|  |
| --- |
| **基金会logo.jpg** |
|  |
| **保险行业信息安全风险研究** |
|  |
|  |
| 北京保研公益基金会 |
| 二〇一八年十二月 |

## 内容摘要

党的十八大以来，我国一直重视网络安全和信息化工作，作出一系列重大决策、提出一系列重大举措，形成了网络强国战略思想，推动我国网信事业取得历史性成就。从2014年中央成立网络安全和信息化领导小组，习近平总书记亲自担任组长，到2015年专门制定“互联网+”战略，再到2016年习近平总书记提出“要以信息化推进国家治理体系和治理能力现代化”……我们前进的脚步始终未停歇。

然而信息技术也是一把“双刃剑”。信息技术正悄然改变着世界，随之相伴的是风险在变异中演进。因此，我们在研究科技创新时，一定要高度重视它所带来的风险。我们一方面要迎头赶上，努力把握机遇，一方面也要防范风险，理性面对挑战。

作为风险管理行业，保险业与新科技的融合更走在时代的前端。作为与信息、数据有着天然联系的保险业，技术的发展颠覆了风险的诸多规律，给保险业带来了巨大的影响。

本文在信息安全理论研究的基础上，全面分析我国保险业的信息安全风险，提出了针对性风险防范建议，并重点解析保险业的信息安全风险评估以及渗透测试的技术要点，以期提升行业的信息安全意识，并为我国保险业未来的信息安全风险防范提供具体的、可操作的防护措施。

目 录

[一、背景与意义 1](#_Toc532983506)

[1.1 信息化浪潮下，保险业数字化转型成必然趋势 1](#_Toc532983507)

[1.2 新技术下，风险管理成为首要逻辑 2](#_Toc532983508)

[1.3 保险业信息安全不容忽视 6](#_Toc532983509)

[二、信息安全理论研究 8](#_Toc532983510)

[2.1 信息安全的概念 8](#_Toc532983511)

[2.2 信息安全的作用与意义 8](#_Toc532983512)

[2.3 我国信息安全行业发展现状 9](#_Toc532983513)

[2.4 信息安全威胁 10](#_Toc532983514)

[三、保险业的信息安全风险 17](#_Toc532983515)

[3.1 用户认证风险 18](#_Toc532983516)

[3.2 保险客户账户风险 18](#_Toc532983517)

[3.3 电子单证风险 20](#_Toc532983518)

[3.4 “非工作”时空风险 20](#_Toc532983519)

[3.5 外网服务风险 21](#_Toc532983520)

[3.6 技术架构风险 21](#_Toc532983521)

[3.7 自动化作业风险 22](#_Toc532983522)

[3.8 外部合作风险 22](#_Toc532983523)

[3.9 数据资产风险 23](#_Toc532983524)

[3.10 数字化互联互通风险 23](#_Toc532983525)

[四、保险业信息安全风险防范 24](#_Toc532983526)

[4.1 个人统一账户管理 24](#_Toc532983527)

[4.2 采取针对性策略应对不同类型风险 25](#_Toc532983528)

[4.3 数字化生态下的风险管控体系思考 27](#_Toc532983529)

[4.4 保险业的信息安全风险评估 28](#_Toc532983530)

[4.5 渗透测试 35](#_Toc532983531)

[附件1：字段与工具说明 56](#_Toc532983532)

[1. 包含”user””的表、字段 56](#_Toc532983533)

[2. 包含”pass”的表、字段 56](#_Toc532983534)

[3. 表tcic\_account的所有字段 56](#_Toc532983535)

[4. 查询表tcic\_account的所有用户密码内容 56](#_Toc532983536)

[5. 读取/etc/passwd文件 57](#_Toc532983537)

[6. 读取/local/htdocs/back/publish\_add.php文件 57](#_Toc532983538)

[7. 读取/local/htdocs/config/dbconf.php文件 57](#_Toc532983539)

[8. 尝试web根目录写入文件 57](#_Toc532983540)

[9. 可能用到的工具 57](#_Toc532983541)

[附件2：漏洞说明 58](#_Toc532983542)

[1. SQL注入漏洞 58](#_Toc532983543)

[2. 物理路径暴露漏洞 60](#_Toc532983544)

[3. 后台登陆绕过（实际上也是SQL注入） 61](#_Toc532983545)

[4. 任意文件上传漏洞 62](#_Toc532983546)

[5. 跨站脚本执行（XSS）漏洞 64](#_Toc532983547)

## 一、背景与意义

### 1.1 信息化浪潮下，保险业数字化转型成必然趋势

《“十三五”国家信息化规划》（以下简称“规划”）中指出， “十三五”时期是全面建成小康社会的决胜阶段，是信息通信技术变革实现新突破的发轫阶段，是数字红利充分释放的扩展阶段。信息化代表新的生产力和新的发展方向，已经成为引领创新和驱动转型的先导力量。

“规划”预测。物联网、云计算、大数据、人工智能、机器深度学习、区块链、生物基因工程等新技术驱动网络空间从人人互联向万物互联演进，数字化、网络化、智能化服务将无处不在。

“规划”明确。到2020年，“数字中国”建设将取得显著成效，信息化发展水平大幅跃升，信息化能力跻身国际前列，具有国际竞争力、安全可控的信息产业生态体系基本建立。

习近平总书记在中央网络安全和信息化领导小组第一次会议上强调，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。

2018年4月20日，全国网络安全和信息化工作会议召开，习近平总书记强调，信息化为中华民族带来了千载难逢的机遇。我们必须敏锐抓住信息化发展的历史机遇，加强网上正面宣传，维护网络安全，推动信息领域核心技术突破，发挥信息化对经济社会发展的引领作用，加强网信领域军民融合，主动参与网络空间国际治理进程，自主创新推进网络强国建设，为决胜全面建成小康社会、夺取新时代中国特色社会主义伟大胜利、实现中华民族伟大复兴的中国梦作出新的贡献。

面对信息化大潮，保险行业数字化转型将成为行业可持续发展的关键驱动因素和内生动力。保险行业的数字化转型，将使保险业态、业务模式、服务模式发生根本变化和代际升级。

### 1.2 新技术下，风险管理成为首要逻辑

#### 1.2.1 科技发展对保险业影响尤为巨大

当代科学技术的发展已经使人们获取信息、处理信息、验证信息、信息决策、权益保障的过程大大缩短。使更精准、更透明、更公正成为现实。用户对数字化渠道接触愈发密切，信息交换更加频繁透明，从而不断改变保险行业的业务模式和底层逻辑。

新技术不光从商业模式、产品形态、服务方式、运营管理、竞合关系等方面影响着保险的业务流程和运行效率，更从本质上影响着保险的底层逻辑。

首先是风险结构的变化。以往大群体、大类别、同质化的风险，正逐步向高维度、精准化、个性化风险转变。过去的保险，由于数据的维度和精准度不高，更依赖大数法则，需要某一风险下有很大的群体来互相弥补。而随着大数据技术的发展，数据的维度越来越高，精准度越来越强，今后的风险厘定也将是多维的，甚至群体不需要那么大，但风险可以厘定得更清楚。

其次是管理逻辑的变化。以产品为中心转向以客户为中心，账户管理与客户体验成为至上的因素。原来的保险销售和运营是按保单类别进行管理，而行业一直在提出以客户为中心，如果不能实现大数据和客户信息的整合，账户管理和客户体验则很难达到应用水平。依托保险科技，账户管理和客户体验在推动产品创新的同时，也驱动了新一轮的以客户为中心的服务体系和风控体系的再造。

#### 1.2.2 新技术推动经济社会进入高维时代，高维信息成新工具

对于高维概念的理解，物理学家和数学家并不陌生，20世纪90年代霍金提出高维空间理论，又称M理论，指出宇宙是十一维的，由震动的平面构成的。在爱因斯坦看来，宇宙只是四维的（三维空间和一维时间），现代物理学则认为还有七维空间我们看不见。而在处理高维数据时，由于算力、成本等原因，通常会对数据进行降维处理，抽取主要研究信息。在日常生活中，人们除了对三维坐标、时间维度有直观认识外，很少会想象维度的范围，使用维度的概念，而小说《三体》给了普通人关于维度非常具象的表达，使得“降维打击”一词红极一时。在“丛林法则”下，维度成为竞争群体间的打击工具。

新技术发展正使社会进入风险高维化时代。以物联网技术作为说明，物联网是作为依托互联网技术而兴起的新型互联网模式，物联网表现为万物互联，其解构了主体之间的关联节点，使得反应链条上可捕获的信息增多，并以此形成有效反馈，影响风险的进程。物联网在发展中产生了大数据，大数据分析为物联网的发展提供了庞大的信息数据资源，进一步推动了物联网产业的快速发展。

