Website Security Checklist

Een overzicht van aandachtspunten bij het ontwikkelen en in gebruik nemen van internet websites en/of webmail

Nationaal Adviescentrum **Vitale Infrastructuur**

Versie: 1.0
Datum: 8-10-2008
Classificatie: Wit (Openbaar)

Inhoudopgave

1. Inleiding

1.1. Wat

Vrijwel alle bedrijven en organisaties hebben vandaag de dag een publiek toegankelijke website op het internet. Het overzicht gepresenteerd in dit document is een checklist met de meest relevante aandachtspunten om op te letten om een website op te zetten. De checklist is opgesteld onafhankelijk van het gekozen web platform.

1.1. NAVI

Het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) is een publiek-private samenwerking waar eigenaren en beheerders van de vitale infrastructuur in Nederland terecht kunnen voor informatie en advies op het gebied van beveiliging tegen moedwillige verstoring. Door het publiek-private karakter van het NAVI is de onafhankelijkheid gewaarborgd. De doelstelling van het NAVI is om de, fysieke en digitale beveiliging van de vitale sectoren in Nederland, daar waar nodig, op een hoger niveau te brengen.

1.2. Waarom

Websites zijn tegenwoordig een belangrijk, en soms zelfs het enige, communicatiemiddel van organisaties naar hun klanten, afnemers, zakenrelaties of het publiek. Websites trekken helaas ook de aandacht van kwaadwillenden. Naast openbare websites, kunnen deze ook informatie bevatten die bestemd is om alleen met een beperkte groep van personen gedeeld te worden. Het internet biedt de mogelijkheid om waar dan ook ter wereld een website fysiek onder te brengen, ongeacht wie deze beheert of welke personen toegang verkrijgen.

Het is belangrijk dat een website voldoende weerstand biedt tegen moedwillig menselijk handelen, per ongeluk voorkomende invoerfouten en betrouwbaar de gevraagde informatie aanbied aan geautoriseerde personen. Bovendien is het belangrijk om te weten waar een website zich fysiek bevindt, waar de data is opgeslagen, wie het beheer voert en toegang heeft, wie verantwoordelijk is en onder welke jurisdictie deze vallen. Een checklist kan helpen om deze aandachtspunten te verduidelijken.

1.3. Voor wie

Deze checklist is bedoeld als een relatief beknopt overzicht van aandachtspunten die ondernemingen en organisaties moeten helpen om minder kwetsbaar te worden voor cyberaanvallen op hun website omgeving. De lijst is gebaseerd op de meest voorkomende zwakke plekken in de beveiliging ten aanzien van de organisatie, beheer en technische aspecten van een website.

Dit document is bestemd voor managers en projectleiders die opdracht geven tot het opzetten van een website, ontwikkelaars van websites en beheerders. Het document is niet geclassificeerd.

1.4. Website beveiliging

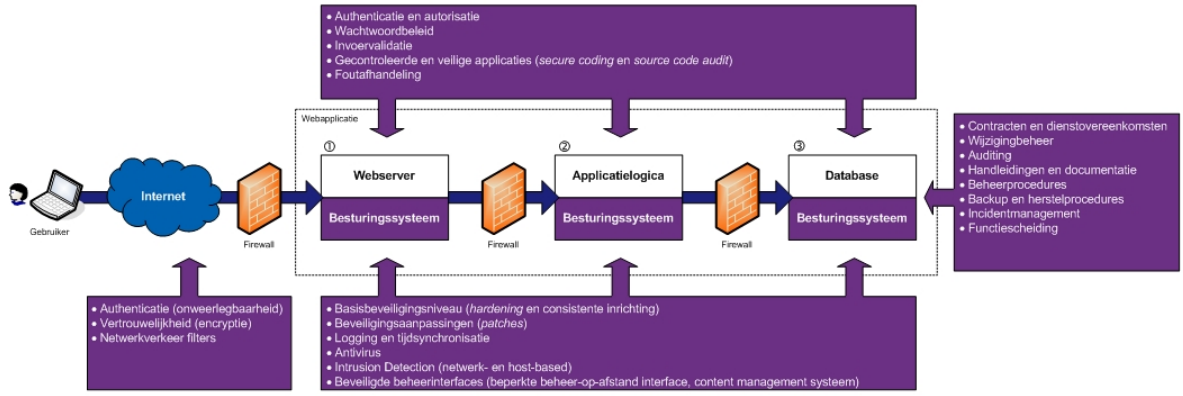
Typisch is een website opgebouwd uit drie logische componenten; een webserver, applicatielogica en data. De webserver verzorgt de communicatie met de gebruiker. Veel gebruikte webservers zijn Apache en Microsoft IIS. De applicatielogica is de tussenlaag die bijvoorbeeld controles kan uitvoeren of keuzes maakt voor het tonen van specifieke gegevens, afhankelijk van de ontvangen informatie. Toegepaste technieken op de applicatielaag zijn bijvoorbeeld ASP, .NET en PHP. De gegevens die een website toont, of de informatie aangeboden door een gebruiker, worden opgeslagen op de datalaag. Hiervoor kunnen eenvoudige tekstbestanden worden gebruikt maar vaker worden databases zoals MySQL, Microsoft SQL Server of Oracle gebruikt.

