Security is a process

Kuna, 2014-08-01

A newspaper report recently warned that many IT products and applications, including payment systems, lack adequate security. The reasons cited are that firstly, security is treated as an afterthought, and secondly, because trained practitioners are not involved in the design and implementation.

F5 views security as a process. It should be managed as such. There's an important role for the security experts who build the policies that ensure security and compliance within the organization. And, there's an equally important role for the programmers who develop the software. But the two are quite distinct from each other.

Business applications are the critical assets of an enterprise. Its security should not be just left to the software engineers to decide because they are not security professionals. Therefore, the prudent approach is to offload the burden of coding security policies from the software programmers onto credible security solutions professionals.

Viewed from that perspective, security is as an end-to-end process, with policies to govern the various areas wherever there is user interaction with the enterprise – device, access, network, application and storage. Given the complexities of the different moving parts, it sometimes makes sense to combine several of the point security concerns into a converged solution. In short, this is akin to process simplification not too different from what consultants would call "BPR" in the business world. However way, you see it, from a CFO perspective, this represents immense cost savings boh operationally as well as in capital costs.

For example, when it comes to application security, the trend is to build it into the application delivery controllers. ADCs are designed to natively deliver applications securely to end users. In today's context, ADCs act as secured gatekeepers to the applications; they prevent unauthorised access and are able to add-on capabilities to mitigate complex application level attacks such as those defined by OWASP.

However, the situation is growing more complex. CIOs are increasingly faced with the task of balancing the needs of a younger, empowered and demanding Gen Y workforce who want the freedom to work from their device of choice as well as the ability to switch seamlessly between their social and enterprise networks. The CIO challenge is how to protect the company's business assets in the face of increasing and more complex threats. Add to this the desire to leverage the cloud for cost control and scale and the security considerations can potentially spiral out of control.

The situation calls for innovative security solutions that can understand the behaviour of enterprise applications as well as user behaviour, and be able to enforce corporate security policies effectively with minimum impact on user experience. F5 believes that security is a trust business. Having the right process and policies trumps choosing a vendor. It is the policies and process that determine the required solution, not vice versa.

For a Japanese version of this post, please go 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