元。作为达成和解协议的一部分，当时川普酒店表示同意支付罚金，也同意更新安全技术。

Sabre的调查发现，未经授权黑客在2016年8月10日首次访问了该公司的预订信息系统，而最后一次未经授权访问是在今年的3月9日。

川普酒店拒绝对此置评。

文章源自：凤凰科技讯，翻译：若水；

原文链接：https://www.easyaq.com/news/880608964.shtml

专家点评

川普酒店此次信用卡支付数据泄露，原因是其所使用的预定服务系统遭受攻击，而此系统是由外部供应商Sabre所提供。其实对于各行业来讲，或多或少都会采购商业公司的软件系统，如果未对系统做准入要求，或是未对系统做定期的安全评估，因系统自身原因造成的信息泄露很难去主动防范，尤其是全球广泛使用的信息系统。绿盟科技建议：

1. 对于采购的外部商业信息系统，要求提供独立第三方机构的安全测评报告；
2. 对于现网运行的信息系统定期进行安全测评，以及在系统版本变更后及时进行安全测评；
3. 购买网络安全保险，以转移部分风险。

报告：美国大型银行 65% 未通过网络安全测试

7月8日讯 非盈利在线信任联盟（OTA）发布“2017在线信任审核&荣誉榜”（2017 Online Trust Audit & Honor Roll）报告。报告评估审核的对象为1000多个网站，其审核标准分为三个构面：消费者保护、安全与隐私。

报告内容

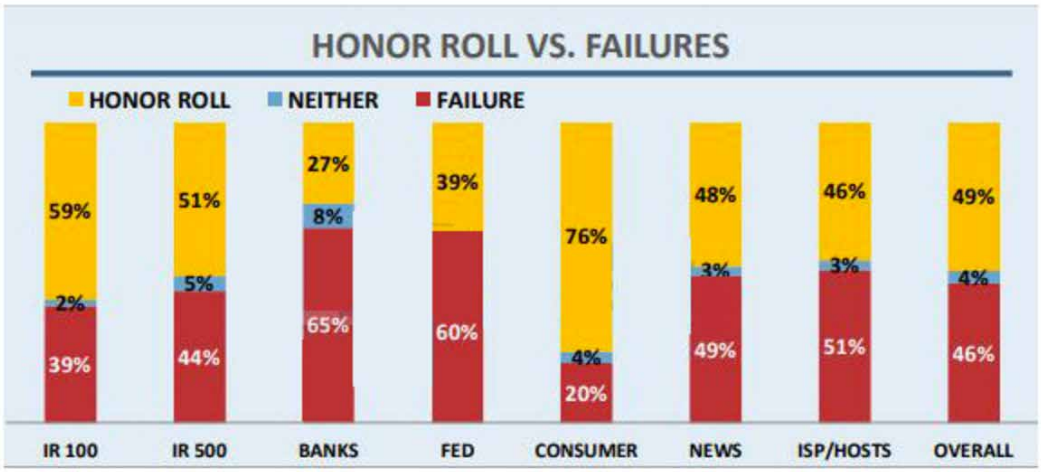
这份报告显示，美国多家银行在安全与隐私方面相当差劲，美国甚至一些大型银行的网站也未满足标准。金融行业的不及格比例最高，而“荣誉榜”入围比例最低。

要荣登“荣誉榜”，在消费者保护、安全与隐私方面的得分必须达到80%。而美国各大银行在这三个方面表现得一塌糊涂。

这1000家网站中，有52%的网站荣登“荣誉榜”，相比2016年，总体增加5%。OTA创始人Spiezle表示，互联网经济靠的是数据。如果数据不安全，或者给用户带有负面体验，那么最终会威胁互联网未来的增长以及收入潜力。

美国银行：安全欠佳、数据易泄露

100家大型的美国银行中，仅27%家银行入围“荣誉榜”，相比2016年减少了28%。OTA表示，该行业呈现出改善的迹象，但由于数据泄露事件增加，隐私得分较低，再加上电子邮件验证等级低，因此情况变得更加糟糕。



美国银行家协会（American Bankers Association，ABA）对此结果表示质疑。ABA支付与网络安全政策高级副总监道格·约翰逊表示，银行“非常重视安全与隐私”。

荣誉榜与顶级美国公司的不及格率

ABA坚称，24%的银行2016年遭遇了数据泄露事件，这不属实。约翰逊表示，银行一直被视为安全典范，是其它行业在安全方面的模板。

调查结果发现，大型银行的网站安全性相对较好（17%不及格），而电子邮件安全（45%不及格）和隐私（34%不及格）表现较差。

文章转载自：网堤安全；

原文链接：https://www.ddos.com/article/detail?id=338。

专家点评

调查分析后发现大多数金融机构严重的入侵行为均源自公司犯下的低级错误，这些错误可通过访问管理、安全方法，以及查看重大异常行为轻松补救。简单有效应对措施，例如物理隔离网络、速率限制、IP信誉，以及改进身份管理等。其它简单的想法，例如隔离区分、对资产和访问进行安全分类，以及管理特权身份和访问会带来高投资回报率，并且能够降低损失。

韩国最大比特币交易所 Bithumb 遭入侵 用户损失数十亿韩元

韩国最大的比特币和以太坊交易所Bithumb最近被黑客入侵。受损帐户的货币损失已经开始浮现，并迅速达到数十亿韩元。

据报道，占有韩国比特币市场份额75.7%的Bithumb是世界五大比特币交易所之一，每天交易量超过13,000比特币，约占全球比特币交易量的10%。

该交易所也是世界上最大的以太坊市场。尽管韩元目前是比特币的第四大货币市场，落后于美元、人民币和日圆，但韩圆市场是以太坊最大的市场。Bithumb在韩国的以太坊交易中占比44%左右。

