Drs. Piet Goeyenbier RE RA RO

Informatietechnologie (IT) is niet meer weg te denken uit de zakelijke en privéomgeving. De recente ontwikkelingen op het gebied van de IT brengen voor organisaties kansen met zich mee, ook risico's. Wat zijn die actuele ontwikkelingen, welke kansen zijn er en welke risico's hangen hiermee samen en wat kan de internal auditor bijdragen om die risico's te beheersen?

Trends in IT en wat de internal auditor kan bijdragen

Het toepassen van informatietechnologie is niet meer weg te denken uit de organisatie. De ontwikkelingen gaan gestaag door. Om de auditor bewust te maken worden de volgende actuele trends nader beschouwd: Apps, big data, bring your own device (BYOD), cloud computing, het nieuwe werken (HNW), internet en cybercrime.
Deze trends bieden organisaties nieuwe kansen, maar brengen helaas ook nieuwe bedreigingen met zich mee. Dit artikel beperkt zich tot de belangrijkste kansen, bedreigingen en maatregelen per trend. De trends big data en cloud computing hoeven door de organisatie niet direct te worden geadopteerd. Bij de andere trends komt de impact van buiten de organisatie: van medewerkers, klanten, hackers en criminelen. Op die trends moet de organisatie reageren, want anders loopt de organisatie risico's of mist zij kansen.[1]

Apps
Met de opkomst van de smartphone hebben ook de Apps hun intrede gedaan. Apps zijn applicaties die specifiek zijn ontwikkeld voor smartphones en tablets. Apps bieden organisaties kansen doordat de klant via een App zaken kan doen met de organisatie, dan wel informatie kan inwinnen. Het toepassen van een App biedt de organisatie een extra communicatiekanaal.
De risico's van een App hangen samen met de nieuwigheid en daarmee ook met de onbekendheid en onervarenheid met de ontwikkeling van Apps en de beveiliging van tablets en smartphones. Dit laatste geldt ook voor de verlies- en diefstalgevoeligheid van deze apparatuur.
De belangrijkste risico's voor de organisatie zijn dat ongeautoriseerden toegang krijgen tot de applicaties van de organisatie en daar bestellingen plaatsen zonder te betalen of dat doen op kosten van derden, dan wel dat zij toegang kunnen krijgen tot vertrouwelijke informatie.
Generieke maatregelen zijn adequate ontwikkel- en testprocedures, toegangsautorisatie tot de bedrijfsapplicatie en bewustwording van de eindgebruiker. De specifieke maatregelen worden ook gebruikt bij de communicatie via internet en betreffen: beveiligd dataverkeer, extra toegangsbeveiliging van de App en waarschijnlijkheidscontroles en limieten.

Big data
Onder big data wordt verstaan alle data die in een organisatie voorhanden is. Dat is de informatie die beschikbaar is in de eigen informatiesystemen (zowel de proces- als de beheersystemen). Ook de data beschikbaar via internet (bijvoorbeeld de gegevens van en over concurrenten, klanten, open data) kunnen daarbij worden betrokken.
De kansen liggen er zowel voor de organisatie als de auditor. De organisatie krijgt door het combineren van data uit de verschillende systemen verrijkte gegevens waardoor een meer gerichte marktbenadering mogelijk is. De auditor kan door het combineren van data verbanden en/of juist geen verbanden, gaten vinden die nader moeten worden onderzocht. Het risico kan zijn dat door de verrijking niet meer wordt voldaan aan de Wet bescherming persoonsgegevens (Wbp). Het ontginnen van deze big data is een uitdaging die investeringen vergt in de vorm van aanpak, tooling en techniek (opslagcapaciteit). In dit kader worden vaak de termen business intelligence en datamining genoemd als aanpakken om de big data te ontginnen.

