Simpele cybersecurity crisisanalyse verrast:

Risicomanagement
risico's nog niet onderkend

Volgens prof. Paté-Cornell van Stanford zijn er twee soorten incidenten waar regulier risicomanagement tekort schiet en een crisis onvermijdelijk is: 'Black Swans' en 'Perfect Storms'. In dit artikel laten we zien dat een analyse van het DigiNotar incident op basis van dit model leidt tot verrassende conclusies. Deze manier van analyseren helpt bestuurders om te komen tot betere keuzes en een effectievere aanpak na een incident.

Rieks Joosten en André Smulders, TNO

'Black Swans' en 'Perfect Storms'

'Black Swans'[1] zijn gebeurtenissen die niet eerder zijn waargenomen en waarvan dus ook niet bekend is dat ze kunnen voorkomen. 'Perfect Storms'[2] zijn gebeurtenissen die het gevolg zijn van een onwaarschijnlijke samenloop van omstandigheden die elk voor zich bekend en hanteerbaar zijn, maar in hun samenhang een calamiteit opleveren.

Paté-Cornell stelt dat alleen gebeurtenissen die een echte 'black swan' of een echte 'perfect storm' zijn, geëxcuseerd kunnen worden. Andere potentieel risicovolle gebeurtenissen dienen opgevangen te worden in het reguliere risicomanagement proces, dat ervoor moet zorgen dat de gevolgen van zulke gebeurtenissen beheersbaar blijven. Door het bewust of onbewust negeren van beschikbare signalen kunnen gebeurtenissen onterecht bestempeld wordt als een 'black swan' of 'perfect storm' en daarmee onterecht worden geëxcuseerd. Gevolg hiervan is dat er weliswaar actie genomen wordt om de schade te beperken en te herstellen, maar niet dat het falende risicomanagement wordt verbeterd.

De DigiNotar casus

De DigiNotar crisis is hiervan een voorbeeld. Deze crisis ontstond doordat bij een groot aantal partijen dat afhankelijk was van DigiNotar in de problemen kwam toen bleek dat de certificaten van DigiNotar niet langer te vertrouwen waren. Verschillende partijen dreigden de ondersteuning voor deze certificaten in te trekken. Dit escaleerde toen duidelijk werd dat er wellicht sprake zou zijn van het intrekken van steun voor bovenliggende certificaten, waardoor het effect versterkt zou worden. We beperken ons voorbeeld tot de situatie waarin alleen sprake was van het intrekken van de ondersteuning van DigiNotar certificaten.

Een partij die van DigiNotar certificaten afhankelijk was, kan niet claimen dat het intrekken van de DigiNotar certificaten een 'perfect storm' was. Voor die partij was slechts één gebeurtenis relevant, namelijk dat de DigiNotar certificaten werden ingetrokken. Dat dit weer het directe gevolg was van het verliezen van het vertrouwen in het DigiNotar certificaat systeem maakt dit nog geen onwaarschijnlijke samenloop van omstandigheden.

Een dergelijke partij kan ook niet stellen dat het DigiNotar incident een 'black swan' was. Een signaal dat tijdens het ontwerp van de dienst beschikbaar was, is het feit dat de PKI structuur in Nederland uitdrukkelijk specificeert dat certificaten ingetrokken kunnen worden als er reden is om aan te nemen dat ze zijn gecompromitteerd. Een ander signaal, dat tijdens het operatio-

[1] De term 'Black Swan' is ontleend aan een gelijknamig boek van Nassim Taleb, waarin de auteur onbekende gebeurtenissen vergelijkt met de ontdekking van zwarte zwanen door Nederlandse ontdekkingsreizigers in het 17e eeuwse Australië, terwijl in Europa tot dan toe alleen witte zwanen voorkwamen.

[2] De term 'Perfect Storm' is ontleend aan het boek 'The Perfect Storm' van Sebastian Junger, waarin de auteur beschrijft hoe een samenloop van gebeurtenissen die elk goed bekend en hanteerbaar zijn, leidt tot een calamiteit van buitengewone proporties. Het doet denken aan de watersnoodramp van 53, waarin een samenloop van zwakke dijken, een zuidwesterstorm en springtij tot een calamiteit leidden. Dit is vergelijkbaar met de 'Swiss Cheese' metafoor (Reason 1990).

nele leven van de dienst beschikbaar was, is de berichtgeving over (mogelijk) gehackte certificate authorities, zoals Comodo (maart 2011) en StartCom (juni 2011), wat het denkbaar maakt dat ook DigiNotar mogelijk gecompromitteerd zou kunnen worden.

