Information Security Management System (ISMS)
Beveiligingsmaatregelen HippoLine

In dit document in het kort onze beveiligingsmaatregelen
Deze zijn opgesteld aan de hand van de richtlijnen van NLdigital

HippoLine versie 01.02 april 2021

Inhoudsopgave

Fysieke toegangscontrole

We beschermen de toegang tot ons kantoor en de middelen die daarin aanwezig zijn.

Ons kantoor bevindt zich op de 2e (bovenste) etage van een pand waar ook andere organisaties toegang toe hebben. Gemiddeld genomen zijn er dagelijks zo'n 15-20 personen in het pand aanwezig.

Ons kantoor is voorzien van een **deurslot.**
Zowel ons kantoor, als het pand zijn voorzien van een deurslot met afzonderlijke sleutel. Al onze medewerkers zijn in het bezit van beide sleutels die nodig zijn om binnen te komen.
Zonder sleutels kan een persoon het pand en ons kantoor niet zomaar binnenkomen.

We hebben een **alarmsysteem**
Het alarmsysteem stellen we op actief wanneer er geen medewerkers aanwezig zijn op kantoor. Het systeem slaat alarm wanneer er toch personen op kantoor aanwezig zijn.
Alle medewerkers beschikken over de (de)activeringscode.
Het alarmsysteem bewaakt het hele pand en is ingesteld per kantoor. Wanneer alle kantoren hun alarmsysteem geactiveerd hebben, wordt ook een alarm op het pand actief.

Maatregelen

- De laatste persoon die het kantoor verlaat doet de *deur op slot* en *activeert het alarm.* Als we de laatste in het pand zijn, doen we ook de *deur van het pand op slot*.
- We controleren dat vertrekkende medewerkers hun *sleutels weer inleveren*

Risico's

Bezoekers worden niet geregistreerd
We leggen niet vast wie er bij ons op bezoek is. Vanwege de omvang van ons kantoor achten we dit niet nodig. Er moet worden aangebeld om binnen te komen, waardoor we op de hoogte zijn van binnenkomende mensen. Het hele kantoor heeft overzicht op de ingang, zodat het voor iedereen direct duidelijk is als er een onbekende binnenloopt.

Onze deur staat open als we aanwezig zijn
We doen de deur tot ons kantoor niet op slot als we aanwezig zijn. De deur tot het pand valt automatisch dicht, waardoor we de toegang voldoende afgesloten achten.
We zijn echter niet op de hoogte van toegang die verleend wordt aan onbekenden door andere kantoren in het pand. In principe kan zo een voor ons onbekende via onze open deur toch toegang krijgen tot ons kantoor. We achten dit voldoende veilig immers we hebben zicht op de ingang en als de laatste collega het kantoor verlaat, gaat de deur naar ons kantoor op slot. Daarbij andere organisaties in het pand laten niet zomaar mensen binnen, en we kunnen indien nodig bij hen navragen wie er toegang tot het pand had. Verder wordt in het pand geen klant /privacy gevoelige data opgeslagen en beschikt het pand niet over een fysieke server.

Toegangscontrole tot systemen

Onze klantgegevens willen we zo goed mogelijk beschermen. We zorgen daarom dat onze medewerkers weten hoe ze met data om moeten gaan. Daarnaast zorgen we dat niet we zomaar gegevens van een ander kan inzien.

Nieuwe medewerkers tekenen een **geheimhoudingsverklaring**
We willen dat onze medewerkers vertrouwelijk omgaan met de gegevens die zij in hun werkzaamheden tegenkomen. Daarom ondertekenen ze onze geheimhoudingsverklaring. Hierin gaan ze onder andere akkoord om de informatie die ze tegenkomen geheim te houden en niet zomaar te delen. Ook niet met collega's.