Bij de beveiliging van websites dient de aandacht niet beperkt te blijven tot alleen de technische architectuur maar ook zaken als de wijze van beheer, wijzigingbeheer en de omgang met incidenten moet zijn geregeld. De meeste succesvolle aanvallen op websites maken nog steeds gebruik van slechts een beperkt aantal verschillende categorieën zwakheden, te weten:

- Onvoldoende controle op de invoer van gegevens (filtering);
- Niet bijhouden van (beveiligings)aanpassingen (patches);
- Gebrekkige implementatie van systemen en applicaties;
- Zwakke authenticatie en autorisatie methoden.

Zwakke controle op aangeboden informatie van de gebruiker kan bijvoorbeeld worden misbruikt voor het meegeven van extra opdrachten aan zoekopdrachten in de database (*SQL injection*) of het ongemerkt doorverwijzen naar andere (kwaadaardige) websites (*cross site scripting*). Daarnaast kan achterstallig beheer van de website leiden tot het blijven voortbestaan van bekende zwakke plekken. Gebreken in de wijze van implementeren is vaak de oorzaak dat standaard wachtwoorden blijven bestaan of dat ongebruikte services blijven geactiveerd.

Een website waarbij de risico's kunnen worden beheerst, gaat uit van een deugdelijk ontwerp, vastgelegde (beheer)afspraken en een afgestemd pakket van beveiligingsmaatregelen. Een vastgesteld basisbeveiligingsniveau en een gelaagd pakket van beveiligingsmaatregelen (*defence in depth*) vergroot hierbij de weerstand en veerkracht tegen aanvallen. De onderstaande figuur illustreert de logische opbouw van een webapplicatie en enkele voornaamste categorieën van mogelijke maatregelen[1].



1.5. Verdere ontwikkeling

De voorliggende uitgave is een eerste versie. Lezers worden van harte uitgenodigd hun ervaringen en expertise met ons te delen opdat wij het document verder met en voor u kunnen blijven ontwikkelen.

1.6. Ondersteuning van NAVI

Dit document geeft de lezer informatie en handvaten om zelfstandig te werken aan de beveiliging binnen de eigen organisatie. Heeft u echter na het lezen van deze uitgave vragen, dan kunt u contact opnemen met het NAVI via info@navi-online.nl of 070-376 59 50.

[1] Eerder gepubliceerd door J. van Beek (KPMG IT Advisory) in ISACA Chapnews, Netherlands Chapter, augustus 2008.

