CBFA

COMMISSIE VOOR HET BANK-, FINANCIE- EN ASSURANTIEWEZEN

Bijlage Circulaire CBFA_2009_17-1 dd. 7 april 2009

Gezonde praktijken inzake het beheer van Internetbeveiligingsrisico's

Toepassingsveld **:**

Kredietinstellingen, verzekeringsondernemingen, beleggingsondernemingen en beheervennootschappen van instellingen voor collectieve belegging naar Belgisch recht en de Belgische bijkantoren van deze instellingen die ressorteren onder het recht van een staat die geen lid is van de Europees Economische Ruimte (EER). De circulaire wordt tevens ter kennis gebracht aan de in België gevestigde instellingen die ressorteren onder een lidstaat van de EER.

1. Inleiding

Financiële instellingen die het Internet gebruiken voor hun dienstverlening worden geconfronteerd met diverse beveiligingsrisico's.

De gezonde praktijken onderscheiden daarom aandachtspunten en aanbevelingen die verband houden met de beveiliging van :

- de eigen informatica-infrastructuur (hardware, besturingssystemen, applicaties, databases, firewalls, mail- en webservers, …) tegen bedreigingen van het Internet ;
- financiële verrichtingen, raadplegingen en beheersdaden over het Internet.

De financiële instellingen worden geacht de gezonde praktijken na te leven of afwijkingen ervan aan de CBFA toe te lichten (*comply or explain*).

2. Beveiliging van de eigen informatica-infrastructuur

2.1. Verantwoording

Elke financiële instelling die zijn informatica-infrastructuur aansluit op het Internet moet gepaste beschermingsmaatregelen treffen om de veiligheid en continuïteit van haar informaticasystemen en de integriteit en confidentialiteit van haar financiële en cliëntengegevens te vrijwaren, tegen alle voorzienbare misbruiken en risico's afkomstig van het Internet.

2.2. Prudentiële vereisten

2.2.1. Beveiligingsbeleid

Elke instelling die zijn informatica-infrastructuur aansluit op het Internet, beschikt over een gepast beveiligingsbeleid waarin aandacht wordt besteed aan :

- het belang van een aangepaste beveiliging van de eigen informatica-infrastructuur en de doelstellingen ter zake ;

Congresstraat 12-14 | 1000 Brussel
t +32 2 220 53 42| f +32 2 220 54 93 | www.cbfa.be

- de interne organisatie en verantwoordelijkheden betreffende :
    - o de opvolging van de Internetbedreigingen en hun toetsing aan de beveiligingsmaatregelen voor de eigen informatica-infrastructuur ;
    - o de beveiliging van de interne informatica-infrastructuur ;
    - o de behandeling van Internetbeveilingsincidenten ;
- de beveiligingsrichtlijnen voor de medewerkers inzake het veilige gebruik van het Internet ;
- het beveiligingskader voor het uitwisselen van e-mails, andere bestanden en boodschappen (bv. *instant messaging*) met de buitenwereld ;
- het beleid en de beveiliging inzake het verlenen van toegang tot de eigen informatica-infrastructuur via het Internet (*remote access*) ;
- de toegepaste criteria en de verantwoordelijkheden voor het periodiek (laten) uitvoeren van gespecialiseerde veiligheidsonderzoeken ;
- de creatie en opslag van gepaste technische logs en hun analyse, opvolging en rapportering.

2.2.2. Analyse en opvolging van de bedreigingen en de eigen beveiligingssituatie

De instelling zorgt voor :

- een goede analyse en opvolging van de Internetbedreigingen voor haar informatica-infrastructuur, rekening houdend met de door de instelling gehanteerde beveiligingsoplossingen en haar gebruik van het Internet;
- een nauwgezette opvolging van de gepubliceerde beveiligingslacunes in de door haar gebruikte Internetinfrastructuur en –beveiligingsoplossingen (software, hardware, ontwikkelingstalen, cryptografie, …). Waar nodig installeert de instelling zo spoedig mogelijk de door de leverancier ter beschikking gestelde correctieve oplossingen (software *patches*, *upgrades*, …) of gebruikt ze andere oplossingen om de beveiligingsrisico's af te dekken.