根据当地的一家主要报刊《京浜新闻》报道，上周末网络攻击Bithumb导致客户账户损失数十亿。一名受害者独自声称，他的账户中“价值1000万韩元的比特币，立即消失”。

黑客成功获取了31,800名 Bithumb网站用户的个人信息，包括他们的姓名、手机号码和电子邮件地址。该交

易所声称这个数字约占客户的百分之三。

Bithumb于6月29日发现违规行为，并于6月30日向当局报告。此后，超过100名Bithumb客户向国家警察局网络犯罪报告中心提出申诉。

Bithumb虽然承认他们的网站被黑客入侵，但表示黑客没有直接访问存储在交易所的资金。尽管如此，许多客户仍在报告他们的数字货币钱包被清空。交易所进一步声称入侵是针对属于员工的个人电脑，而不是交易所的内部网络、服务器或数字货币钱包。

“员工个人电脑，而不是总部服务器被黑客入侵，一些用户的手机和电子邮件地址等个人信息被泄露，但有些客户因电子金融交易中使用的一次性密码而被盗用。”

虽然受害者确切地说出他们的资金是如何被盗的，但却有很大的差异。攻击者似乎已经窃取了足够的证书，开始了一个“语音网络钓鱼”的过程，在那里，骗子们伪装成作为Bithumb的代表给受害者打电话。

一名受害者声称攻击者是Bithumb的一名执行官，并打电话说他是“怀疑外国黑客交易”，并指示受害者给他一份“Bithumb信”中的号码。号码是受害者的一次性密码（OTP），它能够授权攻击者立即获得一千万韩元，价值约8,700美元。

交易所在网站上发布通知，声明 “个人信息泄露案件的赔偿已经确定”。该公司表示，他们将向会员支付每人10万韩元，目前价值870美元。一旦确认金额将进一步赔偿。

他们还声称，他们立即向三家独立机构，韩国通信委员会，韩国互联网安全局（KISA）和最高检察院报告。然而，“先驱报”星期一报道说，预计约有100名受害者将对Bithumb提起集体诉讼。

即使损害赔偿被证明，交易所是否对遗失的资金负有法律责任是不清楚的。由于缺乏对韩国数字货币的监管，情况并不复杂，这些规定尚未得到承认。

文章转自：比特币之家；

原文链接：http://www.btc798.com/article-12132-1.html。

专家点评

比特币是世上第一种分布式、网络由用户构成，不再基于对货币发行机构信任的货币系统。比特币本质就是一个基于互联网的去中心化账本,而区块链就是这个账本的名字。对于比特币等数字货币具备两个特性：

❶ 区块链上的交易公开化：任何人都可以查询某个帐户（地址）的所有相关交易；

❷ 区块链账户（地址）匿名性：除非账户所有者主动公开，否则无法知道某个地址属于谁；

基于这两个特性也就意味着比特币被盗后，可以通过交易公开化这一特性，追踪后续所有的交易，但由于窃贼可以通过各种混币交易的方式让这个追踪变得几乎不可能完成。对于比特币被盗事件，绿盟科技建议用户遵从如下建议：

❶ 妥善保管你的比特币私钥；

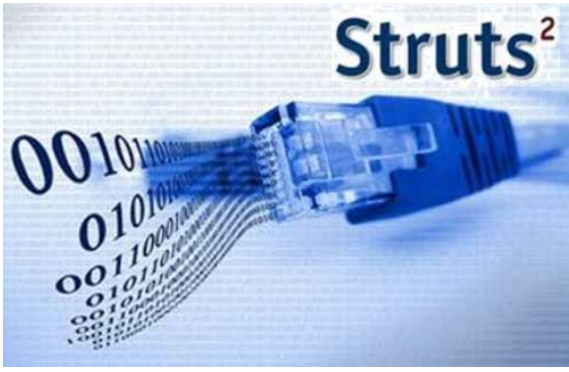
❷ 提防钓鱼网站等各类钓鱼攻击；

❸ 慎用在线电子钱包，在线电子钱包的安全性你无法控制，不要把大额比特币存放其中。

NSFOCUS

漏洞聚焦

Apache Struts2 远程代码执行漏洞（S2-048）技术分析与防护方案



发布时间：2017 年 7 月 8 日

综述

2017年7月7日，Apache Struts发布最新的安全公告，Apache Struts 2.3.x的strus1插件存在远程代码执行的高危漏洞，漏洞编号为CVE-2017-9791（S2-048）。攻击者可以构造恶意的字段值通过Struts2的Struts1的插件，远程执行代码。

