OP WEG NAAR VOLWASSENHEID IN INFORMATIEBEVEILIGING

ISO 27001

De vraag naar verantwoording en transparantie over informatiebeveiliging, die voorheen vooral intern gericht was, groeit en zal naar verwachting blijven groeien, zowel intern als extern. In Duitsland moeten energiebedrijven inmiddels verplicht aantoonbaar in control zijn middels een certificering conform ISO 27001. Deze norm kan – voorafgaand aan en los van certificering – ook als leidraad fungeren om de informatiebeveiliging op hoger plan te brengen.

door Ivo Kouters, Johannes van Luijk, Paul Bloemen

IT WORDT ALGEMEEN GEZIEN ALS GROTE ENABLER, maar informatiebeveiliging heeft het stempel van kostenpost en vervelende beperking. Terwijl informatiebeveiliging juist duidelijkheid kan bieden ten aanzien van de risico's rondom de informatievoorziening. De sleutel ligt in de beleving van het onderwerp, men ziet informatiebeveiliging als:

Onduidelijk veelkoppig monster: Informatiebeveiliging omvat een veelheid van ongelijksoortige onderwerpen, zoals netwerken, datacenters, servers, werkplekken en toepassingen, en ook wetgeving, medewerkers en leveranciers. Dit kan ontmoedigend werken en na verloop van tijd de vraag oproepen of er niet al genoeg aan informatiebeveiliging wordt gedaan.

Hinderlijk: De meeste mensen ervaren informatiebeveiliging als hinderlijk, soms zelfs schadelijk voor een effectieve bedrijfsvoering. Het is moeilijk maatregelen te formuleren die zowel de bedrijfsbelangen dienen als aan de eisen van informatiebeveiliging voldoen.

Virtueel probleem: Dankzij goede informatiebeveiliging doen zich binnen de organisatie relatief weinig incidenten voor. Het beeld kan ontstaan dat men onkwetsbaar is. De noodzaak van maatregelen en gedrag wordt dan niet ingezien.

Extra kosten: Informatiebeveiliging wordt als extra kostenpost gezien omdat het binnen IT-projecten vaak onvoldoende onderdeel is van de initiële eisenspecificaties. Bovendien zijn die eisen vaak in algemene termen geformuleerd, waardoor de consequenties ervan niet tijdig duidelijk zijn.

Technisch complex: Informatiebeveiliging vraagt om expertise. De gedachtewereld en taal van deze specialisten sluit niet aan bij die van het management. Dit bemoeilijkt de communicatie en besluitvorming aangaande de maatregelen.

Een bijzaak: De voor informatiebeveiliging verantwoordelijke information security manager heeft vaak geen eigen budget.

Buiten de comfort-zone: Verantwoording en transparantie. Dat betekent immers dat de organisatie onder een vergrootglas komt en extern geformuleerde eisen moeten worden geaccepteerd. Voor een certificering moeten waarschijnlijk additionele maatregelen doorgevoerd worden, hetgeen tijd en geld kost. Zeker als de voordelen van certificering voor de kwaliteit van de informatievoorziening niet duidelijk zijn, zullen veel organisaties van certificering afzien.

In dit artikel stellen wij een stappenplan voor die bovengenoemde belemmeringen zo veel mogelijk wegneemt.

1 RISICOANALYSE

Om niet lukraak beleid toe te passen is het nodig om risico's in kaart te brengen en bewustwording op het niveau van management te realiseren. Voer een risicoanalyse uit en betrek hierbij alle personen die verantwoordelijk zijn voor de informatievoorziening.
In deze analyse moet aandacht zijn voor de manier waarop de bedrijfsprocessen met informatie omgaan, de door hen gebruikte toepassingen, de infrastructuur waarop ze draaien en de processen en procedures voor de informatievoorziening. Beschrijf voor elk van deze gebieden welke bedreigingen de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening in gevaar kunnen brengen.
De risicoanalyse vormt het uitgangspunt voor de beveiligingsmaatregelen. Geef voor elk in de risicoanalyse geïdentificeerde bedreiging aan welke maatregelen al zijn getroffen op de gebieden organisatie, mens en techniek. Maak hierbij onderscheid tussen vier soorten maatregelen:

- **Preventief:** incidenten voorkomen,
- **Detectief:** incidenten zo snel mogelijk te signaleren,
- **Repressief:** schade zo snel en zoveel mogelijk beperken,
- **Correctief:** de oorzaak wegnemen.

Geef voorts aan welke verdere maatregelen zullen volgen en beoordeel zowel inhoudelijk als financieel, op basis van het geschatte schade van de bedreigingen en de kosten van de maatregelen, of de risico's adequaat worden gemitigeerd.
Doordat het management van de organisatie de risicoanalyse beoordeelt en goedkeurt wordt een eerste stap gezet op het gebied van de bewustwording: het management krijgt zicht op zowel de belangrijke risico's als de hiertegen noodzakelijk geachte maatregelen.

