Aangeboden door 12Secure-U

Inhoudsopgave

Waarom 12Secure-U ®

Virtualisatie, Mobility, Cloud, Datacenter, VoIP, diensten, Outsourcing, consolidatie, centralisatie van IT solutions, authenticatie voor Cloud applicaties. Zo maar enkele zaken waar uw dagelijks mee in aanraking komt.

Deze processen stellen vaak nieuwe eisen aan de inrichting van netwerk- en security infrastructuur.

Heeft u zich wel eens afgevraagd hoe veilig uw bedrijfsdata eigenlijk is? Weet u zeker dat hackers of andere ongenode gasten geen toegang hebben tot uw IT-omgeving, vol met persoonlijke gegevens, essentiële bestanden en andere gevoelige bedrijfsinformatie?

12Secure-U ® speelt in op de toenemende behoefte van bedrijven van groot tot klein om de beveiliging van hun bedrijfsnetwerk te laten onderzoeken. Wij zijn actief in verschillende sectoren zoals de publieke sector, non-profit organisaties, financiële dienstverlening, zorgsector en industrie.

Wij zijn een professionele speler in de IT Security, met jarenlange ervaring op het gebied van cybercrime, security audits en netwerkbeveiliging. Middels een samenwerking tussen 4 organisaties zijn wij experts op het gebied van gebied van Data Protection, Security, Privacy, en Informatisering. Vanuit die specialisaties adviseren wij bedrijven over de kwaliteit van hun ICT.

Als security specialisten weten wij als geen ander hoe belangrijk het is om security op het hoogste niveau te houden. Door de complexiteit, snelle ontwikkelingen op security gebied en het aantal, snel van aard veranderende bedreigingen; nemen de risico's alleen maar toe.

Veel bedrijven zijn genoodzaakt over te gaan tot een ISO certificaat. Een traject waar vaak erg tegenop wordt gezien; hiermee kunt u wel aan uw klanten en relaties laten zien dat u continu werkt aan kwaliteit, verbetering van processen, producten, diensten en mensen.

Met 12secure-u heeft u de partner gevonden met jarenlange ervaring in het opzetten van verschillende ISO omgevingen; geschikt voor alle organisaties, groot of klein en in alle marktsegmenten, commercieel, overheden, non-profit organisaties etc.

Onze professionele IT-auditors, projectleiders en consultants kunnen zich snel in uw bedrijfsprocessen inleven en kunnen u daardoor in een kort tijdsbestek deskundig bijstaan. Daarmee biedt 12secure-u de instrumenten voor het optimaliseren van de beveiliging en prestaties van uw organisatie.

De rode draad van het verhaal is dat wij u helpen een nieuw, beter beveiligingsbeleid te ontwikkelen dat de organisatie steunt in de bescherming van haar kostbaarste bezit, zoals confidentiële persoonsgegevens of intellectueel eigendom.

Meldplicht datalekken

Veel organisaties stellen zichzelf de vraag wat ze nu precies moeten doen en of het mogelijk is om onder de wet uit te komen. Dit is niet mogelijk, maar wel kan door goed beleid de impact worden beperkt, “En als je ook je ketenaansprakelijkheid borgt door bewerkersovereenkomsten met leveranciers te sluiten, dan heb je juridisch gedaan wat je kunt.” Een andere veel gestelde vraag is wanneer moeten bedrijven nu precies data-lekken melden en wanneer is er sprake van 'ernstige nadelige gevolgen', zoals in de meldplicht is opgenomen. De meldplicht is in eerste instantie bedoeld voor de verantwoordelijke van de database".

Ook vanwege de overeenkomst “Safe Harbour” hebben organisaties veel vragen over de noodzaak van een bewerkersovereenkomst. Artikel 14 van de Wet bescherming persoonsgegevens verplicht organisaties om met leveranciers, die in opdracht van hen persoonsgegevens verwerken, een dergelijke overeenkomst te sluiten. In de bewerkersovereenkomst worden de verantwoordelijkheden en plichten vastgelegd maar worden ook de aansprakelijkheid en beveiliging geregeld.

Men denkt dat de Autoriteit Persoonsgegevens niet meteen boetes uitdeelt en in eerste instantie vooral waarschuwt. "Voor een boete is vereist dat men opzettelijk of grof nalatig handelde. Bij een data-lek dat redelijkerwijs niet kon worden voorkomen, zal dus geen boete kunnen volgen. Wie geen beleid heeft, is per definitie grof nalatig, zo staat in die richtlijn."

De boetes mogen dan misschien uitblijven, maar verwacht mag worden dat door de nieuwe meldplicht veel datalekken die tot voor kort onder de radar bleven, nu in de openbaarheid gaan komen. "Dat is misschien pijnlijk voor een bedrijf, maar op de lange termijn nuttig - want het is nog veel pijnlijker als klanten er via andere bronnen achter komen dat hun data is gelekt."

