NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Bijlage 2 Handreiking DigiD ICT-beveiligingsassessments voor RE's

Betreft: Procesmatige kwaliteitsaspecten bij DigiD pentest
Versie: februari 2015

Van toepassing op:

- Norm B0-8: Externe blackbox/greybox infrastructuur en greybox/whitebox applicatie penetratietest
- Norm B3-15: Externe Blackbox penetratietest op kwetsbaarheden in de webapplicatie

Randvoorwaarden

- Pentester staat onafhankelijk ten opzichte van het te onderzoeken object
- Pentester heeft aantoonbare eerdere ervaringen met pentesten
- Pentest vrijwaring ondertekend door opdrachtgever en evt. betrokken derden zoals hosting partij
- Afspraak over beschikbaarheid van pentesters en beheerders bij de onderzochte organisatie
- Afspraak tussen auditor en pentester over het gebruik van pentesttools
- Gedocumenteerde afspraken over communicatie tussen pentesters en contactpersonen bij de opdrachtgevende organisatie
- Overeengekomen doorlooptijd en budget
- Instemming opdrachtgever met uit te voeren pentest

Scope en normstelling

- Vastgesteld object van het onderzoek relevant voor DigiD
- Vastgestelde Logius normen voor DigiD (subset uit de NCSC normen), minimaal OWASP top 10, eventueel aangevuld met SANS 25, WASC criteria, GHDB en leveranciers-specifieke normen en baselines
- Voor DigiD audit is een blackbox/greybox benadering, waarbij zonder veel voorkennis ingelogd wordt als gebruiker, voldoende.
- Vaststellen met welke functionele scope de volledige technische oplossing wordt afgedekt (bijvoorbeeld een selectie van formulieren waarmee alle componenten worden geraakt), waarbij wordt aangetoond dat de technische oplossing adequaat wordt getest)
- Maatwerk formulieren die niet op basis van standaard configuratie functionaliteit zijn ontwikkeld altijd testen.

- Indien standaard formulieren worden gebruikt, waarbij alleen functionele aanpassingen doorgevoerd kunnen worden, kan volstaan worden met vaststellen van de betrouwbare werking van de formulierengenerator (o.b.v. de TPM van de service provider).

Verkenningsfase (vaststellen ingang criteria)

- Inventarisatie gebruikte (webfacing) infrastructuur, applicaties, componenten, e.d.
- Infrastructuurtest vindt altijd plaats op de productieomgeving
- Applicatietest vindt plaats op test omgeving. Opdrachtgever toont aan dat de versie van de applicatie van acceptatieomgeving gelijk is aan die in de productie omgeving
- Acceptatieomgevingen met representatieve testgegevens zijn beschikbaar
- DigiD testaccounts zijn beschikbaar en gekoppeld aan testgegevens, evt. gekoppeld aan mobiele nummers pentesters
- Pentester(s) zijn bekend met de werking van de applicatie
- Contactpersonen bij de opdrachtgever zijn bekend met de werking van de applicatie

Initiële kwetsbaarheden analyse

- Fingerprinting van het object: vaststellen gebruikte merken en versies
- Inventariseren bekende kwetsbaarheden op basis van publicaties van leveranciers en openbare cyber security bronnen
- Selectie van tests voor aantonen van de mogelijke kwetsbaarheden

Geautomatiseerde tests (dynamisch testen)

- Keuze geschikte pentest tools en hun dekkingsgraad van het te testen object (niet ieder pentest tool ondersteunt alle technologieën, denk aan AJAX, Silverlight, Java en dergelijke.)
- Inzicht in het deel van de norm dat door de tool(s) wordt afgedekt en welk deel afzonderlijk zal moeten worden getest
- Doorlopende bewaking door de pentester tijdens de uitvoering om schade te voorkomen, bij voorkeur automatisch afbreken van geautomatiseerde testen bij foutmeldingen waaruit een kritiek probleem blijkt