> "Om niet lukraak beleid toe te passen is het nodig om risico's in kaart te brengen en bewustwording bij het management te realiseren."

AUTEURS

IVO KOUTERS
ivo.kouters@kouters-vandermeer.nl is prestatieverbeteraar bij KoutersVanderMeer.

PAUL BLOEMEN
p.a.bloemen@home.nl is information security officer bij Gasunie en heeft alle in dit artikel genoemde stappen doorgevoerd, wat heeft geresulteerd in een eerste certificering conform ISO 27001 in 2015.

JOHANNES VAN LUIJK
johannes.vanluijk@koutersvandermeer.nl is adviseur beleid, techniek en security bij KoutersVandermeer.

2 RICHTLIJNEN

Wanneer vaststaat welke maatregelen volgen, worden zij concreet gemaakt in het informatiebeveiligingsbeleid (information security policy). Maak hiertoe een lijst van alle maatregelen en stel concrete richtlijnen op die eisen stellen aan de verschillende aspecten van die maatregelen. Doel hiervan is het draagvlak, de aantoonbaarheid en de volledigheid te waarborgen.
Draagvlak betreft het creëren van bewustwording van en commitment aan informatiebeveiliging. Betrek hiertoe IT-professionals en eindgebruikers bij het vaststellen van het informatiebeveiligingsbeleid.
Aantoonbaarheid betreft het opstellen van beheersmaatregels die concreet en meetbaar zijn en in een richtlijn kunnen worden verwoord. Neem tevens in een vroegtijdig stadium kennis van de best-practice-richtlijnen en -maatregelen (ISO 27002), die als voorbeeld en inspiratie voor concrete richtlijnen kan worden gebruikt.
Volledigheid betreft de zekerheid dat de maatregelen de organisatie beschermen tegen alle relevante risico's ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.

3 CONTROLE EN RAPPORTAGE

Informatiebeveiliging is alleen dan effectief wanneer wordt getoetst dat conform de richtlijnen wordt gehandeld. Stel vast van welke richtlijnen naleving moet worden getoetst. Maak daarin onderscheid tussen:

- **Cruciale richtlijnen:** Richtlijnen die bij onvoldoende naleving een groot risico voor de organisatie betekenen. De rapportage hierover vormt de basis voor de KPI-rapportage over informatiebeveiliging aan het hogere management.
- **IT-projecten:** Een project dient aan te geven hoe het zich conformeert aan de richtlijnen en hoe het omgaat met afwijkingen. Controle en rapportage betreft het tijdig opleveren en goedkeuren van het conformiteitsdocument.
- **Toepassingen en infrastructuur:** De doorvoering van de richtlijnen voor beheer van toepassingen en infrastructuur kan in de loop van de tijd teruggelopen zijn. Controle en rapportage betreft de kwaliteit van de doorvoering van de richtlijnen.
- **Tests:** De twee belangrijkste tests zijn de disaster recovery test en de ethical hack. De disaster recovery test is bedoeld om na te gaan of de voorzieningen voor continuïteit daadwerkelijk functioneren. Bij een ethical hack worden de maatregelen voor informatiebeveiliging in de praktijk getest om vast te stellen of zij afdoende robuust zijn.

Ten aanzien van deze toetsing moeten afspraken worden gemaakt over de corresponderende controle- en rapportagetrajecten. Leg richtlijnen vast ten aanzien van onder meer de frequentie, de te hanteren norm en eventuele opvolging.

4 HANDLEIDING INFORMATIEBEVEILIGING

Stel een handleiding op waarin de governance wordt vastgelegd. Deze governance moet waarborgen dat het informatiebeveiligingsbeleid adequaat is en effectief wordt toegepast. Neem hiertoe kennis van ISO 27001 en houd voor de handleiding de indeling van ISO 27001 aan. Dit bestaat uit twee componenten:

1. Een cyclus van continue verbetering
2. De verankering van informatiebeveiliging in de organisatie.

Organisaties, hun processen, de behoefte aan informatievoorziening en de technische mogelijkheden ten aanzien van informatiebeveiliging zijn constant in ontwikkeling. Monitor periodiek of het huidige informatiebeveiligingsbeleid goed functioneert. Maak hiervoor gebruik van een cyclus op basis van ISO 27001. Naast de cyclus dient ook de verankering van de organisatie van informatiebeveiliging in de handleiding vastgelegd te worden.

