ARNO VAN DER LAAN

De belangrijkste misvattingen in beveiligingsbeleid

Hoe goed is úw informatiebeveiliging?

Bedrijven besteden enorme bedragen aan informatiebeveiliging. Dikke rapporten met risicoanalyses en beveiligingsprocedures wekken al snel de indruk dat er voldoende aandacht wordt geschonken aan informatiebeveiliging. Maar is dit wel zo? En gaat die aandacht dan ook uit naar de juiste aspecten van de beveiliging?

Bij het bepalen van het beveiligingsbeleid en het bedenken en implementeren van beveiligingsmaatregelen, kunnen misvattingen rondom informatiebeveiliging ertoe leiden dat het beveiligingsbeleid faalt. In dit artikel zal een aantal van deze misvattingen besproken worden. Deze inzichten kunnen een leidraad vormen om de informatiebeveiliging in uw eigen organisatie te toetsen en mogelijk te verbeteren.
Om met de eerste misvatting te beginnen: het idee leeft dat beveiligingsincidenten vanzelf aan het licht komen. Men vertrouwt op de reeds aanwezige controle binnen het bedrijf. Meestal gaat het hier om fysieke toegangscontrole, sociale controle en een periodieke financiële controle. Men gaat ervan uit dat er geen directe reden tot zorg is zolang alles goed gaat. Kleine beveiligingsincidenten lijken het bedrijf niet te schaden en de kans op een groot beveiligingsincident met veel schade is klein. Het gevolg is dat men weinig energie steekt in het zoeken naar beveiligingsincidenten. Hierdoor kunnen veel kleine incidenten ongemerkt plaatsvinden die bij elkaar opgeteld een aanzienlijke schadepost kunnen veroorzaken. De kans dat zich uiteindelijk een groot beveiligingsincident voordoet neemt toe, doordat de dader onopgemerkt door kan gaan met het vinden van nieuwe toegangen. De ondergang van de bank Barings is hier een goed voorbeeld van. Het is dan ook aan te raden om signaleringssystemen te implementeren.

Signaleringssystemen

Grofweg zijn er drie soorten signaleringssystemen: intrusion detection systems (IDS'en), auditing-systemen en securitymonitors.
IDS'en zijn systemen die controleren of er gebruikers zijn die zich ongeoorloofd toegang proberen te verschaffen tot informatie. Een aanval begint meestal met een poging tot het uitbuiten van bekende beveiligingslekken. Een voorbeeld hiervan is het proberen te versturen van mail met daarin een virus naar een systeem waarop zich alleen een webserver bevindt. Het IDS meldt al dit soort pogingen binnen het netwerksegment waarin het geplaatst is. Het gebruik ervan is aan te raden binnen alle netwerksegmenten waar zich systemen bevinden die te beschermen gegevens bevatten of die beschermd dienen te worden tegen oneigenlijk gebruik.

Het is mogelijk dat een persoon wel toegang heeft tot een bepaald systeem via een bepaalde interface, maar toch beperkte rechten heeft. Dit kan niet met een intrusion detection system gecontroleerd worden. Hiertoe hebben alle grote commerciële informatiesystemen de zogeheten auditingfunctionaliteit. Met auditing wordt vastgelegd wie, wat, wanneer binnen de informatiesystemen geprobeerd heeft en of dit gelukt is. Ongeoorloofde handelingen zijn hiermee terug te voeren naar de veroorzaker. Auditing is aan te bevelen voor dezelfde systemen waarvoor ook IDS'en aangeraden zijn.

