Wachtwoordprotocol

Hoe veilig is het security protocol van Stichting Palludara? Dataverlies of -diefstal is één van de grootste nachtmerries die je kunt hebben. Je moet namelijk direct melding doen bij de Autoriteit Persoonsgegevens waarbij jouw organisatie risico loopt op een flinke dosis imagoschade en ook nog eens een boete te krijgt.

De Wet Meldplicht Datalekken (ingegaan op 1 januari 2016) gebiedt organisaties, waar sprake is geweest van een hack, direct melding te laten doen van het datalek. Dit moet bij zowel de Autoriteit Persoonsgegevens als klanten van de organisatie. De boete die een bedrijf kan krijgen loopt al gauw op tot wel 810.000 euro. Dit geldt met name wanneer er sprake is van nalatigheid. Naast de mogelijkheid van een datalek is er een risico dat kwetsbaarheden worden uitgebuit, spam wordt verstuurd vanuit het gehackte systeem, DDoS-aanvallen (pogingen om een computer/-netwerk/-dienst onbeschikbaar te maken voor de bedoelde gebruiker) worden gepleegd en meer. Het verkrijgen van basisgegevens is vaak al genoeg; er is niet zo heel veel voor nodig om de dienstverlening van een organisatie in gevaar te brengen.

De motivaties voor aanvallen kunnen variëren; van het verzamelen van financiële gegevens en privé gegevens van medewerkers, tot bedrijfsspionage of het verspreiden van malware

Het grootste risico op lekken is toch vooral het gevolg van menselijke nalatigheid. Om te voorkomen dat mensen die daar geen recht toe hebben kunnen inloggen in onze systemen zijn er vooral op het gebied van wachtwoorden een aantal afspraken nodig.

Afspraken omtrent wachtwoorden

- Wachtwoorden zijn minimaal tien tekens lang en bevatten een cijfer en een leesteken
- Wachtwoorden die je prive gebruikt mag je niet voor je werk gebruiken.
- Wachtwoorden worden alleen op papier gezet, wanneer zij achter slot en grendel bewaakt worden. Een wachtwoordmanager wordt aangeraden (lastpas of keepas)
- We maken onderscheid in de applicaties die we gebruiken. Applicaties die we als hoog scoren en die bijzondere persoonsgegevens bevatten beveiligen we extra goed.

Afspraken omtrent wachtwoorden voor applicaties met bijzondere persoonsgegevens:

Het gaat hierbij om de applicaties: Parnassys en de serveromgeving van Accent. De website/ouderportaal verwerkt persoonsgegevens en met name foto's. Snappet en verschillende educatieve applicaties wel of niet onder Basispoort verwerken persoonsgegevens en met name toetsgegevens. Voor mederwerkers zijn de persoonsgegevens in AFAS een aandachtspunt.

- *De serveromgeving van Accent krijgt een lang wachtwoord, van tien tekens met een cijfer en een teken erin en wordt twee keer per jaar verplicht vervangen.*

- *Parnassys wordt beveiligd met een lang wachtwoord van tien tekens met een cijfer en een teken er in. En wordt jaarlijks verplicht vervangen.*
- *De website krijgt een lang wachtwoord en wordt jaarlijks aangepast. Op het communicatieportaal kun je direct toegang krijgen tot de AFAS omgeving en later ook tot Parnassys, mail en agenda.*
- *Het wachtwoord voor Snappet blijft gelijk. Toegangsrechten worden aangepast ism Snappet*
- *Basispoort applicaties worden benaderd via de serveromgeving van Accent. Andere applicaties zullen per applicatie beoordeeld worden op veiligheid en wachtwoordeisen*

Deze afspraken worden gecommuniceerd met de medewerkers:

DE DRIE BASISREGELS VOOR WACHTWOORDEN.

1. JE WACHTWOORD MAG JE NOOIT DELEN, DAT IS IETS VAN JOU.
2. JE WACHTWOORD MAG NIET MAKKELIJK TE RADEN ZIJN

   (BIJVOORBEELD EEN 'WACHTZIN' MIJNKATISLIEFENNIETGROEN!)
3. JE WACHTWOORD MAG JE NIET HERGEBRUIKEN. GEBRUIK VOOR ALLES EEN EIGEN WACHTWOORD.

Wanneer je het vermoeden hebt dat iemand je wachtwoord onrechtmatig heeft gebruikt, moet er melding gedaan worden naar de beveiligingscontactpersoon binnen je werkomgeving (security officer of beleidsmedewerker ICT) Zij kunnen helpen met het aanpassen van het wachtwoord en onderzoeken of er ook schadelijke gevolgen zijn opgetreden.