Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

Beleid Hack-testen DUO 2011-2015

Dienst Uitvoering Onderwijs,
Groningen, september 2011

E.R.A. de Widt MBA
Samensteller : J.K.G.Brouwer dso

Status: definitief v1.2

0 VOORWOORD

De beschikbaarheid, exclusiviteit en continuïteit van de dienstverlening door DUO aan haar klanten en opdrachtgevers, is van vitaal belang voor de Nederlandse samenleving. Het wegvallen van deze dienstverlening kan tot ongemak, verstoring dan wel tot ontwrichting leiden.
Helaas hebben een aantal incidenten in het recente verleden aangetoond dat DUO haar servicegraad op deze elementen niet altijd op de overeengekomen wijze kan waarmaken.
Aangezien het vanaf 2008 van kracht zijnde beleid hacktesten enkele leemten vertoonde, met name op het gebied van escalatie, is het in de vorm van onderliggend document geactualiseerd.
Om het actueel houden van het aangepaste beleid te vergemakkelijken, is dit gesplitst in een strategisch, tactisch en een operationeel deel.

Groningen, september 2011

1. Strategisch beleid m.b.t. het uitvoeren van hacktesten

1.1.De hacktest

Binnen DUO speelt permanent de wens voor een verhoogd beveiligingsniveau en is sprake van een toenemende vraag naar internetfunctionaliteit. Het ligt daarom voor de hand dat het DO hierom besluit tot een meer gestructureerde aanpak om nieuwe dan wel vernieuwde applicaties te testen op risico's uit het deelgebied informatiebeveiliging en draagt de CSO (voor wat betreft het bepalen van de risico's) en dICT (voor wat betreft het uitvoeren van de daadwerkelijke hacktesten) op hier zorg voor te dragen.
Door middel van het verplicht uitvoeren van een hacktest moeten van alle nieuwe dan wel vernieuwde applicaties de risico's ten aanzien van beschikbaarheid, exclusiviteit en integriteit in kaart gebracht worden en moet een risicoafweging ten aanzien van de bevindingen gemaakt worden.
Het normenkader voor de uit te voeren hacktest wordt bepaald door het gestelde in de volgende documenten (wetten, voorschriften, intern beleid):

- het Voorschrift Informatiebeveiliging Rijksoverheid 2007;
- de Wet Bescherming Persoonsgegevens;
- de Code voor de Informatiebeveiliging;
- webrichtlijnen voor de overheid;
- Achtergrondstudie en Verkenning 23 m.b.t. Beveiliging van persoonsgegevens (Registratiekamer 2001);
- de Baseline Informatiebeveiliging DUO 2011

Deze stukken kunnen worden opgevraagd bij ICT/IP/beveiliging.
Om een nieuwe dan wel vernieuwde applicatie in productie te mogen nemen, legt de proceseigenaar, ICT/IP/Beveiliging gehoord hebbend, een verzoek hiertoe voor aan de CSO. Deze gaat al dan niet akkoord.

1.2. Grenzen

Vanuit ICT gezien is Productie meer dan alleen de applicaties en servers in de Productieomgeving. Servers voor Ontwikkeling (ONT), Functionele (FAT) en Gebruikers Acceptatie Test (GAT), zijn verbonden met het productienetwerk en hebben strikt genomen vanuit technisch beheer de status 'in productie'. De Exploitatie (EXP) test omgeving is gescheiden van het reguliere productie netwerk. De ONT en FAT/GAT omgevingen zijn via logische toegangsbeveiliging en fysieke inrichting gescheiden van de productieomgeving.

1.3.Verantwoordelijkheden

Voor de reguliere productieomgeving zijn de volgende verantwoordelijkheidsgebieden onderkend:

Gebied	**Verantwoordelijkheid**
Infrastructuur	Serviceprovider
Applicatie	Proceseigenaar
Data	Gegevenseigenaar

ICT heeft als 'serviceprovider' de verantwoordelijkheid en de zorg dat alle processen onverstoord naast elkaar kunnen draaien. Halfjaarlijks voert ICT een controle uit op servers en applicaties, om vast te stellen of het beveiligingsniveau nog steeds overeenkomt met het gewenste/vereiste niveau.
De noodzaak tot regelmatig testen ligt in het feit dat niet alleen de applicatie aan verandering onderhevig is, maar dat er regelmatig nieuwe kwetsbaarheden in de

gebruikte apparatuur en systeemsoftware (Windows, Websphere ed) worden gevonden die nieuwe risico's introduceren. Reguliere controles, pro-actief beheer en actieve monitoring kan misbruik van systemen voorkomen.

