Veilig Zakelijk Internetten

Ben jij wel goed beveiligd?

De belangrijkste vragen voor mijn:

webdeveloper en hoster

Wie is er verantwoordelijk voor het uitvoeren van het onderhoud (m.n. de installatie van patches en updates) op mijn website of -applicatie?

Welk antwoord mag u verwachten?
U mag een duidelijk antwoord verwachten wie waarvoor verantwoordelijk is. Wellicht bent u zelf ook verantwoordelijk voor het uitvoeren van bepaalde patches en updates; indien u hiertoe niet in staat bent of niet weet hoe dat moet, maak dan duidelijke afspraken.

Extra informatie
Bij een website of –applicatie is het van belang dat periodiek onderhoud wordt uitgevoerd op de webserver (veelal verantwoordelijkheid van de hoster) én op de webpagina's (verantwoordelijkheid van de webdeveloper of van ú). M.n. bij het gebruik van Content Management Systemen (CMS), zoals Wordpress, drupal, Joomla of Magento, zien we dat blijkt dat er géén duidelijke afspraken zijn gemaakt wie verantwoordelijk is voor het onderhoud van de webpagina's met als gevolg dat het onderhoud niet wordt uitgevoerd.

Maak duidelijke afspraken wie-waarvoor verantwoordelijk is (veelal wordt de webdeveloper verantwoordelijk gesteld voor de applicatie/CMS en de hoster voor de webserver).

De beveiliging is voor een belangrijk gedeelte afhankelijk van het uitvoeren van het onderhoud op de diverse systemen. Door duidelijk te weten wie verantwoordelijk is voor welk deel van het onderhoud kunt u het beveiligingsniveau veelal al direct verbeteren.

Maakt mijn site gebruik van de nieuwste internetstandaarden zoals DNSSec en IPv6?

Welk antwoord mag u verwachten?
Zorg er voor dat u inzicht krijgt in of uw website of –applicatie voldoet aan de nieuwste internetstandaarden.

Doe de test op www.internet.nl of **www.veiliginternetten.nl/academy** voor een gratis controle op uw website.

Maak vervolgens een plan om een dergelijke scan periodiek uit te voeren en spreek dit door met uw webdeveloper of –hoster.

Extra informatie
De nieuwste internetstandaarden zorgen er voor dat uw site veiliger zal zijn. Op www.internet.nl kunt u een test doen op het gebruik van de laatste internetstandaarden. Op **www.veiliginternetten.nl/academy** kunt u een test doen, waarbij – naast de nieuwste internetstandaarden – ook direct wordt gecontroleerd op kwetsbaarheden op uw website.

Wordt er periodiek een controle op kwetsbaarheden uitgevoerd om zeker te weten dat we geen online risico's lopen? Kun je mij rapportages van het afgelopen jaar opleveren?

Welk antwoord mag u verwachten?
Zorg er voor dat u inzicht krijgt in de wijze waarop dit voor uw organisatie is geregeld. Overigens is het (periodiek) uitvoeren van scans op kwetsbaarheden van de website of –applicatie bij veel organisaties nog geen gemeengoed. Schijf u in op www.veiliginternetten.nl/academy voor een gratis controle op uw website. Maak vervolgens een plan om een dergelijke scan periodiek uit te voeren en spreek dit door met uw webdeveloper of –hoster.

We adviseren om minimaal jaarlijks een controle uit te voeren (voor kritische systemen vaker, bij voorkeur minimaal maandelijks).

Extra informatie
Per maand worden er wereldwijd zo'n 1.000 nieuwe kwetsbaarheden in hard- en software gevonden. Daarnaast kan het zijn dat een webdeveloper een foutje maakt, waardoor gegevens die niet openbaar mogen zijn bijvoorbeeld eenvoudig vanaf het internet door een kwaadwillende kan worden benaderd. De 10 meest gevonden kwetsbaarheden worden beschreven in de OWASP top-10.

Door de wetgever wordt geadviseerd om periodiek controles op kwetsbaarheden uit te voeren.

Op www.veiliginternetten.nl/academy kunt u een kosteloze test op uw website laten uitvoeren, waarbij direct wordt gecontroleerd op het gebruik van de laatste internetstandaarden (zie alinea direct hieronder). Daarnaast worden ook controles uitgevoerd op mogelijk misbruik van uw E-mail systeem (zgn. controle op spoofing. Spoofing zorgt er voor dat een kwaadwillende eenvoudig E-mails uit uw naam kan versturen).

Is mijn site beschermd tegen (Distributed) Denial of Service (D)DoS aanvallen?

Welk antwoord mag u verwachten?
Indien een anti (D)DoS oplossing wordt ingezet, krijg dan ook duidelijk wie verantwoordelijk is voor het bijhouden van het anti (D)DoS systeem.

Extra informatie
Een (D)DoS aanval zorgt er voor dat u (vanaf 1 of meerdere plekken) veel verkeer naar uw website krijgt waardoor deze overbelast kan raken. Er zijn mogelijkheden om u hiertegen te beschermen (meestal wordt dit niet standaard geleverd bij een hosting pakket). Bepaal in overleg met uw webdeveloper of –hoster of dit nodig is voor uw website of –applicatie.

