Symantec | 网站安全解决方案

Norton SECURED powered by Symantec

赛门铁克指南：
通过建立客户信任度增加网上销售的五种方法

目录

通过建立客户信任度增加网上销售的五种方法

通过建立客户信任度增加网上销售的五种方法

每天，消费者都要面对关于企业数据泄露、黑客攻击大型零售商获取信用卡信息、国家支持的网络攻击、OpenSSL 中的 Heartbleed 漏洞等源源不断的新闻报道。难怪他们会对电子商务心存顾虑。

幸运的是，企业仍然可以在潜在客户中建立信任。他们要做的是显示他们清楚地认识到客户对隐私的顾虑，并已采取控制措施保护客户数据。企业可采取多种使用安全套接字层 (SSL) 证书的关键方法，以赢得客户的信任。

用来保护客户数据的安全控制显然是必要的，特别是互联网通信的端到端加密。除采取安全控制之外，明确显示这些控制措施已经就位也至关重要。SSL 技术是五项安全控制重要措施的基础，并提供证据显示这些控制已经就位。

五项推荐措施分别为：

1. **防止第三方查看通信**
2. **降低客户数据泄露的风险**
3. **在所有 Web 访问服务器上提供 SSL**
4. **显示验证身份**
5. **使用由安全防护领导者提供的 SSL 证书**

这五项措施共同表明了积极保护客户数据的承诺，并为在线通信和电子商务建立了必要的信任。

第 1 步

防止第三方查看通信

为防止第三方监控通信，您需要为浏览器与 Web 服务器、服务器与服务器之间的数据传输进行加密。如果有人能够拦截客户与其中一台服务器之间的数据传输，那么他们获得的将是杂乱无章的随机文字。

例如，一封电子邮件的内容为：

“附件是战略计划的最终草案。请勿传阅。”

它将显示为：

M0niJp2vfKd0ikGzGZW+fTwiH0DHakfhIpOcIwZ Scr5LnTZbDe/hckFRS6x9jaNWS3+ZAI
CYzPk0ESRZTryIt6zfwjxMdu9XQ9Imsq6TP6TO6yQE5F/GnYjjCJQ3vfYQk92/VmdR0vMP
ZhKC7ZvTgLhZzDySxUHGCUZYGhSk6F6c2bMLDkp9GoPPoG7Ig9Z9ig8OEg/4CuNmxIp
CG/Vec6kISRhI4AJdUrZf+i1Z2H2vmFXti40gwJpwu7YgRPG2qPkh6+7txWt8I3CVriofLW9
YgAHDtxfQC4J53Q/sMz0URPT0or6hGw1hagrLd9SJfYxeYnQqLIPgoIYw7mU4Z22Fjb+hou
BcXxyHgHrQ4vMLTaX8TzJB0hzO1OWHB/1toHbPV4b4TTqkK3k0gMN/sUFTTLxPqDSX+
wIIloRZ0hE8h4QVF25PIar58fPO8/PqUSugfpSDMY9bQgQA==

SSL 证书让客户无需采取任何行动，即可进行加密。对 SSL 的支持遍见于当今的浏览器，因此客户使用的浏览器普遍支持它。

第 2 步

降低客户数据泄露的风险

除了对在您的服务器和客户浏览器之间传输的动态数据进行加密之外，您的数据中心内静态的私人及机密数据也需要加密。

为静态数据加密的原因是攻击者可能会破坏其他安全防御，并访问您的服务器。倘若出现这种情况，攻击者可能会有权访问私人及机密数据。如果数据被加密，那么它对攻击者将毫无用处。

当一条加密信息或一个加密文件被入侵时，其他文件也被入侵的风险会上升。在加密时，将此风险降到最低尤为重要。为解决这个顾虑，密匙生成软件最重要的性能是完全正向保密。在每次会话中生成随机公共密匙时，完全正向保密在加密系统中提供，并使用非确定性算法计算这些密匙。建议使用支持完全正向保密的加密系统。

第 3 步

在所有 Web 访问服务器上提供 SSL

IT 部门是动态的。服务器配置并非一成不变，网络也会重新配置，并且各种设备在网络中增减不断。

此外，虚拟化及云计算让实现或破坏虚拟机易如反掌。确保企业服务器可靠性的其中一种方式是通过 SSL 证书保护同一域内的所有服务器。

第 4 步

显示验证身份

创建看似合法的虚假网站对攻击者来说相当简单。欺诈网站可诱骗用户提供登录凭证、个人信息或其他对攻击者有用的信息。为了帮助证明网站的有效性，SSL 证书供应商创建了扩展验证 (EV) 证书。

