novaccent

BK
BO

Bureau voor Kwaliteitsborging
bij de Overheid

Nieuw DigiD assessment

Programma

09.30 uur - Inloop en koffie/thee
10.00 uur - Opening door dagvoorzitter
10.05 uur - Duopresentatie door René IJpelaar en Martijn Mol
11.15 uur - Pauze
11.30 uur - Presentatie Nováccent Cybercrime
11.45 uur - Presentatie BKBO Productportfolio
12.00 uur - Lunch
13.00 uur – Sluiting

Agenda

- **Wie zijn wij?**
- Risico's
- Wat verandert er?
- Wat vervalt er
- Wat blijft hetzelfde?
- Specifieke beveiligingsrichtlijne
- Vragen?

novàccent

BKBO

novàccent

Ambitie met respect

- Opgestart in 2002
- Hoofdkantoor in Leusden, regionale kantoren in Waalre, Gorredijk & HSD
- 90 eigen medewerkers en grote flexibele schil
- Innovation Center
- Samenwerking met BKBO voor audits

nováccent

SECURITY SERVICES

WERKEN AAN EEN VEILIGE ORGANISATIE

MANAGED ICT

ICT DIENSTEN DIE RUIMTE CREËREN

DATA COMPETENCE

LAAT UW DATA VAN WAARDE ZIJN

INNOVATION CENTER

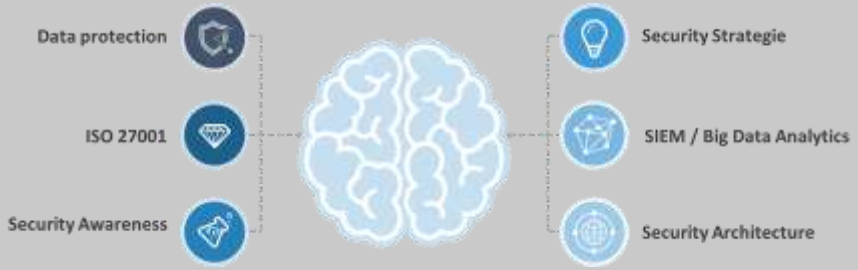
TOEGEPASTE SECURITY OPLOSSINGEN

Novaccent

Security Services

Security Testing Center

Security & Risk Advisory Center



Security Operations Center

CARBON BLACK · Nessus vulnerability scanner · FireEye · Be One Development · Cryptshare

BKBO bv

- Gestart begin 2012
- Uitvoering Digid assessments
- Uitvoering Privacy Impact Assessments
- Uitvoering rekenkameronderzoeken informatieveiligheid
- Uitvoering Suwinet audits
- IT audits
- ISAE 3402 verklaringen
- Samenwerking met Nováccent voor pen en vulnerabilitytesten

Agenda

- Wie zijn wij?
- **Risico's**
- Wat verandert?
- Wat vervalt?
- Wat blijft hetzelfde?
- Specifieke beveiligingsrichtlijnen
- Vragen?

De risico’s

- Ongewild aanpassen webpagina’s
- Bezoekers worden geïnfecteerd
- Website lekt (bijzondere) persoonsgegevens
- Identiteitsfraude
- Stoppen van de digitale dienstverlening
- Reputatieschade en schadeclaims

Agenda

- Wie zijn wij?
- Risico's
- **Wat verandert?**
- Wat vervalt?
- Wat blijft hetzelfde?
- Specifieke beveiligingsrichtlijnen
- Vragen?