De Proceseigenaren[1] zijn verantwoordelijk voor de beveiliging van de applicatie. Daarbij zijn zij gehouden aan wettelijke bepalingen als bijvoorbeeld de Wet Bescherming Persoonsgegevens, Voorschrift Informatiebeveiliging Rijksoverheid en de Wet op de computercriminaliteit. Zij laten regelmatig afhankelijkheid- en kwetsbaarheidanalyses (A&K) uitvoeren en zijn verantwoordelijk voor de invoering van de verbetermaatregelen.

De Gegevenseigenaar zal zich primair richten op de vraag of de applicatie de gegevens veilig en betrouwbaar kan verwerken. De controle of een applicatie en het netwerk is ingericht volgens de (wettelijke) kaders is zijn verantwoordelijkheid. Vaak is de eigenaar van de gegevens ook de proceseigenaar.

1.4 Escalatiepad

Indien geen hacktest is uitgevoerd, dan wel aan de hand van een hacktest is vastgesteld dat de beveiliging onvoldoende gegarandeerd kan worden en een proceseigenaar om moverende redenen toch van mening is dat een nieuwe dan wel vernieuwde applicatie in productie moet, moet schriftelijk decharge worden gevraagd bij dICT en de CSO. In het geval van afwijzing door deze beide functionarissen (of van één van twee) zal de aanvraag door de verantwoordelijke directeur worden voorgelegd aan de DG.
Indien de DG zijn toestemming verleent, stelt de CSO een notitie op met afspraken op welke termijn alsnog een hacktest verricht moet worden teneinde de beveiliging alsnog voldoende te kunnen garanderen. De DG ondertekent deze notitie. De CSO zorgt ervoor dat de notitie via ICT/IP/Beveiliging aan ICT/I&E wordt aangeboden, waarna de nieuwe dan wel vernieuwde applicatie geïmplementeerd kan worden.
De CSO bewaakt de in deze notitie vastgelegde termijnen.

1.5Tenslotte

De DG draagt dICT op de inhoud van dit document ter kennis van alle betrokkenen te brengen en draagt dICT en de CSO op om toe te zien op correcte uitvoering.

[1] In geval van ontbreken van een proceseigenaar is de projectmanager tot en met de implementatie verantwoordelijk voor de beveiliging van de applicatie.

2. Tactisch beleid m.b.t. het uitvoeren van hacktesten

dICT belegt bij ICT/IP/Beveiliging:
- het uitvoeren van de daadwerkelijke hacktest;
- het opstellen de richtlijnen voor dergelijke testen.

Het in productie nemen van een nieuwe dan wel vernieuwde applicatie is pas toegestaan, nadat dICT en de CSO hier beiden toestemming voor hebben verleend.
Deze procedure alsmede het escalatiepad zijn verwoord in art 1.3 en 1.4.

3. Operationeel beleid m.b.t. het uitvoeren van hacktesten

3.1Algemeen

ICT/IP/Beveiliging controleert nieuwe dan wel vernieuwde applicaties op risico's uit het deelgebied informatiebeveiliging. Hierbij worden de risico's ten aanzien van Beschikbaarheid, Exclusiviteit en Integriteit in kaart gebracht. Daarbij maakt de specialist informatiebeveiliging een risicoafweging ten aanzien van zijn bevindingen. Hij doet dit actief door het uitvoeren van hacktesten op nieuwe dan wel vernieuwde applicaties als pro-actief door samen met ICT/Softwarehuis geautomatiseerde Source Code Review te introduceren. Dit zal een inhoudelijke kwaliteitsverbetering van de sourcecode betekenen, waardoor het aantal bevindingen bij hacktesten en eventuele niet ontdekte zwakheden vermindert.
Door deze aanpak is DUO de komende jaren weer verzekerd van adequate controle op functionaliteit. Bij ernstige risico's is goedkeuring nodig van het management. In bijzondere gevallen, zoals bij het achterwege laten van een hacktest of het niet kunnen garanderen van adequate beveiliging, is goedkeuring nodig van de DG.

