Whitepaper

Bewustwording van informatiebeveiliging en privacy in de zorg

Traditionele versus moderne bewustwordingscampagnes

De zorgsector digitaliseert. Achter elk technisch of mobiel apparaat staat echter een bedienend mens. Een arts, een verpleegkundige of een thuiszorgmedewerker. Deze komt tijdens zijn zakelijk leven regelmatig in aanraking met patiëntgegevens, technische en mobiele apparatuur, medische software, apps en natuurlijk met mensen. Tijdens deze ontmoetingen ontstaan vaak situaties, die gevaar met zich meebrengen voor de privacy van de (kwetsbare) betrokkenen. Structurele bewustwording creëren van deze gevaren is key.

Digitale veranderingen in de zorg

De digitale ontwikkelingen in de zorg zorgen voor een andere rolverdeling tussen artsen en patiënten. Het is niet alleen maar het implementeren van techniek, maar het is een veranderingsproces. Hierbij moeten de neuzen van de IT-afdeling, medisch personeel en patiënten dezelfde kant op staan, zodat het belang van informatiebeveiliging en privacy door iedereen begrepen wordt.

Risico's op het gebied van privacy binnen de zorg

Op het gebied van kennis over privacy in de zorg valt dus veel te verbeteren. In vele gevallen weten de artsen, verpleegkundigen en medewerkers van ondersteunende diensten niet wat de rechten en plichten bij privacy in de zorg zijn. Voorbeelden:

- Te veel mensen hebben toegang tot de privacygevoelige gegevens, die buiten hun werkveld liggen.
- Managers geven opdracht aan uitvoerend personeel om patiëntendossiers in te kijken zonder grondige redenen.
- Autorisatie en richtlijnen rondom privacy zijn niet bekend of niet opgesteld.
- Men denkt vaak dat het tekenen van geheimhoudingsverklaring voldoende is om met privacygevoelige informatie om te gaan.
- Privacybewust zijn is vaak meer aanwezig bij de verpleegkundige dan bij artsen en management.
- Dossiers en gegevens van patiënten worden gedeeld met andere instantie zonder de patiënten kennis te stellen.
- Bij de fysieke inrichting van de (inschrijf)balies, servicedesks en informatiezuilen wordt te weinig aan de privacy gelet.
- Op de website van de zorginstellingen wordt onrechtvaardig te veel informatie gevraagd via verschillende formulieren. Dit geldt ook voor de honderden apps via de app-store.
- Bij medische (nood)situaties wordt vaak de volgende “excuusmachine” gebruikt: “het gaat om gezondheid en levens redden, privacy komt later. Als er problemen komen dan leggen we dit bij de

rechtbank uit". Dit wordt te pas en te onpas gebruikt om geen geld en aandacht aan de beveiliging en privacy te schenken.

Gevaren op het gebied van informatiebeveiliging ontstaan dan ook vaak uit:

- onwetendheid;
- onverschilligheid;
- overmoed;
- beïnvloedbaarheid;
- naïviteit;
- kwaadaardigheid;
- behulpzaamheid.

Het vergroten van de bewustwording op het gebied van informatiebeveiliging en privacy helpt om de regels en procedures te begrijpen en te interpreteren, sneller reageren op incidenten en om een "gezonde paranoia" te ontwikkelen.

Hoe verloopt een bewustwordingscampagne in de zorg vaak?

De reden waarom een traditionele campagne van bewustwording op het gebied van informatiebeveiliging en privacy slechts op zeer korte termijn succesvol is, heeft met vijf aandachtspunten te maken:

1. **Campagnes worden eens per jaar uitgevoerd**;

Privacy- en informatiebeveiliging gaat om beleving. Als er geen incidenten of datalekken bekend zijn, betekent dat niet dat de organisatie veilig is. Dan is er misschien simpelweg niets gemeld of gemonitord. Veel bedrijven nemen slechts maatregelen als het kwaad al is geschied. Dat is vaak ook het geval met een standaard, jaarlijkse awareness campagne. Het kost geld en tijd, en wordt niet altijd als nuttig en tastbaar ervaren.

2. **De motivatie ontbreekt om ermee aan de slag te gaan;**

Op de werkvloer wordt een bewustwordingscampagne niet altijd met groot enthousiasme ontvangen. Het brengt een extra activiteit met zich mee, die in de krappe agenda's moet passen. De medewerkers zijn dan niet echt gemotiveerd om de stof op te pakken. Deze extra regels komen er naast alle eisen van ISO- en NEN-normen, die op de afdelingen nageleefd moeten worden, nog bij.

3. **De campagne is te algemeen, de inhoud blijft niet hangen;**

Een campagne is succesvol wanneer iedereen het gevoel heeft dat de campagne op hem of haar persoonlijk van toepassing is. Privacy en informatiebeveiliging raakt iedereen. Niet alleen in zijn of haar professionele, maar ook in de privé levenssfeer. Sinds het concept van "het nieuwe werken" werd geïntroduceerd is de scheidingslijn tussen privé en werk vervaagd. Meer mensen werken thuis met vertrouwelijke (bedrijfs)gegevens. Wanneer de campagne alleen algemene informatie vertelt en niet toegespitst is op "het nieuwe werken" en de specifieke bedrijfsvoering, zal dit niet blijven hangen.

4. **Geen maatwerk op vakgebied, maar "one size fits all";**

In sommige organisaties is informatiebeveiliging en privacy volledig in de processen en de organisatie geïntegreerd en is het veiligheidsbewustzijn bij medewerkers sterk ontwikkeld. Andere organisaties hebben wel protocollen en beleid, maar leven daar in de praktijk niet altijd strikt naar. In het ene geval vraagt de organisatiecultuur om intensieve begeleiding van medewerkers én management. Bij

organisaties die al verder zijn, kan het veel effectiever zijn om leidinggevenden te coachen in hun rol en verantwoordelijkheid om privacy en informatiebeveiliging onder de aandacht te houden.