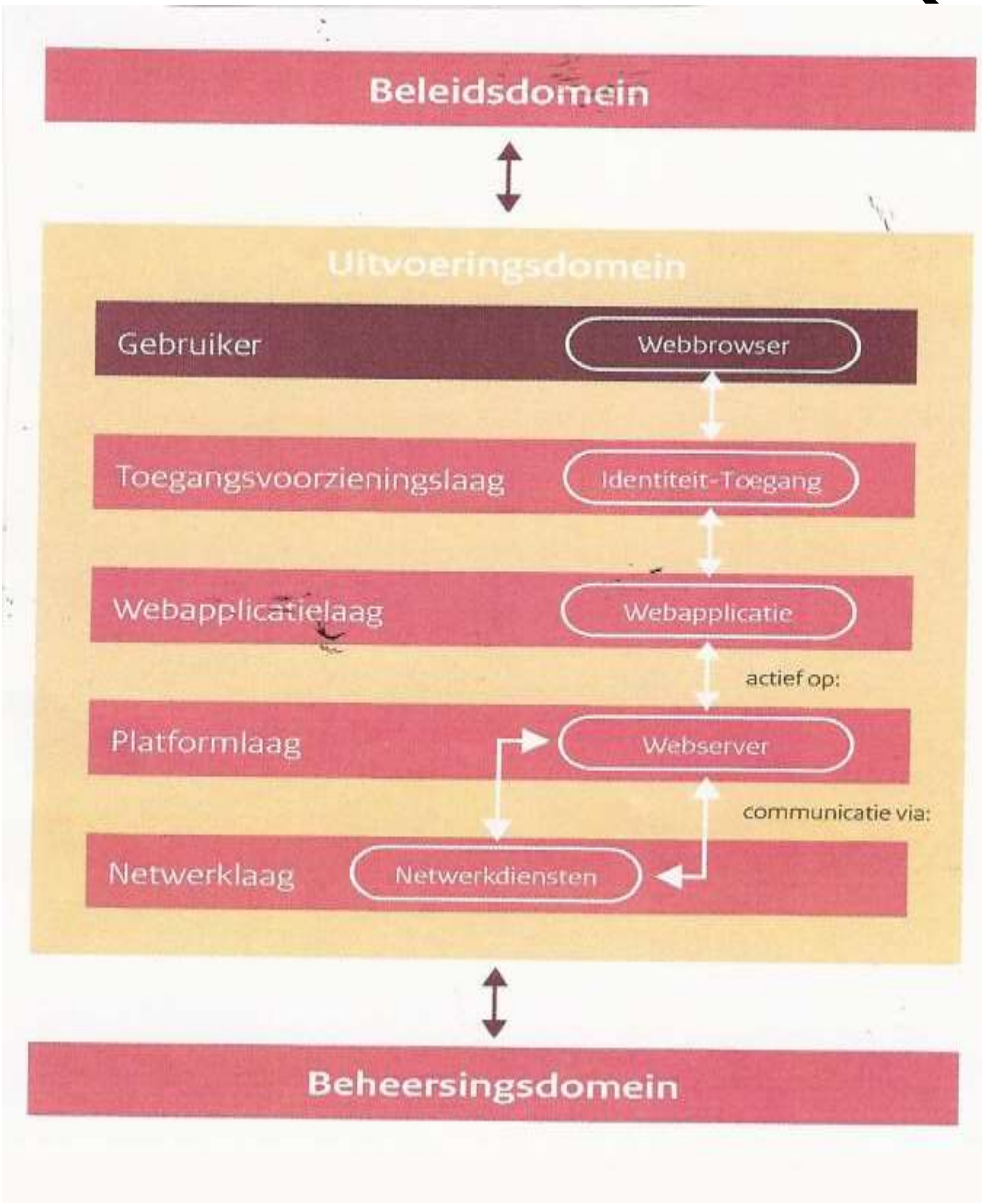
Wat verandert? (1)

- Normenkader DigiD assessment 2.0 van Logius
- Handreiking bij nieuwe normenkader van Norea

Wat verandert? (2)

- Gebaseerd op de beveiligingsrichtlijnen van het NCSC uit 2015 ipv die uit 2013 en een nieuwe nummering
- Daar waar het normenkader effect heeft gehad, wordt de audit verlicht
- 20 ipv 28 eisen van het NCSC verplicht gesteld; oordeel per richtlijn
- Meer risicogericht
- Technisch wat meer ingrijpend
- Nieuw normenkader geldt vanaf 1 juli 2017
- Overgangsperiode t/m 1-11-2017
- Voor gemeenten: integratie met ENSIA
- Begrippenlijst

Wat verandert? (3)



novaccent

BKBO

Wat verandert? (4)

Een vulnerability assessment is een proces waarbij met behulp van technische hulpmiddelen wordt nagegaan in hoeverre in de ICT-componenten kwetsbaarheden voorkomen waarvan ongeautoriseerden gebruik zouden kunnen maken. In de context van het DigiD assessment wordt een (bij voorkeur geautomatiseerde) scan bedoeld die vanaf een intern netwerksegment zo dicht mogelijk bij de server wordt uitgevoerd op bekende kwetsbaarheden en ontbrekende patches.

