Web Application Security

Vince Crose, Manager IT 6/20/16

The protection of personal data has always been a concern of consumers in the health industry. The prevalence of recent security breaches has brought further focus to this important topic. Consumers are demanding greater levels of security and assurances that their data is protected. This has brought about a greater focus on the "Principle of Least Privilege" – allow only access to information and resources that are necessary for legitimate purposes. What this really means is that users should only have the privilege and access to resources that are essential for them to complete their work.

In the Web application space, this has brought about the importance of "walling off - firewall" applications at a technology infrastructure level to prevent malicious users of the applications from being able to exploit any existing or future software vulnerabilities. While the use of firewalls for general web network traffic has been around for a long time, there is now an increased focus on using application specific firewalls. Web Application Firewalls (WAF) take the "walling off" one step further by plugging into the application layer and providing the ability to define rulesets and roles that can access specific applications.

In short, the protection of consumer data is going to require greater levels of controls around how data is accessed. The Web Application Firewall (WAF) technologies provide this ability at the infrastructure level to carry the Principle of Least Privilege beyond user access to the applications and software layers.