Medewerkers ondertekenen het document **informatiebeveiligingsbeleid**
We gaan als BI organisatie om met gevoelige data. Daarom willen we dat onze BI-consultants en andere medewerkers op een verantwoorde manier met die data omgaan. We hebben daarom een informatiebeveiligingsbeleid opgesteld, waarin beschreven staat hoe je als werknemer veilig met data omgaat.

Elke nieuwe medewerker ondertekent het informatiebeveiligingsbeleid. Om de awareness rondom veiligheid hoog te houden, bespreken en ondertekenen we elk jaar allemaal het informatiebeveiligingsbeleid opnieuw.

Systemen en applicaties vereisen **authenticatie**
Lokale systemen, cloud systemen en (online) applicaties zijn voorzien van authenticatie met beveiliging. In de meeste gevallen betekent dit dat we een username en wachtwoord gebruiken om toegang te krijgen waarbij gebruik wordt gemaakt van tweefactor authenticatie waar nodig en kan.

Zonder geldige username en wachtwoord heeft een onbekende geen toegang tot (door ons beheerde) data. Als er extra mogelijkheden tot beveiliging zijn, dan maken we hier gebruik van.

Medewerkers hebben individuele **autorisatie**
We willen ervoor zorgen dat onze medewerkers alleen die data kunnen zien, waar zij voor hun werkzaamheden toegang tot moeten hebben. Daarom gebruiken we individuele accounts voor de authenticatie en autorisatie tot gegevens. We kennen verschillende rollen met verschillende toegangsrechten.

We hebben een interne autorisatiematrix waarin we aangeven welke rollen bij welke data kunnen.

Onze **toegangsbeveiliging** kent **eisen**
Medewerkers zijn uiteindelijk zelf verantwoordelijk voor de accounts die ze gebruiken voor authenticatie. In het informatiebeveiligingsbeleid trainen we medewerkers op veilig beheer van deze accounts. Daarnaast hebben we voor de meest belangrijke accounts minimale eisen aan de complexiteit van het wachtwoord en gebruiken we waar mogelijk 2 factor authenticatie.

Toegang tot onze cloudomgeving **minimaliseren** we zoveel mogelijk
Ook onze online toegang houden we graag minimaal. Onze cloudomgeving is voorzien van firewall, waarvoor we alleen die poorten open zetten die nodig zijn.
Buiten het klantportaal is de toegang tot onze (cloud)systemen alleen mogelijk met een VPN. Ook hier geldt dat de toegang individueel geregeld is; iedere werknemer krijgt zijn eigen VPN profiel, die wordt ingetrokken zodra een werknemer vertrekt.

Lokale devices zijn voorzien van **disk encryptie**
We gebruiken laptops en telefoons voor onze dagelijkse werkzaamheden. Dit zijn draagbare apparaten, omdat onze consultants ook vaak bij klanten zitten. Het feit dat we onze apparaten meenemen, maakt dat ze kwetsbaarder zijn voor verlies of diefstal. We gaan er dan ook vanuit dat dit een reële mogelijkheid is. Om in deze gevallen toch dataverlies tegen te gaan, maken we gebruik van disk encryptie. Zonder authenticatie is de data dan onleesbaar.

Maatregelen

- We trekken de toegang tot onze diensten in wanneer een medewerker uit dienst treed
- Een vertrekkende medewerker levert apparaten weer in en wij verwijderen de bestaande data
- We controleren jaarlijks of de rechten van onze klantgebruikers correct zijn

Risico's

Werknemer kan authenticatiegegevens verliezen of delen met anderen
We trainen medewerkers op de veilige omgang met data. Ze weten hoe ze met authenticatiegegevens om moeten gaan. We achten de kans op onbedoeld verlies daarom klein.
Aan de andere kant is er het moedwillig delen van gegevens met (ongeautoriseerde) derden. We monitoren het gebruik van authenticatiegegevens niet, dus we hebben beperkte mogelijkheden om een dergelijk lek te herkennen. We vinden het risico op een kwaadwillende medewerkers echter beperkt. Vanwege onze geringe omvang, zijn we goed geïnformeerd over waar we met elkaar mee bezig zijn.

