Risicoanalyse of security baselines?

Prof. dr. R. von Solms

Door de opkomst van security baselines beschikken organisaties tegenwoordig over hulpmiddelen om effectief een stelsel van maatregelen te kunnen implementeren. Als voor bepaalde bedrijfsonderdelen een hoger beveiligingsniveau noodzakelijk is, kan een risicoanalyse voor die specifieke onderdelen worden uitgevoerd. De behoefte aan een verdere risicoanalyse zal afnemen naarmate security baselines zich verder ontwikkelen. Zal er ooit een situatie ontstaan waarbij security baselines zo veelomvattend zijn dat er geen behoefte meer bestaat aan verdere risicoanalyses?

Inleiding

Van oudsher is risicoanalyse de belangrijkste techniek om risico's binnen de verschillende bedrijfsonderdelen van een organisatie te identificeren en de waarde ervan vast te stellen. Op basis van deze waardering worden doorgaans specifieke beveiligingsmaatregelen voorgesteld om de verschillende bedrijfsonderdelen afdoende te beveiligen. Helaas is deze techniek tamelijk gecompliceerd, kostbaar en arbeidsintensief. Het gevolg is dat veel organisaties de risicoanalyse omzeilen, weinig tot niets ondernemen en beveiligingsmaatregelen ad hoc implementeren. Hierdoor ontstaat een ander risico, namelijk dat kritische bedrijfsonderdelen onvoldoende beschermd zijn, terwijl minder gevoelige omgevingen te zwaar worden beveiligd.

Volgens een onderzoek naar schendingen op het gebied van informatiebeveiliging ([NCC96]) voeren de meeste organisaties in het midden- en kleinbedrijf geen risicoanalyse uit. Hiervoor zijn twee redenen aan te voeren. Ten eerste beschikken de meeste organisaties in het MKB veelal niet over de vereiste expertise om een goede risicoanalyse uit te voeren, terwijl ze zich in financieel opzicht geen consultant kunnen permitteren. Ten tweede is het besef van de noodzaak tot informatiebeveiliging bij het MKB doorgaans laag.

Een recente ontwikkeling is het gebruik van security baselines. Bij deze benadering wordt meestal een stelsel van maatregelen geïmplementeerd dat aan zekere minimumeisen voldoet. Op die manier kan een organisatie een acceptabel beveiligingsniveau verkrijgen, zonder dat een kostbare risicoanalyse behoeft te worden uitgevoerd. Het resulterende beveiligingsniveau zou onder normale omstandigheden afdoende moeten zijn. Het spreekt voor zich dat dit geen ideale oplossing is. Toch is een baselinebenadering te verkiezen boven een ad-hocbenadering of het achterwege laten van de noodzakelijke maatregelen.

De vraag die in dit artikel zal worden behandeld, is in hoeverre risicoanalyse grotendeels of misschien zelfs geheel kan worden vervangen door een intelligente toepassing van verschillende security baselines.

De risicoanalysebenadering

De traditionele risicoanalyse is gebaseerd op een duidelijk omlijnde methodologie, die verschillende verschijningsvormen kent (zie bijvoorbeeld [ISO96]). In principe kent deze methodologie een aantal duidelijk onderscheiden stappen. Allereerst wordt een grens gedefinieerd om de analyse af te bakenen. Daarna worden alle activa geïdentificeerd en gegroepeerd naar hun fysieke locatie. Vervolgens worden alle mogelijke bedreigingen en zwakke punten geïdentificeerd. Voor elk van deze bedreigingen wordt een inschatting gemaakt van de kans dat deze zich voordoet, alsmede van de mogelijke impact ervan bij het verlies van ieder activum. Op basis van deze schattingen worden risicowaarden berekend en van hoog naar laag geordend. Vervolgens kunnen beveiligingsmaatregelen worden aanbevolen op basis van de risicowaarde en de daarmee samenhangende kosten. Nu kunnen de 'beste' beveiligingsmaatregelen worden uitgekozen om tot de meest rendabele oplossing te komen. Teneinde het meest effectieve stelsel van beveiligingsmaatregelen vast te stellen, wordt een complete analyse uitgevoerd. Hiermee worden de verschillende risicogebieden geïdentificeerd en wordt de prioriteit ten aanzien van het mitigeren ervan bepaald, waarna beveiligingsmaatregelen kunnen worden gedefinieerd om deze risico's op een beheersbaar niveau te brengen.

