INFORMATIEBEVEILIGING

GVIB <editie 6 september 2002>

ACADEMIC SERVICE

DEEL III

BORG-regelingen en IT

Douwe de Jong en Ronald Eygendaal

«Over de auteurs» Douwe de Jong heeft als zelfstandig IT-adviseur voor het Expertisecentrum Informatiebeveiliging Nederlandse Politie invulling gegeven aan fysieke beveiliging als aanvulling op informatiebeveiliging. De artikelen zijn gebaseerd op zijn ervaringen. E-mail: douwep@planet.nl.
Ronald Eygendaal CISMP, CSS is security consultant bij Vizzavi en heeft meer dan 10 jaar ervaring in (informatie)beveiliging. Hij is voorzitter van de vakgroep ICT beveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN) en lid van de International Advisory Board van de IFPO. E-mail: protection.company@hetnet.nl

In deze artikelenserie over informatiebeveiliging en fysieke beveiliging wordt ervoor gepleit meer oog te hebben voor elkaars vakgebied, meer kennis te hebben van elkaars hulpmiddelen en meer samen te werken. Dat zal resulteren in beter op elkaar afgestemde veiligheidsmaatregelen. In dit laatste artikel ligt het accent op de pragmatische aanpak. Een benadering waarbij een set van beveiligingsmaatregelen geldt die beantwoordt aan een bepaald niveau van veiligheid en betrouwbaarheid. Voor de fysieke beveiliging zijn dat onder meer de BORG-regelingen. Wordt daarbij wel voldoende rekening gehouden met IT en de bijbehorende informatie?

Inleiding

Zowel voor informatiebeveiliging als voor fysieke beveiliging geldt dat de bedrijfsprocessen, de te beschermen belangen, centraal staan. Er is een risicoafweging nodig om te komen tot betrouwbaarheids- en veiligheidseisen als opmaat voor de te treffen beveiligingsmaatregelen. Risicoanalyse is een arbeidsintensieve bezigheid en in veel gevallen kan ook worden volstaan met quick scans.

Voor de fysieke beveiliging is het uitvoeren van quick scans en het toepassen van genormeerde producten gemeengoed; bijvoorbeeld de risicoklassenindeling voor de BORG-regelingen en beveiligingsproducten die voldoen aan SKG-normen (Stichting Kwaliteitsborging Gevelelementen).
Vanaf de introductie van de Code voor Informatiebeveiliging is bij informatiebeveiliging een omslag te zien; de Code wordt steeds vaker gebruikt bij het bepalen van een basisbeveiligingsniveau en TNO geeft Common Criteria (ISO-norm) Certificaten uit voor IT-beveiligingsproducten.

Dit artikel gaat over de BORG-regelingen; een norm voor inbraakbeveiliging voor gebouwen. Een gebouw moet voldoende weerstand bieden om bedrijfsprocessen die zich daarbinnen afspelen te beschermen, inclusief de eventueel aanwezige IT-apparatuur met bijbehorende informatie. De praktijk is echter dat IT-risico's niet altijd even goed worden ingeschat en dat de bescherming achteraf onvoldoende blijkt te zijn geweest.

Normen en regelingen

Normering en regelgeving heeft voornamelijk tot doel de efficiency van processen te verbeteren en de kwaliteit van producten te vergroten. Normalisatie is het proces waarbij op nationaal, Europees of mondiaal niveau afspraken worden gemaakt tussen belanghebbende partijen over de (technische) specificaties van een product, dienst of bedrijfsproces. Belanghebbenden kunnen zowel bedrijven als overheden of consumentenorganisaties zijn. Het document waarin de afspraak wordt vastgelegd is een norm of een richtlijn; nationale normalisatie-instellingen begeleiden het (inter)nationale normalisatieproces en leggen de gemaakte afspraken vast in normen en regelingen.

... BORG-regelingen gaan voorbij aan het belang van ICT ...

