Toezicht expertisecentra
ICT risico's

Amsterdam
Postbus 98
1000 AB Amsterdam

Confidentieel

Datum
23 november 2011
Uw kenmerk

Ons kenmerk
2011/762950
Behandeld door
Baveco, M.P.P. (drs. ir.) RE CISSP
Doorkiesnummer

Bijlage(n)

Onderwerp
Circulaire Info beveiliging.definitieve versie.23-11-2011

Geacht bestuur,

Financiële ondernemingen en hun klanten zijn meer en meer doelwit van Cybercrime aanvallen. Daarbij ziet de Nederlandsche Bank (DNB) zowel het aantal incidenten als de bijbehorende impact toenemen. Een ontwikkeling die ook steeds zichtbaarder wordt gezien de recente berichtgeving in de media. Een adequate informatiebeveiliging is daarom essentieel.

Met deze circulaire wil DNB het onderwerp Informatiebeveiliging binnen de financiële sector nader onder de aandacht brengen en u adviseren om vast te stellen in hoeverre binnen uw organisatie er sprake is van een adequaat informatiebeveiligingsniveau.

Informatiebeveiliging behoeft aandacht
Op basis van recent onderzoek[1] heeft DNB vastgesteld dat bij slechts 15% van de onderzochte financiële ondernemingen informatiebeveiliging volledig op orde is. Daarbij zijn soms serieuze aandachtspunten op het gebied van informatiebeveiliging geconstateerd . Dit versterkt de kans op financiële en reputatieschade en kan leiden tot ondermijning van het vertrouwen in de financiële sector. Enkele constateringen uit het DNB-onderzoek zijn:

- Financiële ondernemingen zijn vaak sterk afhankelijk van externe leveranciers, maar hebben veelal geen zicht op de wijze waarop externe leveranciers hun beveiliging daadwerkelijk geregeld hebben en hoe leveranciers met gevoelige klantinformatie omgaan.
- De autorisaties van medewerkers en IT-beheerders voor toegang tot kritische bedrijfsapplicaties zijn veelal te ruim ingesteld, waardoor ongeautoriseerden toegang hebben tot gevoelige informatie.
- De IT-omgeving wordt slecht gemonitord. Hierdoor worden aanvallen vanaf het internet niet of te laat ontdekt. Door het uitblijven van tijdige herstelmaatregelen leiden financiële ondernemingen veelal meer schade dan nodig.
- Ondanks de snelle IT-ontwikkelingen bekijken ondernemingen niet periodiek of nieuwe beveiligingsmaatregelen noodzakelijk zijn. Hierdoor lopen ondernemingen onder meer op het gebied van internet en mobiele beveiliging achter de feiten aan.

1 DNB thema onderzoek Informatiebeveiliging 2010-2011

- Informatiebeveiliging wordt veelal gezien als een IT-aangelegenheid. De omgang met vertrouwelijke documenten, het risicobewustzijn van medewerkers en de toegang tot kantoren zijn echter minstens zo belangrijk. Kortom 'de zwakste schakel' bepaalt het niveau van informatiebeveiliging.

Naar aanleiding van het onderzoek heeft DNB met individuele financiële ondernemingen afspraken gemaakt om de eerdergenoemde aandachtspunten aan te pakken. Daarnaast heeft DNB met diverse koepelorganisaties de onderzoeksresultaten besproken. Voor de betrokken koepelorganisaties is dat aanleiding om het onderwerp Informatiebeveiliging prominenter bij de leden onder de aandacht te brengen. DNB vindt dit een positief initiatief dat u zou kunnen helpen op het gebied van informatiebeveiliging.

Informatiebeveiliging binnen uw organisatie
Voor DNB vormen de eerdergenoemde onderzoeksuitkomsten en de toenemende cybercriminaliteit redenen om het onderwerp Informatiebeveiliging via deze circulaire binnen de financiële sector onder de aandacht te brengen. In dat kader adviseert DNB dat u nagaat in hoeverre de eerdergenoemde punten spelen binnen uw organisatie en of er sprake is van een adequaat informatiebeveiligingsniveau. In het verlengde gaat DNB ervan uit dat zonodig aanvullende maatregelen worden geïmplementeerd om tot een acceptabel restrisico te komen.

Om het niveau van informatiebeveiliging te kunnen vaststellen, heeft DNB een model gebaseerd op CobIT* gedefinieerd. Het model helpt om voor de belangrijkste punten van informatiebeveiliging vast te stellen of ze adequaat worden beheerst. Het betreffende model is beschikbaar via de openbare DNB website (http://www.toezicht.dnb.nl/3/50-203304.jsp).

Vervolgactiviteiten DNB
DNB zal risicogebaseerd financiële ondernemingen benaderen om de beheersing van de IT-risico's te bespreken. In het bijzonder zal beoordeeld worden hoe wordt omgegaan met de beveiliging van vertrouwelijke informatie. DNB zal hierbij specifiek ingaan op de door de financiële onderneming uitgevoerde analyse met eventueel geformuleerde verbeteracties. Daarbij zal DNB het volwassenheidsniveau van alle in het model opgenomen maatregelen meenemen in haar beoordeling. DNB zal bij de wijze waarop maatregelen zijn ingevuld rekening houden met de complexiteit en omvang van de financiële onderneming.

Voor eventuele vragen naar aanleiding van deze brief kunt u contact opnemen met de heer Baveco (email M.P.P.Baveco@dnb.nl) of Bikker (email J.Bikker@dnb.nl).

Hoogachtend,
De Nederlandsche Bank NV

mw mr. dr. F. de Vries
Divisiedirecteur

drs. E. Koning RE RA CISA
Afdelingshoofd

* CobIT (Control Objectives for Information and related Technology) is een open internationale IT governance standaard van ISACA – www.isaca.org.