3.2. Randvoorwaarden

3.2.1. Tijdigheid

Nieuwe dan wel vernieuwde applicaties dienen tijdig aan ICT/IP/beveiliging te worden aangeboden voor het uitvoeren van een hacktest en worden vervolgens in de planning van ICT/IP/beveiliging opgenomen. De opdrachtgever wordt hierover ingelicht. In nader overleg met ICT/IP/beveiliging kunnen bij nieuwe releases deze 3 dagen schuiven in de planning tot maximaal 4 weken later.

3.2.2 De omgeving

Om een adequate securitytest uit te voeren, moet er een adequate omgeving zijn, waarin deze test kan plaatsvinden. Daar waar sprake is van externe koppelingen, zoals met het internet, moet ook gemonitored worden op mogelijk misbruik van buitenaf. De nieuwe dan wel te vernieuwen applicatie is dan ook maatgevend voor de testomgeving.

3.2.3 Werkwijze voor omgevingen

Algemeen:
Daarnaast is de volgende informatie vereist: startpunt van de applicatie, url en ip-adres. Daarnaast moeten voor zover nodig voor de verschillende rollen 3 (test-)useraccounts geleverd worden. De applicatie moet werken in de testomgeving en moet daar 14 dagen stabiel zijn, tenzij in overleg met IP/beveiliging anders is bepaald. Verder is documentatie noodzakelijk zoals het verkeersplan, het technisch ontwerp en –realisatie, de functionele realisatie. In geval van XML-uitwisseling is een XSD voor de XS40 noodzakelijk. Ook moeten de contracten met derden t.a.v. verwerking persoonsgegevens en netwerkkoppelingen overlegd worden (bewerkingovereenkomsten, servicelevelagreements, beveiligingsplannen ketenpartners etc.). De contactpersonen met SWH, Procesbeheer, NT-beheer en de projectleider moeten bekend zijn.
Indien (een deel van) de hacktest wordt uitgevoerd bij een externe partij, is een getekende vrijwaringsverklaring noodzakelijk.
Na het opleveren van de produktie-omgeving wordt de applicatie 3 dagen specifiek gereserveerd voor ICT/beveiliging, ter controle van de productieomgeving.

Afweging:
Bij de beoordeling van de aanpassingen en wijzigingen van al bestaande applicaties kan door IP/Beveiliging worden besloten een eenvoudige test uit te voeren of zelfs om hiervan af te zien.

Exploitatie test netwerk:
Hacktesten worden altijd voorafgaand aan productie, uitgevoerd op de exploitatietest infrastructuur. In overleg met IP/Beveiliging kan besloten worden tot een hacktest in de veldtest.

Veldtest:
Indien er sprake is van externe koppelingen en partijen zullen de hacktesten worden uitgevoerd in een daarvoor specifiek ingerichte veldtestomgeving. Dit gaat vooraf aan de functionele testen samen met de externe partijen.
De veldtestomgeving bevindt zich op de productie-infrastructuur en moet voldoen aan alle productie eisen t.a.v. security, monitoring en beheer.

Productie omgeving:
Na overzetting van de applicatie wordt voorafgaand aan de openstelling, een herscan gedaan op de productieomgeving. Randwaarde voor het overzetten naar productie is tevens, dat eventuele bewerkerscontracten en beveiligingsplannen van ketenpartners ondertekend en goedgekeurd zijn.

Het Lab:
In het Lab van I&E/IP worden nieuwe installaties en technieken eerst uitgetest in een zogenaamde Proof of concept, als preview om de ergste bevindingen op te sporen. Securitytesten zijn hier van belang om een minimum beveiligingsniveau vast te stellen en inzicht te krijgen hoe machines daadwerkelijk ingericht worden.

Het interne netwerk:
Om het beveiligingsniveau op het interne netwerk te verhogen, worden alle interne productie systemen eenmalig gescanned. Hiermee wordt een minimum beveiligingsniveau vastgesteld en inzichtelijk gemaakt welke risico's er aanwezig zijn.
Er wordt een minimum beveiligingsniveau opgesteld voor interne machines en alle nieuwe interne systemen worden voor productie name met behulp van een quickscan en hardeningscontrole beoordeeld.