Voor alle partijen in de beveiligingsbranche neemt het Nationaal Centrum voor Preventie (NCP) een centrale plaats in als het gaat om normering en regelgeving voor fysieke beveiliging. Het NCP is het publiek-private samenwerkingsverband voor veiligheid en beveiliging in Nederland. Het stelt zich tot doel *kwaliteitshandhaving en verbetering van beveiliging en veiligheid in brede zin.*

Het NCP heeft diverse producten en certificatieregelingen ontwikkeld en in de markt gezet. Onder andere de BORG-regelingen voor woningen, winkels, showrooms, onderwijsinstellingen, (fysieke) beveiligingsbedrijven en particuliere alarmcentrales. Het *Handboek Beveiligingstechniek* is het bijbehorende standaardwerk met voorschriften, lijsten met gecertificeerde producten en teksten van de BORG-Regelingen. Het handboek is de opvolger van het *Handboek Risicoklasse-indeling.*

BORG en de risicoklassenindeling

Het NCP heeft een risicoklassenindeling ontworpen als

norm voor inbraakveiligheid van fysieke omgevingen zoals productiebedrijven, werkplaatsen, kantoren en instellingen. De risicoklassenindeling is opgenomen in het *Handboek Beveiligingstechniek* en wordt zonodig geactualiseerd naar beschikbare technieken en beveiligingsinzichten. De risicoklassenindeling is afhankelijk van de inbraakgevoeligheid van een object. Deze gevoeligheid wordt gemeten aan de hand van de volgende aspecten:

- de aard van het object (waarde voor de bedrijfsvoering);
- de ligging van het object (eenvoudig dan wel moeilijk te beveiligen); en
- de attractiviteit van aanwezige goederen (attractief voor een onbevoegde en in relatie tot de verzekerde waarde).

De drie aspecten leveren risicopunten op die worden verdeeld over de risicoklassen 1, 2, 3 en 4. De inbraakpreventieve maatregelen worden weergegeven met de letters B, E, C en/of M en O. Dit betekent respectievelijk:

B = Bouwkundige maatregelen;
E = Elektronische maatregelen;
C = Compartimenterings- en/of meeneembeperkende maatregelen;
O = Organisatorische maatregelen.

Daarnaast is er een implementatierichtlijn, die iets zegt over de 'zwaarte' van de beveiligingsmaatregelen. Met de zwaarte van een maatregel wordt bedoeld de hoeveelheid tijd die effectief nodig is om 'binnen' te komen. Bij Standaard gaat men uit van 3 minuten, bij Normaal is dit 5 minuten en bij Zwaar is het 10 minuten of meer. De implementatierichtlijn wordt aangeduid met een kleine letter:

s = standaard
n = normaal
z = zwaar.

De lettercombinaties worden gebruikt voor het weergeven van de beveiligingsmaatregelen én hun implementatierichtlijn. Tabel 1 bevat de risicoklassenindeling voor inbraakgevoeligheid bij bedrijven in het algemeen. Per klasse kan men kiezen uit een combinatie van soort en zwaarte van maatregelen. Daarnaast zijn altijd bijbehorende organisatorische maatregelen nodig.

Typering bouwkundige maatregelen:

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.

Typering elektronische maatregelen:

Es Het 'standaard' inbraaksignaleringssysteem met componenten SCB1 of SCB2 en doormelding volgens AL1 naar een Particuliere Alarm Centrale (PAC). SCBx verwijst naar een certificaatklasse x van de Stichting Certificatie Beveiligingsapparatuur.

En Het 'normale' inbraaksignaleringssysteem met componenten volgens SCB2 of SCB3 en doormelding volgens AL1 (dat wil zeggen alarmoverdracht via het openbare telefoonnet) naar een PAC.

EZ Het 'zware' inbraaksignaleringssysteem met componenten volgens SCB3, doormelding volgens AL2 (dat wil zeggen alarmoverdracht via een continu gecontroleerde transmissieweg) naar een PAC en nadere eisen voor registratie en alarmopvolging.

Typering Compartimenteringsmaatregelen:

Cs Een 'standaard' inbraakwerende kast of kluis volgens SKG-kwalificaties.

Cn Het 'normale' bouwkundige compartiment; dat moet altijd worden gecombineerd met E-maatregelen buiten het compartiment.

Cz Het 'zware' bouwkundige compartiment; dat moet altijd worden gecombineerd met E-maatregelen buiten het compartiment.

Meeneembeperkende maatregel:

Als alternatief voor C kan in bepaalde gevallen worden gebruikgemaakt van 'meeneembeperkende' maatregelen, bijvoorbeeld het doelmatig bevestigen van een computer op een bureau.

Hiervoor zijn slechts globale beschrijvingen opgenomen, de gedetailleerde uitwerkingen zijn zodanig dat duidelijk is welke (gecertificeerde) beveiligingsproducten voldoen aan de gestelde norm.

