Advies informatiebeveiligings analyse HvA

Wouter Borremans - 0461911 - v1.1

1 Juni 2005

1 Inleiding

Dit document is geschreven met als doel om de Hogeschool van Amsterdam[5] (HvA) te voorzien van een advies omtrent de methode voor haar informatie beveiligingsbeleid.

Als eerste (2) zal de HvA als organisatie worden besproken. Vervolgens worden de soorten aanwezige informatie (3) besproken, hierna zal worden ingegaan op de mate van afhankelijkheid van deze informatie (3.1). Ten slotte zal worden ingegaan op de soorten risico analyse (4) en het advies (5) over de te gebruiken analyse methode.

Wouter Borremans, Juni 2005

2 Organisatorische kenmerken

De Hogeschool van Amsterdam kenmerkt zich als een *non profit* organisatie wat impliceert dat deze geen winst oogkenmerk heeft. De HvA biedt de student hoogwaardig praktijk gericht onderwijs met als doel voldoende kennis op te bouwen om in het bedrijfsleven goed te kunnen presteren. Dit heeft direct gevolg op de besteding van budgetten, deze worden vaak door het Rijk ter beschikking gesteld en zijn dus vaak gelimiteerd. Aangezien een ICT afdeling een van de grootste kostenposten is binnen een organisatie is het zaak met grote zorg de taakspecificering van personeel en inzet van infrastructuur te documenteren om zo een grote mate van efficiëntie te bereiken.

3 Aanwezige informatie

Binnen de HvA zijn een aantal soorten gegevens te onderscheiden te weten;

- Medewerkers gegevens
  - Persoonlijke documenten
  - Adresgegevens
  - Mail
- Student gegevens
  - Persoonlijke documenten
  - Adresgegevens
  - Mail
  - Project data (Blackboard e.d.)
- Website gegevens
  - Mededelingen
  - Vak pagina's
  - Student homepages
- Cijferadministratie
- Salarisadministratie
- Lesroosters

Niet alle gegevens dienen als privacy gevoelig te worden aangeduid, een voorbeeld hiervan is de administratie van de lesroosters. Op alle andere soorten informatie dient in acht te worden genomen dat deze informatie niet publiekelijk mag worden gemaakt. Helaas is recentelijk[6] nog gebleken hoe gaten in een beveiligingsbeleid kunnen leiden tot openbaring van (prive) gegevens van studenten. Dit is een uiterst kwalijke zaak en stelt de ICT beheer organisatie in de verlegenheid. Er zijn verschillende mogelijkheden om dit soort incidenten te voorkomen. (Denk hierbij aan regelmatige scans e.d.). Gegevens dienen te worden geclassificeerd naar privacy gevoeligheid om zo een juist beveiligingsbeleid en de daarbij horende procedures op te stellen.

3.1 Belang van de informatie

Het belang van informatie wordt vaak onderschat. Er is geen bedrijf te vinden welke opereert zonder informatie. Dit geldt ook voor de HvA. Als voorbeeld zou bijvoorbeeld gesteld kunnen worden dat studenten 'geen' les kunnen krijgen door het ontbreken van een lesrooster, de administratie niet kan werken zonder cijfer- en studentgegevens etc. Informatie en de daar bijbehorende beveiliging is dus van groot belang, dit moet worden gekarakteriseerd door het waarborgen van informatie:

- Vertrouwelijkheid

  Alleen diegenen die direct belang hebben bij de informatie mogen de informatie raadplegen. Het is dus ook zaak dat deze niet worden doorgegeven aan derden. Er zijn hiervoor verschillende regels, denk aan de wet bescherming persoonsgegevens.

- Integriteit
  Omvat de correctheid en volledigheid van opgeslagen informatie.
- **Beschikbaarheid**
  Omvat de garantie dat gebruikers op afgebakende (kantooruren) binnen een SLA afgesproken tijd toegang te kunnen bieden tot gegevens en systemen. (Een van de belangrijkste aspecten van informatiebeveiliging)

Informatiebeveiliging hangt direct samen met de interactie met mensen, processen, technische componenten en ondersteunde applicaties. Het gewenste beveiligings niveau is dus sterk afhankelijk van de bedrijfscultuur en de reeds aanwezige bedrijfsprocessen. Het heeft geen zin om het beveiligings beleid zo strak te implementeren dat het mensen belemmerd in hun werk.

