**Methode van Risico Analyse: SPRINT**

Voor de risico analyse is gebruik gemaakt van de SPRINT-methodiek van het ISF. In interviews met het verantwoordelijke management zijn de risico’s per afdeling geïnventariseerd. Deze risico analyse is de samenvatting van de uitkomsten op basis waarvan het basisbeveiligingsniveau is vastgesteld, aangevuld met veelal afdelingsgebonden aandachtspunten, waarvoor additionele maatregelen reeds bestaan dan wel moeten worden gedefinieerd.

In het kort een toelichting op deze methode:

**3.1 Risico analyse checklist**

**Stap 1: Identificeer kritieke onderdelen van de afdeling**

In een tabel zijn de kritieke onderdelen van <PPPP> opgenomen, met een motivatie waarom deze onderdelen kritiek zijn. Onder ‘kritiek’ wordt hier verstaan een veiligheidsrisico lopend.

**Stap 2: Vul de B, I en V tabellen in**

In een tabel wordt weergegeven wat het risico is van een gebeurtenis, rekening houdend met de volgende variabelen:

* de impact van een gebeurtenis;
* de kans dat de gebeurtenis optreedt;
* de schade bij het optreden van de gebeurtenis.

Aan de impact van een gebeurtenis wordt een ‘rating’ toegekend tussen A (verwaarloosbaar risico) en E (hoog risico). De rating is in deze risico analyse al gecorrigeerd voor de reeds genomen maatregelen, waardoor het risico gereduceerd dan wel ondervangen is.

Schematisch kunnen we dit als volgt weergeven:

|  |  |  |
| --- | --- | --- |
| Rating | Ernst | **Schade (in € \* 1000)** |
| E | Bedrijfscontinuïteit in gevaar | >1.000 |
| D | Zware schade | >100 |
| C | Aanzienlijke schade | >10 |
| B | Lichte schade | >1 |
| A | Verwaarloosbaar | <1 |

**4. Vertrouwelijkheid**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gevolgen van inbreuk op vertrouwelijkheid | Rating | | | | | Opmerkingen |
| Concurrentieverlies | **A** | B | C | D | E | Niet echt van toepassing, want <PPPP> is uniek binnen de branche. Wel zijn er vergelijkbare organisaties, maar met een andere scope dan <PPPP>. Deze worden niet gezien als concurrenten. |
| Direct verlies van business | **A** | B | C | D | E | Dit is nauwelijks van toepassing. Vrijwel alle informatie is openbaar of opvraagbaar ihkv de WOB. De wel gevoelige informatie (JZ, PZ, ICT) is goed beveiligd. |
| Extern imago | A | **B** | C | D | E | Als <PPPP> erin slaagt de voorpagina van de Telegraaf of van de vakbladen te halen, dan kan dit gebruikt worden in de stemmingsvorming rondom <PPPP>. De kans hierop is echter zeer klein. |
| Extra kosten | ***A*** | B | C | D | E | Uit een inbreuk op de vertrouwelijkheid is de directe schade gezien de situatie en de maatregelen nihil. |
| Aansprakelijkheid | **A** | B | C | D | E | Gezien de positie van <PPPP> is een claim voorvloeiend uit een incident m.b.t. de vertrouwelijkheid zeer klein. In feite vormt alleen PZ hierop een uitzondering. Voorts vormen hardkopies en laptops een beperkt risico. |
| Interne moraal | **A** | B | C | D | E | Behalve incidenten bij PZ zal de interne moraal niet aangetast worden bij een inbreuk op de vertrouwelijkheid. |
| Fraude | **A** | B | C | D | E | Gezien de hiërarchische opbouw van <PPPP> lopen de bedrijfsprocessen van klant tot klant over meerdere afdelingen, zodat de pakkans bij fraude zeer groot is, als het gaat om vertrouwelijkheid. |
| Overall Rating | A | **B** | C | D | E |  |

De risico’s met betrekking tot vertrouwelijkheid zijn zeer gering. Indien de bestaande procedures worden nageleefd, valt in feite iedere inbreuk op de vertrouwelijkheid uit te leggen. Kwetsbaarheden die periodiek gemonitord moeten worden, opdat het beveiligingsniveau wordt gehandhaafd, liggen op de afdelingen:

