WACHTWOORDBELEID

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

Leuvense Katholieke Scholen aan de Dijle VZW

voor:

Heilige-Drievuldigheidscollege secundair onderwijs (126094 en 32995)

Versie	Datum	Auteur(s)	Opmerkingen
1.0	2018-05-26	Niels Roelands	Eerste versie

Inhoud

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 (leerkrachten, 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 wachtwoord.

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

Deze nota valt onder de eindverantwoordelijkheid van de Leuvense Katholieke Scholen aan de Dijle VZW.

2 Toegangsbeheer

De directeur van de school is verantwoordelijk voor het gebruikersbeheer van de organisatie. De directeur wordt hierin bijgestaan door de beheerder(s). Gebruikersbeheer houdt het aanmaken van gebruikers, toekennen van rechten en intrekken 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 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. Op het Heilige-Drievuldigheidscollege werken we er continu aan om leerkrachten 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

- Hoe langer een wachtwoord hoe beter. Het wachtwoord moet minstens 8 karakters hebben.
  Beter nog is om te werken met een wachtwoordzin (bv: IkGaSinds2018NaarDezeSchool)
- Mix hoofdletters, kleine letters en tekens door elkaar: gebruik minstens 3 van de volgende 4 tekens in het wachtwoord:
  - Hoofdletters
  - Kleine letters
  - Cijfers
  - Niet-alfanumerieke karakters
    Bv: P@dd€nsto€l159
- Gebruik de hoofdletters en andere karakters best niet in het begin van het wachtwoord/wachtzin en wissel met elkaar af.
  Bv: p@dd€NSto€l159
- Keer woorden om.
  Bv: l€otSN€dd@p159
- Maak wachtwoorden/wachtzinnen die enkel betekenis hebben voor jou.
- Verander minstens één keer per schooljaar je wachtwoord.
- Gebruik verschillende wachtwoorden voor verschillende applicaties en hergebruik je wachtwoord niet!
- Indien de ICT-dienst een wachtwoord instelt of “reset” (zie ook §3.5) voor een bepaald platform 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, bv: https://veiliginternetten.nl/wachtwoord-check

3.2 Afraders

- Gebruik geen voor de hand liggende namen, woorden of getallen, bv: NaamVoornaamGeboortedatum of StraatnaamNummer
- Schrijf het wachtwoord niet op: niet op papier, niet elektronisch in jouw GSM of PC en 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!
- Verzend nooit een wachtwoord via email of een ander communicatiesysteem. (Niemand van het Heilige-Drievuldigheidscollege 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 (even) je wachtwoord te tonen, zodat je typfouten kan controleren. Zorg dat er niemand meekijkt op het moment dat je dit gebruikt.

- Besteed bijzondere aandacht aan externe projectie indien dat aangesloten is, zoals bv. een beamer of een tweede scherm.
- Gebruik geen woord uit het woordenboek.
- Herhaal niet te veel karakters of nummers.
- Gebruik geen te makkelijke wachtwoorden.
- 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

- Na 5 pogingen om in te loggen wordt het account vergrendeld. Neem contact op met de dienst ICT om het account terug te ontgrendelen.
- Laat de computer nooit onbeheerd achter maar vergrendel het scherm of log uit.
- Na 20 minuten inactiviteit valt de computer automatisch in slaapmodus en wordt het scherm vergrendeld.
- Er wordt bij zoveel mogelijk applicaties automatisch 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, de dienst ICT en/of systeembeheerder. Meldpunt datalekken: privacy@lksd.ksleuven.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” emailadres, waarmee men een nieuw wachtwoord kan instellen (zonder het vorige te kennen).
- Anders neem je persoonlijk contact op met de dienst ICT en/of systeembeheerder. Zij zullen een nieuw wachtwoord instellen (d.i. een “wachtwoordreset”) waarmee de gebruiker terug kan aanmelden.

3.6 Gebruik van wachtwoordmanagers of wachtwoordkluis

Indien je te veel wachtwoorden moet onthouden, kan je gebruik 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/)

4 Gebruik van two-factor authenticatie

Indien je echt met veel privacygevoelige persoonsgegevens werkt, is vaak een combinatie van gebruikersnaam en wachtwoord niet voldoende veilig. De gebruikersnaam is meestal gekend en een wachtwoord kan eventueel gestolen of ontfutseld worden. Daarom bestaan er two-factor authenticatiemethodes.

Een voorbeeld: Naast het gebruik van een gebruikersnaam en wachtwoord krijg je op je gsm een beveiligingscode doorgestuurd die je dan extra moet ingeven vooraleer je toegang krijgt. Naast het weten van de gebruikersnaam en wachtwoord is het dus ook nodig dat je iets in je bezit hebt, zoals bijvoorbeeld een telefoon waar men via sms een code doorgestuurd krijgt.

Deze systemen zijn veel veiliger en worden binnen het Heilige-Drievuldigheidscollege dan ook toegepast voor iedereen die aan de meest privacygevoelige gegevens binnen de onderwijsinstelling kan. Concreet denken we hierbij aan iedereen die toegang heeft tot ‘geheime’ gegevens (zie **classificatie van gegevens** en **toegangsmatrices**).

5 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 uw account stelt, worden via logging teruggebracht naar uzelf en niet naar diegene die met uw 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 een systeem kan er zeer veel schade berokkend en kunnen gegevens gestolen worden.

Rond deze risico’s worden alle personeelsleden, maar zeker ook de leerlingen en ouders, binnen het Heilige-Drievuldigheidscollege 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