4 Soorten risicoanalyse

In deze sectie zullen de risico analyse methoden *kwalitatieve risicoanalyse, kwantitatieve risicoanalyse, quick scan* en *baseline checklist* worden toegelicht. Ter verduidelijking zal eerst worden ingegaan op wat een risico nu daadwerkelijk inhoud;

```
risico (het, de ~ (m.), ~'s)
  1 gevaar voor schade of verlies
```

Voor een organisatie is het van groot belang om het risico van het verstoren van de bedrijfsgang in kaart te brengen. Dit kan middels een risico analyse. Door het uitvoeren van een risico analyse kan er worden gezocht naar een manier om bijvoorbeeld de informatie voorziening optimaal te beveiligen. Vaak gaan de maatregelen om het risico te voorkomen gepaard met relatief grote investeringen, het is dus zaak om een goede balans te vinden tussen de kosten en de baten. Aangezien de financiële impact van een bedreiging of risico voor een bedrijf van groot belang is zijn er verschillende methoden om dit kwantificeerbaar te maken. De grootte van het risico is dan gelijk aan de te verwachten schade, maal de kans dat de schade optreedt. De verhouding tussen de schade verwachting en de kosten van de daarvoor te nemen maatregelen worden dikwijls weergegeven in een grafiek. Een voorbeeld van zo'n grafiek is te vinden in sectie (6.1)

Een vaak vergeten aspect van een specifiek risico of bedreiging is de indirecte schade ervan. Denk hierbij aan de verstoring van gerelateerde bedrijfsprocessen of nasleep van incidenten bij bijvoorbeeld verzekeringsmaatschappijen of ministerie van Justitie.

Risico's kunnen worden beperkt door effectief en efficiënt maatregelen te nemen en ook daadwerkelijk te implementeren. Het is ten zeerste aan te raden om dit op basis te doen van een risico analyse. Na de implementatie van de

maatregelen is het zaak deze steeds kritisch te bekijken op het functioneren. Zeker als bijvoorbeeld systemen gekoppeld zijn aan de buitenwereld is het zaak om nieuwe bedreigingen constant te blijven analyseren.

4.1 Kwalitatieve Risicoanalyse

Een kwalitatieve risicoanalyse is een analyse die niet in getallen wordt uitgedrukt. Typerend voor deze analyse is dat de onderlinge verhoudingen worden samengesteld uit klassen van bedreigingen. Deze klassen worden door een grafiek tegen elkaar afgezet. Dit gebeurd in overleg met de betrokken in een organisatie, bijvoorbeeld het management. Aan de hand van de grafiek kan er een analyse worden gemaakt welke risico's het bedrijf of management wil overkomen. (Zie bijlage in sectie (6.2)).

De kwalitatieve risicoanalyse is een zeer effectieve methode om op een reeële, (ook niet financiëele) manier de risico's in beeld te brengen.

Een kwalitatieve risicoanalyse bestaat uit:

- **Afhankelijkheidsanalyse**
  Deze analyse beschrijft het belang van een informatiesysteem voor bepaalde bedrijfsprocessen die door het onder de loep genomen systeem worden ondersteund.
  Resultaat: Lijst met betrouwbaarheidseisen voor een informatiesysteem.
- **Configuratieanalyse**
  Deze analyse bepaalt de afhankelijkheden en objecten van informatiesystemen. Tevens worden de eigenschappen van elk object ook geregistreerd.
  Resultaat: Overzicht van objecten en hun relatie.
- **Kwetsbaarheidsanalyse**
  Deze analyse omvat het onderzoek naar de kwetsbaarheid van ieder object in hoeverre deze voor bedreigingen een rol spelen. Binnen deze analyse wordt ook vastgesteld onder welke mate van beveiliging deze optimaal kunnen functioneren.
  Resultaat: Overzicht van objecten, de mogelijke bedreigingen en de mate van beveiliging die nodig is.
- **Maatregelenanalyse**
  Deze analyse omvat de maatregelen die nodig zijn om informatiesystemen op een dergelijke manier te beschermen tegen bedreigingen zodat de risico's die overblijven acceptabel en niet dreigend zijn voor een organisatie.
  Resultaat: Aanbeveling van maatregelen die geïmplementeerd kunnen worden.

