安全&安心：安心保险合规建设分享

安心保险--全国首批互联网创新型保险公司

演讲者 安心技术保障部总经理 王运海

目录

保险行业安全环境现状分析

保险行业安全环境现状分析

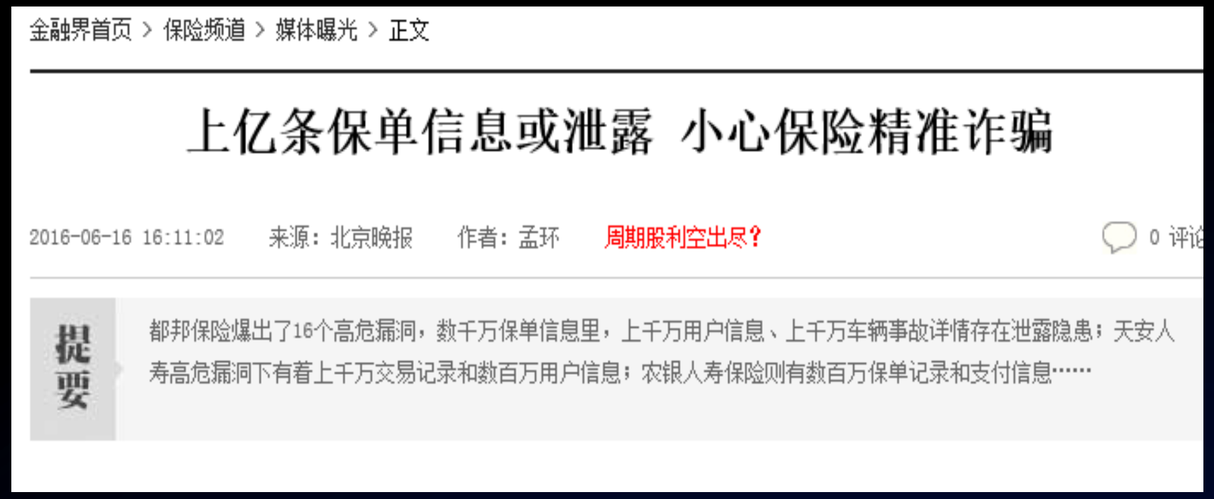

新华网 新闻 新华网 > 信息化 > 正文

惊呆！20多家保险公司千万客户信息或泄露

2015年07月24日 15:28:53 来源： 经济参考报

《经济参考报》记者日前在采访中了解到，近两个月时间内，包括太平洋保险公司、中华保险公司、新华保险、吉祥人寿等在内的保险公司频被曝出漏洞，千万客户的信息面临泄漏风险。

信诚人寿保险“中招” 数十个服务器面临被“攻陷”


金融界首页 > 保险频道 > 媒体曝光 > 正文

上亿条保单信息或泄露 小心保险精准诈骗

2016-06-16 16:11:02 来源：北京晚报 作者：孟环 周期股利空出尽？ 0 评论

提要

都邦保险爆出了16个高危漏洞，数千万保单信息里，上千万用户信息、上千万车辆事故详情存在泄露隐患；天安人寿高危漏洞下有着上千万交易记录和数百万用户信息；农银人寿保险则有数百万保单记录和支付信息……

金融保险系统的漏洞威胁更加复杂

金融行业离钱财最近，因此金融行业网站漏洞受到黑客的关注也最多。据补天平台统计，2017年金融行业网站漏洞数量和高危漏洞数量都处于各行业前列,前11个月金融网站的漏洞曝出数量(超过1700个)、高危漏洞的数量(约700个)，皆领先于教育培训、汽车交通、医疗卫生等行业。

金融行业曝出安全问题，保险领域最为严重

据补天平台收录的漏洞数据，白帽子报告出保险领域260多个漏洞，银行领域130多个漏洞，证券行业70个漏洞,P2P理财服务类网站也报告出180多个漏洞。

支付漏洞影响资金安全

多家第三方支付企业曝出若干漏洞，一旦遭利用，将会影响平台用户的资金流动安全。相关数据显示，移动支付、资费消耗和隐私窃取是手机病毒排行前列的三大危害，其中移动支付类病毒占比68%，随着移动支付越来越普遍，个人账户面临的风险可能会进一步加大。

安心等保测评实施背景

安心等保测评实施背景

- 《网络安全法》的正式颁布施行

随着《网络安全法》的正式颁布施行，网络安全尤其是金融、保险等关系到国计民生的关键信息基础设施安全已成为国家安全的重要体现

- 行业角度横向状态

各友商体量大、起步早，在信息安全建设尤其是等级保护合规建设上投入很大。人保、人寿、阳光、平安等作为保险行业的排头兵，不仅全面响应国家要求，而且积极参加标准制定、政策指导等工作