Wat verandert? (5)

De penetratietest is een specifieke vorm van een vulnerability-assessment. Het is een proces waarbij met behulp van technische hulpmiddelen specifieke componenten of specifieke delen van de ICT-infrastructuur op zwakheden gecontroleerd worden. In de context van het DigiD assessment wordt met een penetratietest een technisch beveiligingsonderzoek bedoeld dat vanaf het internet wordt uitgevoerd door een (ervaren) penetratietester en waarbij scantools worden ingezet en aanvullende handmatige onderzoeks-werkzaamheden worden uitgevoerd

novaccent

BKBO

Criteria voor Vulnerability Assessment

- Infrastructuurtest vindt altijd plaats op de produktieomgeving zowel webbased als hostbased
- Applicatietest vindt plaats op test omgeving. Opdrachtgever toont aan dat de versie van de applicatie van acceptatieomgeving gelijk is aan die in de productieomgeving.
- Acceptatieomgeving bevat representatieve testgegevens DigiD testaccounts zijn beschikbaar

novaccent

BKBO

Agenda

- Wie zijn wij?
- Risico's
- Wat verandert?
- **Wat vervalt?**
- Wat blijft hetzelfde?
- Specifieke beveiligingsrichtlijnen
- Vragen?

Wat vervalt?

- B0-13 Niet (meer) gebruikte websites en/of informatie moet worden verwijderd.
- B1-3 Netwerktoegang is voor alle gebruikersgroepen op een zelfde wijze ingeregeld.
- B3-5 Voor het raadplegen en/of wijzigen van gegevens in de database gebruikt de webapplicatie alleen geparametriseerde queries.
- B3-15 Een (geautomatiseerde) blackbox scan wordt periodiek uitgevoerd.
- B5-1 Voer sleutelbeheer in waarbij minimaal gegarandeerd wordt dat sleutels niet onversleuteld op de servers te vinden zijn.
- B7-09 Governance, organisatie, rollen en bevoegdheden inzake preventie, detectie en response inzake informatiebeveiliging dienen adequaat te zijn vastgesteld

Agenda

- Wie zijn wij?
- Risico's
- Wat verandert?
- Wat vervalt?
- **Wat blijft hetzelfde?**
- Specifieke beveiligingsrichtlijnen
- Vragen?

Wat blijft hetzelfde (1)

- Assessment op opzet en bestaan van beveiligingsmaatregelen (geen werking)
- Bestaande aansluiting voor 1-5-2018 afronden
- Nieuwe aansluiting binnen 2 maanden na aansluiting op DigiD productie
- Per actieve aansluiting een apart rapport
- Uitvoering onder verantwoordelijkheid van Register EDP auditor (NOREA)
- Houder Digid aansluiting = verantwoordelijke

novaccent

BK BO

Agenda

- Wie zijn wij?
- Risico’s
- Wat verandert?
- Wat vervalt er
- **Wat blijft hetzelfde?**
- Specifieke beveiligingsrichtlijnen
- Vragen?

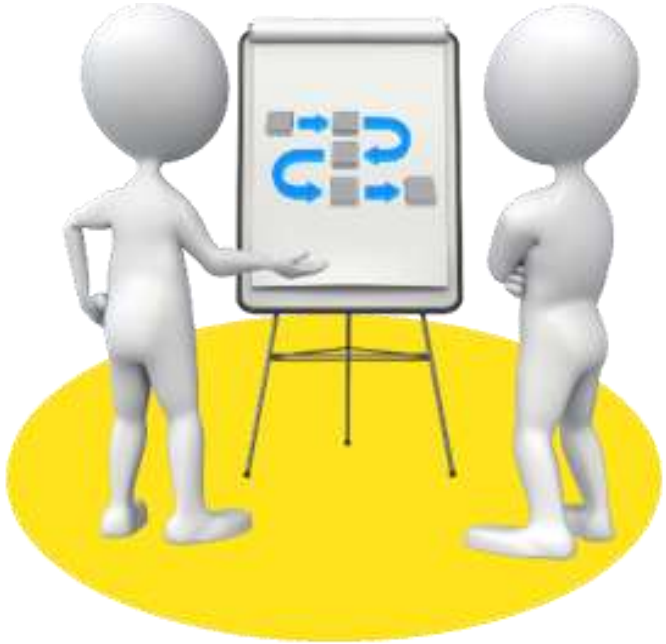
Wat blijft hetzelfde (1)

