Criteria voor een veilige webwinkel

Datum: juni 2008
Projectleden:
E. Coffy, Koopgemak
C. de Jong, Prismarc Communicatieadvies
W.A.M. Jongen, Thuiswinkel.org
B. Koelewijn, Information Risk Control B.V.
T. Masseur, Thuiswinkel.org
P. Overbeek, ECP.NL
A. Posthumus, HBD
F. Schasfoort, Easer
A. van Slooten, Wehkamp
X. van der Voort, ECP.NL

Inhoudsopgave

1. Maak uw webwinkel veilig! Voor u en uw klanten

Als webwinkelier wordt u geconfronteerd met bedrijfsrisico's die specifiek zijn voor de webwinkel. Dat komt omdat uw verkoopkanaal afhankelijk is van de goede werking van uw computersystemen en uw verbinding met het Internet. Omdat uw computersystemen van buitenaf toegankelijk zijn, kunnen uw computers kwetsbaar zijn voor spam, virussen, spyware en ander onheil. Beveilig daarom uw webwinkel.

U kunt met een aantal criteria en maatregelen zorgen voor een beveiliging waaraan u minimaal moet voldoen om beschermd te zijn tegen belangrijke bedreigingen. U voldoet dan ook aan wet- en regelgeving in Nederland.

Gaat het ook om mijn webwinkel?
Elke webwinkel heeft beveiliging nodig. Natuurlijk is niet iedere webwinkel hetzelfde. Er zijn grote verschillen in omvang en in de gebruikte systemen bij webwinkels. Dit document is zo opgesteld dat u het kunt toepassen op webwinkels in alle soorten en maten. Er is namelijk uitgegaan van bedreigingen die voor vrijwel alle webwinkels gelden. Als u nog zekerder van uw zaak wilt zijn is het natuurlijk altijd beter om voor uw specifieke situatie een risicoanalyse te (laten) maken.

Hoe gebruik ik de criteria?
De volgorde van de criteria in dit document zegt niets over het belang er van. Om uw webwinkel goed te beveiligen moet u aan elk criterium aandacht besteden.

Aan de criteria zijn één of meerdere maatregelen gekoppeld. Deze vindt u ook in dit document.

In de bijlage vindt u adviezen en voorbeelden voor de implementatie van maatregelen.

De mate waarin u aan de in dit document genoemde criteria voldoet, bepaalt in hoeverre uw webwinkel bedreigingen het hoofd kan bieden, en of u voldoet aan de wettelijke eisen en eisen van financiële instellingen.

In dit document wordt soms de term "webwinkel" gebruikt. In de rest van dit document verstaan we onder de "webwinkel" de gehele informatievoorziening van het bedrijf. Dat wil zeggen: alle gebruikte automatisering- en communicatiemiddelen (hardware en software), alle gebruikte gegevensverzamelingen en alle procedures en documenten.

2. Bedreigingen voor de betrouwbaarheid van uw webwinkel

Wat bedreigt mijn webwinkel?
Elk soort onderneming kent zo zijn eigen soort risico's. Dat is voor webwinkels niet anders.
Bij webwinkels is het duidelijk, dat het succes valt en staat bij de betrouwbaarheid van de webwinkel.

Die wordt bedreigd op drie punten:

1. Beschikbaarheid,
    - de mate waarin uw webwinkel beschikbaar is.
2. Vertrouwelijkheid,
    - de mate waarin de toegankelijkheid tot uw webwinkel of de gegevens daarin beperkt is tot diegenen die daartoe bevoegd zijn.
3. Integriteit,
    - de mate waarin uw webwinkel op de juiste manier werkt en uw gegegevens de juiste zijn.

1. Beschikbaarheid
Bij beschikbaarheid gaat het erom dat uw webwinkel in de lucht blijft zodat u uw klanten kunt bedienen en u winst kunt maken. De beschikbaarheid van uw webwinkel kan bijvoorbeeld worden bedreigd door brand. Een schets hoe het kan lopen:

Als uw kantoor met daarin computers brandschade oploopt, kan uw webwinkel uitvallen. In dat geval heeft dat meteen invloed op de bedrijfsvoering. Klanten worden niet meer bediend en nieuwe orders komen niet binnen. Tegelijkertijd kunnen bestaande klanten het vertrouwen in uw winkel verliezen omdat u uit de lucht bent. Is uw webwinkel niet beschikbaar, dan lijdt u directe financiële schade en vervolgschade door bijvoorbeeld imagoverlies

Naast brand kan ook diefstal de beschikbaarheid bedreigen. Als iemand er van door gaat met uw computers dan is uw winkel niet meer beschikbaar. Het financiële verlies is vaak vele malen groter dan de waarde van uw apparatuur alleen. Uw apparatuur kan natuurlijk ook gewoon een technisch mankement vertonen, waardoor de webwinkel kan uitvallen. Harde schijven gaan een keertje stuk, internet verbindingen kunnen uitvallen.