De derde categorie signaleringsystemen, securitymonitors, kunnen door het bekijken van het netwerkverkeer trends ontdekken betreffende wie, in welke mate informatiesystemen gebruikt. Na een korte periode die nodig is voor het inregelen en opstellen van regels, kan dit systeem dan signaleren of er afwijkend gedrag van een medewerker te zien is. Een medewerker die normaal gesproken ongeveer 90 procent van de tijd met een debiteurensysteem werkt, valt op als hij opeens de helft van de tijd met het personeelssysteem aan de gang gaat. Bij het introduceren van een securitymonitorsysteem is de kans echter wel groot dat er een 'big brother'-discussie op gang komt. Een dergelijk systeem werkt immers alleen dán indien niet slechts de informatiesystemen bewaakt worden die extra beveiliging nodig hebben (zoals bij een IDS en auditing), maar álle activiteiten van medewerkers geanalyseerd kunnen worden. Het is dan ook aan te raden deze vorm van signalering alleen te gebruiken in omgevingen waar zeer hoge beveiligingseisen gesteld worden.

Risico's onderkennen

Er is in de hierboven genoemde voorbeelden al aangegeven dat er naast externe ook interne bedreigingen zijn. Bij informatiebeveiliging wordt vaak als eerste gedacht aan het beveiligen van de internettoegang. Uit onderzoek van het Computer Security Institute (CSI) blijkt echter dat veel (zo niet de meeste) overtredingen door eigen mede-

Zorg ervoor dat alle beveiligingsincidenten, dus ook alle pógingen tot inbraak, aan het licht komen

werkers worden begaan. De financiële schade die dit veroorzaakt blijkt ook nog eens substantieel groter te zijn dan de schade die veroorzaakt wordt door de activiteiten van hackers. Hier hebben we misvatting twee te pakken! Er wordt (te) weinig gedaan om incidenten tegen te gaan die worden veroorzaakt door eigen medewerkers. Daar is een goede reden voor: veel mensen hebben er moeite mee om een collega te zien als een potentiële overtreder. Het is daarom heel verleidelijk om met de collega's met wie men het informatiebeveiligingsplan opstelt en de maatregelen uitwerkt alleen te spreken over externe hackers. Het gevolg is dat in de uiteindelijke maatregelen onvoldoende aandacht uitgaat naar overtredingen door eigen medewerkers, met na verloop van tijd, als de incidenten zich aandienen, grote financiële schade als resultaat.

Het ontkrachten van deze misvatting is niet eenvoudig. Hoe kom je ertoe om gezellige en vakbekwame collega's wél als mogelijke misdadigers te zien? Een oplossing om deze valkuil te omzeilen is het brainstormen in een multidisciplinaire groep over alle mogelijke bedreigingen. In een groep is de kans veel kleiner dat iemand zich persoonlijk aangevallen voelt als een hypothetisch beveiligingsincident geschetst wordt. Ook door het aanwezig zijn van specialisten met verschillende achtergronden kan een competitie tussen de medewerkers worden geïnitieerd om het meest eenvoudige of effectieve beveiligingsgat te vinden. Dit resulteert niet zelden in de ontdeking van verrassende risico's. Bovendien wordt door dergelijke brainstormsessies de kans kleiner dat er beveiligingsrisico's, en dan met name interne risico's, vergeten worden.

Adequaat reageren

Als alle mogelijke beveiligingsincidenten en risico's in kaart zijn gebracht, moet men bepalen hoe daarop te reageren. Bij het oplossen van de beveiligingsincidenten bestaat nogal eens de misvatting dat bestaande

