Beveiligingsincidenten en datalekken: Hoe te handelen?

Contactpersoon AVG Amadeus Lyceum: Kirsten Brons

Inleiding; een beveiligingsincident of datalek op school?
Een datalek op school is erg vervelend. Helaas komt dit wel eens voor. Maar als dit op onze school gebeurt, weet jij wat je moet doen? En wat is eigenlijk het verschil tussen een beveiligingsincident en een datalek?

Datalek of beveiligingsincident
We spreken van een beveiligingsincident als er iets gebeurt met informatie of informatiesystemen, waarbij de kans aanwezig is dat de vertrouwelijkheid, de integriteit of de beschikbaarheid hiervan in gevaar is, of kan komen. Denk bijvoorbeeld aan:

- Besmettingen met virussen en/of malware.
- Pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken).

Bij een datalek gaat het juist om een beveiligingsincident dat gevolgen heeft voor persoonsgegevens, waarbij de kans aanwezig is dat anderen zonder toestemming toegang hebben tot deze informatie. Het risico is dan groot dat anderen deze informatie zomaar kunnen vernietigen, wijzigen of verspreiden. Denk bijvoorbeeld aan:

- Het (per ongeluk) versturen van een e-mail met persoonsgegevens aan een verkeerde geadresseerde.
- Het verliezen van een usb-stick, laptop, of telefoon met persoonsgegevens, terwijl er dit apparaat niet goed beveiligd is.

Conclusie: alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.

Schade door een beveiligingsincident of datalek
Het is duidelijk dat een dergelijk incident schade kan veroorzaken. Bovendien betekent dit ook dat de genomen beveiligingsmaatregelen niet goed genoeg werken. Dit kan grote gevolgen hebben voor de school, en voor degene van wie de persoonsgegevens zijn. Zij verliezen de controle over hun persoonsgegevens. Dit kan leiden tot:

- beperking van eigen rechten;
- identiteitsdiefstal;
- nadelige financiële gevolgen.

Maar ook voor de organisatie kan een incident negatieve gevolgen hebben, zoals negatieve (media)aandacht en imagoschade.

Registratie beveiligingsincidenten en of datalekken
De AVG verplicht ons in bepaalde gevallen een datalek te melden, maar ook hebben wij de verplichting om alle beveiligingsincidenten registreren. Dat geldt óók voor alle incidenten die niet gemeld hoeven te worden. Om alles rondom het melden van beveiligingsincidenten en of datalekken zijn de volgende tools beschikbaar:

- *protocol beveiligingsincidenten en datalekken*;
- *formulier melding beveiligingsincident* (in te vullen door de betrokken school/afdeling);
- *centrale registratie beveiligingsincidenten en datalekken* (in te vullen door functionaris gegevensbescherming/security officer).

Verplicht melden
Om de mogelijke schade te beperken en de juiste vervolgstappen te bepalen, is het **noodzakelijk** om incidenten en datalekken te melden bij de contactpersoon AVG van de

school. Dit is de eerste en daarmee de belangrijkste stap van het proces, immers wat je niet weet, kun je niet herstellen!

Op deze manier kunnen wij gezamenlijk aan de slag om de juiste vervolgstappen te initiëren. Het is duidelijk, dat iedereen die werkzaam is binnen onze school verplicht is om mogelijke incidenten en lekken zo snel mogelijk te melden. Samen met de contactpersoon AVG kun je het *formulier melding beveiligingsincidenten* invullen.
Het formulier wordt vervolgens door de contactpersoon AVG gemaild naar:

- de functionaris gegevensbescherming van de Willibrord Stichting;
- het privacy loket van de Willibrord Stichting: privacy@pcouwillibrord.nl

Daarnaast neemt de contactpersoon AVG **telefonisch contact** op met de security officer van de Willibrord Stichting. Mocht deze niet direct reageren, dan wordt er contact opgenomen met hoofd ICT & IM. Als deze ook niet direct reageert, wordt er contact opgenomen met de functionaris gegevensbescherming van de Willibrord Stichting.

