安全服务白皮书

恒安嘉新（北京）科技股份公司

❖ 文档记录信息

文档名称	安全服务白皮书			
制作部门	安全服务中心			
版本	修正历史	日期	作者	联系方式
V1.0	创建	2020/7/20	张作峰	zhangzuofeng@eversec.cn

❖ 文档核准信息

版本	核准日期	核准人	所属部门	备注
V1.0	2020/7/20	胡兵	安全服务中心	

❖ 版权声明

❖ 免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

恒安嘉新（北京）科技股份公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但恒安嘉新不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

❖ 信息反馈

如果任何宝贵意见，请反馈：

信箱：yucunnan@eversec.cn

您可以访问恒安嘉新官方网站：http://www.eversec.com.cn，获得最新的技术和服务信息。

目 录

1 服务简介

1.1 服务目标

安全服务旨在满足客户持续发展的网络安全管理和安全技术需求，为企业、政府或特定客户提供全面或部分网络安全解决方案的服务，帮助客户应对来自网络安全领域的各种挑战，为客户的网络安全和业务发展提供安全保障服务。

恒安嘉新安全服务团队由涵盖安全管理、安全攻防、终端安全、网络安全、安全体系建设等领域深耕多年的专家组成，通过现场结合远程的方式为客户提供专业服务，专家团队均具备丰富的安全从业经验。及时发现客户的网络安全事件和安全漏洞，全面掌握网络安全情况、威胁情报线索，为客户网络安全管控工作提供有力支撑。

1.2 服务价值

随着中国信息产业和网络技术的发展，传统的网络安全产品难以满足日益变化的复杂的网络空间，未来中国安全市场将由硬件为主转换为服务为主。以适应

未来用户定制化服务和细分市场等发展趋势。

目前客户侧网络安全人才缺乏、传统技术和产品脱节，通过网络安全服务，可以弥补安全人才不足、安全技术不足、安全信息不足和安全管理理念不足等安全问题，提升客户的信息安全管理水平和安全合规能力，更好的防御安全威胁。

2 服务内容

2.1 安全服务类

2.1.1 安全漏洞扫描服务

2.1.1.1 服务简介

恒安嘉新安服团队针对客户系统提供漏洞扫描服务。漏洞扫描是脆弱性识别的重要手段，能够帮助客户发现设备和系统中存在的严重漏洞，帮助客户了解技术措施是否有效执行，并通过及时修补完善，避免对信息系统造成严重影响。

恒安嘉新将采用具有自主知识产权的漏洞扫描工具对服务范围内各种软硬件设备进行网络层、系统层、数据库、应用层面的全面扫描与分析，扫描设备检测规则库及知识库涵盖了 CVE、CNVD、CNNVD 等标准。扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提出准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案，并由一线驻场服务人员协助客户运维人员实施安全加固并跟踪整个安全加固流程，形成安全风险整改闭环。

通过安全漏洞扫描服务，可以及时发现业务系统中存在的安全漏洞，通过对服务器及安全设备漏洞的整改加固，可以及时地消除安全漏洞可能带来的安全风险。

2.1.1.1 服务交付

针对客户服务器、安全设备等进行漏洞扫描，编写输出漏洞扫描报告，报告

内容详细描述漏洞扫描结果和修复建议。输出内容为：

- 《安全漏洞扫描报告》
- 《安全漏洞问题整改反馈表》
- 《漏洞扫描复测报告》

2.1.2 安全基线评估服务

2.1.2.1 服务简介

恒安嘉新安服团队针对客户系统提供安全基线评估服务。基线评估是参考行业内安全配置规范，通过“自动化工具配合人工检查”的方式进行检查，主要包括网络设备、安全设备、操作系统、数据库、中间件等安全配置基线，采用主流的安全配置核查系统或检查脚本工具，以远程登录或检查脚本工具的方式，完成检查。依据行业内安全技术规范对网络设备、安全设备、操作系统、数据库以及中间件的安全配置基线要求，结合安全评估结果，按照安全整改建议，由一线驻场服务人员协助客户运维人员实施安全加固并跟踪整个安全加固流程，形成安全风险整改闭环。