BYOD
BYOD staat voor: bring your own device. Steeds meer medewerkers stellen het op prijs als zij ook zakelijk hun eigen apparatuur kunnen gebruiken. Voor de organisatie brengt dat

voor- en nadelen met zich mee. De voordelen zijn dat de medewerker prettig kan werken met zijn eigen apparatuur, die hij ook zal koesteren en waar hij zuinig op is. Dit brengt uiteraard besparingen in de aanschaf van apparatuur met zich mee.
Het beheer om de verschillende soorten randapparatuur (Windows, Apple, Android, et cetera) veilig toegang te verlenen tot de bedrijfsapplicaties en bedrijfsdata zal bijzondere aandacht vergen. Deze aandachtspunten hangen samen met de beveiliging om te voorkomen dat de data op straat komen te liggen bij verlies of diefstal. In de praktijk zien we dat organisaties BYOD ondersteunen en dat ook faciliteren door het goed beveiligen van deze apparatuur (toegangsbeveiliging en encryptie van de data). Er zijn steeds meer particuliere en zakelijke mogelijkheden voor de beveiliging van de smartphone en de tablet beschikbaar. Naast het faciliteren van de medewerkers met goede beveiligingsfaciliteiten, moet de organisatie werken aan de bewustwording van de medewerkers de beveiliging toe te passen en alert te reageren bij incidenten (hacking, diefstal, vermissing, et cetera).

Cloud computing en outsourcing
Cloud computing en outsourcing liggen in elkaars verlengde. Cloud computing kan worden gezien als een verregaande variant van outsourcing. Het verschil zit er vooral in dat de gebruiker bij cloud computing niet concreet weet op welke locatie, in welk land of werelddeel zijn data staan. Dat kan Nederland, maar ook Polen, India of VS zijn.
Had vroeger vrijwel ieder bedrijf zijn eigen servers, tegenwoordig komt het steeds vaker voor dat een of meer IT-services via de cloud worden betrokken. De voordelen voor de organisatie zitten in de kostensfeer: geen serverruimte en minder eigen medewerkers voor IT-beheer nodig. De risico's liggen vooral op het terrein van de vertrouwelijkheid (privacy en bedrijfsgeheim) en de continuïteit van de dienstverlening.
De maatregelen beginnen bij de selectie van een betrouwbare dienstverlener, die ook goed aandacht heeft geschonken aan het beheersen van de risico's met betrekking tot de vertrouwelijkheid en continuïteit. Een mogelijke maatregel bij het vertrouwelijkheidsrisico is dat er wordt gewerkt met versleutelde data (encryptie). Voor de continuïteit moet er een betrouwbare uitwijk zijn waar minimaal dagelijks de data worden geactualiseerd en die regelmatig (bijvoorbeeld tweemaal per jaar) wordt getest. Ook voor de langere termijn moet aan de continuïteit worden gedacht, bijvoorbeeld een bewezen exitstrategie in geval van de overgang naar een andere dienstverlener. Voor belangrijke processen zal een ISAE 3000- c.q. ISAE 3402-verklaring worden verlangd van de dienstverlener over de beheer- en verwerkingsprocessen die hij ten dienste van de opdrachtgever uitvoert.

Internet en cybercrime
Internet is een voorziening die al geruime tijd beschikbaar is, maar wordt hier meegenomen omdat de communicatie met internet en de zakelijke transacties via internet een steeds grotere vlucht nemen. Hierdoor wordt internet steeds aantrekkelijker voor criminelen die zich daar ten koste van derden verrijken: de cybercriminelen.
Dit onderwerp sluit aan op het hiervoor behandelde onderwerp Apps. Naast de bewustwording om goed om te gaan met de gebruikersnamen en wachtwoorden spelen de technische beveiligingsmaatregelen die ongewenste toegangspogingen (phishing en DDoS-aanvallen) detecteren en zoveel mogelijk trachten te voorkomen. Firewalls, virusscanners en dergelijke moeten hieraan bijdragen.
Recente aanvallen op Nederlandse banken tonen aan dat cybercrime een weerbarstige problematiek is die bij voorkeur gezamenlijk door de overheid en het bedrijfsleven (zowel nationaal als internationaal) moet worden aangepakt. Recent

heeft minister Opstelten in dit kader een nieuw wetsvoorstel gedaan om de aanpak van de computercriminaliteit te versterken. De politie zal na aanname van dit wetsvoorstel meer mogelijkheden krijgen om binnen te dringen in de computers van verdachten van cybercrime om zo bewijslast te verzamelen. Hopelijk gaat hier een preventieve werking van uit. Maar de bestrijding van cybercrime moet internationaal, want cybercrime overstijgt de landsgrenzen.

Het nieuwe werken

Het nieuwe werken wordt ook wel plaats- en tijdonafhankelijk werken genoemd en heeft een relatie met BYOD. Het nieuwe werken wordt veelal ook toegepast om efficiencyvoordelen te behalen, omdat door flexibeler werken het aantal medewerkers dat gelijktijdig op kantoor is daalt en daardoor ook het aantal benodigde werkplekken teruggebracht kan worden (en flexplekken ontstaan).