- Niet voldaan: verbeterrapport naar Logius
  - Bij technische tekortkomingen 1 tot 2 maanden hersteltijd
  - Bij organisatorische tekortkomingen: 4 maanden hersteltijd

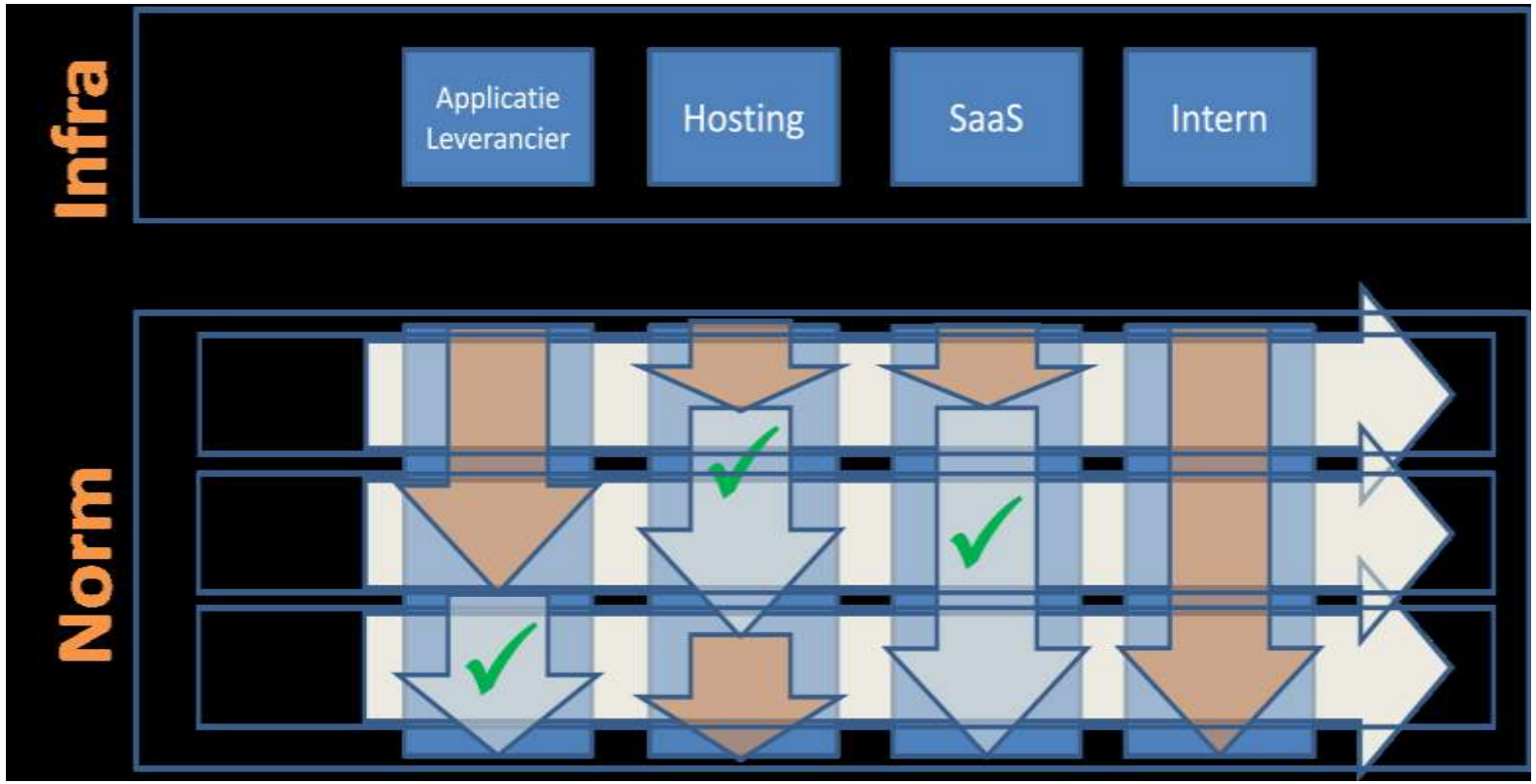
Wat blijft hetzelfde (2)

