IBM Security

推进零信任的风险管理

推进零信任的风险管理

在当今网络环境中，风险管理绝非小事一桩。防火墙作为企业主要网络防御手段的日子早已一去不复返。如今的企业正在向云端迁移，每周都会向其网络中添加新用户和新设备，每天都会创建数 TB 的数据，并且在其 IT 环境中使用数十乃至数百个第三方软件和系统。与此同时，攻击者正在不断改进他们的方法，着力利用这些变化，同时还增加攻击的次数和复杂程度。

为了应对这些趋势变化，业务领导者必须能够收集企业的风险领域，并将其置于相应的情境下优先考虑，以便将风险降至最低，并基于零信任原则执行安全策略。

本文将说明现代风险管理方法是什么样的，介绍零信任框架如何帮助企业加强现有的风险管理策略，或者以此为基础从头开始制定风险管理策略。

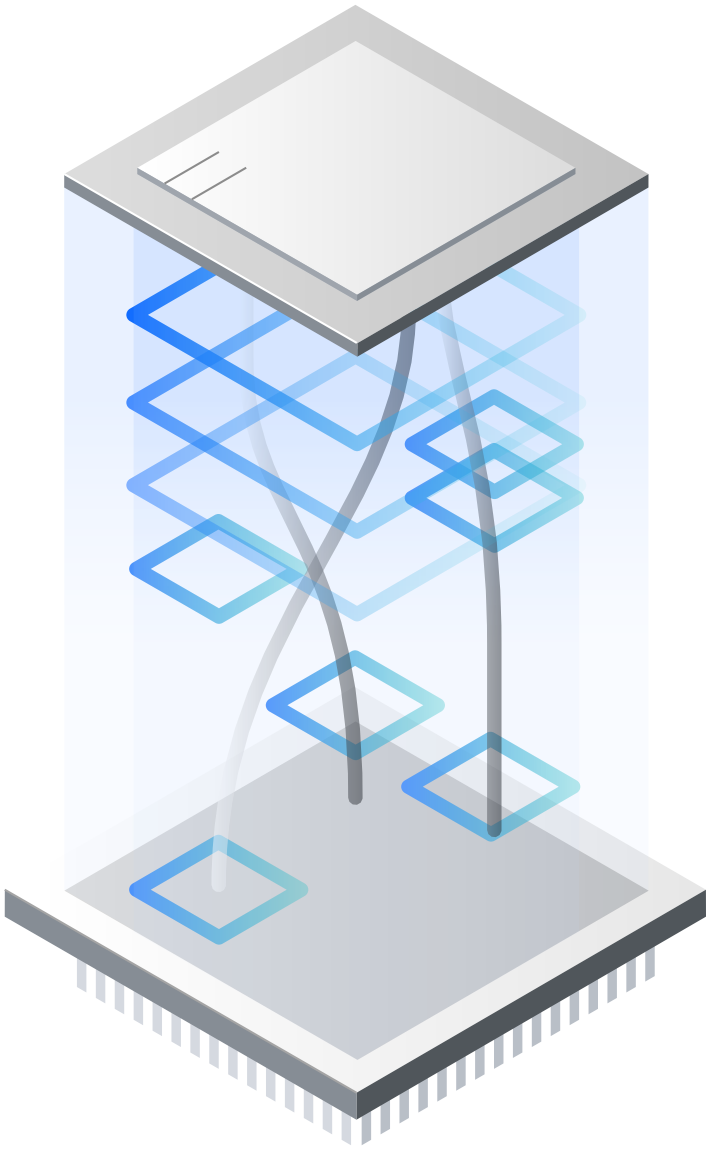
什么是风险管理?