1. PZ,
2. JZ,
3. ICT,
4. Directiesecretariaat.

**5. Integriteit**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gevolgen van inbreuk op de integriteit | Rating | | | | | Opmerkingen |
| Management beslissingen | **A** | B | C | D | E | Als de uitkomsten van onderzoeken onjuist gecommuniceerd worden, kan dit de juistheid van de beslissingen van klanten beïnvloeden. Intern zijn fiatteringsprocedures aanwezig, waardoor functiescheiding wordt geborgd. |
| Direct verlies van business | **A** | B | C | D | E | Niet van toepassing (zie volgende punten) |
| Fraude | A | B | **C** | D | E | Het frauderisico is aanzienlijk op afdeling <QQQQ>. Dit betreft met name interne medewerkers en kan via functiescheiding geregeld worden, maar het is nog niet volledig duidelijk of deze systematiek ook in bijzondere situaties op de afdeling waterdicht is. Gezien hun bevoegdheden vormen vooral FAB’ers een mogelijk risico. Voorts zijn bestanden op de centrale server benaderbaar via programma’s als Excel. Omdat er een diepgaande kennis aanwezig moet zijn van bestandsstructuren, om deze daadwerkelijk voor dit doel te manipuleren, is het risico beperkt, zeker omdat de pakkans relatief hoog is. Indien het vermoeden toeneemt, dat de continuïteit van <PPPP>niet geborgd kan worden, neemt het risico op fraude aanzienlijk toe i.v.m. afnemende loyaliteit. |
| Imago | A | B | **C** | D | E | Hoewel onderzoeken niet door <PPPP> zelf worden uitgevoerd, loopt het als opdrachtgever wel het risico op imagoschade, als het resultaat niet adequaat blijkt te zijn. Persoonlijke deskundigheid van opdrachtgevers dekt dit risico momenteel af, maar dat is geen duurzame oplossing. |
| Extra kosten | A | **B** | C | D | E | Kosten kunnen verhaald worden op de toeleveranciers van informatie. Er moet nog gecheckt worden of dit contractueel waterdicht geregeld is. Voorts kan een interpretatiefout bij <QQQQ> leiden tot herstelacties. |
| Aansprakelijkheid | A | B | **C** | D | E | Zie ook vorige punt. Indien echter <PPPP> uitgebreid aansprakelijk gesteld wordt voor een incident en <PPPP> communiceert niet adequaat, dan kan dat imagoschade opleveren, die de bedrijfscontinuïteit in gevaar brengt. Hiervoor bestaat geen communicatieplan. |
| Interne moraal | **A** | B | C | D | E | De impact van de integriteit op de interne moraal is verwaarloosbaar, gezien andere en veel sterkere prikkels. |
| Verstoring bedrijfsproces | A | B | **C** | D | E | Dit impact van dit risico is beperkt. In de meeste gevallen zal dit slechts tot dubbel werk leiden. Afdeling <QQQQ> is kwetsbaar, als door <QQQQ> zelf ontwikkelde programmatuur niet integer blijkt te zijn. Hier is de functiescheiding onvoldoende om dit te borgen, hetgeen nu gecompenseerd wordt door voldoende deskundigheid van de betrokkenen. |
| Overall Rating(is gelijk aan de hoogste rating) | A | B | **C** | D | E | Voor MB moet er een plan komen hoe in de toekomst de functiescheiding geregeld gaat worden. Er moet een communicatieplan komen om escalaties bij incidenten en calamiteiten te voorkomen. |

De risico’s met betrekking tot de integriteit liggen niet zozeer binnen <PPPP> zelf, maar omdat het in de keten manager is van het klantorder ontkoppelpunt (KOOP), zal <PPPP> bijna per definitie aangewezen worden als de schuldige bij incidenten, zelfs al is <PPPP> onschuldig. Zeker in het huidige krachtenveld is dit voor <PPPP> een feit, waarmee het moet leren leven. Voorkomen van imagoschade in de vorm van goede procedures in combinatie met een adequaat communicatieplan is cruciaal, want de kosten van het aftimmeren van op zich kleine risico’s bedragen een veelvoud van de eventuele kosten van imagoschade. Bovendien zou dit een investering vergen, waardoor de positie van <PPPP> naar de klanten verder wordt verzwakt.