在这一进程中，物联网提供的更加充分的信息，极大地增加了变量的联系逻辑路径，增加了相关世界的维度。以往分析中被忽略的维度信息，在新工具的作用下，被凸显出来。例如，以车险为例，过去的从车数据分析往往以空间维度、时间维度为主，通过物联网、大数据分析等技术的发展和应用，温度维度、声音维度，甚至颜色维度、气味维度等信息都可能被收集并加以利用，从而使信息被刻画为生产链条上的控制工具。

事实上，新技术的发展，更会在安全性、舒适性、感受性、管理性等多维度带来约束和主张的机会。也就是说，技术突破到一定阶段，一项技术的变革，会在多个维度强化甚至缔造诸多因果关系链条上约束和主张的干预逻辑通道。而在当今新技术时代或者称为数据时代、信息时代的今天，这一规律的影响正处于逐步突出的阶段。

物联网、人工智能等技术使得当今世界可供决策的维度急速提升，因而也带来了风险的高维化，经济社会由此将真正进入高维时代。

随之而来，一方面，新技术的发展影响了风险的不确定性、随机性。信息管理维度增加，并对风险进程进行干预，使得风险的随机性随之改变，可能为保险公司带来相关保障成本的巨变。另一方面，大数据带来风险的细分和风险规律的再认识，使得保险业定价基础——大数法则的运用变得比过去困难。风险管理的反应链由过去的风险识别、风险评估、风险处理决策延长为，以智能约束和主张指令、智能干预并反馈为中心的反应链；干预事物发展规律，改变风险进程，升级为风险管理的核心。

#### 1.2.3 新技术推动下，风险发生变异，风险管理工具随之异化

变异是生物学用语,指同种生物后代与前代、同代生物不同个体之间在形体特征、生理特征等方面所表现出来的差别。新技术的发展使得世界处于日新月异的变化中，大数据分析使得认识规律更加清晰，区块链重构信任机制，物联网使得万物互联，人工智能干预事物发展规律，改变风险进程。

新技术对世界的颠覆，导致了风险变异。道路交通风险由马车时代的牲畜风险变异为工业时代的机械故障风险，进而变异为信息时代的信息处理风险。风险变异凸显出科学服务异化，“异化”表示将自己拥有的东西转化成同自己对立的东西。在没有机制约束下，科技的发展可能演变到其初衷的对立面。

科技服务异化，是技术发展进程中不可忽视的问题。在风险处理过程中，就知情权利地位和工具方面，新技术降低了信息不对称；但是就技术服务的利益主体以及技术工具掌握的次第方面，新技术又增加了信息不对称，显著加重了个体对信息工具掌握方面的依赖性。换言之，技术变革的初衷是降低信息不对称和交易成本，但技术黑箱又将绝大部分使用者拒之技术控制门外。掌握信息维度的高低，演化为竞争的焦点。而全球“科技智力”的“分享经济”理想与资本世界大资本阵营垄断愿望冲突巨大，全球精英体系和资本世界的格局发生巨变，原有风险管理工具随之异化。

#### 1.2.4 风险管理逻辑是高维时代的首要逻辑

因此，在高维时代，信息维度的争夺成为新的制高点，高维信息的获得者在社会分工链条中占据了主导权，科技服务出现异化，背离初衷。而如今的信息技术的科技精英，我们暂且称作“科技智力”，挟持以信息科技为中心的新技术的巨大力量时，并不为资本所控制，与原大资本阵营的关系，从被主导阶段，希望几乎要越过唇齿相依、水乳相容阶段，直接到弱相关阶段甚至无关阶段。在面对技术发展的不可控，如何使得技术控制者的利益与社会普遍价值相一致，使科技发展为提高社会福利服务，而不是沦为少数人控制社会、奴役社会大众的工具，使社会堕落为科技“丛林法则”主宰的世界，技术的选择机制与技术道德从未显得像今天这样重要。科技智力本身就需要一定的机制进行约束，至少在一定程度上扬其长避其短。风险管理逻辑，历来是社会治理的重要逻辑，而在新技术时代则成为社会治理的首要逻辑。

### 1.3 保险业信息安全不容忽视

新技术是把“双刃剑”，一方面可以造福社会、造福人民，另一方面也可以被一些人用来危害社会、危害人民。从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。

在2016年4月19日召开的网络安全和信息化工作座谈会上，习近平总书记对互联网管理提出明确要求：“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。‘物理隔离’防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。不出问题则已，一出就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。我们必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。”

2013年11月，党的十八届三中全会通过的《中共中央关于全面深化改革若干重大问题的决定》提出，坚持积极利用、科学发展、依法管理、确保安全的方针，加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全。

　2015年7月，我国《国家安全法》明确将网络空间安全上升至我国国家安全高度，2016年11月，《中华人民共和国网络安全法》（以下简称《网络安全法》）高票通过，成为我国首部网络安全领域的法律。《网络安全法》明确了一系列相关的法律范围、职责和约束，其中第三章“网络运行安全”的第二节明确了重点保障“关键信息基础设施的运行安全”，其中就包括“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域”。保险业作为金融业的重要领域之一，网络与信息安全不容忽视。

## 二、信息安全理论研究

### 2.1 信息安全的概念

信息安全主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。信息安全本身包括的范围很大，其中包括如何防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、消息认证、数据加密等），直至安全系统，如UniNAC、DLP等，只要存在安全漏洞便可以威胁全局安全。信息安全是指信息系统（包括硬件、软件、数据、人、物理环境及其基础设施）受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断，最终实现业务连续性。

### 2.2 信息安全的作用与意义

信息安全的根本目的就是使内部信息不受内部、外部、自然等因素的威胁。为保障信息安全，要求有信息源认证、访问控制，不能有非法软件驻留，不能有未授权的操作等行为。

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。但是，对于不同的部门和行业来说，其对信息安全的要求和重点却是有区别的。

中国的改革开放带来了各方面信息量的急剧增加，并要求大容量、高效率地传输这些信息。为了适应这一形势，通信技术发生了前所未有的爆炸性发展。除有线通信外，短波、超短波、微波、卫星等无线电通信也正在越来越广泛地应用。与此同时，国外敌对势力为了窃取中国的政治、军事、经济、科学技术等方面的秘密信息，运用侦察台、侦察船、侦察机、卫星等手段，形成固定与移动、远距离与近距离、空中与地面相结合的立体侦察网，截取中国通信传输中的信息。

传输信息的方式很多，有局域计算机网、互联网和分布式数据库，有蜂窝式无线、分组交换式无线、卫星电视会议、电子邮件及其它各种传输技术。信息在存储、处理和交换过程中，都存在泄密或被截收、窃听、窜改和伪造的可能性。不难看出，单一的保密措施已很难保证通信和信息的安全，必须综合应用各种保密措施，即通过技术的、管理的、行政的手段，实现信源、信号、信息三个环节的保护，藉以达到秘密信息安全的目的。

### 2.3 我国信息安全行业发展现状

信息安全与技术的关系可以追溯到远古。埃及人在石碑上镌刻了令人费解的象形文字；斯巴达人使用一种称为密码棒的工具传达军事计划，罗马时代的凯撒大帝是加密函的古代将领之一，“凯撒密码”据传是古罗马凯撒大帝用来保护重要军情的加密系统。它 是一种替代密码，通过将字母按顺序推后 3 位起到加密作用，如将字母 A 换作字母 D， 将字母 B 换作字母 E。英国计算机科学之父阿兰·图灵在英国布莱切利庄园帮助破解了 德国海军的 Enigma 密电码，改变了二次世界大战的进程。

中国信息安全行业起步较晚，自本世纪初以来经历了三个重要发展阶段（萌芽、爆发和普及阶段），产业规模逐步扩张，带动了市场对信息安全产品和服务需求的持续增长。另外，政府重视和政策扶持也不断推动中国信息安全产业的快速发展。

但总体上看，我国网络安全的投入水平仍然偏低且不均衡。从权威数字可以看到，2016年全球IT安全市场的规模为755亿美元，而中国仅为43亿美元，全球IT安全占IT市场的比例为3.74%，而中国仅为1.84%，在安全投入上我国还远远不够。另一方面，2016年全球IT安全投入中硬件投入占19.3%，软件投入占36.3%，而服务投入高达44.4%，这三者在中国的比例分别是54.5%、16.7%和28.8%，这既是我们安全投入还不够的结果，也说明我们需要审时度势的改变我们的网络安全观与网络安全策略。

### 2.4 信息安全威胁

#### 2.4.1 攻击者角度：攻击具有极其低的成本

从一个攻击者的角度上看信息安全，其实我们忽略了非常多的内容。2017年5月16日，一款名为“WannaCrypto”又简称“WannaCry”的勒索软件席卷全球，数以十万计的计算机被入侵。他利用了微软Windows操作系统中的文件共享服务的一个高危漏洞，通过程序实现了漏洞的自动利用、自动传播、自动加密所有的文件，实现了一键式全球入侵。