- 安心保险处在快速发展期

IT设施、应用系统的一些安全因素如果在设计实现的时候缺乏考虑，后期承载业务后难以补救

安心实施等保测评的目标

安心实施等保测评的目标

现有系统安全合规整改

依据有关信息系统安全等级保护工作的部署要求，开展信息系统安全等级保护测评工作，对安心保险的信息系统进行差距测评，对照等级保护基本要求的标准查找差距，并针对存在的安全隐患以及未落实的安全措施，制订信息系统整体信息安全防护方案，开展安全整改的实施工作，最终提高安心保险信息系统的安全保障能力。

新系统建设要求

通过对现有系统的安全测评、整改，后续新系统建设时，按三级系统的要求，进行系统建设，保证新老系统均满足等保三级要求。

安心等保测评重要内容

等保测评三级的重要内容

- 信息系统定级工作

确定信息系统的个数、每个信息系统的等保级别

- 信息系统备案工作

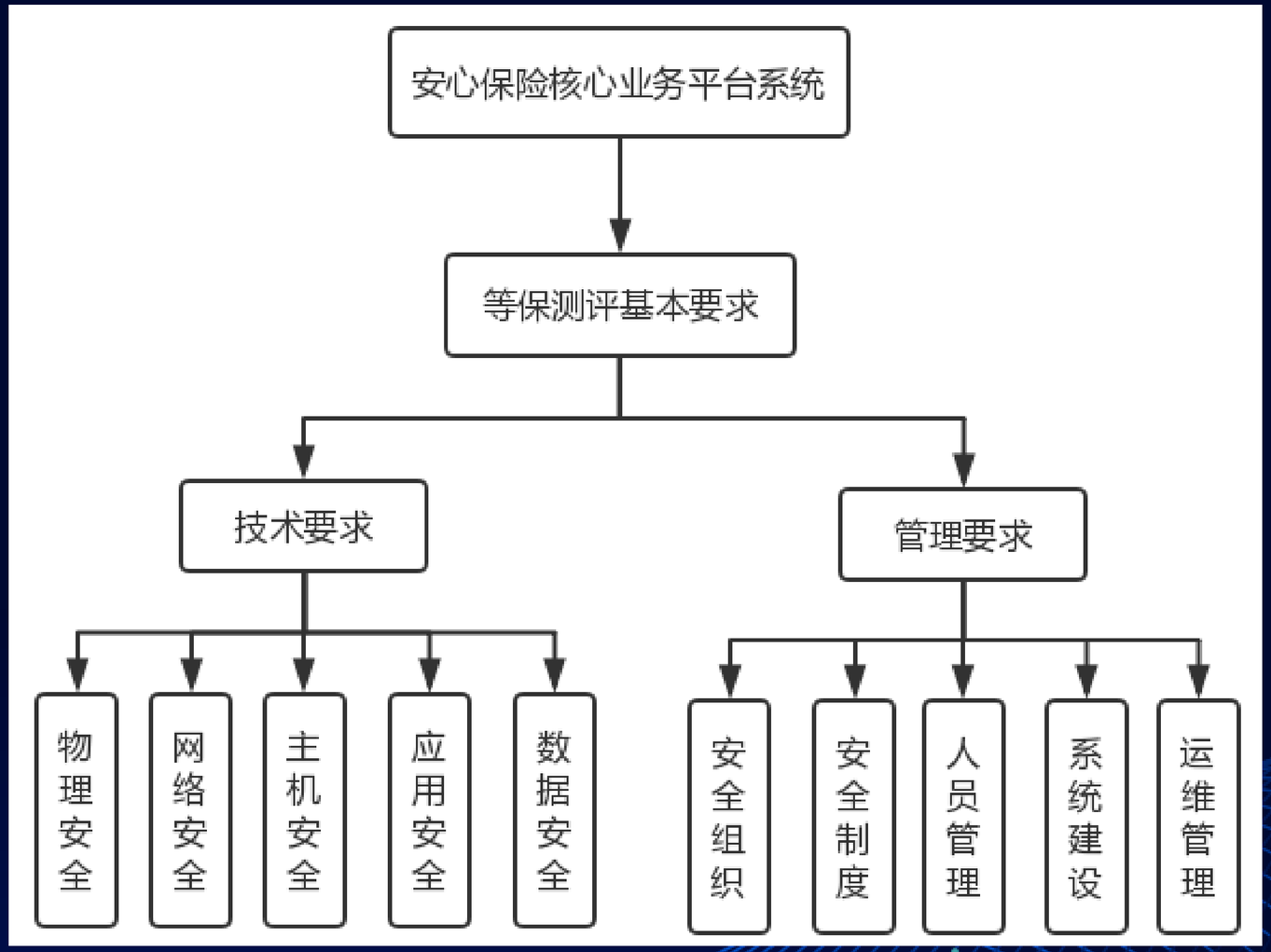
向属地公安机关网监部门提交《系统定级报告》及《系统基础信息调研表》，获取备案证明