Integriteit Controle

Omdat we klantdata op onze systemen ontsluiten, is het erg belangrijk dat we kunnen vertrouwen op de integriteit van onze machines. We hebben hiervoor regels opgesteld die we zoveel mogelijk geautomatiseerd uitvoeren. De regels zijn van toepassing in onze cloudomgeving: ons Active Directory en de ondersteunende netwerksystemen.

Onze **wachtwoorden** moeten aan **minimale complexiteit** voldoen
Wachtwoorden voor onze medewerkers moeten aan minimale eisen voldoen. Jaarlijks controleert de directie in LastPass de beveiligingsscore van de medewerkers. Deze moet jaarlijks 80% zijn. In het document “Veilig omgaan met informatie” zijn de richtlijnen voor het gebruik van wachtwoorden voor onze medewerkers opgenomen.

We installeren de laatste **updates**
Om onze systemen te beschermen tegen beveiligingsgaten in de software, updaten we periodiek onze systemen en applicaties.

De **firewall** laat alleen het **noodzakelijke verkeer** toe
We sluiten onze omgeving zoveel mogelijk af en dat houdt onder andere in dat we de poorten dicht zetten. Enkel de essentiële poorten voor onze SaaS staan open naar de buitenwereld.

Risico’s

Om hun werkzaamheden te kunnen verrichten hebben onze consultants een admin rol op de SaaS omgeving. Hiermee kunnen zij zelf applicaties installeren. De afspraak is echter dat applicaties alleen door, of met uitdrukkelijke toestemming van Technisch Beheer worden geïnstalleerd. Op deze manier heeft Technisch Beheer overzicht op de gebruikte applicaties en kan dergelijke software worden geüpdatet wanneer nodig.

Consultants zijn zich bewust dat zij zelf verantwoordelijk zijn voor de updates voor de software en applicaties op de eigen laptop. Updates voor Windows moeten op automatisch updaten staan.

Accounts van klantgebruikers zijn mogelijk kwetsbaarder
De wachtwoorden van onze klantgebruikers verlopen niet automatisch. De klant is zelf verantwoordelijk voor het beheer van haar wachtwoorden. Deze accounts zijn daarmee mogelijk kwetsbaarder dan onze interne accounts, echter de accounts van klanten zijn van elkaar gescheiden en mogelijke kwetsbaarheid heeft dan alleen betrekking op dat specifieke account

We houden systeemactiviteit niet actief in de gaten
Als er verdachte activiteiten plaatsvinden op onze systemen, dan komen we daar mogelijk niet direct achter. We controleren bijvoorbeeld onze log files niet periodiek. Het risico achten we beperkt.

Toegangscontrole tot data

We beschermen onze klantdata door toegang zo veel mogelijk af te schermen.

We **versleutelen** alle **backupdata** in de cloud
Om onze continuïteit te garanderen maken we backups die we op een externe locatie opslaan. Deze data versleutelen we. Zo voorkomen we dat een lek of kwaadwillende werknemer bij de externe locatie bij onze data komt.

We beheren de toegang tot data aan de hand van een **autorisatiematrix**
De rechten die onze medewerkers hebben zijn onderverdeeld aan de hand van een autorisatiematrix. We willen dat klantdata alleen ingezien kan worden door diegenen die dat voor hun werkzaamheden nodig hebben. Dit hebben we geregeld via verschillende rollen die aan accounts gekoppeld worden. Zowel onze medewerkers, als onze klanten zijn gebonden aan deze procedure. Data van de klant is dus alleen zichtbaar door de klant gebruikers zelf en de betrokken consultants.

Klantaccounts wijzigen we alleen na **goedkeuring** geautoriseerd klantcontact
Klanten kunnen via het internet toegang krijgen tot hun BI dashboard. Ze hebben daarvoor een account met de juiste rechten nodig. Het toewijzen van nieuwe accounts, of wijzigen van bestaande, doen we enkel na goedkeuring van een door ons geautoriseerd contact bij de klant.