Virus, spyware, spam, scripts, hackers als bedreigingen
U kunt ook last hebben van virussen, spyware, of besmetting met gevaarlijke scripts, die zonder uw medeweten, gebruikt worden door hackers en spammers en die uiteindelijk ook de beschikbaarheid van uw webwinkel aan kunnen tasten. Een heel andere ontwikkeling is dat criminele hackers uw site 'bezetten' of lam leggen en deze pas weer voor een grote som geld vrijgeven. Al deze bedreigingen (en anderen) van de beschikbaarheid zult u het hoofd moeten kunnen bieden

2. Vertrouwelijkheid
Bij vertrouwelijkheid gaat het erom dat onbevoegden geen toegang hebben tot uw webwinkel. Dat betekent dat niemand er met uw apparatuur van door kan gaan, maar bijvoorbeeld ook dat hackers geen toegang hebben tot de gegevens van uw klanten.

Bedenk eens welke risico's ontstaan bij het stelen van opslagmedia van een back-up locatie. Onbevoegden krijgen toegang tot de klant- en bedrijfsgegevens, en zo is de vertrouwelijkheid in het geding.

Imagoschade
Op het moment dat persoonsgegevens of ordergegevens van uw klanten op straat komen te liggen, heeft dit gevolgen voor uw imago. En mogelijk heeft het zelfs juridische gevolgen. Diverse Nederlandse webwinkels waarvan klant- en orderinformatie was uitgelekt, hebben dit moeten ervaren. Imagoschade kan leiden tot een groot financieel verlies. Herinnert u zich de grote media-aandacht voor het verliezen van usb-sticks ? Dit had altijd nare gevolgen voor degene die de usb-stick verloor en voor zijn organisatie.

3. Integriteit
Bij integriteit gaat het er om dat u en uw klanten er op kunnen vertrouwen dat uw webwinkel juist functioneert en dat u over de juiste gegevens beschikt. Zo moeten bijvoorbeeld de optellingen van uw winkelmandje wel kloppen, en moet u er van uit kunnen gaan dat bestellingen, betaalgegevens of afleveringsadressen van uw webwinkel niet gemanipuleerd worden. Het is soms kinderlijk eenvoudig om via een gedownload 'programmaatje' van het internet in te breken op uw webwinkel, de website te verminken, spam te versturen via uw computers of klant- en orderinformatie te stelen. Er zijn ook hackers die via uw webwinkel er voor kunnen zorgen dat de computer van de klant wordt gemanipuleerd. Uw klant wil er van uit kunnen gaan dat winkelen bij u geen geïnfecteerde computer oplevert.

De hierna volgende criteria zijn opgesteld om de bedreigingen ten aanzien van de beschikbaarheid, vertrouwelijkheid en integriteit van uw webwinkel het hoofd te kunnen bieden. Voldoet uw webwinkel, middels te nemen maatregelen (zoals in de bijlage), aan deze criteria, dan is uw webwinkel aanvaardbaar beveiligd.

3. De criteria[1]

De criteria voor een veilige webwinkel zijn:

1. **Toegangsbeheersing**
   Onbevoegden hebben geen toegang tot de informatie of functionaliteit van de webwinkel.

2. **Omgaan met incidenten en monitoring**
   Er zijn voorbereidingen getroffen om adequaat te reageren op beveiligingsincidenten en om de schade ten gevolge van een beveiligingsincident te beperken. Beveiligingsincidenten worden gedetecteerd.

3. **Continuïteit van de bedrijfsvoering**
   Onderbrekingen van de bedrijfsvoering worden voorkomen. De bedrijfsvoering is bestand tegen de impact van falende systemen of calamiteiten, en kan na een onderbreking snel worden voortgezet.

4. **Aankoop, ontwikkeling en onderhoud van systemen en diensten**
   Er zijn afspraken over de informatiebeveiliging bij aankoop, ontwikkeling en onderhoud van systemen en diensten voor de webwinkel.

5. **Huisregels informatiebeveiliging**
   Aan de informatiebeveiliging wordt eenduidig richting gegeven door het hanteren van huisregels voor het hele bedrijf.

6. **Fysieke beveiliging**
   Onbevoegden hebben geen fysieke toegang tot de plaats waar de apparatuur of informatie van de webwinkel huist.

7. **Management van kwetsbaarheden**
   Er zijn maatregelen getroffen die de bedreigingen minimaliseren die ontstaan door nieuw ontdekte kwetsbaarheden in software en hardware.

8. **Organisatie van de informatiebeveiliging**
   De informatiebeveiliging moet adequaat georganiseerd zijn. Dat wil zeggen dat er procedures zijn voor de dagelijkse beveiliging, het omgaan met incidenten, omgaan met gebruikersaccounts en controle op toegang tot gegevens en systemen

[1] De criteria zijn gebaseerd op de systematiek van de Code voor Informatiebeveiliging (NEN: ISO/IEC 17799:2005), een belangrijke standaard die veel wordt gebruikt door professionals op het gebied van de informatiebeveiliging. Daarnaast is er aansluiting gezocht bij de “Payment Card Industry Security Standard” (versie 1.1 september 2006), de standaard samengesteld door de gezamenlijke creditcard maatschappijen.

9. **Contacten met derde partijen**
   Bij het gebruik van producten of diensten van derde partijen (zoals service providers, soft- en hardware leveranciers etc.) moet de informatiebeveiliging onder controle zijn.