BORG-regeling en IT

Niet iedereen is even gelukkig met de risicoklassenindeling. De attractiviteitstypering komt uit de verzekeringswereld en houdt geen rekening met commerciële risico's als gevolg van

Risicoklasse	Beveiligingsmaatregelen
1	Bn of Bs + Es
2	Bn + Es of Bs + Es + Cn
3	Bz + En of Bs + En + Cn
4	Maatwerk of Bz + Ez of Bn + Ez + Cz

Tabel 1: Risicoklassenindeling inbraakgevoeligheid bedrijven

diefstal van dossiers of digitaal opgeslagen informatie. De aard van het object kent slechts een driedeling; onder de hoogste klasse vallen productiebedrijven, werkplaatsen, kantoren en instellingen. Als er sprake is van een fysieke IT-locatie zou het onderzoeksobject kunnen worden gesplitst wat leidt tot compartimentering. Dan is de risicoklasseninindeling echter niet meer van toepassing op het totale object. De feitelijke oorzaak hiervan moet worden gezocht in de methodiek van assetwaarde. Daarbij wordt uitgaan van de waarde van de geïnstalleerde systemen. Het probleem is dat er geen methodiek is om de waarde van de processen, draaiende op de geïnstalleerde systemen, te berekenen. Het is daarom van belang ook aandacht te schenken aan de IT, in het bijzonder aan de waarde van de informatie.

De waarde van informatie

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

Het waarborgen van de betrouwbaarheid en het minimaliseren van eventuele schade.

Op basis van deze uitgangspunten kunnen kwalitatieve waarderingen worden benoemd[1]. Deze waarderingen kunnen worden uitgedrukt in de volgende factoren:

- *Betrouwbaarheid;* onder te verdelen in beschikbaarheid, exclusiviteit en integriteit.
- *Misbaarheid en herstelbaarheid;* in relatie tot schadeverwachting.
- *Belangrijkheid;* in relatie tot de attractiviteitswaarde.

Door aan de verschillende waarderingen risicopunten toe te kennen en de som van het puntentotaal in te delen in één van de vier risicoklassen, zou dit kunnen worden gebruikt in de BORG-praktijk. De IT-waarderingsaspecten daarvoor worden hier verder uitgewerkt.

Betrouwbaarheid

Hoe betrouwbaar moet de informatie zijn; betrouwbaarheidseisen zijn gericht op de drie kwaliteitsaspecten van informatiebeveiliging:

- *Beschikbaarheid;* de mate waarin een informatiesysteem in bedrijf is (en dus de informatie beschikbaar is) op het moment dat de organisatie het nodig heeft.
- *Exclusiviteit;* de mate waarin de informatie juist is.
- *Integriteit;* de mate waarin de informatie is afgeschermd voor onbevoegden.

Betrouwbaarheid is een waardebepalingsaspect en zegt iets over de mate van juistheid en beschikbaarheid van informatie. Dit kan van belang zijn voor het bepalen van risicoklassen en kan volgens tabel 2 worden gekwantificeerd.

Bij het onderzoek naar de betrouwbaarheid moet ook de IT-infrastructuur worden meegenomen. Als er bijvoorbeeld belangrijke apparatuur aanwezig is dan zijn zaken zoals manipulatie, misbruik of vernieling van de IT-infrastructuur een reëel risico met name voor de beschikbaarheid.
Voor een aantal IT dienstverleners is beschikbaarheid wettelijk geregeld[2]. Denk bijvoorbeeld aan de schadeclaims die een telecomoperator kan krijgen als het alarmnummer 112 niet bereikbaar zou zijn.

Exclusiviteit, juistheid	Beschikbaarheid			
	Laag	Middel	Hoog	Zeer hoog
Laag	0	4	8	12
Normaal	4	4	8	12
Hoog	8	8	8	12
Zeer hoog	12	12	12	12

Tabel 2: Risicopunten met betrekking tot betrouwbaarheid van informatie

Herstelbaarheid, misbaarheid en hun relatie

Is de informatie uniek en niet reproduceerbaar? Wel reproduceerbaar of zelfs onmiddellijk vervangbaar? Hoe lang kan men zich zonder bepaalde informatie redden, een paar seconden, een paar uur, enkele dagen of zelfs langer? Herstelbaarheid en misbaarheid staan in relatie tot elkaar. Als iets herstelbaar is maar niet misbaar, dan is de hersteltijd een schadebeperkende 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 wordt dit weergegeven in tabel 3.

