BUILDING

AN OFFENSIVE

SECURITY PROGRAM

Common Gaps in Security Programs

- Outsourcing highly skilled security resources can be cost prohibitive.
- Annual assessments don't provide the coverage necessary.
- Software is purchased with minimal or no assurance.
- Deficiencies exist within internal security teams.

What skills do we need?

- **Deep technical roots** – Understanding of underlying fundamentals of networking and applications
- **Self-reliance** – Willing to try something new on their own.
- **Creativity** – Security testing is as much of an art that it is a science.
- **Certifications** – Maybe?

Building Security Internally

- Frequent network scanning – deputize a network admin to conduct scans.
- Inventory applications and or network services. Know your perimeter.
- Build Application penetration testing into SDLC

A New Focus on AppSec

Fuel to the fire:

- Increasing criminal sophistication
- Increasing security of networks and endpoints
- Increasing rapid application development

A “risk analysis” is not enough. Security on paper can build a house of cards.

Understanding Application Attacks

Attacks vary in nature, they may:

- Force a user to perform an operation
- Steal session tokens to hijack the user's session
- Perform an operations as another user
- View another user's data
- Extract database contents

A New Application / Browser Security Model

Leveraging security controls in web browsers is crucial for building robust applications.

- **X-FRAME-OPTIONS** – Used to prevent clickjacking attacks
- **HTTP Strict Transport Security** – Used to enforce secure protocol use.
- **Content Security Policy** – Used to mitigate XSS and content injection attacks.

Managing Security Vendors

- Rotate vendors (Required by many regulators)
- Perform comparative tests, vendor scorecards.
- Evaluate volume vs. boutique vendors.
- Encourage vendors to contribute to your process.

Getting the Most Out of Vendors

- Vendors should produce a VA report for their software, and bear the cost (standard procedure).
- Use conditional POs when purchasing software.
- Must decide if the vendor's third party is reputable.
- Vendors have often never test their own software until they need to.
- Explain expectations of assessments. No software is perfect – A report with zero issues is a red flag.

Policy – Getting people to act

- Use internal policy to require action on assessment results.
- Require remediation times for High/Medium/Low risk issues (30/60/120 days)
- Prevent applications and infrastructure from moving from staging to production.

Meaningful Remediation: System Hardening

- **Invest in yourself** - One change can fix many vulnerabilities across the organization.
- Avoid “squashing ants”.
- Public frameworks exist to create hardened system builds for all popular server software (CIS Benchmark).
- Can be performed by almost any IT staff. Checklists are public and trivial to follow.

Vulnerability Assessments vs. Pentests

- **Vulnerability Assessment** – Identify vulnerabilities without exploitation (most cost effective)

- **Penetration test** – VA with exploitation. Shows true impact (useful for budget justification and attention from stakeholders). Risk of availability impact.

Scoping Application Assessments

- **Black Box–** No authentication, no prior knowledge of the application
- **Grey Box –** Credentials provided, simulates a true insider threat.
- **White Box –** In depth code review, looks for deep rooted vulnerabilities and backdoors.

Scoping Network Assessments

- **External only** – No authentication, no physical access, no prior knowledge of the network.
- **Internal and External** – Covers both external perimeter and internal network.
- **Internal Authenticated** – grants access to automated tools to perform authenticated tests.

Wireless Self Assessments

- **War walks** – Can be performed easily by technical staff. Wireless surveying apps are freely available for mobile devices.

- **Configuration based testing** – Most wireless networks can be assessed passively. Weak and broken protocols are publicly documented.

Moving Forward

Embracing hacker culture:

- Manage organization goals with security goals
- Like herding cats

Build a Creative Process

Develop security processes and controls... but also foster creativity and new ideas.

Encourage the use of new testing tools and methods.. But avoid “shiny box syndrome”

Security should be research driven.

Other Recommendations

- Reduce unnecessary network services at all cost.
- Close gaps between assessments.
  - Know what applications are public facing.
  - Know if applications can be leveraged in phishing attacks.
  - Focus on monitoring, detection, and response.

Questions?

Elliott.Frantz@virtuesecurity.com

646-577-8901