Een risicoanalyse is vaak van toepassing op een informatiesysteem en heeft als uitgangspunt het beveiligingsbeleid te auditen. Er zijn een drietal inzichten waarop een organisatie bekeken kan worden; *risiconeutraal* waarbij de

kosten van de beveiliging in balans zijn met de potentiële risico's. Indien een organisatie grote risico's aanvaard dan wordt deze *risicodragend* genoemd. Als laatste wordt een organisatie *risicomijdend* genoemd indien deze relatief gezien weinig risico's wil lopen.

Het maken van een kwalitatieve risico analyse geeft een goed inzicht in de huidige staat van het beveiligingsbeleid van een organisatie. Er kan geen standaard vragenlijst worden gebruikt, dit maakt de analyse goed toepasbaar voor elke organisatie. De analyse is echter wel zeer tijdrovend omdat elk specifiek aspect van een organisatie goed onder de loep moet worden genomen. Tevens zijn er ook verborgen kosten in de zin van het inzetten van personeel om de analyse uit te voeren, dit kan zeer kostbaar zijn.

4.2 Kwantitatieve Risicoanalyse

De meest uitgebreide vorm van een risicoanalyse. In deze vorm worden alle risico's uitgedrukt in meetbare criteria zoals bijvoorbeeld een financiëel overzicht. Het is van essentiëel belang dat van alle objecten duidelijk is wat de kans op schade daadwerkelijk is. In de praktijk blijkt dit vaak nog moeilijk en maakt deze methode alleen in specifieke gevallen geschikt voor gebruik. De kwantitatieve risico analyse wordt vaak als aanvulling gebruikt op de kwalitatieve risicoanalyse.

Om het risico te berekenen kan de volgende formule worden toegepast:

```
R = K * S (Risico = Kans * Schade)
```

Het nadeel van de kwantitatieve risicoanalyse is dat erg moeilijk blijkt om ook daadwerkelijk de kansen te bepalen, vaak wordt dan ook uitgegaan van schattingen.

4.3 Quick scan

De quickscan bestaat uit een vragenlijst gebaseerd op een door een in het bedrijfsleven samengestelde norm. Binnen deze norm wordt rekening gehouden met bedrijfs specifieke situaties. De analyse gaat uit van een in het bedrijfsleven aanvaardbare normen. Het resultaat van de quickscan is vaak een aanbeveling van beveiligingsmaatregelen die genomen moeten worden om oneffenheden weg te werken binnen een organisatie.

Het is raadzaam de scan na verloop van tijd weer te doen om te zien of er significant verbetering is te meten binnen de organisatie. Een van de belangrijkste voordelen van een quick scan is de reflectie op de vastgestelde normen binnen het bedrijfsleven. Op deze manier kan er binnen een redelijk korte tijd een analyse worden gemaakt welke de bewustwording stimuleert over het nadenken van beveiliging.

Het nadeel van een quickscan is echter dat de analyse alleen volgens een externe norm worden uitgevoerd. Hierdoor kunnen specifieke (essentiële) bedrijfsdetails over het hoofd worden gezien. In de ICT sector veranderd alles snel, de quickscan kan om deze rede dan ook vaak snel verouderd raken.

4.4 Baseline checklist

De baseline checklist kenmerkt zich als een analyse methode welke werkt aan de hand van een standaard checklist. De analyse kan snel worden uitgevoerd. Er zijn vele soorten checklists beschikbaar welke door verschillende organisaties zijn uitgegeven. De checklists gaan uit van een basisniveau van beveiliging welke *security baseline* wordt genoemd. De security baseline is een stelsel van elementaire beveiligingsmaatregelen die een beveiligingsniveau van een organisatie representeren.

