Een checklist voor informatiebeveiliging

Door: **De IT-Jurist**
Versie: 1.0
Datum: juli 2015

Inhoudsopgave

1. Inleiding

De IT-jurist krijgt doorgaans veel vragen op het gebied van informatiebeveiliging. Dat is ook logisch omdat het werkveld van een IT-jurist standaard ligt op het grensvlak van IT, recht en informatiebeveiliging. In deze checklist wordt een overzicht gegeven van aandachtspunten, die kunnen helpen bij het inzichtelijk maken van eventuele verborgen risico's en het vergroten van het beveiligingsbewustzijn.

Het komt regelmatig voor dat werknemers uw organisatie (definitief) verlaten. Vanuit het oogpunt van informatiebeveiliging brengt dat risico's met zich mee. In het laatste hoofdstuk ‘Vertrek personeel’ (H10) is een overzicht van maatregelen (exit-strategie) opgenomen die u kunt nemen om die risico's te minimaliseren.

2. Vragen die betrekking hebben op beleid en organisatie van de informatiebeveiliging

- Is er een informatiebeveiligingsbeleid in de vorm van een document en is dit document bekend bij alle medewerkers binnen de organisatie?
- Is er iemand of is er een werkgroep die de verantwoordelijkheid voor informatiebeveiliging neemt door bijvoorbeeld risico's te signaleren of zich in andere mate bezig te houden met informatiebeveiliging?
- Wordt bij functiebeschrijvingen rekening gehouden met gescheiden bevoegdheden?

Betrokkenheid van het management bij informatiebeveiliging, het uitdragen daarvan binnen de organisatie en de organisatorische inbedding is van groot belang.

3. Toegang door derden en uitbesteding

- Zijn er informatie verwerkende voorzieningen die toegankelijk zijn voor derden zoals bijvoorbeeld leveranciers van ICT-apparatuur i.v.m. onderhoud?
- Doet de organisatie aan outsourcing (bijv. externe salarisverwerking)? Hoe wordt in dergelijke situaties rekening gehouden met de informatiebeveiliging?

In geval van toegang door derden of bij uitbesteding van ICT-diensten moet in contractvorm afspraken zijn gemaakt over informatiebeveiliging.

4. Beheer / procedures

- Zijn er procedures voor correcte en veilige bediening van ICT-apparatuur?
- Zijn er procedures voor het correct en betrouwbaar gebruik maken van applicaties?
- Waarvan worden back-ups gemaakt? Zijn daar vaste procedures voor? Hoe / waar worden de back-ups bewaard en worden back-ups ook regelmatig teruggezet?
- Is er iets geregeld voor het vernietigen van informatiedragers zoals diskettes en tapes maar vooral ook papier?
- Zijn gebruikers bekend met en getraind in beveiligingsprocedures?
- Worden (beveiligings)incidenten door gebruikers gemeld en zijn daar vervolgacties aan gekoppeld?
- Worden bedieningsinstructies voor applicaties en systemen vastgelegd voor beoordeling achteraf (logging)?

Het vastleggen en vooral het naleven van procedures is van groot belang voor de betrouwbare dienstverlening. ICT wordt nog het meest bedreigd vanuit de eigen organisatie, door menselijk falen dan wel door frauduleus handelen.

5. Fysieke beveiliging van ruimtes en van apparatuur

- Wordt bij plaatsing van ICT-apparatuur rekening gehouden met omgevingsfactoren zoals zichtbaarheid en bereikbaarheid van buiten af?
- Is er een "clear desk" policy om te voorkomen dat informatie toegankelijk is voor onbevoegden?
- Wordt ICT-apparatuur volgens voorschrift van de leverancier onderhouden en worden onderhoudswerkzaamheden door deskundig personeel uitgevoerd?
- Worden technische verstoringen inclusief de genomen acties vastgelegd voor evaluatie achteraf?

Voorkomen moet worden dat bedrijfsmiddelen verloren gaan of beschadigd worden, zowel als gevolg van onbevoegde indringing als door het niet functioneren, waardoor de continuïteit van de bedrijfsvoering wordt onderbroken.

6. Bescherming van gegevens

- Wat is er geregeld om te voorkomen dat onbevoegden toegang krijgen tot netwerken, computers en applicaties?
- Is er antivirus software in gebruik? Zo ja, wordt regelmatig een nieuwe versie geïnstalleerd en is voor *alle* gebruikers duidelijk hoe te handelen in geval van besmetting?

Informatie lijkt steeds kwetsbaarder te worden naarmate toegangsmogelijkheden en beschikbaarheid toeneemt; in geval van internettoegang zijn aanvullende maatregelen nodig!

7. Naleving wettelijke en contractuele verplichtingen

- Is de ICT-infrastructuur deskundig aangelegd en wordt ICT-apparatuur volgens voorschrift van de leverancier onderhouden?
- Zijn er maatregelen om het gebruik van illegale software/ kopieën van software tegen te gaan? Is bij de aanschaf van softwarepakketten voldoende zicht op het aantal gebruikers i.v.m. de licenties?
- Hoe wordt omgegaan met de risico's van verlies, vernietiging en vervalsing van belangrijke bedrijfsdocumenten?
- Wordt persoonlijke informatie beschermd conform de privacywetgeving?