Risico's van risicomanagement

Voor elke partij die een van de (meer dan 10.000) door DigiNotar uitgegeven certificaten gebruikte, hadden deze signalen aanleiding kunnen zijn om na te denken over de gevolgen die dit voor hen zou kunnen hebben. Toen het incident plaatsvond werden ze voor de acute vraag gesteld hoe ze hun dienstverlening moesten continueren bij gebrek aan daarvoor benodigde certificaten. De (imago)schade die veel partijen hebben opgelopen is dan ook volledig toe te schrijven aan het feit dat zij het onverwacht intrekken van certificaten niet als ¬risico hebben aangemerkt en dus ook geen mitigerende maatregelen hebben genomen.
Bovenstaande analyse laat zien dat het falen van DigiNotar de daaropvolgende crisis weliswaar heeft getriggerd, maar niet veroorzaakt. De daadwerkelijke oorzaak van de crisis bestaat uit twee factoren: het missen van signalen die het bestaan van dit soort risicovolle gebeurtenissen (het falen van een CA) aantoont, en het onvoldoende aandacht hebben – zowel in de ontwerpfase als in het operationele leven van systemen – voor het zelfstandig dan wel gezamenlijk optreden van zulke gebeurtenissen en de schade die dit kan veroorzaken.

Het feit dat organisaties signalen missen in hun risicomanagement en de risico's van het optreden van (samengestelde) bekende gebeurtenissen in (IT) systeem¬ontwerpen niet meenemen, is wat ons betreft een duidelijk signaal, namelijk dat de huidige manier waarop deze organisaties hun risicomanagement hebben ingericht kennelijk ongeschikt is om bekende en relevante risico's mee te beheersen.

Volgens Paté-Cornell zou het reguliere risicomanagementproces dit signaal dan ook moeten oppakken, maar bovenstaande analyse laat zien dat het herkennen van en acteren op zulke signalen alles behalve gemeengoed is. Dat lijkt ons een belangrijk risico van het risicomanagement proces. Om dit risico te kunnen adresseren is een nieuwe manier van denken over risico's nodig, en een bijbehorend nieuw risicomanagement proces.

Een mogelijk alternatief

Binnen TNO hebben dit soort gedachten geleid tot een nieuwe aanpak. Deze aanpak neemt de (bedrijfs) doelstellingen (verplichtingen) op de verschillende bestuurslagen als uitgangspunt en beoogt de bijbehorende risico's (van het niet halen ervan) expliciet en bestuurbaar te maken. Enerzijds gebeurt dit door bestuurders aan doelstellingen (en dus risico's) te koppelen en anderzijds door in kaart te brengen waar het welslagen van afhankelijk is en signalen te inventariseren die op mogelijke risico's wijzen. Heldere criteria om vast te stellen wanneer lijsten hiervan compleet zijn, signaleren mogelijke risico's in het risicomanagement proces zelf.
Een andere eigenschap van deze aanpak is dat activiteiten een 'menselijke maat' hebben: managers hoeven alleen hun eigen 'scope of control' te kunnen overzien en de verplichtingen c.q. verwachtingen die zij hebben ten aanzien van anderen (al dan niet binnen de eigen organisatie). Gevolg hiervan is dat ook als zij onderdeel zijn van complexe, genetwerkte samenwerkingsverbanden, zij steeds 'in control' zijn omdat expliciet is gemaakt over welke risico's zij afspraken moeten maken en duidelijk is met wie dat moet worden afgestemd.

Inmiddels is een experiment gestart waarin deze methodiek wordt uitgeprobeerd in de praktijk. Totdat de resultaten van dit experiment bekend zijn, kunnen bestuurders het hier gepresenteerde model van 'Black Swans' en 'Perfect Storms' gebruiken om in geval van een incident te kunnen beoordelen of er eventuele tekortkomingen zitten in hun huidige risicomanagement proces.

Referenties

E. Paté-Cornell, 'On "Black Swans" and "Perfect Storms"': Risk Analysis and Management When Statistics Are Not Enough', in: *Risk Analysis*, 32 (2012), 1823–1833.
J. Reason, 'The Contribution of Latent Human Failures to the Breakdown of Complex Systems', in: *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences* 327 (1990-04-12, 1241), 475–484.