风险评估：多重身份验证 (MFA) 安全性

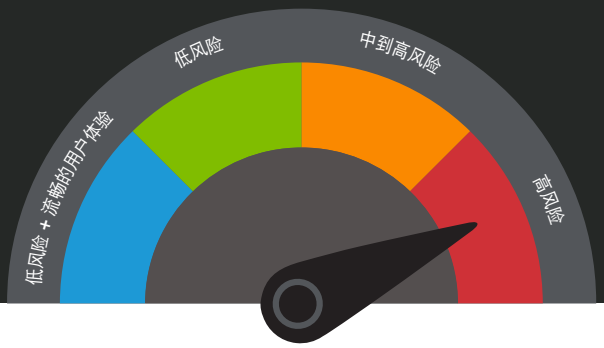
了解当今身份验证解决方案的风险量级

在所有与黑客相关的泄露行为中，有 80% 与用户凭据被盗或密码安全习惯不佳有关，[1] 目前已有超过 6.13 亿个密码因数据泄露而外泄。[2] 添加多重身份验证 (MFA) 并将其作为额外的登录安全层可以显著降低风险，但大多数传统 MFA 解决方案仍然比较容易遭到入侵。

企业的身份验证安全机制成熟度如何？了解当今身份验证模型的风险：

高风险

用户名和密码身份验证



单纯依靠凭据强度进行安全身份验证的企业极易受到攻击。用户名和密码的安全性之低已经达到了前所未有的程度。利欲熏心的恶意攻击者盗窃、破解和掌握登录详细信息，随后自行使用或者在暗网上出售，从而迅速将其变现。

恶意攻击者如何绕过用户名和密码：

- **撞库**
- **网络钓鱼**
- **密码喷洒攻击**
- **暴力破解**
- **先前的数据泄露/重复使用相同密码**
- **密码重置**
- **按键记录**
- **本地发现**

用户往往在多个网站中重复使用相同的密码，这进一步危及了企业安全；企业在岌岌可危的用户个人帐户面前也难以幸免。即使是错综复杂的算法生成的密码也存在固有漏洞，这证明了 MFA 的实施势在必行。归根结底，依赖单独一层安全措施（也就是单一身份验证）绝不可取。卓越的安全机制总是包括多层防御。

中到高风险

标准多重身份验证 (MFA)

您可以将 MFA 功能添加到身份验证安全堆栈中，立竿见影地提高企业安全性。MFA（包括双重身份验证 (2FA) 在内）依靠至少两个独立的身份验证因素来验证用户。第一个因素通常是密码。第二个（可能也包括第三个）因素则可能是您知道的信息（比如 PIN 码或安全问题）；您拥有的某个事物（比如设备、一次性代码/密码或硬件/软件令牌）；或者您自身拥有的某个特征（包括指纹和人脸 ID 等生物特征识别技术，或者位置等情景信号）。

虽然与传统单一用户名/密码身份验证相比，传统 MFA 大大降低了风险，但攻击者仍然可以通过多种绕过身份验证安全机制的方法轻易攻破：

- **网络钓鱼**
- **使用透明代理（中间人攻击）**
- **通过电子邮件或短信拦截验证码**
- **撞库**
- **重放攻击**
- **SIM 卡交换攻击**
- **社会工程**
- **MFA 操作在线页面中的漏洞**

攻击者绕过多重身份验证的示例有很多，也有许多文字记录可循。其中之一就是 2020 年的一次备受瞩目的泄露事件，攻击者结合使用社会工程和网络钓鱼方法绕过了 MFA 解决方案，而当时的受害者如果能使用物理安全密钥，本可避免这次攻击。

低风险

通过物理安全密钥实施 FIDO2 MFA

FIDO2 是目前比较强大的一种基于标准的身份验证方法，填补了传统 MFA 的安全漏洞，消除了网络钓鱼、MITM 和重放攻击的风险。FIDO2 标准由万维网联盟的 Web 身份验证规范和 FIDO 联盟相应的客户端到验证器协议组成。这种身份验证模式成就了 MFA 的未来 - 通过加密的登录凭据进行身份验证，这些凭据永远不会离开用户的设备，也不会存储到服务器上。FIDO2 还支持终极进化版的验证机制 - 无密码身份验证。

不足之处在于，启用 FIDO2 MFA 的唯一方法是为每个用户购买物理安全密钥来用作身份验证因素。

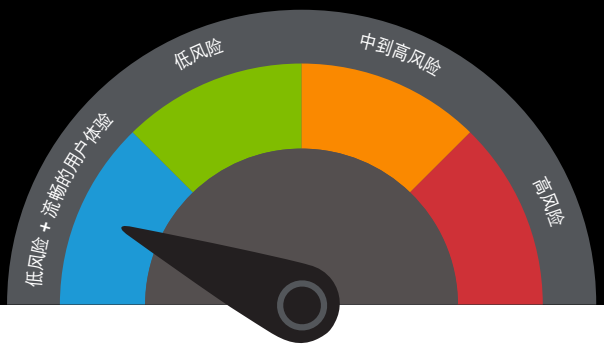
虽然 FIDO2 是一种非常安全的标准，但在通过硬件安全密钥实现时会造成很多挑战。

- **为每个用户购买和维护密钥的费用**
- **密钥分配和管理的复杂性**
- **更换丢失的硬件密钥**
- **无法更新或修补硬件密钥**
- **分配不均 - 只有某些员工能获得密钥**

为所有员工采购、配置、发放和管理物理硬件密钥的成本高、耗时长。此外，如果要求用户每次登录时都要在设备上插入物理密钥，那么就会造成用户体验繁琐，降低用户的使用效率。

低风险 + 流畅的用户体验

在边缘部署的新一代 MFA



Akamai MFA 是新一代的 FIDO2 解决方案，它采用防网络钓鱼身份验证因素，并通过加密技术确保安全。该服务利用智能手机应用程序取代物理安全密钥，解决了经常导致企业无法实施 FIDO2 MFA 的难题。它可以使用现有的智能手机快速、轻松地部署，提供出色的身份验证安全性和流畅的用户体验。Akamai MFA 可消除网络钓鱼的风险，并支持企业最终迈向无密码身份验证的未来。

访问此处进一步了解 Akamai MFA 并开始 60 天免费试用：**akamai.com/mfa**。

来源：

1. https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/
2. https://haveibeenpwned.com/Passwords

Akamai 为全球的大型企业提供安全的数字化体验。Akamai 的智能边缘平台涵盖了从企业到云端的一切，从而确保客户及其公司获得快速、智能且安全的体验。全球优秀品牌依靠 Akamai 敏捷的解决方案扩展其多云架构的功能，从而获得竞争优势。Akamai 使决策、应用程序和体验更贴近用户，帮助用户远离攻击和威胁。Akamai 一系列的边缘安全、Web 和移动性能、企业访问和视频交付解决方案均由优质客户服务、分析和全天候监控提供支持。如需了解全球顶级品牌信赖 Akamai 的原因，请访问 www.akamai.com 或 blogs.akamai.com，或者扫描下方二维码，关注我们的微信公众号。您可访问 www.akamai.com/locations 查找全球联系信息。发布时间：2021 年 03 月。

扫码关注，获取最新 CDN 前沿资讯