Door de meldplicht zullen bedrijven genoodzaakt worden hun beveiliging tegen het licht te gaan houden. Ook de Autoriteit Persoonsgegevens noemt dit preventieve effect een belangrijk onderdeel van de meldplicht.

Tips

- Maak beleid, waarin je vastlegt hoe datalekken intern moeten worden gemeld en wie er besluit naar de Autoriteit Persoonsgegevens te stappen. Maak ook procedures die dit uitwerken, zodat de documentatie op orde is (welke dingen vastleggen, wie bewaart dat en hoe is het inzichtelijk). Documentatie moet worden verschaft aan de Autoriteit immers.
- Dwing bij leveranciers van tools garanties af ten aanzien van datalekken. Verhoog hun aansprakelijkheid voor bugs die datalekken veroorzaken, of laat ze opdraaien voor de kosten van een security audit.
- Sluit met dienstverleners bewerkersovereenkomsten met daarin vergelijkbare garanties plus een meldplicht naar jou, zodat jij een melding bij de Autoriteit kunt doen als deze dienstverleners een lek veroorzaken.
- Publiceer ethisch hackbeleid. Zo krijg je gratis tips over mogelijke datalekken die je kunt fixen voordat ze werkelijk worden misbruikt.
- Audit jezelf. Onderzoek in ieder geval waar de toegang tot persoonsgegevens beperkt kan worden. Moet iedereen echt bij alle klantgegevens kunnen, waarom liggen die papieren dossiers niet in een afgesloten kast en is het echt nodig dat archief twintig jaar te bewaren?
- Stel een incident respons protocol op, zodat je alvast weet wat je moet doen als er een data-lek is.
- Stel een data-lek-team samen, zodat je de juiste mensen alvast bij elkaar hebt.
- Controleer je afspraken met leveranciers, zodat ze jou op de hoogte stellen van een meldplicht bij hun.
- Houd je beveiligingsmaatregelen in de gaten, zodat je snel van een data-lek op de hoogte bent.

Cloud en privacy: waar staan uw bedrijf-kritische gegevens?

Ondernemers, vooral diegene met een groot aantal werknemers, gebruiken steeds minder vaak lokale servers, maar zijn overgestapt naar Cloudoplossingen. Kunt u zeggen waar deze Cloud zich bevindt en met welke privacywetten u rekening dient te houden?

Als u eigenaar bent van een bedrijf, dan is de kans groot dat u klant- en personeelsgegevens in uw beheer heeft. Vandaag de dag is het vaak heel praktisch om die gegevens in de Cloud te hebben omdat u hiermee deze gemakkelijk kunt verwerken en hierdoor ook voor iedereen bereikbaar is.

Er zijn verschillende soorten Cloud, dat is ondertussen al duidelijk geworden. zijn er een aantal onderverdelingen te vinden zodat elke onderneming de best toegespitste Cloud kan kiezen:

Men kan de Cloud onderverdelen op basis van locatie:

- Public Cloud: dit is Cloudomgeving zoals men zich het meestal voorstelt: één toepassing of dienst die aan vele klanten tegelijk ter beschikking wordt gesteld.
- Private Cloud: dit is het andere uiteinde van het spectrum: de Cloud-infrastructuur wordt aan één bedrijf ter beschikking gesteld, al dan niet binnen de muren van dit bedrijf en al dan niet door de ICT-afdeling van het bedrijf zelf.
- Hybride Cloud: dit is een combinatie van beide voorgaande modellen: een deel van de ICT-infrastructuur huist in een Private Cloud, een ander deel in een Public Cloud, en beide delen vloeien (idealiter) naadloos in elkaar over.
- Community Cloud: dit zit tussen Public en Private Cloud in. De infrastructuur wordt wel door verschillende bedrijven gedeeld, maar die hebben gemeenschappelijke belangen. Zo vindt u verschillende Cloudplatformen die specifiek voor overheidsdiensten zijn opgezet.

En een onderverdeling op basis van wat precies als dienst wordt aangeboden:

- SaaS (*software as a service*): de eenvoudigste en meeste gebruikte vorm van Cloudcomputing. Een softwarepakket draait niet meer binnen de eigen bedrijfsmuren maar wordt door een externe partij als dienst aangeboden, vaak gratis. Gekende voorbeelden: Google, Salesforce.com en Hotmail.
- PaaS: (*platform as a service*): hier gaan we al een stapje verder. Hier dient de Cloud als platform voor ontwikkeling van SaaS-software of zelfs van interne toepassingen, wanneer het bijvoorbeeld een eenmalig ontwikkeltraject betreft. Bekendste voorbeelden: Microsoft Azure, Amazon Elastic Cloud en Google.
- IaaS (*infrastructure as a service*): Dit is de extreemste vorm van Cloudcomputing: hier wordt de volledige ICT-infrastructuur als dienst afgenomen, al dan niet als verlengstuk van de eigen interne ICT-infrastructuur, en betaald per periode of zelfs per gebruikte rekenkracht of opslag capaciteit.
- Soms worden hier nog DaaS (*desktop as a service*), BPaaS (*businessprocess as a service*) en zelfs XaaS (alles als een service) aan toegevoegd, maar dat is eerder sporadisch.