3.3. De Hacktest

Om een hacktest te kunnen uitvoeren zijn een aantal voorbereidende acties nodig.
De ICT adviseurs voeren normaliter een impactanalyse uit op het aangeleverde DS of SA. In overleg met de specialisten beveiliging wordt bepaald welk type hacktest het meest geschikt is. Vaak is het ontbreken van een technisch ontwerp hiervan de oorzaak. Ook tijdens de verschillende ontwikkelfasen als FO/TO, maar ook bouw en test, is het van belang om de securityspecialisten te betrekken bij wijzigingen. Hierdoor wordt het risico vermeden van conflicten op het gebied van informatiebeveiliging of afwijkingen op het informatie-beveiligingsbeleid.
Per uit te voeren hacktest kunnen vanuit het auditplan aanvullende eisen worden gesteld.

De ICT adviseurs binnen I&E, zijn verantwoordelijk voor:
- het afstemmen van de impactanalyses en de faganinspecties met de specialisten Netwerk, Telecommunicatie, AS/400, KA en Beveiliging.

De specialist Beveiliging toetst de inhoud aan:
- de door het DO vastgestelde informatiebeveiligingsplan (de DUO-baseline);
- de afgegeven risicoklasse indeling door de privacy officer en de daaruit volgende maatregelen vanuit de Wet Bescherming Persoonsgegevens.

Het project is verantwoordelijk voor:
- het laten uitvoeren van een impactanalyse en fagan inspectie door de ICT adviseurs van I&E;
- vastgestelde documentatie als SA/DS FO en TO;
- Beoordeling door IP/Beveiliging bij nieuwe release of versie op noodzaak hacktest.

Het project levert 2 weken voor de hacktest het volgende aan:
1. SA/DS en FO;
2. Technisch ontwerp inclusief infrastructuur ontwerp;
3. Taken, verantwoordelijkheden en bevoegdhedenmatrix;
4. Contracten met derden t.a.v. verwerking persoonsgegevens en netwerkkoppelingen (bewerkingsovereenkomsten, servicelevelagreements, beveiligingsplannen ketenpartners).

ad 1
Om inzicht te krijgen in de werking van de applicatie moet de hacktester een volledig beeld hebben van wat de applicatie doet.

ad 2
Om inzicht te krijgen in de samenhang met andere infrastructuurcomponenten en applicaties moet inzichtelijk zijn welke computersystemen, verkeersstromen, opslagmedia etc gebruikt worden. Dit schema heeft het project ook nodig om firewallwijzigingen te laten doorvoeren.

ad 3
Tijdens de hacktest kunnen er verstoringen optreden van de applicatie. Er moet afgesproken zijn wie in dat kader als aanspreekpunt fungeert. Daarnaast dient de tvb-matrix voor het beoordelen van functiescheidingen en/of taken ook daadwerkelijk belegd zijn.
Het project levert 1 week voor de hacktest het volgende aan:
- drie werkende testaccounts in de afgesproken omgeving;
- een geteste en werkende omgeving.

In het geval van de veldtestomgeving blijft deze afgesloten voor derden en staat alleen ter beschikking voor IP/Beveiliging.

ad 4
In het geval van een herscan op productie is de applicatie onder voorwaarden beperkt opengesteld.
Pas als alle contracten zijn aangeleverd en ondertekend, is formele productie toegestaan.

3.4 Beschrijving soorten hacktesten.

Een hacktest is opgebouwd uit 3 fasen, waarbij steeds dieper in de applicatie en infrastructuur wordt gekeken. Een nieuwe release van een applicatie hoeft niet altijd te betekenen dat de gehele keten overnieuw getest moet worden. Door hergebruik van computersystemen of andere infrastructurele elementen, is het niet strikt noodzakelijk om alles opnieuw te testen en wordt het principe 'lessons learned' gehanteerd. De beoordeling hiervan vindt plaats in overleg tussen de ICT-securitymanager en het project.
Daarnaast is het door het inzetten van geautomatiseerde scanningtools mogelijk om de aandacht te richten op DUO-specifieke zaken.
Na elke hacktest wordt een bevindingenrapportage opgeleverd, voorzien van een conclusie.
Deze conclusie is bindend en kan alleen door de CSO worden overruled.
In zijn rapportages aan de CSO meldt de ICT-securitymanager de hacktesten regulier.
De infrastructuur is elke dag aan verandering onderhevig. Niet alleen invloeden vanuit de organisatie, maar ook invloeden van buitenaf maken het noodzakelijk om regelmatig de gehele infrastructuur te herscannen. Deze algehele controle vindt halfjaarlijks plaats.