5. **De campagne bestaat alleen uit: posters en vragenlijsten;**

Er zijn tientallen bedrijven die creatieve diensten aanbieden voor een jaarlijkse campagne op het gebied van informatiebeveiliging en privacy. Deze campagnes hebben vaak te maken met budget en worden ingezet omdat het moet voor de certificering, of omdat het op het jaarplan staat. Deze bestaan vaak uit flyers of posters of online enquêtes. De flyers belanden snel in de papierbak, de posters loopt bijna iedereen voorbij en de vragenlijsten op internet worden snel tijdens de lunchpauze weggeklikt.

De aanpak van SafeHarbour om bewustwording blijvend te vergroten

Hoe moet het dan wel? Wat kan SafeHarbour doen?

- Wij starten het bewustwordingsproces op van het belang van het waarborgen van privacy voor de patiënten en de medewerkers.
- Wij brengen het kennisniveau over de regels bij het bestuur en management aanzienlijk op peil.
- Wij zorgen voor een verbetering van de klachtafhandeling (ook voor datalekken) in geval van privacyschending.
- Wij geven voorlichting aan patiënten via de communicatieafdeling over welke informatie wel en niet uitgewisseld mag worden.

Medische gegevens zijn "bijzondere gegevens" volgens de wet. De zorginstelling is verplicht een dossier over de gezondheid van de patiënten bij te houden. Alleen met toestemming van de patiënt mogen deze gegevens aan anderen worden verstrekt. SafeHarbour helpt bij het inrichten van het beheer van het privacyproces en van de bewerkersovereenkomsten om de privacy ook in de keten tussen zorgverleners te waarborgen. Het opstellen van een privacyreglement is een onderdeel van het proces.

Strategie van een doorlopend bewustwordingsproces

Aan een succesvolle aanpak ligt doorgaans een goed doordachte strategie, grondige inhoudelijke kennis van informatiebeveiliging en privacy, en een uitgewerkt communicatieplan ten grondslag. Een goede voorbereiding bepaalt het succes op de lange termijn. Bewustwording vergroten is geen eenmalig project of campagne. Het is een **doorlopend proces** met diverse middelen, op diverse tijdstippen, waarbij de inhoud telkens verandert naar aanleiding van innovatie, veranderingen in de maatschappij en wettelijke verplichtingen.

Voorbereiding

We starten altijd met een **nulmeting**: wat is de situatie nu? Welke afdelingen zijn er? Wat is het niveau van bewustwording? Hoe ziet de bedrijfscultuur eruit? Zo krijgen we zicht op de omstandigheden, het kennisniveau, houding en gedrag, informatiebeveiligingsbeleid en tijd- en stressfactoren in de organisatie. Aan de hand daarvan stemmen we samen af welk maatwerk daarbij past. De inhoud van het proces moet ook aansluiten op de beveiligings- en privacyregels van de organisatie. Maatwerk, soms zelfs per afdeling, leidt tot betere resultaten. Hanteer dus geen uniforme aanpak. Het heeft alles met cultuur en gedrag te maken. Om de bewustwording te vergroten kan een multilevel-aanpak de oplossing zijn.

Aandacht

De aanpak moet zich op de persoon richten met een **heldere doelstelling en boodschap**. De boodschap en de inhoud richt zich op het professionele en privéleven van de persoon. Als de leerstof, de tips en de tools ook in een privésfeer bruikbaar zijn, dan sluit dat beter aan en blijven deze langdurig hangen. Beveiligings- en privacyregels toepassen is geen werkwijze, maar een manier van leven.

Lifestyle

Omdat de traditionele campagne vaak als saai en weinig doeltreffend wordt ervaren, is het vooral van belang om **innovatieve middelen** in te zetten. Privacy- en informatiebeveiliging heeft een hoog "droog-stof" gehalte. Het is zeker mogelijk om deze stof in een moderner jasje te gieten. Denk aan:

- Het gebruik van smartphones met online quiz of gaming.
- Een e-learningomgeving combineren met een certificaat of beloningsysteem.
- Korte films met humor en wetenswaardigheden.
- Een opstart pop-up scherm met tip van de dag om de kennis op peil te houden.
- Het publiceren van een dedicated webpagina op intranet met aantrekkelijke links.

Implementatie

Controle is belangrijk. Dit hoort bij de **lifecycle** van beveiliging en privacy. Beloning naar aanleiding van het melden van datalekken in plaats van straffen, is één van de mogelijkheden. Maandelijkse bijeenkomsten organiseren (pizzasessies) met de medewerkers om de datalekken of beveiligingsincidenten als leerstof te bespreken kan ook nuttig zijn.

Meten

Meten is weten. Met kennis en inzicht in de effectiviteit van een campagne als resultaat. Met behulp van een goede nulmeting en tussentijdse evaluatie(s) kan men de aanpak in de gewenste richting bijsturen. Met behulp van meetbare doelen, zoals: het aantal behaalde certificaten, de bestede tijd aan de verwerving van de kennis, en het aantal deelnemers op de kennissessies per leeftijdscategorie, krijgt u meer inzicht. Er zijn verschillende manieren, buiten een enquête, om de resultaten van de kennis te meten. Een van de opties is het inzetten van een **mystery visitor**. Een andere mogelijkheid is het inlassen van een reguliere securityronde in de organisatie door de CISO/DPO.

Interesse in onze aanpak?

Wij helpen u graag om de bewustwording van informatiebeveiliging en privacy binnen uw zorginstelling te vergroten. Voor meer informatie neemt u contact met ons op via onderstaande gegevens.

[contactgegevens in footer]