

Security Awareness bij outsourcing

Ing. Frank Breedijk > Frank Breedijk werkt op dit moment als Security Engineer bij Schuberg Philis, een organisatie die zich richt op de outsourcing van complexe bedrijfskritische applicatie infrastructures met hoge beschikbaarheidseisen. In het verleden was hij manager van het EMEA Security Operations Center voor managed security services van Unisys en werkte hij als security officer voor Interxion.

Security awareness is onmisbaar voor iedere organisatie, ook bij outsourcing. Echter bij outsourcing heeft security awareness een aantal extra dimensies. Zo moet de klant zich bij het aangaan van een overeenkomst, naast een groot aantal andere security gerelateerde zaken, in korte tijd op de hoogte stellen van de security awareness bij de dienstverlener (de outsourcer). Omdat er sprake is van twee verschillende organisaties kan er sprake zijn van een verschil in kennis en inzicht tussen de twee organisaties. In dit artikel probeer ik een aantal min of meer outsourcing specifieke kanten van security awareness te belichten.

Dat het voor organisaties van levensbelang is security awareness onder haar medewerkers te borgen, behoeft geen discussie, maar hoe zit dat wanneer (een deel van) de IT activiteiten buitenshuis uitgevoerd gaan worden? Hoe kun je als outsourcingklant de security awareness van een outsourcer beoordelen?

Een aantal professionele outsourcingpartijen is in het bezit van een BS7799 dan wel een ISO27001:2005 certificaat. Kun je als klant er vanuit gaan dat een gecertificeerde partij ook een partij is waar de security awareness goed geregeld is? In de basis is dit het geval. Dit internationale normenkader omschrijft de eisen waaraan een Information Security Management System (ISMS) zou moeten voldoen en security awareness maakt hier deel van uit. De eisen voor certificering stellen dat het ISMS regelmatig door een onafhankelijke partij tegen de norm getoetst moet worden. Security Awareness zal hier in de praktijk, in het geval van een goed werkend ISMS, altijd aanwezig zijn. Toch is een certificaat op zichzelf niet altijd zaligmakend, omdat het bijvoorbeeld mogelijk is te certificeren met een zeer beperkte scope. Ik heb in het verleden marketing materiaal gezien waarbij een bedrijf aangaf in het bezit te zijn van een BS7799 certificaat. Bij verdere navraag bleek dit echter alleen te gaan om de operations van één specifiek datacenter. Een kritische klant doet er dus goed aan om te onderzoeken in hoeverre de scope van het certificaat

ook de outsourcingactiviteiten en bij voorkeur ook de specifieke klantsystemen omvat.

Een andere manier om bij het aangaan van een contractrelatie onder andere de security awareness van een outsourcingpartij te testen, is het vragen van een 'Comply or Explain' statement met betrekking tot de security policy van de klant. Hierbij is het aan de outsourcer om aan te geven in welke mate hij aan de security policy van de klant kan voldoen en uitleg te geven wanneer hij hiervan wil afwijken. Hoewel het verleidelijk is om de kwaliteit van een outsourcer aan de hoeveelheid groene vlakjes ('Comply') te verbinden is het eigenlijk veel interessanter om te kijken naar de antwoorden die bij non-compliance ('Explain') gegeven worden, zeker als het om het vaststellen van de security awareness van een organisatie gaat. Omdat we, per definitie, te maken hebben met twee verschillende organisaties is een '100% Comply' statement praktisch onmogelijk en zullen er dus altijd 'Explain' statements zijn. Deze statements zullen een inzicht geven in hoe professioneel de outsourcer met beveiliging omgaat.

Een voorbeeld uit de praktijk: Een klant, die een outsourcingovereenkomst voor een bedrijfskritische applicatie op een Unix platform aan wil gaan, heeft in de security policy staan dat door middel van een password cracker iedere maand de kwaliteit van de gebruikerswacht-

woorden moet worden vastgesteld en dat gebruikers met een zwak wachtwoord hierop moeten worden aangesproken. De outsourcer stelt voor van deze policy af te wijken en geeft middels een 'Explain' statement de volgende verklaring: "Wij werken niet met wachtwoorden, alle logins worden geauthenticeerd via public/private key authenticatie. Er zijn op de systemen geen wachtwoorden aanwezig en het uitvoeren van een dergelijke audit is dus ook niet zinnig."