Op basis van de uitgevoerde analyses en rekening houdend met de aard en schaal van de waargenomen Internetbedreigingen, voert de instelling periodiek een formele risico-evaluatie uit, om na te gaan of en in hoeverre de bestaande beveiligingsmaatregelen, de gebruikte technologieën, de procedures of de aangeboden diensten dienen te worden aangepast.

De conclusies van de uitgevoerde opvolgingen en risicoanalyses worden in functie van hun dringendheid en belang en minstens eenmaal per jaar ter goedkeuring voorgelegd aan de effectieve leiding.

2.2.3. Beveiliging tegen ongeautoriseerde toegangen tot en wijzigingen aan de eigen informatica-infrastructuur

De instelling treft de nodige beveiligingsmaatregelen om ongeautoriseerde toegangen tot en misbruiken van haar informatica-infrastructuur via het Internet te voorkomen.

De instelling maakt hiervoor gebruik van gecontroleerde doorgeefluiken tussen het Internet en de eigen informatica-infrastructuur zoals *firewalls*, *proxy servers*, *mail relays*, antivirusscanners en *content* scanners of andere gelijkwaardige beveiligingsoplossingen. De instelling zorgt ervoor dat deze doorgeefluiken correct ontworpen, geconfigureerd en beveiligd worden en het voorwerp uitmaken van een professioneel dagelijks beheer en een nauwgezette opvolging.

Hierbij is het van groot belang dat alle rechtstreekse en onrechtstreekse[1] verbindingen met het Internet langs de voormelde doorgeefluiken passeren. Om het sluitende karakter van de aldus opgebouwde perimeterbescherming te verzekeren, besteedt de instelling ook bijzondere aandacht aan het voorkomen van ongecontroleerde en onvoldoende beveiligde netwerkverbindingen met de buitenwereld (draadloze netwerken, modems, enz.).

Omdat de voormelde gecontroleerde doorgeefluiken (meestal) niet alle doorgaande informatiestromen op een efficiënte en/of sluitende wijze kunnen nakijken en indien nodig tegenhouden, besteedt de instelling

[1] In sommige gevallen beschikken bv. bijkantoren, agentschappen of dochterondernemingen die aangesloten zijn op de eigen informatica-infrastructuur over Internetverbindingen.

bovendien de nodige aandacht aan de adequate beveiliging van de interne applicaties en databases die gegevens of instructies ontvangen via het Internet (*defense in depth*-principe)[2].

2.2.4. Beveiliging van publieke websites

Publieke websites vertonen een verhoogd "beveiligingsrisico" omwille van hun groot aantal bezoekers en hun gemakkelijke bereikbaarheid vanop het Internet. De instelling besteedt daarom bijzondere aandacht aan de beveiliging van zijn publieke websites om te voorkomen dat deze het slachtoffer worden van ongeautoriseerde wijzigingen of gebruikt worden om kwaadaardige softwares te verspreiden.

Om de kwetsbaarheid van de websites en de bijbehorende servers te beperken, maakt de instelling gebruik van :

- *firewalls*, *proxy servers* of andere gelijkwaardige beveiligingsoplossingen, om de websites en de bijbehorende servers zoveel mogelijk te beschermen tegen aanvallen en misbruiken via het Internet ;
- beveiligingstechnieken waarbij de servers worden "ontdaan" van alle overbodige gevaarlijke functies (*stripping* genoemd) en risicovolle applicaties zoveel mogelijk worden beveiligd (*hardening* genoemd). Om de beveiliging nog verder te verhogen worden ook de toegangen van de applicaties tot de door hun benodigde gegevens en middelen tot het strikte minimum beperkt (*least privilege*-principe).