通过安全基线评估服务，可以及时发现业务系统中存在的安全漏洞，通过对服务器及安全设备漏洞的整改加固，可以及时地消除安全漏洞可能带来的安全风险。

2.1.2.1 服务交付

针对客户服务器、安全设备等进行基线检查，编写输出基线评估报告，报告内容详细描述基线评估结果和修复建议。输出内容为：

- 《安全基线检查报告》

- 《安全基线检查问题整改反馈表》
- 《安全基线复测报告》

2.1.3 渗透测试服务

2.1.3.1 服务简介

恒安嘉新安服团队针对客户系统提供渗透测试服务。渗透测试服务是在用户的授权下，模拟真实的黑客，对评测目标进行非破坏性质的模拟入侵攻击，最大程度挖掘出潜在的安全威胁（包括系统存在的漏洞、脆弱点、网站的不安全因素等）。渗透测试可以用来评估评测目标是否存在可以被黑客利用的漏洞，以及该漏洞引起的风险大小，让企业先于攻击者发现存在的问题，为用户制定完善的安全措施与应对方案提供科学有效的依据。最终结果将以专业安全评测报告的形式呈现，内容包括详细的威胁位置、成因、修复建议等。

通过渗透测试服务，可以模拟黑客常用的入侵方式，通过黑客视角发现业务系统中存在的安全漏洞，及时地消除安全漏洞可能带来的安全风险。

2.1.3.2 服务交付

针对客户的主机和 web 资产，编写渗透测试报告，报告内容详细描述渗透测试结果和修复建议。输出内容为：

- 《渗透测试授权书》
- 《渗透测试报告》
- 《系统复测报告》

2.1.4 风险评估服务

2.1.4.1 服务简介

恒安嘉新安服团队针对客户系统提供风险评估服务。通过风险评估服务可以系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估和分析在网络上存在的安全技术风险，以及业务运作和管理方面存在的安全缺陷、评估安全事件一旦发生可能造成的危害程度，评价风险的优先等级，提出有针对性的抵御威胁的防护对策和安全整改措施，防范和消除信息安全风险，或将风险控制在企业可接受的水平，为网络和信息安全建设与规划提供科学依据。

通过风险评估服务，可以系统的识别企业资产所面临各类威胁和脆弱性，通过风险分析和风险处置，将风险控制在企业可接受的水平，满足企业安全管理要求。

2.1.4.2 服务交付

针对客户的组织架构、管理制度和信息资产，编写风险评估报告，报告内容详细描述风险评估结果和修复建议。输出内容为：

- 《资产清单与风险赋值》
- 《实施方案与计划》
- 《威胁列表》
- 《脆弱性清单》
- 《风险评估报告》
- 《风险处置计划表》
- 《项目总结汇报 PPT》

2.1.5 代码审计服务

2.1.5.1 服务简介

恒安嘉新安服团队针对客户源代码提供代码审计服务。代码安全审计通过分析当前应用系统的源代码，从应用系统结构方面检查其各模块和功能之间的关联、权限验证等内容；基于编程规范和标准，针对应用程序源代码，从结构、脆弱性以及缺陷等方面进行审查，以发现当前应用程序中存在的安全缺陷以及代码的规范性缺陷。在明确当前安全现状和需求的情况下，对下一步的编码安全规范性建设有重大的意义。

通过实施代码安全审计，可以以较小成本快速发现项目中的代码安全漏洞、快速评估系统代码安全风险、增强系统安全性，抵御黑客恶意攻击，保护信息系统资产。

2.1.5.2 服务交付

针对客户提供的源代码，编写代码审计报告，报告内容详细描述代码审计结果和修复建议。输出内容为：

- 《代码审计报告》
- 《代码审计复测报告》

2.1.6 业务安全评估服务

2.1.6.1 服务简介

恒安嘉新安服团队针对客户系统提供业务安全评估服务。业务安全测试通常是指针对业务运行的软、硬件平台（操作系统、数据库、中间件等），业务系统

自身（软件或设备）和业务所提供的服务进行安全测试，保护业务系统免受安全威胁，以验证业务系统符合安全需求定义和安全标准的过程。业务安全主要是指系统自身和所提供服务的安全，即针对业务系统中的业务流程、业务逻辑设计、业务权限和业务数据及相关支撑系统及后台管理平台与业务相关的支撑功能、管理流程等方面的安全测试，深度挖掘业务安全漏洞，并提供相关整改修复建议，从关注具体业务功能的正确呈现、安全运营角度出发，增强用户业务系统的安全性。