Een aandachtspunt is dat het nieuwe werken niet alleen als een technisch vraagstuk wordt aangevlogen, maar ook als een onderwerp dat aandacht verdient vanuit organisatorische (verandermanagement), personele en sociale aspecten. Door het uitrollen van een gedragscode kan gericht gewerkt worden aan het ook op een andere locatie vertrouwelijk en veilig omgaan met de bedrijfsgegevens. Daarbij is het belangrijk dat medewerkers met elkaar afspreken hoe gezamenlijk invulling gegeven kan worden aan dit concept: wat werkt wel en wat werkt niet?

Social media

Onder social media worden de communicatieplatformen verstaan waarmee personen en organisaties zich via internet kunnen manifesteren. Voorbeelden hiervan zijn LinkedIn, Facebook, Twitter en YouTube. Steeds meer organisaties die diensten en artikelen leveren aan de consumentenmarkt willen ook via bijvoorbeeld Facebook in contact kunnen treden met die consument. In het hedendaagse communicatiebeleid nemen de social media een steeds meer prominente plaats in. De risico's zijn dat personen door hun (privé-)uitingen via social media bewust of onbewust hun organisatie in diskrediet brengen of anderszins schaden.

Een maatregel om duidelijkheid te verschaffen en risico's in te perken is dat de organisatie een gedragscode afspreekt met haar medewerkers hoe om te gaan met social media en toeziet op de naleving van deze code.

De bijdrage van de internal auditor

De informatietechnologie zal steeds verder toepassingen vinden in zowel de primaire bedrijfsprocessen als in de ondersteunende processen. Het succes van een organisatie zal meer afhankelijk worden van de mate, de snelheid en de kwaliteit waarmee die nieuwe technologie toegepast wordt.

De internal auditor kan hier een goede bijdrage leveren. Enerzijds door de organisatie tijdig te wijzen op de kansen die de nieuwe technologie met zich meebrengt, anderzijds door aan te geven hoe deze nieuwe technologie zo beheersbaar mogelijk geïmplementeerd kan worden. Iedere internal auditor doet zelf in zijn dagelijkse privé- en zakelijke gebruik steeds meer ervaring op met deze nieuwe technologie. Wel zal hij zich meer moeten verdiepen in de risico's en de beheersing van de risico's die samenhangen met die nieuwe technologie (beleid, risicomanagement en beheersing).

De volgende stappen kunnen worden onderkend bij de beheersing van de IT-trends:

1. Het start met een inventarisatie van de voor de organisatie relevante IT-trends en de daarmee samenhangende risico's. Dit vormt een van de inputs voor het auditjaarplan. In het auditjaarplan moet in dit kader aandacht worden geschonken aan de IT-trends die op korte termijn relevant zijn voor de organisatie, met daarbij een onderbouwing van de risico's.
2. In overleg met het management kan dan worden bepaald welke IT-trends voor de organisatie de grootste risico's vormen en waar de internal auditor zijn aandacht op zal richten bij de beheersing van die risico's.
3. Bij het onderzoek naar de daadwerkelijke beheersing is een taak weggelegd voor de IT-auditor. De IT-auditor kan zich naast de generieke ondersteuning vooral richten op meer diepgaande, meer specialistische onderzoeken naar bijvoorbeeld de daadwerkelijke beheersing van de onderkende risico's alsmede de benodigde informatiebeveiliging.
4. Het rapporteren aan het management over de mate van beheersing van de IT-risico's.

De internal auditor zal proactief de uitdaging aan moeten gaan om de organisatie te ondersteunen bij het beheersen van de uitdagingen en de risico's die de IT-trends met zich meebrengen. <<

Noot

1. Op de website van IIA is een overzicht van relevante websites en artikelen opgenomen waarmee de lezer dieper op een specifieke trend kan ingaan.

Reageren op dit artikel...

p.j.m.goeyenbier@minfin.nl

Piet Goeyenbier is werkzaam als auditmanager bij de Auditdienst Rijk (ADR) van het ministerie van Financiën. Hij is lid van de Commissie Vaktechniek van IIA Nederland. Verder is hij als extern deskundige betrokken bij de AITAP (post-master IT-audit) opleiding aan de Amsterdam Business School (UvA) en penningmeester van Ngi Regio Den Haag. Dit artikel is geschreven op persoonlijke titel.