

Internet: de risico's voor banken

INTERNETRISICO'S VOOR BANKEN: DE VERZEKERINGSOPLOSSINGEN

Wat is er zoal voor nodig om een bank in zwaar weer te doen belanden? Dat een internationale kredietcrisis hiertoe kan bijdragen, mag inmiddels duidelijk zijn. Daarnaast zien we dat het in de markt zetten van onvoldoende doordachte hypotheek- en/of beleggingsproducten tot torenhoge aansprakelijkheidsclaims kan leiden. Ook door de daden van Jérôme Kerviel bij Société Générale is de kwetsbaarheid van bankinstellingen weer eens op pijnlijke wijze aangetoond.

De diverse wet- en regelgevingen, zoals Basel II, Wft en ook MiFid, dragen er gelukkig aan bij dat een groot aantal risico's beter beheersbaar wordt. Zolang bankieren echter een kwestie is van ondernemen en de wereld om ons heen aan verandering onderhevig is, blijven banken geconfronteerd met risico's die niet altijd te vermijden zijn. De risico's, die banken lopen met het gebruik van Internet, zijn hier een voorbeeld van.

De laatste vijftien jaar hebben de vele ontwikkelingen op automatiseringsgebied nieuwe operationele risico's voor banken met zich meegebracht. Internet is niet meer weg te denken uit de financiële dienstverlening en om vernieuwend te zijn, moeten banken nieuwe Internet-diensten blijven aanbieden. Snelheid en timing zijn hierbij essentieel; de zorgvuldigheid en daarmee ook de veiligheid kunnen hieronder lijden. Door deze toenemende afhankelijkheid van Internet, staan banken bloot aan diverse operationele risico's.

Operationele risico's

Er zijn talloze risicovoorbeelden te noemen, zoals het hacken van computersystemen met als doel het kopiëren van geheime informatie, of het op frauduleuze wijze online aanvragen en ontvangen van een lening met een valse of illegaal verkregen elektronische handtekening. Verder is er het risico op het verspreiden van een virus dat essentiële bedrijfsinformatie vernietigt. Een ander gevaar is dat hackers onjuiste informatie op de website plaatsen. Denk hierbij aan de gevolgen van de verspreiding van

BERNARD GOEDE

onjuiste informatie via de website aan aandeelhouders, zoals kwartaalcijfers. Bovendien is het 'spammen' van een website (het in één keer versturen van enorme hoeveelheden e-mails) een risico waardoor een bank haar online diensten, zoals elektronische betalingen of online effectentransacties, niet kan aanbieden.

De risico's voor banken volgens De Nederlandsche Bank

Bij het bepalen van de risico's die banken lopen, maakt De Nederlandsche Bank (DNB) onderscheid in vijf risico's; het krediet-, het markt-, het liquiditeits-, het strategische en het operationele risico. DNB omschrijft het operationele risico voor banken als 'de kans op verliezen als gevolg van inadequate of falende interne processen, mensen of systemen of door externe omstandigheden'. Van deze genoemde risicovormen zijn de operationele risico's het best te verzekeren. Gangbare verzekeringen voor banken zijn dan ook de bestuurdersaansprakelijkheidsverzekering, beroepsaansprakelijkheidsverzekering en de (computer)fraudeverzekering.

Dekking operationele Internetrisico's

Risico's op het gebied van Internet worden in onvoldoende mate afgedekt door traditionele verzekeringen. Bij veel traditionele verzekeringsvormen dient er sprake te zijn van een tastbare schade of er dient aansprakelijkheid te bestaan op basis van een gemaakte beroepsfout.



Veel schades die verband houden met Internet zijn echter niet tastbaar. Daartoe is sinds enkele jaren de uit Amerika afkomstige cybersecurityverzekering in Europa op de markt. Deze cybersecurityverzekering voorziet hiermee in een nieuwe behoefte. Enkele belangrijke dekkings-elementen van deze verzekeringsvorm zijn: *Denial or impairment of E-service, E-Theft, E-communication*.