相关链接如下：

https://cwiki.apache.org/confluence/display/WW/S2-048

威胁影响

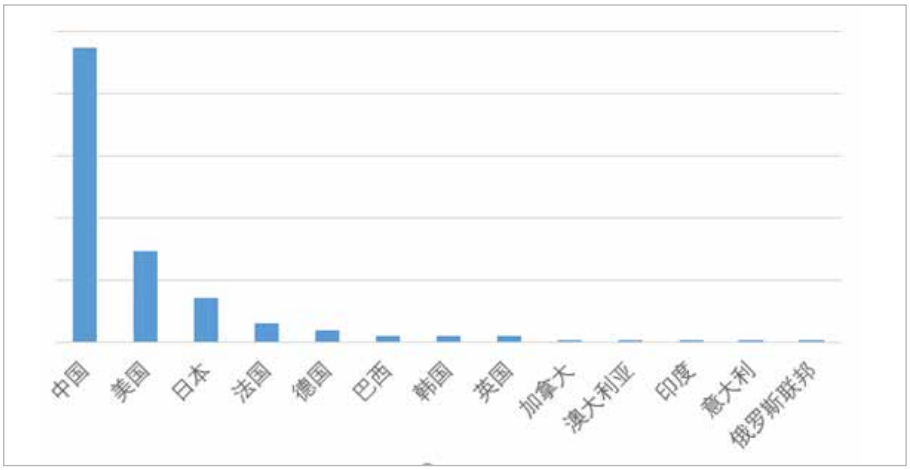
全球分布图

（数据来自绿盟科技威胁情报中心NTI）

国内分布图

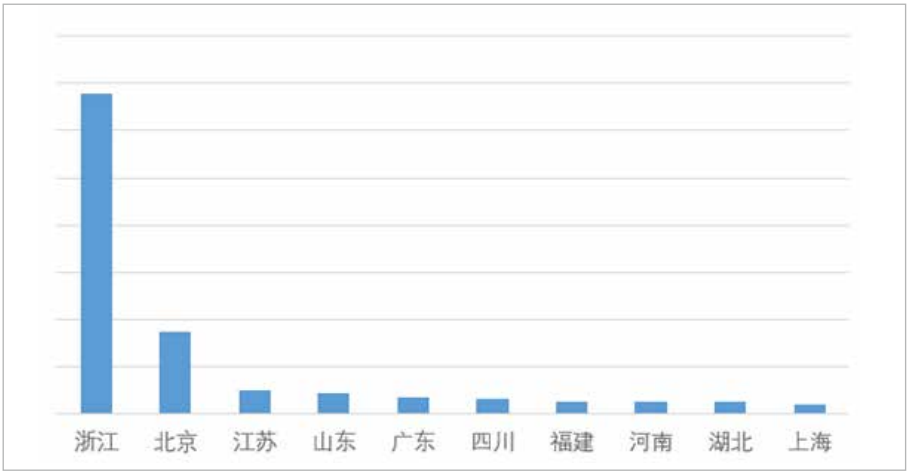
（数据来自绿盟科技威胁情报中心NTI）

全球排行



（数据来自绿盟科技威胁情报中心NTI）

国内排行



（数据来自绿盟科技威胁情报中心NTI）

防护方案

官方解决方案

官方已经发布了版本更新，建议用户升级到Struts 2.5.10.1版本，下载链接如下所示：

- https://github.com/apache/struts/releases/tag/STRUTS_2_5_10_1
- http://struts.apache.org/download.cgi

临时修复方案

- 开发者通过使用资源调用方式替代原始值传递方式给ActionMessage的方式。如下所示：

```
messages.add("msg", new ActionMessage("struts1.gangsterAdded", gform.getName()));
```

不要使用如下的方式：

```
messages.add("msg", new ActionMessage("Gangster " + gform.getName() + " was added"));
```

- 在非必要的情况下禁用struts2-struts1-plugin插件。将struts2-struts1-plugin-2.3.x.jar文件从 “/WEB-INF/lib” 目录中移动到其他文件夹或者删除。

技术防护方案

◆ 绿盟科技检测方案

1) 如果您不清楚是否受此漏洞影响，公网资产可使用绿盟云紧急漏洞在线检测，检测地址如下：

https://cloud.nsfocus.com/#/krosa/views/initcdr/productandservice?page_id=12

2) 内网资产可以使用绿盟科技的远程安全评估系统(RSAS V6)或 Web应用漏洞扫描系统（WVSS） 进行检测。

◆ 远程安全评估系统（RSAS V6）

http://update.nsfocus.com/update/listRsasDetail/v/vulweb

◆ Web应用漏洞扫描系统（WVSS）

http://update.nsfocus.com/update/listWvssDetail/v/6/t/plg

通过上述链接，升级至最新版本即可进行检测！

◆ 绿盟科技防护方案

使用绿盟科技防护类产品（IPS/IDS/NF/WAF）进行防护

◆ 入侵防护系统（IPS）

http://update.nsfocus.com/update/listIps

◆ 入侵检测系统（IDS）

http://update.nsfocus.com/update/listIds

◆ 下一代防火墙系统（NF）

http://update.nsfocus.com/update/listNf

◆ Web应用防护系统（WAF）

http://update.nsfocus.com/update/wafIndex

通过上述链接，升级至最新版本即可进行防护！

◆ 绿盟科技服务方案

绿盟科技提供专业的安全技术服务，全方位的保障客户应用系统安全，避免受此漏洞影响。

◆ 短期服务：我们可以提供应急服务，服务内容包括对客户应用系统有针对性的提供修复建议，保障客户系统的安全升级。

◆ 中长期服务：结合绿盟科技检测与防护产品，提供7*24的安全运营服务，在客户应用系统遭到安全威胁时第一时间通知客户，并定期进行安全检测，针对安全风险提供专业的解决方案。

技术分析

漏洞简介

Apache Struts2.3.x系列版本中struts2-struts1-plugin存在远程代码执行漏洞，进而导致任意代码执行。

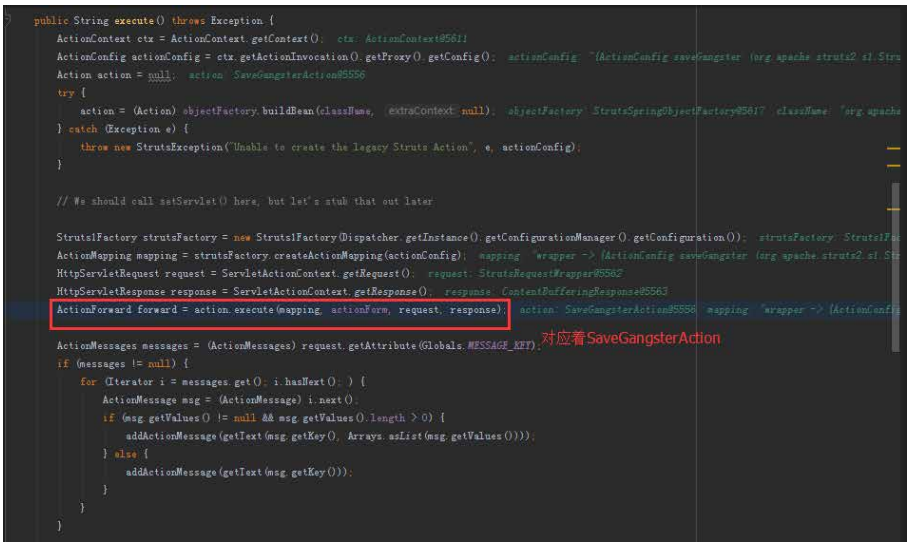
漏洞分析

官方的漏洞描述如下：

> **Problem**
>
> It is possible to perform a RCE attack with a malicious field value when using the Struts 2 Struts 1 plugin and it's a Struts 1 action and the value is a part of a message presented to the user, i.e. when using untrusted input as a part of the error message in the `ActionMessage` class.