但实际上，在两个月前的3月14日，微软就发布了其官方补丁MS17-010；而且之后的4月，“ShadowBrokers”就在互联网上公布了该漏洞和利用工具，且快速传播，并指明其来源是NSA的攻击工具“EthernalBlue”。那么，在4月到5月期间已经接收到补丁的情况下，为何这10万台机器仍遭到了入侵？

这里存在一个被称为漏洞利用时间的曲线，在公布之前被称为0day漏洞，没有太好的办法去预防。但在漏洞的补丁发布后，大众修复的速度远远低于我们的想象，而这些时间受到的攻击是远远没有必要的，是完全可以预防的，而90%以上的已知网络攻击都是在这个时间段发生的。

还有非常多的漏洞尚未被发现。而且不少漏洞，诸如HeartBleed、STRUTS2、FCKEditor等都具有高危害性和高可利用性，这些漏洞的出现意味着全球信息系统的劫难，毕竟互联网世界的首要特点就是即时性、高速性、无边界性和开放性，一倒塌就是一大片，而且是即刻散播，这也是为什么漏洞是国家战略资源的原因。

但是挖漏洞是个高智商的工作，成本太高。但为何攻击却让人感觉那么简单呢？答案之一就是弱口令，成本低、收效好。弱口令是指诸如12345、qwert的不足8位、没有大小写、没有英文数字结合的口令，太简单了，对于攻击者来说那只是一个简单的字典本，网上随手可下。此外弱口令还包括，根据个人信息、习惯生成的特殊字典本，例如有太多人青睐拼音加生日的方式；还有来自于同一人在别的网站上注册的密码，这个又叫社工库，不同网站同密码的现象人人都有；还有就是我们几乎忽略掉的路由器上，有攻击者不停在监听明文的口令，这就是我们常说的不是https加密，密码就是明文的原因。

这就会有些疑问，路由器存在漏洞被攻击者控制还好理解，我们的个人信息、其他网站上注册的密码，攻击者怎么会知晓？前文所述的WannaCry勒索软件，1天内造成了10万台计算机的瘫痪，既然可以勒索，同样也可以窃取数据。2011年12月21日，某黑客在网上公开了程序员网站CSDN的用户数据库，高达600多万个明文的注册邮箱账号和密码、个人信息遭到曝光和外泄，随即，因相同漏洞模式导致天涯、多玩等网站相继被曝用户数据，这拉开了曝光数据这一种黑客炫耀模式，直至今天依然不停有新数据在网上被曝光并快速传播；2013年7月，STRUTS2漏洞被公开，因其高可利用性和使用广泛，仅仅不到4个小时的时间，京东、淘宝、当当等一大批受众极广的应用都被报道有不同程度的数据泄露。

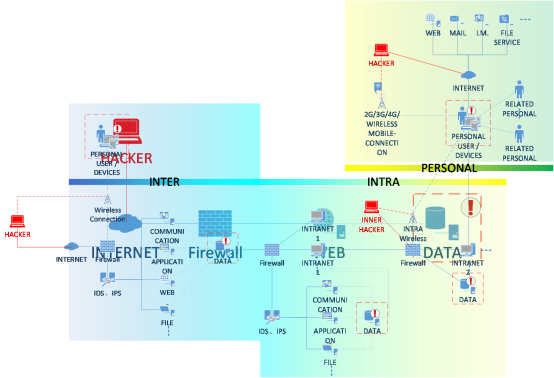
中国信息安全测评中心推出的《年度国家信息安全态势评估》指出，中国目前粗算已有千亿条数据或因漏洞而泄露，几乎覆盖90%以上的网民的相关信息，据估算通过这些泄露数据，中国约60%的网民可被完整勾勒出个人的全部信息和习惯特性，而且上网越多的人，越准确，甚至可以预测行为；更直接的是在用户名和密码上，已有研究表明平均每人最多可以同时记住10个符合高强度的密码，而且70%的人只有约5组不同密码。所以有了这些泄露的信息，即社工库，攻击者随意进出系统，定位诈骗。很多人还在不明所以的追赶大数据这个新名词时，攻击者早就进入了大数据攻击的时代。

我们在网络上访问每一个应用，中间都会经过无数个网络设备。比如从访问百度，就会经过最少9个路由设备，还不包括交换设备。中间如果加了一个攻击节点，几乎没人能够看的出来。但是我们所有的数据都会经过这个节点，被攻击者看一遍内容，这也是美国实施监听的一个主要手段。

这只是网络，我们的WIFI网络、手机因为其无线广播的特性，同样容易实现监听，比如OsmocomBB开源项目和摩托罗拉C118，17元的成本就可以侦听约100m以内2G手机的短信、通话和上网。而信号衰减器可以让3G、4G同范围内信号无察觉的衰减至2G。同样，ExploitDB上也有非常多的Android和苹果手机的开源漏洞，对不升级的手机几乎是一键式入侵。

这些还是违法攻击行为，还有不属于信息安全领域的“个人隐私”问题，服务商合法获取个人数据。安装软件时极少数人真正看过隐私协议，就点击了我同意，但里面明确写着软件会收集你这样那样的信息。

还有非常多的攻击者角度例子，可以颠覆非常多传统安全的认知，例如指纹、人脸识别等等。究其原因，可以用下图来解释（图1）。信息系统是，防火墙、网站、网站数据，攻击者通过互联网实施入侵；但现实是，攻击者的眼中不仅仅是网站，还包括很多应用、使用者，还有与之相连的背后内网、内网的数据、内网的用户，这些更为重要，还包括与之相连的每一个人、每一个个人设备和与其相关的人际网络，入侵者可以在互联网上、也可以在内网、甚至可以直接面向每个个人，而且每个设备都会有20个左右的软件或系统，这些成千上万个点只要有一个突破，很可能就带来着整个系统的坍塌，信息系统不同于人体，免疫这个问题几乎还是个美好的概念，而且攻击程序的运行速度远远超过人的反应，因此如此庞大的系统，想做到安全，岂是一两个设备可以完成的？木桶原理在此完美体现。



**图1：信息环境**

更让攻击者欣慰的是，现在互联网思维深入人心，快节奏、快开发、快上线的做法虽然商业角度成功，占领了市场，但因为太多大脑用在考虑新名词、标题党、资本运作，安全问题肯定会随着浮躁而产生，从近几年对800余个系统渗透测试结果来看，凡是为了急于上线而压缩设计和测试时间的系统，高危漏洞率约覆盖70%，而且这个比例在逐年增加。

再加上攻击工具的开放和免费，这些原因造就了攻击具有极其低的成本。

#### 2.4.2 网络信息泄露案例分析

1）Equifax (NYSE: EFX) 泄露1.43亿美公民信息

2017年9月初，美国最大的个人征信公司Equifax被爆泄露了超过1.43亿条包括社会安全号码在内的美国公民敏感信息。Equifax是一家成立于1899年的百年企业，也是在纽交所上市的公众企业，事发后其主席兼CEO、CIO和CSO相继退休以承担责任。根据事故报告，在从5月13日至7月30日的长达2个半月的时间内，攻击者持续盗取敏感信息，而攻击所利用的ApacheStruts2 S02-045漏洞在3月初就已披露并提供了不受漏洞影响的新版本。

2）德勤泄露逾500万封内部邮件

在上述案例事发仅仅几天后，9月25日，德勤又被爆出泄露了超过500万封内部邮件，时间段是从2016年10月至2017年3月，原因是邮件系统的管理员账户仅使用了密码认证，被攻击者获取，没有采用业界普遍使用的双因素认证。而最近5年，德勤连续被Gartner评为全球第一大（按收入计）安全咨询服务公司，其向全世界的客户提供自身关于网络安全的最佳实践。

3）某数字货币交易平台多币种失窃案件

2017年10月初国内一家数字货币交易平台的包括比特币和莱特币在内的多个数字货币的钱包失窃，损失金额非常巨大。区块链是一个公开的体系，能够持续追踪这些失窃货币的流向。经过一段时间的追查，发现这些货币最终流入了一个国外的交易所。通过沟通，得知一个攻击者注册用的邮箱，基于这个邮箱进行深入挖掘后，在一个交平台上发现了木马的样本，这是一个非常专业的木马，专门用于窃取数字货币的钱包，而且这个样本经过了非常强的免杀处理，在66款杀毒软件中只有5款能够识别它，而且没有一个是国内的杀毒软件。这个木马软件是怎么进入受害者的网络呢？整个攻击事件的起因是在9月13日的下午，有一个运维人员打开百度，搜索了Bitcoin，下载了BTC的软件，被捆绑在其中的木马软件就此激活。