Aan de uitleg van de outsourcer, die een preventieve maatregel neemt in plaats van een achteraf controlerende maatregel, kan worden afgelezen hoe security aware deze organisatie is.

Security awareness, een integrale benadering

Zodra de outsourcingovereenkomst is aangegaan, verandert security awareness van eenrichtingsverkeer (heeft mijn outsourcer wel voldoende security awareness?) naar een bidirectioneel mechanisme. Immers nu beide partijen een relatie zijn aangegaan, zullen zij beiden verwachtingen hebben met betrekking tot elkaars security awareness.

Security awareness en business awareness liggen hier zeer dicht bij elkaar, immers het accepteren van bepaalde risico's is te allen tijde een business decision waarbij de techniek slechts de input kan geven. Outsourcer en klant zullen elkaars business moeten begrijp-

pen om tot een optimale wederzijdse security awareness te komen. Immers de business van de klant bepaalt in zeer hoge mate hoe er in bepaalde situaties gereageerd moet worden. Een voorbeeld hiervan is de prioriteiten bij het herstellen van incidenten. Bij de ene klant, bijvoorbeeld bij een online shop, zal de prioriteit liggen op beschikbaarheid, terwijl bij een andere klant, bijvoorbeeld een online bank, de data integriteit en vertrouwelijkheid een veel hogere prioriteit zullen hebben. Een outsourcer die ervoor kiest zich rond de klant te organiseren en daardoor een beter begrip van de klant krijgt, zal ook beter in staat zijn risico's op waarde te schatten.

Risicomanagement en daarmee ook securitymanagement zullen op een geïntegreerde wijze en met een nadrukkelijk afgestemde governance tussen partijen en binnen de afzonderlijk partijen moeten plaatsvinden om helder en eenduidig richting te geven aan de gewenste doelstellingen, maatregelen en (onafhankelijke) controle van die maatregelen. Met name de wederzijdse governance zal er voor zorgen dat er een gezonde balans ontstaat tussen de security belangen van de klant en van de outsourcer, zonder dat dit de, voor de klant zo noodzakelijke, flexibiliteit in de weg staat. In deze wederzijds governance structuur is het belangrijk de verantwoordelijkheden en bevoegdheden van zowel security organisaties van de klant en outsourcer afzonderlijk als die van de gezamenlijke security organisatie vast te leggen. Daarnaast is het belangrijk vast te leggen hoe security beslissingen in noodsituaties en onder tijdsdruk genomen worden.

Reverse awareness

Er zullen zich situaties voordoen waarbij de outsourcer security risico's anders ziet dan de klant. Dit kan komen door een verschil in de mate van inzicht en ervaring of omdat de outsourcer vanuit zijn werkzaamheden een beter inzicht heeft in wat er in de omgeving gebeurt en welke mogelijke risico's dit met zich mee brengt. Een goede manier om de klant van de risico's bewust te maken is hem meer inzicht te geven. Een voorbeeld kan dit beter illustreren.

Bij een outsourcer komt een verzoek binnen tot het opstellen van Internet

toegang via TCP port 6667 zodat gebruikgemaakt kan worden van een 'online collaboration tool'. Een kort onderzoek van de outsourcer leert dat de zogenaamde 'online collaboration tool' waarschijnlijk IRC is, het grootste online chat netwerk op het Internet. Hoewel zakelijk gebruik van IRC niet ondenkbaar is, weet de outsourcer dat het gebruik van chat boxen in de security policy van de klant nadrukkelijk verboden is. Door het wijzigingsverzoek van de klant middels een impact analyse met mogelijke risico's toe te lichten, kan de klant het verzoek in de juiste context beoordelen en een onderbouwde business decision nemen.