传统安全测试主要依靠基于漏洞类型的自动化扫描检测，辅以人工测试，来发现如 SQL 注入、XSS、任意文件上传、远程命令执行等传统类型的漏洞，这种方式往往容易忽略业务系统的业务流程设计缺陷、业务逻辑、业务数据流转、业务权限、业务数据等方面的安全风险。过度依赖基于漏洞的传统安全测试方式脱离了业务系统本身，不与业务数据相关联，很难发现业务层面的漏洞，企业很可能因为简单的业务逻辑漏洞而蒙受巨大损失。

恒安嘉新安服团队基于多年的业务安全测试经验，整理出版了一套关于业务安全测试的书籍—《web 攻防之业务安全实战指南》。书中详细介绍了业务安全测试的方法论，设计出了一套业务安全评估模型，主要通过前台和后台、业务和支撑系统四个不同的考察维度出发，可全方位识别和分析各个业务关键流程可能存在的安全风险，并提供相应的修复建议。

通过实施业务安全评估服务，可以发现传统的安全工具如扫描器，IDS 等不能直接定位到的漏洞，从业务逻辑层面发掘客户系统存在的安全漏洞，及时消除漏洞可能带来的业务风险。

2.1.6.2 服务交付

针对客户提供的业务系统编写业务安全评估报告，报告内容详细描述业务安全评估结果和修复建议。输出内容为：

- 《业务流程表》
- 《业务安全评估报告》
- 《业务安全复测报告》

2.1.7 APP 安全测试服务

2.1.7.1 服务简介

恒安嘉新安服团队针对客户的移动应用提供 APP 安全评估服务。采用人工结合工具开展 APP 安全评估工作，对 APP 网络通讯、服务器端、手机端、数据和业务逻辑等多个层面进行细致的梳理、测试和分析，发现移动 APP 面临的安全风险。

APP 安全评估包含手机端（IOS，Android）和服务端。APP 安全评估主要针对 APP 客户端和的 APP 服务端进行安全测试。其中 APP 客户端的安全测试包括 APP 的漏洞和 APP 所调用的系统组件漏洞。服务端的安全测试包括传输安全测试和服务端应用安全测试。

通过 APP 安全测试服务，可以及时发现客户 APP 存在的安全漏洞，通过对 APP 整改加固，可以及时地消除 APP 漏洞可能带来的安全风险。

2.1.7.2 服务交付

根据客户实际需求针对所有检测的 APP 系统编制输出检测报告描述其发现

的问题并给出相应的解决方案。输出内容为：

- 《APP 安全评估报告》
- 《APP 安全复测报告》

2.1.8 安全监测服务

2.1.8.1 服务简介

恒安嘉新安服团队针对客户提供的系统开展多维度的远程监测服务，监测内容主要包括网页篡改监测、挂马监测、暗链监测、暗网数据泄露监测、github 数据泄露监测、网盘文库数据泄露监测、社交工具数据泄露监测、安全事件监测、舆情监测等。及时提供用户安全信息，使其多角度了解安全现状。恒安嘉新提供了邮件通告、电话通告、短信通告等多种安全信息通告方式。

通过安全监测服务，可以及时发现客户系统的安全事件和信息泄露情况，从而可以及时进行事件处置和信息保护。

2.1.8.2 服务交付

根据客户提供的系统输出安全监测分析报告，描述监测到的各类安全事件并给出相应的解决方案。输出内容为：

- 《安全监测报告》

2.1.9 护网演练服务

2.1.9.1 服务简介

恒安嘉新安服团队根据客户护网相关需求提供红蓝两队服务。其中红队负责提供攻击服务，蓝队负责提供防守服务。2016 年，公安部会同民航局、国家电网，

第一次组织开展了“护网 2016”网络安全攻防演习活动。同年，《网络安全法》颁布，并于 2017 年实施。出台网络安全演练相关规定：关键信息基础设施的运营者应“制定网络安全事件应急预案，并定期进行演练”。自此“护网行动”成为每年的惯例。

通过护网演练服务，可以从真实对抗中发现客户系统及产品的薄弱环节，从而帮助客户及时修复系统漏洞，完善产品功能。最终帮助客户及时发现并整改网络安全深层次问题隐患，提升客户的网络防护能力、攻防双方技术对抗能力、决策指挥及应急处置能力。

