

# 陕西省网站APP网络安全风险评估报告编制编写公司

产品名称	陕西省网站APP网络安全风险评估报告编制编写公司
公司名称	河南融河矩媒科技有限公司
价格	.00/件
规格参数	品牌:融河矩媒 服务项目:文案定制 服务方向:专业领域
公司地址	中国 河南 南阳市 卧龙区 蓝钻星座
联系电话	18338218580 13323693821

## 产品详情

“网络风险评估用于识别、估计和优先考虑因信息系统的运营和使用而对组织运营、资产、个人、其他组织和国家造成的网络风险。”（NIST 风险评估指南）

网络风险与信息、数据或系统的安全性、机密性、完整性或可用性的丧失有关，并反映了这些可能对组织产生的潜在不利影响。恶意行为者试图利用网络威胁，主要是为了经济利益和吹嘘的权利。

为什么数字时代需要网络风险评估服务？

数字化转型带来了一系列由组织采用的技术带来的风险。其中包括第三方应用程序、大数据、物联网、云服务、社交媒体资产和移动应用程序。企业对数字服务的使用越深入，遭受网络威胁的风险就越高，对网络风险评估服务的需求就越大。

为什么要进行网络风险评估？

网络风险评估使公司能够清楚地了解他们在网络威胁环境中面临的挑战。全面的风险评估将涵盖组织面临的两种网络威胁：

### 外部威胁

这些是由组织外部的恶意行为者使用以下一种或多种黑客策略造成的：网络钓鱼、恶意软件和勒索软件。这些攻击可能针对组织的任何安全域，包括远程访问、安全策略和程序、网络级别、数据管理、服务器级别、端点、供应链或云安全。

## 内部威胁

这些是由组织内部人员或经批准访问组织的人员造成的，例如员工和第三方供应商。这些威胁是糟糕的安全协议和安全培训不足的结果，并且是由希望伤害组织的员工实施的，或者是那些只是作为进入公司的入口而不知道他们间接造成的伤害的员工所实施的。

## 为什么网络风险评估是必要的第一步？

CRA 识别公司面临的外部 and 内部网络威胁。只有当一家公司能够充分了解其威胁态势后，才能设计出应对威胁的安全计划。全面的网络风险评估不仅概述了公司面临的网络风险，还允许安全团队根据严重程度对风险进行优先排序，使他们能够首先将注意力和资源用于比较紧迫的威胁。

## 何时进行网络风险评估

网络风险评估不是一旦完成就可以搁置的一次性项目。如果公司要保持他们在第一次 CRA 后取得的安全改进，他们将需要定期执行这些评估，以了解威胁形势发生了什么变化，并相应地修改他们的安全计划。

“ 风险评估和风险管理不是一次性的，而是作为一个循环重复的连续过程，即识别风险、制定解决这些风险的计划、根据这些计划采取行动以及监测行动结果。 ”（SANS 研究所白皮书：安全项目管理和风险）

## 谁来进行网络风险评估？

安全提供商可能会提供不同的方法来进行网络风险评估，方法从关注攻击向量到威胁建模不等。无论安全团队采用何种方法，网络风险评估而终都应涵盖组织的整个攻击面。

CRA 可以由内部安全团队执行，也可以外包给第三方安全提供商。这将取决于组织的规模、安全团队的规模、专业水平、预算以及监管方面的考虑，例如需要外部方执行 CRA。

## 全面网络风险评估的5个步骤

我们相信详细的增量方法可以提供高级别的可见性和监控。基于这种方法，网络风险评估可以大致分为五个步骤：

### 1. 了解组织现有的安全计划

通过对 IT 和管理层的问卷调查和访谈，评估团队将了解公司必须保护的关键业务资产，以及公司目前用于保护机密数据的安全措施、流程、程序和合规要求、知识产权、领域和场所。

### 2. 定义公司的威胁

在此阶段，评估团队将收集有关公司威胁态势的信息，并估计这些威胁影响组织的可能性。为了全面了

解公司面临的威胁，评估团队将调查所有可能想要攻击公司的威胁行为者，包括国家支持的行为者、勒索软件团伙、支付信息后的犯罪分子以及企图窃取的竞争对手知识产权。

### 3. 识别公司漏洞和攻击路径

在评估的这个阶段，团队将结合其获得的关于公司必须保护的资产的知识，以及它发现的漏洞，并确定每个漏洞如何导致攻击者进入组织并通过其系统到达关键业务资产。然后，评估团队将建议绘制这些攻击路线，以便组织可以清楚地了解每个漏洞可能如何影响每个关键资产，以及阻止每个攻击路线将如何帮助保护这些资产。

在选择网络风险评估提供商时，公司应询问提供商的映射解决方案，以确保此可视化过程是评估的一部分。

### 4. 可视化攻击的后果

在绘制出组织的威胁态势并且评估团队清楚地了解公司的安全计划之后，是时候将两者放在一起估计公司将如何处理攻击了。这是评估的关键部分，因为它让安全领导者和管理层尽可能准确地了解他们现有安全计划的有效性，以及攻击的潜在后果（包括收入损失、对正在进行的业务的损害、声誉损坏、私人数据丢失、知识产权丢失）。

### 5. 确定缓解计划

我们讨论了网络风险评估如何根据比较相关的威胁与组织比较宝贵的资产的关系以及它们被攻击的可能性来确定比较相关的威胁。然而，安全团队仍然需要知道要缓解什么以及首先要处理哪些威胁。

在此阶段，优先级排序过程用于帮助安全团队充实缓解计划，该计划根据严重性首先倾向于比较关键的漏洞。

### 组建网络风险评估团队

全面的网络风险评估包括由受过定位漏洞和攻击路线培训的安全专家进行的多项检查和分析过程。获胜的网络风险评估团队将包括红队和蓝队、网络威胁情报分析师、威胁猎手和漏洞检查员，以及能够获取这些数据并将其转化为可量化指标的分析师。

网络风险评估的结果应提供一个框架，公司可以在此框架上推进网络风险量化过程，在该过程中，发现的风险与业务指标相关联，从而为风险分配货币价值。

### 网络风险评估可以做什么？

网络风险评估可以发现大量漏洞和网络漏洞，这些漏洞和漏洞存在于组织的不同部分，跨越多个安全领域，并且严重程度各不相同。选择网络风险评估提供商时，重要的是要考虑多种因素，包括：

可视化和演示

缓解计划和跟踪

成本敏感的修复计划

风险量化能力

动态且可调整以适应不断变化的威胁形势

敏捷性和可扩展性潜力