Risicoanalyse is een zeer complex, kostbaar en arbeidsintensief proces. Het belangrijkste doel van een risicoanalyse is, na het inventariseren van de risico's, het definiëren van zodanige beveiligingsmaatregelen dat een aanvaardbaar niveau van informatiebeveiliging binnen de organisatie kan worden bereikt. Als een organisatie in staat is deze beveiligingsmaatregelen met behulp van een andere techniek te identificeren, hoeft er in het geheel geen risicoanalyse te worden uitgevoerd.

De security-baselinebenadering

De security-baselinebenadering is een al lang bestaand concept dat de laatste tijd flink terrein heeft gewonnen. Baselines kunnen worden gezien in het licht van een bottom-upbenadering, waarbij een stelsel algemeen geldende beveiligingsmaatregelen wordt gedefinieerd voor de 'gemiddelde' organisatie of het 'gemiddelde' bedrijfsonderdeel, onder normale omstandigheden. Door het implementeren van deze security baselines kan een organisatie er zeker van zijn dat de meest voorkomende en ernstige risico's onder normale, algemeen geldende omstandigheden voldoende zijn afgedekt. Benadrukt moet worden dat de doelstelling van security baselines het bieden van een minimumbeveiligingsniveau is.
Een probleem dat zich voordoet bij het in kaart brengen van security baselines is het ontbreken van richtlijnen voor het bepalen van de beveiligingsmaatregelen die op een specifieke organisatie of op specifieke bedrijfsonderdelen van toepassing zijn. Een set security baselines bestrijkt de totale omgeving van het informatiesysteem: van fysieke beveiliging tot personeelsbeveiliging en logische toegangsbeveiliging.

Het is goed denkbaar dat een deel van deze beveiligingsmaatregelen bij een bepaalde organisatie niet kan worden toegepast of behoeft te worden toegepast, bijvoorbeeld omdat die organisatie op specifieke gebieden niet actief is. Stel bijvoorbeeld dat een organisatie niet toestaat dat derden toegang hebben tot het netwerk, dan kunnen de betreffende beveiligingsmaatregelen verder worden genegeerd.

Een inventarisatie van baselines leidt niet tot duidelijke en definitieve richtlijnen over de wijze waarop uit het stelsel van beveiligingsmaatregelen juist die maatregelen kunnen worden gekozen die voor het bereiken van een acceptabel beveiligingsniveau noodzakelijk zijn. Dit brengt zekere risico's met zich mee. Een organisatie kan hierdoor besluiten bepaalde beveiligingsmaatregelen te negeren, terwijl zulke maatregelen wel degelijk (in samenhang met andere) noodzakelijk zijn.

Organisaties hadden vroeger geen echt goed alternatief voor het uitvoeren van een risicoanalyse. Wie geen risicoanalyse uitvoerde, kon in feite geen onderbouwde aanbeveling voor het implementeren van specifieke beveiligingsmaatregelen doen. Security baselines bieden dit alternatief wel. De baseline kan worden gebruikt voor het identificeren van beveiligingsmaatregelen die de meeste risico's in de meeste gevallen afdoende afdekken.

Risicoanalyse tegenover security baselines

Risicoanalyse is gebaseerd op een in mathematisch opzicht zeer degelijke methodiek. De uitkomst van een gedetailleerde risicoanalyse is het resultaat van een zeer nauwkeurig proces. Niettegenstaande de nauwkeurigheid van de methodiek worden tijdens een risicoanalyse echter veel subjectieve beslissingen genomen. Zo moet bijvoorbeeld worden bepaald of een bedreiging klein, middelgroot of ernstig is, of wordt er een schaal van één tot vijf gebruikt om de mogelijke impact van een bedreiging op een activum of een groep activa te bepalen. Ook al is de risicoanalysemethodiek zeer nauwkeurig, er kunnen vanwege eventuele subjectieve inputbeslissingen tijdens het proces toch vraagtekens worden gezet bij de accuraatheid van de resultaten.

Hierdoor twijfelen veel schrijvers aan de betrouwbaarheid van een risicoanalyse. Risicoanalyse is bijvoorbeeld ([Jaco96]):
* eentonig: er moeten veel besluiten worden genomen en er moeten veel gegevens worden verzameld;
* verdacht: critici beweren dat resultaten 'subjectief' zijn;
* inconsistent: resultaten kunnen niet altijd worden gereproduceerd;
* zinloos: managers negeren de resultaten;
* kortom: pijnlijk.

