12
December
2009

This Issue

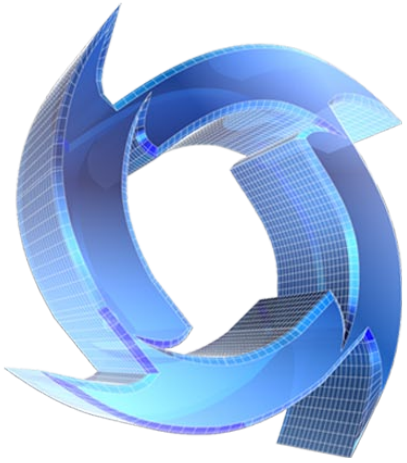
digicert®
Your Success is Built on Trust™

SSL Year in Review

DigiCert Strong Amidst Malicious Tactics

The SSL and TLS protocols remain proven as the best methods for encrypting the transfer of sensitive information. Though new attacks surfaced in 2009, DigiCert's vigilance and foresight have allowed it to remain a stalwart among SSL Certificate Authorities.

At the beginning of January, the MD5 Algorithm was shown to be vulnurable to a new collision attack. Through the use of a strong computer network, rogue organizations were able to create signed, trusted SSL certificates for a domain of their choosing from Certificate Authorities using this algorithm. Because DigiCert uses the stronger SHA-1 encryption algorithm, its customers were unaffected by this vulnerability



In February, SSLstrip, was released during the Black Hat conference in Washington D.C. Designed to remove SSL using advanced man-in-the-middle techniques, the tool did not represent a weakness in SSL, but rather took advantage of users who do not look for trusted markers such as the lock symbol in a browser's interface. DigiCert's Extended Validation certificates proved to be an effective countermeasure by showing the "Green URL Bar."

In March, special attention was given to the US National Institute of Standards and Time (NIST) recommendation to use 2048-bit keys after 2011. DigiCert's trusted roots comply with this recommendation.

In July, the Null Character attack vector was demonstrated. By inserting \0 in the common name field for wildcard certificates, a rogue organization could

Continued on page 2

Win an XBOX 360 or Wii

Today marks the last chance to win a microsoft XBOX 360 or Nintendo Wii by participating in the DigiCert customer survey. To be eligible, you must be a DigiCert customer and participate in our survey found at http://www.digicert.com/survey.php. Please give us your honest opinions and be sure to include your contact information.

The winner will be chosen at random today, December 10th, 2009. Terms and Conditions can be found at https://www.digicert.com/survey-drawing-terms.txt.

Holiday Online Retailing Tips

Wary Shoppers Buy From Trusted Retailers

By: Travis Tidball, VP of Sales & Marketing

With a rise in technology adoption amidst a difficult economic climate, analysts forecast 2009 to have upwards of 20% more shoppers online. However, the average spending per shopper will decrease significantly from past years. What does this mean for online retailers?

Since buyers are more discriminate in their spending, the most successful online retailers are those that positively separate themselves from the competition. Building trust online is a powerful way to reassure timid buyers and establish your business as a leader in your industry. Here are some tips for making the most of the opportunity:

- Implement an Extended Validation SSL Certificate. The "Green URL Bar" provides your customers a visual cue that not only is your site secure, your identity has been confirmed as well.

- Add the DigiCert Site Seal above the "fold" of your site. Users can click on the seal to receive confirmation from www.digicert.com about the steps we performed to verify your identity.

- Avoid SGC certificates. Although they enable older browsers to connect with strong, 128-bit encryption, they encourage the use of software that is inherently dangerous. Older browsers that need SGC typically have critical security flaws and enable malicious software to fraudulently obtain sensitive data. A better option is to simply force 128-bit encryption through your server software settings. (If you don't know how to do this, contact DigiCert support at +1-800-896-7973 or support@digicert.com and we will be happy to help.)

- Set, publish, and follow strong privacy policies. Users may be happy with your products or service, but unwilling to buy if they aren't sure their information will remain safe after the sale.

These steps will help your online business build lasting trust with your customers.

"SSL Year in Review" Continued

by Travis Tidball, VP of Sales & Marketing

obtain a trusted certificate for any domain.

Between DigiCert's automated checks and validation done by real people, there was never any chance that such certificates would be issued by DigiCert.

In 2009, DigiCert also sponsored two events - the Giving of the Green student donation fund and the Online Trust Summit. Both events educated and promoted online awareness and trust.

DigiCert looks forward to demonstrating in 2010 why it remains the best value in SSL with a continued focus on security, new features, and fantastic support.

Support Pages Available for Exchange 2010

By: Bart Mensinger, Senior Manager of Content Optimization

As the dust settles around Microsoft's recent release of Exchange 2010, users are recognizing significant differences from Exchange 2007, including the return of a graphical user interface for SSL certificate installations (though powershell is still available for those who prefer).

DigiCert is pleased to announce that full support instructions are available online at http://www.digicert.com/security-certificate-support.htm, including screencasts with step-by-step implementation instructions.

Be sure to contact DigiCert support if you have any questions with your Exchange 2010 server at +1-800-896-7973 or support@digicert.com.

Feedback? Article Suggestions? We want to know! Send an email to newsletter@digicert.com

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
+1-866-842-0223 fax
www.digicert.com