Om misbruiken te bemoeilijken met nepwebsites die gelijken op legitieme websites van financiële instellingen, worden transactionele en bij voorkeur ook informatieve websites, geïdentificeerd via kwaliteitsvolle[3] digitale certificaten op naam van de financiële instelling of andere gelijkwaardige authentificatiemechanismen.

2.2.5. Geautoriseerde toegangen tot de eigen informatica-infrastructuur via het Internet (*remote access*)

De instelling beschikt over een beleid inzake de toegestane toegangen tot de eigen informatica-infrastructuur via het Internet, met bijzondere aandacht voor de regels inzake hun toekenning, goedkeuring, opvolging, herroeping en beveiliging.

Deze toegangen maken gebruik van hoogstaande beveiligingsoplossingen die :

- steunen op sterke authentificatieoplossingen die toelaten met een zeer hoge graad van zekerheid de identiteit van de personen die zich aanmelden na te gaan. Een beschrijving van deze sterke authentificatieoplossingen bevindt zich onder punt 3.2.3.a. ;
- nagaan of de handelingen van aangemelde personen geautoriseerd zijn ;
- de externe toegangen tot de informatica-infrastructuur tot het strikt noodzakelijke minimum beperken (*least privilege* principe) ;
- adequate beveiligingsmaatregelen voorzien om ongeautoriseerde toegangen tot of wijzigingen aan de eigen informatica-infrastructuur te vermijden, ten gevolge van beveiligingslacunes (virussen, kwaadaardige softwares, *back doors*, …) op de computer(infrastructuur) van de aangemelde personen. Voor de toegangen tot kritieke en sensitieve componenten van de informatica-infrastructuur wordt in principe uitsluitend gebruik gemaakt van speciaal daarvoor voorbehouden beveiligde computers.

---

[2] *Defense in depth* is een beveiligingsstrategie waarbij meerdere verdedigingslijnen in en rond een te beveiligen object zijn aangebracht. Het falen van één verdedigingslijn wordt daardoor opgevangen door de volgende lijn.

[3] Het betreft *extended validation* SSL certificaten met minimaal 128 bit encryptie van gereputeerde en algemeen aanvaarde certificatieautoriteiten.

2.2.6. Beveiligingsrichtlijnen voor de medewerkers

De operationele leiding keurt de richtlijnen voor de medewerkers inzake het veilig gebruiken van het Internet goed en ziet toe op de naleving ervan. Hierbij wordt bijzondere aandacht besteed aan:

- de risico's verbonden aan het downloaden en installeren van risicovolle bestanden ;
- de voorzorgsmaatregelen inzake het gebruik van e-mails (verdachte e-mails, spam, …) en andere Internetcommunicatietechnieken (bv. *instant messaging*) ;
- de voorzorgsmaatregelen en omkaderingsvoorwaarden voor het transfereren van bestanden ((s)ftp[4], …) ;
- de risico's verbonden aan de vaak uitgebreide Internettoegangen en –machtigingen van bepaalde gebruikers of informatici.

In het licht van de *phishing* e-mails[5] die erop gericht zijn cliënten te misleiden en door de zeer lage beveiliging van e-mails op het vlak van de confidentialiteit en de integriteit van hun inhoud, stelt de instelling richtlijnen op betreffende het aanvaardbare gebruik van e-mails bij diverse commerciële en andere externe contacten. Hierbij wordt eveneens aandacht besteed aan de andere gebruikte Internetcommunicatieoplossingen zoals bv. *instant messaging*.

2.2.7. Incidentbeheersprocedure

De instelling beschikt over een incidentbeheersprocedure voor de behandeling van Internetbeveiligingsincidenten. Hierin worden de taken/bevoegdheden toegewezen in het geval van ernstige Internetbeveiligingsincidenten en de te volgen escalatieprocedures toegelicht. Deze incidentbeheersprocedure legt ook de taken en verantwoordelijkheden vast inzake de interne en externe communicatie met betrekking tot belangrijke Internetbeveiligingsincidenten.

