Gert Kogenhop *is operationeel manager bij Kader Group, erelid van het Business Continuity Institute en voorzitter van de BCM & CM normcommissie bij NEN.*

Samenwerken voor een optimaal resultaat

Het aantal cybersecurity-incidenten neemt eerder toe dan af. Kleine, maar ook grote, gerenommeerde organisaties worden getroffen. De afhankelijkheid van IT of ICT is enorm, eigenlijk onaanvaardbaar groot. Nagenoeg niemand heeft een alternatief, bijvoorbeeld een handmatige wijze van werken, in situaties waarbij applicaties, het netwerk of internet niet beschikbaar of bereikbaar zijn, bestanden 'verdwenen' zijn of gecompromitteerd. In ernstige gevallen leidt dit tot een crisissituatie waarbij de samenwerking tussen verschillende disciplines in de (tijdelijke crisis-) organisatie van doorslaggevend belang is bij het oplossen van het probleem, het geven van een adequate reactie en schadebeperking, zowel organisatorisch, financieel alsook met betrekking tot de reputatie.

Iedere organisatie is afhankelijk van informatietechnologie en we hebben deze situatie notabene zelf gecreëerd. Als gevolg daarvan zijn informatiebeveiliging en gegevensbescherming belangrijke elementen waaraan aandacht moet worden besteed. ICT-afhankelijkheid maakt organisaties kwetsbaar en we kunnen niet wegkijken en doen of het ons niet zal raken. ICT-uitval veroorzaakt een enorme verstoring en kan voor veel organisaties zelfs fataal zijn. Organisaties kunnen worden geconfronteerd met een crisissituatie als gevolg van een ernstige verstoring, dus Crisis Management (CM) en Business Continuity Management (BCM) zijn voorwaarden voor een goed gemanagede organisatie. In sommige landen zijn deze zelfs verplicht. Onvoorbereid zijn is niet acceptabel en *"we kijken wel als er wat gebeurt"* is onmogelijk, onverantwoordelijk en wordt zeker niet beschouwd als een 'good business practice'.

Hoe pak je dit aan?

Organisaties moeten stabiel, robuust en tegelijkertijd veerkrachtig (resilient) en wendbaar (agile) zijn. Een aantal disciplines of expertisegebieden moeten gecombineerd worden in een gezamenlijke inspanning om de toekomst van een organisatie veilig te kunnen stellen in de continu veranderende omgeving waarin deze opereert. Risk Management (RM), Information Security & Data Protection (IS & DP), BCM en CM moeten op het juiste niveau samenwerken. Het is absoluut een uitdaging om de verschillende expertisegebieden optimaal te laten samensmelten, terwijl elk gebied nog steeds in staat moet zijn onafhankelijk te werken. En wie is vervolgens de eigenaar van dit proces? Er moet aandacht worden besteed aan samenwerking, informatie-uitwisseling en het juiste niveau van (systeem)integratie. Deze gecombineerde gebieden hebben al een gemeenschappelijke doelstelling, namelijk het beschermen van de kroonjuwelen van de organisatie en het veiligstellen van de toekomst. Het koppelen van de inspanningen is een kwestie van consistentie en coördinatie door afstemming, met tal van synergiemogelijkheden. De professionals die werkzaam zijn in deze vijf expertisegebieden zullen veel effectiever en efficiënter kunnen functioneren, terwijl zij nog steeds in staat zijn om onafhankelijk te werken en zij hun onpartijdigheid kunnen behouden voor die zaken waarvoor dit gewenst en soms wettelijk vereist is.

Geselecteerde strategiën implementeren

Het verzamelen en delen van informatie tijdens een cyberincident, de samenwerking tussen het Crisis Management Team (CMT), het Cyber Security Incident Response Team (CSIRT) en het Business Continuity Management Team (BCMT), is cruciaal om de impact op de organisatie, de productlevering en de dienstverlening te kunnen minimaliseren. De benodigde middelen om geselecteerde strategieën te kunnen implementeren zijn in ieder geval: mensen, informatie en gegevens, gebouwen, werkplekken en faciliteiten, machines en materialen, ICT, transport en logistiek, financiële middelen en zeker ook partners en leveranciers. Het belang, de vorm en hoeveelheid is als vanzelfsprekend afhankelijk van het soort organisatie. In het geval van een cyberincident dient er een aantal specifieke elementen toegevoegd te worden, zonder te pretenderen compleet te zijn: vertrouwelijkheid van (persoons)gegevens, wet- en regelgeving, merk en reputatie en communicatie met stakeholders en de media.