De naam van de aanbieder weet u, maar weet u ook waar hij uw gegevens verwerkt en hoe ze zijn beschermd? Toch is het in het huidige landschap van cyberaannvallen en datalekken niet onverstandig bewust te zijn van; waar de informatie en gegevens over uw personeel en klanten worden opgeslagen en door wie. De Cloud klinkt misschien als een ongrijpbare locatie, in werkelijkheid kunnen die gegevens overal ter wereld op een server staan.

Het is niet zo dat iedereen maar Clouddiensten mag aanbieden. Er is een regelgeving waar een aanbieder van Cloudoplossingen aan moet voldoen en die is binnen de Europese Unie centraal geregeld. Voor alle lidstaten geldt een wetgeving waar landen zich minimaal aan moeten houden. De lidstaten kunnen bovendien afzonderlijk meer privacyregels handteren. Dat verklaart waarom gegevens in het ene land beter

beschermd kunnen zijn dan in het andere land. Buiten Europa kennen de afzonderlijke landen een eigen regelgeving.

De wetgeving die in Nederland over privacy van persoonsgegevens gaat is de Wet Bescherming Persoonsgegevens (Wbp). In veel gevallen zal een aanbieder echter ook rekening moeten houden met de bepaalde wetgeving van landen binnen de EU en daarbuiten, zoals de Verenigde Staten. Om te begrijpen hoe de wet omspringt met uw gegevens die in verschillende landen worden gestald, is het handig om eerst het basisprincipe van de Wbp te doorgronden. Deze bepaling is van toepassing op een geautomatiseerde verwerking van persoonsgegevens én legt een aantal algemene verplichtingen op.

De Wet maakt onderscheid tussen drie partijen die van belang zijn bij de privacybescherming bij clouddiensten: de verantwoordelijke, de bewerker en de betrokkene. De verantwoordelijke is de aanbieder van de dienst. Voert u het beheer over persoonsgegevens van uw klanten en personeel, dan bent u in veel gevallen de verantwoordelijke. De klanten en het personeel (de betrokkenen) verstrekken immers hun gegevens aan u en geven toestemming voor verwerking hiervan. U kunt vervolgens de verwerking – bijvoorbeeld met opslag in de Cloud - de persoonsgegevens aan een ander overlaten. Dit is de bewerker en is degene die de gegevens verwerkt.

Er is dus een verschil tussen de verantwoordelijke en de bewerker: de laatstgenoemde bepaalt niet de doelen en middelen voor de verwerking van de gegevens, maar verwerkt deze slechts in opdracht van u, de verantwoordelijke. De bewerker moet ook aan de regels voldoen. Die worden vastgelegd in een overeenkomst tussen de verantwoordelijke en de bewerker; de bewerkersovereenkomst.

Welke wet geldt nu als uw bedrijf in Nederland gevestigd is, maar de gegevens wel op een server in Amerika hebt staan? Om te bepalen aan welke wet uw organisatie zich moet houden, kijkt de Wbp voornamelijk naar de vestigingsplaats van uw bedrijf. Bent u in Nederland gevestigd, dan gelden de Nederlandse regels. Het is in de regel dus alleen relevant waar de verantwoordelijke zijn hoofdactiviteiten heeft, de plek waar de gegevens later worden verwerkt doet er in beginsel niet toe bij bepaling van de juiste wetgeving.

Toch maakt het voor uw bedrijf wel degelijk uit waar de gegevens waar u de verantwoordelijkheid over heeft worden verwerkt. Niet elk land is immers even veilig en transparant. Daarom stelt de Wbp dat u als verantwoordelijke niet zomaar in elk willekeurig land gegevens van anderen mag opslaan en verwerven. Om als provider zaken te kunnen doen met bedrijven uit landen buiten de EU, moet er zeker worden gesteld dat deze landen en deze bedrijven een passend beschermingsniveau van persoonsgegevens hebben. Als verantwoordelijke bent dan ook verplicht om een zogenoemde ‘Bewerkingsovereenkomst’ met de bewerker te sluiten waarin deze bescherming staat vermeld.