Aan de andere kant zijn de meeste security baselines die vandaag de dag beschikbaar zijn, gebaseerd op een risicoanalyse die voor een generieke omgeving is uitgevoerd of op een algemene consensus die tussen een aantal organisaties is bereikt. De introductie van een beveiligingsbaseline biedt dus niets meer dan een minimale bescherming onder zeer algemene omstandigheden. Security baselines en risicoanalyse kunnen elkaar onder bepaalde omstandigheden aanvullen. Indien een organisatie die een reeks security baselines introduceert, een specifieke bedreiging of een mogelijk abnormaal grote impact vaststelt wanneer bepaalde risico's zich daadwerkelijk voordoen, dan is het zeer zeker aan te raden een risicoanalyse voor die bedrijfsonderdelen uit te voeren om zich ervan te verzekeren dat deze risico's op de juiste wijze worden vastgesteld en om stringentere beveiligingsmaatregelen te implementeren teneinde afdoende bescherming van deze risicodragende gebieden te bieden.

> Security baselines en risicoanalyse kunnen elkaar onder bepaalde omstandigheden aanvullen.

Zoals we hierboven hebben gezien, bieden security baselines een minimaal beschermingsniveau. Om meer bescherming te bieden aan bepaalde onderdelen met een hoog risico of om zich ervan te verzekeren dat sommige unieke situaties worden gedekt, wordt aanbevolen een risicoanalyse uit te voeren teneinde dekking te bieden aan buitengewone situaties die niet door de baseline-beveiligingsmaatregelen worden afgedekt. Het moge duidelijk zijn dat als security baselines steeds meer dekking gaan bieden aan (voorheen unieke) situaties en/of bepaalde risicodragende bedrijfsonderdelen, de behoefte aan een verdere risicoanalyse zal afnemen. De uiteindelijke oplossing wordt duidelijk geboden door alle situaties en onderdelen met een hoog risico in een bepaalde beveiligingsbaseline op te nemen, waarna een organisatie alleen de juiste baseline of reeks baselines hoeft te kiezen.

Diverse niveaus van security baselines

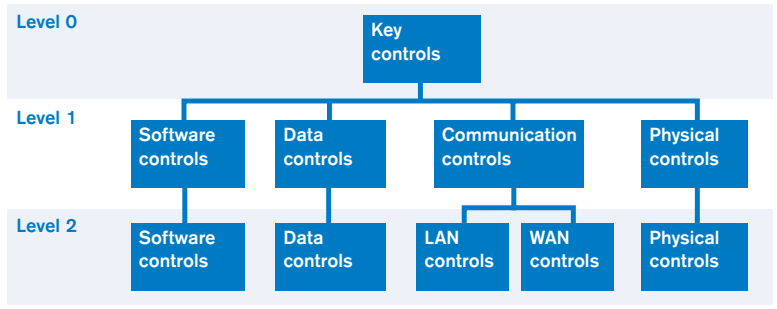
Het bedrijfsleven heeft reeds de beschikking over een aantal verschillende security baselines. Sommige baselines zijn ontworpen voor organisaties die voldoen aan een algemeen profiel en niet behoren tot een specifieke sector. Andere baselines richten zich meer op bepaalde specifieke sectoren. Voorts schrijven sommige baselines niet alleen beveiligingsmaatregelen voor die nodig zijn voor een minimale bescherming, maar ook voor bescherming op middelhoog niveau.

Eén van de bekendste baselines is de *Code of Practice for Information Security Management* (BS7799 ([BSi95])). De *Code of Practice* geeft een algemeen overzicht voor verschillende typen organisaties en richt zich alleen op minimale beschermingseisen. De Code is verdeeld in tien categorieën, waarbij elke categorie een aantal voorgestelde beveiligingsmaatregelen bevat. Onder deze beveiligingsmaatregelen bevinden zich tien kernmaatregelen op het gebied van beveiliging. Deze tien kernmaatregelen zullen te allen tijde en onder alle omstandigheden op alle organisaties van toepassing zijn en dienen deel uit te maken van de in iedere organisatie geïnstalleerde beveiligingsmaatregelen. De overige beveiligingsmaatregelen bieden eveneens een minimale bescherming, maar kunnen mogelijk niet altijd in iedere situatie worden toegepast. Een organisatie moet zelf besluiten welke van deze minder belangrijke beveiligingsmaatregelen op haar situatie van toepassing zijn.