Handmatige tests

- Adequate expertise van de pentester(s), eventueel aanwezige certificeringen ter onderbouwing; aantoonbare kennis/ervaring met gebruikte technologieën
- Technische details van gecontroleerde SSL-certificaten en SSL-versleutelde verbindingen
- Details van gecontroleerde cookies en volledige dekking tijdens de testen
- Alle bevindingen uit de geautomatiseerde testen zijn handmatig geverifieerd
- Op basis van bevindingen uit de geautomatiseerde testen zijn handmatige vervolgtesten uitgevoerd
- Kwetsbaarheden in functionele flows zijn handmatig onderzocht, bijvoorbeeld manipulatie van velden bij meerstaps-formulieren

Optioneel: Code review (statisch testen) afhankelijk van de norm

- In principe kunnen alle normen getest worden op basis het bepalen van het gedrag van de applicatie. Bij gerede twijfel over het gedrag alsnog een code review uitvoeren.
- Dekkingsgraad van de review bepalen (steekproef, volledig, ..?)
- Aantoonbare ervaring van de pentester(s) met de programmeertaal en omgeving, eventueel beschikbare certificeringen ter onderbouwing
- Bij gebruik van tools voor statische testen: dekkingsgraad ten opzichte van de norm

Risicoanalyse op bevindingen (vaststellen uitgang criteria)

- Risicoafweging van aangetroffen afwijkingen t.o.v. de norm tegen het daadwerkelijk kunnen exploiteren
- Onderbouwen van de ernst van de aangetroffen afwijkingen
- Geen uitspraken over risiconiveau vanuit business perspectief (beoordeling hiervan kan alleen door de opdrachtgever plaatsvinden)

Rapportage

- Conceptrapportage
    - Classificatie van de rapportage conform DigiD norm, beleid opdrachtgever en auditor en eventueel naar publieke standaarden
    - Beschrijving object van het onderzoek: webfacing infrastructuur, servers, verbindingen
    - Indien van toepassing: overzicht van onderdelen die niet of onvoldoende getest konden worden
    - Overzicht afwijkingen ten opzichte van de norm met bijbehorende mate van risico o.b.v. norm en na risicoanalyse
    - Overzicht en details resultaten en afwijkingen per onderdeel uit de norm
    - Proof of Concepts of details in rapportage waarmee de bevinding kan worden gereproduceerd
    - Concrete aanbevelingen per bevinding
- Afstemming met auditor (review)
    - Versleuteld, beveiligde uitwisseling met de auditor
    - Controle op volledigheid en consistentie
    - Controle of met de verkregen diepgang tijdens de testen de norm is afgedekt
- Melden kritieke bevindingen aan opdrachtgever indien deze naar verwachting in een productieomgeving aanwezig zijn
    - In overleg met de auditor melden
    - Proof of Concept of stappen om te reproduceren
    - Versleuteld, beveiligde uitwisseling details van de kwetsbaarheid
- Afstemming met opdrachtgever
    - Versleuteld, beveiligde uitwisseling met de auditor
    - Afstemming over planning van oplossing en hertesten van bevindingen
- Definitieve rapportage
    - Versleuteld, beveiligde uitwisseling met de opdrachtgever
    - Bevindingen waarvoor een hertest is uitgevoerd zijn als zodanig opgenomen in het rapport met de uitkomst van de hertest (tbv traceerbaarheid)

- Archiveren rapportage
    - Indien van toepassing: archivering in een afgeschermde omgeving met passende beveiligingsmaatregelen

Periodiciteit

- Een jaarlijkse pentest laten uitvoeren ten tijde van de DigiD audit is minimaal. De voorkeur heeft het op basis van en risicoafweging dit enkele keren per jaar te laten doen, zodat ingespeeld kan worden op nieuwe bedreigingen
- Een pentest dient uitgevoerd te worden bij het uitbrengen van een nieuwe release van de applicatie of een grote het upgrade van het onderliggende platform.

Vulnerability assessment (Norm B0-9)

- Vulnerability assessments vinden intern plaats, meerdere malen per jaar op basis van een risicoafweging.