

ARTIKELN | 1 JULI 2019

FOCUS OP ESSENTIËLE ZAKEN IN IT-AUDITS

Auteur: Robert Metsemakers

Beeld: Adobe Stock - pexels - Janna Hamra

Leestijd: 6 min



Dit artikel is eerder gepubliceerd op deitauditor.nl.

Waar let je op als je de kwaliteit van informatiebeveiliging wilt verbeteren of op het reeds hoge niveau wilt houden? Let je op het ontbrekende deel in de beheersmaatregelen of juist op wat wél aanwezig is? Focus is meestal goed, maar richt daarbij de aandacht dan wel op de juiste onderwerpen.

Britse vliegtuigen bombardeerden en beschoten in de Tweede Wereldoorlog steden in nazi-Duitsland. Ze werden zelf ook geraakt, door vliegtuigen en luchtafweergeschut – de nazi's verdedigden immers hun burgers, militairen, handel en industrie tegen deze aanvallen. Alle Britse vliegtuigen werden daarom bij terugkeer op de vliegvelden in het Verenigd Koninkrijk nauwkeurig onderzocht en de bepantsering werd verstevigd. Maar de geallieerden hadden er enige tijd plus het inzicht van wiskundige, statisticus en econoom Abraham Wald voor nodig, om in te zien dat het verstevigen juist moest gebeuren op de plaatsen waar de vliegtuigen niet geraakt waren. Want de geraakte plaatsen, zichtbaar aan de kogelgaten of aan de geheel weggeschoten delen, waren duidelijk niet essentieel om terug te kunnen keren naar de vliegbasis. Juist de niet-geraakte delen hadden het teruggekeerde vliegtuig gedragen.

AUDIT

MAGAZINE



Hel en verdoemenis... niet dus

Laten we nu eens een te auditen afdeling of proces vergelijken met het vliegtuig, en de auditor oneerbiedig met het luchtafweergeschut. De auditor raakt in zijn audit of onderzoek het vliegtuig en zet een flink aantal bevindingen als kogelgaten op papier. Die bevindingen verschillen onderling in omvang, plaats, invloed op het 'vliegtuig' en daarmee in hun belang. Elke auditor weet dat bij gerapporteerde bevindingen die niet urgent, dringend, of belangrijk worden genoemd, de aandacht van de lezer al snel verslapt. Zeker als de auditee toch al te weinig tijd heeft of neemt om het hele rapport te lezen en zich daarom beperkt tot de aanbevelingen op de bladzijde met de managementsamenvatting. De belangrijkste bevindingen komen immers in de managementsamenvatting en de enigszins belangrijke halen enkel het rapport zelf.

De (interne) auditor bespreekt het conceptrapport met de bevindingen met de auditee, er worden per oplosactie realisatiedata en verantwoordelijke personen bepaald en dit alles wordt vastgelegd binnen een actielijst. Sommige bevindingen zijn urgent en moeten snel, binnen drie maanden, worden opgelost. Zo niet, dan gaat het licht uit. Andere zijn iets minder dringend en moeten over zes maanden of een jaar klaar zijn.

Sommige bevindingen zijn urgent en moeten snel, binnen drie maanden, worden opgelost. Zo niet, dan gaat het licht uit

Vaak duurt het echter langer, veel langer dan de vooraf afgesproken periode, om bevindingen op te lossen. Toch blijft het licht ondertussen branden, gaat de tent niet failliet en komen er geen enorme boetes van de toezichthouder. Werkend aan de auditeekant dronk ik ooit champagne omdat een tot urgent bestempelde bevinding, die dus binnen drie maanden opgelost moest worden, reeds zes volledige jaren 'open' op de actielijst stond, terwijl de onderzochte afdeling nog steeds succesvol draaide. Met andere woorden, het vliegtuig vloog nog steeds! Het door de auditor gevonden 'gat' was weliswaar een tekortkoming, maar niet essentieel. De auditor achtte de kans dat het op dat punt fout zou gaan zo groot, dat de bevinding geen drie maanden meer open kon blijven. De auditee hoorde daarin echter alleen de tijdsdruk en prioriteit en niet de mogelijke impact. Als de auditee erin slaagt om toch jarenlang in de lucht te blijven, zonder die urgente bevinding ooit aan te pakken, gaat het tijdsdrukgevoel echter verloren. 'The thrill is gone', zou bluesgitarist B.B. King zingen, want 'the sense of urgency for the auditee' heeft te veel lettergrepen. Het mooiste is wanneer auditor en auditee gezamenlijk de prioriteit van oplossen bepalen en daarbij rekening houden met de impact én de kans op een bedreigende gebeurtenis.

Urgentie van issues in soorten en maten

AUDIT

MAGAZINE

Er kunnen goede en minder goede redenen zijn waarom een auditor vindt dat bepaalde bevindingen urgent zijn en dus als eerste opgelost moeten worden, namelijk omdat ze:

1. zeer riskant zijn door een hoge impact als het fout gaat;
2. zeer riskant zijn door een hoge kans van optreden;
3. noodzakelijk zijn om daarna andere bevindingen goed, goedkoop of snel (slechts twee van de drie zijn tegelijkertijd mogelijk) op te kunnen pakken;
4. niet veel tijd hoeven te kosten en de auditee het gevoel kunnen geven 'dat zijn medewerkers meters maken' met de noodzakelijke verbeteringen.