Het Duitse *IT Baseline Protection Manual* ([BSI96]) is een veel volledige document en behandelt beschermingseisen op laag en middelhoog niveau. In tegenstelling tot de *Code of Practice* biedt het *Baseline Protection Manual* richtlijnen voor de wijze waarop de specifieke beschermingseisen voor een organisatie moeten worden vastgesteld. Indien een hoog of zeer hoog beschermingsniveau nodig is, stelt het tevens voor een gedetailleerde risicoanalyse uit te voeren.

Daarnaast beginnen zich enkele sectorspecifieke security baselines te ontwikkelen. Zo is er bijvoorbeeld al een beveiligingsbaseline voor de medische sector ontwikkeld. Veel van de omgevingsspecifieke risico's die in de medische wereld voorkomen, worden met deze baselinebeveiligingsmaatregelen afgedekt. Ziekenhuizen die zulke baselinebeveiligingsmaatregelen introduceren zullen vanzelfsprekend veel meer risico's in hogere mate afdekken, dan zij zouden doen door het introduceren van een algemene baseline, zoals de *Code of Practice*.

Figuur 1. Hiërarchische ordening van beveiligingsmaatregelen.



Op basis van deze verschillende benaderingen van baselinebeveiliging, zoals hierboven besproken, kan worden geconcludeerd dat security baselines niet langer slechts een minimale beveiliging bieden. Als er bovendien meer omgevingsspecifieke of sectorspecifieke baselines worden ontwikkeld, zal de behoefte aan het uitvoeren van een risicoanalyse na de introductie van een aantal relevante security baselines sterk afnemen. Alleen in echt abnormale situaties zal dit nog steeds nodig zijn.

De hiërarchische organisatie van security baselines

Beveiligingsmaatregelen die in verschillende security baselines zijn opgenomen, voldoen aan verschillende beveiligingseisen. Deze eisen variëren van de tien kernbeveiligingsmaatregelen in de *Code of Practice*, het absolute minimum aan te implementeren maatregelen, tot meer algemene beveiligingsmaatregelen in het overige deel van de *Code of Practice* tot beveiligingsmaatregelen die een middelhoog beschermingsniveau bieden. Sectorspecifieke security baselines kunnen ook een hoger beschermingsniveau bieden.

Als alle security baselines hiërarchisch kunnen worden gestructureerd, variërend van een absolute minimumbescherming, zoals de kernbeveiligingsmaatregelen, tot stringentere beveiligingseisen, ontstaan veel nieuwe mogelijkheden. Een organisatie kan dan bepalen welk beschermingsniveau nodig is en of sectorspecifieke beveiligingseisen moeten worden geïmplementeerd. Zodra deze besluiten zijn genomen, hoeft de organisatie slechts de hiërarchische structuur van boven naar beneden af te werken totdat het vereiste beschermingsniveau is bereikt.

Figuur 1 geeft een voorbeeld weer van een baselinehiërarchie, waarbij de afzonderlijke beveiligingsmaatregelen zijn gegroepeerd naar de verschillende te beschermen categorieën.

Om sectorspecifieke beveiligingsmaatregelen in de hiërarchie op te nemen, is het mogelijk een verdere dimensie aan de baselinehiërarchie toe te voegen. Op een bepaald niveau in de hiërarchie kan een specifiek gebied, bijvoorbeeld fysiek, verscheidene sectorspecifieke alternatieven bieden. Figuur 2 geeft deze verdere dimensie in een grafiek weer.

Door verschillende, stringentere security baselines te integreren kunnen hogere beschermingsniveaus worden verkregen zonder dat men hoeft terug te vallen op een risicoanalyse.

Zoektechniek door middel van de baselinehiërarchie

Zoals hierboven reeds is genoemd, is één van de zwakke punten van de meeste baselines het feit dat er weinig begeleiding wordt geboden bij de keuze van de beveiligingsmaatregelen en welke beveiligingsmaatregelen in een specifieke situatie van toepassing zijn. Indien baselines op hiërarchische wijze worden geordend, zal er een techniek moeten worden gekozen om de gebruiker door

de verschillende beveiligingsmaatregelen te leiden en om te bepalen welke beveiligingsmaatregelen van toepassing zijn en welke niet.

Een hoogwaardige analyse moet bepalen welk baselineniveau het juiste zal zijn. Deze analyse moet de bedrijfswaarde van alle IT-systemen en de risico's vanuit het zakelijk oogpunt van de organisatie in overweging nemen.

