中小企业网站最容易遭遇网络攻击

HelpNetSecurity 网站于 2022 年 1 月 12 日发表的文章《中小企业仍然很容易成为网络犯罪分子的攻击易目标》指出：对于中小企业，网络犯罪仍然是一个主要问题，51%的中小企业经历了网络攻击，因为中小企业缺乏资源，无法向大企业那样能在网络安全方面投入。在没有采取网络安全防护的受访者中，成本是造成这种情况的主要原因，11%的受访者表示他们不会在网络安全上花费任何费用。88%的企业至少有一种形式的网络安全防护（如防病毒、防火墙或多因素身份验证）。遭遇网络攻击的后果可能对小型企业造成毁灭性打击，这些企业可能无法从网络漏洞的财务影响中恢复过来，或者会失去客户的信任。

这篇文章虽然是针对国外中小企业的调查，其实也非常适合于我国的中小企业的情况，在目前这个大环境下，中小企业能活着不倒已经很不容易了，所以，中小企业主会认为“我的网站没有什么可以偷的”、“我这么小的公司网站不会引起黑客的注意的”。其实不然，黑客完全可以使用自动化工具找到没有任何防护的网站并自动植入木马，让你的网站成为“肉鸡”，成为攻击其他系统的“打手”而被动违法，这就是为何中小企业网站最容易遭遇各种网络攻击的主要原因，如：网站被植入木马、网页篡改、SQL 注入、拖库和邮件欺诈等。据国家互联网应急中心发布的报告，2020 年我国境内 53,171 个网站被植入后门，这些攻击不仅会影响网站的正常访问和泄露网站数据，而还面临《网络安全法》的合规压力，可能会收到行政处罚。怎么办？

(C) 2022 零信技术（深圳）有限公司

零信网站安全云服务是一个集网站 https 加密、WAF 防护和可信认证于一体的网站安全解决方案，不仅能有效解决明文传输泄密问题、解决网站被攻击问题和网站被假冒问题，而且是全自动实现，并且是支持中小企业常用的虚拟主机网站，不需要有自己的独立服务器，不需要在服务器上安装 SSL 证书或者安装其他客户端软件，只需做两次 CNAME 域名解析就可以全自动实现三位一体的网站安全防护，其中云 WAF 防护由业界领先的阿里云 WAF 提供服务。

最重要的是，这个三位一体的网站安全防护服务的费用是中小企业负担得起的，并且可以按月购买，花很少的钱就能满足《网络安全法》合规要求，不用担心网站被攻击，不用担心浏览器会显示“不安全”，可以放心地全力做好自己的业务，这才是中小企业所需的能负担得起的普惠安全服务。

王高华

2022 年 6 月 6 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。

(C) 2022 零信技术（深圳）有限公司