从官方的漏洞描述可以知道，这个漏洞本质上是在struts2-struts1-plugin这个jar包上。这个库是将struts1的action封装成struts2的action以便在strut2上使用。本质问题出在struts2-struts1-plugin包Struts1Action.java文件中，Struts1Action类中的execute方法调用了getText函数，这个函数会执行ognl表达式，更为严重的是getText的输入内容是攻击者可控的。以下会基于struts2的官方示例进行分析。

Struts1Action的execute方法代码如下，从红框中信息可以看出其实质是调用SaveGangsterAction.execute方法，然后再调用getText(msg.getKey()….)。



在struts2-showcase的integration模块下有SaveGangsterAction类的execute方法（位于SaveGangsterAction.java文件）用于实现。具体如下：

```
@Override
public ActionForward execute(ActionMapping mapping, ActionForm form, HttpServletRequest request, HttpServletResponse response) throws Exception {

    // Some code to save the gangster to the db as necessary
    GangsterForm gform = (GangsterForm) form;
    ActionMessages messages = new ActionMessages();
    messages.add( property: "msg", new ActionMessage( key: "Gangster " + gform.getName() + " added successfully"));
    addMessages(request, messages);

    return mapping.findForward( forwardName: "success");
}
```

在这个方法中就带入有毒参数gform.getName()放到了messages结构中，gform.getName()的值是从客户端获取的。

Gangsterform.getName()的实现如下：

```
public String getName() {
    return name;
}
```

这里传入了${1+1}，有毒参数已经带入，就差ognl表达式，继续回到Struts1Action类的execute方法下半部分，有getText()的入口，能清晰看到参数已经被污染，具体如下图：

```
ActionMessages messages = (ActionMessages) request.getAttribute(Globals.MESSAGE_KEY);
if (messages != null) {
    for (Iterator i = messages.get(); i.hasNext(); ) {
        ActionMessage msg = (ActionMessage) i.next();
        if (msg.getValues() != null && msg.getValues().length > 0) {
            addActionMessage(getText(msg.getKey(), Arrays.asList(msg.getValues())));
        } else {
            addActionMessage(getText(msg.getKey()));
        }
    }
}

if (forward instanceof WrapperActionForward || actionConfig.getResults().containsKey(forward.getName())) {
    return forward.getName();
} else {
    throw new StrutsException("Unable to handle action forwards that don't have an associated result", actionConfig);
}
}
```

${1+1}被带入

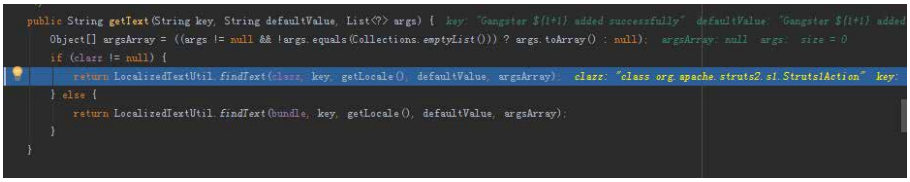
下面进入getText的实现函数，这个调用栈比较深，首先我们给出栈图：

```
findText:372, LocalizedTextUtil (com.opensymphony.xwork2.util), LocalizedTextUtil.java
getText:208, TextProviderSupport (com.opensymphony.xwork2), TextProviderSupport.java
getText:123, TextProviderSupport (com.opensymphony.xwork2), TextProviderSupport.java
getText:103, ActionSupport (com.opensymphony.xwork2), ActionSupport.java
execute:108, Struts1Action (org.apache.struts2.s1), Struts1Action.java
```

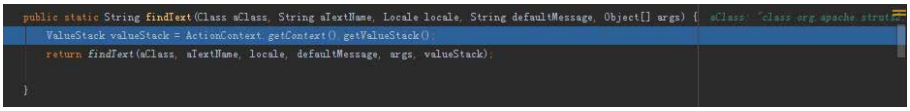
从Struts1action.execute函数开始，到ActionSupport的getText()方法，方法如下：

```
public String getText(String aTextName) {
    return getTextProvider().getText(aTextName);
}
```