VAN BELEID TOT UITVOERING

Zelfs als goed in kaart is gebracht welke gegevens in welke mate beveiligd dienen te worden, is het nog een lange weg naar een complete set aan beveiligingsmaatregelen. Op het gebied van benodigde functionaliteit is eenvoudig te controleren of alles opgeleverd is, maar hoe test je of er voldoende maatregelen genomen zijn om alle mogelijke beveiligingsaanvallen het hoofd te bieden? De misvatting hier is dat dit op dezelfde wijze te testen is als de benodigde functionaliteit. Zo worden alleen de genomen beveiligingsmaatregelen getest op de juiste werking, maar er wordt niet gecontroleerd op volledigheid. De oorzaak van deze misvatting ligt in het feit dat het bedenken van andere risico's en het testen daarop een oneindig proces is. Er is nooit te garanderen dat een informatiesysteem geen beveiligingslekken bevat. Dit betekent voor een project dat er niet te bepalen is wanneer deze activiteit eindigt, wat strijdig is met de definitie van een project.
Medewerkers van een project wordt dan ook gevraagd om voor de bekende beveiligingsrisico's maatregelen te bedenken en te implementeren. Tijdens tests worden deze genomen beveiligingsmaatregelen beproefd, waarmee het systeem voldoende beschermd lijkt. Het nagaan of de beveiligingsmaatregelen als geheel wel voldoende zijn, is secundair en wordt alleen gedaan als er tijd en geld over is. Het gevolg is een beveiliging van informatiesystemen die er cosmetisch goed uitziet. Kijkt men verder, waarbij ook de niet gebruikelijke toegangspaden bekeken worden, dan zijn veel beveiligingslekken te constateren. Het eindresultaat is dan alsnog dat de informatiebeveiliging het doel niet bereikt.
Het advies is goed te documenteren welke beveiligingsmaatregelen genomen worden en waarom. Laat een aangestelde beveiligingsfunctionaris tijdens elke fase in het project controleren of de voorgestelde beveiligingsmaatregelen voldoende zijn. Dit is goedkoper dan er in een laat stadium achter komen dat er nog beveiligingslekken in het informatiesysteem aanwezig zijn: het herstellen van gemaakte fouten wordt duurder naarmate het project vordert. Nog erger is het natuurlijk als er een beveiligingsincident voorvalt als het systeem al in productie is.

middelen voor het oplossen van incidenten adequaat genoeg zijn. Meldingen worden echter eerst door eerstelijns beheer opgevangen en pas als men er daar niet uitkomt, wordt een specialist ingeschakeld. Deze dienstdoende specialist heeft veelal beperkte middelen om analyses uit te voeren en als er hulp van een collega nodig is, dan moet deze ook weer opgeroepen worden. Dit alles kost tijd en die is er vaak niet. Ook hier geldt weer dat er geen directe reden tot zorg is zolang alles goed gaat. Er is echter één groot verschil met signalering: is het nog relatief goedkoop om signalering te implementeren, het zorgen voor een adequate afhandeling van de meldingen die hieruit voortkomen is een stuk duurder. Dit vanwege de 7x24-uurs-economie waarbij de beschikbaarheid van systemen gegarandeerd moet zijn. Het kost veel geld om ook 7x24 uur een groep specialisten paraat te hebben, een zogeheten 'computer emergency response team', dat de meldingen van signaleringssystemen goed kan afhandelen.

Het werken volgens de bestaande procedures en met de al beschikbare middelen zorgt ervoor dat het stellen van de juiste diagnose erg lang duurt. Dat de hoeveelheid schade die aangericht kan worden sterk toeneemt wanneer niet snel gereageerd wordt, is eerder aangegeven: de dader kan eenvoudig meer van dezelfde overtredingen begaan of zich een weg banen naar informatie met meer waarde. Het advies is snel en adequaat te reageren op beveiligingsincidenten. Een mogelijkheid is het instrueren van eerstelijns beheer om bij het optreden van ongewone meldingen het betreffende informatiesysteem niet meer toegankelijk te maken, zodat de mogelijke pogingen om daar oneigenlijk gebruik van te maken gestopt worden. De beschikbaarheid van de diensten neemt hierdoor echter ernstig af. De voorkeur gaat daarom uit naar zo'n emergency response team. Deze duurdere oplossing moet zich terugverdienen door een stabielere en betere afhandeling van beveiligingsincidenten, in combinatie met een goede beschikbaarheid van de informatiesystemen. Eventueel kan deze taak extern belegd worden.