Er zijn elementen en middelen die voor het CMT, CSIRT of BCMT team-specifiek zijn, zoals merk en reputatie en de communicatie voor het CMT, terwijl genoemde vertrouwelijkheid van (persoons)gegevens worden beheerd door het CSIRT. Middelen specifiek gerelateerd aan de bedrijfscontinuïteit zoals gebouwen, werkplekken en faciliteiten, uitrusting en verbruiksmaterialen plus transport en logistiek liggen bij het BCMT. Alle andere middelen zijn voor ieder team een vereiste, echter in de meeste gevallen met een ander doel. Dit wordt duidelijk wanneer het gaat om de informatiebehoefte. Zo is informatie over het cyberincident voor het CMT van het grootste belang om de ernst te bepalen en voor het vaststellen wat, wanneer te communiceren aan wie, rekening houdend met van toepassing zijnde wet- en regelgeving. Voor het CSIRT is informatie een vereiste voor het proces van detecteren, monitoren en adequaat reageren, daar hier hun specifieke verantwoordelijkheid ligt tijdens een cyberincident. Het BCMT heeft informatie nodig om de situatie te beoordelen en het juiste scenario uit te voeren om productlevering en dienstverlening op aanvaardbare vooraf gedefinieerde niveaus voort te kunnen zetten. Samenwerken, informatie delen en integratie zijn de sleutelwoorden en tegelijkertijd uitdagingen.

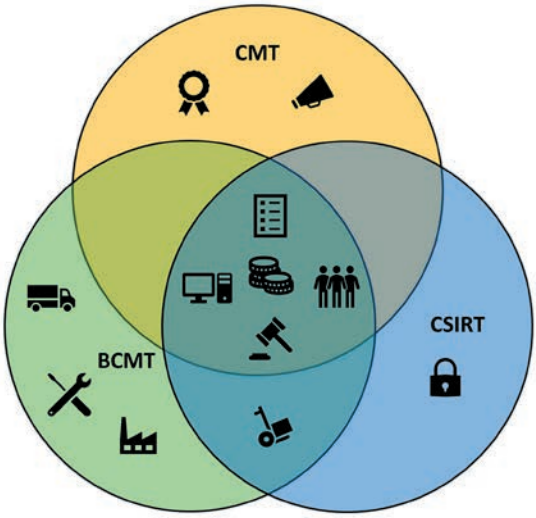
CYBER INCIDENT – SAMENWERKEN, INFORMATIE DELEN EN INTEGRATIE

Elke organisatie kent de volgende typen middelen benodigd voor het leveren van producten en diensten:

- a) mensen;
- b) informatie en gegevens;
- c) fysieke infrastructuur zoals gebouwen, werkplekken of andere faciliteiten en bijbehorende voorzieningen;
- d) uitrusting en verbruiksmaterialen;
- e) systemen voor informatie en communicatietechnologie (ICT);
- f) transport en logistiek;
- g) financiën;
- h) partners en leveranciers.

In geval van een Cyber Incident is er tevens aandacht voor de volgende zaken vereist:

- a) Vertrouwelijkheid van (persoons)gegevens;
- b) wet en regelgeving (incl. juridisch);
- c) merk en reputatie;
- d) communicatie met stakeholders en media.



Eén gezamenlijke inspanning

Voor veel organisaties is dit niet eenvoudig. Zij zijn op zoek naar richting, ondersteuning en 'best practices' om hun inspanningen te verbeteren en de organisatie verder te brengen. Het is al een enorme verbetering wanneer silo's, eilandjes en koninkrijkjes, waarin de vijf expertisegebieden zijn gevestigd, worden teruggebracht tot één gezamenlijke inspanning. Nogmaals, de professionals die werkzaam zijn in deze vijf expertisegebieden zullen veel effectiever en efficiënter kunnen functioneren, terwijl zij nog steeds in staat zijn om onafhankelijk te werken en zij hun onpartijdigheid kunnen behouden voor die zaken waarvoor dit vereist is. Een vooruitgang met perspectief.