网站安全的三大误区

最近同多个政府网站的主管和多个企业老板聊过他们的网站没有部署 SSL 证书是不安全的话题，普遍认为网站没有什么内容需要加密，不能理解为何显示一些公开的供用户浏览的信息的网站，所有浏览器非要警告为“不安全”，都一致认为这是浏览器厂商或者 SSL 证书厂商在吓唬用户，目的是为了推销 SSL 证书。甚至有的主管说我们网站都通过了某某权威测评，都过了等保三级了，怎么就不安全了？怎么还违法了？

从用户角度来讲，视乎大家都说得很有道理，但是从网站安全专业人士的角度来讲，这些观点都是错的，但是我们不能怪用户，这是我们的科普工作做得很不够，所以，笔者动笔写下了这篇博文，希望真正关心自己网站安全的主管和业主能耐心看完本文，一定会有收获，只有网站安全了，才能安心做好自己的业务。

第一大误区：网站没有任何需要加密的内容，不需要部署 SSL 证书加密

目前地市和县区级政府网站一般都只剩下显示一些本市县区的本地信息发布和本地特色介绍的内容了，真正需要用户登录和输入机密信息的电子政务系统都已经划归到省政务服务网统一管理了，本地政府网站只需**链接**到相应的省政务服务系统即可，至于省政务服务网站是否部署了 SSL 证书实现了 https 加密已经不属于本市县区的管辖范围了。这是现实也是实情，从这个角度来看就不难理解为何大家都认为不需要 https 加密了。但是，从网站安全专业角度来讲，有三大理由仍然需要 https 加密。

理由一：防止网页篡改和非法盗链

市县区级政府网站的确只有公开披露的信息，的确没有登录页面需要加密用户名和口令，但是有大量的链接到省政务服务网的链接，如果网站没有 https 加密，则攻击者(包括所有 Wi-Fi 提供商)都可以非常容易地篡改网页上的链接把用户引到一个假冒政务服务网站，从而非常容易获得用户在省政务服务网的用户名和口令。相信这不是本地政府网站希望看到的结果，这些不采用 https 加密的市县区政府网站成为了省政务服务网站安全的危害者！这就是为何我多次呼吁为何省政务服务网主管机构应该强制要求下面的市区县官网也必须实现 https 加密的原因。

理由二：保护网站访问者的用户隐私

这个理由我是十几年前从谷歌官网看到的，谷歌在推出搜索服务时就讲了为何搜索页需要 https 加密，保护用户隐私，如果不加密，则用户搜索什么关键词，则非常容易被非法获取这些信息，可能用户正在搜索一个非常隐私的需要找到解决方法的问题，如果搜索网站不加密，则其他人能知道他/她正在搜索什么和点击了哪个搜索结果，这就暴露了个人隐私，是不是很可怕？

市县区政府网站虽然都是可以公开浏览的信息，但是上网浏览的用户不希望无关人员知道他/她正在浏览什么内容，这就是需要 https 加密。市县区政府网站理应依据“**人民至上**”的原则实现全站 https 加密来保护人民上网行为的个人隐私，让本市县区市民能放心地浏览本地政府网站的信息，增强人民群众的安全感和幸福感。

理由三：消除所有浏览器的“不安全”警告

所有浏览器对没有实现 https 加密的网站提示“不安全”绝对不是为了推销 SSL 证书，而是因为笔者在上面讲到的的确不安全。如果上面的两个理由还不够的话，那就为了“面子”工程，也应该解决浏览器提示网站不安全的问题，用户上网时看到浏览器提示“不安全”，用户对这个网站的第一印象一定不会太好，一定不敢多看，除非实在没有办法。

而消除浏览器的“不安全”警告的唯一方法是网站采用 https 加密访问，网站部署 SSL 证书或者使用云 WAF 防护都可以实现 https 加密，所有浏览器都会显示加密锁标识，不会提示不安全。目前市场上有免费 SSL 证书，有非常便宜的收费 SSL 证书，都可以解决问题。如果不想动网站，不想费力去申请 SSL 证书和部署 SSL 证书，可以选购网站安全云服务，需要做 3 次域名解析，把原网站变成 WAF/CDN 的源站即可自动实现 https 加密和云 WAF 防护。

第二大误区：我这么小的一个企业网站，没有任何值得攻击的信息

这个误区是很多企业老板的想法。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，中小企业主都会认为“我的网站没有什么信息可以偷的，不需要加密，不需要防护”、“我这么小的公司网站不会引起黑客的注意的”。所以，大量的中小企业网站都没有部署 SSL 证书，都是 http 明文访问，也没有任何其他安全防护措施。

其实不然，一个网站如果没有任何防护措施，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，其中政府网站有 256 个！这些攻击不仅会影响网站的正常访问，而且还面临《网络安全法》的合规压力，可能会收到行政处罚。

怎么办？需要 https 加密和云 WAF 防护，https 加密可以防止明文传输时被非法修改代码和非法植入攻击链接，而云 WAF 防护则可以实时阻止各自攻击，有效保护网站的机密信息安全和企业宝贵的用户数据和经营数据安全。

根据 Gartner 的 2021 年报告预测：到 2024 年，也就是 2 年后，70%的组织都会为 Web 应用实施云 WAF 防护，因为现在的网站攻击已经成为了常态，与网站大小和网站是否有有价值的数据无关。为了保护企业的宝贵数据和网站的正常可靠运行，推荐选用网站安全云服务，一键实现 https 加密和云 WAF 防护，让网站主能放心和专心地做好自己的业务而不用为网站是否能正常运行而操心。

第三大误区：只有登录页面才需要加密，其他页面不需要加密

这个问题为何排在第三位，并不是说这个问题不重要，是必须先讲清楚网站为何需要 https 加密。这个问题的用户是已经为用户登录页面实现了 https 加密，但是用户认证通过后的网站又变成了明文 http 网站了，这在不少政府网站、政务服务网站、高校网站和电商网站也常见到。

首先需要肯定和表扬的是用户登录认证页面使用了 https 加密，这能有效地保证用户输入的用户名和口令的加密传输安全。但是，用户认证通过登录系统后更应该加密，因为登录后的系统才是最重要的有需要保护的核心数据，有用户的个人隐私信息，有各自订单信息和收货地址等等，这些重要数据是企业的核心资产，怎么能不加密保护呢？如果含有这些重要数据的页面不加密，黑客更不不用攻击用户登录认证系统，直接侦听用户登录后的数据包即可，根本不用攻击就可以轻松获取政府网站和企业网站的重要机密数据。

下图是笔者在十几年前使用的全站 https 加密的宣传图，现在仍然适用，因为现在还有许多网站只是在登录页面实现了 https 加密。全站 https 加密能有效防止中间人攻击，防止重要机密数据泄密和流失重要的宝贵的客户资源信息，必须高度重视。

最后，笔者总结重要的两点：

(1) 所有网站都必须实现 https 加密，无论网站大小和网站主单位性质。

(2) 实现 https 加密并不一定要自己动手改动服务器，可以选用云服务，一键轻松实现 https 加密和云 WAF 防护，多方位保障网站安全，并同时满足《密码法》和《网络安全法》的合规要求。

王高华

2022 年 12 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。