Elke organisatie heeft te maken met wet- en regelgeving zoals het auteursrecht, de wet computercriminaliteit, de wet bescherming persoonsgegevens, richtlijnen documentbeveiliging etc. Organisaties zijn zich niet altijd voldoende bewust van de consequenties; hierbij kan juridisch advies gewenst zijn.

8. Continuïteit

- Is er bewust voor gekozen bepaalde aspecten niet te beveiligen en zijn daarvoor continuïteitsmaatregelen getroffen?
- Wordt ook rekening gehouden met infrastructurele verstoringen zoals brand, onderbreking van stroom of telecommunicatie, etc.?
- Worden continuïteitsmaatregelen regelmatig getest?

Continuïteitsmaatregelen zijn een vaak verwaarloosd maar belangrijk onderdeel van beveiligingsmaatregelen; bijvoorbeeld de afhankelijkheid van leveranciers kan worden afgedekt door de beschikbaarheid van de broncode goed te regelen.

9. Bewustwording

Zijn gebruikers zich bewust van risico’s als:

- het slordig omgaan met gebruikerswachtwoorden?
- het slordig omgaan met vertrouwelijke documenten?
- het onbeheerd achterlaten van onbeveiligde Pc’s?
- het zichtbaar transporteren en het onbeheerd achterlaten van laptops?

Beveiliging is mensenwerk! Het is nodig gebruikers bewust te maken van het belang van informatiebeveiliging. Een onderneming is verplicht zijn medewerkers te voorzien van de juiste middelen om het beveiligingsbeleid te ondersteunen tijdens het uitvoeren van de normale werkzaamheden.

10. Vertrek personeel

Het komt regelmatig voor dat werknemers uw organisatie (definitief) verlaten. Vanuit het oogpunt van informatiebeveiliging brengt dat risico's met zich mee. In dit artikel een overzicht van maatregelen (exit-strategie) die u kunt nemen om die risico's te minimaliseren.

Om u een idee te geven wat een 'exit strategie' zoal inhoudt, zijn een aantal belangrijkste punten hieronder weergegeven. Omdat elke organisatie een andere werkwijze hanteert is deze 'exit strategie' algemeen van opzet en alleen al om die reden niet volledig. Belangrijk zijn met name de aandachtspunten bij vertrek van personeel uit uw organisatie. Hier kan het gaan om vaste personeelsleden, uitzendkrachten, stagiaires en andere externen.

- Sluit direct alle accounts en inlogmogelijkheden met wachtwoorden van de betreffende medewerker op het interne systeem;
- Zorg dat e-mail van de betreffende medewerker wordt doorgestuurd naar een ander zakelijk emailadres;
- Sluit e-mailbox(en), ook of juist voor webmail van de betreffende persoon;
- Laat de medewerker eventuele badge(s)/pasje(s) inleveren;
- Laat de medewerker een geheimhoudingsverklaring tekenen. Doe dit trouwens het liefst bij binnenkomst;
- Laat de medewerker eventueel hardware van de zaak inleveren (mobiele telefoon, tablet);
- Laat de receptie/portier weten dat betreffende persoon niet langer bij uw organisatie werkzaam is;
- Schakel eventueel het telefoonnummer van betreffende persoon door naar juiste vervanger.

Gegevens op straat
Niet alleen werknemers, ook hardware of software verlaten de organisatie. En ook daar kan het nodige mis gaan. Het is aan te bevelen ook hiervoor een 'exit strategie' vast te stellen en te bespreken binnen het managementteam. Enkele aanbevelingen zijn:

- Verwijder of vernietig de harde schijf (schijven) bij hardware;
- Verwijder alle gegevens die evt. in de software opgenomen zijn;
- Laat niets zomaar overnemen door wie dan ook. Blijf daarbij ook alert met het overnemen door werknemers voor thuisgebruik (houdt dit dan ook bij);
- Opslagmedia die gevoelige informatie bevatten, dienen in plaats van op de standaard manier te worden gewist, fysiek te worden vernietigd of op een veilige manier te worden overschreven;
- Alle onderdelen van de apparatuur waarop gegevens kunnen worden opgeslagen, bijvoorbeeld vaste schijven, dienen te worden gecontroleerd om te waarborgen dat alle gevoelige gegevens en in licentie gebruikte software zijn verwijderd of overschreven voordat de apparatuur wordt afgevoerd.

Website
Controleer tot slot ook de website van uw bedrijf waar vaak ook contactgegevens op staan vermeld. Controleer de gehele site op namen, telefoonnummers en e-mail adressen van personeelsleden die uw organisatie verlaten hebben en verwijder of verander de betreffende gegevens.

Meer informatie

Informatiebeveiliging is een veelzijdige kwestie. De IT-jurist bv heeft alle disciplines in huis om organisaties op dit belangrijke aandachtsgebied van dienst te zijn. Heeft u vragen, neem dan contact op via www.it-jurist.nl/.