3 partijen betrokken softwareleverancier, de hostingleverancier en de houder van de DigiD aansluiting

SAAS = 1 leverancier als contractpartner



Wat blijft hetzelfde (3)



novàccent

BKBO

Wat blijft hetzelfde (4)

- Een Third Party Mededeling is een verzekering dat de “serviceorganisatie” de beheersmaatregelen correct heeft geïmplementeerd en voldoet aan de norm
- Een TPM is met vermelding gebruikte software en/of infrastructuur en naam klant
- TPM is gebaseerd op een bepaald normenkader
- TPM verlaagt de auditkosten
- **In hoofdstuk 4 van de TPM worden de “user control considerations” beschreven.**

novàccent

BKBO

Agenda

- Wie zijn wij?
- Risico's
- Wat verandert?
- Wat vervalt?
- Wat blijft hetzelfde?
- **Specifieke beveiligingsrichtlijnen**
- Vragen?

U/WA.03 (B3-1)

De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.

- Invoer moet worden gevalideerd;
- HTTP request voor alle invoermethodes zoals gespecificeerd in de ICT-Beveiligingsrichtlijnen van NCSC moeten worden gevalideerd (testen op type, lengte, formaat en karakters van invoer en speciale tekens (bv. <, >, ', ", & , /, --, etc.).

novàccent

BKBO

U/WA.04 (B3-4)

De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.

- Uitvoervalidatie voorkomt dat de webapplicatie ongewenste opdrachten geeft aan de client, bijvoorbeeld in het geval van XSS;
- De webapplicatie codeert dynamische onderdelen in de uitvoer waarbij mogelijke gevaarlijke tekens (bv. <, >, ', ", & , /, --, etc.) worden genormaliseerd.

novaccent

BKBO

U/WA.05 (B5-3/B5-2)

De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.

- de encryptie van gevoelige gegevens tijdens de opslag en de encryptie van alle gegevens tijdens transport;
- classificatie van gegevens op basis van een risico analyse
- mogelijke versleuteling of hashing van gevoelige gegevens. Gegevens in de backoffice vallen buiten de scope;
- de HTTPS configuratie en de TLS configuratie.

U/PW.02 (B3-2)

De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.

- HTTP-requests moeten een correct type, lengte, formaat, tekens en patronen hebben;
- HTTP-requests alleen van initiators met een correcte authenticatie en autorisatie;
- Sta alleen HTTP-request als GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke HTTP requests;
- *Verstuur alleen HTTP-headers die voor het functioneren van HTTP van belang zijn;*
- *Toon in HTTP-headers alleen de hoogst noodzakelijke informatie;*
- *Foutinformatie tot een minimum beperken.*

U/PW.03 (B3-16)

De webserver is ingericht volgens een configuratie-baseline.

- *aanwezigheid van een configuratie-baseline*
- *feitelijke configuratie van de webserver cf baseline*;
- *directory listings worden niet ondersteund;*
- cookie flags staan op 'HttpOnly' en 'Secure';
- *bij alle HTTP-responses wordt de HTTP-headers 'Content-Security-Policy: frame-ancestors' en (tijdelijk) 'X-Frame-Options' verstuurd*.

U/PW.05 (B2-1)

Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.

- beheerinterfaces via internet alleen via sterke authenticatie (zoals IP Sec VPN) worden afgehandeld;
- *operationeel beleid mbt gebruik van veilige protocollen (conform industriestandaarden) voor het benaderen van beheermechanismen (beheerinterfaces*).
- *het gebruik sterke authenticatie voor zowel technisch als functioneel beheerders (2FA)*

novàccent

BK BO

U/PW.07 (B0-6)

Voor het configureren van platformen is een hardeningsrichtlijn beschikbaar.