Binnen de EU vormt dit uiteraard geen probleem aangezien elke lidstaat zich aan minstens dezelfde richtlijnen moet houden. Wanneer uw bedrijf over de Europese grens zaken gaat doen, zult u kritischer moeten zijn. Een handig hulpmiddel waartoe u zich kunt wenden is de ‘Witte lijst’ waarop landen staan waarvan de EU heeft bepaald dat de privacybescherming voldoende is. Het is een nuttige lijst, maar u blijft degene die zorg moet dragen dat de binnen- of buitenlandse bedrijven die de gegevens verwerken, zich aan de afgesproken privacyregels houden.

Waar het uiteindelijk om gaat is dat het voor alle partijen duidelijk is waar ieders zijn verantwoordelijkheden en rechten liggen, vooral in het geval dat er onverhoopt een data lek ontstaat.

Cybercriminaliteit via de website

Er lijkt wel sprake te zijn van een keerpunt in het denken over cyber crime. Steeds meer bedrijven, overheden en organisaties hebben een duidelijk besef dat cyber security niet een 'one-day-fly' is, maar bittere noodzaak. Dit is mede het gevolg van dat bedrijven steeds meer producten en diensten aanbieden via internet; ze moeten wel willen ze niet achterop raken op de concurrentie.

Vaak liggen websites onder vuur als we kijken naar cybercriminaliteit en dus ook data die via een webserver benaderbaar is. Na de werknemer zorgt de webserver voor de grootste security risico's; dit is omdat een webserver een open deur is vanuit een organisatie naar de rest van de wereld.

Belangrijke stappen om dit risico zo klein mogelijk te houden zijn: de server goed te onderhouden, de updates van de webapplicaties op orde hebben en de codering van uw website bepalen uiteindelijk hoe groot uw deur is. Als u uw bedrijf kritische data linkt aan het internet of u wordt via website of webshop "zichtbaar" gemaakt dan kunt u er zeker van zijn dat uw web security getest gaat worden.

Op uw website is het voor bezoekers mogelijk gemaakt om:

- een nieuwe pagina te laden met dynamische content;
- zoeken naar een product of dienst;
- invullen contactformulier;
- zoekfunctie op de site;
- mogelijkheden om via web aankopen te doen;
- een account creëren of het inloggen via een bestaand account.

In elk van de bovenstaande gevallen is het voor uw bezoeker mogelijk om een commando via of door uw webserver te versturen en in veel gevallen is dit een database. Een veel voorkomend probleem is dat uw site bestaat uit meerdere programmeer lagen, die door verschillende programmeurs is ontwikkeld en geschreven. Sommige van de codes zijn oud en zijn aangepast of voorzien van nog meer codes door de webdesigner of webmaster. Ook software die jaren geleden is aangeschaft, die misschien niet meer gebruikt wordt en draaiend op verschillende resources zorgen voor grote security risico's en dan vooral door het missen van de belangrijke updates. Elk formulier of script geïnstalleerd op uw site kan zwakheden of zelfs bugs bevatten en zorgen voor beveiligingsproblemen bij u, maar ook bij uw bezoekers. Uw webpagina is namelijk niet het eindstation want dat is vaak uw bezoeker die via uw website wordt besmet.

Het zijn voornamelijk oude beveiligingslekken die cybercriminelen inzetten om exploits te initiëren. Vaak zijn er wel patches uitgebracht, maar het wordt dan vergeten om deze updates te installeren. Hackers maken veel gebruik van deze bekende vulnerabilities omdat betreffende organisaties of websites interessant zijn, maar ook om te kijken of het mogelijk is om ergens in te breken. Ook gezien het feit dat er maar weinig hackers zijn die daadwerkelijk een nieuwe manier vinden om de web security weer te omzeilen.

Op een Website worden gemiddeld 79 beveiligingslekken gevonden en deze worden pas na 18 maanden ontdekt (bron: ICT Waarborg)

Voordelen van ISO certificering

De voordelen van invoering van ISO certificering kunnen zich op diverse gebieden manifesteren. Het verhogen van de kwaliteit van goederen en diensten, het verhogen van klanttevredenheid, het verhogen van de productie, het verlagen van de kosten en het vergroten van bewustwording van medewerkers zijn slechts enkele voorbeelden.

Volgens een onderzoek onder het bedrijfsleven wordt er jaarlijks een behoorlijk percentage van de omzetwaarde gespendeerd aan het oplossen van fouten en klachten. De zogenaamde faalkosten. Door te investeren in het voorkomen hiervan, is het aandeel faalkosten behoorlijk terug te dringen. Dit is ook één van de resultaten van een goed certificeringstraject.

Door bij kwaliteit management de verbetercyclus te integreren en zodoende belangrijke zaken meetbaar te maken, ontstaat een organisatie die kan sturen op basis van cijfers. Dit geeft bij veel opdrachtgevers verassende inzichten en rendementsverbeteringen.