Dynamiek

Wanneer adequaat gereageerd wordt op pogingen tot inbraak en de aan het licht gekomen beveiligingslekken gedicht worden, zou men mogen verwachten dat op den duur steeds minder tijd besteed hoeft te worden aan informatiebeveiliging. Ook dit blijkt een misvatting te zijn. Door de introductie van nieuwe (versies van) technologie zijn beveiligingsmaatregelen al snel achterhaald. Dit wordt veroorzaakt door de 'technology push' vanuit de softwarebranche en de time-to-market, zodat de eigen bedrijfsdoelstellingen gehaald kunnen worden. Het gevolg hiervan is dat de informatiebeveiliging steeds achterloopt op het gewenste beveiligingsniveau. Na enige tijd van dichten van beveiligingslekken zal de beveiliging van het ene informatiesysteem op orde zijn. Maar ondertussen komt een volgend informatiesysteem (dat met nieuwe technologie is ontwikkeld) met nieuwe beveiligingslekken. Beveiligingsincidenten zijn dan ook altijd te verwachten, maar het oplossen ervan is niet in te plannen. Bovendien kan het dichten van nieuwe beveiligingslekken ten koste gaan van het implementeren van andere beveiligingsmaatregelen uit het beveiligingsplan. Het is dan ook noodzakelijk om dit plan regelmatig te herzien en dat verlangt enige dynamiek van de organisatie. Uiteraard moet hiervoor budget geregeld zijn: wachten met het aanpassen van de beveiligingsmaatregelen omdat er geen budget is, kan fatale gevolgen hebben. Om steeds weer adequaat te kunnen reageren op nieuwe technologie dient er planmatig en budgettair rekening mee gehouden te worden dat bij het introduceren van nieuwe technologie beveiligingslekken te dichten zijn. Het beveiligingsplan wordt zo een levend document dat regelmatig bijgesteld wordt.

Helder doel

Het inzetten van nieuwe technologie vanwege nieuwe bedrijfsdoelen kom je in de praktijk vooral tegen bij de dienstverlening richting businesspartners en klanten via internet. De informatiesystemen die daarvoor in het begin ingezet werden, waren wegens te grote beveiligingsrisico's losgekoppeld van de backoffice-systemen. De huidige eisen die aan informatiesystemen gesteld worden, maken integratie noodzakelijk.

POSITIEVE PUBLICITEIT

Zelfs als er alles aan gedaan is om beveiligingsincidenten te voorkomen, zal het toch nog gebeuren dat op een dag een beveiligingslek aan het licht komt. Hoe moet hiermee omgegaan worden? Het idee dat het bekendmaken van beveiligingslekken in de eigen of geleverde informatiesystemen het bedrijf schaadt, is ondertussen achterhaald. Enige jaren geleden was het nog opvallend als er beveiligingslekken ontdekt werden in software. De opvatting was dat de software dan slordig in elkaar zat. Een bedrijf dat in de publiciteit kwam vanwege een beveiligingslek, kreeg direct negatieve reacties van de omgeving. Als gevolg hiervan worden bij veel bedrijven beveiligingslekken die ontdekt worden zo veel mogelijk verzwegen. Hierbij gaat het voornamelijk om de aanvallen die gepleegd worden door interne medewerkers, met als gevolg dat hier nog steeds te weinig aandacht naar uitgaat. In alle gevallen bestaat het risico dat een beveiligingslek in de publiciteit komt doordat anderen dit melden. Als blijkt dat de eigenaar of leverancier van het informatiesysteem hiervan al op de hoogte was, zonder de klanten op de hoogte te stellen, is het geven van een positieve draai aan dit onfortuinlijke beveiligingslek niet meer mogelijk.
Een meer actieve houding kan daarentegen juist positieve reacties opleveren. Bedrijven zijn ondertussen gewend aan beveiligingslekken die overigens ook steeds ingenieuzer worden, denk aan 'buffer overrun exploits'. Men doet graag zaken met leveranciers en partnerbedrijven die open zijn over hun bedrijfsvoering, inclusief onvolkomenheden in de geleverde diensten. Overigens is dit in andere bedrijfstakken al gewoon: meldingen van fabrikanten over bijvoorbeeld ondeugdelijke remmen van een auto of glasstukjes in levensmiddelen staan regelmatig in de kranten. Het effect van deze meldingen blijkt te zijn dat deze bedrijven gezien worden als bedrijven die serieus met de kwaliteit van hun producten omgaan. Het is dan ook het beste om de negatieve publiciteit die ontstaat als anderen met een beveiligingslek komen, voor te zijn door zelf hier melding van te doen. Klanten of partnerbedrijven kunnen eventueel discreet geïnformeerd worden, maar als dit niet mogelijk is, schuw dan de publieke media niet. Aandachtspunt is wel dat wanneer een beveiligingslek gemeld wordt, ook aangegeven moet worden hoe men hiermee moet omgaan. Als er nog geen permanente oplossing voorhanden is, geef dan advies hoe tijdelijk de risico's weggenomen kunnen worden, zelfs als dat het stilleggen van het betreffende informatiesysteem betekent.

