BORG *in de* ICT omgeving

Ronald Eygendaal, CPO

BORG is een kwaliteitssysteem, zodat beveiligingsbedrijven garant kunnen staan voor het leveren van kwalitatief goede beveiligingsproducten en/of diensten. Als het product en/of dienst is geleverd, kan een klant een schriftelijk bewijs hiervoor ontvangen: het zogenaamde BORG Certificaat. Dit certificaat is voor verzekeraar een 'bewijs' dat alle beveiligingsmaatregelen zijn uitgevoerd volgens een bepaalde risicoklasse methodiek. Daarmee is binnen gestelde criteria voldaan aan risicobeperking in relatie tot acceptatie door de verzekeraar van het risico.

Betrouwbaar heid is ook een waarde-bepalings-aspect.

BORG EN ICT

Elektronische inbraaksignaleringssystemen, dit zijn stelsels van detectoren centrales en alarmgevers, welke er op zijn gericht om de inbreker vroegtijdig op te merken, zowel buiten als binnen een gebouw. In combinatie met andere maatregelen, zoals bouwkunde, mechanische en organisatorische maatregelen, geven dergelijke systemen een goede beveiliging en geven tevens recht op het BORG certificaat. Als er sprake is van een ICT omgeving, kunnen er veel fouten worden gemaakt met de risicoklasse indeling, zoals beschreven binnen BORG. Hierdoor worden de risico's welke verbonden zijn aan ICT omgevingen, verkeerd ingeschat en zijn bij schades de gevolgen niet te overzien.

Als we de feitelijke oorzaken naast de gebruikte methodiek leggen of plaatsen, vallen er een aantal zaken op. Een van de oorzaken van deze fouten zou kunnen zijn dat BORG geen methodiek heeft om de risicoklasse voor bedrijven met veel ICT dienstverlening in kaart te brengen. Vroeger speelde deze problematiek alleen bij de grote bedrijven; tegenwoordig zijn bij voorbeeld 'e-business', 'webwinkels' en dergelijke begrippen die in het midden- en kleinbedrijf dagelijkse praktijk zijn geworden.

VERWACHTINGEN VAN DIT ARTIKEL.

Dit artikel is geschreven om de discussie los te maken hoe we deze ' nieuwe' risico's kunnen onderbrengen in een 'BORG systeem' voor de ICT omgeving. Met de uiteindelijke bedoeling dat het Nationaal Centrum voor Preventie, in overleg met deskundigen uit het ICT beveiligingswerkveld, al dan niet in samenwerking met de VBN vakgroep ICT Beveiliging, tot een aanpassing komt van BORG.

Ik wil nogmaals nadrukkelijk vermelden dat het hier uitsluitend gaat om preventieve maatregelen tegen fysieke inbraak en NIET tegen zaken zoals brand, stroomuitval en dergelijke.

DE KNELPUNTEN IN DE RELATIE BORG & ICT

Zoals al eerder aangegeven is BORG een kwaliteit methodiek. Een onderdeel van BORG is het 'meten' van het inbraakrisico en het bepalen van de meest geschikte inbraakpreventieve maatregelen. Hiervoor hebben de verzekeraars de 'risicoklasse indeling' ontwikkeld. Dit is een systeem om de inbraakgevoeligheid van gebouwen te meten en dit met behulp van het systeem van risicopunten, in een aantal klassen in te delen. Bij iedere risicoklasse hoort vervolgens een beveiligingsklasse, dit is geschaald van 1 tot 4, die de meest geschikte combinatie van inbraakpreventieve maatregelen omvat. Een nadeel van deze methodiek is dat deze niet aansluit op de 'nieuwe' risico's veroorzaakt door de ICT. Hierdoor komen bedrijven met veel ICT dienstverlening vaak in de verkeerde beveiligingsklasse terecht. De inbraakpreventieve maatregelen worden weergegeven met de letters B, E, C en/of M en O. Dit betekent respectievelijk:

- B = Bouwkundig,
- E = Elektronische,
- C = Compartimenterings en/of Meeneem beperkende maatregelen
- O = Organisatorische maatregelen

Daarnaast is er een implementatierichtlijn, welke iets zegt over de 'zwaarte' van de beveiligingsmaatregelen. De implementatierichtlijn wordt aangeduid met een kleine letter:

- s = standaard
- n = normaal
- z = zwaar

Kort samengevat worden de navolgende lettercombinaties gebruikt voor het weergeven van de beveiligingsmaatregelen en hun implementatierichtlijn.

Bouwkundige maatregelen [1]

Bs De 'standaard' toe te passen bouwkundige maatregelen, waarmee een inbraakvertraging wordt beoogd van 3 minuten.