De toegevoegde waarde van een gecertificeerd managementsysteem is dat een bedrijf op deze manier aantoont dat het een werkende systematiek heeft om de naleving van wet- en regelgeving te borgen. Een goed functionerend managementsysteem brengt afwijkingen naar boven, waardoor het bedrijf zelf verbeteringen kan aanbrengen. Door het certificatieproces worden in het managementsysteem verbeteringen aangebracht die tot een hoger niveau van naleving leiden.

Het hele ISO certificeringstraject heeft veel bedrijven verder gebracht. Zij zijn intern bijvoorbeeld efficiënter gaan werken en communiceren. De effecten van dit certificeringstraject hebben zeker bijgedragen aan kwaliteitsverbetering en bewustwording van informatiebeveiliging.

ISO certificering helpt om de processen die er toe doen te identificeren en te optimaliseren:

- Hierdoor krijgt het management een hulpmiddel ter beschikking om de organisatie te sturen;
- Processen en structuren worden voor de gehele organisatie duidelijk, waaronder communicatiestructuren, taken en verantwoordelijkheden;
- Betrokkenheid van de medewerkers kan hierdoor vergroot worden, wat bevorderlijk kan zijn voor de werksfeer, werkdruk en ziekteverzuim;
- Verhoging van efficiency, wat kan resulteren in kostenbesparingen;
- Problemen kunnen tijdig gesignaleerd en geïdentificeerd worden, waardoor actie ondernomen kan worden om fouten in de toekomst te voorkomen;
- Klant en klanttevredenheid staat centraal; klanttevredenheid kan geoptimaliseerd worden;
- ISO certificering levert een positief bedrijfsimago op, zowel nationaal als internationaal, wat resulteert in een voorsprong op de concurrentie.

Waarom Standaardisatie

Stelt u voor dat een incident uw bedrijfsvoering stagneert; stroom valt uit, er breekt brand uit, in geval van waterschade, iemand breekt bij u in of uw vitale systemen worden gehackt. U of iemand van uw personeel wordt ziek of erger nog vertrekt naar een andere werkgever, wat gaat u doen?

Continuïteit is niet alleen belangrijk voor grote organisaties, maar ook voor kleine want die zouden bij grote interruptie hoogstwaarschijnlijk de deuren kunnen sluiten. Er vanuit gaan dat het u niet overkomt, is niet slim, want het kan gebeuren! Standaarden kunnen u juist in deze omstandigheden helpen om snel weer operationeel te zijn. Zij zorgen er tevens voor dat uw toeleveranciers, uw merk en uw reputatie veilig zijn.

10 dingen die standaardisatie voor uw organisatie kunnen betekenen:

- Verbeteren van de goederen, producten en diensten;
- Bewijs van toewijding aan kwaliteit;
- Het verkrijgen van nieuwe klanten en behouden van bestaande klanten;
- Het verbeteren van uw bedrijfsprocessen;
- Kosten reduceren en verhogen van winst;
- Geeft uw bedrijf een onderscheidend vermogen;
- Draagt zorg voor het naleven van geldende wet- en regelgeving binnen een organisatie;
- Helpt u innoveren;
- Ondersteunt uw export inspanningen;
- Versterkt uw commerciële en marketing strategieën.

Juist voor kleine en middelgrote organisaties zou het invoeren van een ISO standaard interessant zijn om een duidelijke structuur aan te brengen binnen de organisatie.

Verder heeft het grote voordelen als we kijken naar marketingstrategieën, want met een ISO certificaat laat u duidelijk zien naar uw klanten dat u een betrouwbare organisatie bent.

Uit ervaring en onderzoek is gebleken dat het tevreden houden van de klant goede handel is omdat het vinden van een nieuwe klant gemiddeld 6 x zoveel kost. Dus ervoor zorgen dat uw klant tevreden is, lijkt ons dan erg belangrijk en hier komen ook de voordelen van standaardisatie naar boven.

Bepaal uw standaard en win hiermee nieuwe handel:

- Wat zou u beter willen doen: efficiënter werken, beter contact met klant;
- Wat zou u willen bereiken en wat zou een standaard hierin betekenen;
- Bekijk de concurrentie, omschrijf uw doelen beter en wat zou uw voordeel zijn;
- Welke voordelen heeft uw klant van uw standaardisatie, ander prijsniveau
- Welke voordelen levert het u op als we kijken naar toeleveranciers, zou u hiermee nieuwe toeleveranciers kunnen binden die u nog verder differentiëren.
- Als u eenmaal bovenstaande heeft omschreven wordt het makkelijker om een passende standaard te vinden die voor uw bedrijf het verschil gaat betekenen
- Implementeer uw standaard binnen de organisatie, vraag een certificaat aan en bekijk uw voortgang regelmatig
- Laat het iedereen weten dat u de lat een stuk hoger heeft gelegd.