2.2.8. Audit trails, analyses en rapportering

Om onregelmatigheden of aanvallen tegen de aangeboden Internetdiensten te kunnen opsporen, analyseren en indien nodig stappen te ondernemen, houdt de financiële instelling de nodige technische logs en *audit trails* bij van toegangen tot en activiteiten op haar computersystemen (inclusief de applicaties) en netwerkcomponenten. Deze logs en *audit trails* dienen adequaat te worden beveiligd en opgeslagen om hun integriteit en bewijskracht te vrijwaren. Het verzekeren van hun rechtsgeldigheid vormt hierbij een belangrijk aandachtspunt.

In regel worden de voormelde logs en *audit trails* minimaal 6 maanden bijgehouden om te kunnen dienen bij latere disputen of analyses van misbruiken.

In functie van het risicoprofiel en de omvang van de aangeboden Internetdiensten analyseert de instelling met een gepaste frequentie de logs en *audit trails* met oog op het identificeren van onregelmatigheden of misbruiken. De instelling voorziet hiervoor de nodige gespecialiseerde middelen en effectieven.

De vastgestelde onregelmatigheden of misbruiken worden op een gepaste wijze aan de effectieve leiding gerapporteerd.

2.2.9. Uitvoeren van onafhankelijke veiligheidsonderzoeken

Instellingen die hun informatica-infrastructuur aansluiten op het Internet, laten de geïmplementeerde Internetbeveiligingsmaatregelen, door een onafhankelijke expert onderzoeken. Dergelijke onderzoeken omvatten penetratietesten en worden proactief uitgevoerd vooraleer de eigen informatica-infrastructuur of een nieuw onderdeel voor het eerst met het Internet wordt verbonden. Ze worden nadien herhaald in functie van de evolutie van de bedreigingen, het gebruik of het belang van de aangebrachte wijzigingen aan de gebruikte Internet(beveiligings)infrastructuur.

---

[4] *(Secured) File Transfer Protocol.*

[5] Frauduleuze namaak-e-mails die legitieme e-mails nabootsen met de bedoeling de ontvanger ervan te misleiden en hieruit een bepaald voordeel te halen. In de financiële wereld zijn *phishing* e-mails er vaak op gericht om geheime kredietkaart- of e-banking-authentificatiegegevens (gebruikersnamen en paswoorden, …) te verkrijgen.

In het algemeen wordt verwacht dat deze gespecialiseerde onderzoeken gebeuren door onafhankelijke externe deskundigen die hiervoor over de nodige knowhow, ervaring en aangepaste middelen beschikken. In uitzonderlijke gevallen kan het aanvaardbaar zijn dat de instelling deze onderzoeken zelf uitvoert op voorwaarde dat ze hiervoor over de nodige expertise beschikt en de uitvoerder van de test op geen enkele wijze betrokken is bij de ontwikkeling, de implementatie of het operationele beheer van de aangeboden Internetdiensten (bv. de interne IT-audit).

3. Beveiliging van financiële verrichtingen over het Internet

3.1. Verantwoording

Financiële instellingen die hun cliënten toelaten gegevens te consulteren of te beheren en/of verrichtingen uit te voeren en/of (in batch) door te sturen via het Internet (hierna transactionele diensten genoemd), worden blootgesteld aan bijkomende beveiligingsrisico's, bovenop de risico's die verband houden met het aansluiten van de (interne) informatica-infrastructuur op het Internet (cf. hoofdstuk 2).

Omdat financiële instellingen voor hun transactionele diensten over het Internet, steeds over een aansluiting moeten beschikken tussen de eigen informatica-infrastructuur en het Internet, vormen de navolgende beveiligingsvereisten een aanvulling op de beveiligingsrichtlijnen uit hoofdstuk 2.

Financiële instellingen die hun cliënten de mogelijkheid bieden om via hun Internetbeveiligingsoplossingen en/of -infrastructuur deel te nemen aan gangbare Internetbetalingsdiensten van derden (bv. *3D secure*-betalingen bij e-handelaars), dienen hiervoor aan bijkomende omkaderingsmaatregelen te voldoen (cf. punt 3.2.8.).