Bn De 'normaal' toe te passen bouwkundige maatregelen, waarmee een inbraakvertraging wordt beoogd van 5 minuten. In de praktijk kan Bn vaak worden gerealiseerd door het treffen van aanvullende maatregelen op Bs.

Bz Dit zijn 'zware' bouwkundige maatregelen, waarbij de vereiste inbraakvertraging dient te zijn afgestemd op de zwaarte van het risico. Tevens dient glasafscherming dan wel glasvervanging te worden toegepast.

Elektronische maatregelen [1]

Es Het 'standaard' inbraaksignaleringssysteem met componenten SCB 1 of SCB 2 en doormelding volgens AL1 naar een Particuliere Alarm Centrale (PAC).

En Het 'normale' inbraaksignaleringssysteem met componenten volgens SCB 2 of SCB 3 en doormelding volgens AL1 naar een PAC.

Ez Het 'zware' inbraaksignaleringssysteem met componenten volgens SCB 3, doormelding volgens AL2 naar een PAC en nadere eisen voor registratie en alarmopvolging.

Compartimenteringsmaatregelen [1]

Cs 'Standaard' inbraakwerende kast of kluis volgens SKB-kwalificaties.

Cn Het 'normale' bouwkundige compartiment (dat altijd moet worden gecombineerd met E buiten het compartiment).

Cz Het 'zware' bouwkundige compartiment (dat altijd moet worden gecombineerd met E buiten het compartiment).

m Als alternatief voor C kan in bepaalde gevallen gebruik worden gemaakt van 'meeneembeperkende' maatregelen bijvoorbeeld: het doelmatig bevestigen van een computer op een bureau).

ORGANISATORISCHE MAATREGELEN

Beveiliging staat en valt met Organisatorische maatregelen (O). De Code voor informatie beveiliging geeft een goed kader om de O maatregelen in te richten en uit te werken. Uiteraard is bewustwording een belangrijk issue van de organisatorische maatregelen.

DE WAARDE VAN INFORMATIE EN DE RELATIE MET BORG

De waarde van informatie laat zich moeilijk in geld uitdrukken. Een uitgangspunt zou kunnen zijn:

Het waarborgen van de continuïteit en het minimaliseren van eventuele schades.

Op basis van deze uitgangspunten kunnen kwalitatieve waarderingen worden benoemd. Deze kwalitatieve waarderingen kunnen worden uitgedrukt in de volgende factoren:

- Herstelbaarheid
- Misbaarheid
- Betrouwbaarheid
- Belangrijkheid

Uiteindelijk willen wij dat uit deze vier kwalitatieve waarderingen risicopunten en een risicoklasse komen zodat men dit in de BORG praktijk kan gebruiken. Hoe komt nu de risicoklasse indeling tot stand zodat we de risicoklasse kunnen vaststellen. Aan één van de of een combinatie van de kwalitatieve waarderingen wordt een aantal risicopunten toegekend. De som van het puntentotaal leidt tot de indeling in één van de vier risicoklassen. Hiervoor moeten eerst de definities van de vier genoemde kwalitatieve waarderingen worden vastgesteld en afgekaderd:.

1. HERSTELBAARHEID

Is de informatie uniek en niet reproduceerbaar, wel reproduceerbaar of zelfs onmiddellijk vervangbaar?

2. MISBAARHEID

Hoe lang kunt u zich zonder bepaalde informatie redden, een paar seconden, een paar uur, enkele dagen of zelfs langer?

3. BETROUWBAARHEID

Hoe betrouwbaar moet de informatie zijn en op welk niveau?

4. BELANGRIJKHEID

Wie hebben er belang bij de informatie: voor het werk, vanwege de wettelijke bepalingen of om er misbruik van te maken.

HERSTELBAARHEID EN MISBAARHEID EN HUN RELATIE

Herstelbaarheid en Misbaarheid staan in relatie tot elkaar. Als iets herstelbaar is, maar het is niet onmisbaar, dan is dat een schade beperkende factor. In dat geval wordt de hersteltijd een belangrijke factor. Immers als iets herstelbaar is, maar het herstellen kost heel veel tijd, dan neemt de schade toe. Als iets niet herstelbaar en onmisbaar is, is de schade groot. Uitgedrukt in de bekende punten zou dit op de volgende tabel kunnen uitkomen:

	Misbaarheid						
Herstelbaarheid	**30 min**	**60 min**	**4 uur**	**8 uur**	**24 uur**	**48 uur**	**>48 uur**
Onmiddellijk vervangbaar	2	4	6	8	10	12	14
Vervangbaar	4	6	8	10	12	14	16
Uniek en wel reproduceerbaar	6	8	10	12	14	16	18
Uniek en niet reproduceerbaar	8	10	12	14	16	18	20

1 overgenomen uit Handboek Risicoklasse-indeling Deel 1

2 Artikel 14. BUITENGEWONE OMSTANDIGHEDEN Telecommunicatiewet, datum 1998

vervolg naar pagina 22

vervolg naar pagina 19

BETROUWBAARHEID

Betrouwbaarheid is ook een waardebepalingsaspect. Onder betrouwbaarheid wordt verstaan de mate van juistheid en beschikbaarheid van informatie. Voor de berekening van de risicoklasse kan dit zeer belangrijk zijn.