10. **Beheer van bedrijfsgoederen en -informatie**
    Er moet een up-to-date overzicht zijn van alle bedrijfsgoederen en bedrijfsinformatie, zodat duidelijk is waar wat aanwezig is en of het bedrijfskritische goederen of informatie betreft.

11. **Omgang met informatiedragers**
    De omgang met informatiedragers zoals CD-ROM's, USB-sticks, harde schijven e.d. is onder controle en de informatiedragers zijn fysiek beschermd bijvoorbeeld door ze in een kluis te bewaren.

12. **Informatie-uitwisseling**
    De uitwisseling van informatie met bijvoorbeeld klanten of leveranciers vindt veilig plaats.

13. **Overeenstemming met wetten en regelgeving**
    De bedrijfsvoering is in overeenstemming met de actueel geldende wet en regelgeving, contracten en beveiligingsvoorschriften.

4. De maatregelen

De maatregelen die genomen kunnen worden zijn:

1. Maatregel toegangsbeheersing
Toegang tot informatie, informatiesystemen en bedrijfsprocessen dient te worden beheerst op basis van bedrijfs- en beveiligingsvereisten.

2. Maatregel omgaan met incidenten en monitoring
Alle beveiligingsincidenten moeten zo snel mogelijk gedetecteerd en gerapporteerd worden op één centraal punt in de organisatie. Voor beveiligingsincidenten moeten “incident response procedures" ingericht zijn.

3. Maatregel continuïteit van de bedrijfsvoering
Richt een continuïteitsproces in. In dit proces beheert u de beveiligingsmaatregelen die er voor zorgen dat een onderbreking van uw bedrijfsvoering wordt voorkomen en dat u snel weer aan de gang kunt na een mogelijke onderbreking.

4. Maatregel aankoop, ontwikkeling en onderhoud van systemen en diensten
In een functioneel ontwerp voor nieuwe systemen of bij verbeteringen of onderhoud van systemen dienen de vereisten voor beveiligingsmaatregelen te zijn opgenomen.

5. Maatregel huisregels informatiebeveiliging
Er moet een document worden opgesteld met daarin de huisregels van het bedrijf ten aanzien van de informatiebeveiliging. Dit document moet worden gepubliceerd en worden gecommuniceerd met alle medewerkers en derde partijen die werkzaam zijn voor het bedrijf. Dit document moet worden onderhouden en nageleefd.

6. Maatregel fysieke beveiliging
Maak gebruik van middelen voor fysieke toegangsbeveiliging voor de locatie waar uw apparatuur staat opgesteld en de bewaarplaats van documenten of informatiedragers (b.v. back-ups).

7. Maatregel management van kwetsbaarheden
Zorg voor tijdige informatie over kwetsbaarheden in software en hardware, en bepaal of deze kwetsbaarheden op de webwinkel van toepassing zijn. Indien van toepassing neem dan de bij de kwetsbaarheid behorende beveiligingsmaatregelen.

8. Maatregel organisatie van de informatiebeveiliging
De informatiebeveiliging moet ook op een minimum niveau georganiseerd zijn. Er moeten op zijn minst procedures zijn voor de dagelijkse beveiliging, voor het omgaan met incidenten, voor het omgaan met gebruikersaccounts. Maar ook voor de controle op de toegang tot gegevens en systemen.

9. Maatregel contacten met derde partijen
Beperk de toegang voor derde partijen tot gegevens en functionaliteit zoveel mogelijk tot het noodzakelijke. Stel contractuele eisen aan beveiliging. Controleer of de afspraken worden nagekomen.

10. Maatregel beheer van bedrijfsgoederen en informatie
Alle bedrijfsgoederen en informatie dienen te worden geïdentificeerd en te worden geïnventariseerd. Deze informatie dient up-to-date te worden gehouden.

11. Maatregel omgang met informatiedragers
Voer procedures in om documenten, computer media, input/output en systeemdocumentatie te beveiligen tegen ongeautoriseerde of onbedoelde openbaarmaking, wijziging, verwijdering en vernietiging.

12. Maatregel informatie-uitwisseling
Procedures en standaarden dienen te worden ingevoerd zodat bij informatie-uitwisseling gegevens en fysieke media zijn beschermd.

13. Maatregel overeenstemming met wetten en regelgeving
Alle voor uw bedrijf geldende wetten en regelgeving, contractuele verplichtingen en de manier waarop u hier aan voldoet moeten gedocumenteerd zijn voor elk systeem in uw bedrijfsvoering. Deze documentatie moet up-to-date worden gehouden.

Bijlage 1: Adviezen voor implementatie van maatregelen

1. Toegangsbeheersing

Het volgende is een stappenplan voor eenvoudig toegangsbeheer:

Stap 1
Identificeer welke gegevens of functies van uw informatiesysteem voor u van groot belang zijn. Denk aan klant- en ordergegevens, financiële administratie, inkoopafspraken, personeelsbeoordelingen, ziekterapportages, maar ook bankier-, inkoop- en betalingssystemen. Overweeg of deze gegevens of functionaliteit kan worden overgeheveld naar niet extern toegankelijke back-officesystemen.