De standaard vragenlijsten van een baseline checklist kunnen worden aangepast naar de specifieke beveiligingsbehoefte van een organisatie. (dit gebeurd alleen op de meest belangrijke bedrijfs(kritische) processen die typerend zijn voor een organisatie. Vaak wordt op basis van een normen een checklist opgebouwd, hierbij speelt het Nederlands Normalisatie Instituut[2] (NNI) een belangrijke rol. Het NNI heeft de 'Code voor Informatiebeveiliging' opgesteld welke een goede basis biedt voor de op te stellen checklist.

De baseline checklist is beschreven op een bij voorkeur niet technisch afhankelijke wijze. Hierdoor wordt een bruikbaar abstractieniveau bereikt welke de te nemen maatregelen goed in kaart brengt.

Het voordeel van het afnemen van een baseline checklist is dat het een goed inzicht geeft in de beveiligingsstatus van de huidige infrastructuur, daarbij stimuleert het het nadenken over de beveiliging wat vaak resulteert in de bewustwording van de lopende processen binnen de organisatie. De baseline checklist geeft bovendien een maatstaaf aan voor een basisniveau van beveiliging. Het nadeel van de baseline checklist is echter dat mensen met een niet positieve bedoeling snel inzicht kunnen krijgen in de staat van het beveiligingsniveau met alle gevolgen van dien...

Door de standaarden waar de baseline checklist op is gebaseerd kan er grote weerstand ontstaan vanuit een organisatie. Een baseline checklist moet dus worden aangepast op de bedrijfscultuur.

5 Advies

In deze sectie zal ik concluderend een advies uitbrengen op basis van de informatie beschreven in dit artikel.

Gezien de aanwezige documentatie[7][8][9] kan er gesteld worden dat er voldoende inzicht is in de huidige status en onvolkomenheden binnen de HvA ICT beheeromgeving. Uit de documentatie blijkt dat er een aantal ernstige zwakke plekken in de ICT infrastructuur zitten, deze zijn middels een quick scan naar voren gekomen. Niet alle geconstateerde zwakheden zullen relevant zijn voor de beschikbaarheid en integriteit van de IT infrastructuur van de HvA. De scan die is uitgevoerd is namelijk niet toegespitst op de bedrijfs specifieke situatie van de HvA organisatie. Wellicht niet relevante systemen zoals laptops en andere (student) systemen kunnen door de scan als zwakke plek zijn aangeduid terwijl deze niet direct invloed hebben op de bedrijfsprocessen. Er kunnen hierdoor zogenoemde "false positives" ontstaan die op papier zeer ernstig lijken maar in de praktijk wellicht nauwelijks aanmerkbaar zouden kunnen zijn.

De quickscan biedt zoals hierboven beschreven niet het goede resultaat op, deze is op een aantal punten te beperkt. Ik zou dan ook willen adviseren om een *kwalitatieve* risicoanalyse uit te voeren. Deze vorm risicoanalyse is naar mijn mening de beste met als redenen:

- Door nauwe samenwerking met het management bij het opstellen van bedreigingsklassen onstaat er een goed inzicht in de te analyseren bedrijfsprocessen
- De kwalitatieve risicoanalyse levert een duidelijk beeld over reeële bedreigingen van de gehele organisatie. Het management kan op basis hiervan een beslissing nemen waar de knelpunten liggen en hoe deze opgelost dienen te worden.
- Ook niet financiële risico's kunnen relatief eenvoudig in beeld worden gebracht.
- Door het gedetailleerde beeld wat de kwalitatieve risicoanalyse oplevert is het mogelijk deze voor langere termijn te gebruiken als richtlijn voor de waarborging van de beschikbaarheid en integriteit van de ICT infrastructuur.
- Het resultaat van kwalitatieve risico analyse is zeer bruikbaar voor een organisatie aangezien er een direct bruikbaar advies uitgehaald kan worden.

Tenslotte zou ik willen aanraden de analyse te laten uitvoeren door een externe partij, dit waarborgt zorgvuldigheid en objectiviteit. Aan het uitbesteden van een risicoanalyse zijn wel hoge kosten verbonden. Ik ben echter van mening dat het belang van de ICT binnen de HvA dermate groot is dat de organisatie hier op langere termijn alleen maar profijt van zal hebben.

