Veilige webapplicaties boven alles

Betrouwbaar en veilig overkomen

Mike Wardi (IT professional)

17 november 2005 OWASP Dutch Chapter

We dachten dat we veilige web-applicaties hadden …

- We scoorden goed met de security audits
- We voerden regelmatig penetratie scans uit op de websites
- We voldeden aan de zware interne veiligheidsrichtlijnen, zowel technisch als organisatorisch

Maar toch … het onverwachtse gebeurde

We constateerden

- Anomalieën in web-logs
- Wachtwoorden die werden misbruikt
- Gewijzigde database tabellen
- Sporen van een mogelijke site deface

Hoe was dit nu mogelijk?

Analyse

- Nieuwe type webaanvallen verplaatsten zich van de netwerklaag naar de presentatielaag van het OSI-model
- Er waren geen interne richtlijnen die specifiek web applicatie ontwikkeling betreffen, dus voldeden we toch aan de richtlijnen?
- Huidige opzet penetratiescans voldeed niet meer, achterhaald door de Tijd

Genomen maatregelen

- Wijzigen opzet penetratiescans
  - Focus op webapplicaties ipv infrastructuur
  - Marktanalyse leverancier-selectie
- Onmiddellijk herstel van fouten met risico-classificatie kritisch en hoog
- Aanscherpen autorisatie (herkomst)
- Opstellen richtlijnen voor veilige webapplicaties
- Implementatie richtlijnen in de organisatie en m.n. bij projectleiders

Richtlijnen en richtlijnen

- Moet in lijn liggen met interne en internationale richtlijnen
- Mag geen propriety zijn afhankelijk van een software-product: moet ‘open’ zijn
- Onderdeel van nieuwe software-contracten?
- Herstel op wiens kosten?

Resultaten

- Vaststellen van richtlijnen als appendix op bestaande richtlijnen
- Effectueren voor internet en intranet applicaties
  - Distributie naar alle projectleiders
  - Toetsen richtlijnen op bestaande web applicaties
  - Standaard bij nieuwe en bestaande applicaties
- Onmiddellijk herstel van fouten na elke scan
- Periodieke preventieve penetratiescans

Meerwaarde OWASP chapter

- Bewustwording dat internet applicaties terdege veiligheidsrisico's vormen
- Globale kennis delen
  - Security officers
  - Programmeurs
  - Methodieken
  - Tools & technologie

Bedankt voor uw aandacht!

Mike Wardi
(mike@wardi.net)