通过这三个案例可以看到，虽然攻击者有非常强的专业性，但从受害者的角度，他的第一步都是溃败在某一个非常小的蚁穴上面。

#### 2.4.3 高频漏洞应对难题

仅以Struts2为例，几年来已披露超过50个漏洞。这对金融机构的网络安全体系造成了极大的冲击。

在应对安全事件的实践中，暴露了两方面的难题：风险信息的及时、全面获取和基于资产的脆弱性闭环管理。一方面，第一时间获取到相关的威胁情报能获得更长的应急时间，但对金融机构来说，威胁情报只能从外部获取；另一方面，清晰的资产库和漏洞处置跟踪流程可以帮助更快的处置漏洞，否则临时、手工的应急处理方式很难跑赢攻击者的速度。

#### 2.4.4 协同漏洞应急处理

传统的堡垒建设模式的网络安全建设已不足以应对现在的安全威胁，多方协同运营的新时代已经来临。以漏洞管理为例，以客户侧部署的脆弱性综合管理平台为核心，从本地脆弱性和外部脆弱性来源获取脆弱性信息，从外部获取威胁情报，并整合内外部的专家力量，将是对网络安全的有力保障。更进一步的，协同运营的模式可以推广至安全事件应急响应和日常安全工作等更多场景，帮助金融机构在日新月异的攻击发展中保证业务的安全、稳定运行。

当然，协同运营模式对金融机构和厂商也提出了新的调整。对金融机构来说，改变对服务的观念，改变预算决策机制及预算结构；将安全运营能力、工具与现有的开发体系整合，实现高效自动化安全开发和运维；以及监管合规的限制都是需要破解的难题。对厂商而言，从单点技术产品转化为解决方案，从产品交付到能力交付；积累安全能力，提升对抗水平和速度；建设有效的协同运营体系也是亟待提高的能力。

## 三、保险业的信息安全风险

保险客户旅程，涵盖保险用户注册认证、保险账户设立、保险服务凭证取得、保险服务的时间和空间、支撑保险服务基础设施和基础平台、体现保险服务成果的数据以及保险行业与其他行业互连互通等多个方面。在数字化生态下，其风险表现形式和风险驱动因子，均与传统保险模式有明显不同，其应对策略也必须与时俱进，适应数据字化生态环境。

### 3.1 用户认证风险

传统的用户认证依托营业场所、实物凭证和面对面的服务方式，具有高自主可控的特性，仿冒作假的可能性较低。在数字化生态环境下，网上非现场、非实物原始凭证、非面对面的方式，使用户身份识别难度显著提高。

“在互联网上，没人知道你是一条狗”。身份认证机制不完善，导致身份错配，导致投保人、被保人真实性得不到保障，与保险“最大诚信”原则背道而驰，从而引发销售误导、理赔难、理赔欺诈等风险。

“互联网上，他们都知道你是条狗”。身份认证机制不规范、不安全，分散式、碎片化、无最低安全标准，导致身份泄漏，投保人、被保人的隐私得不到保护，从而引发电信和网络诈骗等风险。

### 3.2 保险客户账户风险

传统的保险账户按保单管理，基于保单等物理凭证处理本保单项下的保险服务。在事实上没有建立起以客户为中心的保险账户的基础上，开展基于实物凭证的保险服务，尽管保险消费者感到不便，但能基本保障交易的安全性。

在数字化生态环境下，一个保险消费者多张保单、多个产品，现有以保单为中心的系统平台，未能实现多张保单、多个产品有效整合，导致线上服务不仅繁琐，而且无法保证多张保单、多个产品归集至统一客户账户下的准确性，更不能打通保险承保、理赔、给付等在一个账户下协同处理，也不能将道路救援等保险增值服务以及保险服务延伸而来的其他金融和社会服务协同处理。使客户保险账户难以保障完整性、一致性、准确性。

保险客户账户缺失或缺乏完整性、一致性、准确性管理，不仅造成客户体验不佳，而且易引发保费、保额、保险责任计量不准、定价偏差、服务差错、理赔差错等风险，也易引发反洗钱管理不到位风险和舞弊风险。

从整个行业看，不同保险机构间的客户，在行业层面缺乏保险客户统一账户，不仅存在上述风险，还存在客户在保险机构间逆选择等风险。

客户身份认证的核心是真实，客户保险账户的核心是支付，两者管理不到位，贯穿于保险服务全流程的诚信风险就通过销量误导、理赔难、舞弊欺诈等乱象体现出来，穿透式诚信、穿透式服务、穿透式监督难以得到根本保障。

### 3.3 电子单证风险

传统的保险作业模式以实物原始单证为依据进行单证流转，其中关键是保单。保险公司的作业风险控制是围绕保单这一关键实物凭证而设计的。承保后签发保单，退保、给付期满时收回保单。由于实物单证具有不可再生和不可原样复制性，通过“收回保单”，或在实物单证上加盖变更签注，确保了客户不可能二次持证进行索赔、给付，从而保证了风险的可控性。

在数字化生态环境下，所有业务单证，包括保单也进行了电子化。由于电子保单供下载后，客户可无限制地进行原样复制，因此，一方面在发生退保、满期给付等情况下，无法全部收回电子保单；另一方面，在保单发生变更时，无法在客户持有的电子保单上加盖相关签注，无法保证客户凭电子保单二次索赔、二次给付的诉求，从而使保险公司要自我举证前次作业的准确性且没有发生差错而拒绝二次索赔、二次给付变更就十分困难。

另外，电子单证一旦因保险人内部差错而分发至投保人、被保险人时，将难以收回电子保单，即使要求对方回收清理，也无技术手段可以保证对方清理时没有数据残留。

### 3.4 “非工作”时空风险

传统的保险作业模式通常在工作时间、工作场所内完成，保险人、投保人、被保人、监管机构、行业机构等保险利益相关方均配置有效资源，满足各方需求，出现突发事件，应对能力也较充足。

在数字化生态环境下，保险作业模式从5\*8小时的工作时间，更多地转向非工作时间，升级为7\*24小时不间断运营，特别是在节假日和重大活动期间，保险服务需求更加活跃，线上服务需求转化线下现场服务的要求更加强烈。“非工作”时空风险表现在三个方面：一是存在非工作时间服务资源配置不到位风险；二是非工作时间线上服务稳定性风险；三是非工作时间从线上服务转化为线下现场服务响应能力风险。

### 3.5 外网服务风险

传统的保险作业模式通常由保险公司内部员工和代理人在公司内网运用相关信息系统完成保险日常作业。内部网络和内部员工为保险公司风险防范构筑了一道“长城”，客户需求通过员工、代理人“代办”而满足。因此，风险管控聚焦于“城内”安全即可基本满足需要。

在数字化生态环境下，客户自服务是大势所趋，将成为主要服务渠道，代理人和员工进化为保险专家顾问。客户自服务必然导致客户自服务APP等自服务工具突破内网保护，走向互联网开放环境。而互联网环境下，防攻、防断、防改、防漏、防毒的风险始终存在，而且成为主要风险。

### 3.6 技术架构风险

传统保险信息系统服务对象是内部员工、代理人和外部合作机构的员工，用户数一般是十万或百万量级，采用传统的单一数据库集中式部署架构能较好满足集约化、一致性和安全性要求。

在数字化生态环境下， 保险信息系统服务对象是客户和外部合作机构的客户，用户数达到千万级、亿级甚至十亿级。传统的单一数据库集中式部署架构将导致严重的运行性能风险、容量风险和运维时间窗口风险，无法提供快速、稳定、持续不断的运行服务。

### 3.7 自动化作业风险

传统保险信息系统的时效要求相对较低，批处理自动化作业通常为T+1模式，作业人员有相对宽裕的时间窗口来抽检批处理产生的批量结果，发现问题可及时纠正。

在数字化生态环境下，业务批处理自动化作业进一步提速，走向实时化。此时如果产生批处理差错，可能造成影响巨大的“乌龙指”风险，将对客户、公司甚至行业造成难以弥补的声誉风险。

在数字化生态环境下，云计算技术使IT运维工作自动化，也可能造成大批量系统差错和停机，从而造成巨大的业务连续性和声誉风险。

### 3.8 外部合作风险

传统保险服务模式下，对外合作通常依托实物单证和系统对接，外部合作风险要传导至保险机构内部，有较复杂的业务流程和业务单证控制。

在数字化生态环境下， 对外合作主要依电子单证和数据对接，外部合作风险传导速度快，关联性风险控制成为新课题。如合作方私自制作电子单证、业务不符合规范、数据对接不完整不一致，合作方信息安全控制失效等风险极易传导到保险业内部。

### 3.9 数据资产风险

传统保险服务模式下，保险公司通常自建和租赁自主可控的数据中心，并将信息系统与数据部署于自主可控的数据中心内，数据资产的拥有与保全得到基本保障。

在数字化生态环境下， 公有云服务机构天然存在引导保险机构利用公有云服务的动力，围猎中小保险公司和大公司部分业务入云将成为新的挑战。一旦保险机构选择公有云服务，保险公司的数据资产拥有与保全将面临无技术手段加以保障的风险。利用公有云服务的法律风险、数据风险、责任风险、声誉风险等成为新课题。特别是在公有云服务商的生命周期短于保险公司生命周期时，或在公有云服务商因故变更和终止服务时，这一风险将更加突出。