Stappenplan
Als zich een incident voordoet, worden de volgende stappen doorlopen:

1. Signaleren/constateren mogelijk beveiligingsincident
2. Direct melden bij interne contactpersoon AVG.
3. Contactpersoon AVG start in overleg met de melder met het verzamelen van de feiten en beschrijven van het *formulier melding beveiligingsincident (zie hieronder)*
4. Fact finding; het exact definiëren van het beveiligingsincident en/of datalek. Contactpersoon AVG school verzamelt zo veel mogelijk feitelijke informatie en neemt binnen 24 uur contact op met privacy loket.
5. Privacy loket analyseert:
    - het incident en besluit/adviseert of vervolgacties nodig zijn;
    - of melding van data-lek bij de Autoriteit Persoonsgegevens[1] noodzakelijk is, zo ja dan zal dit worden gedaan.
6. Privacy loket informeert het CvB, schoolleiding en AVG contactpersoon van de school van de gedane melding.
7. School en privacy loket bepalen samen welke vervolgacties nodig zijn en leggen deze vast in een actielijst. Deze wordt via de mail met de betrokken personen verspreid.
8. Verzorgen communicatie[2] richting alle direct betrokkenen. Denk hierbij aan:
    - Ouders/leerling/medewerkers die betrokken zijn bij het incident. Dit is de verantwoordelijkheid van de school.
    - ICT leveranciers; mogelijke acties. Dit is de verantwoordelijkheid van de afdeling S&A ICT&IM.
    - Politie (indien noodzakelijk) in onderlinge afstemming

[1] Melden bij de Autoriteit Persoonsgegevens. Dit geldt alleen als er sprake is van een datalek met een hoog risico (hoeveelheid informatie en soort informatie). Deze melding wordt gedaan door functionaris gegevensbescherming in samenwerking met de desbetreffende directeur of rector.
[2] Communicatiemiddel is afhankelijk van grootte en ernst datalek. Mogelijke communicatiemiddelen zijn een telefoongesprek, een brief, een informatiebijeenkomst, etc.

9. School analyseert het incident en formuleert verbetermaatregelen.
   Analyse en verbetermaatregelen worden door de school gedeeld met het privacy loket. Privacy loket geeft eventueel aanvullende tips en adviezen. Indien gewenst/noodzakelijk kunnen de afdelingen van S&A hierbij ondersteunen.
10. School realiseert en communiceert verbetermaatregelen met alle betrokkenen (zie ook
    punt 8).
11. Datalek wordt afgesloten.

Formulier Melding Beveiligingsincident

Melding Beveiligingsincident		
School		
Melding gedaan door		
Contactpersoon		
Telefoon		
E-mail		
Incident nr. PI-YYMMDD-volg nr.		

Beschrijving van de gebeurtenis
Korte beschrijving wat er is geconstateerd

Datum en tijdstip van de gebeurtenis en de constatering
Wanneer geconstateerd*; datum, tijdstip* **Wanneer incident heeft plaatsgevonden***; datum, tijdstip (beste schatting)*

Feiten
Verzamel alle relevante gegevens in relatie tot het incident - *Data* - *Communicatie* - *Gedane acties* - *Betrokken personen bij het incident* - *Etc*

Inventarisatie van de betrokken gegevens				
Type gegevens (financiële, persoons, schoolresultaten, etc)	Omschrijving van de betrokken personen of groep (leerling, verzorgers, ouders)	Kwantitatieve gegevens (welke gegevens; naam, adres, medische, onderzoeken, etc)	Ander betrokken partijen (b.v. ketenpartners, leerplichtambtenaar, etc	Medium (bijvoorbeeld laptop, papier, schijf, usb-stick, etc)

Aard van het beveiligingsincident
Kies een of meerdere van de onderstaande categorieën: 1. Verlies of diefstal van papieren dossier/leerlingdossiers, gegevensdragers zoals usb-stick, tablet of andere gegevensdragers 2. Niet naleven van beleid of richtlijnen 3. Inbreuk op fysieke beveiligingsvoorzieningen 4. Toegangsovertredingen 5. Opzettelijk foutief handelen (fraude, diefstal) 6. Onzorgvuldig omgaan met persoonsgegevens door een bewerker 7. Cyberaanvallen zoals een ddos, computerhacking of besmetting met ransomware, 8. Technische falen van apparatuur, stroomuitval, wateroverlast 9. Anders: Toelichting:

Impact op betrokkene
Inschatting van de consequenties voor de betrokkene/partijen die geraakt worden door dit incident (sensitiviteit van de gegevens)

Opmerkingen
Aanvullende informatie; opvallende zaken, zorgen, risico's, verdenkingen, noodzakelijke/mogelijke acties