进入TextProviderSuppport.getText，调用其另一个重载类方法getText(),示例如下：



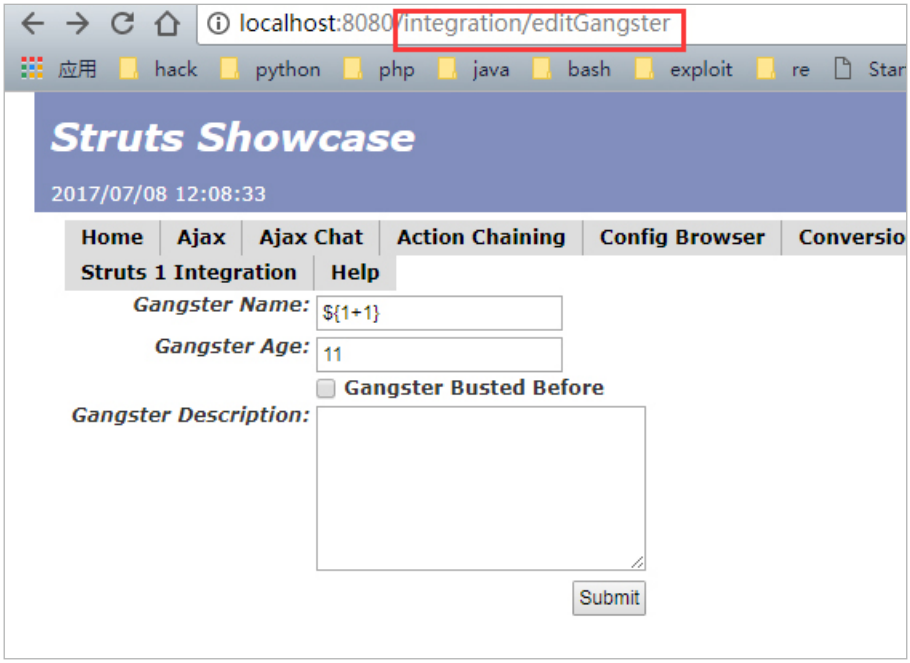
进入LocalizeTextUtil.findText，继续分析其实现：从名字上也能看出其是根据用户的配置做一些本地化的操作。代码如下：

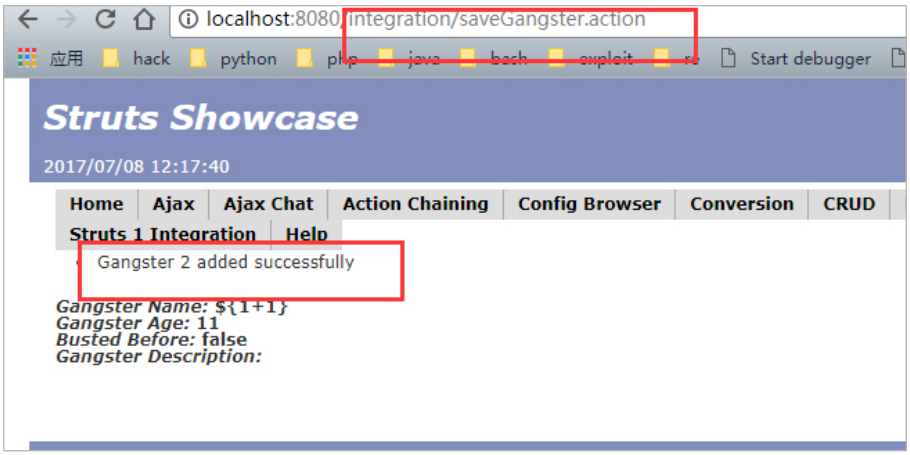


到这里就能发现这就是一个很典型的ognl表达式入口，先是得到一个valueStack，再继续递归得到ognl表达式的值。官方参考链接：

https://struts.apache.org/maven/struts2-core/apidocs/com/opensymphony/xwork2/util/LocalizedTextUtil.html

最后附上一个简单的测试用例图：





声 明

TP-LINK WR841N V8 Router 代码执行漏洞 安全威胁通告

发布时间：2017 年 6 月 21 日

综述

近日，IoT安全公司Senrio 披露了存在于TP-LINK WR841N V8版本的路由器的2个安全漏洞，成功利用漏洞可以使得攻击者在该路由器上执行任意代码。据Senrio的研究人员表示，该型号的路由器的配置服务（configuration service）存在一个逻辑漏洞（CVE-2017-9466），攻击者可以绕过访问限制来重置路由器的验证信息（密码等）。在利用该漏洞获得更高权限后，攻击者可以再次利用一个配置服务里存在的栈溢出漏洞来执行代码。针对本次安全问题，TP-LINK官方已经发布了相关的固件升级补丁，用户可以升级来防护该漏洞。

参考链接：

http://blog.senr.io/blog/cve-2017-9466-why-is-my-router-blinking-morse-code

http://www.ibtimes.com/router-vulnerability-tp-link-issues-patch-fix-remote-code-execution-exploit-old-2555113

https://threatpost.com/tp-link-fixes-code-execution-vulnerability-in-end-of-life-routers/126416/

受影响的版本

☐ TP-LINK WR841N V8 路由器（以及更早的固件版本）

不受影响的版本

☐ 其他版本不受影响

规避方案

TP-LINK已经不再支持该型号的硬件产品，但是也发布了相关的固件升级补丁并且去除了存在漏洞的服务，仍在使用WR841N V8版本产品的用户应该及时下载更新固件版本来防护该漏洞，下载链接:

http://service.tp-link.com.cn/list_download_software_1_0_222.html

更多关于此路由器的信息，请参考：

http://www.tp-link.com.cn/product_222.html

多家企业感染 MBR 勒索病毒威胁预警通告

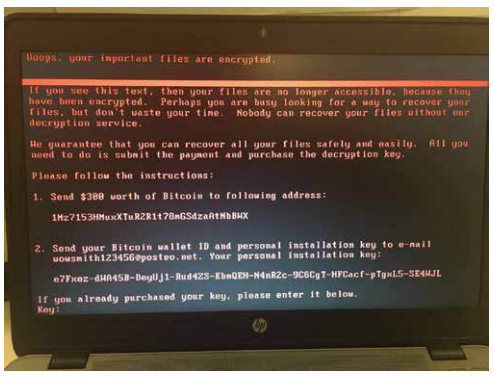
发布时间：2017 年 6 月 27 日

综述

北京时间6月27日，据国外社交媒体消息，乌克兰、俄罗斯两国的政府机构、机场、银行以及多家大型工业企业部分计算机系统遭受勒索病毒威胁，导致主机无法正常引导开机，严重影响了国家多个正常业务的运转；同时6月27日晚间，国内部分外企也确认有发现感染同样的勒索病毒。