3.4.1 Complete hacktest

Een complete hacktest is noodzakelijk bij nieuwe technieken en nieuwe systemen.
De impact kan niet op voorhand worden vastgesteld, de doorlooptijd is dan ook variabel.

(Voorbeeld: de koppelingen met DIGID en het project Bron PO; de doorlooptijden varieerden hierbij tussen de 3 tot 9 weken)
In het geval van een complete hacktest wordt altijd een auditplan gemaakt.
Dit dient vooraf ter goedkeuring door de projectmanager/proceseigenaar voor de aanvang van de hacktest te worden bevestigd.

3.4.2 Verkorte hacktest

Een verkorte hacktest vindt plaats indien (delen) de infrastructuur (hard- of software) niet wijzigt.
Vaak zijn dit projecten die voortborduren op eerder gebruikte technieken en applicaties.
Een verkorte hacktest kenmerkt zich door een handmatig deel en een sterk geautomatiseerd deel, ook wel Quickscan genoemd. Het handmatig deel is vooral van toepassing voor DUO-specifieke toepassingen tbv authenticatie. Veelal zijn dit applicaties vanuit risicoklasse 2 volgens de Wet Bescherming Persoonsgegevens, waarbij sterke authenticatie is vereist, dus meer dan alleen gebruikersnaam en wachtwoord.
Er wordt geen auditplan gemaakt, maar volgens een vast stramien gewerkt.
Gemiddelde tijd is 12-24 uur per omgeving met een doorloop tijd van maximaal een week.
Ervaring leert dat de verkorte hacktesten worden uitgevoerd in de Veldtest- of Exploitatietest- omgeving en een herscan in Productie.

3.4.3 Quickscan (internet)

Een quickscan is een totaal geautomatiseerde scan.
Geschikte applicaties hiervoor zijn applicaties waarbij geen sterke authenticatie is vereist (risicoklasse 0 en 1).
De benodigde tijd varieert van 2 x 40 uur maximaal met een doorlooptijd van maximaal 1 week.
Een quickscan kan plaatsvinden in zowel VT EXP als in productie.
Daarnaast wordt bij de halfjaarlijkse controle van de quickscan gebruik gemaakt.

3.4.4 Quickscan (intern netwerk)

Een quickscan op het interne netwerk vindt plaats voordat nieuwe systemen of applicaties op het interne netwerk actief worden.

3.5Rapportage

3.5.1 Rapportagestructuur

De security-specialist rapporteert aan de opdrachtgever. Indien de rapportage door beide partijen wordt onderschreven kan het in productie nemen gefiatteerd worden door dICT en de CSO.
Indien door IP/Beveiliging beveiligingsrisico's aangetroffen worden, dan geeft deze een gemotiveerd negatief advies en kan de nieuwe dan wel vernieuwde applicatie niet in productie.
Indien geen gezamenlijk eindoordeel kan worden overeengekomen dan wordt door de ICT-security manager een negatief oordeel gegeven en escaleert deze richting dICT en de CSO. Hij escaleert eveneens indien naar zijn mening binnen zijn werkterrein waar dan ook beveiligingsrisico's dreigen.
Bij een negatief oordeel door de ICT-security manager kan de projectmanager/proceseigenaar de CSO verzoeken de risico's te accepteren. Indien het gaat om bevindingen op infrastructureel gebied moet ook dICT accorderen.

3.5.2 Bewaartermijnen

De rapportages van de security specialist, al dan niet samen met de testdossiers, blijven minimaal bewaard zo lang de betreffende applicatie in productie is.

3.5.3 Bewaking bevindingen

De ICT-security manager bewaakt de bevindingen uit uitgevoerde hacktesten. Door ontwikkelingen in de ICT kunnen bevindingen later een lager niveau dan wel een hoger risicoprofiel krijgen.
Proceseigenaren zijn verantwoordelijk voor het oplossen van hun specifieke bevindingen. Indien die niet binnen de overeengekomen termijn worden opgelost, kan dat leiden tot een negatief advies bij nieuwe ontwikkelingen.