ISO 27001

Uitgangspunt van ISO is dat het niet verplicht is; dus hoeveel waarde moet men hier dan aan hechten. Aan de andere kant moeten we ergens beginnen dus waarom niet een internationale norm die richtlijnen geeft inzake informatiebeveiligingsbeheer, waaronder de selectie, implementatie en het beheer van beheersmaatregelen die rekening houden met de segmentatie waarin de informatiebeveiligingsrisico's van de organisatie gelden.

Met het ISO 27001 certificaat laat u zien dat uw systeem gecertificeerd is op het gebied van informatiebeveiliging. Met het certificaat kunt u bewijzen dat uw organisatie de nodige voorzorgsmaatregelen heeft genomen om vertrouwelijke informatie te beschermen tegen ongeautoriseerde toegang. Richting uw opdrachtgevers geeft u aan dat u het informatieproces beheerst en gegevens van uw opdrachtgevers goed heeft beveiligd. Met het ISO 27001 certificaat voldoet uw organisatie tevens aan de eisen op het gebied van informatiebeveiliging bij aanbestedingen. De Code voor Informatiebeveiliging, generiek aangeduid als de ISO 27000 bestaat uit twee delen: een norm (NEN ISO 27001) en een 'code of practice' (NEN ISO 27002). Certificering gebeurt tegen de norm, de 'code of practice' en geeft handreikingen voor de implementatie van maatregelen in de organisatie

ISO 27001 specificeert eisen voor de implementatie van beveiligingsmaatregelen in het kader van de algemene bedrijfsrisico's voor uw organisatie. Dit houdt in bescherming van persoons- en/of bedrijfsgegevens, bescherming tegen hackers, inbraak, enz. ISO 27002 geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie. Steeds meer organisaties kiezen ervoor de beveiliging van hun informatie te structureren op basis van de ISO 27001 norm. Na ISO 22000 – die betrekking heeft op voedselveiligheid – is ISO 27001 inmiddels de meest gebruikte standaard van ISO.

ISO 27001:2013 is de eerste norm die voldoet aan de High Level Structure (HLS). De doelstellingen die in deze internationale norm worden beschreven, geven richtlijnen voor de algemeen aanvaarde doelen van informatiebeveiliging.

Deze Internationale ISO norm is ontworpen om te worden gebruikt door organisaties die voornemens zijn om. Certificeringen zijn vaak gericht op NEN ISO 27001 omdat dit een bekende naam is in de markt. Maar misschien is dit wel niet de best passende certificering voor uw organisatie. Het raamwerk van de ISO 27001 is namelijk vrij rigide en vereist voor de certificering dat alle normen (ook die niet direct relevant hoeven te zijn voor uw organisatie) wel geïmplementeerd moeten worden.

Het ISO 27001 certificaat toont aan dat de (interne) processen en de informatie die daarbij verwerkt wordt, beheerst en dat gevoelige gegevens beveiligd zijn tegen ongeautoriseerde toegang en bewerking. Hiermee wordt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie van aangesloten keurbedrijven en uitgevoerde keuringen geborgd. Doordat het bij de ISO 27001 om een generieke maatregelen set gaat, is het niet mogelijk om een reële risicoafweging en diversificatie aan te brengen. Daardoor kan een traject voor ISO 27001 certificatie kostbaar worden, veel tijd vragen en dan nóg niet volledig aansluiten bij de wensen en eisen van de klanten. Gelukkig is er sinds kort ook een alternatief, namelijk de ISO 27002. Deze is ontwikkeld voor organisaties die niet (willen) passen binnen de standaard van 27001 en wél gecertificeerd willen worden. Het certificeringtraject op basis van ISO 27002 is maatwerk en sluit aan op de specifieke risico's van de organisatie. Een ISO 27002 certificering sluit hierdoor vaak beter aan op de wensen en eisen én zijn de kosten meestal aanzienlijk lager omdat alleen de reële maatregelen dienen te worden geïmplementeerd.

ISAE 3402

Veel (gebruikers)organisaties besteden delen van hun activiteiten uit aan serviceorganisaties. Het betreft steeds vaker activiteiten die bij verstoring een grote impact kunnen hebben op de gebruikersorganisatie. Daarom is het continue goed functioneren van de serviceorganisatie van essentieel belang voor de gebruikersorganisatie. Afspraken over de dienstverlening worden vaak vastgelegd in een Service Level Agreement (SLA). De SLA biedt over het algemeen echter niet voldoende zekerheid over de kwaliteit van de dienstverlening van de serviceorganisatie.

Dit is de reden waarom de gebruikersorganisatie periodiek gerapporteerd wil worden over de kwaliteit van de uitbestede activiteiten door een onafhankelijke auditor. De rapportage over uitbestede activiteiten heet een ISAE 3402-verklaring.
Met de ISAE 3402-verklaring toont de serviceorganisatie aan in hoeverre zij voldoet aan de kwaliteitseisen van de gebruikersorganisatie. Deze informatie is van belang voor de gebruikersorganisatie om vast te stellen in hoeverre zij in control zijn over de uitbestede activiteiten.

