Jaarverslag 2014

Informatieveiligheid

Versie	Datum	Auteur(s)	Wijziging	Status	Vertrouwelijkheid
0.1	30/01/2015	Jacques Verleijen		ontwerp	Intern
0.2	26/02/2015	Hélène De Keyser	taalcorrectie	ontwerp	Intern

5-2-2015
Informatieveiligheid
Huis van het GO!
Willebroekkaai 36
1000 Brussel

Inhoudsopgave

Mission statement

Het GO! wil de nieuwe informatie- en communicatietechnologie toegankelijk en beschikbaar maken voor iedereen, met respect voor privacy, de specifieke wet- en regelgeving en conform zijn pedagogisch project. Daarom moet de beschikbare informatie op een veilige manier behandeld worden.

Informatieveiligheid is meer dan het implementeren van technische oplossingen; zij steunt vooral op het bewust maken van alle personeelsleden binnen het GO! zodat zij dit beleid begrijpen, steunen en toepassen.

In die zin streeft het GO! naar een geïntegreerde systeemaanpak, met als resultaat dat de risico's voor de confidentialiteit, de integriteit, authenticiteit en beschikbaarheid van de informatiebronnen en -systemen tot een minimum beperkt blijven.

Het GO! zal zijn veiligheidsbeleid ontwikkelen in overeenstemming met de ISO27000 normen en de richtlijnen van de Vlaamse Gemeenschap.

Voor de uitwerking van dit beleid verwijzen we naar de beleidsverklaring voor informatieveiligheid van het GO! die wordt opgevolgd door de stuurgroep "Informatieveiligheid" en gecoördineerd door de informatieveiligheidsconsulent.

0. Woord vooraf

Op 2 januari 2014 werd het Huis van het GO! in gebruik genomen. Dit was niet enkel een fysieke verhuizing maar ook de start van talrijke nieuwe werkvormen en een volledig nieuwe ICT-infrastructuur. Dit betekent dat er ook veel vooruitgang werd geboekt op het vlak van beveiliging. Het komt er nu op aan om dit in de toekomstige werking te consolideren.

De focus werd verlegd naar de scholengroepen want ook daar wordt de druk van de regelgeving (Vlaams, federaal en Europees) op de onderwijsinstellingen groter.

Onze ambitie reikt hierbij verder dan louter te voldoen aan de wettelijke verplichtingen. Wij willen ook - in overeenstemming met ons pedagogisch project - leerlingen en personeel op een kritische en veilige manier met informatie leren omgaan.

Jacques Verleijen
informatieveiligheidsconsulent (IVC)

Brussel 30 januari 2015

1. Informatieveiligheidsbeleid

1.1. Jaarverslag 2013

Het jaarverslag van 2013 werd op 26 februari 2014 aan de directieraad voorgesteld en daar goedgekeurd. Op 24 maart werd dit door de Raad van het GO! bevestigd.

1.2. Meerjarenplan 2014-2017

Er werd een strategisch meerjarenplan 2014-2017 opgesteld. De grote krachtlijnen daarin zijn de ISO 27001 certificatie voor de centrale (ICT-) dienst(en) en de uitrol naar de scholen(groepen). Dit plan werd op 26 februari goedgekeurd door de directieraad en op 24 maart door de Raad van het GO!.

1.3. Beleidsverklaring

De “Beleidsverklaring informatieveiligheid GO!” werd aangepast vermits het vorige document drie jaar oud was. Het werd enerzijds aangepast aan de nieuwe ISO 27002 norm (2013) en anderzijds aan de situatie waarin het GO! zich bevond. Enkele praktische aanpassingen waren dringend nodig.
Deze beleidsverklaring werd op 19 september goedgekeurd door de Raad van het GO!.

1.4. Aanbeveling

In het kader van de ISO-certificatie van de ICT-dienst van GO! centraal moet een bijlage bij de beleidsverklaring opgesteld worden.

2. Organisatie

2.1. Interne organisatie

2.1.1. Centrale adviescommissie ICT/COM

De informatieveiligheidsconsulent wordt nu steeds uitgenodigd voor deze commissie. Zij is vorig jaar 5 maal samengekomen. Zij besprak het meerjarenplan en bereidde acties voor ten aanzien van de scholengroepen.

2.1.2. Lerende netwerken

Om de communicatie tussen GO! centraal en de scholen(groepen) te bevorderen worden de acties ook toegelicht in de lerende netwerken. De stand van zaken en de toekomstige acties werden toegelicht tijdens de 2de ronde in oktober en november in de vijf provincies.

2.1.3. Aanspreekpunten

In 2012 werden aanspreekpersonen aangesteld in de CLB's, de CVO's en de scholengroepen. In januari en februari werden vergaderingen georganiseerd om het project "Veilige wachtwoorden" te evalueren. Dit gebeurde in drie (gemengde) groepen.

2.1.4. Wekelijks overleg

Om de ISO-certificatie voor te bereiden is er een wekelijks overleg met de ICT-manager. De IVC wordt ook uitgenodigd op de vergaderingen van de projectleiders ICT.

2.1.5. Werkgroep ICT-integratie in Onderwijs (BRICT)

De gemengde werkgroep waar technisch en pedagogisch verantwoordelijken (ICT, IVC, NAS, PBD, Smartschool) deel van uitmaken, werkte verder aan de projecten.
Een van de projecten is het uitwerken van een driedimensionaal ICT-beleidsplan (op de drie beleidsniveaus). Dit werd opgesteld in samenwerking met de ICT-coördinatoren van de scholengroepen.

