ICT-beleid binnen de H.E.M.A.-bond en geassocieerde clubs.

Door Robin Verhoef,
Veiligheidscomissie HEMAbond

Inhoud

1. Voorwoord

Dit document heeft als doel om standaarden vast te leggen waar de HEMA-bond en zijn leden aan moeten voldoen om een kwalitatief acceptabele bescherming van de gegevens van zijn leden te garanderen. Het doel is de methodes zo makkelijk mogelijk te maken, met software die of voor iedereen beschikbaar is of betaalbaar is. Het beschermen van de gegevens is een wettelijke en ethische plicht. Door de aard en het doel van de verzameling van de gegevens worden er namelijk veel persoonlijke gegevens verzameld en zelfs ook bijzondere persoonsgegevens zoals gegevens over de medische situatie van leden.

2. Wachtwoordbeleid

In dit document zal het veel gaan over wachtwoorden voor bijvoorbeeld de versleuteling van gegevens of de toegang tot die gegevens. Van alle wachtwoorden die toegang geven tot persoonsgegevens moet bekend zijn wie ze heeft. Verder mogen deze nooit digitaal gedeeld worden. Dit wil zeggen dat de wachtwoorden niet via sms, whatsapp of email verstuurd worden. Bellen of skypen en dan het wachtwoord zeggen is prima. Dit voorkomt dat de wachtwoorden ergens digitaal onversleuteld opgeslagen worden. Wachtwoorden moeten langer zijn dan 10 tekens. Er hoeven geen cijfers of leestekens in te zitten. Dit helpt wel een beetje, maar wachtwoorden die moeilijk zijn te onthouden zijn ook onveilig omdat ze opgeschreven moeten worden.
De beste methode om een mensvriendelijk wachtwoord te maken is de volgende. Zoek 5 dobbelstenen of ga naar deze[1] website. Voer in de velden van boven naar beneden 1, 6, 1 in. Druk op *get sequence*. Schrijf de eerste 5 cijfers op en herhaal nog 2 keer. Dit kan dus ook met dobbelstenen. Ga daarna naar deze[2] website en vind de woorden die bij je 3 cijfers horen met behulp van CMD + F op Apple of ctrl + f op Windows. Je hebt nu 3 random woorden. Deze zijn je wachtwoord. Je mag zelf de volgorde bepalen.
Reden waarom: dit artikel[3] en dit artikel[4]
Je kunt ook een wachtwoordbeheerprogramma gebruiken en dat een random wachtwoord laten maken. Hierbij moet het hoofdwachtwoord dan wel weer veilig zijn.

[1] https://www.random.org/sequences/
[2] http://theworld.com/~reinhold/DicewareDutch.txt
[3] https://blog.agilebits.com/2011/06/21/toward-better-master-passwords/
[4] http://www.explainxkcd.com/wiki/index.php/936:_Password_Strength

3. Toegang tot gegevens

Voor alle opslag van persoonsgegevens moet een lijst bijgehouden worden van wie het wachtwoord heeft. Bij een wisseling van bijvoorbeeld het bestuur van een vereniging moeten alle wachtwoorden worden veranderd om zo de toegang van de oud-leden te beperken. Ook moeten alle oud-leden alle bestanden met persoonsgegevens verwijderen van hun persoonlijke apparaten. Alle clubs die lid zijn van de HEMA-bond en de HEMA-bond zelf moeten streven om de ledengegevens zo snel mogelijk alleen op een versleutelde server op te slaan, en eventueel een goed beveiligde back-up. Hierbij kan software als LedenAdministratieOnline helpen, zie 5. Bij de HEMA-bond moeten alle wachtwoorden van de diensten die het bestuur gebruikt veranderd worden. Dit zal gebeuren onder toezicht van de voorzitter van de veiligheidscommissie. Hierbij zullen de oud-bestuursleden hun oude wachtwoorden invullen om daarna het nieuwe bestuur nieuwe wachtwoorden te laten kiezen. Deze kunnen het best van tevoren afgesproken worden en gemaakt op de manier uit 2. Wachtwoordbeleid.