Hebben wij een back-up procedure en kun je aangeven wanneer deze voor het laatste is getest, waarbij ook werkelijk is gekeken dat alle data van de back-up teruggezet kan worden?

Welk antwoord mag u verwachten?
Zorg er voor dat u inzicht krijgt in de back-up procedure, d.w.z. wanneer worden er back-ups gemaakt en op welke momenten wordt gecontroleerd dat deze werken en ook teruggezet kunnen worden in het geval van een calamiteit. Spreek verder door dat er een wachtwoord op de back-ups wordt gezet, dat de gegevens versleuteld worden opgeslagen en dat de gegevens van de back-up alleen over beveiligde verbindingen wordt getransporteerd.

Extra informatie
Bij een calamiteit zijn 2 dingen van belang, nl. de gegevens die verloren zijn gegaan op het moment van de calamiteit (in het geval van een dagelijkse back-up zal dit maximaal 24 uur zijn) en de tijd die het kost om weer up-and-running te zijn (hoe snel kan een back-up weer teruggezet worden). Uiteraard is dit laatste afhankelijk van het soort calamiteit Spreek dit dus met uw webdeveloper en - hoster door.

Welke (groepen) gebruikers hebben rechten voor beheer en onderhoud op de website?

Welk antwoord mag u verwachten?
Zorg er voor dat u inzicht krijgt in uw autorisatiematrix (welke gebruikers(groepen) hebben rechten tot welke data/applicaties en welke gebruikers kunnen beheerstaken uitvoeren). Zorg voor een beleid voor het gebruik van een bepaalde lengte en/of moeilijkheidsgraad van wachtwoorden. M.n. de lengte van het wachtwoord is van belang (hoe langer, hoe lastiger te achterhalen voor een kwaadwillende). Overleg met uw webdeveloper en/of –hoster hoe dit is ingeregeld.

Extra informatie
Regelmatig worden default gebruikersnamen of wachtwoorden gebruikt, waardoor een website of –applicatie volledig overgenomen kan worden door een kwaadwillende. Dit kan leiden tot diefstal van data, maar ook tot (geautomatiseerde) inzet van uw website of –applicatie voor zogenaamde botnets. Zorg dus voor een adequaat beschermingsniveau.

Maken we gebruik van SSL certificaten voor beveiligde gegevensoverdracht?

Welk antwoord mag u verwachten?
Zorg er voor dat u inzicht krijgt in de wijze waarop dit voor uw organisatie is geregeld. Indien u persoonsgegevens opvraagt (bijvoorbeeld in een contactformulier) dan bent u feitelijk al verplicht om dit versleuteld te doen. Zorg er dus voor dat u SSL certificaten op uw website of –applicatie gebruikt.

Extra informatie
Een SSL certificaat zorgt voor versleuteling van gegevens, waardoor deze beveiligd worden getransporteerd tussen uw website en de bezoeker. Daarnaast leveren websites die zijn voorzien van SSL een hogere ranking op in zoekmachines.

Voor de gebruiker is het gebruik van SSL direct zichtbaar door een groen slotje in de navigatiebalk. Er zijn diverse soorten SSL certificaten te verkrijgen (bijvoorbeeld met extra validatie). Vraag bij uw webdeveloper of hoster naar de mogelijkheden indien u nog geen SSL certificaat gebruikt.

Op welke wijze is er bij de opzet van onze website of webapplicatie al voor gezorgd dat security is ingebed in het systeem?

Welk antwoord mag u verwachten?
Bij voorkeur is een website of –applicatie opgezet conform de beveiligings-richtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC). We verwijzen naar de inhoud van **dit document**.

Extra informatie
Deze vraag is vooral van belang indien u een webapplicatie heeft of belangrijke data of persoonsgegevens via uw website of -applicatie verwerkt.

Op welke wijze worden belangrijke data en (privacy) gevoelige data opgeslagen?

Welk antwoord mag u verwachten?
Bij voorkeur is een website of –applicatie opgezet conform de beveiligings-richtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum (NCSC). We verwijzen naar de inhoud van **dit document**.

Extra informatie
Deze vraag is vooral van belang indien u een webapplicatie heeft of belangrijke data of persoonsgegevens via uw website of -applicatie verwerkt.

Wordt er gebruik gemaakt van een Intrusion Detection System (IDS) en/of -Prevention (IDP) systeem?

Welk antwoord mag u verwachten?
Indien een IDS/IDP wordt ingezet, krijg dan ook duidelijk wie verantwoordelijk is voor het bijhouden van het IDS/IDP.

Extra informatie
Een IDS/IDP zorgt er voor dat bij vreemd gedrag op uw website direct wordt geconstateerd en de sessie van de gebruiker die dat gedrag veroorzaakt wordt afgebroken. Bepaal in overleg met uw webdeveloper of –hoster of dit nodig is voor uw website of –applicatie.

Op www.veiligzakelijkinternetten.nl/zakelijk kunt u een kosteloze test op uw website en bedrijfsnetwerk laten uitvoeren.

Laat de Cyber Risico Scan gratis uitvoeren!