What did we just buy?

Getting the most from Security Assessments

November 10, 2016

weaver
Assurance • Tax • Advisory

Trip Hillman

weaver
Assurance • Tax • Advisory

- Manager, IT Advisory Services @ Weaver
- IT auditor, specializing in all things security related
- Methodology coordinator for Weaver's IT Security Services
- 5+ years experience in IT auditing and consulting
- CISA - Certified Information Systems Auditor (ISACA)
- CEH - Certified Ethical Hacker (EC-Council)
- GPEN - Certified Penetration Tester (GIAC)
- BBA in MIS from Baylor University
- ISACA– NTX Chapter member since 2011

2

Agenda

- Level Setting
- Top Definitions
- Deliverables and Output
- Recap Considerations
- Q&A

3

Level Setting

- What we are talking about
  - Issues that can arise when organizing a security assessment and a path to success
  - Lessons learned
- What we aren't talking about
  - A detailed playbook for conducting every type of assessment

4

Scenario

- Internal IT audit department has been asked by the Board of Directors to select a vendor and conduct a security assessment.
- Need an update at the next BoD meeting and the results presented at the following meeting.
- What do you do?

5

Buzz Words Got Us Here

6

Security Assessment

7

Security Assessment…

- Risk Assessment & Security Governance
  - Policy & Procedure, Org & Training, Network Topology
- Vulnerability Assessment (Scanning)
- Penetration Test (Pen Test)
- Social Engineering & Security Awareness Training
- Access Reviews
- Infrastructure & Configuration – Review & Validation
  - Firewalls, Wireless Networks, Virtualized (Hypervisor), Mobile Device Management, Application

8

Professional Skepticism

- Unstructured technical procedures masquerading as a security assessment
  - What _____ (standard, framework, requirement, guidance, etc.)are you basing this against?
- "Proprietary technology"
- Compliance = best practices?

9

Who is Shopping?

- Any and All!
  - Small (5 person Co.) to Large
- Boards concerned about Security
- Financial Institutions
- Public Companies
- Holders/Processors of PII or PHI
  - Customers, Patients, Students
- Organizations that value proprietary, sensitive, or confidential information & data

10

Why me?

- IT audit is a good go between
- Understand Organizational Risk
- Bridge Relationships

11

Vulnerability Assessment

- Vulnerability Scan vs Assessment?
  - What does the deliverable look like?
  - Value is in Analysis and Assessment of Result Business Risk
- Internal (on-site) vs External (remote)
- Credentialed? Timing? Announced?
- Entire network or sample?
- Why do it?
  - Verify: Baselining & Inventory of Issues
  - Inform: Blueprint from an attacker's perspective
  - Assess: Good Indicator of Security Posture and Patch Mgmt.

12

Penetration Test

- Methodology, Approach
- Rules of Engagement / Scope
- Certifications vs Testing
- Personnel - Contractor
- Internal (on-site) vs External (remote)
- Notification and Detection
- Why do it?
  - Best way to test the locks is to try them
  - More accurate assessment of risk to organization
- Should we do it? Jump in vs ease in

13

Pentest Coverage

- Scope
  - What is being tested?
  - What is winning?
    - May not be domain admin
    - Availability may be enough
- Rules of Engagement
  - Timing, Shunning, Status, Communication
  - PoC – Batphone
  - Limitations
    - DoS – Oh, you want every thing?

14

Social Engineering

- E-mail Phishing
- Baiting (Media/USB Drops)
- Phishing Calls (Vishing)
- Tailgating (Physical Access)
- Methods Allowed
  - Spear Phishing, prohibited premises / schemes
- Sampling
- Metrics
- Data Capture, Storage, Retention

15

Deliverables

- What do you get?
  - Raw Data Output
  - Issues List
  - Executive Summary
  - Board Presentation
  - Internal Audit Report
- Responses
  - Some include it, Some Don't. Does it Matter?
- Participation

16

weaver
Assurance • Tax • Advisory

Considerations for Practitioners

Practical Considerations

weaver
Assurance • Tax • Advisory

- Define terminology for clear communications
- Understanding of approach / methodology
- Authorization for procedures
- Ownership of data
- Use of third parties
- Necessary deliverables and participation
- Beware of “proprietary” technology & masquerading procedures

http://www.pentest-standard.org/
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

18

weaver
Assurance · Tax · Advisory

Wrap-up & Questions

Trip Hillman, CISA, CEH, GPEN
972.448.9276
Trip.Hillman@weaver.com