对于许多人来说，风险具有主观性。想象一下走在赌场里时，您所看到的赌桌旁形形色色的人。在一张轮盘赌桌上，您可能会发现有人反复在编号的方格上投入大赌注，这种情况下成功的概率非常之低，但随之而来的却是 25:1 的高赔率。在同一张赌桌上，您可能还会看到另一种人，他更厌恶风险，只是在红色或黑色区域投入小额或中等赌注，这种情况下的胜算率接近 50:50，但赔率也低得多，仅为 2:1。这两种人之间的区别在于他们是否愿意或有能力承受经济损失，也就是他们在轮盘旋转时所下注的金额。

公司与人一样，也各有各的风险门槛，这会受到各种各样因素的影响，例如，它在市场上的地位、投保的程度、其资本结构、其经营所在司法辖区的法律或法规等等，简直不胜枚举。就像个人一样，对于特定概率下可以承受的财务损失，公司也各有各的容忍度。当我们在业务环境中谈论风险时，我们所说的就是这种潜在财务损失的风险。

风险管理关乎企业如何结合运用技术、流程、政策和人员，以经济有效的方式实现和维持可接受的风险水平。[1] 由于实现利润最大化的一个关键就是实现损失最小化，因此各个企业都在忙于开展某种形式的风险管理。然而，并非所有企业都采用战略方法，许多企业只能推测他们是否正在以经济有效的方式管理风险。

是什么让风险管理对当今的企业如此具有挑战性？



- 比较风险的主观定义：安全生态系统由各种工具组成，这些工具旨在保护数据、设置和强制执行用户权限、识别和阻止威胁以及修复漏洞等。许多现代安全工具都为用户提供了风险分析功能。这些分析具有主观性，它们依赖于不同的风险定义，并使用不同的变量。比较不同工具的风险数据所存在的难处，可能是理解企业整体风险状况时所面临的一大障碍。

- 衡量和量化风险：重要的财务和战略决策是在考虑潜在风险的情况下制定的，但量化安全风险可能极具挑战性。假设是所有风险分析的核心，包括威胁事件发生概率的假设、威胁利用已知漏洞以达到最大效果的假设，以及您的防御系统抵御威胁能力的假设。如果没有在整个企业中应用一组一致的假设，就不可能准确地衡量总体风险。

- 优先补救风险领域：如果没有一致的方法来衡量、比较和量化风险，业务领导者就将依靠直觉来决定要优先补救哪些风险领域。由于并非基于数据，他们的直觉可能是错误的，并有可能导致公司出现财务损失。

- 跟踪补救的有效性并逐步应用所学知识：如上所述，风险管理不仅仅关乎减少损失，而且还要以经济有效的方式来做到这一点。如果没有量化，业务领导者就无法采取切实可行的方法来评估他们在所部署的安全工具或所组建的团队上取得的投资回报。他们也无法随着时间的推移，衡量为化解威胁而建立的流程所产生的影响。

[1] “Measuring and Managing Information Risk: A FAIR Approach” , Jack Freund 和 Jack Jones

零信任模型能为安全风险管理做些什么？

安全形势瞬息万变，原先的边界早已不复存在，而威胁也可能源自于各种载体，为了应对这种状况，Forrester Research 创建了零信任框架。零信任的关键在于确保企业的所有数据和资源在默认情况下都无法访问，并且只能在有限的基础上、适当的条件下进行访问。[2]

为了成功实施零信任方法，安全领导者需要构建一个 IT 基础架构，将来自整个企业的信息编织在一起，进而提供必要的环境，帮助验证所请求的连接是否可信。[3] 要生成零信任安全所需的环境，理想的方法就是遵循以下四个指导原则：

1. **定义环境：**企业需要了解在整个组织范围内哪些用户、数据和资源已互联互通。定义环境包括根据风险发现资源并加以分类。

2. **验证和强制执行：**请求访问资源的每个实例都需要不断进行验证和持续监控，确保它与相关权限保持一致。

3. **解决事件：**面对层出不穷的威胁、不断变化的状况，企业必须做出调整并不断演变，这将要求企业在解决事件的同时，尽可能地降低对业务连续性造成的影响。这包括面向用户、设备和网络做出改变、化解威胁以及报告合规性

4. **分析和改进：**零信任意味着自适应；随着威胁的性质不断演变，企业的 IT 生态系统须适应新的业务需求，安全和 IT 领导者必须审查和调整他们的战略，从而顺应不断变化的现实。这个持续改进的过程应该以最大限度减少业务连续性干扰的方式进行。