Denk aan voorbeelden als telebankieren en ketenintegratie waarvoor een 'near-real-time-koppeling' nodig is. Vanwege de haast met het realiseren van deze nieuwe informatiesystemen worden routinematig beveiligingsmaatregelen aangebracht. Deze richten zich voornamelijk op de 'voorkant', waar het informatiesysteem raakvlakken heeft met de gebruikers. Impliciet wordt dan aangenomen dat alles voldoende beschermd wordt. Dit kunnen we zeker een misvatting noemen. De oorzaak uitleggen is niet eenvoudig en vergt een blik in het verleden. Wat heeft zich (in vogelvlucht) afgespeeld tussen 1980 en het heden?

- Rond 1980: applicaties draaien op enkele systemen (mainframes/minicomputers) en de personeelsleden die de applicaties gebruiken hebben per systeem een terminal, loginnaam en wachtwoord nodig. Autorisaties zijn beperkt binnen de applicaties aan te geven.
- Rond 1990: pc's worden via een netwerk aan elkaar gekoppeld en via terminalemulatiepakketten is toegang tot de applicaties op de mainframes en minicomputers mogelijk. Nieuwe filesharing- en client/server-applicaties worden ontwikkeld, waarbij autorisatiemogelijkheden afhankelijk zijn van de applicatie. De achterliggende gegevens zijn alleen toegankelijk via de applicaties.
- Rond 2000: de automatiseringsgraad in organisaties is enorm toegenomen. Koppelingen tussen systemen zijn aangebracht zodat gegevens kunnen worden vastgelegd binnen één systeem en hergebruikt in alle andere systemen die de gegevens nodig hebben. Ook partners en klanten krijgen toegang tot systemen. Door de bredere ontsluiting van de gegevens is een eenvoudige beveiliging niet meer voldoende. De vraag is niet meer alleen wie toegang tot welk systeem moet krijgen, ook de informatiebeveiliging is gedetailleerder geworden. Voorbeeld hiervan is het dusdanig autoriseren van een gebruiker dat deze informatie mag raadplegen van leveranciers uit een bepaalde regio, alleen tijdens kantooruren via het internet.

