Code voor de beveiliging van computergegevens

De Code voor Informatiebeveiliging is een leidraad voor praktische informatiebeveiliging en ontwikkeld in antwoord op de vraag naar praktische hulpmiddelen voor beveiliging van informatie in computers en netwerken. De Code biedt een gemeenschappelijke basis voor bedrijven om beveiligingsbeleid te ontwikkelen, de nodige plannen op te stellen en zo tot 'beveiliging op maat' te komen.

Dr.ir. P.L. Overbeek *

Informatiebeveiliging staat momenteel volop in de belangstelling. De kranten staan vol met de meest spectaculaire incidenten. De ene keer is het justitie of de politie waar diskettes worden gestolen, een andere keer is het een hoge ambtenaar die zijn lap-top met strategische informatie in de trein laat liggen.
Maar deze gevallen zijn niet representatief voor de huidige stand van de beveiliging. Uit verschillende onderzoeken, ook in Europees verband, blijkt namelijk dat het vooral het Midden- en Klein Bedrijf (MKB) is waar het meest geleden wordt, en waar ook de meeste schade ontstaat door gebrekkige beveiliging.

Urgente problemen

In de publiciteit is er vaak kritiek op de gebrekkige technische beveiliging. Deze kritiek is maar ten dele terecht. Het gaat altijd om een evenwicht in de maatregelen: fysieke afscherming, technische hulpmiddelen, ondersteunende procedures, en dat geheel ingebed in een passende organisatie.

In de publiciteit is er vaak kritiek op de gebrekkige technische beveiliging.

De Code voor Informatiebeveiliging is juist ontwikkeld om aan die meest urgente problemen wat te doen: een eenvoudig hulpmiddel - ook toepasbaar in het MKB - om evenwicht in de beveiliging te brengen.
De Code biedt een basis voor de bescherming van informatie. Deze basis wordt gegeven als een verzameling basisprincipes voor beveiliging, zeg maar 'de tien geboden' voor informatiebeveiliging. In de eerste plaats is het de bedoeling van de Code om in eigen huis orde op zaken te stellen. Bovendien is de Code bedoeld als referentiekader tussen (elektronische) zakenpartners. In zaken moet u op elkaar kunnen vertrouwen. Dat geldt zeker als uw organisatie afhankelijk wordt van (de beveiliging bij) partners waarmee u elektronisch zaken doet.

Ontstaansgeschiedenis

De Code voor Informatiebeveiliging is overgewaaid uit Engeland. De Engelse versie is ontwikkeld door onder andere Marks and Spencer, Midlands Bank, Shell, Unilever en British Telecommunications en zal eerdaags de status van British Standard verkrijgen.
De Nederlandse introductie van de Code wordt onder andere gestimuleerd door het Ministerie van Economische zaken dat hiermee het belang van informatiebeveiliging voor het Nederlandse bedrijfsleven onderschrijft.

Eerst moet duidelijk zijn welke kant de organisatie op moet met de beveiliging.

Ook organisaties als de Federatie van Nederlandse Informatie Technologie (FENIT), Raad Centrale Ondernemingsorganisaties (RCO), en de Raad voor de Informatie Technologie (RIT) ondersteunen het gebruik van de Code.
Eerst moet duidelijk zijn welke kant de organisatie op moet met de beveiliging. Daar is niet meteen een uitgebreide risico-analyse voor nodig. Veelal is het voldoende om een prioriteitenlijstje te maken voor de meest urgente beveiligingseisen en -wensen. De eerste bron daarvoor is een inschatting van de grootste beveiligingsrisico's (bedreigingen en zwakke plekken) voor de informatie in de computers en netwerken; dit in het licht van het bedrijfsbelang.

De 'Tien Geboden'

De tweede bron is simpel naar buiten kijken: wat schrijven wetten en contracten voor en wat is goed gebruik in de branche (en natuurlijk proberen altijd iets beter dan de concurrent te zijn)?
De derde bron komt uit het bedrijf zelf: waar zijn de bedrijfsdoelstellingen op gericht, wat betekent dit voor de informatievoorziening en hoe moet de informatiebeveiliging daar op anticiperen? Afstemming met andere vormen van beleid, zoals het informatiebeleid en het algemene beveiligingsbeleid, is daarbij noodzakelijk.

De Code gaat uitgebreid in op de eerste bron met een beschrijving van risico's en mogelijke maatregelen. Voor de tweede en derde bron wordt een raamwerk gegeven. In de Code zijn tien categorieën vastgesteld als aandachtsgebieden voor beveiliging, zie tabel 1.