3.2. Prudentiële vereisten

3.2.1. Beveiligingsbeleid

De instelling besteedt in zijn beveiligingsbeleid op een gepaste wijze bijkomende aandacht aan :

- het belang van een aangepaste beveiliging van de aangeboden transactionele Internetdiensten en de doelstellingen ter zake ;
- de interne organisatie en verantwoordelijkheden op het gebied van :
    - de opvolging van de Internetbedreigingen voor de aangeboden transactionele diensten ;
    - de beveiliging van de aangeboden transactionele Internetdiensten ;
    - de centralisatie, behandeling en opvolging van beveiligingsgerelateerde klachten, inclusief de klachten van cliënten ;
- de afscherming en beveiliging van bij de transactionele Internetdiensten gebruikte authentificatiegegevens van de cliënten en de financiële instelling ;
- de afscherming en beveiliging van de via het Internet uitgewisselde informatie en cliëntenverrichtingen ;
- de beveiliging van de gebruikte transactionele Internetapplicaties ;
- de communicatie met de cliënteel over de aangeboden Internetdiensten en de wijze waarop de cliënten geacht worden bij te dragen tot de beveiliging van de aangeboden Internetdiensten ;
- de creatie en opslag van gepaste technische logs en logische *audit trails* van de Internetverrichtingen en hun analyse, opvolging en rapportering.

3.2.2. Analyse en opvolging van de bedreigingen en de eigen beveiligingssituatie

De instelling zorgt voor een goede analyse en opvolging van de bedreigingen voor de aangeboden transactionele Internetdiensten, rekening houdend met de door haar gebruikte en de aan de cliënten aangeboden beveiligingsoplossingen. Hierbij wordt de beveiliging in zijn geheel en component per component beoordeeld.

Op basis van de uitgevoerde analyses en rekening houdend met de aard en schaal van de aangeboden Internetdiensten, voert de instelling minstens jaarlijks een formele risico-evaluatie uit, om na te gaan of en in hoeverre de bestaande beveiligingsmaatregelen en de gebruikte technologieën of procedures dienen te worden aangepast. Hierbij houdt de instelling ook rekening met de tijd die nodig is om de benodigde aanpassingen te implementeren (inclusief de uitrol bij de cliënten) en de verwachte evolutie van de bedreigingen in deze periode.

De conclusies van de uitgevoerde opvolgingen en risicoanalyses worden in functie van hun dringendheid en belang en minstens éénmaal per jaar ter goedkeuring voorgelegd aan de effectieve leiding.

3.2.3. Beveiliging van de authentificatie

Het is van primordiaal belang dat alle toegangen tot en elk gebruik van de aangeboden Internetdiensten legitiem zijn. De instelling hanteert daarom sterke authentificatieoplossingen die aangepast zijn aan de aard en de risico's van de aangeboden Internetdiensten en die toelaten de identiteit van aangemelde gebruikers met een zeer hoge graad van zekerheid te verifiëren.

De instelling houdt bij de keuze van de gehanteerde authentificatieoplossing rekening met de Internetbeveiligingsrisico's langs de cliëntenzijde en de mogelijkheid van de cliënten om deze risico's in te schatten en af te dekken.

a) Authentificatieoplossingen voor particulieren

In de voormelde context en gelet op de sterk toegenomen bedreigingen van onder andere :

- de *phishing*-aanvallen ;
- vervalste websites ;
- de toegenomen verspreiding van kwaadaardige softwares op de computers van de cliënten die diverse confidentiële gegevens zoals authentificatie- (bv. gebruikersnamen, wachtwoorden, …) en financiële gegevens (bv. kredietkaartgegevens, ...) trachten te ontvreemden;

