Securing Startups

Where to Start with Securing Your Startup

Christie Grabyan, Enterprise Security Practice Lead at Stach & Liu

December 7, 2012

STACH&LIU

AnalyzeThis

STARTUP PROFILE

- Self-funded since June 2011
- 25 employees and contractors across 3 continents
- Develops a suite of data analytics products with a web front-end hosted on AWS EC2 infrastructure
- Customer base is currently one Fortune X00 company
- Looking to expand product availability to competitors within same industry vertical
- Revenue comes from consulting and licensing

Security Controls

YOU CAN RUN, BUT YOU CAN'T HIDE!

1: Security Governance	Documentation and responsibility
2: Asset Management	Know what you have and where it is
3: Configuration Management	Use published security configuration guides
4: Secure Design	Secure coding, scanning, pen testing
5: Identity and Access Mgmt.	Account and password management
6: Technical Ops. Mgmt.	Do you even have a system administrator?
7: Security Incident Mgmt.	Know when things go wrong and lock it down
8: Physical Security	The original security
9: Business Continuity Mgmt.	What can you do without and for how long?

Startups' Head Start

STARTING WITH A CLEAN SLATE

Easier

- Opportunity to bake in security from the beginning
- Root cause analysis and remediation
- No such thing as a legacy system
- Security as a differentiator

Harder

- Timeline pressure
- Fewer people available for oversight
- Being the lone security SME

Strategic Questions

1. Who are your customers? What do they care about?

2. What laws and regulations do you need to consider?

3. What are your worse-case security scenarios?

Real World Solutions

YOU CAN RUN, BUT YOU CAN'T HIDE!

1: Security Governance	Policies, Standards, and SOC2 Compliance
2: Asset Management	Asset tag all physical assets
3: Configuration Management	Use published security configuration guides
4: Secure Design	Emphasis on protecting the source code
5: Identity and Access Mgmt.	Manual, but auditable, process
6: Technical Operations Mgmt.	Automated backup schedule
7: Security Incident Mgmt.	Logging and alerts configured, process identified
8: Physical Security	Office locks, encrypted drives
9: Business Continuity Mgmt.	Annual test of the DR site and systems

Your Next Steps

1. Identify what your customers care about
2. Don't put your security head in the sand
3. Prepare for failing and fixing
4. Limit your scope of sensitive data and systems

Thank You

Christie Grabyan
Enterprise Security Practice Lead
cgrabyan@stachliu.com