Door het inschakelen van geautoriseerde klantcontacten verzekeren we dat de klant op de hoogte is van de wijziging en voorkomen we dat ongeautoriseerde personen toegang krijgen tot klantdata.

We gebruiken **geen externe opslagmedia**
Naast onze (draagbare) laptops gebruiken we geen externe opslagmedia, zoals USB-sticks of externe harde schijven. We vinden dat externe opslag te makkelijk verloren of gestolen kan worden.

Risico's

Toegangsrechten kunnen ongemerkt aangepast worden
Onze (IT) administrators hebben controle over onze systemen en toegangsrechten. We monitoren het gebruik van de administrator accounts niet, waardoor een eventuele fout over het hoofd kan worden gezien.

We vinden dit risico gering. Het aantal administrators beperken we tot een minimum om fouten tegen te gaan en voor het dagelijkse werk worden administrator accounts niet gebruikt. Daarnaast doen we andere controles om fouten die een administrator maakt toch boven water te krijgen.

Beveiliging van gegevens in transit

De data die over en weer wordt verstuurd beveiligen we. Op z'n minst gebruiken we encryptie, maar bij voorkeur doen we dataoverdracht via een VPN.

Webverkeer beveiligen we met **TLS encryptie**
Via onze SaaS kunnen gebruikers hun gegevens inzien. Tijdens het gebruik wordt klantdata over (en weer) verstuurd en we willen niet dat deze zomaar uit te lezen zijn.
We maken standaard gebruik van HTTPS om SaaS-data te versleutelen.

Dataoverdracht doen we via **beveiligde kanalen**
Om onze BI applicaties van data te voorzien moeten we data bij de klant ophalen. We doen dit enkel via veilige en versleutelde kanalen.

We hebben een eigen oplossing voor dataoverdracht op basis van een versleutelde FTP verbinding.

Veel van onze klanten gebruiken een VPN om de data te isoleren van het netwerkverkeer.

Risico's

We zijn bij externe afhankelijk van hun netwerkbeveiliging
Onze consultants werken regelmatig bij de klant zelf. Ze sluiten hun apparaten dan aan op het netwerk van de klant en isoleren hun netwerkverkeer niet met een VPN. We doen in principe enkel werk voor de betreffende klant als we extern zitten, waardoor de kans op datalek klein is.
We vertrouwen op de netwerk setup van derden als we extern werken.

Toezicht op invoer van gegevens

De data die wij bewaren voor onze SaaS klanten wordt synchroon gehouden met de klant. Zelf doen we geen bewerkingen; nieuwe en gewijzigde data krijgen we periodiek van de klant. We voeren zelf geen data in en beperken de toegang tot het ophalen van gegevens.

Per overeenkomst **registreren** we **welke data** onze systemen binnenkomt
Bij de overeenkomst met een klant spreken we af met welk soort data er gewerkt wordt. We stellen op dat moment vast of er bijvoorbeeld persoonsgegevens verstuurd worden.

We hebben **gedocumenteerd** waar onze **data opgeslagen** staat
Bij de opzet van een klantomgeving gebruiken we een standaard procedure. Hierin staat vastgelegd waar klantdata wordt opgeslagen.
We weten in alle gevallen waar data voor een bepaalde klant staat opgeslagen.

Risico's

Gegevens van de klant kunnen we aanpassen
We krijgen data van de klant binnen. Technisch hebben we de mogelijkheid om deze data aan te passen. Dit doen we niet en hebben we opgenomen in ons medewerkers beveiligingsbeleid.

Toezicht op sub-verwerkers

We hebben een aantal sub-verwerkers die we gebruiken voor onze SaaS diensten: CloudVPS, Amazon en Auth0. Ons SaaS platform wordt in het geheel gehost op de infrastructuur van CloudVPS. We gebruiken Amazon voor de opslag van onze back-ups.