2. Aandachtspunten t.a.v. documentatie

#	Omschrijving	Voldoet
D.1	**Contracten en dienstenovereenkomsten** (*service level agreements*). Er is een contract en een dienstenovereenkomst (*Service Level Agreement*) met alle betrokken partijen. Contracten en overeenkomsten leggen tevens afspraken t.a.v. vertrouwelijkheid, het omgaan met beschikbaar gestelde informatie en jurisprudentie vast.	
D.2	**Installatie handleidingen**. De installatie handleidingen zijn dusdanig dat deze voor een systeembeheerder (die niet bekend is met eventuele specifieke maatwerk configuraties) voldoende informatie biedt om de productiesystemen volledig opnieuw op te bouwen.	
D.3	**Beheerprocedures**. De beheerprocedures omvatten tenminste: • Gebruikersbeheer (aanmaken, wijzigen, deactiveren en verwijderen); • Wijzigen van wachtwoorden; • Toekennen en wijzigen van autorisaties; • Bekijken en/of wijzigen van specifiek voor het systeem benodigde instellingen; • Starten/stoppen van services; • Backup en herstel; • Bekijken van logbestanden; • Wijzigingsprocedures (*patchmanagement*); • Overzicht van mogelijke foutcodes; • Overzicht van specifieke foutherstel procedures; • Onderhoudsinstructies;	
D.4	**Functioneel beheer / moderator handleidingen**. De handleidingen omvatten tenminste: • De aanmeldprocedure; • Gebruikersbeheer handelingen; • De wijze waarop berichten kunnen worden bekeken, verwijderd en gearchiveerd; • De wijze waarop documenten kunnen worden toegevoegd, verwijderd en gearchiveerd;	
D.5	**Technische documentatie**. De technische documentatie omvat tenminste: • Overzichtstekening van infrastructuur en netwerk; • Beschrijving van de (hardware) configuraties, gebruikte software en versienummers; • Beschrijving per platform (OS, services, netwerkpoorten); • Overzicht van alle (netwerk)connecties, VPN's en met (externe) systemen; • Overzicht van gebruikt domeinnamen en DNS systemen; • Lijst van gebruikersaccounts; • Autorisatiematrix; • Overzicht van getroffen beveiligingsmaatregelen; • Overzicht van alle maatwerkaanpassingen en scripts; • Lijst van firewall regels; • Lijst van specifieke IDS regels (indien aanwezig); • Specificatie van gebruikte encryptie protocollen; • Overzicht van beveiligingsinstellingen (incl. *hardening* configuratie); • Locatie van encryptiesleutels;	

3. Algemene aandachtspunten

#	Omschrijving	Voldoet
A.1	De websites, servers en database systemen met alle daarop opgeslagen informatie bevinden zich fysiek in Nederland.	
A.2	De fysieke locatie is alleen toegankelijk voor bevoegde personen. De locatie is niet toegankelijk voor derden. Bezoekers moeten vooraf zijn aangemeld en worden permanent begeleid. Er wordt een bezoekersregister bijgehouden.	
A.3	Alle systemen zijn aangesloten op noodstroomvoorzieningen en ondergebracht in een geconditioneerde en permanent bewaakte en gecontroleerde ruimte. De ruimte is voorzien van een gecertificeerde inbraakalarmvoorziening.	
A.4	De beschikbare bandbreedte is voldoende voor de nominale verwachte belasting en eventuele (kortstondige) piekbelastingen. Bijvoorkeur zijn er extra maatregelen getroffen om *denial-of-service* aanvallen te weerstaan.	
A.5	De minimale beschikbaarheid is in overeenstemming met de vereisten vastgelegd in een dienstenovereenkomst (SLA). Onderhoudsvensters zijn vastgelegd.	
A.6	De minimale reactietijd bij (beveiligings)incidenten en (technische) storingen binnen en buiten kantoortijden zijn in een dienstenovereenkomst (SLA) vastgelegd. De reactietijd is in overeenstemming met de overige vastgelegde vereisten.	
A.7	Leveranciers hebben onderliggende contracten en overeenkomsten met onderleveranciers (*back-to-back agreements*).	
A.8	Indien overeengekomen in een contract of dienstenovereenkomst (SLA), is er een responseplan waarin tenminste is vastgelegd welke acties (op hoofdlijnen) worden ondernomen als de website (mogelijk) gecompromitteerd is.	
A.9	Er wordt gebruik gemaakt van een beveiligde website beheer toepassing (*content management systeem*) en technische systeembeheer voorzieningen (*SSH, VPN*).	
A.10	Alle beheerders hebben een eigen individuele beheeraccount. Er is geen algemene beheeraccount.	
A.11	Beheerders (technisch en functioneel) kunnen alleen worden toegevoegd na toestemming van de eigenaar van de website.	
A.12	De websites, servers en database systemen zijn beschermd met één of meerdere aparte *firewalls*. Bijvoorkeur worden tevens *intrusion detection systemen* (IDS) gebruikt.	
A.13	De websites, servers en database systemen zijn beschermd met of door een anti-virus oplossing.	
A.14	De specifieke beveiligingssystemen zijn gescheiden van de website en onderliggende systemen. Functies als een *firewall* en *IDS* zijn op afzonderlijke systemen ondergebracht.	