Stap 2
Onderzoek of uw systemen de functionaliteit bieden om toegang per functionaliteit op verschillende niveaus kunnen instellen, wijzigen en intrekken. Overweeg om zonodig andere systemen te gebruiken, indien de huidige systemen niet voldoende functionaliteit bieden. Sla informatie niet onnodig op en alleen daar waar een gepaste vorm van toegangsbeheer mogelijk is.

Stap 3
Inventariseer voor alle gegevens, functies of deelsystemen uit stap 1 de verschillende rollen die te onderscheiden zijn in het werken daarmee. Voorbeelden van rollen zijn: aankopen doen, inkopen doen, productcatalogus bijwerken, facturen boeken, uitbetalen, personeel administreren, voorraad beheren. Bepaal per rol dan welk toegangsrecht er moet zijn (bijvoorbeeld: lezen, schrijven, onderhoud). Maak dit overzicht niet onnodig gedetailleerd. als een bepaalde rol in het systeem meer rechten heeft dan strikt noodzakelijk is dit niet altijd een groot risico.

Stap 4
Koppel nu de rollen aan specifieke gebruikers of gebruikersgroepen. Nu heeft u een ‘autorisatieschema’. Bijvoorbeeld: een ‘geregistreerde klant’ mag ‘aankopen doen’ betekent dat hij bepaalde lees en schrijf toegangen heeft. Of: een ‘financieel medewerker’ mag ‘uitbetalen doen’ wat betekent dat deze medewerker toegang heeft tot internet bankieren. Wees spaarzaam met uitzonderingen, want die worden vaak vergeten en maken het geheel complex.

Stap 5
Geef nu de verschillende gebruikers vervolgens persoonlijke accounts met wachtwoorden.
Houd deze accounts ook echt persoonlijk en zorg ervoor dat deze voldoende worden beschermd. Denk aan het vernieuwen van wachtwoorden, geen wachtwoorden op briefjes onder het toetsenbord schrijven, enz. Zorg dat anonieme toegang beperkt is tot een minimum (bijvoorbeeld: alleen rondkijken vanaf het internet). Alle andere toegang moet gebaseerd zijn op unieke gebruikersnamen en herleidbaar zijn tot een natuurlijke persoon of gedefinieerde klant.

Stap 6
Hanteer een procedure die de verleende toegangsrechten actueel houdt. Krijgt een medewerker nieuwe taken toebedeeld of een andere functie? Trek dan de oude rechten in en verleen de op de nieuwe functie toepasselijke rechten. Treedt een medewerker uit dienst? Sluit dan het betreffende account en de bijbehorende rechten af. Controleer dit regelmatig. Hanteer deze procedure ook voor tijdelijke krachten.

2. Omgaan met incidenten en monitoring

Bepaal voor alle mogelijke beveiligingsincidenten:

- Of die van toepassing zijn op uw webwinkel
- Of het gevolg voor u acceptabel is
- Of uw huidige beveiligingsmaatregelen voldoende zijn

Betrek daarbij alle personen en partijen die een rol spelen in levering, ontwikkeling of onderhoud van uw webwinkel. Neem daar waar u het gevolg onacceptabel vindt zonodig extra beveiligingsmaatregelen. Stel voor deze incidenten een zogenaamde ‘incident response’ procedure op. Hierin staat voor dit specifiek soort incident welke handeling wanneer verricht moeten worden en door wie.

Incident response procedure
Hoewel het detecteren van incidenten onnodig lijkt, is het cruciaal voor de effectiviteit van de incident response procedure. Hoe lang duurt het voordat u door heeft dat uw website is verminkt? Dat uw computers misbruikt worden om spam of virussen te versturen naar uw klanten? Dat uw systemen storing ondervinden en er geen orders meer gedaan kunnen worden? Dat medewerkers fraude plegen? Bedenk daar waar nodig detectie mechanismen, in de vorm van techniek en/of procedures.

Herhaal de bovenstaande methode periodiek, en toets of de beveiligingsmaatregelen en incident response procedures nog steeds effectief zijn voor de actuele situatie. Oefen de incident response procedures met regelmaat, zodat u niet voor ongewenste verrassingen komt te staan.

De eerste incident response procedure die u gaat opstellen en met regelmaat gaat testen is natuurlijk het volledige herstel van uw webwinkel met back-ups.

3. Continuïteit van de bedrijfsvoering

Identificeer de kritische bedrijfsprocessen en geef de prioriteit daarvan aan. Bepaal de kans op en de impact van uitval van deze bedrijfsprocessen (of laat deze bepalen). Neem maatregelen voor de kritische bedrijfsprocessen waarvoor u de kans op en de impact van uitval te groot vindt.

continuïteitsplan
U stelt voor deze bedrijfsprocessen een continuïteitsplan op. Hierin staat voor dit specifieke bedrijfsproces welke handelingen wanneer en door wie verricht moeten worden om het proces weer zo snel mogelijk in de lucht te krijgen.