### 3.10 数字化互联互通风险

传统信息化模式下，尽管信息系统和共享平台规模有大有小，但系统与系统、系统与平台、平台与平台间关联性不强，从结构上抑制了风险快速传导。

在数字化生态环境下，保险机构信息系统、共享平台本身越来越庞大，系统与系统、系统与平台、平台与平台、保险系统与第三方系统和平台之间的联通性越来越紧密，数据交换也越来越频繁。处于基础地位或关键节点的核心系统、共享平台、第三方平台，一旦出现风险，可能波及全行业的安全风险。

## 四、保险业信息安全风险防范

新业态、新模式、新技术，使保险行业的风险动因、风险识别和风险防范带来全新的挑战，“安全可控”成为“数字保险”转型升级的必然要求，需要建立保险数字生态环境下的新型风险防范体系。

防范数字化风险，需要有新业态、新模式相匹配的风险防范机制与策略，同时也要充分利用新技术，研发新工具，有效识别和处置风险。

### 4.1 个人统一账户管理

在金融市场上，对重要的金融单证从源头开始控制，用科技手段管理市场和控制风险，是金融业的稳健发展不可或缺的方法。目前，我国保险市场的监管仍以保单为中心，存在信息不对称、客户识别手段匮乏、数据缺失等问题。可行的解决方法是，建立以保险统一帐户为核心的统一信息共享平台，集中登记并监管保险公司与保单持有人之间的责任关系和权益事实，将原有的固化的纸质保单逐步转化为电子保单，并为每位保单持有人开立单独的保险统一账户，以统一帐户为主键，汇集每一帐户关联的全部保单信息，实现在保单电子化签发过程中，保单将自动存入保单持有人的电子保险账户下。通过保险统一帐户的建立，一是可以实现全行业各公司关键数据的统一归集，二是实现个人帐户下财险、寿险等各险种信息的统一管理，三是实现信息流、资金流、服务流的统一渠道，并通过建立以保险统一帐户为核心的统一信息共享平台推动中国保险监管由以保单为中心向以账户为中心转移。

信息技术、大数据、云计算、人工智能等科学技术的不断进步和飞跃，为我国保单集中登记制度的推行以及全民保险统一账户的建立提供了有力的技术支撑。而这一重大举措得以实施对规范保险市场秩序、重构诚信基础、提升风险管控能力均具有重要意义。

建设以保险统一帐户为核心的统一信息共享平台是我国保险行业电子业务建设与发展的关键一步，是数据统一归集和智能分析的基础工程，是实现监管多维分析的重要举措，是以大数据应用促进保险行业服务社会经济发展、构筑民生保障的关键一步。

### 4.2 采取针对性策略应对不同类型风险

建设并完善保险统一账户信息管理平台，加强行业基础设施建设，是应对用户认证、账户以及电子单证风险的有力措施。

应对“非工作”时空风险，则需要统筹网上网下两个空间，统筹工作与非工作两个时空，做好网上网下、工作与工作时空资源配置协同。推进信息化基础设施“多中心多活”结构化布局，保障信息系统稳定、不间断运行；应对外网服务风险。强化信息安全保障体系，做好“防攻、防断、防改、防漏、防毒”的五防工作。

应对技术架构风险，需要推进信息系统分布式架构升级，加快推进分布式计算、分布式存储、分布式数据库、分布式核心系统的升级换代等。

应对自动化作业风险，则需要对资金收付、电子保单签发、电子发票生成的“快风险”和致命风险，在难以依赖人工校验的情况下，实施“双工校验”机制。利用数据可复制这一特性，采用2个独立团队分别开发相同业务需求的应用软件，将两个分别独立开发的应用软件所产的结果进行逐条自动比对，结果一致则放行，反之则重新评估检查；应对自动化运维可能导致大面积故障的风险，可采取灰度发布、故障快速自愈机制。

应对外部合作风险，一方面在对外合作中加强合同条款的信息安全保障；另一方面可建立“白名单”机制，外部系统产生单证等关键信息要在保险公司内部登记，进行白名单管理；也可建立“内外握手”机制，相关内容需求保险公司后台比对验证通过后放行。

应对公有云服务产生的数据资产风险，需要建立公有云服务评估审批机制和数据回传机制。

应对数字化互联互通风险，应抓紧分布式架构优化升级，构建信息系统“水密舱”，确保不发生大面积停机。制定互联互通技术接口与安全规范，防范风险病毒性、即时性、穿透性传导。

### 4.3 数字化生态下的风险管控体系思考

关注数字化模式升级痛点，设计针对性解决方案。加强数字化基础能力建设，抓住实名制身份认证和保险客户账户管理的核心要害，认证管入口，账户管出口，解决保险诚信全流程、穿透式维护痛点。利用第三方电子保单认证机制和区块链新技术，解决保险供需双方行为“可信任”机制痛点。全面升级分布式技术架构，化解集中式技术架构风险高度集中痛点。充分利用合同条款，解决违法违规止损、补偿和托底痛点。

统筹网上网下风险管控，构筑数字与实体防火墙。抓住支付与现场服务核心环节，控制网上网下风险交叉传播。

探索数字化风险保险制度，研发数据风险保障产品。针对数字化可能产品的差错、攻击、渗透、泄漏、篡改、病毒、停机、断网、延迟等新型风险，设计保险保障产品，为数字化转型保驾护航。

建立数字化风险共享机制，强化联防联处协同。建立监管、行业、企业数字化风险共享机制，形成统一高效的风险报告、信息共享、风险处置体系。

加强数字化风险侦测预警，研发风险监控平台。建立数据化风险监控平台，利用大数据、人工智能技术对数字化风险信息进行分析和洞察，提前预警数字化风险。

完善数字化风险应急预案，加强应急实战演练。研发分级分类数字化风险应急处置预案。并组有计划性的演练和无预警实战演练。

### 4.4 保险业的信息安全风险评估

“风险、受众、概率、标准”是保险的基础。其中最重要的就是风险，保险的一切根基就是风险，它是分摊意外事故的财务模式，是国家经济保障制度的重要组成部分；而其他的受众面、风险发生概率和赔付标准（或称事故评估），只是其经济性运行的一些必要因素，毕竟保险业也是需要以盈利为目的。

因此，保险业需要信息安全的漏洞分析与风险评估。如果说疾病保险面向的是个人的健康，那么信息安全风险评估的受众就是信息系统，评估的对象就是可以被利用的漏洞。信息安全对抗的风险就是网络攻击、病毒、蠕虫等等，就像体检机构，可以评估人们的亚健康风险。

#### 4.4.1 传统风险评估

传统的风险评估或者是叫测评，是以资产为核心要素的，大致分为四大步骤。一是资产识别；二是威胁识别，包括威胁的分类和赋值；三是确认已有安全措施；四是风险分析，包括记录、计算和形成报告。主要的操作方法也包括被评估方提供证明材料并审计、实体设备抽样检查、人员访谈、网络扫描和渗透测试等。

因为风险评估是以资产为核心要素，所以评估工作所面临的是一张庞大的网络拓扑（图2），包括外网环境、内网环境、涉密隔离环境等，这就包括数以百计千计的计算机、服务器、网络设备等等，同时还会有很多的员工、外协公司等一切相关的人员。而每一个点都可能包括7个层次的评估目标：硬件、BIOS、底层协议栈、操作系统、中间件或是通用服务框架、通信协议、自编程软件。总和下来，一次全面的风险评估是一个机极其庞大的工程量，而且有数十计的风险评估标准（表1）、等级保护使得一个风险评估过程十分复杂，况且不说被评估方有很多涉密、高端的系统，不希望被测试。



**图2：网络拓扑**

**表1：信息安全风险评估标准**

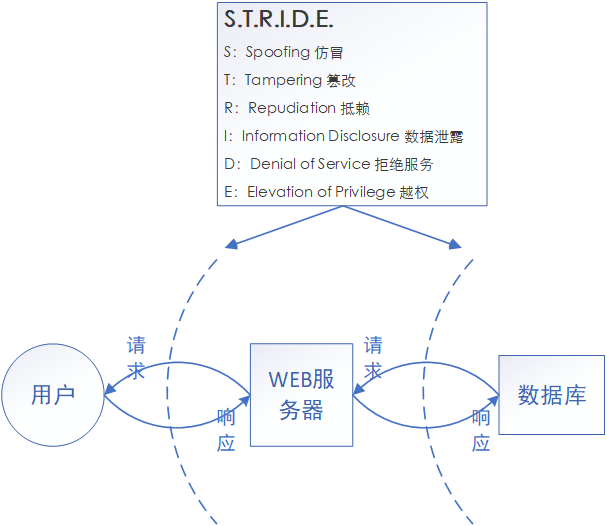
|  |  |
| --- | --- |
| **编号** | **名称** |
| GB/T 20274.1—2006 | 《信息安全技术 信息系统安全保障评估框架 第1部分：简介和一般模型》 |
| GB/T 20274.2—2008 | 《信息安全技术 信息系统安全保障评估框架 第2部分：技术保障》 |
| GB/T 20274.3—2008 | 《信息安全技术 信息系统安全保障评估框架 第3部分：管理保障》 |
| GB/T 20274.4—2008 | 《信息安全技术 信息系统安全保障评估框架 第4部分：工程保障》 |
| GB/T 22239-2008 | 《信息安全技术 信息系统安全等级保护基本要求》 |
| GB/T 22240-2008 | 《信息安全技术 信息系统安全等级保护定级指南》 |
| GB/T 25058-2010 | 《信息安全技术 信息系统安全等级保护实施指南》、《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》 |
| GB/T 20984-2007 | 《信息安全技术 信息安全风险评估规范》 |
| GB/T 31509-2015 | 《信息安全技术 信息安全风险评估实施指南》 |

