



INFORMATIEBEVEILIGING EEN GECONTROLEERD PROCES

INLEIDING

In dit informatie tijdperk is het voor organisaties van groot belang om over tijdige en correcte informatie te beschikken om bijvoorbeeld haar klanten beter te kunnen bedienen of om voordeel ten opzichte van concurrenten te behalen. De voorziening van informatie wordt in toenemende mate steeds meer afhankelijk van ICT, zodanig dat deze als vanzelfsprekend wordt beschouwd zoals water uit de kraan. Het gevaar van deze vanzelfsprekendheid is dat men vaak niet bewust is van de mogelijke gevolgen voor de organisatie, indien de informatievoorziening niet beschikbaar is.

Het in kaart brengen en beheersen van deze risico's wordt ook wel informatiebeveiliging genoemd. Zo zou een informatiebeveiliging een continu proces moeten zijn, dat telkens weer bijgesteld wordt om te kwaliteit van de informatievoorziening te verhogen. Immers, het wordt ook als vanzelfsprekend beschouwd dat een autofabriek continue bezig is om de veiligheid en efficiëntie van haar productiemachines te verbeteren.

De vraag is welke concrete stappen er ondernomen dienen te worden, om te komen tot een informatiebeveiliging zoals hierboven beschreven. Hier is niet een eenvoudig antwoord op te geven, omdat dit van veel factoren afhangt. Om toch antwoord te kunnen geven op deze vraag, kan gesteld worden dat er minimaal drie stappen kunnen worden uitgevoerd.

In stap 1 zal d.m.v. een risico analyse in kaart moeten worden gebracht welke risico's de informatievoorziening aan bloot gesteld kan worden, het bepalen van de vervolgschade en welke kosten dit met zich mee brengen om te deze te beperken.

In stap 2 zal bepaald worden welke maatregelen (zowel technisch als organisatorisch) er al aanwezig zijn en hoe deze beter ingezet kunnen worden om te komen tot een gecontroleerd informatiebeveiliging proces.

In stap 3 worden eventuele aanvullende maatregelen bepaald, mochten de al bestaande maatregelen niet voldoende zijn.

Uiteraard zijn dit niet enige stappen die moeten worden ondernomen, echter ze vormen wel de basis van een effectieve informatiebeveiliging.

RISICO ANALYSE

De eerste stap is tevens de moeilijkste, namelijk bepalen wat beveiligd moet worden en wat de financiële of vervolg schade kan zijn indien dit niet gebeurt. De uitkomst hiervan zal bepalen welke maatregelen financieel gerechtvaardigd zijn te nemen; immers het is niet verstandig dat de oplossing meer kost dan het probleem. Uiteraard zullen er maatregelen zijn die ondanks dat toch genomen moeten worden.



Een pragmatische aanpak is om eerst gezamenlijk met alle belanghebbenden (eigenaren, leidinggevendenden etc.) de bedrijfsprocessen in kaart te brengen. Deze worden vervolgens stap voor stap doorlopen waarbij telkens afgevraagd wordt welke componenten (mensen, hardware, software, gegevens en infrastructuur zoals licht, stroom, water etc.) hiervoor nodig zijn en wat de financiële schade is als de betrouwbaarheid hiervan verminderd c.q. verstoord wordt.

Betrouwbaarheid wordt bepaald door de integriteit (correctheid, authenticiteit), confidentialiteit (vertrouwelijkheid, exclusiviteit) of beschikbaarheid (tijdigheid, bereikbaarheid) van een component.

Om te kunnen bepalen welke maatregelen er gerechtvaardigd zijn, dient tevens de waarschijnlijkheid van een dergelijke verstoring te worden bepaald. Dit kan in termen van procenten, aantal keren per jaar of andere vormen.

Als resultaat is er een compleet overzicht van alle bedrijfsprocessen, hun afhankelijkheden en risico's.

Er moet benadrukt worden dat het van cruciaal belang is deze exercitie te laten uitvoeren door de juiste personen uit de organisatie. Alleen op deze manier kan gegarandeerd worden dat juiste energie (tijd, geld, mensen etc.) wordt besteed aan het oplossen van de juiste beveiligingsproblematiek. Tevens zorgt het er voor dat er een groter draagvlak ontstaat binnen de organisatie, ook als genomen maatregelen een verandering van werkwijzen vereisen.

BESTAANDE MIDDELEN

Tijdens de vorige stap is er een duidelijker beeld ontstaan op welke gebieden de informatiebeveiliging zich in eerste instantie zal richten. In de volgende stap wordt gekeken naar de al aanwezige maatregelen en hoe deze wellicht beter in te zetten zijn. Bestaande maatregelen kunnen zowel technisch als organisatorisch van aard zijn. Onder technische maatregelen wordt o.a. verstaan alle software, hardware, netwerken en andere infrastructuur.

De meeste apparatuur en programmatuur kunnen verder worden beveiligd door het maken van de juiste configuratie wijzigingen. Zo kan de bijvoorbeeld de beveiliging van een besturingssysteem enorm verbeterd worden door het uitvoeren van eenvoudige configuratie wijzigingen zoals het uitzetten of verwijderen van onnodige software en diensten.

Een ander aspect is de opstelling of plaatsing van apparatuur. Het verplaatsen van belangrijke apparatuur en systemen naar beter beveiligde ruimtes (zoals een computer ruimte) kan vele vervelende storingen voorkomen. Ook het anders inrichten van het netwerk kan voordelen opleveren. Door gebruik te maken van de mogelijkheden in moderne switches, kan het netwerk worden opgedeeld in segmenten, waarbij de onderlinge toegang kan worden geregeld. Zo kunnen problemen in een gedeelte van het netwerk niet voor problemen zorgen in andere delen.