Onderdeel van deze plannen is de identificatie van de bedrijfsmiddelen die bij dit proces betrokken zijn.
Andere onderdelen van continuïteitsplannen zijn bijvoorbeeld procedures voor het terugzetten van back-ups. Daarnaast moet cruciale informatie dubbel opgeslagen zijn, communicatieapparatuur dubbel uitgevoerd zijn en moeten er uitwijkmogelijkheden zijn als de kantoorruimte (tijdelijk) niet beschikbaar is bijvoorbeeld bij brand. Reserveer ook geld, mensen en tijd voor deze plannen en zorg dat die in tijden van nood beschikbaar zijn. Zorg dat je weet wie je moet bellen als er een calamiteit is.

Zorg ook dat essentiële systeemcomponenten up-to-date zijn, en sluit een onderhoudscontract met korte responsetijden. Houd hierbij rekening met servicewindows: bij een storing op vrijdagochtend garandeert een “next business day contract” response vóór maandagavond!

Zorg voor (afspraken over) vervangende apparatuur en voor een procedure om deze aan te sluiten, te configureren en van de benodigde applicaties en gegevens te voorzien. Herzie deze procedures bij iedere wijziging in apparatuur of software. Test de procedure ook regelmatig in de praktijk (halfjaarlijks is een goed idee).

Bij webhosting maakt u afspraken met de hosting partij over storingsoplossingstijden, en ontvangt u op gezette tijden informatie omtrent opgetreden storingen en hersteltijden.

Om grote toestroom van verkeer op te vangen maakt u afspraken met de ISP (Internet Service Provider) over levertijden van grotere bandbreedte. Als noodmaatregel kunt u een reserve website met beperkte functionaliteit en snelle schermopbouw achter de hand hebben.

Weeg de kosten van deze beveiligingsmaatregelen af tegen de kosten van verzekering. Sommige risico’s kunnen beter afgedekt zijn door verzekering dan door beveiligingsmaatregelen.
Draag niet alleen zorg voor beveiliging maar ook voor veiligheid van mensen, systemen en goederen.

Herzie de continuïteitsplannen periodiek, en toets of de beveiligingsmaatregelen en de procedures nog steeds effectief zijn voor de actuele situatie. Test en oefen eens een continuïteitsplan, zodat u niet voor ongewenste verrassingen komt te staan.

Zorg dat het beheer van de continuïteit onderdeel uitmaakt van uw normale bedrijfsvoering en maak het onderdeel van uw beveiligingsbeleid.

4. Acquisitie, ontwikkeling en onderhoud van systemen en diensten

Fouten die gemaakt worden tijdens het bouwen van een webwinkel, kunnen later kwetsbaarheden vormen in het totale systeem. Denk aan inrichtings- en configuratiefouten of fouten in de programmacode van de webwinkel. Let bij het uitzoeken van hard- en software niet alleen op functionaliteit, maar ook op de beveiligingsmogelijkheden. Bedenk van te voren welke beveiligingsfunctionaliteit u nodig heeft, bijvoorbeeld:

- encryptie (informatie uitwisseling)
- toegangsrechten (toegangsbeheer)
- wachtwoord beleid (toegangsbeheer)
- log en alarm mogelijkheden (incident monitoring)
- back-up en herstel mogelijkheden (noodherstel)
- testomgevingen (onderhoud en beheer)

Fouten die gemaakt worden tijdens onderhoud en beheer zijn vaak de oorzaak van storingen. Daarnaast kunnen er met wijzigingen in systemen, nieuwe kwetsbaarheden geïntroduceerd worden. Deze wijzigingen moeten dus zorgvuldig worden voorbereid. Probeer wijzigingen niet uit op uw online webwinkel maar gebruik daarvoor een testomgeving. Maak back-ups voordat u de uiteindelijke wijzigingen uitvoert en zorg dat u altijd snel kan terugschakelen naar de oude situatie. Beoordeel de beveiliging van de nieuwe situatie. Vraag u ook af of:

- Updates goed worden getest en of de update procedure helder is? Ook als er voor uw bedrijf maatwerk is toegepast?
- Er in de licentievoorwaarden ruimte is voor het inrichten van een testomgeving? Of zijn hier nieuwe licenties voor nodig?
- Er in geval van calamiteiten ondersteuning mogelijk is?

Heeft u deze zaken uitbesteed? Maak dan afspraken over de uitvoering van deze taken en de rapportage hierover. Neem deze afspraken op in de overeenkomst (SLA). Heeft u een huurwinkel bij een serviceprovider? Informeer u dan goed op welke manieren de serviceprovider is beveiligd. En, of u compensatie krijgt bij schade door slechte beveiliging.

Het is van belang op de hoogte te blijven van belangrijke informatie over de software of webwinkeloplossing die u gebruikt, bijvoorbeeld via forums, mailing lists en security reports. Als er belangrijke updates uitkomen die te maken hebben met veiligheid, installeer deze dan ook! Daarnaast kunt u regelmatig sites bezoeken die bijhouden welke software niet goed is beveiligd. Er worden voortdurend nieuwe ‘lekken’ ontdekt in sofware en op diverse sites worden deze gerapporteerd, bijvoorbeeld op:

• http://osvdb.org
• http://secunia.com
• http://securitytracker.com
• http://www.securityfocus.com

5. *Beveiligingsbeleid en personeel*

De huisregels of de gedragscode beschrijven de verantwoordelijkheden van informatiebeveiliging voor alle werknemers en derde partijen. Deze zetten de toon voor het hele bedrijf en geven aan de medewerkers duidelijkheid over wat er van hen wordt verwacht.