根据勒索信息判断，该病毒为去年出现的新型勒索Petya的变种，Windows主机感染该病毒后，整个硬盘的MBR将会被覆盖，并导致系统崩溃蓝屏，而当用户重启计算机时，修改后的MBR会阻止Windows正常加载，而显示攻击者的勒索信息，在支付赎金获得解密秘钥前，用户将无法正常启动主机，从而失去文件和计算机的访问权限。

该Petya变种病毒还具备蠕虫传播特征，目前有证据表明其蠕虫功能利用了永恒之蓝（EternalBlue）漏洞，同时结合今年4月份曝出的Office 0day漏洞（CVE-2017-0199），通过恶意RTF文件进行钓鱼攻击，此外结合绿盟科技安全事件响应团队以往对此类病毒的应急处理经验，其往往还会通过多种应用弱口令进行自动化攻击，例如：RDP、WEB中间件、数据库等。



临时防护方案

1. 及时更新终端安全防护软件及Windows安全补丁，重点检查MS17-010补丁安装情况

2. 利用威胁分析系统（TAC）检测通过网页、邮件或文件共享方式试图进入内部网络的恶意软件

3. 及时告知终端用户尽量避免打开未知邮件中的链接或附件，谨慎从网络下载各类可执行程序

微软发布 7 月补丁修复 55 个安全问题
安全威胁通告

发布时间：2017 年 7 月 12 日

综述

微软于周二发布了7月安全更新补丁，修复了55个从简单的欺骗攻击到远程执行代码的安全问题，产品涉及Internet Explorer、Microsoft Edge、Microsoft Windows、Microsoft Office和Microsoft Office Services and Web Apps、.NET Framework、Adobe Flash Player以及 Microsoft Exchange Server。

相关信息如下（红色部分威胁相对比较高）：

产品	CVE ID	CVE 标题
.NET Framework	CVE-2017-8585	.NET 拒绝服务漏洞
Adobe Flash Player	ADV170009	7 月闪存安全更新
ASP .NET	CVE-2017-8582	Https.sys 信息泄露漏洞
HoloLens	CVE-2017-8584	HoloLens 远程执行代码漏洞
Internet Explorer	CVE-2017-8592	Microsoft 浏览器安全功能绕过漏洞
Internet Explorer	CVE-2017-8594	Internet Explorer 内存损坏漏洞
Internet Explorer	CVE-2017-8618	脚本引擎内存损坏漏洞
Kerberos	CVE-2017-8495	Kerberos SNAME 安全功能绕过漏洞
Microsoft Browsers	CVE-2017-8602	微软浏览器欺骗漏洞
Microsoft Edge	CVE-2017-8611	Microsoft Edge 欺骗漏洞
Microsoft Edge	CVE-2017-8596	Microsoft Edge 内存损坏漏洞
Microsoft Edge	CVE-2017-8617	Microsoft Edge 远程执行代码漏洞

产品	CVE ID	CVE 标题
Microsoft Edge	CVE-2017-8599	Microsoft Edge 安全功能绕过漏洞
Microsoft Edge	CVE-2017-8619	脚本引擎内存损坏漏洞
Microsoft Exchange Server	CVE-2017-8621	Microsoft Exchange 打开重定向漏洞
Microsoft Exchange Server	CVE-2017-8560	Microsoft Exchange 跨站脚本漏洞
Microsoft Exchange Server	CVE-2017-8559	Microsoft Exchange 跨站脚本漏洞
Microsoft Graphics Component	CVE-2017-8577	Win32k 提升特权漏洞
Microsoft Graphics Component	CVE-2017-8578	Win32k 提升特权漏洞
Microsoft Graphics Component	CVE-2017-8573	微软图形组件提升特权漏洞
Microsoft Graphics Component	CVE-2017-8574	微软图形组件提升特权漏洞
Microsoft Graphics Component	CVE-2017-8556	微软图形组件提升特权漏洞
Microsoft Graphics Component	CVE-2017-8580	Win32k 提升特权漏洞
Microsoft NTFS	CVE-2017-8587	Windows 资源管理器拒绝服务漏洞
Microsoft Office	CVE-2017-0243	Microsoft Office 远程执行代码漏洞
Microsoft Office	CVE-2017-8502	Microsoft Office 内存损坏漏洞
Microsoft Office	CVE-2017-8501	Microsoft Office 内存损坏漏洞
Microsoft Office	CVE-2017-8570	Microsoft Office 远程执行代码漏洞
Microsoft Office	CVE-2017-8569	SharePoint Server 跨站脚本漏洞
Microsoft PowerShell	CVE-2017-8565	Windows PowerShell 远程执行代码漏洞
Microsoft Scripting Engine	CVE-2017-8610	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8601	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8604	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8598	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8608	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8605	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8606	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8603	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8607	脚本引擎内存损坏漏洞

产品	CVE ID	CVE 标题
Microsoft Scripting Engine	CVE-2017-8609	脚本引擎内存损坏漏洞
Microsoft Scripting Engine	CVE-2017-8595	脚本引擎内存损坏漏洞
Microsoft Windows	CVE-2017-8557	Windows 控制台信息泄露漏洞
Microsoft Windows	CVE-2017-8566	Windows IME 提升特权漏洞
Microsoft Windows	CVE-2017-0170	Windows 性能监视器信息泄露漏洞
Microsoft Windows	CVE-2017-8590	Windows CLFS 提升特权漏洞
Microsoft Windows	CVE-2017-8562	Windows ALPC 特权提升漏洞
Microsoft Windows	CVE-2017-8589	Windows 搜索远程执行代码漏洞
Microsoft Windows	CVE-2017-8563	Windows 提升特权漏洞
Microsoft 写字板	CVE-2017-8588	写字板远程执行代码漏洞
Windows 内核	CVE-2017-8564	Windows 内核信息泄露漏洞
Windows 内核	CVE-2017-8561	Windows 内核提升特权漏洞
Windows 内核模式驱动程序	CVE-2017-8486	Win32k 信息泄露漏洞
Windows 内核模式驱动程序	CVE-2017-8467	Win32k 提升特权漏洞
Windows 内核模式驱动程序	CVE-2017-8581	Win32k 提升特权漏洞
Windows Shell	CVE-2017-8463	Windows 资源管理器远程执行代码漏洞