Belangrijkheid

Om het belang van informatie af te kunnen wegen gaat het om de vraag hoe erg het is dat de informatie 'op straat' komt te liggen en wat de attractiviteit is voor een buitenstaander. Het mag ook 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 gemakkelijker zijn een cd-rom of een diskette te stelen dan een computerinbraak te plegen.

Herstelbaarheid	Misbaarheid; benodigde hersteltijd			
	Kort direct	Redelijk binnen 4 uur	Lang Binnen 1 dag	2 dagen of meer
Onmiddellijk vervangbaar	1	2	4	6
Vervangbaar	2	4	6	8
Uniek en wel reproduceerbaar	4	6	8	10
Uniek en niet reproduceerbaar	6	8	10	12

Tabel 3: Risicopunten met betrekking tot herstelbaarheid en misbaarheid van informatie

Uitgaande van de het feit dat men het belang van de informatie kan indelen in een schaalverdeling tussen 1 en 12, resulteert dat bijvoorbeeld in tabel 4.

Tabel 4: Risicopunten met betrekking tot belang van informatie

Belang van informatie	punten
Commerciële informatie	10
Informatie met de classificatie geheim	12
Informatie met de classificatie vertrouwelijk	8
Klant/orderinformatie	8
Koersgevoelige informatie	10
Personeelsinformatie	8
Privacygevoelige informatie	8
Medische informatie	12

De risicoklassenindeling

Het totale aantal risicopunten van de drie invalshoeken bepaalt de indeling in één van de vier risicoklassen (zie tabel 5). Deze risicoklassenindeling kan worden bepaald naast de gangbare indeling. De hoogste risicoklasse is bepalend voor de te selecteren beveiligingsmaatregelen. Wanneer de indeling als gevolg van de waardebepaling van informatie hoger scoort dat de gangbare indeling kunnen ook extra maatregelen voor een IT-compartiment worden overwogen.

BORG-regeling voor integrale veiligheid?

In informatiebeveiligingsland bestaat nogal wat weerstand tegen de hier geschetste werkwijze, velen vinden dat de realiteit te complex is om in eenvoudige tabellen weer te geven. Maar de praktijk leert ook dat er vaak geen geld, geen tijd en vooral onvoldoende betrokkenheid is voor een gedegen risicoafweging en zolang er bij fysieke beveiliging nog nauwelijks rekening wordt gehouden met IT, is een pragmatische gulden middenweg aan te bevelen. Het mag niet zo zijn dat een bedrijf als gevolg van een calamiteit failliet gaat omdat bij het bepalen van beveiligingsmaatregelen IT-risico's niet zijn meegenomen.

De invloed van IT op BORG-regelingen verdient dan ook zeker aandacht. Op het moment dat dit artikel wordt geschreven is er een werkgroep in oprichting die gaat onderzoeken hoe bij BORG-regelingen rekening kan worden gehouden met informatiebeveiliging om wellicht te komen tot een afzonderlijke BORG-regeling voor IT-bedrijven.

... in de praktijk is er vaak geen geld, tijd en betrokkenheid voor een gedegen risicoafweging ...

Praktische tips

Ter afsluiting van deze artikelenserie enkele opmerkingen en praktische tips; in alle gevallen is de boodschap dat informatiebeveiliging en fysieke beveiliging niet op zichzelf staan maar overlappende disciplines zijn die steeds meer met elkaar te maken zullen krijgen.

- ☐ Let op, toegangsverlenings- en camerasystemen zijn soms aan het IT-netwerk gekoppeld. Bij uitval van het IT-netwerk zullen ook deze systemen niet meer werken.
- ☐ Voor iemand die informatie wil stelen kan het wel eens gemakkelijker zijn om een fysieke inbraak te plegen (toegankelijke informatiedragers!) dan een computerinbraak.
- ☐ Laat de BedrijfsHulpVerleningsorganisatie (BHV) onderdeel uitmaken van het disaster recovery plan. pag 30

Risicopunten	Risicoklasse	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**

Tabel 5: Risicoklassenindeling en implementatierichtlijnen

vereist meer kennis dan voorheen. We kunnen niet meer volstaan met een netwerkontwerp waarin op een statische wijze de boze buitenwereld wordt afgescheiden. Een nieuw architectuurdenken moet ontstaan, waarbij de beveiligingsarchitect niet alleen kijkt naar de externe gevaren, maar ook naar de aanpasbaarheid van het ontwerp bij nieuwe bedreigingen.