Duidelijk is dat er in het begin fysieke beveiliging was in de vorm van het moeten beschikken over een terminal, gekoppeld aan het systeem waar de applicatie en gegevens zich op bevonden. Deze beveiliging verdween met de komst van netwerken. Hierna moest vertrouwd worden op de kwaliteit van de beveiliging van de applicaties. Door het aanbrengen van koppelingen tussen applicaties is de grip op beveiliging van de onderliggende gegevens in handen gekomen van meerdere applicaties. Dat het overzicht van hoe applicaties de onderliggende (kopieën van) gegevens benaderen niet meer aanwezig is in veel bedrijven, moet als verontrustend aangemerkt worden. Na deze schets van de situatie die door de jaren heen ontstaan is, wordt duidelijk dat wanneer verlangd wordt gegevens te ontsluiten naar bijvoorbeeld partners of klanten, direct weer gedacht wordt aan het implementeren van beveiligingsmaatregelen aan de voorkant, waar de gebruikers normaal gesproken direct mee in aanraking komen. Hierbij is het risico zeer groot dat bepaalde beveiligingsmaatregelen onnodig (wellicht dubbel) geïmplementeerd worden, of dat de beveiligingsmaatregelen niet kunnen voorkomen dat de onderliggende gegevens op een andere wijze, via een zijingang benaderd kunnen worden.

Door de introductie van nieuwe technologie zijn beveiligingslekken aan de orde van de dag

Een oplossing hiervoor is op korte termijn niet voorhanden. Het ontbreken van bruikbare standaarden op het gebied van zogenaamde 'end-to-endbeveiliging' maakt het implementeren van beveiligingsmaatregelen de komende jaren nog maatwerk. Het advies is om vanuit de gegevens te bepalen welke maatregelen genomen moeten worden. Stel dus allereerst een risicoanalyse op van de meest waardevolle gegevens die in het bedrijf aanwezig zijn. Ga vanuit dat perspectief het pad af hoe deze gegevens ontsloten worden en pas daar de beveiligingsmaatregelen op aan. Het uitvoeren van deze stappen, met als resultaat het weer in kaart hebben van de totale gegevenshuishouding, is niet eenvoudig, maar het is de enige juiste insteek.

Conclusie

Door de hierboven geschetste misvattingen kan de beoogde informatiebeveiliging tekortschieten. De basis van een goede informatiebeveiliging ligt bij het in kaart brengen van wat beveiligd moet worden en waartegen. Vergeet niet de risico's te onderkennen van ongeoorloofde handelingen die worden gepleegd door eigen medewerkers. Het achterhalen van alle bedreigingen gaat het beste door hier in een multidisciplinaire groep over te brainstormen. Dit beveiligingsbeleid moet regelmatig worden herzien vanwege veranderingen in de omgeving. Het is ook noodzakelijk te controleren of het beleid op een juiste wijze uitgevoerd wordt, door bij projecten die nieuwe informatiesystemen ontwikkelen gedurende alle fasen te controleren of de juiste beveiligingsmaatregelen getroffen worden. Dit moet worden gedaan door een beveiligingsfunctionaris die geen druk voelt op het gebied van budget of realisatiedatum.

Door introductie van nieuwe technologie zijn beveiligingslekken aan de orde van de dag. Deze moet men snel signaleren en adequaat oppakken. Bij voldoende omvang, kan men hiervoor een zogeheten 'computer emergency response team' oprichten of deze dienst uitbesteden. Zorg ervoor dat alle beveiligingsincidenten, maar ook alle pogingen tot inbraak aan het licht komen. In ieder geval zouden intrusiedetectiesystemen en auditing in gebruik moeten worden genomen bij belangrijke informatiesystemen. In bedrijven waar informatiebeveiliging zeer belangrijk is, is het toepassen van een securitymonitorsysteem te overwegen.
Wanneer blijkt dat er in een eigen informatiesysteem dat gebruikt wordt door klanten of partnerbedrijven een beveiligingslek aanwezig is, is het beter om deze informatie zelf op gepaste wijze naar buiten te brengen (zie kader 'Positieve publiciteit'). Het melden van een beveiligingslek met daarbij een advies hoe hiermee om te gaan toont verantwoordelijkheid voor de kwaliteit.

ARNO VAN DER LAAN
(arnol@infosupport.com)
is werkzaam bij Info Support B.V.