AKAMAI 检查清单

Web 应用程序和 API 保护功能检查清单

在规划、实施或优化信息安全策略的同时部署 Web 应用程序和 API 安全解决方案，让您的企业获得理解独有风险、识别安全漏洞和检测威胁的强大能力。您需要的是这样一种 Web 应用程序和 API 保护 (WAAP) 解决方案 - 它能够提供持续的监测能力和综合全面的见解，还具有识别和阻止大部分复杂攻击的全面能力。

这份检查清单可用于评估供应商能力，也可以用作实施有效的 WAAP 解决方案时需要满足的需求列表。

类别 1：平台要求

企业的类型和规模林林总总，并且具有不同水平的需求。您的 Web 应用程序安全解决方案应该灵活、可扩展，并且易于管理。

- [ ] 具备与流量需求匹配的可扩展性，提供持续保护并且不会导致性能下降
- [ ] 架构能够应对跨地域分布式应用程序带来的挑战
- [ ] 具备审核日志功能，以确保合理使用
- [ ] 保护本地、私有云或公有云（包括多云或混合云）源站
- [ ] 能够抵御网络层 [L3/4] 分布式拒绝服务 (DDoS) 攻击，并且提供零秒服务等级协议
- [ ] 在整个平台中融入通过众包模式获得的攻击情报，支持发现攻击者、攻击频率和攻击严重程度
- [ ] 通过端口 80 和 443 提供 Web 流量反向代理功能
- [ ] 利用 SSL/TLS 加密保护网络隐私

类别 2：自适应 Web 应用程序和 DDoS 防护

您的 Web 应用程序安全机制必须超越基于签名的传统检测，采用更加高级的自适应 Web 应用程序和 DDoS 防护，以获得最为精准和可靠的安全效果。

- [ ] 提供基于异常和风险的评分功能，而不仅限于基于签名的攻击检测
- [ ] 具备机器学习、数据挖掘和启发法驱动的检测能力，从而识别快速不断变化的威胁
- [ ] 自动 Web 应用程序防火墙 (WAF) 规则能够根据安全研究人员持续发布的实时威胁情报更新
- [ ] 支持测试新的或更新的 WAF 规则在处理实时流量方面的效果，然后再将这些规则部署到生产环境
- [ ] （至少）抵御 SQL 注入、XSS、文件包含、命令注入、SSRF、SSI 和 XXE 攻击
- [ ] 提供可全面自定义的预定义规则，以满足特定客户需求
- [ ] 能够抵御应用程序层 [L7] 容量耗尽型拒绝服务 (DoS) 攻击，这种类型的攻击会通过递归式应用程序活动造成 Web 服务器不堪重负
- [ ] 完全托管式 WAF 规则，无需持续配置和更新
- [ ] 提供针对个人和共享 IP 地址的客户端声誉评分和情报
- [ ] 提供能快速抵御特定流量模式的自定义规则（虚拟修补）
- [ ] 具备请求速率限制功能，能够抵御自动化或过多的爬虫程序流量
- [ ] 能够抵御指向源站的攻击
- [ ] 通过多个网络列表实施 IP/地域控制，阻止或允许来自特定 IP、子网或地理区域的流量
- [ ] 抵御自动化客户端（例如漏洞扫描和 Web 攻击工具）发起的攻击

类别 3：API 监测能力、保护和控制

API 防护已经成为 Web 应用程序安全的关键部分。您需要具备稳健的 API 发现、防护和控制能力的 WAAP 解决方案，它应该能消除 API 漏洞，减少您面对风险时的攻击面。

- ☐ 自动发现和分析未知和/或不断变化的 API（包括 API 端点、特征和定义）
- ☐ 支持自动检查 XML 和 JSON 请求，从而检测基于 API 的攻击
- ☐ 支持自定义 API 检查规则，以满足特定用户需求
- ☐ 能够预定义可接受的 XML 和 JSON 格式，以限制 API 请求的大小、类型和深度
- ☐ 为 API 后端基础架构提供防护机制，抵御专为耗尽资源而发起的低速缓慢攻击（例如慢速 POST、慢速 GET）
- ☐ 可在 API 级别生成实时警报、报告和仪表板
- ☐ 提供基于 API 密钥的 API 端点速率控制（节流功能）
- ☐ 支持基于 IP/地域的 API 网络列表（允许列表/拦截列表）
- ☐ 带有版本控制的 API 生命周期管理
- ☐ 通过 JSON Web 令牌 (JWT) 验证保护身份验证和授权
- ☐ 支持按密钥（每个独立定义的密钥具有相应配额）定义允许的 API 请求，从而全面掌控用量
- ☐ 使用标准 API 定义（Swagger/OAS 和 RAML）进行 API 初始配置

类别 4：灵活管理

您需要简单且自动化的工作流程来尽可能提升投资价值并提高运营效率。无论是保护全新应用程序、更改应用程序、采用新的 WAF 规则，还是将保护延伸到 API，所采用的流程都必须无缝且直观。

- ☐ 支持开放式 API 和命令行界面 (CLI)，可将安全配置任务集成到 CI/CD 流程中
- ☐ 集成本地和基于云的安全信息以及事件管理 (SIEM) 应用程序
- ☐ 提供完整的暂存环境和实施变更控制的能力
- ☐ 具备能自动适应流量的自行调整式安全防护
- ☐ 包含实时仪表板、报告和启发法驱动的警报功能
- ☐ 具备能访问详细攻击遥测数据并分析安全事件的集中式用户界面 (UI)
- ☐ 提供深度控制能力和/或完全自动化的防护机制，以灵活管理 WAAP
- ☐ 提供完全托管式安全服务，以收缩或扩展安全管理、监控和威胁抵御方面的功能

Akamai Connected Cloud 每天从数百万次 Web 应用程序攻击、数十亿次爬虫程序请求和多达数万亿次的 API 请求中获取见解。这种程度的见解辅以先进的机器学习和威胁研究，让我们可以不断提升能力、捕获新型威胁，并开发创新功能。

如需了解更多信息，请访问 akamai.com 或联系您的 Akamai 销售团队。

扫码关注，获取最新CDN前沿资讯

 | 支持 | 发布时间：2023 年 10 月