Hierbij een reactie van mij persoonlijk en dan gaat het er mij in het bijzonder om ‘waar hebben we precies mee te maken bij certificatie’. Ik ben zelf 15 jaar security manager in de ICT geweest en heb meegewerkt met de voorbereidingen voor de Commissie Franken bij de wetswijziging computercriminaliteit van 1993. Dit als achtergrond voor u.
Een strategische opmerking is of men hiermee niet de standaard verplichting voor een incident, waar iedereen zich aan te houden heeft voor de certificaten, opnieuw aan het specificeren is. Als die er is, dan dient de CA, bedoeld wordt de Certification Authority, zich aan die verplichting te houden. Is die er niet dan moet je overwegen of niet een standaard meldplicht voorschreven moet worden ipv. deze exclusieve versie.
Goed is te weten dat wat hier beschreven wordt geen security of integriteit betreft maar ‘controle’, immers de security noch de integriteit wordt hier verbeterd, wel de controle . Voor het gezamenlijke beeld heb ik een kopie bijgevoegd uit een leerboek van mij o.a. over de volgorde bij een incident: dit verloopt van preventie via detectie naar repressie en correctie (Beveiliging bij Datacommunicatie, 1989).
[redacted] de CA zich bij een incident ook aan deze stappen houdt, om [redacted]ri het incident verplicht te melden ongeacht of de [redacted] het maar helemaal de vraag of de toezichthouder voldoende operationele bevoegdheden heeft om beheersmatig te interveniëren zoals bedoeld. Ik denk ook niet dat de toezichthouder elke stap uitvoert maar de CA zelf.
Het is goed om te beseffen dat informatie wel een goed betreft maar dat de empiriek rondom informatie dusdanig troebel is dat van een één-op-één afbeelding van analoog op digitaal geen sprake kan zijn. Zo is het stelen van informatie slechts het kopiëren daarvan, want de informatie blijft achter namelijk. Men steelt informatie door die te wijzigen, immers de bron is dan niet meer aanwezig. In de analoge wereld raakt een gestolen document inherent ook zoek en bij een wijziging in een document blijft het document toch aanwezig en bij het kopiëren van een document raakt men hooguit het stelen van copyright, dus daarin verschilt een analoog goed met een digitaal goed.
Waar gaat het nu om, gaat het om de snelheid of gaat het om de impact. Let wel, u bdrijft hier gewoon een stukje risicomanagement, welnu kies dan om vanuit die optiek te gaan en benoem het ook zo.
Ik heb opgelet of er nu vanuit het pure incident (is gemakkelijker) voorschreef of ook vanuit ‘het vermoeden van’ en dat laatste is een risicoanalyse benadering. Immers met de huidige dreiging van de Chinese staatshackers b.v. kan men bij het openstaan van toegangscontrole gevoeglijk aannemen dat dit altijd gehacked is.
Overigens zal het lastig blijken om vanuit de beveiliging van informatie te praten, dit omdat het meestal om de beveiliging van de systemen gaat. Dus een lek is een lek in je systemen en niet in je informatie, terwijl die juist wel gecompromitteerd raakt.
Over het feit of u over het incident praat of over het risico kunnen we kort zijn want zo wordt het gigantisch lastig. Het openstaan van beveiliging betreft namelijk geen incident, dus dat hoef je niet te melden, terwijl dat welde bedoeling is. Dit is namelijk niet hetzelfde als een deur die open staat, dat kan men juist wel melden. Het is vaak nog een probleem om aan te tonen dat het lek niet alleen is gevonden door de hacker maar belangrijk is of er ook valse zelfverrijking mee is verricht. Criminaliteit is als dan wel vastgesteld.
Als gedaan wordt wat gesteld is dan zou je ook een gelukte tigerteam attack moeten melden, dus met ethical hackers (zijn die er dan?) aan de toezichthouder. Deze zal dat niet waarderen als er slechts iets ergens en te veel openstond. Overigens als er iets openstaat, neem dan gevoeglijk aan dat het gehacked is tegenwoordig en daar heeft men dan geen idee van, dat is nu ook zo. Maar ga dus maar uit van een risicobenadering, dus niet ‘hoe groot is de impact’, maar hoe groot is het risico (met alles wat daarbij hoort).
INHOUDELIJK
Blz.3 Virussen behoeven op zich niet actief te zijn geweest, maar het maakt wel verschil als dat zo is. Het gaat eerder over ‘het vermoeden van … inbreuk bv’ en specificeer dan wel dat het uit een rapportage stamt die formeel is, bedoeld wordt b.v. een auditrapportage.
Blz.3 dat NCSC nu bij het ministerie van Veiligheid behoort is niet wezenlijk. Als NCSC wordt geïnformeerd en vervolgens aan de minister gemeld dient te worden(wie dat ook is op een gegeven moment), benoem dat dan ook zo. Veiligheid is hier toevallig de gastheer voor NCSC maar dat kan volgende maand anders zijn.

Blz.6 Bij het preciseren is het noemen van voorbeelden zoals hier ‘een klein aantal certificaten gecompromitteerd’ geeft een grote kans voor verwarring. Benoem het volgens de risicoanalyse als Klein, Midden. Slechts bij Groot is het vervolgens meldingsplichtig. Dat er geen universele risico-schaal is doet niet ter zake in de praktijk, zolang er maar een risicoanalyse is.
Tot zover mijn reactie,
Vriendelijke groet en succes
Rob van den Boom MIM
Het Kasteel 758
7325PZ Apeldoorn
0654 614930
r.vandenboom1@chello.nl