比起传统的 SSL 证书，EV 证书需要额外的验证步骤。只要按照 SSL 证书应用的要求提供了有效的电子邮件地址，有些服务级别较低的 SSL 证书提供商就可能会提供证书。对于低风险网站（如个人网站），这种安全级别可能已经足够，但商业网站需要更加严格的验证程序。

EV SSL 证书以清晰的视觉提示表明网站的正当性，如浏览器地址栏显示为绿色。如图 1 所示，它还提供更多信息。

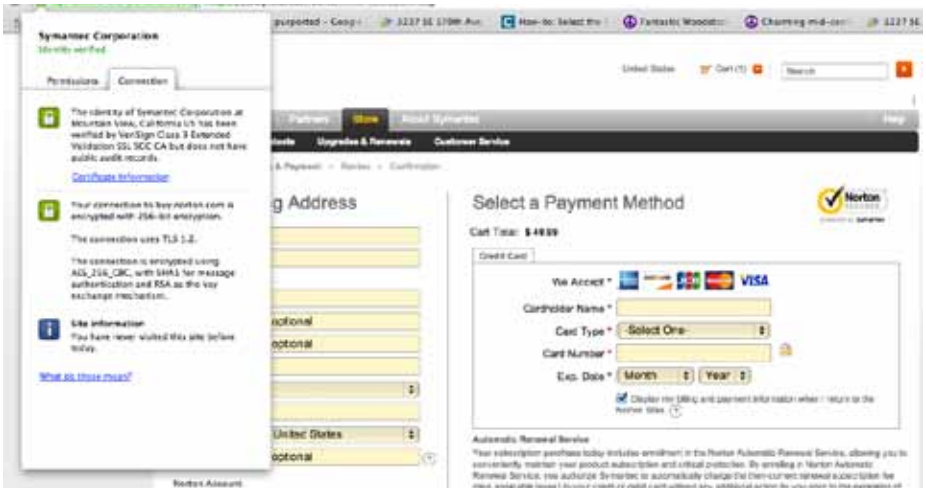


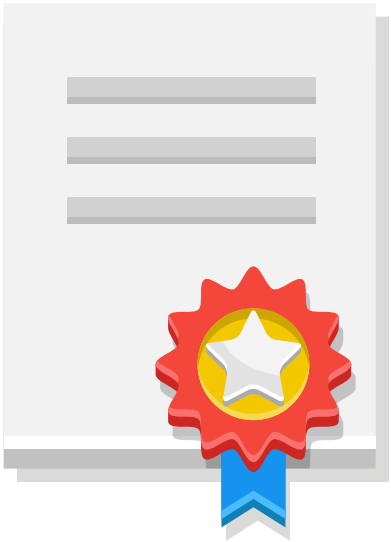
图 1：扩展验证证书表明这家企业采取了比通常所需更严格的验证程序

第 5 步

使用由安全防护领导者提供的 SSL 证书

本质上来说，SSL 证书供应商保证了 SSL 证书持有者的真实性。

除了生成和分发证书之外，提供 SSL 证书还有更多工作。供应商必须保护它们的基础设施和证书信息。不幸的是，有些 SSL 供应商已遭入侵。使用知名度高、备受推崇并遵循最高级别的验证方法的供应商提供的证书极为重要。



建立信任度

公众关注隐私和数据泄露，这无可厚非。

通过部署现有安全控制（包括基于 SSL 的控制措施），并表明积极保护客户利益的承诺，企业可建立客户的信任。这五项措施有助于充分发挥 SSL 在建立并维持这一信任的作用。

关于赛门铁克

Symantec Corporation（纳斯达克：SYMC）是信息保护领域的专家，帮助个人、企业和政府随时随地自由探索技术所带来的机遇。赛门铁克成立于 1982 年 4 月，作为一家财富 500 强公司，运营着全球最大的数据情报网络之一，为重要信息的存储、访问和共享提供一流的安全、备份和可用性解决方案。公司拥有 20,000 多名员工，分布在 50 多个国家。99% 的财富 500 强公司是赛门铁克的客户。在 2013 财政年度，赛门铁克的营收为 69 亿美元。要了解更多信息，请访问 **www.symantec.com** 或登录 **go.symantec.com/socialmedia** 与赛门铁克联系。

Symantec | 网站安全解决方案

Norton SECURED
powered by Symantec

如需了解特定国家或地区的办事处
和联系电话，请访问我们的网站。
有关亚太地区的产品信息，请致电：

澳大利亚：+61 3 9674 5500
新西兰：+64 9 9127 201
新加坡：+65 6622 1638
香港：+852 30 114 683
台湾：+886 2 2162 1992
或发送电子邮件至：ssl_sales_au@symantec.com
ssl_sales_asia@symantec.com

赛门铁克
Symantec Website Security Solutions Pty Ltd
3/437 St Kilda Road, Melbourne,
3004, ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates