Opinie: Het politieke spel van het verbergen van rechten

Spanningsvelden bij het oplossen van kritische rechten

14 september 2021

Mark Deiss

(Publicatiedatum: 14 september 2021)

Bedrijven met ERP-software bepalen aan de hand van functieprofielen welke rechten hun medewerkers krijgen. Daarbij moeten medewerkers niet te veel kritische rechten of combinaties van rechten krijgen die samen een functiescheidingsconflict opleveren: een segregation of duties (SoD)-conflict. Het verstrekken van deze rechten kan door de complexiteit van het systeem gemakkelijk doorschieten naar ontoelaatbare niveaus. Het gebruik van SoD-detectietooling kan helpen kritische rechten en SoD-conflicten beter inzichtelijk te maken. Hoewel dit nu inzichtelijk is geworden voor een bedrijf, wil dit niet direct zeggen dat deze conflicten meteen verwijderd worden. Een van de taken van een auditor is de aangegeven SoD-conflicten te vertalen naar begrijpelijke risico's, en het bedrijf keuzes te laten maken in hoeveel risico men wil lopen.

Dit artikel is gebaseerd op de persoonlijke ervaringen van een SAP-autorisatie-consultant die zijn ervaring heeft opgedaan bij een groot aantal nationale en internationale bedrijven. Hij spreekt over de problemen bij het verwijderen van SoD-conflicten en de onderliggende redenen ervan. Ook komt hij stelselmatig manieren tegen die controle door de auditor omzeilen. Hij doet uit de doeken met welke technieken dat gedaan wordt en welke politieke strategieën er gebruikt worden.

Efficiëntie gaat voor security

Een SoD-tool geeft inzicht in welke gebruikers een functieprofiel hebben dat op de een of andere manier met rechten overladen is. Oplossen lijkt vanaf dat moment relatief eenvoudig. Als er een probleem is, en je kent de oorzaak, dan lijkt oplossen alleen een kwestie van tijd. In werkelijkheid is het verwijderen van functiescheidingsconflicten verre van gemakkelijk. Dit artikel legt stap voor stap uit hoe deze functieconflicten steeds maar weer terug blijven komen. De drie grootste oorzaken van het niet kunnen verwijderen van SoD's zijn:

- vergroeiing van autorisaties;
- onderbezetting;
- gekozen over-efficiëntie.

Vergroeiing van autorisaties

Een autorisatiesysteem is goed te vergelijken met een apothekerskast vol potjes. Als het goed is, kun je iets makkelijk opzoeken. Ook zit er in het potje wat er op het etiket staat. Onder de druk om een hele specifiek oplossing te leveren, worden er soms zaken gecombineerd die niet bij elkaar horen. Als dit een aantal jaren doorgaat dan zit niet meer in het potje wat er op het etiket staat. Bij een autorisatiessysteem geldt dat hoe hoger de mate van standaardisatie is, hoe beter het te besturen is. Er zijn echter autorisatiesystemen waar alles aan elkaar vastzit, door jaren van onzorgvuldige wijzigingen. In dat geval is het niet meer mogelijk om rechten goed uit te leveren. Ook corrigeren is niet goed meer mogelijk. Een verandering heeft dan heel veel onbedoelde neveneffecten. Alles is verweven.

Onderbezetting

SAP-gebruikers, of ERP-gebruikers in het algemeen, in de grotere bedrijven van ons land hebben het lang niet altijd makkelijk. Vaak is er een minimale bezetting op een afdeling. Dit betekent dat alle afdelingsfuncties over deze mensen verdeeld moeten worden. Het is dan niet mogelijk om aan SoD-conflicten te ontkomen. Je zit eraan vast. Het kernprobleem is dus dat onderbezetting bijna altijd leidt tot autorisatievergroeiing, die moeilijk kan worden ontvlochten.

Gekozen over-efficiëntie

Efficiëntie en economisch belang gaan bij de meeste bedrijven voor de veiligheid van hun gegevens. Heel verbazingwekkend is dat niet, want kosten zijn heel goed meetbaar terwijl veiligheid van gegevens minder zichtbaar en minder meetbaar is. Met meer autorisaties kun je ook zelfstandig meer zaken oplossen, en dat is dus uiteindelijk ook economischer. Van te brede rechten heb je dus niet direct last.

Je kunt met opzet iemand zo'n brede autorisatie geven dat hij virtueel drie verschillende functies vervult. Deze over-efficiëntie is in eerste instantie heel handig voor het bedrijf. Pas later beseft het hoger management dat die over-efficiënte werkwijze ook zijn keerzijde heeft: als de medewerker met meerdere functies ineens thuis ziek in bed ligt, dan vallen er ook meteen meerdere functies in het bedrijf uit. Er is een zeer sterke afhankelijkheid gecreëerd die kan leiden tot een zekere discontinuïteit. Dit is alleen op te lossen door andere medewerkers nog meer te overladen met rechten. Voor de mensen zelf is deze werkwijze natuurlijk ook niet goed. Bij mensen die nu thuis zitten met een burn-out, is vast ook wel eens de vraag opgekomen hoeveel collega's ze nu eigenlijk aan het vervangen waren. Er komt pas een kanteling in de over-efficiënte, maar fraudegevoelige werkwijze als er een dringende reden is. Dat is bijvoorbeeld als de jaarrekening niet meer automatisch wordt goedgekeurd, of een toezichthouder boos wordt. Op dat moment ontstaat er pas een intern belang om van de fraudegevoelige rechten af te komen.

Fasen in het oplossen van functieconflicten-leveranciers in één gebied zijn gevestigd

Een accountant die tijdens de jaarcontrole een zeer fraudegevoelige omgeving aantreft, zal met recht beweren dat fraude nu slechts een kwestie van tijd is. Daarom moeten de vergroeide autorisaties eerst los worden gemaakt. Dat komt erop neer dat je kleine brokjes autorisaties samenstelt waarmee je tot de ene functie óf tot de andere functie toegang kunt geven. Je hebt vanaf dat moment dus een keuze in het toekennen ervan.

Dit zijn de fasen in het oplossen van SoD-conflicten:

Fase 1: Bewust worden van het feit dat elimineren van functieconflicten nodig is.
Fase 2: Aanschaffen van een applicatie die SoD's kan detecteren.
Fase 3: Herbouwen van autorisatie als deze vergroeid is.
Fase 4: Opnieuw samenstellen van het takenpakket van medewerkerteams op basis van de oude situatie.
Fase 5: Tactisch verschuiven van verschillende taken zodat SoD-conflicten vervallen.
Fase 6: Zoeken naar oplossingen voor SoD-conflicten die vastzitten.

De fundamenten om te komen tot een oplossing worden in fase 1 en 2 gelegd. Als de top van het bedrijf van mening is dat er geen probleem is, dan ís er ook geen probleem tot-dat een fraude of datalek het tegendeel bewijst. Daarom gaan fase 1 en 2 ook vaak hand in hand en kan er een kip-eisituatie ontstaan. Zonder SoD-detectie (fase 2) geen goede gegevens en dus ook geen bewustwording (fase 1). Er is in deze eerste twee fasen naast goede gegevens ook een goede rapportagestructuur nodig die uiteindelijk de bewustwording moet waarborgen.
De werkelijke oplossing wordt pas behaald in fase 5 en 6 waar de business zelf met taken gaat schuiven om zo het aantal SoD-conflicten te verminderen. Dit betekent dat teams meer specialistisch worden ingericht en dat bestaande teams soms gesplitst worden in hun uitvoerende taken.

Dit is natuurlijk niet waar de business op zit te wachten. De business heeft jaren gewerkt aan een efficiënte werkwijze met uiteenlopende taken per team en dus brede autorisaties. Deze werkwijze is verankerd en zit vast in het hoofd van de medewerkers. In het veranderen van deze werkwijze moet de business zichzelf vaak herontdekken. Er is dus sprake van business transformatie. Dit zorgt voor een spanningsveld tussen het management en de business waar enig vuurwerk aan te pas kan komen. Dit artikel gaat over dit spanningsveld en hoe het zich ontwikkelt. Een spanningsveld waar Internal Audit middenin zit gezien haar taakstelling binnen veel organisaties.

De grote terugslag en de grote duik

De grote terugslag komt als men ontdekt dat sommige SoD's 'muurvast' in de organisatie zitten terwijl ze technisch gezien verwijderd zouden kunnen worden in het ERP-systeem. De business claimt dat de efficiënte, maar risicovolle werkwijze nodig is. Vanaf dit punt bouwt de druk alleen nog maar meer op om tot een oplossing te komen. Het hoger management wil de SoD-conflicten weg hebben wegens het goedkeuren van de jaarrekening of toezichtvereisten, maar de business wil de huidige werkwijze behouden wegens efficiëntie.

Internal Audit is op zoek naar het werkelijke risico van een functieconflict. Daarnaast is men op zoek naar de maatregelen die genomen kunnen worden om dat risico te verminderen. Een goede formulering van het risico is heel belangrijk om door de organisaties opgepakt te worden. Dat is lang niet altijd gemakkelijk omdat verschillende tools alleen inzicht in SoD's leveren, en niet het risico dat SoD-conflicten vertegenwoordigen. Dit omzetten in concrete risico's blijft vakwerk, wat bij uitstek het terrein van de auditor of risicomanager is. Er zit helaas zeer vaak een laagje 'zeep' tussen Internal Audit en de business: de business zal nooit risico's gaan melden bij Internal Audit. Zij hebben te veel baat bij deze 'efficiënte' werkwijze die soms inderdaad ook risico's met zich meebrengt. Internal Audit wordt dus niet altijd even goed geïnformeerd. De eerdergenoemde SoD-tool is voor Internal Audit dus ook een belangrijk ankerpunt om objectief inzicht te krijgen in de werkelijke stand van zaken.

Bij de interpretatie van de gegevens van de SoD-detectietool ontstaat een tweedeling tussen Internal Audit en de business(operatie). Vrij vertaald komt dit neer op: óf de lijst met SoD-conflicten moet leeg en dat wordt bereikt door business-transformatie, óf de risicovolle toegang met veel rechten blijft bestaan ten behoeve van flexibiliteit in de business en de business past ontduiking toe om detectie te voorkomen.

Business-transformatie is in deze context het veranderen of automatiseren van interne processen, zodat kwaadaardige manipulaties er geen vat op hebben. Bij financiële instellingen slaat deze tweedeling doorgaans door naar de kant van Internal Audit of risicomanagement. Dat is inderdaad goed, want banken willen zo min mogelijk risico lopen op elke technische mogelijkheid tot fraude. Er mogen dus geen grote SoD-conflicten ontstaan, ongeacht het verhaal erachter. Als men met geld omgaat, is fraude plegen al snel verleidelijk. Denk hierbij aan de fraudedriehoek. [1] Bij sommige bedrijven slaat het echter weer door naar de businesskant. Managers wuiven het risico weg omdat men de kans op bonussen en gewin groter acht. Dit is de kant van technisch en politiek vuurwerk dat uiteindelijk uitmondt in wat ik 'de grote duik' noem. Maar voordat we het hebben over de grote duik en duistere manieren om frauderisico onzichtbaar te verbergen, eerst de opties die je hebt bij een functieconflict dat zich niet laat verwijderen.

De manieren om SoD-conflicten te verwijderen zijn:

- Splitsen van de taken van een team zodat het SoD-conflict vervalt.
- Gebruik van noodusers of firefighters.
- Automatisering van een van beide taken van het conflict.
- Een extra controle voor de uitoefening van het SoD-conflict.
- Een extra controle na de uitoefening van het conflict.
- Verlaging van het risico door andere omstandigheden.

Splitsen van de taken. Dit is eigenlijk de natuurlijke manier van verwijderen. In veel gevallen lukt dit niet, zeker niet als men kiest voor 'agile' werken.

Gebruik van noodusers. Dit is het inzetten van een nooduser-account. Het idee is dat bij een noodsituatie de gebruiker de beschikking krijgt over een nooduser-account met uitgebreide(re) rechten dan een gewone gebruiker. De noodsituatie kan hiermee worden afgehandeld zonder dat de medewerker permanent de beschikking heeft over deze rechten. Daardoor kunnen de rechten van het normale account van de medewerker lager zijn, waarmee dus een SoD-conflict kan worden voorkomen. Het gebruik van de nooduser wordt goed bewaakt en meestal is er goedkeuring nodig. Daarmee is er een effectieve extra controle op beide functies. Tot zover de theorie.

Automatisering. Dit komt neer op één van beide taken automatiseren via de application controls. Dit is een elegante manier om van het SoD-conflict af te komen. Hierbij vervallen de rechten van een gebruiker om één van beide taken zelf handmatig uit te voeren.

Een extra controle voor de uitoefening van het SoD-conflict. Dit vergt soms wat customizing of programmeerwerk. Er wordt vooraf een extra controle gedaan waardoor het risico inderdaad lager wordt. Een voorbeeld is het vier-ogen-principe bij het invullen van een rekeningnummer.

Een extra controle na de uitoefening van het conflict. Dit komt neer op min of meer alles laten bestaan van de SoD en achteraf te controleren of er daadwerkelijk fraude is gepleegd. Dit kan wel prijzig uitvallen, omdat achteraf nog veel controlewerk nodig is.

Verlaging van het risico door andere omstandigheden. Hiervan is sprake als er iets speciaals is dat het risico verlaagt. Dat kan inderdaad een serieuze en realistische situatie zijn. Bijvoorbeeld als de hoeveelheid winst of geld die je er mee zou kunnen opstrijken heel beperkt is.

‘Ondergrondse’ toegang en het omzeilen van Internal Audit of Control

Zoals gezegd, zit er een tweedeling in de interpretatie van de resultaten van de SoD detectie-tool. De business heeft er soms alle belang bij om ten koste van alles bepaalde toegang te behouden. Dit is meestal niet eens onredelijk, het gaat dan om efficiëntie of ondervangen van ernstige onderbezetting. Vaak ook weer veroorzaakt door de directie die stuurt op (extreme) kostenverlaging. Dit betekent dat Internal Audit of Control omzeild moet worden. Mazen in het toepassen van de bovenstaande manieren om SoD-conflicten te verwijderen geven daar de gelegenheid toe. Daarbij ontstaan vaak groteske en absurdistische situaties.

De onderstaande situaties zijn niet hypothetisch, maar concrete praktijkvoorbeelden.

Uitwisselen van het wachtwoord/dubbele accounts

Teams zijn soms gesplitst in een A- en B-kant om daarmee bepaalde conflicterende taken te voorkomen. Met het uitwisselen van het wachtwoord kan dat effectief omzeild worden. Dit is echter ook totaal onzichtbaar. Het lijkt net of er twee mensen aan het werk zijn terwijl dat niet zo is. Een andere manier is twee accounts gebruiken.

Misbruik van de nooduser

De nooduser wordt permanent gebruikt om extra rechten te krijgen. Er is dus geen sprake meer van een noodsituatie, maar van een operationele situatie waarin op tactische wijze gebruik wordt gemaakt van de nooduser.

Nieuwe naam

De SoD-tool herkent alleen dingen die hij kent. Hij herkent bijvoorbeeld geen bedrijfseigen maatwerk; dit moet je bekend maken aan de tool. Gebeurt dit niet, dan kan al een hele sloot aan maatwerk onder de radar van Internal Audit schuiven. Als je een nieuwe SAP-transactie maakt dan wordt deze dus initieel niet herkent. Slordigheid en gecalculeerde listigheid voeren beide naar dit punt van niet gedetecteerde SoD’s.

De ontbrekende IT-architect

Ontbreekt de IT-architect in een organisatie, dan kan alles op een eigen manier gemaakt worden. Zolang maatwerk maar functioneel werkt, zal het door de business geaccepteerd worden. Je kunt dus iets maken wat net twee taken combineert die gescheiden zouden moeten blijven. Dit komt voor bij SAP Fiori-applicaties. Bij een goed ontwerp worden functieconflicten in Fiori-applicaties net zo goed gedetecteerd als bij normale transacties. De praktijk is dat dit lang niet altijd gebeurt. Er worden op die manier applicaties gemaakt die functioneel goed werken maar SoD-technisch toch een haakje missen of erger … een datalek kunnen veroorzaken.

Extra toetsing achteraf

Velen die bepaalde toegang met een frauderisico willen houden, zullen beargumenteren dat het niet gaat om de detectie van de mogelijkheid tot het plegen van fraude, maar de detectie van werkelijke fraude. Met dit argument in de hand worden dan inhoudelijke loggingen opgezet om zo de fraudegevallen te filteren uit de operationele stroom van bewerkingen. Het gaat dan om situaties waarbij zowel functie A als functie B op hetzelfde subject worden uitgevoerd. Als er echter fraude wordt uitgevoerd dan gebeurt dit door die mensen die dit systeem heel goed kennen. Er zijn bijzonder interessante constructies gevonden waarbij de logging uit te schakelen was. Daarbij ontstaat een situatie waarbij een logschaduw van een paar minuten ontstaat. Daarmee ontloop je automatische detectie. Ook zijn er situaties gezien waarbij de logging door 'technische problemen' niet aan stond, net aan het begin van het jaar toen de jaarafsluiting werd gedaan. Dat is inderdaad heel toevallig…

Omzeilen van mitigaties

Mitigaties zijn extra controles die een bepaald risico effectief kunnen verminderen. Waar een SoD-conflict 'vastzit' kunnen mitigaties een goede oplossing zijn om een kritieke combinatie van taken wel toe te staan, terwijl het risico niet proportioneel stijgt. Zeker als mitigaties geautomatiseerd zijn kunnen ze zeer effectief zijn. Eenvoudig gezegd heb je een situatie met 'meer licht', waar onregelmatigheden eerder aan het licht komen.
Als mitigaties echter niet geautomatiseerd zijn, kunnen zij een extra druk vormen op de organisatie die niet op het aanleveren van bewijsmateriaal te wachten zit. Soms worden deze extra controles geschrapt wegens drukte of ondercapaciteit.
Als er een les is die geleerd kan worden uit cybercriminaliteit, dan is dat de daarbij toegepaste middelen extreem subtiel en onnavolgbaar zijn. Een mitigatie kan omzeild worden door net buiten het gebied van de controle te blijven. Een concreet voorbeeld: het wijzigen van een rekeningnummer. Een extra controle is dan bijvoorbeeld het rekeningnummer vergelijken met referentiegegevens. Als in een eerder stadium deze referentiegegevens al zijn aangepast, dan zal een controle niets aan het licht brengen. Dit is bijvoorbeeld equivalent aan een vervalst veranderverzoek voor een rekeningnummer.

Politiek

Het laatste wapen bij het in stand houden van een omgeving met fraudemogelijkheden is politiek. Zoals eerder gesteld, is security bijna altijd ondergeschikt aan het commerciële bedrijfsbelang, terwijl security juist een van de bedrijfsbelangen zou moeten zijn.
Als het om economische winst gaat, legt veiligheid van gegevens het vaak af. [2] Er zijn documentaires over de Space Shuttle die het fenomeen van politiek versus risico's haarfijn uitleggen. Dit wordt bijvoorbeeld gedaan door niet de SoD's zelf te ontkennen, maar glashard het risico ontkennen dat ze vormen. Er bestaan gevallen van geïnstitutionaliseerde risico-ontkenning die betreurenswaardig zijn. Gewoon aanhouden van 'wij zien het risico niet' en uiteindelijk wint de retoriek. Bedrijven die ransomware in hun systemen

hadden, hebben de les van de hele kleine kansen wel geleerd. Een andere manier dan de risico-ontkenning is de acceptatie van het risico en daarmee ook het SoD-conflict voor lief nemen. [SECU15] Dus alles houden zoals het is, en misschien een extra verzekering afsluiten. Er is inderdaad een ondergrens aan het risico waar men nog iets mee moet. Dat klopt. De politieke manager beheerst daarom de vaardigheid om, op het moment dat het tapijt wordt opgelicht, er een aantal extra risico's onder te vegen.

Referentiekader: 'wij kunnen dat wel'

Je kunt je afvragen wie er werkelijk gewonnen heeft als de politiek binnen een bedrijf wint. Het punt dat hier gemaakt wordt, is dat als je de afslag naar ontduiking neemt, je daarmee het enige goede argument naar een oplossing verspeelt. De oorzaak van functieconflicten is namelijk meestal onderbezetting. Met de afslag naar ontduiking verspeel je de kans daar iets aan te veranderen en blijf je tevens met een onveranderde werkdruk zitten. Gek genoeg is dat vaak een geaccepteerde oplossing. Dit komt omdat het referentiekader is: 'wij zijn in staat om met deze kritische rechten zorgvuldig om te gaan'. Dat mag zelfs nog waar zijn ook, maar daarbij vergeten wij dat niet alleen wij deze rechten kunnen uitoefenen maar dat botnets en ransomware dat in onze naam ook kunnen doen. Daarnaast hoeft fraude niet op eigen initiatief te gebeuren, maar kan ook het gevolg zijn van afpersing. Uiteindelijk geldt altijd: te veel macht is voor niemand goed. Als de afslag naar Internal Audit wordt genomen en alle SoD-conflicten met al hun gevolgen op tafel komen, dan staat elk conflict direct in verband met een economisch belang. En daar is wél oog voor. Dit betekent óf uitbreiding van het aantal mensen, andere taakverdeling óf automatisering om het probleem op te lossen. SoD-conflicten zijn op die manier het wisselgeld om een steeds uitgestelde automatisering wel te krijgen. Dit is het ombuigen van een probleem naar een kans.

De auditor verschuift het kantelpunt

Het is interessant te bekijken waar nu werkelijk het kantelpunt zit. Een risico bestaat uit een bepaalde impact maal de kans dat dit kan voorkomen.[3] Elke ondernemer is echter bezig met kansen voor de groei van zijn onderneming, niet met de hele kleine kansen dat er iets mis kan gaan. Dit is wel het dagelijkse speelveld van een auditor. Hij kan goed uitleggen hoe een risico is opgebouwd en inzicht geven in de kansen dat zoiets voor komt. Het bedrijf kan echter met passende retoriek elk risico van tafel vegen door te stellen dat de kans verwaarloosbaar klein is, uitgaande van de eigen interne ervaring. Een risico goed kunnen uitleggen, is op dat moment van weinig meerwaarde meer. Dit soort gesprekken verlopen heel anders als het management van het bedrijf een eerdere ervaring met fraude of malware heeft gehad. Er is in dat geval een intrinsieke motivatie om een gebalanceerde

risicoschatting te doen. Deze motivatie is helaas niet direct op het management van andere bedrijven over te brengen. Dit is de plek waar het kantelpunt zit en waar de auditor een rol kan vervullen.

Een passend voorbeeld maakt dit duidelijk: de ransomware-aanval bij de Universiteit van Maastricht van begin 2020. De Universiteit van Maastricht is een organisatie die zich zeer zeker van vele gevaren bewust is of was. Toch hadden zij in 2020 een ransomware-aanval, waarbij ook de back-up versleuteld werd. [TIMA20] Dit was mogelijk omdat de beheerders zelf toegang hadden tot dit systeem, en daarmee ook de malware. Dat beheerders zelf toegang hebben tot een systeem is echter vrij normaal bij veel bedrijven en organisaties. Heel Nederland doet dit. Toch ziet bijna niemand daar een groot risico in. Gesprekken met deze bedrijven of organisaties om dit als een risico te adresseren, zouden vruchteloos zijn verlopen. Totdat het uiteindelijk toch gebeurt natuurlijk. De echte ervaring met een werkelijke uitoefening van een kwetsbaarheid blijft noodzakelijk om de motivatie voor een goede risicoschatting aan te wakkeren. Eigen lessen leren wat dat betreft het hardst, maar ook lessen uit het leed van anderen werken.

Een audit met alleen het benoemen van risico's kan verlopen zoals boven geschetst voorbeeld. Terwijl een audit samen met een penetratietest of bewijs van enige uitoefening van de kwetsbaarheid een heel andere lading kan gaan hebben. Dit maakt het minder theoretisch. Hiermee verschuift de auditor handig het kantelpunt in motivatie van grenzeloos naïef naar een zorgvuldige risicoschatting. En ook daarom vormen statistieken en berichten uit de media en beroepsorganisaties een belangrijk onderdeel in het voorlichten van het management van een bedrijf.

Tot slot

Kern van dit artikel is dat er tal van technische mogelijkheden zijn om gevaarlijke rechten te verbergen en daarmee een audit te omzeilen. Ook zijn goed gekozen mitigaties bewust te omzeilen. De stellige mening van de auteur is dat dit op de lange termijn niet goed is voor een bedrijf. Zeker niet omdat ook derden hier misbruik van kunnen maken. Mitigatie is een goed hulpmiddel maar geen eindoplossing terwijl businesstransformatie dat wel kan zijn. Het artikel laat vervolgens zien op welke manieren de auditor op een onzichtbare manier is te omzeilen. Liegen is hierbij nog niet eens nodig. Strategisch zwijgen, insinuaties van bepaalde voortgang geven, of selectief gegevens verstrekken doet het ook al. Dit is jammer van al die tijd die hiermee gemoeid is. Meer dan eens stellen bedrijven dat het risico op iets verwaarloosbaar is omdat men al tientallen jaren zo werkt zonder dat er problemen waren. Daarom kijkt de auditor ook naar de markt en ziet verschuivingen waardoor de exposure toeneemt en daarmee uiteindelijk ook het risico. Zonder dat er veranderingen in het bedrijf zijn kan het risico door externe factoren wel degelijk toenemen.

Het nut van het hebben van audits op reguliere basis lijkt in eerste instantie alleen om compliancy redenen te zijn. Audits zijn echter veel belangrijker. Als de resultaten van een audit niet goed zijn, dan is misschien wel een moment van bezinning op zijn plaats. Al die activiteiten die uitgevoerd moeten worden vereisen hoge rechten voor verschillende mensen met uiteraard de bijhorende risico's. De vraag is echter of al deze activiteiten wel nodig zijn. Is het mogelijk om al deze handelingen te automatiseren? Moeten deze handelingen wel uitgevoerd worden? Soms kan een risico geheel uitgesloten worden door gebruik te maken van een externe dienst. Dit is vernieuwing en businesstransformatie. Hierbij wordt de activiteit in zijn geheel onder de loep genomen, met soms verrassende wendingen. Een audit helpt dus om even een pas op de plaats te maken en een verandering in te zetten die niet vanzelf was gekomen. Natuurlijk veranderen we niet vanzelf, daar is altijd een aanleiding voor nodig. Een audit levert een bestuurder dus inzicht maar ook een reden om een wijziging te rechtvaardigen en door te zetten. Dit is de reden dat het omzeilen van een audit niet in het belang van het bedrijf is.

Literatuur

[IMAOxx] Risicoclassificatie: wegingsmethodiek van Kinney & Wiruth, Imaonline.nl, zonder jaartal. https://www.imaonline.nl/sites/default/files/faq/files/wegingsmethodiek-van-kinneyw.pdf, geraadpleegd op 12 juli 2021.

[SECU15] Acceptatie risico's is ook mitigatie? Security.nl, 23 december 2015. https://www.security.nl/posting/455400/Acceptatie+risico%27s+is+ook+mitigatie%3F, geraadpleegd op 12 juli 2021.

[TIMA20] Dilip Timal, What We Can Learn From the Maastricht University ransomware attack? LinkedIn, 17 februari 2020. https://www.linkedin.com/pulse/what-we-can-learn-from-maastricht-university-ransomware-dilip-timal/, geraadpleegd op 12 juli 2021.

[WIKI21] List of data breaches, Wikipedia, 7 September 2021. https://en.wikipedia.org/wiki/List_of_data_breaches, geraadpleegd op 12 juli 2021.

Noten

1 Fraudedriehoek: druk, gelegenheid, rationalisatie.

2 Dit wordt verder onderbouwd met het grote aantal gegevenslekken bij gerenommeerde bedrijven, zie [WIKI21].

3 In literatuur wordt dit vaker uitgedrukt als: risico = impact x kans. Kans bestaat weer uit waarschijnlijkheid en blootstellingsfactor (Kinney & Wiruth), zie: [IMAOxx].

M. (Mark) Deiss CISSP | Securityconsultant bij *NewITera*

Mark Deiss is een securityconsultant met meer dan vijftien jaar SAP/ERP-ervaring. In zijn werk van het implementeren van autorisatiesystemen viel het hem op hoe makkelijk bepaalde systemen te omzeilen zijn. Zijn aandacht ligt sindsdien op de aspecten die het ontduiken van detectie mogelijk maken en in stand houden.
Mark voert security-assessments uit voor grotere bedrijven met de focus op het lekken van bedrijfsgevoelige gegevens.