WACHTWOORDBELEID

vzw Onderwijsinrichting van de Ursulinen te Onze-Lieve-Vrouw-Waver

voor:

Sint-Ursula-Instituut (instellingsnummers 126946, 126953, 126961)

Bosstraat 9

2861 Onze-Lieve-Vrouw-Waver

Deze nota maakt deel uit van het informatieveiligheids- en privacybeleid (IVPB).

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-05-25	GELDIG	A. Vanhaeren, AIV	

1 Inleiding

Een goed beveiligingsbeleid is tegenwoordig noodzakelijk voor elke school. Steeds meer privacygevoelige gegevens worden (online) gedeeld en een zwak beveiligingsbeleid zorgt ervoor dat je de deur openzet voor duidelijke risico's. Een goed beveiligingsbeleid geeft gebruikers (leraren, leerlingen, CLB-medewerkers…) toegang tot alle informatie die ze nodig hebben om hun taak naar behoren uit te oefenen maar ontzegt hen alle toegang tot informatie die ze niet nodig hebben.

Er zijn drie pijlers waarop een goed beveiligingsbeleid berust: **authenticatie**, **autorisatie** en **auditing**.

Authenticatie is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). Vaak doen we dit door combinatie van een gebruikersnaam en een wachtwoord.

Autorisatie is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen. Bijvoorbeeld: een leraar zal toestemming hebben om in het puntenboek van de klas te schrijven, de leerling mag alleen zijn eigen punten lezen. Enkel de leerlingencoaches, de zorgverantwoordelijke en de directie kan in het zorgdossier van een leerling schrijven.

***Auditing* (*Controleerbaarheid*)** is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet. Vaak heb je hiervoor een hulpmiddel nodig dat je kan vertellen wat er op elk moment gebeurde. Dit kan onder meer in de vorm van een logboek.

In dit document zullen we ons beperken tot de authenticatie en in het bijzonder het gebruik van wachtwoorden en andere, bijkomende authenticatiemethodes in het Sint-Ursula-Instituut.

Deze nota valt onder de eindverantwoordelijkheid van vzw Onderwijsinrichting van de Ursulinen te O.-L.-V.-Waver.

2 Toegangsbeheer

De algemeen directeur van de school is verantwoordelijk voor het gebruikersbeheer van de organisatie. Gebruikersbeheer houdt het aanmaken van gebruikers, toekennen van rechten en stopzetten van rechten in. Dit betekent dat er in de school een inventaris moet opgezet worden die het overzicht houdt van alle rollen en rechten gekoppeld aan personeelsleden in de school.

Het opzetten van een dergelijke procedure rond het toegangsbeheer is belangrijk om de controle te kunnen houden op alle gebruikers die er zijn in de organisatie. Dit is de eerste stap in het authenticatiebeleid.

Zie ook § 3 in het onderdeel van de ***toegangsmatrices***, waarin het vergrendelingsbeleid uitgewerkt wordt.

3 Authenticeren

Er zijn verschillende manieren om je in systemen te authenticeren. De meest gebruikte vorm is de combinatie van een gebruikersnaam en een wachtwoord. Een ander voorbeeld is het gebruik van je bankkaart en je pincode waarmee je je aan een bankautomaat kan authenticeren. Maar ook een vingerafdruk of een irisscan kunnen gebruikt worden om te kijken of je wel diegene bent die je beweert te zijn.

Wachtwoorden zorgen er mee voor dat de toegang tot applicaties goed beveiligd is. Het is dus van belang om een sterk beleid op te zetten om het inlogproces en -procedures te beheren. In het Sint-Ursula-Instituut werken we er continu aan om leraren en leerlingen het belang van sterke wachtwoorden bij te brengen.

Een wachtwoordbeleid heeft als doel enkele bepalingen op te leggen rond het correct gebruik van wachtwoorden om de toegang tot gevoelige data (waaronder privacygevoelige persoonsgegevens) te beveiligen middels een wachtwoord.

Een sterk wachtwoord is moeilijker te achterhalen en dus veiliger dan een 'zwak' wachtwoord. De sterkte van een wachtwoord hangt af van de lengte, complexiteit en de onvoorspelbaarheid.

3.1 Wachtwoordbepalingen

We raden aan om rekening te houden met onderstaande richtlijnen bij het aanmaken van een wachtwoord.

- Hoe langer een wachtwoord, hoe beter. Het is aan te raden om een wachtwoord van minstens 12 karakters te gebruiken. (*Tegenwoordig zijn 8 karakters heel snel te raden.*)
  Beter nog is om te werken met een wachtwoordzin (bijv: `IkGaSinds2015NaarDeSchool`).
- Mix hoofdletters, kleine letters en tekens door elkaar. Gebruik volgende tekens in het wachtwoord:
  - hoofdletters;
  - kleine letters;
  - cijfers;
  - niet-alfanumerieke karakters.

  Bijv. `P@dd€nsto€l579`

- Gebruik de hoofdletters en andere karakters best niet in het begin van het wachtwoord/wachtzin en wissel ze met elkaar af. Bijv. `p@dd€NSto€l579`
- Keer woorden om. Bijv. `l€otSN€dd@p579`
- Maak wachtwoorden/wachtzinnen die enkel betekenis hebben voor jou.
- Verander minstens één keer per schooljaar je wachtwoord.
- Gebruik verschillende wachtwoorden voor verschillende applicaties. We raden je aan om je wachtwoord niet te hergebruiken.
- Indien de ICT-dienst een wachtwoord instelt of “reset” (zie ook § 3.5) voor een bepaald platform of voor het netwerk, dan zal de gebruiker dit steeds moeten veranderen naar een persoonlijk wachtwoord, bij de eerste aanmelding.