受影响的状况

见附件部分。

修复建议

微软官方已经发布更新补丁，请及时进行补丁更新。

NSFOCUS

产品动态

绿盟科技产品更新提示

1.1 Web应用防火墙规则库更新

Web 规则库最新版本	规则更新
6.0.6.0.36741	新增规则： 服务器漏洞防护 27526148 apache_http2_dos 防护 apache mod_http2 模块引用空指针漏洞 27004856 struts2_struts1_remote_code_exec 防护 struts2-struts1 插件远程代码执行漏洞
	修改更新规则： 1. 跨站脚本防护 19136534 xss_dom_event 规则优化 19136545 xss_specific_function 规则优化 2. 服务器插件防护 27526124 lighttpd_contentLength_overflow 界面展示优化

1.2 网络入侵防御/检测系统规则库更新

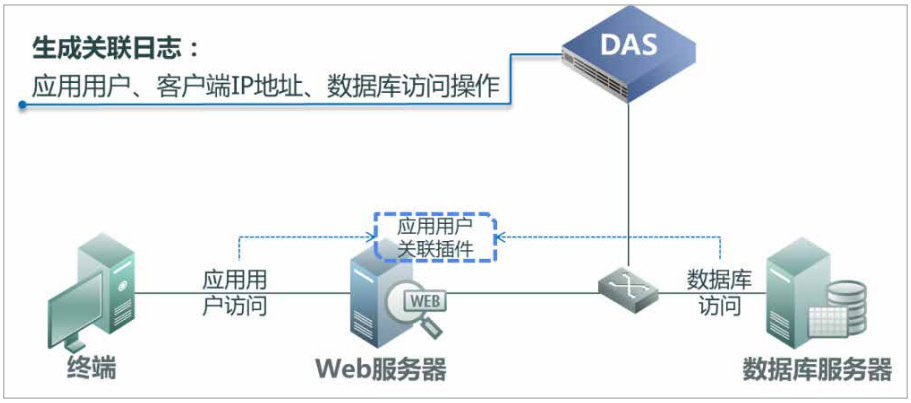
网络入侵防御 / 检测规则库最新版本	规则更新
5.6.10.16295	新增规则： 攻击 [24075]:Disk Pulse Enterprise Server HttpParser 缓冲区溢出漏洞 攻击 [24076]:MailStore Server search-result Reflected 跨站脚本漏洞 攻击 [24077]:McAfee ePolicy Orchestrator SQL 注入漏洞 攻击 [24078]:Microsoft Edge 远程内存破坏漏洞 (CVE-2017-8605) 攻击 [24079]:Microsoft Edge 远程代码执行漏洞（CVE-2017-8619） 攻击 [24080]:Microsoft Edge 远程代码执行漏洞 (CVE-2017-8617) 攻击 [24081]:Aerospike 数据库服务器 IndexName 栈缓冲区溢出漏洞
	修改更新规则： 攻击 [20926]:Samba MS-RPC 远程 Shell 命令注入执行攻击 攻击 [10453]:Apache HTTP Server mod_http2 空指针间接引用漏洞 (CVE-2017-7659) 攻击 [41351]:HTTP URL 目录插入规避尝试

绿盟数据库审计系统实现准确的应用用户关联审计

绝大多数用户环境中的数据库服务器均为三层部署环境，即客户端-Web服务器-数据库服务器，终端用户通过Web服务器实现对数据库的访问操作。传统的数据库审计产品只能通过时间戳等信息来关联前端的Web访问和后端的数据库请求，在并发量较大的情况下关联的准确率直线下降。

绿盟科技数据库审计系统是国内首个做到100%准确关联应用用户的同类产品。

绿盟科技数据库审计系统通过对前端应用访问和后端数据库操作请求进行多层业务关联审计，实现访问者信息的完全追溯，包括发起操作的应用用户、URL、客户端的IP、请求报文等信息，精确地定位事件发生前后所有层面的访问及操作请求，使得追责、问责到人成为现实，真正做到数据库操作行为可监控、违规操作可追溯。



应用用户关联示意图

绿盟科技数据库审计系统提供的关联方法，避免了传统数据库审计产品关联中基于时间匹配所造成的大量错审现象，使应用用户与SQL语句实现实时、准确关联；也使针对应用用户危险行为描述、审计和实时告警成为可能。

会话ID	客户端IP	数据库用户	工具和应用	操作系统用户	黑白名单	风险级别	应用用户
6439	192.168.1.245	BENCHMARK	JDBC THIN CLIENT	Administrator			joe
UPDATE PERFORMANCE_C SET BALANCE=:BALANCE,SECURITYCODE=:SECURITYCODE,DATEFIELD=TO_DATE(:DATEFIELD,'YY							
6439	192.168.1.245	BENCHMARK	JDBC THIN CLIENT	Administrator			joe
INSERT INTO PERFORMANCE_C(PID,PERSIONID,DATEFIELD,NAME,ACCOUNT,BALANCE,SECURITYCODE)VALUES(:PID,:PERSIC							
6439	192.168.1.245	BENCHMARK	JDBC THIN CLIENT	Administrator			mark
DELETE FROM PERFORMANCE_C WHERE PID=:PID							

应用用户关联审计日志

漏洞扫描报告自动化生成

系统漏洞扫描和配置基线核查作为一项基础的安全风险评估技术措施，需要定期和不定期的开展，而每次开展评估工作后往往需要导出风险评估报告进行保存，通常我们需要等待任务完成后再次登录设备进行报表导出工作。

