Why Legacy Security systems fail - Take 1

Nathan Pearce, 2012-31-07

Why 'Take 1'?? Because I expect I will use this title a few more times. I recently spoke at the Government National Security Conference on the topic of why organisations that spend £millions - sometimes ten's of millions - on network security still regularly appear in the media over avoidable data theft attacks.

Interesting reading this morning from Phil Muncaster about a Chinese Cyber Crime Gang suspected of making over *£30 million* because they were able to hack applications and make changes to government databases. It is alarmingly simple to attack web-based applications when only

~~network~~ legacy security models are implemented. Only application security can protect applications.
Learn more about the many attacks invisible to legacy network security (Firewalls) from OWASP - the Open Web Application Security Project:

- Top 10 Application Attacks - here
- Downloadable Virtual Machine, WebGoat that teaches you how to hack web applications

Application Security focuses on the communication within the encrypted connection between the consumer/customer and the Application itself. This is where most data theft attack attempts take place and, conversely, is often overlooked in favour of heavy spend on e.g. network firewalling.

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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113