Gebruik een online tool om te zien hoe sterk jouw wachtwoord is: bijv. https://veiliginternetten.nl/wachtwoord-check

3.2 Afraders

We raden aan om rekening te houden met onderstaande richtlijnen bij het aanmaken van een wachtwoord.

- Gebruik geen voor de hand liggende namen, woorden of getallen.
  Bijv. `NaamVoornaamGeboortedatum` of `StraatnaamNr`
- Schrijf het wachtwoord niet op: noch op papier noch elektronisch in jouw gsm of pc. Bewaar ze zeker niet op een Post-it aan de computer.
  - Indien je toch liefst je wachtwoord opschrijft, bewaar het dan ver van de gebruiker en schrijf er niet bij voor welke applicatie het dient.
- Geef het wachtwoord niet door, op geen enkele wijze aan niemand (ook niet aan iemand van ICT).
- Verzend nooit een wachtwoord via e-mail of een ander communicatiesysteem. (Niemand van het Sint-Ursula-Instituut zal ooit je wachtwoord, om eender welke reden, op deze manier opvragen.)
- Zorg dat niemand op je vingers kijkt bij het ingeven van een wachtwoord.
- Er is soms de optie om een wachtwoord (even) te tonen, zodat je typfouten kan controleren. Zorg dat er niemand meekijkt op het moment dat je dit gebruikt.
- Besteed bijzondere aandacht aan een externe projectie indien die aangesloten is, zoals bv. een beamer of (groot) tweede scherm.
- Gebruik geen woord uit het woordenboek.
- Herhaal niet te veel karakters of nummers (bijv. `11223344`).
- Gebruik geen te makkelijke wachtwoorden (bijv. `NaamAchternaamGeboortejaar`, `azertyuiop`).
- Bewaar je wachtwoord niet in de browser.
- Maak geen gebruik van de functie om ingelogd te blijven in een bepaalde applicatie.
- Gebruik andere wachtwoorden dan privé-wachtwoorden.

3.3 Wachtwoordbeheer

- Laat de computer nooit onbeheerd achter maar vergrendel het scherm of log uit.
- Na 40 minuten inactiviteit valt de computer automatisch in slaapmodus en wordt het scherm vergrendeld.
- Bij een eerste aanmelding in wijziging van het wachtwoord wordt gecontroleerd op het gebruik van goede wachtwoorden.

3.4 Wat doen bij vermoeden van misbruik?

Misbruik kan ontvreemding of onrechtmatig gebruik van een wachtwoord zijn.

- Verander het wachtwoord onmiddellijk.
- Neem direct contact op met het aanspreekpunt informatieveiligheid of de dienst ICT (ict@sui.be). Meldpunt datalekken: privacy@sui.be.

Deze personen gaan na of er sprake is van een misbruik en proberen zo nodig de schade te herstellen.

3.5 Wat doen indien het wachtwoord vergeten werd?

- Blijf niet proberen; na een aantal pogingen zal je account vergrendeld worden (zie § 3.3).
- Indien het platform over deze mogelijkheid beschikt, kan je de “wachtwoord vergeten”-optie gebruiken. Meestal zorgt dit ervoor dat er een link gestuurd wordt naar een vooraf ingesteld “backup” e-mailadres, waarmee men een nieuw wachtwoord kan instellen (zonder het vorige te kennen).
- Anders neem je persoonlijk contact op met de dienst ICT via ict@sui.be. Zij zullen een nieuw wachtwoord instellen (d.i. een “wachtwoordreset”) waarmee de gebruiker terug kan aanmelden.

3.6 Gebruik van wachtwoordmanagers of een wachtwoordkluis

Indien je te veel wachtwoorden moet onthouden, raden we je aan om gebruikt te maken van een wachtwoordkluis. Wachtwoordkluizen slaan al de wachtwoorden versleuteld op in een beveiligd bestand. Dit bestand wordt geopend met één sterk wachtwoord. Dit wil zeggen dat er maar één wachtwoord meer nodig is om alle wachtwoorden veilig te ontsleutelen.

De volgende wachtwoordkluizen werden veilig bevonden voor onze school:

- KeePass (http://keepass.info/)
- LastPass (https://lastpass.com/nl/)
- Dashlane (https://www.dashlane.com/)
- 1Password (https://agilebits.com/onepassword)
- Passwordsafe (https://www.pwsafe.net/)
- iCloud-sleutelhanger (voor iPad)

4 Risico’s

Aan een slecht wachtwoordbeleid zijn risico’s verbonden. Met dit beleid willen we onderstaande risico’s verkleinen en/of uitschakelen.

- **Identiteitsdiefstal:** iemand die jouw wachtwoord achterhaalt, kan zich binnen de systemen in kwestie voordoen met jouw identiteit. Alle handelingen die men met jouw account stelt, worden via logging teruggebracht naar jezelf en niet naar diegene die met je digitale identiteit aan de haal ging.

- **Phishing:** via phishing proberen oplichters achter persoonlijke gegevens/wachtwoorden te komen, meestal via e-mail of telefoon. Met deze informatie kunnen oplichters persoonlijke gegevens stelen en publiceren.

  Zie ***Achtergrondinformatie*** – § 1 voor meer informatie rond “phishing”.

- **Hacking:** door zwakke wachtwoorden wordt het zeer eenvoudig om in te breken in de informatiesystemen. Eens binnen in het systeem kan er zeer veel schade berokkend worden en kunnen gegevens gestolen worden.

Rond deze risico’s worden alle personeelsleden, maar zeker ook de leerlingen en ouders, binnen het Sint-Ursula-Instituut actief en herhaaldelijk gesensibiliseerd.

O.a. via Safe on Web kan er veel praktisch materiaal gevonden worden rond dit beleid en rond de hier vermelde risico’s:

https://www.safeonweb.be/nl/home