# 湖南公司企业网络安全风险评估报告编制编写

| | |
|---|---|
| 产品名称 | 湖南公司企业网络安全风险评估报告编制编写 |
| 公司名称 | 河南世耀诚实业集团有限公司 |
| 价格 | .00/件 |
| 规格参数 | 品牌:融河矩媒<br>服务项目:文案定制<br>服务方向:专业领域 |
| 公司地址 | 南阳市卧龙区工业路华龙广告二楼 |
| 联系电话 | 13140513661 18338218580 |

# 产品详情

几乎每个企业都有互联网连接和某种形式的IT基础设施，这意味着几乎所有企业都面临网络攻击的风险。为了了解这种风险有多大，并能够管理它，企业需要完成网络安全风险评估，这个过程可以确定哪些资产比较容易受到企业面临的网络风险的影响。

减轻评估过程中发现的风险将预防和减少代价高昂的安全事件和数据泄露，并避免监管和合规问题。风险评估过程还要求企业内的每个人考虑网络安全风险如何影响企业的目标，这有助于创建一种更有风险意识的文化。

网络安全风险评估包括哪些内容?

网络安全风险评估要求企业确定其主要业务目标，并确定对实现这些目标至关重要的信息技术资产。然后是识别可能对这些资产产生不利影响的网络攻击，决定这些攻击发生的可能性及其可能产生的影响;总之，为特定的业务目标构建威胁环境的完整图像。这允许安全团队就如何以及在何处实现安全控制做出明智的决定，以将总体风险降低到企业可以接受的程度。

如何进行网络安全风险评估:5个步骤

网络安全风险评估可以分为许多部分，但五个主要步骤是确定范围、风险识别、风险分析、风险评估和记录。

第 一步:确定风险评估的范围

风险评估从决定评估范围开始。它可能是整个企业，但这通常是一个太大的任务，所以它更有可能是一

个业务部门，如支付处理或web应用程序。获得其活动在评估范围内的所有利益相关者的全力支持至关重要，因为他们的投入对于了解哪些资产和流程比较重要、识别风险、评估影响和确定风险承受能力水平至关重要。可能需要一个专门从事风险评估的第三方来帮助他们完成这种资源密集型的工作。

第二步:如何识别网络安全风险

2.1资产识别

您无法保护不知道的东西，因此下一个任务是识别并创建风险评估范围内的所有物理和逻辑资产的清单。在识别资产时，重要的是不仅要确定那些被认为是对业务至关重要的资产，可能是攻击者的主要目标，而且还要确定攻击者想要控制的资产，例如服务器或图片存档和通信系统，以用作扩展攻击的枢轴点。根据资产清单列表创建网络架构图是一种很好的方法，可以可视化资产和流程之间的互连性和通信路径，以及进入网络的入口点，从而使识别威胁的下一个任务更容易。

2.2识别威胁

威胁是威胁行为者使用的战术、技术和方法，有可能对企业的资产造成损害。为了帮助识别每个资产的潜在威胁，可以使用威胁库，如MITRE ATT&CK知识库和来自网络威胁联盟的资源，它们都提供高质量、新的网络威胁信息。安全供应商报告和建议可以成为特定行业、垂直行业、地理区域或特定技术中出现的新威胁的绝 佳新闻来源。

还要考虑每个资产在公司网络杀伤链中的位置，因为这将有助于确定他们需要的保护类型。网络杀伤链列出了典型现实世界攻击的阶段和目标。

2.3确定可能出现的问题

此任务涉及指定已识别的威胁利用漏洞攻击范围内资产的后果。例如:

威胁:攻击者对数据库执行SQL注入

弱点:应用补丁的

资产:web服务器

后果:客户的私人数据被盗，导致监管罚款和声誉损害。

在这样简单的场景中总结这些信息，使所有涉众更容易理解他们在关键业务目标方面面临的风险，并使安全团队更容易确定适当的措施和良佳实践来解决风险。

第三步：分析风险并确定潜在影响

现在是时候确定步骤2中记录的风险场景实际发生的可能性，以及如果它确实发生，对企业的影响。在网络安全风险评估中，风险可能性、给定威胁能够利用、给定漏洞的概率应该基于威胁和漏洞的可发现性、可利用性和可重复性来确定，而不是基于历史事件。这是因为网络安全威胁的动态性质意味着可能性与过去发生的洪水和地震等事件的频率并没有密切联系。

将可能性分为1级:罕见到5级:“ 极有可能 ”，影响分为1级:可忽略到5级:“ 非常严重 ”，这样就可以直接创建如下步骤4所示的风险矩阵。

影响是指利用漏洞的威胁所造成的后果对企业造成的损害的程度。应在每个场景中评估对机密性、完整性和可用性的影响，并将高影响作为终点得分。这方面的评估本质上是主观的，这就是利益相关者和安全专家的投入如此重要的原因。以上面的SQL注入为例，对机密性的影响等级可能是“ 非常严重 ”。

第四步：确定风险的优先级

使用如下所示的风险矩阵，其中风险级别为“ 可能性乘以影响 ”，可以对每个风险场景进行分类。如果SQL注入攻击的风险被认为是“ 可能 ”或“ 极有可能 ”，那么我们的示例风险场景将被归类为“ 非常高 ”。

任何超出商定的容忍水平的情况都应优先进行治疗，使其处于企业的风险容忍水平内。有三种方法:

避免。如果风险大于收益，停止一项活动可能是良好的行动，如果这意味着不再接触它。

转移。通过将某些业务外包给第三方(如DDoS缓解)或购买网络保险，与其他方分担部分风险。第 一方保险通常只覆盖因网络事件而产生的成本，例如通知客户数据泄露，而第三方保险将覆盖数据泄露后的和解资金成本以及罚款。但它不包括知识产权损失或品牌声誉受损的无形成本。

减轻。部署安全控制和其他措施，以降低可能性和/或影响，从而将风险水平降低到商定的风险承受水平。实施措施以降低不可接受的高风险的责任应分配给适当的小组。还应设置进度和完成报告的日期，以确保风险所有者和治疗计划保持新的。

然而，没有任何系统或环境可以做到100％安全，因此总会有一些风险。这被称为剩余风险，必须被高级利益相关者正式接受，作为企业网络安全战略的一部分。

第五步:记录所有风险

在风险登记册中记录所有已识别的风险场景是很重要的。应定期审查和更新，以确保管理层始终掌握其网络安全风险的新的情况。

网络安全风险评估是一项庞大而持续的工作，因此如果要改善企业的未来安全性，就需要提供时间和资源。随着新的网络威胁的出现，新的系统或活动的引入，它将需要重复，但如果第1次做得好，它将为未来的评估提供一个可重复的过程和模板，同时降低网络攻击对商业目标产生不利影响的可能性。

融河矩媒企业云网络，新一代企业网络解决方案，通过全球骨干网络和虚拟化技术帮助企业建立私有的企业网，并内置“ 零信任 ”安全体系，以细颗粒度保障内部网络安全。

融河矩媒企业云网络解决方案，适用于多分支网络互联、移动办公接入、应用加速、上云/混合云、身份准入、网络隔离、上网行为等多种应用场景，并帮助企业节省约 75%
网络成本，持续提升企业网络体验并创造价值。