zijn authentificatieoplossingen die uitsluitend steunen op een beperkt aantal herbruikbare geheimen (bv. gebruikersnaam en wachtwoord al dan niet in combinatie met persoonlijke TAN-kaarten[6] of cijferreeksen of private software PKI-sleutels[7],…), die ongemerkt ontvreemd kunnen worden via het Internet, niet langer aanvaardbaar voor fraudegevoelige Internetdiensten. Voor Internetdiensten van louter consultatieve aard, dient de instelling een sensitiviteitsanalyse uit te voeren en een aangepast vertrouwelijkheids- en beveiligingsbeleid vast te leggen. Bij het gebruik van eenmalige wachtwoorden ter authentificatie, dienen de instellingen er bovendien voor te zorgen dat de geldigheidsperiode van deze eenmalige paswoorden tot het noodzakelijke minimum (i.e. maximum enkele minuten) wordt beperkt.

b) Authentificatieoplossingen voor bedrijven en professionelen

Voor de transactionele Internetdiensten aan bedrijven of professionelen kan de instelling gebruik maken van aangepaste authentificatieoplossingen waarbij de tegenpartij geheel of gedeeltelijk instaat voor de beveiliging van zijn persoonlijke authentificatiegegevens en *hard*- en *softwares* binnen zijn eigen informatica-infrastructuur. In voorkomend geval worden de bedrijven en/of professionele tegenpartijen door de instelling geïnformeerd over de verwachtingen ten aanzien van hun interne beveiligingsmaatregelen en worden de betreffende verantwoordelijkheden duidelijk afgelijnd in de bijbehorende contracten.

---

[6] I.e. kaarten of andere gegevensdragers met een beperkt aantal vooraf gegenereerde paswoorden die de cliënt dient in te voeren bij het aanmelden of het uitvoeren van verrichtingen. De Internetapplicatie geeft hierbij aan welk paswoord door de cliënt dient te worden ingevoerd.

[7] Bij een software PKI (*public key infrastructuur*) wordt elke gebruiker op een unieke manier geïdentificeerd aan de hand van een hem toegekende private softwaresleutel die vaak op de computer van de cliënt wordt opgeslagen.

c) Interne beveiligingsmaatregelen

De instelling ziet erop toe dat alle door de cliënten benodigde authentificatiegegevens én cliëntgebonden *hard*- en *softwares* op een veilige manier aan de cliënten worden bezorgd. *Softwares* die aan de cliënten worden ter beschikking gesteld en door de cliënten moeten worden gebruikt, worden fysiek verzegeld en/of digitaal ondertekend door de financiële instelling, om de cliënten toe te laten de authenticiteit ervan na te gaan.

Om haar transactionele websites te identificeren ten aanzien van haar gebruikers maakt de instelling gebruik van kwaliteitsvolle digitale certificaten[8] op haar naam of andere gelijkwaardige authentificatiemechanismen.

De instelling draagt er zorg voor dat alle gegevens of bestanden om haar cliënten en haar eigen websites te identificeren, op een gepaste wijze worden beveiligd tegen diefstal of ongeautoriseerde consultaties of wijzigingen.

De instelling beperkt het maximale aantal toegelaten foutieve aanmeldpogingen waarna de toegang tot de Internetdienst al dan niet tijdelijk wordt geblokkeerd, evenals de maximale tijdsduur waarna openstaande niet-gebruikte Internetsessies worden afgebroken (in regel maximaal 15 minuten). De instelling beschikt over een beveiligde procedure om de geblokkeerde toegangen te ontgrendelen.

3.2.4. De afscherming en beveiliging van de informatie en verrichtingen

Om de confidentialiteit van de informatie en verrichtingen tussen de cliëntencomputer en de financiële instelling te vrijwaren, maakt de instelling gebruik van sterke en algemeen erkende “encryptie”-technieken.

De instelling beschikt over technische authenticiteitscontroles (bv. *message authentication codes* (MAC’s), …) om accidentele wijzigingen van de cliëntenverrichtingen ten gevolge van technische storingen op te sporen.

