网站被入侵，违法了，怎么办？

标题中的这个“违法了”是指网站业主违法了，违反了《中华人民共和国网络安全法》。可能有些读者就糊涂了，我的网站被入侵，我是受害者，怎么是我违法了呢？没有错，入侵者当然是违法了，但是网站业主没有履行安全保护义务也是违法了。今天是《中华人民共和国网络安全法》实施 5 周年纪念日，也是我公司的网站安全云服务上线的好日子，笔者特撰文讲一讲《网络安全法》中涉及到网站安全的有关条款。

根据国家互联网应急中心(CNCERT)发布的 2020 年《中国互联网网络安全报告》，2020 年我国境内 53,171 个(5 万多)网站被植入后门，其中政府网站有 256 个。这个数据是在《网站安全法》施行后的第 3 年的数据，仍然有 5 万多网站被入侵，其中还有不少政府网站！我们再看看今年 4 月份的一周数据，CNCERT 监测发现境内被篡改网站数量 3611 个；被植入后门的网站数量为 738 个。其中被篡改的政府网站有 17 个，被植入后门的政府网站有 12 个。可以看出：网站后门量有所下降，但网页篡改量比 2020 年周平均量几乎翻了一倍，两年后的今天形势不但没有好转，而且还更加严峻，并且仍然有不少政府网站被植入后门和网页被篡改。

大家应该从这些数据中可以看出我国网站安全的态势是不容乐观的，可以说是非常严峻的。所以，笔者认为加强《网站安全法》的宣传很有必要和很重要，当然，更重要的是得提供解决方案，提供更多更好的用户用得起的保护用户网站安全的产品和服务，本文就从这两个方面给大家指明一条捷径，花很少的钱规避违法风险。

《网络安全法》第二十一条明确指出：网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，必须采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施，采取数据分类、重要数据备份和加密等措施，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

这里有两点要求：一是必须采用防止网络攻击和网络侵入的安全防护技术措施，二是重要数据必须加密。我们再对照一下零信网站安全云服务提供的服务 - https 加密加 WAF 防护加可信身份，也就是说，只要选购了零信网站安全云服务，就可以满足《网络安全法》的两项网站安全防护技术措施要求，其中要求的网站入侵防护由全球领先的云服务提供商阿里云 WAF 提供，不仅能满足合规要求而且确实能保护网站安全，让网站业主可以专心做好自己的业务而不用担心网站可能被入侵而违法！而 https 加密就是全自动实现了重要数据的传输加密，保证了重要数据不会在浏览器到服务器的传输过程中被非法窃取和非法篡改，有效防止数据泄露。

既然有法律在，为何还有那么多网站被动违法了呢？让我们再看看《网络安全法》第五十九条，网络运营者不履行上述的第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。也就是说，这个违法成本比较低，只是要求改正和给予警告。更何况，更多的情况是网站业主自己根本就不知道自己的网站被入侵了，执法部门也不知道，甚至是忙不过来也顾不上这些网站的入侵事件，除非造成了恶劣的社会影响，那就要顶格罚款 10 万元了。

现在我们应该能理解为何阿里云 WAF 产品页宣传“阿里云 WAF 满足等保合规需求”了，有了云 WAF 的防护，网站入侵挂马和篡改等安全问题都统统没有了，满足了《网络安全法》第二十一条的要求，满足了等保合规要求。也即是说，网站业主为了合规守法，需要购买云 WAF 服务实现安全防护和购买 SSL 证书实现 https 加密，这些都是要费不少钱的，一年少则上万多则几十万，这个合规成本太高，以至于只能任其网站有被入侵的风险和不管是否有可能犯法。这又是另外一个层面的问题，一方面要合规，另一方面是合规成本太高的问题。怎么办？

怎么办？选购零信网站安全云服务，一个用户负担得起的、全球顶级品牌 SSL 证书加顶级云 WAF 防护的包年收费服务，保网站一年安全，满足网站安全合规要求，实现网站安全防护和网站传输加密，并且只需在申请时只做两次 CNAME 域名解析即可，不用花大价钱购买阿里云 WAF 服务，但是享受阿里云 WAF 防护，不用找 CA 申请 SSL 证书，但是享受 https 加密服务。

零信网站安全云服务是一个把阿里云 WAF 和全球信任的 SSL 证书打包的一个全自动实现 WAF 防护和 https 加密的创新服务，不仅大大降低了网站安全合规成本，而且也是最重要的，保护了网站重要的数据安全，保障了网站业主的正常业务顺利运行。合规是一方面，保护自己的重要业务数据更重要！欢迎选购零信网站安全云服务，尽享 365 天网站安全无忧！

王高华

2022 年 6 月 1 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。