ONE ASP RASP

Introduction and The Value of RASP

ONEASP Framework 引言及 RASP 的价值

系统安全防护就像一场枪斗不是你死就是我亡，没有中间的结果，安全专家应该经常问自己这样一个问题：“我们怎么做才能更好的管控风险进而提高产品和企业的生存机会？”。业务线（LOB）应用程序是所有业务的基础，应用层安全至关重要，仅仅做好网络层的安全是远远不够的，安全决策者应当在应用程序的保护上投入更多的精力和资源。

根据 Gartner 的报告，超过 80% 的攻击是以应用层为目标的，而大多数破坏活动是通过应用程序进行的。他们发现，软件提供商对应用程序安全防护的投入普遍不足。Gartner 专家指出“周界安全防护费用与应用程序安全防护费用之比为 23:1”。在一个完美的模型中，开发人员的开发生命周期（SDLC）应当符合安全防护标准，从而开发出安全的软件。在如今的信息社会里，IT 技术日新月异，新的高级安全攻击层出不穷，攻击方式变得越来越隐蔽和致命，同时为适应新的业务需求和技术革新，迭代开发和快速部署越来越流行，比如在“软件即服务”（SaaS）环境中，即使真的找出了问题，也可能无法足够快速地修改和删除不良代码，以阻止实时攻击。现代软件系统通常都很复杂，需要很多程序员一起协助，每个程序员的代码能力不一样，并且通常还会有很多遗留代码或者使用第三方程序，通过修改代码的方式来完全解决漏洞问题基本上不可行。提高程序安全性需要投入大量的时间和资源，在快速迭代和快速部署的模式下，安全需求往往会被迫为快速上线让路，带病上线是非常常见的事情。

应用程序安全测试（SAST/DAST/IAST）也是一种能够比较有效的防止安全漏洞进入生产环境工具，但即使最成熟的应用程序安全测试工具也不可能捕获所有漏洞。况且，找出漏洞只是第一步，只有修复所有漏洞才有意义。在大型项目里修复所有漏洞是所有程序员的噩梦，不仅需要花费大量的人力，同时也可能大大延迟开发和发布的进度。这是无法承受的代价。

现在网络层保护技术（如 NGFW、UTM、IPS、IDS 等）已经成为大部分企业的标准配置，一些应用层保护技术（WAF 等）也逐步得到应用。这些技术的确在一些场景下能够部分保护企业安全，但是在云时代网络边界越来越模糊，很多情况下企业都不清楚应用程序具体部署在什么地方，同时黑客对防火墙技术已经非常熟悉，翻墙技术也已经非常成熟。传统安全防护技术对于新一代威胁是无能为力的。使用自适应应用安全防护技术应对新型安全威胁是非常必要的。

部署 OneRASP 能以最小代价并且快速解决上述难题，你只需要非常简单的修改一下 JVM 的启动配置，就可以将安全保护代码像疫苗一样注入应用程序，瞬间修复已知漏洞，使所有代码变成安全代码，任何攻击都无法绕过，它能全面洞察应用程序的逻辑、配置、数据和事件流，使应用程序能够保护自己，免遭通过运行时环境实施的网络攻击。OneRASP 拥有应用程序内部的上下文，不只是监控威胁，它还会采取措施来实时阻止攻击，它是一种从根上解决安全问题的有效方案。同时 OneRASP 采用先进的漏洞库实时升级方案，最新的漏洞通过实时升级系统快速部署到应用程序里，让应用程序免受最新威胁攻击。

最优的解决方案是将 OneRASP 和网络安全解决方案、应用安全扫描与测试等安全防护系统结合起来，形成多层次立体的防御体系，如今各种攻击手段层出不穷，单靠其中任一技术来防范应用程序的安全是不科学的。但 OneRASP 永远是应用程序安全保护的最后一道无法逾越的壕沟，它可以帮你快速提升应用程序的安全级别，你再也不用担忧没有合格的安全程序员了，当然也确保你的组织不会作为下一个安全受害者而登上头条。