#	Omschrijving	Voldoet
A.15	Bijvoorkeur is het beheer van specifieke beveiligingssystemen zoals een firewall en IDS, is ondergebracht bij een gespecialiseerde (interne of externe) beheerder. Deze beheerder heeft geen bijzondere rechten of privileges op de websites, servers en database systemen. Omgekeerd hebben de website- of systeembeheerders en/of database administrators geen beheerpermissies op beveiligingssystemen (*functiescheiding*).	
A.16	Bijvoorkeur worden de systemen en applicaties 24 x 7 x 365 bewaakt op beveiligingsincidenten (*managed security monioring*).	
A.17	Bijvoorkeur wordt een application-level firewall gebruikt.	
A.18	Er worden regelmatig beveiligingskopieën (*backups*) gemaakt van de website. Het kunnen herstellen d.m.v. de backups is op een aparte omgeving getest. Kopieën van de testdata worden na afloop weer verwijderd.	
A.19	Er zijn procedures om regelmatig nieuwe (beveiligings)aanpassingen, van bijvoorbeeld de leverancier, te implementeren.	
A.20	Bijvoorkeur wordt beveiligingsniveau van de website regelmatig geverifieerd, bijvoorbeeld door het gebruik van geautomatiseerde scanners[2].	

[2] Let op: Voor het uitvoeren van beveiligingscontroles zoals het gebruik van scanners, is een formele toestemming nodig van (alle) eigenaren van de website(s) en server(s).

4. Technische aandachtspunten

#	Omschrijving	Voldoet
T.1	De besturingssystemen moeten veilig zijn geconfigureerd in overeenstemming met bekende *good practice* richtlijnen (*hardening*). Onnodige services zijn uitgeschakeld, ongebruikte gebruikeraccounts en overbodige bestanden zijn (waar mogelijk) verwijderd. De getroffen (hardening) maatregelen zijn gespecificeerd dan wel wordt verwezen naar de gevolgde richtlijnen.	
T.2	De web-engine(s) moet(en) veilig zijn geconfigureerd in overeenstemming met bekende *good practice* richtlijnen (*hardening*). Waar mogelijk worden http verzoeken genormaliseerd, alleen benodige http methoden toegestaan, zijn bestandextensies beperkt, vindt http header validatie plaats en zijn 'directory listings' uitgeschakeld.	
T.3	De database(s) moet(en) veilig zijn geconfigureerd in overeenstemming met bekende *good practice* richtlijnen (*hardening*).	
T.4	Alle beveiligingsaanpassing (patches) moeten zijn geïnstalleerd voor zowel het besturingssysteem, web-engine(s), database(s) en applicatie(s).	
T.5	De website en alle achterliggende systemen zijn beschermd door een firewall die tenminste al het ongebruikte netwerkverkeer blokkeert.	
T.6	Als de website extern gericht is (internet), dient deze alleen data te bevatten die de gehele wereld mag zien (openbaar). De server en onderliggende systemen waarop de website functioneert bevat in overeenstemming alleen data die iedereen mag zien. Gebruikers, moderators en beheerders worden er opgewezen als ze een document, bericht of andere inhoud wensen te publiceren op het openbare deel van de website. Deze notificatie vindt plaats voordat de data daadwerkelijk wordt gepubliceerd of zich bevindt op het openbaar toegankelijk gedeelte van de website of de onderliggende systemen. De desbetreffende gebruiker heeft de gelegenheid om de handelingen te annuleren of ongedaan te maken.	
T.7	Als de website data bevat die niet door de gehele wereld mag worden gezien, dient de website niet direct extern te benaderen te zijn. De server en onderliggende systemen waarop de website functioneert zijn in overeenstemming niet van buitenaf benaderbaar. Er wordt bijvoorbeeld gebruik gemaakt van een proxy, portaalsysteem of een (extra) firewall.	
T.8	Alle test-, ontwikkel-, backup- en andere overbodige bestanden dienen te zijn verwijderd van de actief in gebruik zijnde (productie) website.	
T.9	Alle systeembeheer en website beheer toepassingen zijn alleen toegankelijk vanaf interne netwerken of vanaf vooraf ingestelde IP-adressen.	
T.10	Er worden aparte accounts gebruikt voor beheertaken. Authenticatie van beheer toegang tot de systemen en website beheer toepassingen dienen tenminste te voldoen aan het eigen beveiligingsbeleid van de organisatie ten aan zien van gebruikersaccounts en wachtwoorden[3]. Bijvoorkeur hebben beheerders sterke authenticatie nodig (*token*).	
T.11	Indien de website beschikt over een besloten gedeelte of een individueel deel voor iedere gebruiker, vindt authenticatie plaats door middel van individuele gebruikersaccount. Deze voldoen aan het eigen beveiligingsbeleid van de organisatie ten aan zien van gebruikersaccounts en wachtwoorden. Bij voorkeur wordt een I&AM oplossing gebruikt.	

