Practitioner Perspectives

WOLF DEN
ASSOCIATES, LLC

February 2014 *(Vol.3; Issue 2)*

Top 10 Takeaways from Wolf Den's Participation at ShmooCon X

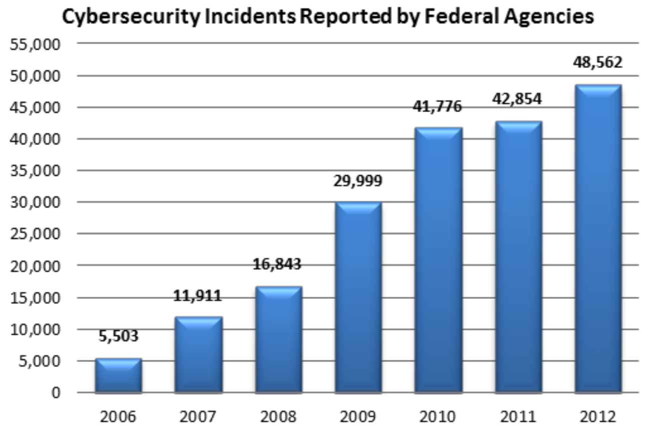
1. ***Social Engineering works because it exploits the weakest link – humans***
2. ***Nessus and Retina are not substitutes for a comprehensive pentest***
3. ***Intrusion is inevitable; resilience and risk management drive success***
4. ***Insider threats cannot be ignored; encourage employees to report suspicious behavior***
5. ***Training cannot and should not replace direct hands-on InfoSec experience***
6. ***C&A is not a substitute for actual security engineering***
7. ***The enemy is at least one step ahead of InfoSec policy***
8. ***Iron sharpens iron; engage with the security community to test systems' mettle***
9. ***To firms with EOSL COTS applications: consider the system compromised***
10. ***Dear Developer: XSS and SQLi have been solved for many years, so please stop introducing them into new applications***

Taming of the Shmoo: InfoSec in 2014

- In the current post-perimeter world, the challenge is not just securing information technology, but securing broader infrastructure
- Living in a connected world is harder; developers need to write both exceptional code and thorough test and security plans
- Today code is not so much written as it is assembled, so securing the software supply chain is critical as vulnerabilities federate
- Black hat, White hat, and Gray hat – the best security advisors have hands-on experience both attacking and defending
- When securing the cloud, emphasize resilience, recognizing that hackers are always ahead of point-in-time policies like FedRAMP and FISMA
- Despite all cyber "fairy dust" used to increase InfoSec mystique, the solution is simply applying engineering rigor to cybersecurity discipline

Hax

The IT Security industry is failing to mitigate the risks of the modern cyber exploitation landscape. The recent outbreak of the BlackPOS point of sale malware, the theft of user data from the last seven years at Adobe, and the steady stream of exploited Java vulnerabilities all provide evidence of a systemic problem in how networks and software are designed and protected. Many firms are relying on a certification and accreditation process, as well as structured testing with Retina and Nessus, to validate the security of their users' data. Both of these approaches only prove that an enterprise is resistant to known threats. To diminish unknown threat damage, CISOs must employ regular unstructured penetration testing that emulates the methodology of malicious adversaries to discover flaws in network business logic and application configuration. The combination of structured and unstructured network testing along with a comprehensive accreditation process and defense-in-depth approach has become the bare minimum standard for the web-enabled enterprise.



Incidents reported to the U.S. Computer Emergency Readiness Team increased 782% from 2006 to 2012, a Compound Annual Growth Rate (CAGR) of 43.75% .

Data Source: GAO analysis of US-CERT data for fiscal years 2006-2012.

Vulns

Prominent voices in the security world are quick to blame data loss on vulnerabilities introduced by third party software. While software vulnerabilities are inevitable, the root cause of these security incidents lies in a combination of poorly architected systems, incorrectly configured COTS platforms, and poorly written custom applications. To maintain a reputation as the source for secure applications, developers must include security early in the requirements phase of the SDLC. After delivery, applications must be routinely updated to mitigate risk introduced from emerging threats. At this phase, the onus is on the maintenance team to license and patch and on the operations team to properly configure applications. Vulnerabilities can be reduced with security-conscious design and development, along with maintaining software currency.

n00bs

The October launch of HealthCare.gov brought media attention to the complex challenges prime federal contractors face when conducting systems integration. Stronger adherence to systems engineering principles could have saved the vendors involved from a tremendous amount of bad press. If the back-end developer and front-end developer had employed an intermediary enterprise architecture firm to define requirements, track dependencies, and design testing, many of the issues that plagued the launch would have been alleviated. An Enterprise Architecture combined with full life-cycle System Engineering is critical to delivering secure products within scope, schedule, and cost constraints.

1337 Skillz

The best remediation plan is one that never gets invoked. For a greenfield program, companies need to lead with security at the proposal level. The overall solution should be security focused, emphasizing risk minimization over intrusion prevention. Assume an attack will happen, assume the system will be compromised, but strive to limit damage. Once compromised, companies must bring in a security focused technical team with direct experience attacking and defending cyber targets that can get the systems back to green permanently. The best security teams take a holistic view and understand the big picture as well as the details, designing security into all "n" tiers of the architecture. Security engineering is a combination of art and science, is unique to every organization, and requires seasoned practitioners.

8280 Greensboro Drive
McLean, VA 22102
wolfdenassociates.com

Rick Tossavainen
(703) 638-5924
rick@wolfdenassociates.com

Ian Kline
(571) 253-2522
ian@wolfdenassociates.com

John Shellhouse
(301) 356-1027
rambo@wolfdenassociates.com