#### 4.4.2 保险行业特色的风险评估

传统的通用的风险评估并不完全适用于保险行业，况且保险业大多数都是人工操作，而且有严格审计，信息化更多的是辅助和统计，这套风险评估方法不适合。保险行业的信息安全痛点，既不在于设备、也不在于单个用户的数据，而是“总数据”。

既然通用风险评估方法并不能适用于所有行业，那么如何建立保险行业的风险评估呢？国家网安法支持建立自己行业标准和建立适用于自身的风险评估。

保险行业的主要对象是“总数据”，那么以资产为目标的测评体系显然不适合，以“数据流”为目标的测评体系可能会更适应一些。这种体系的核心技术主要来自于微软提出的一种威胁建模模式，是“软件安全开发生命周期”中的一种，他主要以面向业务为核心，只有三种对象：一是角色，如用户、管理员、经理等；二是应用设备，如WEB网站等；三是数据库，即数据汇总存储。根据对象之间的通信请求、响应形成数据流动模型，并在每个流动的部分，分析潜在的安全隐患，分别是：仿冒（Spoofing）、篡改（Tampering）、抵赖（Repudiation）、信息泄露（Information Disclosure）、拒绝服务（Denial of Service）、越权（Elevation of Privilege），缩写总称为S.T.R.I.D.E.（图2），每种隐患都有较为成熟的防护和加固建议。微软官方称这种分析可以杜绝绝大部分的安全隐患，虽然言过其词，但从实践效果来看还是不错的。



**图3：S.T.R.I.D.E.**

这个风险评估更像是抛开了被测方的建设状况，直接从业务设计角度回答了系统应该如何开发。确实，这种模式一般是先验证什么是对的，然后再验证错在哪儿，毕竟保险行业的信息系统庞大但不复杂，这种模式更贴近业务和逻辑，又被称为面向业务流的风险评估。之后的风险评估操作相比传统可以大大简化。面向此“数据流”模型，分为如下五个主要部分。

第一，通用硬件或软件。可概括为一句话：“打补丁、及时打补丁、第一时间打补丁”。也就是建立跟踪机制，随时发现需要安装和更新的补丁；并建立扫描机制，不定期或定期扫描，确保补丁处于及时更新状态。这个也许是老生常谈，也没什么技术含量，但却是解决绝大部分安全隐患的首要方式，也是评估工作中最繁琐的部分。我们常见的重大安全事件，如STRUTS2、WANNACRY勒索等等就都可以得到防范。

第二，对于自编程软件部分，如网站、统计系统等等，对此风险评估应该作为重中之重执行。主要包括的是源代码审计，即白盒测试；某些场合不方便提供源代码时，会用到黑盒测试。无论黑盒白盒，测试主要会面向三个部分，一是功能符合性测试，即验证安全设计部分是否能够真的发挥作用，或存在纰漏；二是意外流程处理的测试方法，这个极为重要，目前我们听到的主要网页入侵方式，如SQL注入、跨站脚本等，都是由于没有考虑到意外流程而造成，并没有那么复杂；三是漏洞挖掘，主要针对二进制分析和逆向分析等。

第三，配置和运维的评估。这个是最容易被忽略的问题，我们常说的弱口令问题等等，此类需要通过审计来完成。简而言之，就是不该开放的服务关闭掉，该打开的安全配置、日志打开，这些只能人工检查；此外，还包括面向数据流通性的检查，主要是网络可用性的问题，如网络划分、设备性能等。从我个人来说，安全必须是为业务可用性而服务的，不能给业务增加负担，因此测评工作必须以业务出发，易用性、可用性和安全性兼顾。

第四，人员安全与业务流程安全评估。在传统中主要是指人员的入职离岗审核、制度、安全意识培训，但真正的核心部分大多数传统评估都没考虑到，是流程的审核，是关注在访问数据是否可以被越权访问，包括加密方式、强度、访问控制等等。很多场景下，企业公司的数据是被未加密直接存放在数据库里，系统运维人员可以直接看到全部数据，这样全数据的暴露风险就是不可控的。

第五，持续渗透测试和监控。渗透测试是指在授权和可控前提下，对目标进行攻击性测试。这个是与传统风险评估一致的，因为安全是一个持续的事，包括有新的设备、系统、功能等上线，社会也会不断有新的攻击方式发布，对互联网开放的系统持续渗透测试和监控，当然还包括很多自身无法控制的部分，比如DNS解析问题、仿冒钓鱼网站问题等，都需要持续监控。

这种数据评估方式不像传统风险评估，围绕资产而出发，由资产上升业务，相反是以业务为起点，直接面向核心数据安全的，这样才更符合保险的行业特点。

#### 4.4.3 保险行业的风险评估V2.0

符合行业特色的信息安全风险评估还有很多发展空间，或者叫风险评估2.0，其中一个重要的方向就是——个人隐私。

现今社会个人隐私信息泄露严重。我们每个人都会接到无数的推销电话。有推销家政服务的、海外代购奶粉的、早教中心的等等，当然还有各种种类卖保险的。他们定位准确，时机适合，直击用户需要，不得不让人感叹：“我的信息又被卖了。”

隐私必将是一个趋势，也越来越受到民众的关注。国家更是将其纳入发展战略之中，《网络安全法》中明确提出了关于隐私的法律责任，同时《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》也随之给于了部分司法解释，而且在十九大中，定制《中华人民共和国网络隐私保护法》在时隔九年之后再次提上工作日程。

隐私就是来自于不同企业公司、政府机关的个人数据，但是必须看清的现实是，《财经》杂志公布数据黑产调查结果，80％的数据泄露自企业内鬼，黑客仅占20％。而这些数据，或者说是隐私数据的价值，从个人来说，可以勾勒你的行为；从群体来说，可以分析和预测动向；从国家来说，可以预测国家策略，影响国家命运。所以，小小的定向广告、骚扰电话，只是一种小的不能再小的危害。目前我国有数千TB的数据在黑产中流通，不同程度涉及到我国几乎所有网民。因此隐私安全必将是国家趋势。

当然，隐私这个问题一直是个悖论，没有好的办法可以证明数据的使用去向，比如：“微软收集了用户这么多数据，怎么证明他们没交给CIA？”但是从一些研究和实践中，还是可以发现一些出路的，比如参考“征信”的实践模式，即虽不能证明安全，但可以通过公布评估内容提供给用户信心。

如：通过外部渗透测试，证明外界无法取得数据；通过内部风险评估，证明内部无法获得完整数据，并造成外泄；通过流程合法性评估和审计，确保使用数据时征得用户同意；通过流程合法性评估，能让民众清晰认知企业公司违规时的法律责任。

当然还包括向用户提供用户信息泄露的提醒服务，这样可以增加用户的信赖感。当然，这种用户隐私服务对于公司来说受限于法律因素，需要联合国家职能测评机构来开展。

#### 4.4.4 风险评估+

在“互联网+”的潮流中，我们也总结出“风险评估+”。一是，风险评估应该不仅是体检，而是企业的一张“名片”，是对安全建设良好的企业的一种宣传，起到模范作用，更是增加用户安全信心的手段；二是，风险评估不仅仅是在增强自身内部安全方面体现价值，同时在面对“网络安全保险”、人工智能、无人驾驶等这一类新兴事物中，也需要对投保对象，即信息系统进行风险评估。

### 4.5 渗透测试

#### 4.5.1 什么是渗透测试

渗透测试是指安全工程师尽可能完整地模拟黑客使用的漏洞发现技术和攻击手段，从攻击者的角度对目标网络、系统、主机应用的安全性作深入的非破坏性的探测，发现系统最脆弱环节的过程。