- *Verwijzing naar leverancier/SANS/NIST/CIS met een vermelding van "pas toe of leg uit";*
- *Ook daadwerkelijk toepassen;*
- Wat "open" staat moet een reden hebben en wat "open" staat moet secure worden aangeboden.
- *De hardening van interne systemen mag minder stringent.*
  - *beheer functies moeten secure*
  - *geen onveilige protocollen*
  - *standaard wachtwoorden moeten zijn gewijzigd & applicaties verwijderen als deze niet worden gebruikt*

U/NW.03 (B1-1)

Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.

- DMZ en compartimentering d.m.v. (2 virtuele) firewalls;
- *materieel (feitelijk bestaan en inrichting van DMZ) als formeel qua opzet (netwerkschema of tekening);*
- *Aantonen van voldoende inzicht in de architectuur, zowel van het DMZ als van de systemen die zich daarin bevinden.*

U/NW.05 (B1-2)

Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.

- *Er is een inrichtingsdocument waaruit blijkt op welke wijze content beheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend;*
- Het gebruik van fysieke scheiding, veilige VPN verbindingen (zoals IPSec) of VLANs waardoor het beheer- en productieverkeer van elkaar wordt gescheiden.

U/NW.06 (B0-6)

Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.

- Hardeningrichtlijnen van de leverancier(s)/SANS/NIST/CIS met een vermelding van “pas toe of leg uit”;
- Alles wat open staat moet een reden hebben en alles wat open staat moet secure worden aangeboden;
- *Verplicht gebruik van DNSSEC;*
- *Actueel overzicht van de noodzakelijke netwerkprotocollen, -poorten en –services;*
- Uitschakelen van alle netwerkprotocollen, -poorten en –services uit, behalve de noodzakelijke;
- *Aanpassen van configuraties van netwerkcomponenten conform richtlijnen*

C.03 (B0-9)

Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICTcomponenten van de webapplicatie (scope).

- Netwerk based scan gericht te hebben op de hardening en patching van de infrastructuur en het detecteren van mogelijke kwetsbaarheden;
- *Vulnerability assessments vinden ook intern plaats minimaal een keer per jaar en vaker op basis van een risicoafweging;*
- Scope van het vulnerability assessment omvat de infrastructuur voor de webapplicatie.
- Actieplan om tekortkomingen op te heffen;
- *Voldoende voortgang in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen;*
- *Uitvoering door onafhankelijke partij.*

C.04 (B0-8)

Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).

- Voorkeur om enkele keren per jaar een penetratietest te laten uitvoeren;
- Penetratietest dient minimaal eenmaal per jaar te worden uitgevoerd *en na significante wijzigingen*;
- Scope is de webapplicatie voor het digitale loket;
- Actieplan om de tekortkomingen op te heffen.
- *Voldoende voortgang in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen;*
- *Uitvoering door onafhankelijke partij.*

Agenda

- Wie zijn wij?
- Risico's
- Wat verandert?
- Wat vervalt?
- Wat blijft hetzelfde?
- **Specifieke beveiligingsrichtlijnen deel 2**
- Vragen?

novàccent

BKBO

B.05 (B0-14)

In een contract met een derde partij voor de uitbestede levering of beheer van een web-applicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.

- door beide partijen ondertekend;
- een beschrijving van de diensten;
- *de relevante leveringsvoorwaarden;*
- *de relevante eisen vanuit het beveiligingsbeleid;*
- *het melden van beveiligingsincidenten en datalekken;*
- *de behandeling van gevoelige gegevens;*
- *toegang van de leverancier;*
- *Service Level Reporting;*
- *het jaarlijks uitvoeren van audits bij de leverancier(s);*
- *back-to-back sub-leveranciers.*

novaccent

BKBO

U/TV.01 (B0-12)

De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit, het toekennen van de rechten, het controleerbaar maken van het gebruik en het automatiseren van arbeidsintensieve taken.

- focus op beheerprocessen m.b.t. toegang tot de applicatie en webservers, de routers en de firewalls;
- *wachtwoordinstellingen cf wachtwoordbeleid*;
- *aantoonbare controle op joiners/movers/leavers*;
- wijzigen van de standaard wachtwoorden;
- *beperken eventuele shared accounts;*
- periodieke reviews;
- *wachtwoorden die leveranciers hebben voor toegang tot de systemen.*

novaccent

BKBO

U/WA.02

Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.

