企业网络安全评估服务 公司网络安全 企业网络安全

产品名称	企业网络安全评估服务 公司网络安全 企业网络安全
公司名称	广东蓝讯智能科技有限公司
价格	.00/套
规格参数	
公司地址	东莞市南城街道周溪隆溪工业区隆溪路10号金汇科技园A238
联系电话	18028990096

产品详情

勒索病毒是全球严峻的网络安全威胁之一。2019年，在老牌勒索病毒持续活跃的同时，新型勒索病毒层出不穷，东莞网络安全公司认为企业网络安全形势不容乐观。东莞网络安全公司了解到，2019年勒索病毒围绕目标优质化、赎金定制化的勒索策略，以数据加密、数据窃取、诈骗恐吓为主要战术，全年勒索金额明显增长。

据东莞网络安全公司了解，从遭受勒索病毒攻击的国内地域分布来看，攻击范围扩大到全国，其中以广东、北京、江苏、上海等沿海地区及网络资源较为丰富的地区较为突出。从行业来看，勒索病毒攻击主要瞄准具有较高潜在数据价值的对象，传统企业、教育行业、政府机构等遭受攻击很多，其次为互联网、医疗、金融、能源等行业，与往年分布趋同。

2019年，勒索病毒运营团队采取更精确的攻击策略，呈现出目标优质化、赎金定制化等新特点。勒索病毒团伙开始偏向赎金定制化，根据被加密数据的潜在价值进行定价（通常在60000-1000000元人民币）。这种手法大幅提高了黑客团队单笔勒索收益，这也导致个别大型政企机构在遭受到针对性的加密攻击后，被开出高达数百万元的勒索金额。

一、当前信息安全形势

1、外部威胁不断升级安全事件频发

根据verizon 2018年数据泄露调查报告，黑客往往在数分钟内就攻击成功，而作为防守方发现攻击事件往往需要数周，甚至数月。造成这种情况的本质是攻防双方知识积累不对等。作为安全部门，每天需要面对可随时调集互联网上资源的黑客，这些黑客很有可能借助庞大的地下黑产链条对单位业务系统实施网络攻击，且大部分黑客均由兴趣和利益驱动，催生很多攻击高手，攻击手法多变。而安全部门能够调集

的资源有限，威胁情报来源不足，日常工作以单位业务为目标，难以一直集中精力研究攻防技术，导致现阶段安全攻防不对等。目前单位边界防火墙每天收到的攻击日志高达几千次，可见当前业务系统面对的安全压力巨大

2018 年，CNCERT 捕获勒索软件近 14 万个，全年总体呈现增长趋势！勒索软件GandCrab一年时间内就出现了约19个版本，还一直快速更新迭代。其次伴随“ 勒索软件即服务 ”产业的兴起，活跃勒索软件数量呈现快速增长势头，且更新频率和威胁广度都大幅度增加。一切迹象表明外部威胁变化过快，作为安全部门，当前缺乏新威胁的监测以及及时响应能力。

2、我国合规监管越来越严格

随着网络空间战竞争越来激烈，2014年将网络安全提到战略层面。
这一战略的层面给我们信息化安全工作带来了多方面改变：

《网络安全法》已于2017年6月1日正式实施，针对违法行为可直接处罚相关单位和相关人员，目前已有不少单位受到实质性处罚。《等保2.0标准》已正式发布，从以前的业务到现在的云大物移工，该标准相较于《等保1.0标准》细化了很多条款，要求越来越严格。

2019年HW行动的演习范围有增无减，攻击方和防守方数量均属空前。HW行动的本质是以实战性的检验方法检验单位的信息安全防护水平。大量被攻破的案例告诉我们，安全防护水平的提升不单单依靠现有产品，更重要的是查漏补缺，以及具备高阶的安全专家用好现有的防护体系，目前单位内部安全保障压力较大。

二、为什么要做安全评估服务

信息安全保障本质上是风险管理的工作，信息安全风险和事件不可能完全避免，关键在于如何控制、化解和规避风险。风险评估是风险管理的重要组成部分，要想更好地理解风险评估，首先要了解风险管理。

风险管理是识别、控制、降低或消除可能影响信息系统的安全风险的过程。是一个识别、控制、降低或消除安全风险的活动，通过风险评估来识别风险大小，通过制定信息安全方针，采取适当的控制目标与控制方式对风险进行控制，使风险被避免、转移或降至一个可被接受的水平。

三、安全评估服务的内容

1、风险评估服务

在综合考虑资产面临威胁的破坏力及发生几率，脆弱性的严重程度和被利用几率等因素分析资产可能存在的安全风险，结合风险对业务战略的影响程度区别是否可以接受，并针对不可接受的风险采用降低、规避、转嫁、接受等处置方式进行协助整改。

2、渗透测试服务

通过模拟恶意黑客的攻击方法，检测系统抵抗攻击的能力。这个过程包括对系统的所有技术弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者的位置和角度进行的，更容易发现实际生产过程中危害较大的安全隐患、脆弱性利用路径及利用方式

3、漏洞扫描服务

使用自研和其它商用漏扫工具，能够快速从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁，并给出关于安全隐患的详细信息

4、基线核查服务

安全基线是一个信息系统基本的安全保证,即该信息系统基本需要满足的安全要求。基线核查是业务系统及所属设备等在特定时期内，根据自身需求、部署环境和承载业务要求应满足的基本安全配置，全面集中检查和分析各类系统存在的本地安全配置问题。