Referenties

[1] Risico en risicoanalyse, Dirksen http://www.dirksen.nl/paginas/proeflessen/ISF/604-02.1.pdf

[2] Nederlands Normalisatie Instituut, www.nni.nl/

[3] Baseline checklist voorbeeld, Aircraft certification Service, http://www.cessna.org/public/saib/docs/saib-ce-03-52.pdf

[4] Windows 2000 Server Baseline Security Checklist, http://www.microsoft.com/technet/archive/security/chklist/w2ksvrcl.mspx

[5] Hogeschool van Amsterdam, http://www.hva.nl

[6] "Adresgegevens 1758 HvA-studenten op straat", http://frontpage.fok.nl/nieuws/49298?highlight=hva

[7] Projectplan informatiebeveiliging, K. Feuerstein (Hogeschool van Amsterdam)

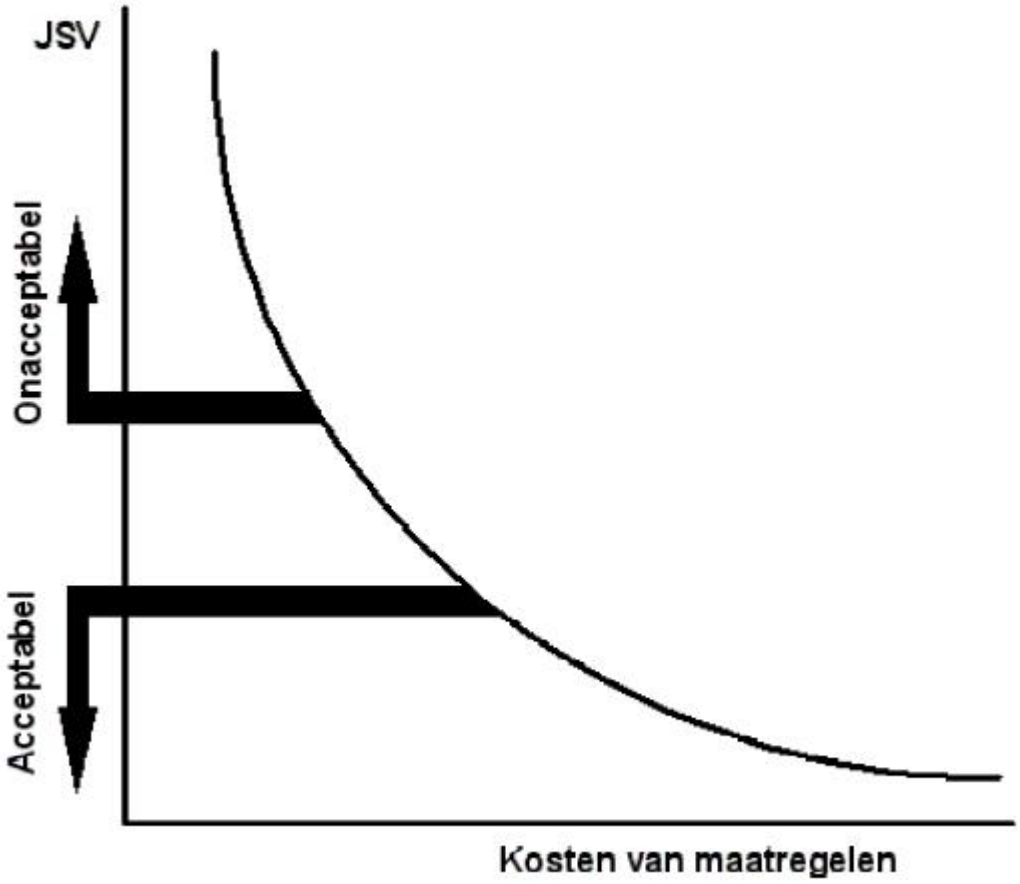
[8] Het informatiebeveiligingsbeleid Hogeschool van Amsterdam, K. Feuerstein (Hogeschool van Amsterdam)

[9] Advies met betrekking tot Risk Audit KPMG, K. Feuerstein (Hogeschool van Amsterdam)

6 Bijlagen

In deze sectie zullen bijlagen te vinden zijn met betrekking tot dit document.

6.1 Relatie tussen schadeverwachting en kosten van maatregelen



6.2 Kwalitatieve risicoanalyse