Bij het onderzoeken van de betrouwbaarheid moet de ICT infrastructuur worden meegenomen. Als er bijvoorbeeld in een object voor de ICT infrastructuur belangrijke apparatuur aanwezig is, dan zijn zaken zoals manipulatie, misbruik of vernieling van uw ICT infrastructuur een reël risico met name voor de beschikbaarheid.

Voor een aantal ICT dienstverleners is betrouwbaarheid en beschikbaarheid wettelijk geregeld [2] . Denk bijvoorbeeld eens aan de schadeclaims welke een telecom operator kan krijgen als het alarmnummer 112 niet bereikbaar zou zijn.

	Betrouwbaarheid			
Juistheid	**Laag**	**Middel**	**Hoog**	**Zeer hoog**
Laag	0	1	2	4
Normaal	1	2	4	6
Hoog	2	4	6	8
Zeer hoog	4	6	8	10

BELANGRIJKHEID

Bij de belangrijkheid van informatie gaat het om de vraag, wat is de attractiviteit van de desbetreffende informatie. Het mag duidelijk zijn dat informatie een grote hoeveelheid verschijningsvormen kent. Informatie kan dus een vel papier met geprinte gegevens zijn maar ook een CD-ROM, een diskette of iets dergelijks. Voor criminelen kan het wel eens makkelijker zijn om een CD-ROM of een diskette te stelen dan om een computerinbraak te plegen.

Verschijningsvormen van informatie	**punten**
CRM applicaties	2
Data met de classificatie geheim	4
Data met de classificatie openbaar	1
Data met de classificatie vertrouwelijk	3
Databases	2
Documenten met de classificatie geheim	4
Documenten met de classificatie openbaar	1
Documenten met de classificatie vertrouwelijk	3
Klanteninformatie	4
Koersgevoelige informatie	3
Log files	2
Orderinformatie	3
Personeelsinformatie	2
Privacygevoelige informatie	3
Productinformatie	1
Productieprocesinformatie	4

Uitgaande van de het feit dat men de attractiviteit van desbetreffende informatie kan indelen in een schaalverdeling tussen 1 en 4, resulteert in de volgende tabel:

DE RISICOKLASSE INDELING

Het totale aantal risicopunten bepaalt de indeling in één van de vier risicoklassen en de meest geschikte combinatie van inbraakpreventieve maatregelen. Zoals eerder aangegeven worden deze maatregelen weergegeven met de letters B, E, C en/of M en O. En hun implementatierichtlijn wordt aangeduid met standaard (s), normaal (n) of zwaar (z). Het onderstaand schema kan dan als volgt worden ingevuld:

Risicopunten	risico-klasse	Beveiligingsmaatregelen	
7 – 14	1	**Bs**	+0
15 – 24	2	**Bn of BS + Es**	+0
25 – 29	3	**Bn + En**	+0
30 en meer	4	**Maatwerk, of Bz+En of Bn + Ez**	+0

Uiteraard worden alle maatregelen altijd aangevuld met een O maatregel.

COMPARTIMENTERING ALS OPLOSSING?

Het plaatsen van de computersystemen en de benodigde netwerkapparatuur in een aparte ruimte, welke we als BORG compartiment moeten beschouwen, zou als oplossing kunnen zijn. Als we dit goed willen doen dan moeten we rekening houden met een aantal elektrotechnische zaken zoals netwerk bekabeling en de telecommunicatie infrastructuur.

Hiervoor zouden we de hierboven beschreven methodiek kunnen gebruiken. Door een compartiment conform de risicoklasse-indeling te implementeren kunnen in een aantal gevallen de kosten beheersbaar blijven.

LITERATUUR

- Overbeek, P. en Sipman, W. Informatie beveiliging, 2e druk.
- Handboek risicoklasse indeling, Nationaal Centrum voor Preventie.
- Managing Risk and Building Trust in e-business, IBM consulting Group, Daniel Keely, 1999
- Code voor informatie beveiliging, NNI, 1994

Auteur is werkzaam als Security consultant voor Vizzavi, is voorzitter van de vakgroep ICT beveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN) en is lid van het International Advisory Board van de International Foundation for Protection Officers (IFPO).