[2] “Protect your workforce; Grow your business with context-based zero trust”，Forrester Research [来源]

[3] “Protect your workforce; Grow your business with context-based zero trust”，Forrester Research [来源]

通过零信任方法制定有效的风险管理策略

零信任策略是解决整个企业内的风险并明确其优先级的有效方法。对于希望最大限度降低企业潜在损失风险的业务领导者来说，他们应该着重通过统一的安全分析平台，将自身 IT 环境中已部署的各种安全工具所产生的信息连接起来。由于其中一些解决方案随附预先存在的风险分析功能，因此业务领导者应部署一个解决方案来收集这些来源所产生的风险数据，对数据进行标准化处理以便于比较，并关联数据以发掘洞察。

理想的风险管理解决方案将会通过通用算法运行不同的风险数据，提供分析功能，解释风险事件可能产生的影响和程度。该解决方案应提供深入钻取工具，用于调查特定的风险领域，并且与安全编排、自动化与响应 (SOAR) 解决方案相集成，从而加快问题修复，并尽可能地降低对业务连续性造成的影响。

最后，为了实现持续改进，理想的解决方案将向用户展示，作为先前补救策略所带来的结果，风险趋势会如何随着时间的推移而变化。这种反馈循环必不可少；安全领导者将拥有必要的可见性，用于确定其事件响应行动的效力并根据需要做出调整。

帮助管理风险的解决方案和服务

面向 IBM Cloud Pak for Security 的 IBM Security Risk Manager 就是这样一种解决方案。它可为安全领导者赋能，让他们能够从其安全环境中收集风险数据，并将这些数据置于一定的情境中。通过从各种载体（包括身份和访问管理解决方案、数据安全解决方案以及连接到 **Cloud Pak for Security** 实例的基础架构安全解决方案）搜集风险数据输入信息，并使用通用风险引擎分析输入信息，Risk Manager 有助于形成一个更完整的风险状况画面，并为业务领导者提供必要的信息来优先处理风险领域和采取补救措施。**该解决方案**在单个仪表板上向用户展示企业风险的统一视图。作为 Cloud Pak for Security 的一部分，Risk Manager 可与该平台的其他本机应用程序（如 Data Explorer 和 SOAR）无缝集成，进一步扩展了该解决方案的调查和问题修复功能。

如前所述，量化安全风险可能是风险管理中面临的一个障碍，但是，用财务术语来表达风险对于有效的企业规划至关重要。安全风险量化也有助于为安全团队和业务领导者实施零信任项目提供清晰的战略和路线图。通过显示对企业安全的最大影响，风险量化可以在实施零信任策略之前标记需要解决的风险和责任。事先了解了这些知识，零信任项目就可以通过要求对所有连接进行验证和授权，始终将业务与预期和意外风险隔离开来。最终带来的结果就是，通过给安全风险设定一个数值，不论是从技术上还是业务角度，企业高管都在该风险方面得到了可靠的保证。

为了实现这一结果，您需要将安全情报集成到量化的业务风险和指标中，进而将安全风险管理与您的整体业务战略联系起来。**IBM 的安全风险量化方案**为首席级高管提供了一种整体方法，以便使用量化的财务术语来制定风险计划。

“一刀切”的方法行不通

每个企业都是不同的，都有各自独特的业务重点和风险承受能力。专业的风险量化咨询团队可以帮助您的企业了解潜在威胁的真实经济影响，在相应的情境中明确安全风险的轻重缓急，并为企业带来安全投资回报。

对于寻求快速有效地最大限度降低业务风险的安全领导者来说，他们需要一种解决方案来规范化处理风险数据并将其置于一定的情境中，促进优先级排序，同时帮助他们确定可降低整体风险的最佳行动方案。没有任何两家企业会完全相同，因此，您所寻求的解决方案应能够满足自身企业的需求，可以灵活变化，并能够随着企业的发展而轻松扩展。