Stel medewerkers bij hun indiensttreding al op de hoogte van uw beleid (laat hiervoor een verklaring tekenen of regel dit in het arbeidscontract).

Breng minimaal jaarlijks het beveiligingsbeleid onder de aandacht van het personeel (bijvoorbeeld door nieuwsbrieven, posters, memos, bijeenkomsten etc.).

Toets met enige regelmaat of aan deze huisregels of gedragscode wordt voldaan. Stel de huisregels of code bij waar nodig. Gebruik de huisregels ook in de communicatie met medewerkers, klanten en derde partijen.
Zorg dat de procedures voor de dagelijkse werkzaamheden in overeenstemming zijn met de huisregels of gedragscode.

De huisregels of gedragcode moeten minimaal de volgende eisen bevatten:

- Handel altijd volgens de beveiligingsprocedures die van toepassing zijn.
- Bescherm bedrijfsgoederen, bedrijfsgegevens en systeemfunctionaliteit tegen verboden of onbedoelde toegang door onbevoegden, openbaarmaking, wijziging, vernietiging of verstoring.
- Voer specifieke beveiligingsprocedures en activiteiten uit.
- Werknemers zijn persoonlijk verantwoordelijk voor de acties die zij uitvoeren of nalaten.
- Rapporteer beveiligingsincidenten of potentiële incidenten of andere beveiligingsrisico's aan de organisatie.

6. *Fysieke beveiliging*

Beveilig tegen inbraak en diefstal, maak gebruik van beveiligingsapparatuur, en beheer zorgvuldig uw sleutels. Gebruik identificatiebadges voor werknemers en bezoekers. Leg het bezoek van niet-werknemers schriftelijk vast in een log.
Hanteer een procedure die regelt dat mensen die niet langer voor u werken geen toegang meer hebben. Hanteer deze procedure ook voor tijdelijke krachten. Controleer dit regelmatig.

Veel back-upapplicaties bieden de mogelijkheid de duplicaatgegevens te versleutelen. Gebruik deze faciliteit altijd, op het hoogst mogelijke beveiligingsniveau indien keuzes bestaan. De extra verwerkingstijd weegt zeker op tegen de problemen die een al dan niet eerlijke vinder ondervindt als hij/zij uw gegevens wil achterhalen.

7. Management van kwetsbaarheden

Bouw en onderhoud een veilige netwerkomgeving:

- Zorg voor de bescherming tegen kwaadaardige software (virussen, trojans, etc). door middel van een goede virusscanner, speciaal op personal-computers en servers.
- Zorg voor een afscherming tussen internet en alle systemen van de webwinkel door middel van een firewall.
- Wijzig alle door fabrikanten en leveranciers aangebrachte standaard wachtwoorden en parameters.

Inventariseer alle hard- en software onderdelen van uw webwinkel, met de bijbehorende fabrikanten of leveranciers. Vooral onderdelen die in verbinding staan met internet of gegevens verwerken afkomstig van het internet moet u zorgvuldig inventariseren. Een aantal voorbeelden:

- internet modem/router/firewall
- wireless access point
- web-servers (Apache, Microsoft IIS)
- email-servers
- databases
- programmeer omgevingen (PHP, .NET, Java)
- besturingssytemen (Microsoft Windows, Linux)
- office software (Microsoft Office, Adobe PDF)
- email software (Microsoft Outlook, Mozilla Thunderbird)
- virusscanner, firewall, spy-ware blocker, phishing filter, spam-filter

Installeer alle beveiligingsupdates van de fabrikanten. Blijf op de hoogte van beveiligingskwetsbaarheden. Controleer zelf of er nieuwe beveiligingsupdates zijn, of gebruik - als dat kan - de automatische update functie. Bekijk goed welke software wel en niet door de automatische update functie wordt bijgehouden. Deze sites geven uitgebreide informatie over beveiligingskwetsbaarheden:

- www.waarschuwingsdienst.nl
- www.securityfocus.com/vulnerabilities

Er zit ook een nadeel aan updates. Het komt vaak voor dat onderdelen van de software niet meer goed functioneren of samenwerken na het toepassen van een update. Test de updates van kritische onderdelen daarom altijd eerst in een testomgeving. Op kritische systemen is het verstandig de automatische update-functie handmatig te bedienen. Pas nadat de testen succesvol zijn afgerond, installeert u de beveiligingsupdates.