Beveiligingscategorieën
Beleid
Organisatie
Classificatie en beheer
Personeel
Fysieke beveiliging & omgeving
Computer- en netwerkbeheer
Toegangsbeveiliging
Bouw & onderhoud van systemen
Calamiteit en continuïteit
Toezicht

Tabel 1.

Iedere categorie is op dezelfde wijze opgebouwd: er zijn doelstellingen en er is basisverzameling aan beveiligingsmaatregelen om een doelstelling te bereiken.
Als voorbeeld uit de Code nemen we categorie 2: de organisatie van de beveiliging. De doelstelling is om een managementkader op poten te zetten voor informatiebeveiliging.
Als maatregelen zijn tenminste vereist: het toekennen van verantwoordelijkheden, coördinatie tussen verantwoordelijken en duidelijke rapportagelijnen. Activiteiten zijn bijvoorbeeld: herziening van beleid, toezicht op veranderende risico's, opstellen van uitwijkplannen, reageren op incidenten, organiseren van externe onafhankelijke beoordeling van de beveiliging.

Belangrijkste maatregelen
Doelstellingen voor beveiliging
Verantwoordelijkheden
Training en opleiding
Rapportage van incidenten
Viruscontrole
Reageren op calamiteiten
Import/export (o.a. programmatuur, informatie)
Veiligstellen van informatie (back-up)
Voldoen aan wet/regelgeving (o.a. privacy-wet)
Interne controle

Tabel 2.

Alle categorieën worden zo behandeld: de doelstellingen, mogelijke beveiligingsmaatregelen - eigenlijk een ondergrens - en soms activiteiten om tot een selectie van maatregelen of zelfs het opstellen van een plan te komen.
Om de drempel te verlagen is een top-10 opgesteld van beveiligingsmaatregelen, zie tabel 2. Het idee is dat deze maatregelen de hoogste prioriteit moeten hebben als een organisatie nog niets aan beveiliging heeft gedaan.

Er is tevens een ondersteunend stappenplan beschikbaar als een 'vliegende start' voor het van de grond tillen van een beveiligingsorganisatie volgens de stappen:

1 Beleid;
2 Organisatie;
3 Prioriteiten stellen/risico-analyse;
4 Selectie en implementatie van maatregelen;
5 Ontwikkeling van plannen (uitwijk, continuïteit);
6 Training en opleiding;
7 Controle en evaluatie;
8 Terug naar stap 1.

Natuurlijk is beveiliging geen eenmalige exercitie maar een continu proces. Heeft u uw beveiliging eenmaal op orde, dan is het misschien de moeite waard om nogmaals naar uw externe afhankelijkheden te kijken: is de beveiliging bij uw zakenpartners voldoende voor uw belangen?

De Code: een startpunt

De Code voor Informatiebeveiliging is een middel voor het leggen van een bodem, het noodzakelijke draagvlak, voor beveiliging in uw organisatie. Met de Code kan tenminste een algemeen geldend minimumniveau voor beveiliging in uw organisatie bereikt worden. Voor specifieke toepassingen zijn aanvullende maatregelen noodzakelijk, zoals ook in de Code wordt aangegeven. Voorbeelden waarin extra beveiligingsmaatregelen nodig zijn: de systemen waarmee bijzonder strategische of gevoelige gegevens worden verwerkt, de systemen waarvan uw bedrijfsvoering direct afhankelijk is (mission critical systems) en de systemen die mogelijk schade aan de belangen van derden kunnen veroorzaken (safety critical systems). In dit soort gevallen zijn aanvullende maatregelen mogelijk en noodzakelijk.

Met het gebruik van de Code kan het algehele IT-beveiligingsniveau in Nederland verbeteren.

Met het gebruik van de Code kan het algehele IT-beveiligingsniveau in Nederland verbeteren. Vooral het midden- en kleinbedrijf zal hier voordeel bij hebben. Tevens kan de Code gebruikt worden tussen zakenpartners, zodat op een verantwoorde manier gebruik gemaakt kan worden van de nieuwe technologische mogelijkheden in de industrie. Dat is goed voor het Nederlandse bedrijfsleven.
De Code voor Informatiebeveiliging is te bestellen bij het Nederlands Normalisatie Instituut in Delft, telefoon: 015 - 690390. Tevens is er een gratis helpdesk voor het gebruik van de Code ingericht door de Raad voor de Informatietechnologie in Den Haag (070 - 3819444). ◄

* is werkzaam bij TNO - Fysisch en Elektronisch Laboratorium, Den Haag