Secure Software Foundation

Framework Secure Software

Secure software in de strijd tegen cybercrime

Woensdag 8 oktober 2014

Postillion Hotel Utrecht Bunnik

Fred Hendriks (directeur a.i. Secure Software Foundation)

Tim Hemel (CTO iComply)

Digitale agenda “Brussel & Den Haag”: veilige hard- en software

Secure Software Foundation

“If 50% of vulnerabilities are removed before software goes into the production environment, enterprise management and incident response costs are reduced by 75%.”

Gartner

Veilige software: een “must”

- Informatiebeveiliging bij softwareontwikkeling staat in de kinderschoenen en wordt in de praktijk reactief ingericht

- Ontwikkelde software wordt veelal pas na oplevering getest op eventuele lekken en zwakheden,
  waardoor het aspect beveiliging achteraf pas aandacht krijgt

Veilige software: aantoonbaar?

Secure Software Foundation

- Tot op heden is er geen alles omvattend meetbare norm / certificaat voor ontwikkeling en toetsing van veilige software beschikbaar

- Een *Framework Secure Software & Secure Software Certificate* zal veiligheidsincidenten aanzienlijk verminderen door “objectief meetbare controle” toe te voegen

Ontwikkeltraject

Secure Software Foundation

- **Oktober 2012:** vastlegging concept
  “Normenkader Secure Software” & “way to market”
  (Initiatiefnemers: Security Academy & iComply)
- **November 2012 – jan. 2013:** toetsingsfase (ca. 25 organisaties; start samenwerking met Ministerie van Economische Zaken)
- **Februari 2013:** kick-off meeting met alle betrokkenen
- **Maart – mei 2013:** technisch-inhoudelijke toetsing door diverse kennispartijen

Ontwikkeltraject

Secure Software Foundation

- **Juni 2013:** annoncering bèta versie; toekenning bijdrage Min. van Economische Zaken (via ECP, programma Digivaardig/Digiveilig)
- **September 2013:** Start pilot trajecten
- **Januari-april 2014:** vastleggen Release 1 “Framework Secure Software” op basis van pilottrajecten

Ontwikkeltraject

Secure Software Foundation

- **27 Mei 2014:** Annoncering “Framework Secure Software”
  Oprichting “Secure Software Foundation”

  in aanwezigheid van:

  Ministerie van Economische Zaken
  Nationaal Cyber Security Centrum
  Cyber Security Raad
  NOREA

  Pilot organisaties
  Security Academy
  iComply
  EXIN

EXIN SECURE PROGRAMMING

Doelstelling Framework Secure Software

Secure Software Foundation

- Openbare methodologie voor veilig ontwikkelen van software tijdens alle fases van het ontwikkelproces

- Secure Software Certificate (veiligheid code / applicatie)

Secure Software Foundation

Doelstelling
Secure Software Foundation

- Bewaken en bevorderen van een uniforme toepassing van het Framework Secure Software
- Bewaken van de kwaliteitsregeling m.b.t. het benoemen van audit partijen en auditors
- Aansluiten bij internationale initiatieven en volgen van internationale ontwikkelingen op het gebied van veilige software
- Bevorderen van veilige software ontwikkeling in het algemeen

Secure Software Foundation: Stand van zaken

- SSF is “live” (www.securesoftwarefoundation.org)
- Framework nu gratis te downloaden (> 400 x)
- Consulting-, training- en audit partijen kunnen “aanhaken”
- Afnemers / gebruikers van software kunnen zich oriënteren
- Eerste certificeringen gepland eind 2014
- Normcommissie / bestuur geïnstalleerd

Licentie van het Framework

Creative Commons Naamsvermelding-GeenAfgeleideWerken 4.0 Internationaal

- Vrij te verspreiden
- Commercieel gebruik is toegestaan
- Naamsvermelding bij verspreiding
- Geen afgeleide werken

Eisen aan auditpartijen/auditors

- Aantoonbare meerjarige ervaring in software engineering en software security
- Ervaring met audit processen (bijvoorbeeld CISA, RE etc.)
- “Registered Secure Software Auditor” (RSSA)
- Verdere invulling door de SSF

Secure Software Foundation: vervolg

- SSF moet “op eigen benen gaan staan”
- SSF moet gedegen structuur krijgen
- SSF moet streven naar draagvlak

Oproep aan marktpartijen

Secure Software Foundation

- Softwareontwikkel-organisaties
- Consulting partijen

  (advies secure software op weg naar certificering)
- Audit partijen (audits en pre-audits)
- Training partijen

Secure Software Foundation

Doel

Nederland “in the lead” bij Secure Software (development) & verificatie

Oproep

Aan alle belanghebbenden (overheid, politiek, bedrijfsleven, onderwijs, overige organisaties) om bij te dragen aan “veilige software”

Secure Software a must !

Secure Software Foundation

Europese overheden moeten regelgeving maken om softwareontwikkelaars te dwingen de beveiliging van software te verbeteren. Ontwikkelaars zullen dit namelijk niet uit zichzelf doen. Dit stelt Troels Oerting, hoofd van de cybercrime-afdeling bij Europol. Oerting is van mening dat de beveiliging van software alleen kan verbeteren als tijdens het ontwikkelproces al wordt nagedacht over security. Oerting is daarom van mening dat de samenleving van softwaremakers moet eisen dat zij meer aandacht besteden aan beveiliging. De overheid kan hierbij helpen, door bijvoorbeeld een keurmerk op te zetten waarmee de veiligheid van software wordt gegarandeerd.
(Bron: infosecurity 10 okt. 2013, interview tweakers)

Secure Software Foundation

Doe mee!