Beveiligingsupdates

Beveiligingsupdates zijn niet het antwoord op alle beveiligingsproblemen. Ten eerste is er altijd een periode tussen het bekend worden van een kwetsbaarheid en de beschikbaarheid van een beveiligingsupdate. De fabrikant heeft namelijk tijd nodig om een oplossing te vinden en een update uit te brengen, wat weken tot zelfs maanden kan duren. In deze periode bent u zeer kwetsbaar. Ten tweede zijn er tal van andere

manieren waarop uw systeem kwetsbaar kan zijn, bijvoorbeeld door configuratie- of inrichtingsfouten. Daarom wordt geadviseerd uw webwinkel goed te beveiligen door bijvoorbeeld virusscanners, firewall en goede monitoring toe te passen. Er zijn ook bedrijven die op afstand uw webwinkel scannen op kwetsbaarheden. Afhankelijk van uw, betaalde, abonnement gebeurt dit incidenteel, regelmatig of continue. Deze bedrijven geven ook uitleg hoe eventuele gevonden lekken kunnen worden gerepareerd. Bekende bedrijven met deze service zijn:

- www.acunetix.com
- www.hackersafe.com
- www.secunia.com

8. Organisatie van de informatiebeveiliging

Om de organisatie van de informatiebeveiliging op een minimum niveau te regelen moeten deze taken belegd zijn:

- Ontwikkelen, documenteren en distribueren van beveiligingsprocedures.
- Monitoren en analyseren van beveiligingalarm. Doorzetten van het alarm naar de daarvoor verantwoordelijke mensen.
- Ontwikkelen, documenteren en distribueren van beveiligingsincident respons procedures en continuïteitsplannen.
- Het beheren van gebruikersaccounts (toevoegingen, verwijderingen en wijzigingen)
- Het monitoren en beheersen van alle toegang tot data- en systeemfunctionaliteit.

9. Contacten met derde partijen

Derde partijen moeten slechts toegang krijgen tot die gegegevens, functionaliteit en fysieke ruimten die strikt noodzakelijk zijn voor de werkzaamheden die zij uit moeten voeren. Voor deze werkzaamheden moet zij een contract tekenen dat ingaat op de beveiligingsvereisten van de werkzaamheden. Denk daarbij ook aan een geheimhoudingsclausule als er inzage in bedrijfsgevoelige of privacygevoelige gegevens is vereist.

10. Beheer van bedrijfsgoederen en informatie

Een inventarisatie van bedrijfsgoederen en informatie vormt de basis voor het beheer van de informatiebeveiliging. Vaak is zo'n inventarisatie ook nodig voor de verzekering of de boekhouding. De inventarisatie is ook een van de basisvoorwaarden voor het inrichten van de fysieke beveiliging en de toegangsbeheersing. Men moet immers weten waar welke goederen of informatie aanwezig zijn. Ook vormt zo'n inventarisatie de basis voor het beheer van de bedrijfscontinuïteit. Daarbij moet het immers duidelijk worden welke goederen en informatie bijdragen aan de kritische bedrijfsprocessen. Vaak vermeldt men bij de inventarisatie ook de verantwoordelijke of de eigenaar van de goederen of informatie.

11. Omgang met informatiedragers

Zorg voor fysiek juiste omstandigheden bij gebruik, opslag en transport van gegevensdragers. Denk daar bij aan juiste omgevingsomstandigheden:

- een cd'tje in de auto op een zomerse dag kan onleesbaar worden
- op een spindel opgeslagen beschreven cd-rom's kunnen door onderlinge draaiing krassen krijgen en onleesbaar worden.
- magnetische gegevensdragers kunnen gegevens verliezen als ze in de buurt van sterke magneten komen (geluidsboxen zijn berucht).

Gegevens verliezen is één ding, gegevens in handen van anderen is een ander probleem. Voorkom dit door overal waar mogelijk encryptie toe te passen.

12. Informatie-uitwisseling

- Zorg voor 'Secure Socket Layer' (SSL) encryptie van de bedrijfskritische, vertrouwelijke of klantgegevens gegevens tijdens datacommunicatie en transport. Dit doet u door een SSL certificaat aan te vragen en te installeren voor uw webwinkel of dit door uw hosting provider te laten uitvoeren. SSL verbindingen worden door de browser van uw klanten herkend en weergegeven als https in plaats van http-pagina's. Klantgegevens kunnen op die manier versleuteld worden verzonden aan uw database.
- Zorg bij fysiek transport van gegevens voor een herkenbaar transportpad (aangetekend verzenden met ontvangstbevestiging, tracking en tracing bij pakketverzending).
- Zorg dat u altijd een exacte kopie hebt van de verzonden informatie, ook in de vorm van logging bij real-time transactieuitwisseling.
- Bij fysieke gegevensdragers bestaat het risico dat een onbevoegde tijdens de transportfase een kopie van de gegevens voor eigen gebruik maakt. Zorg daarom dat dergelijke gegevens altijd versleuteld zijn.

13. Overeenstemming met wetten en regelgeving

Denk al bij de aankoop en de ontwikkeling van uw systemen aan de geldende wet- en regelgeving. Onderzoek periodiek of u nog voldoet aan alle geldende regelgeving ten aanzien van de informatiebeveiliging en privacy. Of laat dit onderzoeken. Veel van de beveiligingsmaatregelen die in dit document staan, zijn ook vereist uit oogpunt van de bescherming van de privacy van uw klanten en werknemers. Zorg dat u voldoet aan de vereisten van de *Wet Bescherming Persoonsgegevens.* Voor het aanmelden van persoonsregistraties bestaan genormeerde vrijstellingen. Zie verder de website: www.collegebeschermingpersoonsgegevens.nl

Publiceer een privacystatement op uw website en maak dat onderdeel van uw algemene leveringsvoorwaarden. Zorg dat de zorgvuldige omgang met privacygevoelige informatie deel uit maakt van uw beveiligingsbeleid (uw huisregels of gedragscode).