4. Email

De emailadressen die leden aan hun club of aan de HEMA-bond geven zijn privégegevens en vaak ook hun privé emailadres. Deze gegevens moeten beschermd worden. Om te voorkomen dat iemand de emailadressen iedere keer dat er een mail wordt gestuurd moet kopiëren en plakken is het verplicht om een emailservice zoals MailChimp te gebruiken. Een **Starting up** account kost niks, zolang je niet meer dan 12000 mails per maand verstuurt of meer dan 2000 mensen op je emaillijst hebt. Op dit moment is dit voor geen enkele club binnen de HEMA-bond het geval. Met een service als MailChimp voorkom je het uitlekken van gegevens.

5. Ledengegevens

Het beveiligen van ledengegevens is wat moeilijker. Deze worden namelijk in een aantal formats opgeslagen zoals Excel spreadsheets, SQL databases en misschien ook op papier. Hiervoor is niet een universele oplossing. Wel zijn er om te beginnen een paar algemene tips.

1. Gebruik voor alles waar een wachtwoord wordt gevraagd de tips uit het wachtwoordenbeleid. Schrijf dit wachtwoord zo min mogelijk op en als het echt moet, dan het liefst op papier en berg dit op een veilige plek op.
2. Verzamel niet meer gegevens dan je nodig hebt. Immers, hoe minder gegevens je hebt, hoe minder je er kwijt kunt raken.

Van verenigingen.nl:

In vier stappen een betere beveiliging van de ledenadministratie bij vereniging en club:

1. Bewustwording bestuur en administratie
2. Betrouwbare webserver
3. Up-to-date administratie software
4. Installeren extra veiligheidsvoorzieningen

1. Als eerste moet het bestuur van de verenging zich bewust worden van de noodzaak van gegevensbeveiliging. De ledenadministratie en webmaster moeten vervolgens weten dat de gegevens van leden vertrouwelijk zijn en dus vertrouwelijk moeten worden behandeld.
   Aangezien zij toegang hebben tot de database, zullen ze een sterk wachtwoord moeten kiezen, voorzichtig met hun wachtwoord moeten omspringen, en het regelmatig wijzigen. Omdat e-mail via het openbare internet wordt verstuurd, is het niet aan te raden om de ledenadministratie export of een wachtwoord per e-mail te versturen naar derden.

2. Een tweede stap is het kiezen van een hostingbedrijf die zijn beveiliging goed op orde heeft. Het is geen uitzondering dat aanbieders van webhosting op verouderde servers de websites van klanten draaien. Dit gebeurt met name bij de prijsconcurrenten, die eigenlijk alleen geschikt zijn voor particulieren die het niet erg vinden als hun gegevens zoek raken, of zelfs door anderen kunnen worden beheerd. Een hostingbedrijf moet dus de server software goed up-to-date houden en een goede firewall hebben geïnstalleerd. En software installeren die inbraakpogingen ieder moment van de dag in de gaten houdt.

3. De derde stap is het up-to-date houden van de software waarop de website draait: vaak worden door verenigingen en clubs CMS-en gebruikt, waarmee de website wordt beheerd. Voor dergelijke software, zoals Joomla, komen geregeld bug fixes uit, en die moeten zo snel als

mogelijk worden "geüpdate"; de programmacode van opensource is openbaar, maar dat geldt ook voor de fouten. Zo kan uw neefje van 10 versie 1.5 van Joomla waarschijnlijk hacken, maar de actuele versie 2.5 niet.

4. De laatste stap is het toevoegen van extra beveiligingsoplossingen, zoals een certificaat voor https of uitbreidingen van het CMS. Voor Joomla bestaan er bijvoorbeeld uitbreidingen die het aantal foute inlogpogingen vanaf een bepaald IP-adres bijhouden, en na drie of vijf pogingen dat IP-adres voor een dag te blokkeren. Ook is het mogelijk de gevoelige informatie in de database versleuteld op te slaan, zodat die informatie alleen nog door de administratie op te vragen is met een wachtwoord zin.

Conclusie

Bovenstaand zijn vier stappen benoemd die een vereniging of club zou moeten nemen om de beveiliging optimaal te houden. Heeft uw vereniging geen zin, tijd of kennis om dit te doen, neem een goede partij in de arm die deze zaken voor uw vereniging oppakt. Beveiliging is geen eenmalige activiteit; dit hoort bij het omgaan met vertrouwelijke gegevens een continu proces te zijn, dat begint met bewustwording bij de mensen die met die gegevens omgaan, en resulteert in een constante verbetering van de veiligheid.