Daarnaast beschikt de instelling over gepaste effectieve beveiligings- en/of *monitoring*-oplossingen, die toelaten frauduleuze verrichtingen met een hoge waarschijnlijkheid te verhinderen of te detecteren vóór ze worden uitgevoerd. Voorbeelden van effectieve beveiligingsoplossingen op dit vlak zijn eenmalige paswoorden of elektronische handtekeningen die worden gegenereerd met betekenisvolle kenmerken van de cliëntenverrichting (bv. bedrag en/of een deel van het rekeningnummer van de begunstigde) of kwaliteitsvolle *dual channel*-oplossingen[9], waarbij de Internetverrichting van de cliënt wordt bevestigd via een tweede onafhankelijk communicatiekanaal (bv. via de mobiele telefoon). Bij de Internetdiensten aan bedrijven en professionelen wordt bovendien vaak beroep gedaan op in de Internetapplicatie ingebouwde functiescheidingen, waardoor een verrichting door meerdere personen moet worden ingevoerd en/of goedgekeurd (principe van *independent checker of validator*).

De instelling verifieert op een gepaste manier, in functie van de aard en het risico van de verrichting, de identiteit en de daaraan gekoppelde bevoegdheid van de cliënt voor elke cliëntenverrichting[10] die ze ontvangt.

3.2.5. De beveiliging van de Internetapplicaties en -servers

De instelling besteedt bij de ontwikkeling en het onderhoud van de Internetapplicaties voldoende aandacht aan :

- de veiligheidskenmerken en -risico’s van de door haar gebruikte applicatiearchitectuur, programmeertechnieken en routines, om de kwetsbaarheid van de applicatie voor kwaad-

[8] Het betreft *extended validation* SSL certificaten met minimaal 128 bit encryptie van gereputeerde en algemeen aanvaarde certificatieautoriteiten.

[9] I.e. *dual channel*-oplossingen waarbij het gebruikte tweede communicatiekanaal niet aan dezelfde risico’s is blootgesteld als het eerste communicatiekanaal. Omdat steeds meer communicatiekanalen op het Internet worden aangesloten en gebruik maken van Internettechnologieën, dient de onafhankelijkheid van de 2 gebruikte kanalen minstens jaarlijks opnieuw geëvalueerd te worden.

[10] De bundeling van meerdere soortgelijke cliëntenverrichtingen is toegestaan voor zover dit de benodigde hoogstaande veiligheid van de verrichtingen niet in het gedrang brengt.

aardige aanvallen (bv. *session hijacking*, *SQL injection*, *cross site scripting*, *buffer overflows*, …) tot een minimum te beperken ;
- de gevolgen van de door haar gemaakte technologische keuzes op de beveiliging langs de cliëntenzijde (bv. gebruik van multimedia-applicaties, plug-ins, externe doorverwijzingen, …).

Hierbij is het van belang dat zowel de ontwikkelaars van de applicaties als de beheerders van de gecontroleerde doorgeefluiken tussen het Internet en de interne informatica-infrastructuur (cf. punt 2.2.3), over een afdoende kennis beschikken inzake de organisatie en de werking van de verschillende verdedigingslijnen *(defense in depth*)[11] en de interactie daartussen.

De beveiliging van de transactionele websites en servers dient **voor het overige** aan dezelfde eisen te voldoen als de publieke websites (cf. punt 2.2.4.).

3.2.6. De cliëntencommunicatie

Hoewel het gebruik van technologische oplossingen noodzakelijk is voor de beveiliging van financiële diensten over het Internet, volstaan deze meestal niet om hun beveiliging te garanderen. Het gebruik van de ter beschikking gestelde technologieën en toepassingen door de cliënt, evenals de zorg door de cliënt voor de veiligheid van de door hem gebruikte computer(infrastructuur), vormen immers vaak de zwakste schakels in de beveiligingsketting.

De instelling stelt in dit verband eenvoudige en goed verstaanbare handleidingen en documentatie op voor de cliënt, waarbinnen de cliënt gewezen wordt op zijn verantwoordelijkheden voor het veilig gebruik van de aangeboden Internetdiensten.

