CENTRE FOR
CYBER SECURITY
BELGIUM

Baseline Security Guidelines (BSG)

Management samenvatting (NL)

CENTRE FOR

CYBER SECURITY BELGIUM

Rue de la Loi, 16 – Brussels

info@ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be

Inleiding

Informatiebeveiliging is een organisatorische uitdaging geworden die elke manager moet begrijpen. Het is een cruciaal element in elke organisatiestrategie die erop gericht is haar essentiële middelen (activa) te beveiligen, en dit om minimaal volgende zaken te kunnen garanderen:

- Winnen (en niet verliezen) van het vertrouwen van de klant
- Bescherming van de reputatie
- Bedrijfscontinuïteit
- Betere weerbaarheid tegen cybercriminaliteit (zoals ransomware en andere malware)
- Veerkracht in geval van een cyberincident

Op zich zijn gegevens vaak niet veel waard, totdat ze worden verwerkt, georganiseerd, samengevoegd, gemanipuleerd om er informatie en kennis van te verschaffen.

Informatie is de basiswaarde van een organisatie en deze moet goed beschermd worden via adequate beveiligingsmaatregelen die deel uitmaken van het goede beheer dat een overheidsinstantie moet invoeren.

Informatiebescherming wordt ook steeds complexer in een onderling verbonden wereld.

Informatiebeveiliging is niet alleen een technische aangelegenheid, maar vereist ook om regels vast te leggen en ervoor te zorgen dat deze worden nageleefd.

Het belang van informatiebeveiliging voor leidinggevenden

De voordelen van een informatiebeveiligingsbeheersysteem voor uw organisatie zijn:

- Verhoging van de gepercipieerde waarde en reputatie van uw organisatie door een goed beheerssysteem aan te tonen
- De vermindering van beveiligingsrisico's en -incidenten
- Bescherming tegen wettelijke of reglementaire vereisten
- Een structuur om IT-investeringen efficiënter te besteden
- Een waardevol hulpmiddel bij het reageren op grote cyberbeveiligingsincidenten
- Het vertrouwen verhogen dat beslissingen gebaseerd zijn op feitelijke gegevens
- Een manier om uw externe partners te tonen dat informatieveiligheid serieus wordt genomen en hun deze ook op te leggen
- Zij zorgen voor de vertrouwelijke behandeling van de gegevens

Opmerking: IT-beveiliging is veel beperkter dan informatiebeheer, aangezien deze betrekking heeft op het "geautomatiseerde" deel van het informatiebeheer. De mondelinge verspreiding van informatie, informeel, zoals in een lift, valt buiten IT-beveiliging maar wel binnen informatiebeveiliging.

Om de implementatie van een informatiebeveiligingssysteem te begeleiden hebben wij deze gids ontwikkeld. De BSG (Baseline Security Guidelines) is volledig gebaseerd op ISO27001 maar heeft als focus de overheidsinstellingen en bevat een stapsgewijs voorstel voor een methode.

De wettelijke verplichtingen met betrekking tot de bescherming van persoonsgegevens (GDPR) worden niet hier niet letterlijk overgenomen maar zijn zeker ook toepasbaar op dit specifiek domein.

Informatiebeveiligingsbeheer - 4 basisprincipes -15 aandachtspunten

Bij het vaststellen van een goed informatiebeveiligingsbeheer moet rekening worden gehouden met **vier belangrijke basisprincipes**:

1. Beveiligingsstrategie en ondersteuning
2. Inventarisatie van activa en risicoanalyse
3. De uitvoering van veiligheidsmaatregelen
4. Evaluatie van de beveiligingsmaatregelen

Deze basisprincipes voor informatiebeveiliging horen continu geëvalueerd te worden om de kwaliteit te verbeteren (het PDCA-model = "Plan, Do, Check, Act").

Deze vier principes bevatten **15 aandachtspunten** die als volgt zijn geformuleerd:

Beveiligingsstrategie en ondersteuning

1. De **betrokkenheid en ondersteuning van het management** is noodzakelijk om een beveiligingsstrategie te borgen en te zorgen dat operationele structuren, procedures en middelen hierop geënt worden.
2. Ontwikkel een **informatiebeveiligingsstrategie (veiligheidsbeleid)** afgestemd op de strategie van de organisatie om de doelstellingen te ondersteunen met inachtneming van wet- en regelgeving.
3. Stel een meerjarenplan op voor regelmatige **training en sensibilisering** van alle interne en externe medewerkers en uw organisatie als geheel.
4. Integreer vanaf het begin **een cultuur van informatieveiligheid en risicoanalyse** voor alle nieuwe projecten, of het nu gaat om de ontwikkeling van nieuwe toepassingen of bedrijfsprojecten.
5. Beschik over een plan voor grote/ernstige **veiligheidsincidenten** en -crises.

6. Beschik over een beheerd register van belangrijke wijzigingen in de omgeving.
7. Beschik over een **bedrijfscontinuïteitsplan** (BCP) en een ondersteunend IT gerelateerd **Disaster Recovery Plan (DRP).**

Inventaris van activa en risicoanalyse

8. **Identificeer belangrijke informatiesystemen en gegevens** en de eigenaars ervan en definieer vervolgens de rollen en verantwoordelijkheden.
9. Stel met ondersteuning van het management, een **beleid voor de categorisering van gevoelige informatiesystemen en gegevens** vast, op basis van de principes van confidentialiteit, integriteit en beschikbaarheid (CIB, in het Engels CIA) voor de gehele levensduur. Dit moet geregeld worden herzien.
10. **Beheer de informatiebeveiligingsrisico's** om prioriteiten vast te stellen en passende maatregelen te nemen om deze te verminderen op een door de organisatie aanvaardbaar niveau zodoende dat de mogelijke effecten beperkt worden.

Uitvoering van veiligheidsmaatregelen

11. Implementeer **specifieke (technische/organisatorische/proces-) maatregelen** om de informatie te beveiligen.
12. **Beheer de middelen** die zijn toegewezen aan informatiebeveiliging en -infrastructuur, op een effectieve en efficiënte manier, inclusief de aanwijzing van informatiebeveiligingsfunctionarissen.

4. Evaluatie van de beveiligingsmaatregelen

13. Voer minstens **een jaarlijkse evaluatie van de beveiligingsmaatregelen** uit om de status van het beveiligingsplan te beoordelen. De mogelijke verbeteringen en aanvullingen ervan zijn voor elke organisatie noodzakelijk.
14. **Meet de prestaties van uitgevoerde acties** (vorige punten) maar ook de evolutie van bedreigingen en kwetsbaarheden op regelmatige tijdstippen om ervoor te zorgen dat de doelstellingen worden bereikt (cyclus van continue verbetering: PDCA).
15. Overweeg het **verfijnen van de risicoanalyse en de beheersmaatregelen** in het licht van evaluaties (punt 13) audits, de gebeurde incidenten en belangrijke wijzigingen die impact hebben/hadden op de bedrijfsactiviteiten