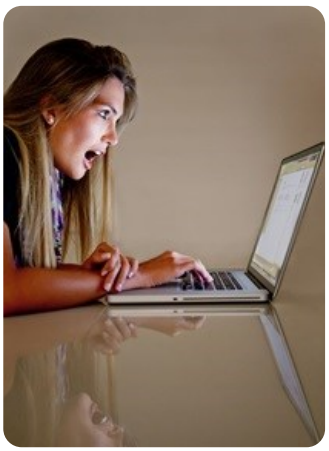
BIZCOMMUNITY

How context can provide application-centric security

Despite the innumerable terrible headlines we've seen over the last few years, data breaches continues to dominate the security space. Mobile firms, hotel chains, government bodies, dating websites, retailers and more are all targets.

By Martin Walshaw 30 May 2016



©Andres Rodriguez via 123RF

Names, email addresses, physical addresses, credit card information, passwords, social security numbers... just about ar personal, identifiable and sensitive information you can think of fall into the hands of hackers. As well as the material impa they can cause on the businesses that fall victim to hackers - such as the resulting compensation payouts - these attacks can also have a huge impact on a company's brand. How many people will happily return to a business knowing that it ma not be able to adequately protect their data?

Data gateway

Now, I'm not going to comment on the security in place at the companies involved with these breaches, but instead I want talk more generally about why attacks are becoming more common and more successful. Ultimately, it's a reflection of the changing way businesses operate, and security practices and processes that have to adapt to keep companies secure.

It's the applications themselves that are the targets, because that is where the data is housed. Applications are a gateway the data, the door that lets the hackers in. As businesses get more mobile and more cloud-based, these applications conta larger amounts of data, becoming an even greater target for cyber attackers.

Also, applications have historically resided in the data centre. As a result, this is where the perimeter and primary cyber defences have been set up.
However, because of the rise of mobile and emergence of the cloud, the data centre isn't always the most vulnerable area these days.

The proposed approach would be to think about security within the following four pillars:

1. Organisations are moving to the cloud
2. Growth in BYOD and remote/mobile workers
3. Prevalence of SSL, resulting in many security applications being blind to encrypted traffic and threats hiding within
4. More sophisticated security threats.

All of these, and the fourth one in particular, mean the perimeter approach is no longer adequate. Instead the perimeter ha to be the application itself, wherever it resides. It's almost like security is reverting back to its baseline design principles, b one that has a solid foundation that should help businesses fight even the most advanced threats.

The key is context

The key to application-centric security, and to dealing with the complexities that those four elements listed above bring, is context - context of the user, the traffic, and the application. Context = knowledge = power ... to borrow and expand on a famous phrase.

Let me give you an example I recently heard and adopted from a colleague, of what is meant by context. Look at toll roads In some countries there is nothing more than a machine you throw some coins into, then you drive a few miles and throw some more coins into another machine. That system has no understanding of its users - where are they coming from? Where are they going?

In contrast there are more sophisticated toll roads, such as those in South Africa, that are monitored by cameras or ticket that follow users. So the system knows where the driver has been and where the driver is going and more. That gives the organisation supplying the service much more context that can be used for marketing or security, for example.

But how is that relevant to an organisation? Well, context around the user, the data traffic and the application - such as wh client platform the connection is being made from, where it is geographically located, what browser is being used, what protocols are being used, what application is being accessed - enables the organisation to see anything and everything th goes on between the user and the application.

So going back to the 'context = knowledge = power' equation, if an organisation understands what's coming its way, it has the ability to take the right action.

To protect an application you have to understand the application, and that is done through the contextual awareness mentioned above. Focusing security efforts on applications is an effective way of stopping security threats. It can also pro to be more cost-effective, because you can assign protection based on the value the app has to the business, instead of trying to protect everything equally.

Protect the application, wherever it resides, and you'll protect the business as a whole.

ABOUT MARTIN WALSHAW

Martin Walshaw is a senior engineer at F5 Networks and has multiple accreditation from being a CCIE to being a CISSP to being an F5 Certified Professional. His background is in securi but he has also has skills in multiple different areas including unified communications, application acceleration and optimisation.
View my profile and articles...