[3] Bijvoorbeeld een basisniveau dat gebruikersaccounts blokkeert na 3x verkeerd aanmelden en verplicht om wachtwoorden tenminste iedere 90 dagen te wijzigen. Wachtwoorden moeten bestaan uit een combinatie van normale en toegestane bijzondere karakters met een totale lengte van 7 karakters of meer.

#	Omschrijving	Voldoet
T.12	Alle standaard wachtwoorden (zowel van besturingssystemen, CMS en databases) zijn aangepast. Er worden geen voor de hand liggende gebruikeraccount en wachtwoorden gebruikt. Bij voorkeur wordt het wachtwoordbeleid afgedwongen.	
T.13	Indien de website beschikt over een besloten gedeelte of een individueel deel, wordt een gebruiker afgemeld wanneer geen activiteit plaatsvindt of als de verbinding na 30 minuten niet meer onderhouden.	
T.14	Indien de website beschikt over een besloten gedeelte of een individueel deel, moeten gebruikeraccounts worden goedgekeurd door een website beheerder of moderator nadat alle benodigde gegevens zijn ontvangen. Bijvoorkeur ontvangt de beheerder en/of moderator automatisch per email een melding als een nieuwe gebruiker zich aanmeldt.	
T.15	Een gebruiker kan pas een gebruikersaccount aanvragen als alle benodigde gegevens zijn verstrekt en als de voorwaarden zijn geaccepteerd.	
T.16	Een gebruikeraccount kan pas worden gebruikt nadat deze is goedgekeurd door de beheerder/moderator. Bijvoorkeur ontvangt de gebruiker hiervan automatisch een email bericht.	
T.17	Voor het goedkeuren van gebruikersaccounts, berichten geplaatst door gebruikers, forum berichten (*postings*) etc. kunnen delen van het beheer van de website worden toegewezen aan meerdere beheerders/moderators.	
T.18	Gebruikersaccounts kunnen worden toegevoegd aan gebruikersgroepen en/of rollen. Gebruikers kunnen lid zijn van meerdere gebruikersgroepen. Bij het gebruik van gebruikersrollen is de gebruiker slechts lid van één rol. Toegangsrechten tot besloten delen van de website of informatie vindt plaats op individueel of gebruikersgroep/rol niveau.	
T.19	Indien de website beschikt over een besloten gedeelte of een individueel deel, is het basis niveau van toegang tot alle informatie in het besloten deel GEEN TOEGANG.	
T.20	Indien de website beschikt over een besloten gedeelte, is alle informatie aangeboden in het besloten deel voorzien van een classificatieniveau. Toegang wordt alleen verstrekt aan gebruikers die beschikken over de juiste autorisatie (zoals het lid zijn van de overeenkomstige gebruikersgroep voor toegang op het desbetreffende classificatieniveau).	
T.21	Indien de website beschikt over een besloten gedeelte, blijft de vertrouwelijkheid van alle informatie opgeslagen in het besloten deel gehandhaafd wanneer van de website en onderliggende systemen een veiligheidskopie (*backup*) wordt gemaakt. De veiligheidskopie is bijvoorkeur versleuteld.	
T.22	Alle website (beheer) toepassingen gebruiken versleuteling om te voorkomen dat gebruikersgegevens en wachtwoorden kunnen worden gecompromitteerd tijdens transport.	
T.23	Alle website (beheer) toepassingen gebruiken versleuteling om te voorkomen dat gebruikersgegevens en wachtwoorden kunnen worden gecompromitteerd wanneer deze zijn opgeslagen.	
T.24	Vertrouwelijk informatie en *cookies* zijn versleuteld. Bij voorkeur wordt gebruik gemaakt van elektronische handtekeningen waar relevant.	
T.25	Indien meerdere (virtuele) websites actief zijn op hetzelfde platform, heeft iedere website zijn eigen virtuele hostname. Website adressen zoals www.navi-online.nl/kennisknooppunt moeten worden vermeden.	
T.26	De website en alle onderliggende systemen beschikken over een nauwkeurige tijdregistratie die (onderling) is gesynchroniseerd.	