- 信息系统等级保护测评工作

依据确定的等级标准，确定等保测评机构，对目标系统开展等保测评工作

- 信息系统安全整改工作

完成测评工作后，将《信息系统等级保护测评报告》提交网监部门备案，针对报告中的待整改项，完成整改工作。



成立等保测评领导小组，全力推进测评工作

- 成立专项小组，任命项目经理，及时召开信息系统安全等级保护定级相关会议；
- 提请各相关部门重视、协调内部资源，做好等保测评计划安排；
- 组织开展政策和技术培训，掌握定级工作规范和技术要求；
- 根据被测系统的业务运行高峰期、网络情况等，适时安排测评时间；
- 全面跟进定级保护工作的进展情况和存在的问题，对存在的问题及时协调解决。

开展信息系统调研梳理，确认定级系统

开展信息系统基本情况的摸底调查

组织各部门各科室开展对所属信息系统的摸底调查，全面掌握信息系统的数量、分布、业务类型、应用或服务范围、系统结构等基本情况，按照《信息安全等级保护管理办法》和《信息系统安全等级保护定级指南》的要求，确定定级对象。

确认定级对象为安心保险核心业务平台系统

安心保险核心业务平台系统包括安心互联网保险官网系统、安心互联网保险微信系统等。该平台系统集投保、理赔于一体，包括了车险、非车险、健康险、理赔、承保等众多子系统，构成安心保险核心业务平台系统。

确定安全保护等级、积极推进定级备案工作

- 按照《信息安全等级保护管理办法》和《信息系统安全等级保护定级指南》，确定定级对象的安全保护等级为三级，起草定级报告。
- 评审。召开专家委员会进行系统安全等级保护评审组进行评审。
- 备案。根据《信息安全等级保护管理办法》，信息系统安全保护等级为第三级，积极联系延庆公安局，准备并提交定级备案材料。

积极配合测评小组，整改现有安全问题

- 各部门认真按照评级要求，组织专人配合测评小组进行审核。
- 积极配合测评小组，整改现有安全问题

问题1：初步建立了信息安全规章制度，但还不完善，未能覆盖到信息系统安全的所有方面。 整改方案：完善信息安全相关规章制度，实现信息安全的规范管理。

问题2：专业技术人员较少，信息系统安全投入的力量不足。整改方案：加强对计算机安全知识的培训，定期开展信息安全检查工作，提高人员安全防护意识。提高信息安全专岗技术力量。

问题3：开发应用安全环节问题较多，整改方案：加强安全防范，包括安全审计、软件容错、身份鉴别、访问及资源控制等方面。

安心安全体系规划

安心安全体系规划

- 主机安全：通过对主机木马文件查杀、登录行为审计、密码破解拦截、系统组件漏洞检测、Web 组件漏洞检测、安全基线检测，等发现主机漏洞，并及时整改。

- 应用安全： 通过web漏扫强大的并发扫描能力，检测web应用，业务上线前，通过web漏扫，提前发现系统问题，并进行整改，整改完成后进行系统上线。

- 网站安全：使用WAF产品，对 Web 入侵防护、0Day 漏洞补丁修复、恶意访问惩罚、云备份防篡改等建立多维度防御策略，全面防护网站的系统及业务安全，安心目前已对所有外网开放的业务进行了WAF防护。

- 网络安全：使用腾讯云提供的 DDoS 防护、DNS 劫持检测和安全认证三大功能，进行网络安全防护，并通过安全域的划分、网络设备的双因子认证，保障网络的接入安全。

安心安全体系规划

- 移动安全：通过对移动应用（APP）的安全加固、安全测评、兼容性测试、盗版监控、崩溃监测、安全组件等服务，保障安心APP的移动应用安全。

- 运维安全审计：使用堡垒机，切断终端计算机对网络和服务器资源的直接访问，采用协议代理的方式接管了端计算机对网络和服务器的访问。拦截非法访问和恶意攻击，对不合法命令进行命令阻断，过滤掉所有对目标设备的非法访问行为。

- 桌面安全：以安全防御为核心、以运维管控为重点、以可视化管理为支撑、以可靠服务为保障的全方位终端安全解决方案。为用户构建能够有效抵御已知病毒、0day漏洞、未知恶意代码和APT攻击的新一代终端安全防御体系。

以我所能 为你而+

腾讯云 | 安心 互联网保险