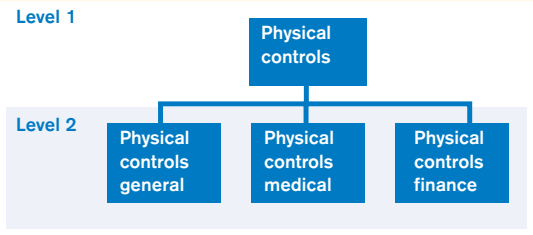
Zodra het juiste beveiligingsbaselineniveau is vastgesteld, moet een verdere selectie van zoektechnieken degene die de beveiligingsmaatregelen implementeert, helpen bij het bepalen van de juiste aanbevolen beveiligingsmaatregelen om het van tevoren vastgestelde beveiligingsniveau te verkrijgen. Zodra deze beveiligingsmaatregelen zijn geïdentificeerd, kunnen zij worden geïnstalleerd, beheerd en gecontroleerd.

Conclusie

Organisaties worden aan veel verschillende risico's blootgesteld. Deze risico's moeten worden afgedekt door het implementeren van de juiste beveiligingsmaatregelen. Er bestaat geen simpele procedure om de meest effectieve beveiligingsmaatregelen te bepalen. Traditiegetrouw worden beveiligingsmaatregelen eerst na een risicoanalyse geïmplementeerd. Helaas is risicoanalyse een zeer complex, kostbaar en arbeidsintensief proces. Dientengevolge kiezen veel organisaties ervoor geen risicoanalyse uit te voeren. Dit geldt in het bijzonder voor het MKB. Het gevolg is dat organisaties mogelijk onvoldoende beschermd zijn of dat er ineffectieve beveiligingsmaatregelen worden geïnstalleerd.

Een beveiligingsbaseline bestaat uit een reeks beveiligingsmaatregelen die de meeste organisaties een afdoende beveiligingsniveau zullen bieden tegen de meest voorkomende algemene risico's. Indien een organisatie een hoger beveiligingsniveau voor een specifiek, zeer gevoelig of belangrijk bedrijfsonderdeel wenst te installeren, kan een risicoanalyse voor dat onderdeel worden uitgevoerd om de specifieke risicosituaties af te dekken. Als deze baselines ook hogere beveiligingsniveaus en/of specifieke sectoren gaan afdekken, zal de behoefte aan een verdere risicoanalyse afnemen. Uiteindelijk zullen security baselines zo effectief worden, dat de behoefte aan een verdere risicoanalyse zal verdwijnen. Een vereiste voor de effectieve implementatie van een dergelijke techniek is het vaststellen van een effectief zoek- of selectiemechanisme dat de gebruiker kan helpen bij het kiezen van een geschikt beveiligingsniveau en van de bijbehorende beveiligingsmaatregelen.

Een dergelijke bottom-upbenadering zal de traditionele benadering zeker niet eenvoudig vervangen. Het ontstaan van security baselines heeft al veel bedrijven gemotiveerd beveiligingsmaatregelen te implementeren, juist omdat het zo eenvoudig is te bepalen welke beveiligingsmaatregelen moeten worden geïnstalleerd om een evenwichtige bescherming te bieden. Het is echter zeer wel denkbaar dat de intelligente manipulatie van security baselines de complexe, eentonige, inconsistente risicoanalyse in de toekomst geheel zal vervangen.



Figuur 2. Sectorspecifieke beveiligingsmaatregelen.

Literatuur

[BSi95]
Code of Practice for Information Security Management, BS7799, BSi, United Kingdom, 1995.

[BSI96]
IT Baseline Protection Manual, BSI, Duitsland, 1996.

[ISO96]
Guidelines for Information Security Management, Deel 3, PDTR 13335-3, ISO/IEC JTC 1 SC27, 1996.

[Jaco96]
R.V. Jacobson, CORA *Cost-of-Risk Analysis*, IFIP >96 WG 11.2, Samos, Griekenland, 1996.

[NCC96]
The Information Security Breaches Survey, NCC, dti, ICL & UKITsec, 1996.

Prof. dr. R. von Solms is hoofd van de afdeling Informatietechnologie van Port Elizabeth Technikon sinds 1989. Hij heeft een graad (*PhD*) aan de Rand Afrikaans Universiteit in Johannesburg. Voor internationale tijdschriften schreef hij veel artikelen en ook presenteerde hij een aantal artikelen op internationale en nationale conferenties. Tevens is hij voorzitter van Werkgroep 11.1 van de *International Federation for Information Processing (IFIP)*, die zich bezighoudt met Information Security Management.