#	Omschrijving	Voldoet
T.27	De website en alle onderliggende systemen houden een uitgebreid gebeurtenissen logboek bij. Het gebeurtenissen logboek is beveiligd tegen manipulatie en wissen.	
T.28	Zoekmachines respecteren de beveiligingsinstellingen en de autorisaties toegekend aan de (internet) gebruiker. Zoekmachines tonen alleen resultaten voor documenten waartoe de desbetreffende gebruiker gemachtigd is.	
T.29	Gebruik alleen database systemen die een uitgebreid granulair niveau van permissies binnen de database toestaan. Database systemen zoals MSAccess, Foxpro en DB zullen niet worden gebruikt.	
T.30	Iedere website gebruikt een eigen database. Het delen van databases met meerdere websites is niet toegestaan.	
T.31	Iedere website gebruikt voor elke database een afzonderlijk account waarmee de publieke internet website gebruiker de database bevraagd. Dit account heeft een extreem robuust wachtwoord.	
T.32	De account gebruikt voor het bevragen van de database door de publieke internet website gebruiker heeft zo min mogelijk permissies binnen de database (alleen query permissie).	
T.33	Website service accounts[4] hebben alleen leesrechten op de directories van de website. Uitvoer- (*execute*) en scriptrechten worden beperkt gebruikt en alleen op speciaal daarvoor ingerichte directories. De website service accounts hebben op de rest van de file systemen op de server(s) expliciet geen rechten (*deny*) tenzij absoluut noodzakelijk voor het functioneren van de website.	
T.34	Alle web formulieren bevatten aanwijzingen voor het invullen door de website gebruiker en zijn voorzien van een waarschuwing om geen gevoelige informatie via het web formulier aan te bieden.	
T.35	Alle web formulieren (*forms*) moeten zijn beschermd tegen het meerdere malen aanbieden van de data.	
T.36	Web formulieren met een email optie dienen te zijn beveiligd zodat deze niet kunnen worden misbruikt voor het verzenden van andere email (*mail relay*) of uit naam van een ander (*spoofing*).	
T.37	Ieder bestand, inclusief *cookies*, die invoervalidatie kunnen uitvoeren, moeten dit doen. Bestanden van zoals .asp, .aspx, .php, .jsp, .pl, .cfm, etc. moeten allemaal invoervalidatie uitvoeren om te garanderen dat variabelen die worden doorgegeven voldoen aan de verwachte variabelen, niet meer en niet minder.	
T.38	Invoervalidatie vindt plaats door middel van een lijst van toegestane goede invoer. Invoer validatiefilters laten alleen verwachte data door en blokkeren alle onverwachte data. Het filteren op basis van alleen 'foute invoer' en foute karakters is onvoldoende.	
T.39	Wanneer een invoervalidatie faalt, wordt door de website een (404) melding terug gegeven. Bij voorkeur wordt de standaard (404) melding gebruikt.	
T.40	Wanneer een bestand of directory die niet bestaat wordt opgevraagd, wordt door de website een (404) melding terug gegeven. Bij voorkeur wordt de standaard (404) melding gebruikt.	