渗透测试还具有的两个显著特点是：渗透测试是一个渐进的并且逐步深入的过程。渗透测试是选择不影响业务系统正常运行的攻击方法进行的测试。

#### 4.5.2 为什么要做渗透测试

作为网络安全防范的一种新技术，渗透测试对于网络安全组织具有实际应用价值。

渗透测试，是为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，企业定期更新安全策略和程序，时时给系统打补丁，并采用了漏洞扫描器等工具，以确保所有补丁都已打上。如果企业早已做到了这些，为什么还要请外方进行审查或渗透测试呢？因为，渗透测试能够独立地检查企业的网络策略，也就是给企业的系统安了一双眼睛。而且，进行这类测试的，都是寻找网络系统安全漏洞的专业人士。

#### 4.5.3 渗透测试的一般流程

渗透测试的方法包括黑盒测试（对目标一无所知，最初的信息均来自公开搜集）、白盒测试（通过正规渠道向被测单位获取相关的各种资料，比如网络拓扑、员工资料及系统代码等，可与员工进行交流沟通，模拟内部员工提权）和灰盒测试。

渗透测试的一般流程包括：目标发现（定位目标的网络状态、操作系统和相对网络架构），目标枚举（找出目标系统中所有开放的端口；相关目标收集），信息收集，漏洞映射（发掘），社会工程，漏洞利用，提升权限，扩大成果、维持访问，清理痕迹，文档和报告等。

这里的渗透测试流程指的是常规渗透测试（系统和应用的），也有一些有针对性的渗透测试流程，比如网银客户端的渗透测试流程（或者测试内容）就有比较大的差别，包括键盘钩子测试，客户端完整性测试、内存读取、屏幕截图及录像和截发包测试等等。

如何进行渗透测试，我们除了需要了解流程外，更需要理清思路。因此，通过对一个真实的目标进行渗透，来理解整个渗透测试流程。域名：www.xxculturalpark.org

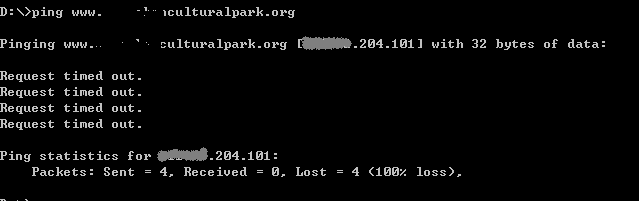
##### 4.5.3.1 信息收集

信息收集的目的是扩大攻击面。

1. 目标IP、域名信息（C段查询、旁注查询）的收集

工具1：Ping

作用：反查IP；判定目标存活；模糊判定目标防护程度；TTL模糊判定OS类型



TTL表示生存时间，不同操作系统会有默认的值，但可以修改。TTL表示包在被丢弃前最多能经过的路由器个数。PING命令时可以用-i参数指定TTL值，可将TTL设置为0，则该包将被立即丢弃。UNIX 及类 UNIX 操作系统 ICMP 回显应答的 TTL 字段值为 255；Compaq Tru64 5.0 ICMP 回显应答的 TTL 字段值为 64；微软 Windows NT/2K操作系统 ICMP 回显应答的 TTL 字段值为 128；微软 Windows 95 操作系统 ICMP 回显应答的 TTL 字段值为 32。

工具2：Whois

Whois收集的管理员名称、电话、单位、信箱、地址等都是我们需要的信息。

作用：判定目标所涉IP范围；域名管理者信息

方法：http://www.apnic.net/

http://whoissoft.com/



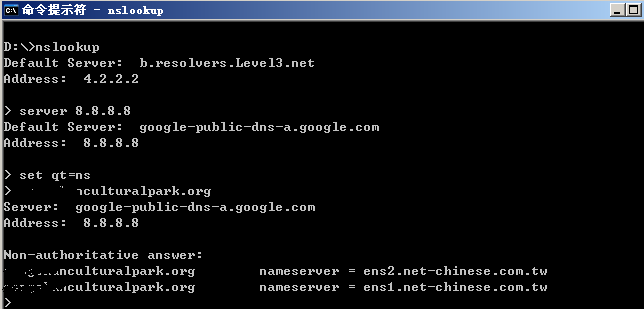
工具3：DNS查询

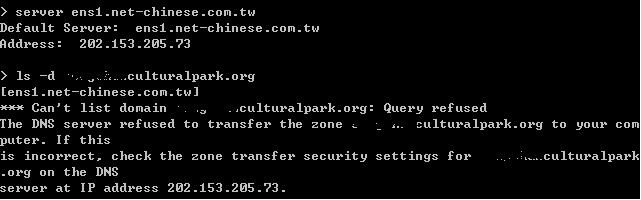
作用：域名DNS服务器信息；尝试区域传送

区域传送（zone transfer）操作指的是一台后备服务器使用来自主服务器的数据刷新自己的zone数据库；一般来说，DNS区域传送操作只在网络里真的有后备域名DNS服务器时才有必要执行，但许多DNS服务器却被错误地配置成只要有人发出请求，就会向对方提供一个zone数据库的拷贝。域名传送可以获取企业内部其他的站点信息，扩大攻击面。

方法：nslookup

BT5:dnsenum, dnswalk…





nslookup的使用方法：

Server 8.8.8.8：设置DNS查询服务器

Set qt=ns：查询名字服务器记录，其他的包括:a,mx

server ens1.net-chinese.com.tw，ls –d：查询其DNS服务器的上的目标域名信息。

工具4：旁注查询

旁注即从旁注入，利用同一主机上面不同网站的漏洞得到webshell，从而利用主机上的程序或者是服务所暴露的用户所在的物理路径进行入侵。

作用：扩大攻击面，殊途同归

方法：http://ip.wen.la/

http://ip.chaxun.la/

部分注入工具

工具5：C段查询

对whois查询确定的目标所涉及的IP段进行一个web探测。旁注查询与C段查询是每次必做的工作，对我们对当前目标无有效手段（如主页就一个登录页面），扩大攻击面帮助很大。

作用：扩大攻击面，绕道而行

方法：http://c.wlan.im/

快速的端口扫描工具：fscan,scanline等

2. 端口（服务）信息收集

试想为何做渗透的每一个人都会去做端口扫描？目标是一个大房子，我们要进去。但墙体很硬，我们只能去踹大门和窗户。已知的80web服务是一道大门，但我们不能忘记它还有很多小门(web服务443,8080,7001,..)，很多窗户(21,22,23,139,445,1433,1521,3306,3389,...)。旁注查询和C段查询就是为了找到与我们目标这个大房子相同或者相连的其他大房子。端口扫描就是要知道目标有几道门、几扇窗，使下一步的漏洞映射更具针对性。

端口扫描工具包括：nmap和快速扫描工具fscan,scanline。

手动验证扫描结果：telnet xx.xx.xx.xx xxxx

Nmap不仅可以较高准确率探测它有几道门几扇窗，还能探测这座房子以及大门窗户的使用材料（os类型，服务软件banner信息等），甚至哪些大门或窗户在篱笆或者围墙（防火墙）之内，哪些又在其之外！除了踹开，还可以拿钥匙（用户名密码）打开。

端口（服务）信息的内容包括：

（1）系统OS类型、版本

（2）系统开放了哪些应用层服务，服务的server类型、版本等banner信息

（3）系统安全防护（IPS,WAF,FW等）状况

（4）Web 服务的server类型、HTTP方法、脚本语言、数据库等的类型、版本等信息

手工探测的一些技巧包括：通过修改URL中目录的大小写判断Win还是unix；firebug判定web server类型版本；对动态URL输入特殊字符报错探测SQL类型等等。

3. Web应用程序信息收集

Web应用程序信息内容包括：

（1）服务器console、管理后台、上传等重要目录

（2）网页编辑器

（3）CMS（通用or独立开发）

（4）网站物理路径

信息收集方法包括：

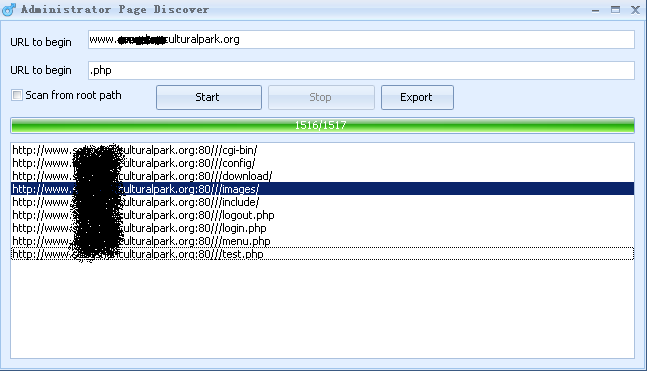
（1）充分熟悉目标站点内容

（2）目录遍历工具：AppScan、AWVS等

（3）目录暴力扫描：wwwscan、Pangolin Admin Page Tools等

（4）Google search

（5）错误页面



目录遍历不在于工具如何强大，而在于使用的目录库是否全面、针对性。有几个常用技巧，手工探测常见重要目录；robots文件；图片的URL地址往往能暴露其后台地址。工具探测的缺点是，留下大量的痕迹。