绿盟远程安全评估系统RSAS、安全配置核查系统BVS、Web应用漏洞扫描系统均具备报告自动生成、自动上传FTP服务器、自动通过邮件发送报表，可大大减少用户手动导报表的工作量。

下面我们就详细介绍一下如何实现报表自动生成、自动上传FTP服务器、自动通过邮件发送报表的使用技巧。

在实现报表自动上传FTP服务器、自动通过邮件发送报表前需进行FTP服务器和邮件服务器的配置，详细配置如下。

3.1 FTP服务器配置

将报表备份到FTP服务器功能的实现是以正确配置FTP服务器为前提的。配置FTP服务器的操作如下所示：

选择菜单系统管理 > 配置 > 任务配置，进入任务配置页面，“报表FTP设置”区域如图所示。

配置FTP服务器参数，参数说明如表所示。

配置项	描述
FTP 服务器地址	FTP 备份服务器的 IP 地址。服务器地址可以是 IP 地址（支持 IPV4 和 IPV6），也可以是域名。
FTP 服务器编码	FTP 服务器存储报表的编码方式。
路径	将日志信息备份到 FTP 服务器的哪个目录下。根目录使用“/”表示。
用户名 / 密码	登录 FTP 服务器的用户名及其密码。该帐号必须具有读写权限。

参数配置完成后，单击【确定】按钮，使配置生效。

3.2 邮件服务器配置

使用邮件服务器自动发送报表依赖于正确配置报表邮件服务器，下面介绍配置报表邮件服务器的具体方法。

步骤一 选择菜单 系统管理 > 配置 > 任务配置，进入任务配置页面，“邮件服务器设置”区域如图所示。

步骤二 设置邮件服务器参数，参数说明如表所示。

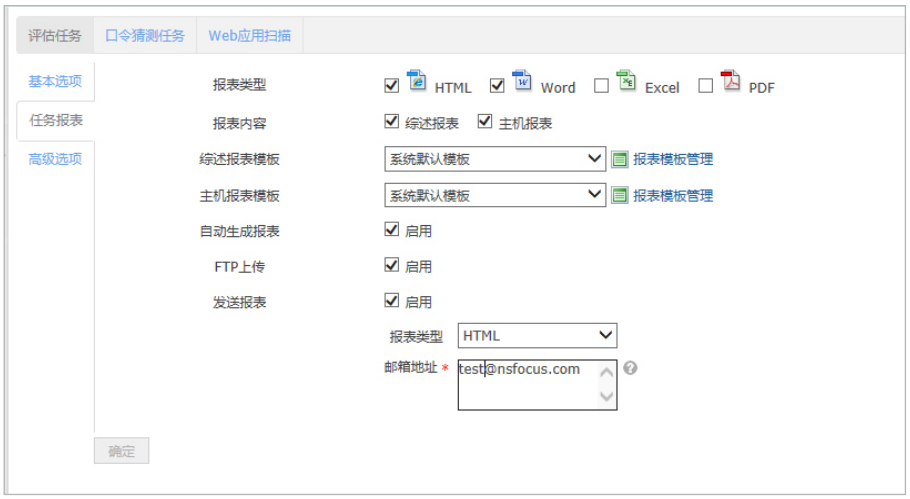
参数	说明
认证方式	登录邮件服务器的认证方式。
邮件服务器地址	邮件服务器的 IP 地址。地址可以是 IP 地址（支持 IPV4 和 IPV6），也可以是域名。
端口	邮件服务器用于发送邮件的端口。
邮箱帐号	用户登录邮件服务器的邮箱。
密码	用户登录邮件服务器的邮箱密码。

步骤三 单击【确定】按钮，配置立即生效。

3.3 报表自动生成、上传FTP、邮件发送

用户在使用绿盟远程安全评估系统RSAS、绿盟安全配置核查系统BVS、绿盟Web应用漏洞扫描系统WVSS建立评估任务时可配置任务报表参数实现自动生成报表、自动上传报表到FTP服务器、自动发送报表到指定邮箱。

详细配置如下图所示：



配置参数如下表所示：

参数	描述
报表类型	支持 html、word、excel、pdf 格式。
报表内容	综述报表：从整体上对评估任务进行综合分析、风险描述和分类展示，并根据不同视角出具漏洞统计图表、操作系统分布、帐号信息和评估标准等。 主机报表：针对单个主机进行风险分析和详细描述。包括单个主机的扫描数据的统计信息、各种 Profile 信息、漏洞列表与解决方案等。若需要分析扫描任务中出现的问题，请生成主机报表。
自动生成报表	启用：扫描任务结束后将自动生成离线报表。可进入报表列表查看输出离线报表的进度，待报表输出完成后，可下载离线报表到本地查看。 不启用：扫描任务结束后，可以在任务列表中查看该任务的相关报表信息。
FTP 上传	只有启用“自动生成报表”参数后，才可以配置该参数。 启用：扫描任务完成后，自动将离线报表上传到指定的报表 FTP 服务器。此时需要配置报表 FTP 服务器，具体操作请参见 FTP 服务器设置。
发送报表	只有启用“自动生成报表”参数后，才可以配置该参数。 启用：扫描任务完成后，自动向指定的电子邮箱发送离线报表，此时需要配置邮件服务器，具体操作请参见邮件服务器设置。 报表类型：报表的文件格式。 邮箱地址：接收报表的电子邮箱地址。

绿盟邮件高级威胁解决方案

轻松应对APT攻击、勒索病毒攻击等高级邮件威胁

邮件高级威胁净化器

全面 | 精确 | 及时

适配通用邮件网关，
隔离APT攻击邮件，
未知勒索软件等高级威胁

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

安全月刊

绿盟科技金融事业部

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

欢迎您扫描目录页左下角二维码，关注绿盟科技、绿盟科技金融事业部官方微信。

月刊电子版下载：http://www.nsfocus.com.cn/research/list_145_145.html