- *Functioneel en het applicatiebeheer;*
- *Beschrijving van taken, verantwoordelijkheden en bevoegdheden*
- *Autorisatiematrix*
- *Autorisatiebeheerproces voor het onderhouden en toekennen van beheerrollen*
- *Uitvoeren van een periodieke review.*

U/NW.04 (B7-1)

De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.

- Implementatie en het gebruik van IDS/IPS;
- Inkomend en uitgaand verkeer moet worden gemonitord om mogelijke aanvallen tijdig te detecteren en hier acties op te kunnen ondernemen;
- Voorkeur om gebruik te maken van een Intrusion Prevention Systeem (IPS) dat automatisch preventieve maatregelen neemt tegen bedreigingen;
- *Voorkeur voor plaatsen van het IDS of IPS na decryptie van het oorspronkelijk versleuteld netwerkverkeer omdat anders de inhoud van de berichten niet kan worden beoordeeld door het systeem.*

C.06 (B7-1)

In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.

- ingeperkt tot het detecteren van aanvallen met detectiesystemen in de webapplicatie-infrastructuur;
- C.06 richt zich op het tijdig signaleren van aanvallen;
- *Het definiëren van alarm situaties en drempelwaarden;*
- Het configureren van de alarm situaties en drempelwaarden in het IDS/IPS en het genereren van de bijbehorende alerts;
- *De inbedding van alert afhandeling in het incidentenbeheerproces inclusief een escalatieprocedure*.

C.07 (B7-8)

De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICTsystemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.

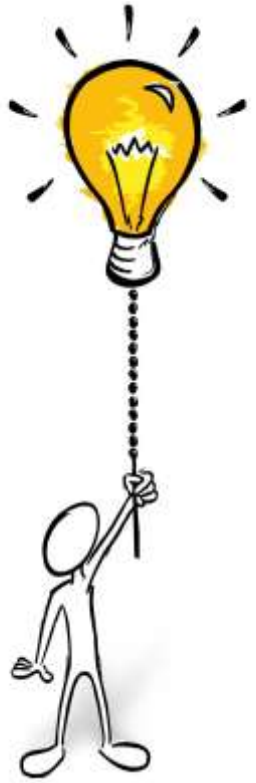
- ingeperkt tot het detecteren van aanvallen met detectiesystemen in de webapplicatie-infrastructuur
- *Procedurebeschrijving hoe en wanneer controles op logging moeten plaatsvinden en hoe taken belegd zijn.*
- *Het uitvoeren van periodieke controles op:*
  - wijzigingen aan de configuratie;
  - optreden van verdachte gebeurtenissen en schendingen van de beveiligingseisen;
  - ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden;
  - toegangslogs.

novaccent

BKBO

C.07 (vervolg)

- *Periodieke analyse op ongebruikelijke situaties (incidenten) die de werking van webapplicaties kunnen beïnvloeden.*
- *Periodieke rapportage van de geanalyseerde en beoordeelde gelogde gegevens*
- *Opvolging van bevindingen naar aanleiding van de analyse.*



novaccent

BKBO

C.08 (B0-5)

Wijzigingsbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.

- Alle wijzigingen moeten altijd eerst worden getest voordat deze in productie worden genomen en via wijzigingsbeheer worden doorgevoerd;
- *Ingeval formulieren worden gebouwd die beveiligingsrisico's introduceren is wijzigingenbeheer in scope;*
- *Bij SAAS-toepassingen ligt de verantwoordelijkheid doorgaans bij de leverancier en/of gebruikersgroep*.

C.08 (vervolg)

- Procedure, waarbij zo nodig onderscheid wordt gemaakt tussen wijzigingen op de applicatie, de servers en de netwerkcomponenten.
- *Het inrichten van een OTAP omgeving zodat wijzigingen eerst in een testomgeving worden getest voordat zij in productie kunnen worden;*
- *Het hanteren van een testscript en de vastlegging van de testresultaten.*
- Een formele acceptatie voor het in productie nemen;
- *Het beperken van het aantal personen die wijzigingen in productie kunnen nemen.*
- *Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het platform moet, bij voorkeur via penetratietest, worden onderzocht of er geen kwetsbaarheden zijn geïntroduceerd.*

C.09

Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.

