Publicatiedatum 01-05-2025

Informatiebeveiligingsbeleid James Software B.V.

Inzicht in de organisatie en haar context
Als SAAS-leverancier van een EPD voor (para)medische praktijken waarbij persoons- en gezondheidsgegevens worden verwerkt en opgeslagen is adequate informatiebeveiliging essentieel voor de continuïteit van de bedrijfsvoering van de Organisatie.

Inzicht in de behoeften en verwachtingen van belanghebbenden
De Organisatie heeft de volgende externe belanghebbenden: klanten, patiënten van klanten en VECOZO. Alle belanghebbenden hebben er belang bij dat de Organisatie adequate informatiebeveiliging waarborgt.

Het toepassingsgebied van het managementsysteem voor informatiebeveiliging
Het managementsysteem voor informatiebeveiligingsbeleid ziet op de samenhangende processen, personeel, infrastructuur en applicaties ten behoeve van de verwerking van persoons- en gezondheidsgegevens alsmede de opslag en uitwisseling hiervan.

Managementsysteem voor informatiebeveiliging
Het managementsysteem voor informatiebeveiliging omvat de volgende vijf stappen o.b.v. de Deming cirkel: beleidsvorming -> risicoanalyse -> planvorming -> implementatie -> monitoring, evaluatie, controle (waarna de cirkel opnieuw begint met beleidsvorming, etc.).

De samenhang tussen deze vijf stappen en de Deming cirkel is als volgt
- Plan: beleidsvorming en risicoanalyse
- Do: planvorming en implementatie
- Check: monitoring, evaluatie en controle
- Act : het verbeterproces

Leiderschap
Gezien het grote belang van informatiebeveiliging is de directie van de Organisatie nauw betrokken het formuleren van het doel, doelstellingen, de risico-analyse, het zelf uitvoeren van taken en het toezicht op taken van medewerkers. Het op de voet volgen van ontwikkelingen in het dreigingslandschap, dit vertalen naar aanvalspaden en de snelheid waarmee mitigaties worden geïmplementeerd is essentieel voor het handhaven van een goede beveiligingspostuur.

Beleid
De doelstelling van het informatiebeveiligingsbeleid van de Organisatie is het blijvend realiseren van de beschikbaarheid, integriteit en vertrouwelijkheid van de persoons- en gezondheidsgegevens die worden verwerkt en opgeslagen in de Webapplicatie. Bij het realiseren van deze doelstelling moet rekening worden gehouden met relevante wet- en regelgeving alsmede met de algemene voorwaarden van de Organisatie.

Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie
Los van het uitvoeren van richtlijnen door alle medewerkers liggen de verantwoordelijkheden en bevoegdheden vooral bij de directie van de Organisatie en 2 developers. De rol van Security Officer is toegewezen aan 1 van de directieleden.

Risicobeoordeling
Van de belangrijkste categorieën van dreigingen – phishing mails, exploitatie van kwetsbaarheden in webapplicaties en remote services- is bekend wat de verdeling is bij geslaagde aanvallen, namelijk ongeveer ieder 1/3. Data over de waarschijnlijkheid van een

aanval is niet bekend. Het bepalen van “risico = waarschijnlijkheid x impact” is dan ook niet mogelijk.

Het uitvoeren van een risico analyse wordt hiermee gereduceerd tot een holistische aanpak waarbij los van de waarschijnlijkheid wordt bepaald dat de impact van dreigingen zoveel mogelijk beperkt moet worden door 1 of meerdere beheersmaatregelen, in het laatste geval “Defense in Depth” genoemd. Een meer granulaire aanpak betreft ”Zero Trust” en “Breaking the attack chain”. De Organisatie hanteert alle genoemde mitigatiestrategieën, ook vanwege de visualisatiemogelijkheden van deze concepten.

Los van zaken als redundantie van data is het mitigatiedoel van dreigingen als volgt, beter gezegd de metafoor die we nastreven: de beveiligingspostuur van de Organisatie tegen aanvallen van opportunistische aanvallers moet altijd beter zijn dan die van de “buren” en tegelijk proberen we ook een aantal beheersmaatregelen te implementeren die “targeted attacks” een stuk moeilijker maken.

Op basis van betrouwbare bronnen zoals het Verizon Databreach Report, het Microsoft Digital Defense Report en het Microsoft Security blog wordt de risico-beoordeling telkens weer uitgevoerd.

Planning en uitvoering
De planning van activiteiten wordt in Excel gedaan. Hiermee wordt ook de voortgang gemeten. Planning en voortgang van verbeterpunten zijn een vast agendapunt in het periodieke informatiebeveiligingsoverleg. Naast verbeterpunten zijn er periodiek terugkerende controles m.b.t. informatiebeveiligingstaken die uitgevoerd moeten worden.

Evaluatie en audit
Jaarlijks voert de directie een evaluatie uit van de documentatie m.b.t. de informatiebeveiliging. Iedere 3 jaar laat de Organisatie de “informatiebeveiliging” doorlichten door een bij Norea aangesloten auditor. Het doel hierbij is een TPM verklaring ten behoeve van VECOZO.