F5 Forum London 2013: Preston Hogue and the importance of Context in a changing threat landscape

Nick B, 2013-06-03

Preston Hogue is a globe-trotting security expert at F5. We were fortunate that he was able to come along to F5 Forum and TechXchange in the UK, which took place at Chelsea FC's West Stand.

Context runs through what F5 offer in the security space as well as in the broader application delivery sense. We focus on two major trends – mobility and access, and securing the data centre. Preston focused on the latter.

Challenges include BYOD, mobility, Web 2.0. Every app that is being developed right now is web-enabled, making this latter challenge the most pressing one. Web 2.0 security concerns makes deploying Siebel or a helpdesk in the cloud (just as two quick examples rather than anything inherently wrong in these apps) incredibly time-consuming. Years in some cases.

Another defining characteristic of the Web 2.0 environment is how dynamic it is. Look at all the updates you get to apps on your iPhone for everyday proof. Look how often websites are updated, especially those that are social media enabled.

Agility has become absolutely essential. But agility doesn't really lend itself to threat modelling. This, and an expanding network perimeter, make for some specific security concerns when attempting to protect applications. When you consider that some single applications represent a huge proportion of a company's revenue, this problem becomes acute.

Factors like lack of regulation in emerging countries, vast spam networks and botnets, and hackers evolving into sophisticated organisations that can call on many more people to target geopolitical events like the Arab Spring mean the average threat spectrum is vastly different compared to a few years ago.

Social media is a part of this – an enabler of hacker collaboration, changing the way they communicate just as it has done for most of the rest of us.

F5 are in a good place to address these things. Ask your security vendor about if they provide three crucial levels of context. The first is the ability to know about the client (what browser, what OS, what kind of device?) accessing your web app. The second is understanding what the attacks are. The third is having some awareness of what is being protected. The answer, by the way, is 'the application', but not all network-focused security technology will know this, let alone if it is being effectively secured.

F5 have always been able to give you this context, because we are application-aware and have always focused our business on delivering this context in order to deliver applications securely, quickly and making them highly available. It is crucial that we knew these things.

So it becomes much more understandable that F5 are now talking up how we compliment traditional network perimeter-focused technology. The world has changed, in threat terms, and context is is incredibly important as applications become front and centre for revenue generation and Web 2.0 in general.

More here.

An F5 white paper on the firewall of the future here.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com