Dekkings-elementen cybersecurityverzekering

- Denial or impairment of E-service biedt dekking voor de ontstane bedrijfsschade en de extra kosten als gevolg van een cyberaanval, bijvoorbeeld door het gebruik van 'worms' of 'spamming'. De gederfde inkomsten zijn verzekerd voorzover de verzekerde bank haar Internetdiensten niet of niet naar behoren kan aanbieden. Het belangrijke verschil met een traditionele bedrijfsschadeverzekering is, dat de cybersecurityverzekering niet vereist dat er fysieke schade moet zijn aan tastbare eigendommen.
- E-Theft biedt onder andere dekking voor de geleden schade doordat hackers gevoelige klanteninformatie kopiëren, dupliceren en/of misbruiken. Ook frauduleuze financiële transacties, gedaan door hackers, worden hieronder verzekerd. Opvallend is de dekking in gevallen waarbij een geautoriseerde gebruiker zijn bevoegdheden te buiten gaat. De traditionele computerfraudeverzekeringen voor financiële instellingen, bieden uitsluitend dekking voor computerfraude door ongeautoriseerde gebruikers.
- E-communication ziet toe op de gevallen waarbij er iets mis gaat in de elektronische communicatie tussen twee banken. Bij het grote aantal financiële transacties dat via Internet wordt verricht, is het bijna onmogelijk te garanderen dat alle transacties 100% veilig zijn. De verzekering treedt in werking wanneer bij een financiële transactie tussen twee banken een betaling onderschept of gemanipuleerd wordt.
- Naast de genoemde dekkings-elementen voorziet de cybersecurityverzekering in dekking voor E-Vandalisme (vandalisme op websites zoals het moedwillig verwijderen van informatie of het doorlinken van bezoekers naar andere sites), E-Threat (afpersing door te dreigen met een cyberaanval of met het openbaar maken van gevoelige informatie die door hacking is verkregen) en E-Signature (fraude met elektronische handtekeningen, bijvoorbeeld bij het aanvragen van een hypotheek).
- De polis kan nog verder worden uitgebreid met een cybersecurity-aansprakelijkheidsdekking, waardoor de bank verzekerd is voor aansprakelijkheid jegens cliënten of derden indien bijvoorbeeld de electronic bankingsystemen niet functioneren of omdat vertrouwelijke informatie door hackers openbaar is gemaakt.



Een hiaat gedicht

De verzekeringsindustrie dicht met de cybersecurityverzekering een hiaat in de verzekeringsmogelijkheden van bancaire operationele risico's. Dit is zeker geen onbelangrijke ontwikkeling nu het onderwerp risicobeheer bij veel banken hoog op de agenda staat.

De ontwikkeling van de dienstverlening door banken via Internet zal de komende jaren onverminderd doorgaan. Dit leidt onvermijdelijk tot een nog grotere afhankelijkheid van IT-infrastructuren dan vandaag de dag al het geval is. Door deze toenemende afhankelijkheid nemen automatisch ook de risico's toe. Met hetzelfde tempo waarin de dienstverlening via Internet zich ontwikkelt, verandert immers ook de mate van veiligheid. Een beveiligingsmaatregel die vandaag nog afdoende is, kan morgen waardeloos zijn.

Naast het voeren van een actief risicomanagement- en veiligheidsbeleid, is het van belang voor zowel verzekeren als verzekeraars om zich doorlopend te blijven afvragen welke Internetrisico's verzekerd zijn onder de bestaande verzekeringen en welke niet.

Het is dan ook essentieel dat verzekeraars blijven innoveren en blijven streven om dekkingen te ontwikkelen voor de nog onbekende en ongeïdentificeerde risico's die Internet met zich meebrengt. •

Bernard Goede (1968) is sinds 1996 werkzaam bij de Chubb Insurance Company of Europe S.A. Sinds 2005 is hij verantwoordelijk voor de afdeling Financiële Instellingen in de Benelux. Deze afdeling biedt verzekeringsoplossingen voor o.a. banken, verzekeraars, vermogensbeheerders, (vastgoed)investeringsfondsen en venture capital ondernemingen.