

Adviezen op het gebied van veiligheid

BING verbreedt de scope van haar dienstverlening: van integriteit naar veiligheid en van veiligheid naar beveiliging. BING concentreert haar dienstverlening op de overheid. En de overheid heeft, behalve aan diensten op het terrein van integriteit, behoefte aan diensten op de aanpalende gebieden veiligheid en beveiliging. En: beveiliging biedt bescherming tegen een bepaald soort integriteitsbreuken. Vandaar.

Het dilemma openheid en toegankelijkheid versus veiligheid is een belangrijk issue.

De openbare weg loopt tot in het stadskantoor of gemeentehuis. Maar hoe openbaar mag de werkplek van de ambtenaar zijn? Voordat je het weet komen de risico's van de openbare weg binnen op de werkplek.

Beveiligen: organisatie en techniek

Beveiliging concentreert zich vaak op technische aspecten. Maar het belangrijkste gaat daaraan vooraf: het maken van een risicoanalyse, het voeren van een discussie hoe ver je moet gaan om bepaalde risico's te vermijden of te beperken, het ontwikkelen van een beleidsplan, het draagvlak vinden voor dat plan, het nemen van organisatorische maatregelen, het beïnvloeden van het handelen van mensen, etc. Het daaropvolgende technische deel dient vervolgens een evenwichtige schakel te zijn te midden van de andere maatregelen. De techniek kan een gebrek in de organisatie niet opheffen. En BING is sterk in het inventariseren en in het oplossen van organisatorische problemen. Vandaar.

Beveiligingsrisico-analyse

Waartegen beveiligen? Wat zijn de risico's en wat kan je er tegen doen? En wat is er al aan gedaan? Ieder vitaal belang van een overheidsorganisatie moet afdoende worden beschermd. Eerst inventariseren dus. Inventarisatie van de risico's en een inschatting van hun effect.

Bij een inventarisatie komt het naast kennis aan op ervaring en op een afstandelijke kritische blik. Werk voor een specialist. Een specialist die weet dat incidenten die door onbewust menselijk handelen worden veroorzaakt, om andere maatregelen vragen dan de incidenten die een gevolg zijn van bewust handelen. Of een gevolg zijn van technische problemen of van natuurgeweld.

De adviseurs van BING hebben ervaring in het uitvoeren van beveiligingsrisicoanalyses. Naast deze analyse kan BING met de *Quick Scan Beveiliging* snel en op hoofdlijnen een goede indruk geven van de mate waarin een organisatie risico's loopt.

Beveiligingsbeleid

Na de inventarisatie volgt het ontwikkelen van beleid: Hoe ver moet je gaan? Wat mag het kosten? In hoeverre mogen processen vertraagd worden of mag de burger het als 'onvriendelijk' ervaren? Een beleidsplan maken dus. En keuzes maken. Waar liggen de prioriteiten: personen, kritisch processen, gebouwen en inventaris of de informatie?

Het ad hoc nemen van beveiligingsmaatregelen zal nooit tot een goed resultaat leiden. Zij leiden wel tot een verspilling van middelen.

Implementatie

Hiervoor werden de eenvoudig te realiseren onderdelen besproken. Inventariseren en plannen maken: daar zijn veel mensen goed in. Maar zoals zo vaak, ook bij beveiliging komt het aan op de implementatie. Het beveiligingsbeleid dient binnen de gehele organisatie herkenbaar te zijn en een onlosmakelijk onderdeel te zijn van de werkprocessen. En wat te denken van de naleving 'in vredestand'? En wat als er een ernstig incident is?

Noodplannen

Honderd procent beveiliging is onmogelijk en onbetaalbaar. Dus staat het – statistisch gezien – vast dat er op een gegeven moment iets mis gaat. Het hebben van noodprocedures wordt voor organisaties waar relatief veel personen verblijven overigens bij wet voorgeschreven. Artikel 22 van de Arbeidsomstandighedenwet verplicht de werkgever namelijk tot het organiseren van zogeheten bedrijfshulpverlening als vervolg op de algemene verplichting tot Arbozorg. Bij bedrijfshulpverlening valt bijvoorbeeld te denken aan het verlenen van eerste hulp bij ongelukken, bestrijding van een beginnende brand, ontruiming, evacuatie en communicatie.

De adviseurs van BING zijn met deze materie bekend en kunnen hierbij met hun kennis van dienst zijn door een noodplan op te stellen of te toetsen.

Continuïteitsplanning

Na het succesvol hanteren van een noodprocedure, is de continuïteit van een organisatie nog niet gewaarborgd. De vraag die onvermijdelijk opkomt is: En hoe gaan wij morgen verder? Met het innemen van de verzekeringsuitkering is dat probleem niet opgelost.

Veel organisaties hebben daar invulling aangegeven vanuit de IT-processen, maar met een na een calamiteit weer werkend IT-systeem, is de continuïteit van de belangrijkste taken nog verre van zeker gesteld. BING heeft een methode ontwikkeld om een continuïteitsplan op te stellen voor alle niet IT-gerelateerde bedrijfsprocessen. Daarbij staan, net als bij de eerste stap van risicoanalyse, alle vitale werkprocessen centraal.

Helpdesk

Kleinere gemeenten beschikken zelden over voldoende expertise om een 'veiligheidscoördinator' aan te stellen. Maar ook bij kleinere gemeenten komen met regelmaat vraagstukken voor op dit terrein. BING stelt haar expertise beschikbaar via een abonnement op een helpdesk.

Waarom BING

BING adviseert vanuit een volstrekt onafhankelijke positie. BING verkoopt namelijk geen 'spullen' zoals beveiligingspoorten, camera's, etc. En BING biedt geen uitvoerende diensten aan zoals receptionisten of beveiligingspersoneel.

Voor meer informatie: Tom Boot, tel. 033 - 2474300.