[4] zoals de *IUSR account* op Microsoft IIS platformen.

#	Omschrijving	Voldoet
T.41	De website moet voor de meeste gangbare browsers (Internet Explorer, Firefox, Safari, Opera) beschikbaar zijn, op zodanige wijze dat ook browsers met een hoge beveiligingsinstelling niet belemmerd worden in hun toegankelijkheid. Het gebruik van javascripts, Java, AxtiveX, pop-up vensters en plug-ins is beperkt en bijvoorkeur geheel niet vereist.	
T.42	Filters geïmplementeerd op het niveau van de web server, onderscheppen fout of moedwillig aangepaste URL's en geven een (404) melding terug voor iedere URL die wordt geblokkeerd door de filters. Voor bestandsnamen worden de volgende extensies geblokkeerd en een (404) melding teruggegeven: *.asp *.aspx *.bak *.bat *.cdx *.cer *.cfg *.cmd *.com *.conf *.dbf *.dll *.exe *.htr *.log *.mdb *.old *.php *.rar *.udl *.zip De volgende (combinatie van) karakters worden eveneens geblokkeerd en een (404) melding teruggegeven: .. . / \ : % & # < > $ @ ! , ~ ‘ ” ( ) ; = .c _derived _vti admin backup bak bkup etc netcat nobody odbc passwd password root temp test w3svc	
T.43	De netwerkverbindingen over publieke telecommunicatie verbindingen (internet) van/naar de website zijn beveiligd door middel van SSL 3.1 / TLS 1.1 (of beter). Het hiervoor toegepaste X509 certificaat is via publieke services verifieerbaar voor bezoekers van de website. Bij voorkeur kunnen website bezoekers de betrouwbaarheid van de website eenvoudig herkennen en verifiëren door het tonen van een bijbehorend website veiligheidszegel.	
T.44	De website en onderliggende servers ondersteunen de volgende standaarden (of beter) wanneer cryptografische bewerkingen (versleutelingen) dienen te worden uitgevoerd: • SSL 3.1 of TLS 1.1 voor het beveiligen van de communicatie van en naar de website zoals gedefinieerd in RFC 4346; • SHA-256 voor hash functies zoals gedefinieerd in de ISO/IEC 10118-3, FIPS PUB 180-2 en ETSI TS 102 176-1 standaarden; • AES-256 voor symmetrische cryptografie functies zoals gedefinieerd in de FIPS PUB 197 standaard; • RSA-1024 voor asymmetrische cryptografie functies zoals gedefinieerd in de IETF RFC 3447 en ETSI TS 102 176-1 standaarden; • ETSI TS 101 733 Electronic Signature Formats en de FIPS PUB 186-2 standaarden voor elektronische handtekeningen; • CEN norm CWA 14170 voor ondersteuning met gekwalificeerde certificaten; • CEN norm CWA 14171 voor de verificatie van elektronische handtekeningen.	

5. Verwijzingen

Onder andere op de volgende websites zijn aanvullende (specifieke) controlelijsten en aanvullende informatie verkrijgbaar:

http://www.govcert.nl *(Raamwerk Beveiliging Webapplicaties)*

http://www.navi-online.nl

http://www.cpni.gov.uk/Products/guidelines.aspx

http://iase.disa.mil/stigs/checklist/index.html

http://checklists.nist.gov/

http://www.sans.org

http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp

http://www.cisecurity.org/

http://www.nsa.gov/snac/downloads_redhat.cfm?MenuID=scg10.3.1.1

http://www.cert.org/tech_tips/usc20_full.html

http://www.microsoft.com/technet/archive/security/chklist/xpcl.mspx?mfr=true

https://www.securityforum.org/

http://www.getsafeonline.org/