Reden (a) is de beste motivatie en ook goed te onderbouwen met een inschatting van de mogelijke schade bij optreden. Maar dit onderbouwen moet de auditor dan wel expliciet doen in zijn managementsamenvatting, want anders denkt de auditee dat de bevinding urgent is om reden (b).

Reden (b) is ook een goede, maar de auditor moet daarvoor wel beschikken over een kristallen bol van uitzonderlijke kwaliteit of gewoon uit de losse pols zelf de toekomst kunnen voorspellen. De ingeschatte kans van optreden kun je met statistisch goochelen omrekenen naar een periode waarin de vervelende impact naar verwachting zal gaan optreden, maar wanneer die periode inmiddels meerdere jaren verstreken is (zie het champagnevoorbeeld) worden voortgangsgesprekken over de actielijst tussen auditor en auditee wel een beetje ongemakkelijk. Zeker wanneer de prioritering puur van de kant van de auditor komt en de auditee, achteraf, 'de kans altijd al te hoog had gevonden'.

Reden (c) is misschien wel de beste, maar uiteindelijk ook gebaseerd op een niet al te harde inschatting.

Reden (d) is de politieke of verkoopmotivatie. Wat verkocht wordt is het 'laaghangend fruit' dat misschien niet zo voedzaam of lekker of gezond is als de hoger hangende vruchten, maar je kunt er wel gemakkelijker bij. Het motiveert de plukker dat hij/zij het eerste mandje al snel gevuld heeft. Bijkomend nadeel is dat zo de moeilijke en tijdrovende issues overblijven, wat vervolgens de eerder via deze truc opgebouwde motivatie bij de auditee weer teniet kan doen. Niet de allerbeste reden dus.

Wat verkocht wordt is het 'laaghangend fruit' dat misschien niet zo voedzaam of lekker of gezond is als de hoger hangende vruchten, maar je kunt er wel

gemakkelijker bij

Hoe dan wel?

Begrijp me goed: auditors moeten blijven auditen (lees: schieten op vliegtuigen) en daarbij letten op zaken die niet voldoen aan een voorafgaand vastgestelde set normen. Ook moeten ze die 'foute' zaken en bijkomende urgentie blijven melden. Maar ik zou er graag een lans voor breken onze audits te verrijken door nadrukkelijk ook aandacht te geven aan de niet-geraakte delen van het onderzochte vliegtuig (de wel onderzochte aspecten waar echter geen bevindingen waren). Dat betekent analyseren wat er juist wél goed gaat in de uitvoering van precies die vitale, dus onmisbare delen en daar lessons learned en best practices uit te halen. Want andere auditees met hetzelfde proces kunnen dat proces daarmee vaak verbeteren en/of tijd en geld besparen. Hierbij ga ik uit van de situatie dat een (interne) auditor een proces een aantal keren onderzoekt, zoals in een thema-onderzoek, waarbij hetzelfde proces bij meerdere afdelingen wordt beoordeeld. Er zijn natuurlijk ook audits of onderzoeken gericht op de oorzaak van een groot incident, of met een forensisch karakter waar een dader van een eerdere (moedwillige) foutieve actie moet worden opgespoord. Daar zijn de bevindingen anders van aard en is het lastiger, ook door de noodzakelijke vertrouwelijkheid, om tot elders toepasbare lessons learned te komen.

"Voorspellen is moeilijk, vooral als het om de toekomst gaat", zoals natuurkundige Niels Bohr ons al waarschuwde. Als onafhankelijke buitenstaander kan een auditor soms beter het belang of de prioriteit van een aanbeveling inschatten dan de auditee die verantwoordelijk is voor uitvoering of implementatie ervan. Maar als tegenhanger hiervan moeten we als auditor wel conclusies trekken uit het gegeven dat het 'vliegtuig', ondanks alle in de audit ontdekte werkelijke gaten en tekortkomingen, nog steeds vliegt en terugkeert op de basis.

Natuurlijk moeten we als auditors de auditee blijven helpen door voor en het liefst samen met hem, de bevindingen te prioriteren naar hun belang en ernst. Maar laten we daarbij ook de durf hebben om na enige tijd die inschatting te heroverwegen en dan een nieuwe inschatting en dus nieuwe selectie voor de actielijst te maken: hoe zit het zes jaar later eigenlijk met die destijds tot urgent bestempelde bevindingen, waren die echt allemaal zo urgent? Dat er al die tijd niets vervelends is gebeurd, betekent niet per definitie dat de urgentie aanvankelijk was overschat, maar het stemt wel tot nadenken of het in de audit aangetroffen 'gat' inderdaad een vitaal of essentieel punt in het proces of de onderzochte organisatie is. Dat is waar ik de focus zou willen leggen.

Over

Robert Metsemakers | IT-auditor en informatiebeveiligingsexpert. Hij gaat graag uitdagingen aan op gebieden als de inrichting van informatiebeveiliging, security advies en schrijfp opdrachten op verschillende terreinen.
Robert.metsmakers@gmail.com.

Tags: informatiebeveiliging

Bron url: <https://auditmagazine.nl/artikelen/focus-op-essentiele-zaken-in-it-audits/>