4. 公开信息收集

通过搜索引擎搜集目标站点的公开信息。内容包括：

（1）企业或单位信息

（2）管理员或员工信息（email、电话、生日等）

最后，进行信息收集的总结，即整理所收集到的目标信息。可进行会员注册。

##### 4.5.3.2 漏洞映射

不同的漏洞类型会造成不同的系统缺陷。SQL注入、上传/下载漏洞、XSS漏洞（Cookie窃取）、访问控制漏洞会造成Web功能实现缺陷；弱口令漏洞、Server/中间件配置漏洞、编辑器漏洞、CMS漏洞会造成Web配置管理缺陷；弱口令漏洞、系统及服务软件漏洞则会造成系统（服务）通用缺陷。

1. 漏洞映射—SQL注入

检测页面是否存在SQL注入。

方法一：

and 1=1 返回正常页面

and 1=2 返回错误页面

方法二：

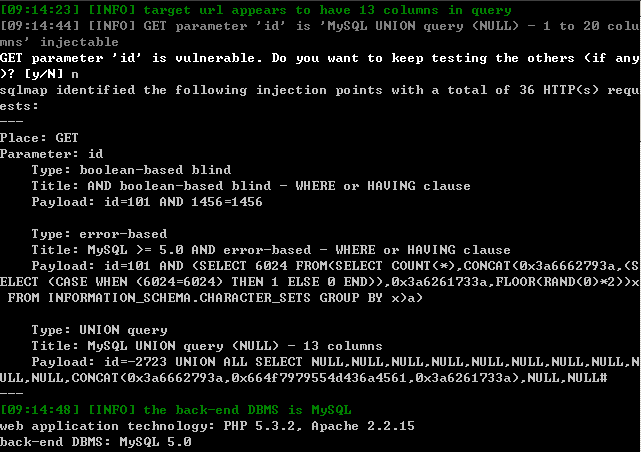
order by n-1 返回正常页面

order by n 返回错误页面

确认存在注入漏洞：获取数据库版本、用户名、数据库名：

union select version(),user(),database(),……





2. 漏洞映射—上传、下载漏洞

检测下载页面（链接）是否存在漏洞：

URL:http://www.xxculturalpark.org/download/xx.zip

静态下载，未发现漏洞

检测上传页面（链接）是否存在漏洞；

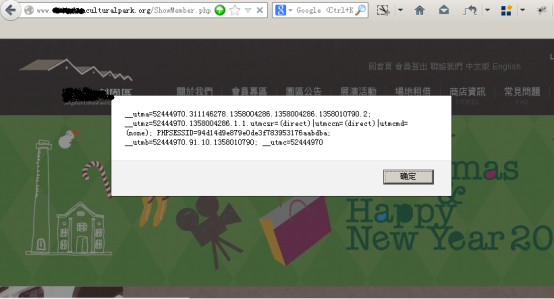
通过信息收集未找到上传链接

3. 漏洞映射—XSS漏洞

检测站点页面是否存在XSS漏洞：

所有可能的用户输入

“><script>alert(document.cookie)</script>



4. 漏洞映射—访问控制漏洞

检测站点是否存在访问控制漏洞：

* 匿名用户访问需要后台管理员权限相关页面
* 匿名用户访问需要会员权限相关页面
* 会员用户访问需要后台管理员权限相关页面
* 会员、后台登录绕过，直接获得会员用户、后台管理员权限
* 无法直接通过匿名或会员用户访问后台相关页面



后台及会员登录可绕过



5. 漏洞映射—其他漏洞

Web配置管理缺陷：

没有使用成熟的CMS信息，编辑器，server管理控制台。

系统（服务）通用缺陷：

仅开放了80，无法尝试系统服务方面的漏洞。

##### 4.5.3.3 漏洞利用

根据发现的漏洞，利用路径：

A. SQL注入漏洞

获取数据库相关信息

暴库，获取后台登录的管理员用户名和密码

* 通过管理后台尝试上传webshell；
* 通过SQL注入漏洞尝试读取/写入文件，获得webshell

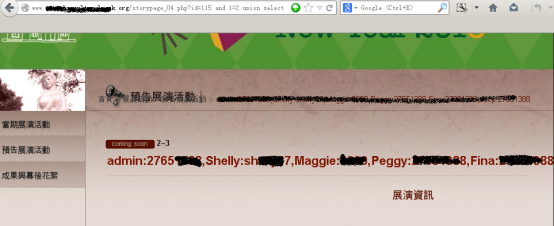
B. 后台绕过漏洞

绕过登录，确认后台登录用户的权限，尝试上传webshell

总结下来，有两个途径：

* 通过后台突破上传获取webshell;
* 直接通过sql注入漏洞获取webshell

1. 获取后台管理员密码

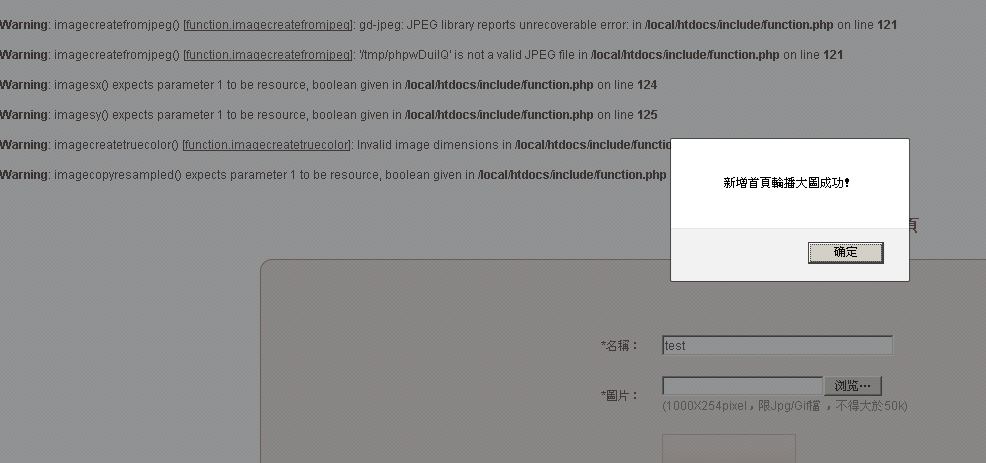


2. 通过后台直接上传webshell

直接上传php文件

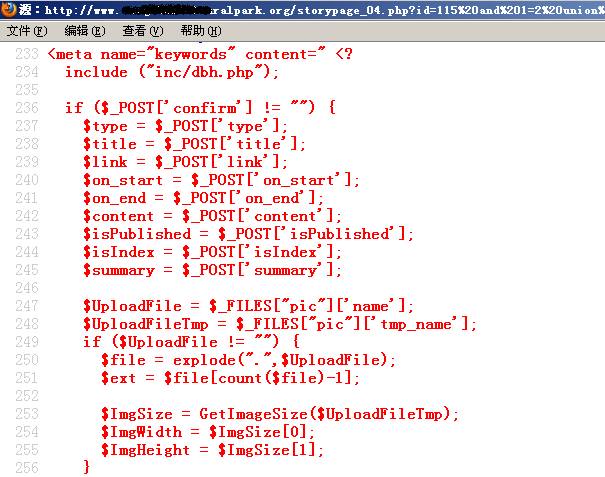
结果：1.提示上传成功，但图片显示为通用图片，上传路径及文件名未知；2.上传过程中出现报错信息。

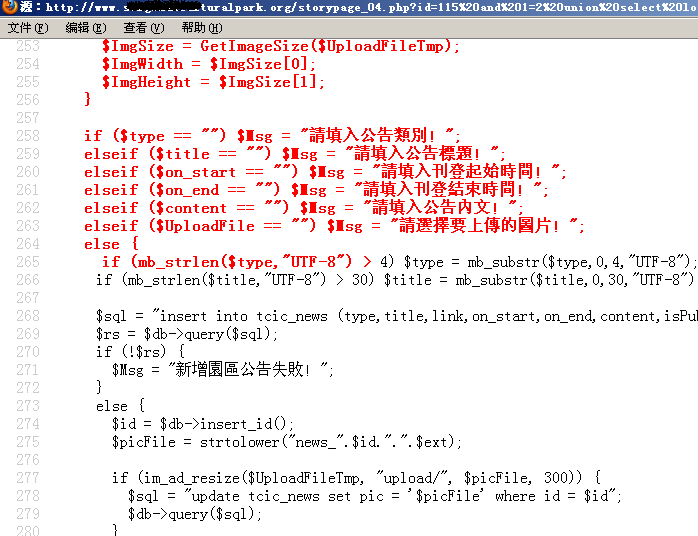
读取上传相关的代码，可通过报错信息获得物理路径。



3. 读取系统文件

读取负责上传的代码文件：publish\_add.php





还可以读取哪些系统文件？