Officiële status van ISAE 3402

Op 18 december 2009 heeft de IAASB de TPA-standaard gepubliceerd: de ISAE 3402 (International Standard For Assurance Engagements). De ISAE 3402 heeft in 2013 de SAS70 standaard vervangen. De ISAE 3402-verklaring is een internationale standaard die door nationale beroepsorganisaties, zoals de Nederlandse Beroepsorganisatie voor Accountants (NBA) en Nederlandse Organisatie Register EDP-auditors (NOREA), is opgenomen in hun body of standards. Hierdoor mogen Register accountants (RA) en Register EDP-auditors (RE) de verklaring afgeven.

Meer dan alleen financiële processen

De ISAE 3402 kent een uitgebreidere scope dan de SAS70 waardoor deze voor een bredere soort activiteiten is toe te passen. De scope beperkt zich niet tot de beheersmaatregelen voor de financiële processen. Ook zaken als betrouwbaarheid van het primaire proces, informatiebeveiliging en continuïteit kunnen worden opgenomen in een ISAE 3402-rapport. De nadruk ligt met name op de beheersmaatregelen die de uitbestedende organisatie verwacht aan te treffen.

De ISAE 3402 type 1 versus de ISAE 3402 type 2

De ISAE 3402 kent twee typen rapportages, het type I-rapport betreft een momentopname. Hierin wordt beschreven hoe een het proces en de beheersingsmaatregelen zoals deze op een bepaald moment zijn geïmplementeerd. De auditor toetst de haalbaarheid van de beschreven beheersingsmaatregelen om de gestelde beheersingsdoelstelling te bereiken en stelt de implementatie ervan vast. Een type I-rapport moet worden gezien als informatief rapport. Het ontbreken van zekerheid over de werking betekent dat het rapport geen direct bewijs levert voor de oordeelsvorming over de uitkomsten van het proces.

Het type II-rapport betreft een periode, meestal zes maanden tot een jaar. Het rapport beschrijft het proces en de beheersingsmaatregelen zoals deze gedurende de gedefinieerde periode hebben gewerkt. De auditor toetst de haalbaarheid van de beschreven beheersingsmaatregelen voor het bereiken van de beheersingsdoelstelling en stelt vast dat de implementatie ervan gedurende de rapportageperiode in overeenstemming is met de beschrijving. Daarnaast wordt de effectiviteit (werking) van de beheersingsmaatregelen gedurende de rapportageperiode gecontroleerd.

Identity & Access Management (IAM)

Er ontstaan steeds meer relaties tussen organisaties waarbij geen hiërarchische of organisatorische leiding/management is en waarbij het wel noodzakelijk is om (stukken) informatie te delen, om te kunnen komen tot het gezamenlijke doel of resultaat. Voorbeelden hiervan zijn Veiligheidshuizen, Gezondheidsorganisaties, hulpverleningsinstanties, Verzekeringskantoren, Crisisteams etc.

Om tot een effectief eindresultaat/proces te komen wordt vaak voor een dergelijk samenwerkingsverband een keten informatisering proces opgezet. Bij een keten informatisering proces worden processen óver organisaties heen geïntegreerd. Informatie delen binnen deze keten én toch ook dezelfde (persoons-)gegevens goed beschermen, kan alleen door binnen de keten en de processen, op efficiënte wijze inrichten van Identity & Access Management (IAM).

IAM heeft betrekking op het zekerheid verkrijgen omrent de identificatie, bevoegdheden en toegangsbeheer van de gebruikers van een informatieproces.

Om in een samenwerkingsverband gebaseerd op ketenintegratie efficiënt te kunnen werken als gebruiker, wordt vaak gebruik gemaakt van Single Sign-on (SSO). Dit is een mechanisme waardoor een gebruiker slechts één maal hoeft in te loggen om vervolgens meerdere systemen en applicaties te kunnen gebruiken.

12secure-U en IAM

12secure-U heeft experts in dienst die al jarenlange ervaring hebben opgedaan met Ketenintegratie, SSO en IAM. Door het begeleiden en participeren in projecten hierover is gedegen kennis opgebouwd en zijn we in staat om u en uw organisatie goed te adviseren ten aanzien het opzetten, organiseren en inrichten van uw Identity- en Accesmanagement (IAM).

