fasthosts ProActive

Google's proposal

to shorten lifespan of TLS certificates

Whether you know it or not, you're using certificates on the internet every day. From browsing your favourite news sites and logging into social media to scoping out new clients online.

We've all been told to take precautions to make sure our data is secure so no one can 'snoop' on it as it transits the multitude of cables and servers that connect you to your bank or online merchants. One of those protections is the 'padlock' in your browser search bar. It being there shows that when you use the site you're visiting, your data is encrypted to a high-enough standard, and that the website owners and hosting can be trusted.

What are TLS certificates?

You might already know the ins and outs of digital certificates but let's recap. Transport Layer Security (TLS) certificates, also known as Secure Sockets Layer (SSL), are essential to securing internet browser connections and transactions through data encryption. TLS/SSL is the standard security technology that works behind the scenes to keep your online transactions and logins secure.

Without getting too technical, TLS/SSL use a public and private key system for data encryption and data integrity. Public keys can be made available to anyone (hence the term public). Because of this there's a question of trust, specifically how do you know a particular public key belongs to the person/entity that it claims to be? For example, you receive a key claiming to belong to your bank. How do you know that it does indeed belong to your bank? The answer is in a digital certificate.

Certificate authorities issue TLS/SSL certificates with an expiration date. The life span of these certificates has been shrinking over the past few years, since frequently cycling them makes it harder for attackers to use fraudulent certificates.

Google's proposed plan for TLS certificates

Google have suggested a new expiry period of just 90 days, and as the most commonly used browser, they have the clout to 'make it so' without getting the normal consortium or browser makers, certificate authorities and other stakeholders all aligned.

So, what does this mean?

The impact goes beyond browser makers and certificate authorities because organisations will need to renew their digital certificates more often. If you've ever come into the office in the morning and found something isn't working because the 'browser says no', you've probably had the facepalm moment where you've realised that a certificate has expired.

Certificate replacement, if handled manually, can be like performing open heart surgery because it involves identifying certificates about to expire, getting new ones issued, revoking the old ones, and deploying the new certificates. Having to do this 4 times a year is going to become an arduous task considering most businesses have many certificates and that number is growing rapidly.

That's why Fasthosts ProActive have our Certificate Management managed service. It's all about removing the stress of expiring certificates and making sure certificate changes are seamless, whatever the tech giants decide to implement.

Curious to know more? Learn about our services and get in touch today to have a chat with one of our experts.