De belangrijkste maatregel daarin is een oude bekende: bewustwording bij de gebruikers – en met name bij hen die veel thuis werken – dat hun systemen kwetsbaar zijn indien deze aan internet zijn gekoppeld. Maar bewustwording is één ding, ernaar leven een ander. Gebruikers moeten ook de mogelijkheden krijgen aangereikt om op een goede manier te kunnen werken: anti-virussoftware en persoonlijke firewalls op hun systemen.

Een andere maatregel is om het gebruikersnetwerk – het interne netwerk waaraan de gebruikers zijn aangesloten – volledig te scheiden van de servers en centrale computers. We kunnen hier zelfs nog verder gaan en terugkeren naar de oude stervormige netwerken, waarin onderlinge koppelingen tussen gebruikers niet meer mogelijk zijn. Door op de switches elke gebruiker een afzonderlijke poort te geven en gebruik te maken van Personal vLAN's of van VPN's kan dit worden gerealiseerd. Door vervolgens de grenzen tussen de verschillende omgevingen (internet ←→ servers ←→ gebruikersnetwerken) te controleren door middel van diverse technische maatregelen, zoals firewalls, IDS, enzovoort, kan het oude en toen nog vertrouwde interne netwerk worden gecontroleerd en behandeld als de nieuwe en gevaarlijke binnenwereld.

Conclusie

Met Code Red en Nimda hebben we enkele vingeroefeningen gezien rond het nieuwe type e-wapens waarmee de digitale onderwereld van plan is te gaan aanvallen. Door deze nieuwe wapens zullen de aanvallen niet alleen meer komen vanuit internet, maar ook vanuit de interne netwerken zelf, doordat veel systemen niet alleen zijn aangesloten op de interne netwerken, maar ook (thuis) op het gevaarlijke internet en daar reeds zijn besmet.
Dit heeft gevolgen voor de architectuur van de IT-infrastructuur. We kunnen niet langer volstaan met het paradigma van de boze buitenwereld versus de veilige binnenwereld, maar zullen moeten accepteren dat ook het interne gebruikersnetwerk gevaarlijk is geworden.

<URL's-artikel>
www.incidenten.org met een uitgebreide analyse van Code Red I en ***www.grc.com*** met een analyse van een DDoS-aanval op de website van GRC.

<URL's - Favoriet>
www.sans.org, een must voor elke security specialist
www.infosyssec.com een zeer uitgebreide security portal

pag 27

Bij een evacuatie als gevolg van een niet- IT-calamiteit worden wel de IT-aspecten meegenomen.

- ☐ Informatiebeveiligingsmaatregelen en compartimentsindeling moeten op elkaar afgestemd worden.
- ☐ Beveiligingsactiviteiten die herkenbaar moeten zijn voor de medewerkers op de werkvloer kunnen gezamenlijk worden uitgevoerd. Denk daarbij aan bewustwordingsactiviteiten en veiligheidsprotocollen. Maak voor werkplekken uniforme, op elkaar afgestemde instructies als het gaat om afsluitdiscipline voor ruimten, clear desk policy voor IT-apparatuur en veiligheid in het kader van de Arbo-wet.
- ☐ Overweeg een centraal meldpunt voor alle veiligheidsincidenten: het moet voor betrokkenen uitnodigend zijn om incidenten te melden, één aanspreekpunt op een voor iedereen toegankelijke locatie, liefst naast de personeelsingang en beslist niet in een extra beveiligd gebied.

Oproep

We zijn benieuwd naar reacties en vooral naar ervaringen met overlappende activiteiten op het gebied van fysieke beveiliging en informatiebeveiliging. Wellicht kan dat resulteren in een klankbordgroep die de verschillende initiatieven kan voeden en stimuleren. Mail naar: douwep@planet.nl

<Noten>

[1] Zie ook: Paul Overbeek *Informatiebeveiliging: een praktische gids voor de bescherming van uw gegevens* (ISBN 90 72194 31 4)

[2] *Artikel* 14 Buitengewone omstandigheden, *Telecommunicatiewet, 1998*

<URL's-artikel:>
www.ncpreventie.nl de site van het NCP
www.commoncriteria.nl evaluatiefaciliteit voor IT beveiligingsproducten op basis van de Common Criteria/ISO15408
www.vbbs.nl site van de Vereniging van Bouwkundige Beveiligings Specialisten, een samenwerkingsverband van 20 bedrijven o, erkzaam op het gebied van (fysieke) beveiliging
www.politiekeurmerk.net site van het Inbraak Preventie Team Arnhem Veluwezoon
www.vvb.nu site van de Vereniging voor Veiligheid en Beveiliging