Over de auteur: Mark Boos, eigenaar van LedenAdministratieOnline.com, werkt sinds 1999 samen met specialisten om de veiligheid van de websites van zijn klanten te optimaliseren.

LedenAdministratieOnline is een optie voor ledenadministratie.

5.1. Standaard computerbeveiliging

Volg deze[5] gids van De Correspondent om je computer waar je ledengegevens opslaat beter te beveiligen.

5.2. Excel

Als ledengegevens in een spreadsheet opgeslagen worden, moet dit bestand op een harde schijf staan die versleuteld is (zie 5.1.) en op de computer moet ook een goed wachtwoord zitten. Als je een spreadsheet met ledengegevens gaat versturen, versleutel deze dan met bijvoorbeeld Veracrypt (https://veracrypt.codeplex.com/) of GPG suite

---

[5] https://decorrespondent.nl/5243/de-digitale-zelfverdedigingsgids-bescherm-jezelf-op-het-web/255318371-e8ae3068

(https://gpgtools.org/gpgsuite.html). Zo hoef je niet te vertrouwen op de beveiliging van de email server. Zorg dat er een lijst is van iedereen die het wachtwoord heeft en zorg ook dat bijvoorbeeld kinderen niet in het computeraccount kunnen waarop de spreadsheet opgeslagen is.

5.3 SQL

Als ledengegevens in een SQL database opgeslagen zijn, zorg dan voor goede wachtwoorden en ook een lijst van mensen met toegang. Zorg er verder voor dat updates zo snel mogelijk worden geïnstalleerd.

5.4 Cloudopslag

Oplossingen als Google Drive en een versleutelde Dropbox map zijn oke als niemand de bestanden download, voor toegang een account nodig is wat door iemand uitgenodigd/toegevoegd moet worden. Verder worden de wachtwoordregels dan wel uitgebreid naar deze accounts. Ook moet de computer nog steeds een goed account hebben! Dit omdat de meeste mensen hun google drive account niet uitloggen waardoor iemand met toegang tot de computer alsnog bij de gegevens kan.

5.5 Papier

Als je nog een papieren administratie gebruikt, zorg dan dat alle gegevens achter een slot worden opgeborgen en ook hier weer een lijst met iedereen die toegang heeft.

5.6 Oud-leden gegevens.

Gegevens van oud-leden, personen die geen lid meer zijn van een club, mogen nog maximaal tot een maand na het einde van het boekjaar waarin zij hun lidmaatschap hebben opgezegd bewaard worden. Na afloop van het boekjaar moeten de gegevens zo snel mogelijk verwijderd worden.

6. Verantwoordelijkheid voor gegevens

Iedereen die op een toegangslijst van een bestand met persoonsgegevens staat is verantwoordelijk voor de geheimhouding en beveiliging van deze gegevens. Dat houd dus o.a. in dat hij/zij zorgvuldig met het bestand omgaat en minimaal alle tips uit deze gids volgt.

6.1 Verantwoordelijkheden en bestuursleden

Leden van het bestuur van een club die aangesloten is bij de HEMA bond of leden van het bestuur van de HEMA bond zelf moeten een verklaring ondertekenen waarin zijn aangeven de gegevens waar zij toegang tot krijgen geheim zullen houden en deze ook tot hun beste vermogen zullen beveiligen. Verder zullen zij verklaren dat zij, nadat zij uit het bestuur zijn gegaan – op welke manier dan ook -, zij alle persoonsgegevens van hun digitale apparaten en bijbehorende servers zullen verwijderen. Denk hierbij aan email servers, smart phones en computers. Er wordt wel naar gestreefd door het bestuur om de hoeveelheid persoonsgegevens op persoonlijke apparaten te verminderen en zo snel mogelijk overbodig te maken.

7. Nawoord

Graag ontvangen wij tips en toevoegingen op dit bestand op het emailadres veiligheid@hemabond.nl o.v.v. gegevensbescherming. Deze gids biedt geen garanties tegen gegevenslekken, maar wij hopen de kans sterk te verlagen door effectieve en gemakkelijke middelen te bieden die de veiligheid verbeteren.

Veiligheidscommissie HEMA bond