Anders wordt het wanneer de outsourcer en de klant na het delen van de informatie nog steeds een verschil van inzicht hebben. Ik heb mij hier altijd op het standpunt gesteld dat de beheerde infrastructuur eigendom is van de klant en dat de oud-Hollandse stelregel 'Wie betaalt die bepaalt' dus van toepassing is. Met andere woorden, de klant bepaalt waar hij met zijn infrastructuur heen wil. Dit wil echter niet zeggen dat veranderingen waar de outsourcer het niet mee eens is, zonder meer uitgevoerd moeten worden. Ik heb in het verleden, en ook in mijn huidige functie, hiervoor meerdere malen gebruikgemaakt van een zogenaamd risk statement. Een risk statement bevat een omschrijving van de ontstane situatie of de voorgestelde verandering, de gevolgen en risico's die hiermee genomen (zouden) worden en de verklaring dat de klant zich bewust is van deze risico's en deze bewust neemt. Een dergelijk risk statement heeft twee functies: ten eerste legt het document vast dat de outsourcer aan zijn (morele) zorgplicht heeft voldaan en beschermt daarmee de outsourcer indien het mis gaat en ten tweede laat het de klant nogmaals goed nadenken over de te nemen risico's en heeft een dergelijk statement soms tot gevolg dat een klant tot een ander inzicht komt. Of de klant de verandering nu afblaast of juist bereid is het in kaart gebrachte risico bewust te nemen, het risico statement zorgt dat de verantwoordelijkheid uiteindelijk daar ligt waar die hoort, namelijk bij de business. De ervaring leert dat indien dit risicomanagement-proces zorgvuldig en adequaat wordt uitgevoerd klanten zeer goed in staat zijn juiste afwegingen

te maken, redenerend vanuit de risico's en kansen voor hun dagelijkse business.

Periodieke risicoanalyse

Er zijn maar zeer weinig outsourcers die ervoor kiezen om samen met de klant periodiek via een gestructureerde methode, bijvoorbeeld CRAMM, een risicoanalyse te maken van de uitbestede applicatie infrastructuur. Doordat klant en outsourcer in een gezamenlijke sessie nadenken over het belang van de applicatie infrastructuur voor de klant, de mogelijke risico's en de eventuele gevolgen als er iets misgaat, ontstaat in beide organisaties een verhoogd (security) bewustzijn. Aan de hand van het resultaat van de risicoanalyse kan worden vastgesteld of genomen maatregelen nog steeds passen bij het risico-profiel. Een periodieke risicoanalyse voorkomt ook dat verzuimd wordt na te denken over de gevolgen van een geleidelijke verandering van het belang van de applicatie infrastructuur. Iets dat bij de meeste bedrijven door de drukte van de dagelijkse praktijk gemakkelijk over het hoofd wordt gezien. Het is, zeker bij outsourcing van belang dat een applicatie infrastructuur na de implementatie niet bevroren wordt, maar met organisatie die ze ondersteunt mee verandert. Een klassiek voorbeeld hiervan zijn bijvoorbeeld reisorganisaties die de afgelopen jaren de verkoop via het Internet hebben zien stijgen, veelal ten koste van de verkoop via het callcenter. Doordat de bezoekersaantallen en de omzet van de webshops soms gestaag en, op basis van marketing acties, soms zeer sterk veranderen, realiseert men zich vaak pas te laat dat de maatregelen ter bescherming van bijvoorbeeld de privacy, beschikbaarheid, performance en schaalbaarheid niet meer in verhouding staan tot het belang van de, steeds meer kritische, applicatie infrastructuur voor de continuïteit van de organisatie. De periodieke strategische risicoanalyse creëert en onderhoudt de security awareness bij beide partijen op het noodzakelijke hoogste niveau.

One size fits all?

Uit het voorgaande mag worden afgeleid dat security awareness specifiek op de doelgroep en de situatie afgestemd moet worden. Hoewel er zoiets is als een basis awareness, waaronder zaken als omgaan met wachtwoorden vallen, is het een illusie te denken dat er zoiets

als een generiek security awareness programma bestaat. Het door de klant eenzijdig opleggen van maatregelen met betrekking tot awareness aan de outsourcer is weinig effectief. In het geval van een outsourcingrelatie is security awareness een co-productie van betrokken partijen, waarbij de risicoanalyse en het constateren van (mogelijke) security violations ingebed dient te zijn in de dagelijkse operatie en waarbij de outsourcer in alle lagen van het bedrijf zicht moet hebben op de business van de klant. Op basis van adequate analyse waarin de outsourcer

op basis van haar expertise dient te voorzien, zal binnen de afgesproken governance de risico-afweging vervolgens door de klant moeten worden gemaakt. Juist deze keuzes moeten worden vastgelegd, zodat een auditor kan constateren dat er op een gecontroleerde wijze wordt omgegaan met risico's en dat er sprake is van een integrale security awareness.

Link die aangeeft waarom awareness op alle lagen van de organisatie belangrijk is: http://worsethanfailure.com/Articles/The_Direct_Approach.aspx