30 Mar 201 477dc

30 Mar 2016 SecureWorld

30 Mar 2016 SecureWorld

Monday, May 22, 2017

7:10 AM

- Joe Jarzombek

o Former Director of Software Assurance at DHS

- IoT is a growing concern
- Shifting concerns for software liability

o Concern doesn’t usually peak until actual risk/integrity exposed

- Assurance relative to trust newer model over CIA for IoT security relative to safety

o Overlap between quality, safety, security - Trust

- Enterprise response mostly reactive

o Firewalls, IDS, IPS, logging/monitoring, SIeM, crypto

o Security after the fact

o Control of attack vectors and surface

- Things like XSS and SQL injection are over allowed ports/services that bypass the security feature
- 2016 trends

o Known unmatched vulnerabilities continue to enable breaches

o Chained attacks via 3rd websites grow

o Vulnerable web applications

o 3rd party code and plugins

o Server misconfiguration

o Vuln in systems that can’t be patched (IoT)

o Primary causes will be exploited vulnerabilities thru software defects and bugs

o Application logic errors will become more frequent

o Mobile apps as increasing source of attack vector

o IoT will have exploited weaknesses publicly reported because of consumer risk

- 92% of vulnerabilities in application layer not in networks (reported by US DHS CIO)
- Residual risk through supply chain issues

o Global sourcing/manufacturing

o Lack of risk Mgmt in acquisition, logistics, chain of custody for hardware handling processes

- Are you reviewing your approved vendors and products been tested for exploitable weaknesses (CWE)
- Need to contractually expect suppliers to mitigate known vulnerabilities prior to delivery and use
- Up to 90% of an application consists of 3rd party code (a lot of application development is re-using components esp. Open source)

o Do you trust what's in your 3rd party code? How do you gain trust in the 3rd party code?

o Software composition analysis is a method for addressingthis info

#learning/conferences