2.1.9.2 服务交付

根据客户提供的系统输出护网演练相关报告，描述红蓝两队发现的安全问题。输出内容为：

攻击服务（红队）输出：

- 《众测服务方案》
- 《资产信息收集表》
- 《护网众测报告》
- 《众测总结报告》

防守服务（蓝队）输出：

- 《护网备战方案》
- 《资产信息收集表》
- 《护网众测报告》
- 《护网复测报告》
- 《护网期间注意事项》

- 《攻防演练报告》
- 《防守方成果报告》
- 《护网防守总结报告》

2.1.10 应急响应服务

2.1.10.1 服务简介

恒安嘉新安服团队针对客户需求提供应急响应服务。应急响应服务对客户发生的安全事件进行应急响应与处置，安全事件包括但不限于网站入侵、网页篡改、挖矿木马、蠕虫、勒索病毒、DDOS 攻击等。

应急响应服务方式可以是 7*24 小时远程支持或现场支持。远程支持可以采用电话、传真、E- MAIL，远程加密登录等手段。当远程支持无法解决问题时，将派遣专业的应急响应服务人员在第一时间到达客户所在地提供现场服务

当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作；然后再对入侵者进行追查。

通过应急响应服务，可以在客户系统发生安全事件时及时协助客户进行事件处置与恢复，将事件影响降至最低。

2.1.10.2 服务交付

根据安全事件的类型和过程输出事件分析报告，描述安全事件的处置过程并给出解决方案。输出内容为：

- 《安全事件应急报告》
- 《安全事件总结与建议》

2.1.11 应急演练服务

2.1.11.1 服务简介

恒安嘉新安服团队根据监管单位要求为客户提供应急演练服务。恒安嘉新通过提前制定各业务系统应急演练预案，协助客户完成监管部门要求的应急演练科目，提高应对网络与信息安全事件的处置能力，预防和减少网络与信息安全事件造成的危害和损失。应急演练服务内容包括编写应急演练方案、演练剧本、录制相关视频、彩排和正式演练等。应急演练科目通常包括网页篡改、挖矿木马、蠕虫、勒索病毒、DDOS 攻击、手机恶意程序等。

通过应急演练服务，可以帮助客户了解安全事件发生时的应急处置流程，制定切实可行的应急预案，动态调整相应的安全措施，同时满足合规性要求。

2.1.11.2 服务交付

根据演练科目输出对应的演练报告，描述应急演练的方案和剧本。输出内容为：

- 《应急演练方案》
- 《应急演练科目剧本》
- 《应急演练科目视频》
- 《应急演练总结汇报》

2.1.12 重大活动保障服务

2.1.12.1 服务简介

恒安嘉新一线驻场人员负责提供在重保时期（包括：两会、春节、互联网大

会等）对客户现有网络运行的服务器、终端、网络设备、安全设备、网站及应用系统等开展安全检查和安全监测，从而发现硬件、软件、协议的实现或系统安全策略上的缺陷问题，对发现的问题协助相关单位进行安全整改，在重保时期做好安全加固及防护，保障系统安全稳定运行。

通过重大活动保障服务，可以帮助客户维护系统安全，保障重大活动平稳正常运行。

2.1.12.2服务交付

针对客户重保时期提供的服务器、应用、数据库、安全设备等进行安全检查的，编制并提交相关报告。输出内容为：

- 《重保工作方案》
- 《业务系统重点时期安全检查报告》
- 《业务系统重点时期漏洞修复报告》
- 《业务系统重点时期安全监测报告》

2.2 安全培训类

2.2.1 安全培训服务

2.2.1.1 服务简介

恒安嘉新安服团队为客户提供各类安全培训服务。团队根据客户实际需求开发对应的培训课程、联系培训地点和设计培训时间，所有培训教材和资料由恒安嘉新提供。定制化培训课程包括安全意识培训、渗透测试技术培训、安全应急培训、安全开发培训、护网相关培训等内容。

通过安全培训服务，可以帮助客户提高安全技能水平和安全意识，使其能更优质高效地完成安全相关的工作。

2.2.1.2 服务交付

针对客户进行安全技能培训，输出相关的培训课件和靶场环境。输出内容为：

- 《培训工作计划方案》
- 《培训课件》
- 《靶场环境》
- 《培训记录表》
- 《培训满意度调查表》
- 《培训考核记录表》