**6. Beschikbaarheid**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Gevolgen van inbreuk op beschikbaarheid | Bus. Impact Rating | | | | | Opmerkingen |
| 1u | 1dg | 3dg | 1wk | 1m |
| Management beslissingen |  |  |  | X |  | Managementbeslissingen zijn meestal niet tijdkritisch. Gezien de maximale uitvaltijd van de ICT en thuiswerkplekken is er een verwaarloosbaar risico. |
| Direct verlies van business |  |  |  |  |  | Niet van toepassing als er een BCP is. |
| Extern imago |  |  |  | X |  | Mits er een BCP met een communicatieplan bestaat, is er een verwaarloosbaar risico. |
| Extra kosten |  | X |  |  |  | Dit betreft alleen het niet productief zijn van het personeel en mogelijk renteverlies bij <RRRR>. |
| Aansprakelijkheid |  |  |  |  |  | Niet van toepassing. <PPPP> sluit geen contracten met harde deadlines. |
| Herstelwerkzaamheden |  |  |  | X |  | Alleen in geval van calamiteiten (zie BCP). |
| Verstoring bedrijfsproces |  |  |  | X |  | De belangrijkste bedrijfsprocessen kunnen vanaf een externe werkplek gecontinueerd worden. Na een week wordt het ontbreken van dossiers en communicatie een probleem. |
| Interne moraal |  |  |  | X |  | Zie vorige punt |
| Fraude |  |  | X |  |  | Omdat transacties handmatig afgehandeld worden, is controle minder goed mogelijk. Dit mag maximaal 3 dagen stil liggen. |

Gezien het uitwijkplan is het niet beschikbaar zijn van de ICT geen ernstige dreiging. Wel dient er een BCP te komen om te borgen, dat <PPPP> snel kan communiceren en binnen een week weer kan functioneren.

**7. Conclusies**

Gelet op de uitgangspunten gedefinieerd in het informatiebeveiligingsbeleid, de gegevensclassificatie en de genomen maatregelen doen we de volgende aanbevelingen:

* Een baseline voor informatiebeveiliging geldend voor alle afdelingen, die voldoet aan ISO 17799 en waardoor het nu adequate beveiligingsniveau eenvoudig bewaakt kan worden.
* Vastlegging aanvullende maatregelen voor afdeling <QQQQ> om te voldoen aan de normen van externe toezichthouders. Op zich zijn deze (grotendeels) beschikbaar.
* Een tweejaarlijkse toetsing op de handhaving van de maatregelen met betrekking tot de vertrouwelijkheid op de afdelingen PZ, JZ, ICT en het Directiesecretariaat.
* Het onder beheer brengen van de laptops en USB-sticks van de buitendienst. Dit betreft zowel de apparatuur als de data.
* Functiescheiding bij <QQQQ> met betrekking tot ontwikkelen en onderhouden van applicaties.
* Auditing van testresultaten op binnen <PPPP> ontwikkelde of gewijzigde programmatuur. Dit geldt met name voor applicaties, die buiten de afdeling Automatisering ontwikkeld of onderhouden worden.
* Heldere communicatie over de rol van <PPPP> naar klanten, zodat het niet onterecht slachtoffer wordt van incidenten, die buiten zijn invloedssfeer liggen.
* Het uitwijkplan dient tweejaarlijks getest te worden.  
  Het BCP dient voltooid te worden inclusief bijlagen (communicatieplan).
* Jaarlijks moet beoordeeld worden of het uitwijkplan en het BCP aanpassingen behoeven vanwege investerings- of wijzigingsvoorstellen.
* Acceptatie van het beperkte risico dat bestanden op de centrale server benaderbaar zijn via Excel.
* Gezien de dreiging voor de bedrijfscontinuïteit is het niet onaannemelijk, dat veel expertise <PPPP> in de komende jaren gaat verlaten, waardoor een negatieve spiraal ontstaat en de integriteit van de informatievoorziening onder druk komt te staan. We gaan op dit issue als beveiligingsissue niet verder in.
* Acceptatie van de genoemde risico’s in deze analyse door de directie.

Het spreekt vanzelf, dat niet ieder risico is afgedekt en iedere schade kan worden voorkomen. Ingeschat wordt echter dat met deze aanbevelingen bedrijfseconomisch een optimum bereikt wordt op een niveau dat minimaal marktconform is en waarmee ook voldaan wordt aan ISO 17799.