De omgang met creditcardgegevens stelt bijzondere eisen aan uw systemen, zorg dat u voldoet aan de vereisten van uw payment service providers.

Administreer uw software licenties en verleng ze tijdig. Denkt u ook aan regelgeving van de belastingdienst? (www.belastingdienst.nl)

Bijlage 2: Verklarende woordenlijst

spam - e-mail die op grote schaal ongevraagd wordt toegestuurd.

(computer)virussen - een vorm van schadelijke software (malware). Het is een computerprogramma dat zich in een bestand kan nestelen,vermenigvuldigen naar andere computers en schade kan aanrichten aan de geïnfecteerde computers.

spyware - computerprogramma's (of delen daarvan) die informatie vergaren over een computergebruiker en deze doorsturen naar een externe partij. Vaak zonder de computergebruiker daarover in te lichten.

firewall - heeft het doel te voorkomen dat ongewenst netwerkverkeer van het ene netwerk terecht komt in een ander netwerk, met als doel de veiligheid van het laatstgenoemde netwerk te verhogen. Denk aan bijvoorbeeld een firewall die netwerkverkeer blokkeert vanaf het internet naar een bedrijfsnetwerk.

modem - een apparaat waarmee digitale informatie over telefoonlijnen of andere kabelverbindingen kunnen worden verstuurd. Bijvoorbeeld een ADSL modem, dat digitale informatie over een telefoonlijn kan versturen naar de internetprovider.

router - een apparaat dat twee of meer verschillende computernetwerken aan elkaar verbindt, bijvoorbeeld internet en een bedrijfsnetwerk. Wordt vaak gecombineerd in één apparaat met een modem en firewall.

wireless accesspoint - een apparaat dat draadloze apparaten (laptop, palmtop, telefoon) verbindt aan een vast netwerk, bijvoorbeeld een bedrijfsnetwerk. Wordt vaak gecombineerd in één apparaat met een router, modem en firewall.

webserver - een computer die websites aanbiedt aan bezoekers over een netwerk, zoals het internet. Bezoekers gebruiken een browser om de webpagina weer te geven.

emailservers - een computer die e-mails ontvangt, in de postbussen van de lokale geadresseerden stopt en de email voor externe geadresseerden doorstuurt naar de emailserver van de externe partij.

database - de plaats waar gegevens staan opgeslagen, in een structuur van tabellen en rijen. Bijvoorbeeld de financiële gegevens van een boekhoudprogramma zijn opgeslagen in een database.

programmeeromgevingen - een computer of een verzameling computerprogramma's, waarmee computerprogramma's kunnen worden gebouwd.

besturingssystemen - het basis computerprogramma, dat het mogelijk maakt de fysieke computer en alle aangesloten apparaten (printer, muis, toetsenbord) te gebruiken. Binnen een besturingssysteem kunnen andere computerprogramma's gestart worden, zoals een emailprogramma, tekstverwerker of internetbrowser.

configuratie - de instelbare parameters die het gedrag van een computerprogramma beïnvloeden. Hierdoor kan een algemeen computerprogramma worden afgesteld op de specifieke wensen van de gebruiker.

monitoring - het al dan niet automatisch in de gaten houden van de activiteiten van gebruikers en/of computerprogramma's, met het doel ongewenste gebeurtenissen snel op te merken. Bijvoorbeeld een storing in een computer of computerprogramma.

systeemfunctionaliteit - de taken die een bepaald computerprogramma kan vervullen. Zo is het uit kunnen printen van facturen of betalingen kunnen doen een functionaliteit geboden door computerprogramma's in een bedrijf.

'Secure Socket Layer' (SSL) encryptie - een mechanisme om netwerkverkeer tussen bezoeker en webserver te beschermen tegen afluisteren, waarbij de echtheid van de webserver kan worden gecontroleerd. Bijvoorbeeld tijdens het internet bankieren, moet het
netwerkverkeer beschermd worden tegen afluisteren en wil de bezoeker er zeker van zijn dat zij daadwerkelijk met de webserver van de bank verbonden is.

Track en trace dienst - Dienst van koeriersbedrijven, waarmee de zending via een webpagina op het internet kan worden gelokaliseerd en gevolgd.

Tracking - online track en trace dienst bij pakketverzending

Logging bij real-time transactieuitwisseling - het vastleggen van informatie over transacties tijdens het plaatsvinden van de transactie. Bijvoorbeeld een webserver die de tijd, zender en ontvanger vastlegt tijdens het plaatsen van een bestelling door een bezoeker.

Bijlage 3: Handige links

Consumentenautoriteit
http://www.consumentenautoriteit.nl

Belastingdienst
http://www.belastingdienst.nl

OSVDB
http://www.osvdb.org

Secunia
http://www.secunia.com

Security tracker
http://www.securitytracker.com

Security focus
http://www.securityfocus.com

Digibewust
http://www.digibewust.nl

Thuiswinkel.org
http://www.thuiswinkel.org

Hoofdbedrijfschap Detailhandel
http://www.hbd.nl

ECP.NL
http://www.ecp.nl