- **Context en scope:** de business- en IT-processen die onderhevig zijn aan informatiebeveiliging, en de interne en externe partijen die zijn.
- **Commitment:** de wijze waarop van de leiding goedkeuring verkregen wordt voor het informatiebeveiligingsbeleid en voor de activiteiten om maatregelen afdoende door te voeren.
- **Rollen en verantwoordelijkheden:** het organisatorische raamwerk van het proces en de wijze waarop hierover verantwoording wordt afgelegd.
- **Competenties:** de eisen op het gebied van opleiding en vaardigheden van personen en organisaties die delen van het proces informatiebeveiliging uitvoeren.
- **Middelen:** de wijze waarop financiële middelen beschikbaar gesteld worden om het beleid uit te voeren. De belangrijkste bron hiervoor zijn de maatregelen die in de risicoanalyse informatiebeveiliging worden aangegeven. Vaak heeft het proces informatiebeveiliging geen eigen budget en moet gebruik gemaakt worden van de budgetten van de IT-processen.
- **Bewustwording:** de planmatige, continue inspanning om medewerkers, management en IT-specialisten kennis te geven over risico's en gewenst gedrag aangaande informatiebeveiliging. Meet de resultaten van de inspanning, rapporteer hierover aan het management.

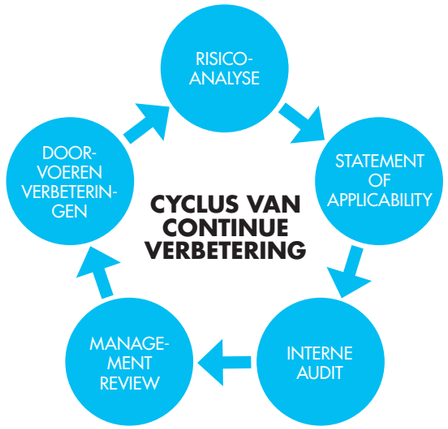
CERTIFICERING IN FASEN

Veel organisaties zien op tegen de omvangrijke operatie waarin de organisatie audit-ready wordt gemaakt en geaudit. Voer het certificeringstraject daarom gefaseerd uit:

• Nulmeting: Een proefcertificering met als doel op basis van ISO 27001 de sterke en de zwakke punten boven water te krijgen. Een organisatie kan tijdens de nulmeting wennen aan certificering en de zwakke punten wegnemen.

• Eerste certificering: Een ISO 27001 certificering kan voor een beperkte scope van een organisatie uitgevoerd worden. Kies hiervoor een organisatiedeel dat de organisatie sterk in de greep heeft waardoor men snel afspraken kan maken en acties kan doorvoeren. De organisatie krijgt een beperkte periode om eventueel gevonden tekortkomingen weg te werken, waarna certificering volgt.

• Vervolgcertificeringen: Met de ervaring van de eerste certificering kan de certificering van andere processen beginnen. Aangezien bekend is welke eisen aan de certificering gesteld worden, kunnen deze in de aanloop van de vervolgcertificering met de betrokkenen besproken worden. Op basis hiervan kunnen verbeterende acties ondernomen worden. Na iedere fase kan bezien worden of, en voor welke onderdelen een volgende fase nodig is.



Risicoanalyse informatiebeveiliging: Gebruik formele en door de organisatie gehanteerde methodes voor het uitvoeren van de risicoanalyse, het waarderen van risico's en het accepteren van restrisico's, het goedkeuren van de risicoanalyse door het management, en de opvolging van de risico's.
Statement of Applicability: Toon aan welke normen van ISO 27002 van toepassing zijn en welke niet: in het laatste geval moet aangegeven worden waarom niet. Het Statement of Applicability moet door het management formeel goedgekeurd worden.
Interne audit informatiebeveiliging: De organisatie moet zich er formeel van vergewissen dat de cyclus voor informatiebeveiliging conform de eisen van ISO 27001 doorlopen wordt. De auditerende partij moet gecertificeerd zijn voor het uitvoeren van ISO 27001-audits.
Management review: Het management dient zich ervan te overtuigen dat het proces informatiebeveiliging goed doorlopen wordt.
Doorvoeren van verbeteringen: Uit alle hierboven genoemde onderdelen van de cyclus komen acties ter verbetering voort. De uitvoering van deze acties dient bewaakt te worden, over de voortgang ervan moet worden gerapporteerd.

5 VERANTWOORDING EN TRANSPARANTIE

Als laatste stap naar volwassenheid kan een organisatie besluiten de informatiebeveiliging door een externe partij te laten toetsen, bijvoorbeeld met een certificering conform ISO 27001. ISO 27001 certificering wordt uitgevoerd door een formeel daartoe geaccrediteerde instantie. De certificering gebeurt in een drietal slagen: na de initiële certificering wordt na één en na twee jaar een verder verdiepend onderzoek uitgevoerd, waarbij bij goed gevolg het certificaat verlengd wordt.

CONCLUSIE

Door ISO 27002 te gebruiken om de risico's van de organisatie te beheersen en aan ten sluiten bij de best practice uit ISO 27001, kan een organisatie efficiënt en effectief op aantoonbare wijze niet te weinig, maar ook niet te veel doen. Jaarlijks terugkerende evaluatie- en verbetermomenten zijn de stok achter de deur waardoor het bouwwerk in goede staat blijft.