CloudVPS opereert binnen Nederland en Amazone vanuit de EU. We besteden veel aandacht aan de regelgeving waar onze sub-verwerkers zich aan dienen te houden. Vanuit dat oogpunt werken we graag met dienstverleners binnen Nederland, of anders binnen de EU.

Onze sub-verwerkers zijn **gecertificeerd** voor gepaste **omgang met data**
We houden de certificeringen van onze sub-verwerkers bij. Met betrekking tot onze SaaS zorgen we ervoor dat onze sub-verwerkers gedocumenteerde procedures voor de omgang met AVG hebben.

Maatregelen

- We controleren elk jaar of onze sub-verwerkers nog voldoen aan onze eisen

Risico's

Sub-verwerkers kunnen **toegang** krijgen tot **data**
Dit risico achten we beperkt en niet groter dan bij andere sub-verwerkers. Onze sub-verwerkers zijn gecertificeerd en hebben een verwerkersovereenkomst waar nodig.

Sub-verwerkers kunnen voorwaarden wijzigen
In beginsel zouden wij altijd vooraf geïnformeerd moeten worden over wijzigende voorwaarden en kunnen wij hier, indien nodig op inspelen.

Beschikbaarheid

Voor onze diensten gebruiken we geen eigen hardware. Voor de beschikbaarheid van het SaaS platform zijn we deels afhankelijk van onze cloudprovider. Buiten dat doen we ons best om downtime te voorkomen.

Onze **cloudprovider** heeft een **SLA**
De cloudprovider die we gebruiken voor ons SaaS aanbod garandeert uptime van 99,8%. We kunnen uitgaan van een minimale beschikbaarheid.

Back-ups controleren we op werking
Elk half jaar testen we de back-ups op juiste werking. We hebben een vaste procedure om steekproefsgewijs te controleren of de juiste bestanden geback-upt worden, en of een restore correct uitgevoerd kan worden.

Maatregelen

- We hebben een monitoringsysteem waarmee we onze systemen in de gaten houden. Dit systeem geeft ons automatisch een melding wanneer een systeem onderuit gaat, zodat we snel actie kunnen ondernemen.

Risico's

We hebben geen **alternatief plan**
Bij complete, langdurige uitval van onze cloud provider, hebben we geen gepland alternatief.
Dit heeft mogelijk (langdurige) gevolgen voor de beschikbaarheid van onze diensten.

Onze diensten dragen niet bij aan kritieke bedrijfsprocessen van onze klanten. Daarnaast hanteren we geen afspraken over beschikbaarheid. Bij langdurige uitval kunnen we in enkele dagen op basis van back-ups en/of snapshots en de technische documentatie de omgeving opnieuw toegankelijk en werkend hebben voor de (SaaS) klant.

Gescheiden verwerking

Verschillende componenten van onze infrastructuur worden gedeeld door klanten. Desondanks willen we de verschillende klantomgevingen toch zoveel mogelijk scheiden. Onze nadruk ligt hierbij op het scheiden van (toegang tot) de data.

SaaS **data** van klanten **scheiden** we softwarematig **af**
Onze klantomgevingen zijn zoveel mogelijk gescheiden. Hoe we dit doen verschilt per klant. Dit varieert van volledig gescheiden omgevingen d.m.v. hardware, tot aan softwarematig gescheiden d.m.v. regels met betrekking tot toegangsrechten.
Met de scheiding van klantomgevingen zorgen we dat gegevens afzonderlijk kunnen worden verwerkt.

Risico's

Software regels zijn niet op elkaar afgestemd
We hebben beveiligingsregels op verschillende niveaus: van opslaglocatie tot applicatie. De regels voor de afscherming van gegevens zijn niet standaard op elkaar afgestemd. Voor externe gebruikers heeft dit geen impact, maar interne consultants kunnen via applicatieniveau overige klantdata zien, dit is ook nodig aangezien de consultants elkaar te allen tijde moeten kunnen vervangen.