12secure-U kan u helpen op het gebied van autorisatiebeheer, ook wel Identity en Access Management (IAM) genoemd zijn bijvoorbeeld:

- Heeft uw organisatie steeds meer behoefte aan Single Sign-on (SSO)?
- Hoe kunnen toegangsrechten worden gebruikt en gekoppeld aan bevoegdheden?
- Hoe om te gaan met groepsaccounts?
- Het belang van uitrollen en beheren van accounts
- Voldoen aan huidige beveiligingseisen en wetgeving
- Behoefte aan ontdubbelen (dubbele accounts)
- Belang van Naamgevingsconventie
- Federatie*/samenwerking komt dikwijls voor?
- Wilt u aantoonbaar maken voor uw klanten en/of de Accountant dat informatie adequaat is beveiligd en afgeschermd zodat er geen onbevoegd gebruik van gegevens kan worden gemaakt en inzage mogelijk is?
- Vragen of advies nodig over het opstellen van een plan voor het organiseren en inrichten van Identity- en Accesmanagement?

Federatie is een mechanisme dat door toepassing van verschillende protocollen (zoals bijvoorbeeld SAML**) het identiteitsbeheer kan overdragen aan een derde partij. ** SAML (Security Assertion Markup Language) is een standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen domeinen

Trainingen gericht op Wbp

12secure-u geeft ook trainingen gericht op de Wet bescherming persoonsgegevens, namelijk een 1-daags of 2-daagse Training Privacy & Security en het Wbp. Deze training “Praktisch omgaan met Privacy & Security en het Wbp” gaat in op alle aspecten waar een bedrijf mee te maken heeft op het moment dat er persoonsgegevens worden verwerkt of dat derden deze voor uw organisatie verwerken. Persoonsgegevens worden steeds meer geautomatiseerd verwerkt en dat heeft invloed op de informatiebeveiliging.

Het interessante aan deze training is dat er een link wordt gelegd tussen de wetten en richtlijnen enerzijds en de invoering ervan in de praktijk en de relatie met informatiebeveiliging anderzijds. Het is dus een training waarbij de wetten vanuit juridisch oogpunt worden bekeken en er wordt in die context ook direct een relatie gelegd naar de praktijk. De training is vooral voor deelnemers die zoeken naar praktische oplossingen en richtlijnen.

Daarom 12secure-u

Juist door de samenwerking van meerdere organisaties bieden wij expertise op het gebied van huidige en aankomende privacywetgeving. Verder zijn wij op de hoogte van de laatste ontwikkelingen op dit gebied en hebben jarenlange ervaring met het opstellen en uitvoeren van privacy beleid, beveiligingsrichtlijnen, bewerker overeenkomsten, etc.

Als organisatie beschikt u vaak over veel persoonsgegevens. Koppelen en integreren van data, big data, business intelligence, Cloud Solutions, etc. zijn allemaal thema's waar steeds meer organisaties mee bezig zijn.

Op het moment dat hierbij persoonsgegevens worden gebruikt is het van belang om te voldoen aan de wet. De Data Protection Officer (DPO), ook wel Functionaris voor de Gegevensbescherming (FG) genoemd, bewaakt dit en signaleert tijdig problemen en (mogelijke) knelpunten. Daarnaast denkt hij ook mee met de organisatie om het gebruik van persoonsgegevens zo eenvoudig en veilig mogelijk te maken (PIA, PET).

Bent u op zoek naar een Security Officer, coördinator informatiebeveiliging, Information Security Officer, een Security Expert of een IT-Security consultant met kennis op het gebied van de informatiebeveiliging en de bekende methodieken en kaders zoals onder andere; ISO 7510, ISO 9001, ISO 14001, ISO 20000 ISO 22301, ISO 27001 of ISO 45001, dan wel ISAE 3000 of ISAE 3402; ook dan bent u bij 12secure-u aan het juiste adres.

Of u bent op zoek naar een Privacy Expert met verstand van de nieuwe EU Privacy verordening, regelgeving Meldplicht, een Data Protection Officer of een IT-Security consultant met kennis op het gebied van de Wet bescherming Persoonsgegevens? 12secure-u heeft die consultants voor u binnen haar grenzen!

Strippenkaart:

Voor het regelmatige gebruik maken van de ervaring en deskundigheid van onze Informatie beveiligings-consultants van 12secure-u bieden wij een “strippenkaart” aan. Deze kunt u inzetten voor advies en testen. De strippenkaart vertegenwoordigt een tegoed aan consultancy-dagdelen en hiermee kunt u - zonder daar steeds opnieuw een opdrachtbevestiging voor te hoeven tekenen - gebruik maken van onze consultancydienstverlening. De strippenkaart die we uw organisatie willen aanbieden is voor 5 dagen (= 10 dagdelen en bieden we fixed-price aan voor € 4.500,- ex btw, Normale prijs € 5.000,- ex btw.
Facturering in zijn geheel vooraf.

De in rekening gebrachte tarieven zijn exclusief btw doch inclusief reis-, verblijfs-, kantoor- en ondersteuningskosten. Er zullen geen posten in rekening gebracht worden onder de noemer ‘overige kosten’ en soortgelijke –voor de opdrachtgever onduidelijke- kostenposten.