- Patching proces kan gedifferentieerd zijn naar OS, DBMS en netwerk;
- Maandelijks patching cyclus is aanvaardbaar tenzij er security alerts zijn.
- Voor internet facing systemen de laatste stabiele beveiligingspatches te zijn geïnstalleerd.
- Indien patching niet mogelijk is moet dit risico aantoonbaar zijn afgewogen.

C.09 (vervolg)

- *Beleid/proces hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een kritieke patch en welke stadia moet de patch doorlopen.*
- *Registratie van patches met vastlegging of de patches niet, wel of versneld worden doorgevoerd.*
- Het tijdig doorvoeren van patches.

Vragen?

nováccent

Cybercrime

Gemiddeld klikt 30% van de medewerkers op phishing mails en laat gegevens zoals gebruikersnaam en wachtwoord achter

U heeft

TOEGANG

die cybercriminelen willen

Samen sterk

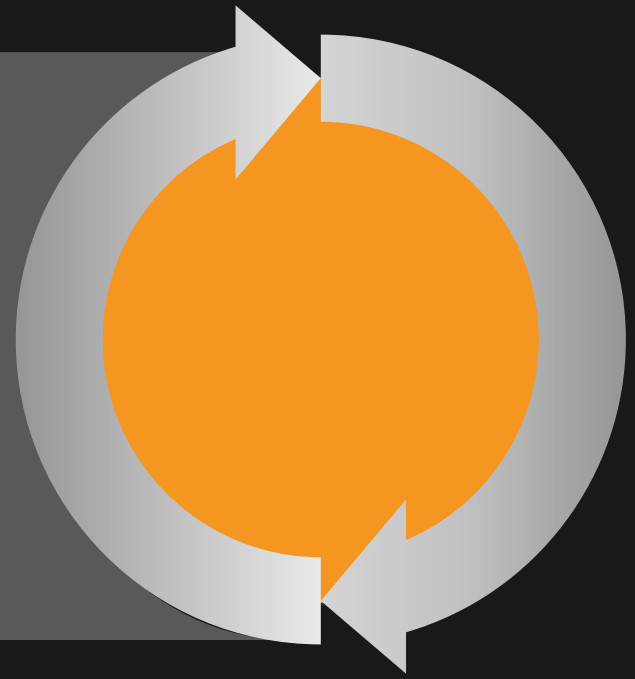
Gemeente aanpak

VAMP

VULNERABILITY ANALYTICS & MANAGEMENT PORTAL

TITAN

THREAT INTELLIGENCE & ANALYTICS



NOVASUITE


TITAN
VAMP
Cyber Security Sensor
SIEM 2.0
Vulnerability Management
BIG Compliance rapport
Bouwperiode
Q2 - Q4 2017
Eind 2017
Integrated Cyber Security Dashboard
TITAN
VAMP
VULNERABILITY ANALYTICS & MANAGEMENT PORTAL
NOVASUITE

Novaccent Innovations

Business Impact Analyse Tool

- Beoordeling van IT systemen en data op vertrouwelijkheid, integriteit en beschikbaarheid
- Koppeling BIA aan maatregelen
- (ISO 27001/BIG)
- Workflows en heldere dashboards

Gemeente Utrecht

BKBO

Bureau voor Kwaliteitsborging
bij de Overheid

Productportfolio

Productportfolio- PIA

- Onderzoek om de effectiviteit van de privacybescherming vast te stellen
- Mengvorm tussen audit en advies
- Gekoppeld aan een bedrijfsproces
- Documentenonderzoek
- Gerichte interviews
- Vastlegging cf auditnormen
- Cf werkwijze Norea en Autoriteit Persoonsgegevens
- Verplicht vanaf mei 2018

Productportfolio-Rekenkameronderzoek

- Effectiviteit van de informatiebeveiliging vast te stellen
- Status implementatie BIG
- Governance
- Bewustwording
- Inzoomen op de risico’s van een bedrijfsproces
- Combineren met phishingmail attack, mystery guest, wifi scan, infrascan, pentest door Nováccent

Vragen?

novàccent

BKBO
Bureau voor Kwaliteitsborging bij de Overheid