Aspecten die hierin minimaal aan bod dienen te komen zijn :
- de vereiste geheimhouding door de cliënt van de geheime authentificatie- of pin-codes ;
- de regels inzake het correct en veilig gebruiken van alle door de cliënt aangewende *hard*- en *softwares* (cliëntencomputer, …) ;
- de te volgen procedures bij diefstal of het verlies van geheime gebruikersgegevens of de cliëntgebonden *hard*- en *softwares* die nodig zijn om zich aan te melden of transacties uit te voeren ;
- de te volgen procedure bij vaststelling van of een vermoeden inzake misbruiken ;
- de door de instelling gevoerde politiek inzake het verzenden van e-mails of andere elektronische berichten (bv. *instant messaging*, SMS, …) naar cliënten.

De instelling beschikt bovendien over een aangepaste communicatiepolitiek om de cliënten tijdig te informeren over en/of te sensibiliseren voor nieuwe evoluties en aandachtspunten inzake het veilig gebruik door de cliënt van de aangeboden Internetdiensten.

3.2.7. Uitvoeren van onafhankelijke veiligheidsonderzoeken

Instellingen die het Internet gebruiken voor transactionele doeleinden (bv. het afsluiten van een verzekeringspolis, het doorgeven van betalingsinstructies en/of beursverrichtingen, …) en/of hun cliënten toelaten confidentiële gegevens te consulteren, laten de veiligheid van hun transactionele Internetdiensten door een onafhankelijke expert onderzoeken vóór de lancering van de Internetdiensten, daarna gevolgd door onafhankelijke gespecialiseerde veiligheidsonderzoeken in functie van de evolutie van de bedreigingen of de aangebrachte technologische of functionele wijzigingen aan de aangeboden Internetdiensten. De uitgevoerde testen omvatten zowel penetratie[12]- als applicatietesten[13] voor verschillende soorten *online*-aanvallen.

De vereisten inzake de deskundigheid en de onafhankelijkheid van de ingeschakelde experten zijn gelijk aan deze in punt 2.2.9.

---

[11] *Defense in depth* is een beveiligingsstrategie waarbij meerdere verdedigingslijnen in en rond een te beveiligen object zijn aangebracht. Het falen van één verdedigingslijn wordt daardoor opgevangen door de volgende lijn.

[12] Bij een penetratietest wordt de beveiliging van de perimeter van de eigen informatica-infrastructuur nagegaan.

[13] I.e. *application cracking* om na te gaan of de applicatie vatbaar is voor aanvallen zoals *SQL injection*, *cross site scripting*, *buffer overflows*, enz.

3.2.8. Deelname aan gangbare Internetbetalingsdiensten van derden

Financiële instellingen die hun cliënten de mogelijkheid bieden om via hun Internetbeveiligingsoplossingen en/of –infrastructuur deel te nemen aan gangbare (internationale) Internetbetalingsdiensten van derden (bv. *3D secure*-betalingen), ontwikkelen ter zake een aanvaardingsbeleid waarin aandacht wordt besteed aan:

- de reputatie en de financiële en operationele soliditeit van de aanbieder van de Internetbetalingsdiensten ;
- de aard en de risico's van de aangeboden betalingsdiensten in hun globaliteit (bedragen, begunstigden,…), rekening houdend met de aangeboden beveiligingsoplossingen en/of -mogelijkheden ;
- de aflijning van de verantwoordelijkheden tussen de betrokken partijen voor de beveiliging van de verrichtingen en de vergoeding van cliënten bij misbruiken en/of betwistingen ;
- het wettelijk (controle)statuut van de aanbieder van de Internetbetaaldiensten ;
- mogelijke reputatierisico's voor de financiële instelling.

De effectieve leiding (in de regel het directiecomité) keurt het aanvaardingsbeleid goed en ziet toe op zijn naleving. De instelling zorgt bovendien jaarlijks voor een goede analyse en opvolging van de bedreigingen voor de aanvaarde derde Internetbetalingsdiensten, rekening houdend met de gehanteerde beveiligingsoplossingen.