Bij organisatorische maatregelen wordt o.a. gekeken naar bestaande procedures en andere afspraken. Zo kan het bijvoorbeeld zijn dat er al procedures zijn voor het wijzigingen van wachtwoorden, echter kunnen deze nog aangescherpt of nageleefd worden. Een vaak onderbelicht aspect is het verbeteren van de back-up procedures. Vooral het veilig opslaan en regelmatig testen van back-ups kan veel leed voorkomen. Een ander voorbeeld is het aanscherpen van de procedures voor het toelaten en registreren van bezoekers. Regelmatige voorlichting over deze bestaande regels kunnen al gedragsveranderingen te weeg brengen, die het beveiliging niveau verhogen.

Het loont dus om na te gaan welke mogelijkheden er al aanwezig zijn en hoe deze kunnen bijdragen tot het onder controle krijgen van de informatiebeveiliging.

AANVULLENDE MAATREGELEN

Mocht blijken dat de bestaande maatregelen niet voldoende zijn, dan zullen aanvullende maatregelen genomen moeten worden. Aanvullende maatregelen (zowel technisch als organisatorisch) kunnen een preventieve, detective, repressieve of correctieve doel hebben.

Preventieve maatregelen voorkomen schade, repressieve maatregelen verminderen het effect van schade. Zo zal een antivirus programma proberen te voorkomen dat systemen geïnfecteerd raken. Mochten er toch systemen besmet raken, dan kan het effect hiervan worden verminderd door kantoornetwerken op te delen in verschillende segmenten, die indien nodig van elkaar kunnen worden gescheiden.

Detective maatregelen richten zich op het opsporen en herkennen van beveiligingsovertredingen. Zo zal een netwerk intrusion detection oplossing in staat zijn om aanvallen op het netwerk te herkennen en daar de systeembeheerder over in te lichten. Correctieve maatregelen zorgen er voor dat de situatie weer hersteld kan worden. Het terug zetten van een back-up is een voorbeeld van een correctieve maatregel.

Voorbeelden van preventieve organisatorische maatregelen kunnen zijn het opnemen van boete clausules in contracten met derden. Een zowel correctief als repressief voorbeeld is een goed getest calamiteitenplan om schade te beperken. Het uitvoeren van controle in de vorm van een audit is een voorbeeld van een detective maatregel.

Welke type maatregel nodig is hangt geheel af welke risico's er afgedekt moeten worden en wat de kosten hiervan zijn. Zo kan men een systeem dubbel uitvoeren om de beschikbaarheid van informatie te garanderen, maar men kan ook volstaan met het terug zetten van een back-up. Het laatste geval is waarschijnlijk goedkoper te realiseren, maar het duurt ook langer voordat de informatie weer beschikbaar is. Dit is een afweging die telkens gemaakt moet worden. In dit geval kan een correctieve maatregel (de back-up) prevaleren boven een preventieve maatregel (redundantie). Vaak kan een risico alleen worden ondervangen door gebruik te maken van meerdere types maatregelen. Belangrijk bij het kiezen van maatregelen is deze minder kosten dan de schade die ze voorkomen.



VOLWASSENHEID

De hiervoor beschreven aanpak beschrijft de meest elementaire stappen die ondernomen moeten worden. Echter er is meer nodig om informatiebeveiliging als kwaliteitsproces tot een integraal onderdeel van de bedrijfsvoering in te richten.

Toch valt wel te bepalen waar een organisatie staat met het realiseren van dit doel. Een veel gebruikt model is het Amerikaanse Capability Maturity Model (CMM), welke aangeeft hoe via gerichte stappen automatiseringsprocessen te verbeteren zijn. Als dit model wordt toegepast op de inrichting van informatiebeveiliging, dan zijn de volgende volwassenheidsniveaus te onderkennen:

Initieel: Een organisatie bevindt zich op niveau 1 als de aan informatiebeveiliging alleen wordt gedragen vanuit de IT organisatie, zonder een draagvlak vanuit het hoger management of de business. Bij de invoering van maatregelen stuit men regelmatig op weerstand bij de organisatie, omdat het belang daar nog niet wordt onderkend;

Bewustwording: Het belang van informatiebeveiliging door het hoger management wordt onderkend. Er wordt een risico analyse door verschillende belanghebbenden uitgevoerd, om te achterhalen wat van belang is te beschermen en tegen welke kosten. Bij de invoering van nieuwe maatregelen valt men nog wel terug op niveau 1;

Gedefinieerd: De resultaten van de risico analyse worden verwerkt in een informatiebeleid, waarin op hoofdlijnen wordt beschreven wat de organisatie dient te beveiligen en waarom. Verantwoordelijkheden zijn gedefinieerd en is een beveiligingsprogramma gestart die aangestuurd wordt vanuit het hoger management. Procedures zijn ontwikkeld en maatregelen worden een projectmatige wijze geïmplementeerd;

Beheerst: Beveiligingsincidenten worden op een vakkundige wijze afgehandeld en wijzigingen worden gedegen beoordeeld en uitgevoerd. Informatiesystemen worden regelmatig gecontroleerd op kwetsbaarheden en indien nodig bijgewerkt;

Optimaliserend: De informatiebeveiliging wordt systematisch verbeterd op basis van regelmatige metingen of audit en vormt een geïntegreerd onderdeel van de bedrijfsvoering. Nieuwe technologieën kunnen beheerst worden ingevoerd.

Als een organisatie weet op welk volwassenheidsniveau zij zich bevindt, dan is in combinatie met een risico analyse te bepalen welke activiteiten gestart kunnen worden om de informatiebeveiliging naar een volgend volwassenheidsniveau te brengen.

Michiel Broekhuijsen, CISSP
Information Security Consultant
Andarr