2.2. Relaties met de Vlaamse Toezichtcommissie (VTC) en de Commissie voor bescherming van de private levenssfeer (CBPL)

2.2.1. Aanvragen

In 2014 werden geen nieuwe machtigingen aangevraagd voor nieuwe gegevensoverdrachten.
De machtiging in verband met de gegevensoverdracht tussen het GO! en Jongerenwelzijn werd praktisch uitgevoerd. Dit was een eenmalige actie.

2.2.2. Besprekingen

Op 21 maart was er een overleg tussen de VTC en de CBPL enerzijds en de koepels en netten anderzijds om de stand van zaken te bespreken. De machtigingen voor gegevensuitwisseling gelden voorlopig tot 31 juli 2014. Als reactie op deze vergadering werd door AgODi een nota voorbereid om de minister te informeren over de situatie.

Op 2 oktober was er op vraag van de VTC een nieuw overleg om te peilen naar de stand van zaken binnen de diverse koepels/netten en binnen het departement Onderwijs. De verlenging van de machtigingen stond op het spel.
Het GO! en het POV zijn de enigen die de voorwaarden van de VTC gerespecteerd hebben. De VTC begrijpt dat men de machtigingen niet zomaar kan stoppen, maar zal er bij de minister op aandringen om orde op zaken te brengen.

Het GO! liet in een brief aan AgODi zijn standpunt weten: mocht de VTC beslissen om de machtigingen in te trekken, dan moet ze dat doen ten aanzien van die instanties die niet in orde zijn met de voorwaarden.

2.3. Samenwerking met andere organisaties

2.3.1. Agentschap voor Onderwijsdiensten (AgODi)

In januari vond een vergadering plaats met de informatieveiligheidsconsulenten van de diverse netten om te spreken over het veiligheidsbeleid van de CLB's, in het kader van de toegangspoort Jeugdhulp. De CLB's voldoen reeds aan de voorwaarden en moeten geen extra actie ondernemen.

Er waren ook vergaderingen tussen AgODi en de diverse netten en koepels om de besprekingen met de VTC voor te bereiden (zie 2.2.2)

2.3.2. AHOVOS

In verband met de CVO's was er een vergadering met AHOVOS om de situatie van onze CVO's binnen het veiligheidsbeleid van het GO! te kaderen.

2.3.3. POV

Het Provinciaal Onderwijs heeft ons informatieveiligheidsbeleid als voorbeeld genomen om hun beleid te ontwikkelen. Hierover was er een overlegmoment in mei en oktober.

2.3.4. Edubit

Edubit vzw (ICT op school) nam in december contact op voor eventuele samenwerking. Dit wordt in de loop van 2015 verder onderzocht.

2.4. Aanbevelingen

De uitrol naar de scholen(groepen) moet in 2015 voortgezet worden, vermits de overheid er almaar meer op hamert om werk te maken van informatieveiligheid.
Terzelfdertijd moeten we ervoor waken dat wij niet de dupe worden van het feit dat anderen niet voldoen aan de voorwaarden die de overheid oplegt.

3. Personeel - Vorming

3.1. Centrale diensten

3.1.1. Gedragscode

In samenwerking met de personeelsdienst werd een gedragscode opgesteld, in het kader van het Nieuwe werken. De algemene principes zullen in de deontologische code geïntegreerd worden. De nieuwe ICT-gedragscode van de Vlaamse overheid zal geïntegreerd worden in onze gedragscode.

3.1.2. Werkgroep integriteit

Samen met andere diensten werd een analyse gemaakt van de kwetsbare functies binnen de centrale diensten van het GO!.

3.1.3. Nieuwe personeelsleden

Op 21 juni werd aan de nieuwe personeelsleden de basisopleiding “informatieveiligheid” gegeven.

3.1.4. Gebruik van telefonie en multimedia

In het kader van de nieuwe huisvesting werden demonstraties gegeven over het gebruik van Lync als nieuw communicatiesysteem.

3.2. Scholengroepen

3.2.1. Vorming voor directeurs en kaders

- Er werd één dag nascholing georganiseerd rond “informatieveiligheid - management” voor Scholengroep Oostende (11/12);
- Vorming Informatieveiligheid, een halve dag bestemd voor alle personeelsleden op 2/12.

3.2.2. Onthaalbrochure

In de nieuwe versie van de startersgids voor leerkrachten is er ook aandacht besteed aan de informatieveiligheid en de privacy.

3.2.3. Vorming op aanvraag

- Aan de ICT-coördinatoren van Scholengroep Mandel en Leie werd een presentatie gegeven over ISO27000.
- Voorstelling van Informatieveiligheid aan Scholengroep Kempen
- Nascholing GO! atheneum Deinze: mediawijsheid
- Scholengroep Mechelen: tablets op school en mediawijsheid

3.3. Mediawijsheid

In samenwerking met GO! nascholing werd vorming gegeven rond mediawijsheid:

- Nascholing op maat GO! basisschool Lint (5/2)
- Scholengroep Maasland (7/2)
- Scholengroep Midden-Brabant (12/2)
- Scholengroep Agora (19/03)
- Van Wijs naar Mediawijs (2de dag, vervolg van november 2013)

3.4. Centra voor leerlingenbegeleiding

In maart werd aan nieuwe CLB-medewerkers een vormingssessie gegeven.

3.5. Eigen vorming - bijscholing

De volgende vormingen werden bijgewoond:

- 13 februari: Ethical Hacking
- 27 februari: Security Congres (Gent)
- 10 maart: Onderwijs in 2030 (dep. Ond.)
- 14 maart: mogelijkheden van de digitale handtekening
- 27 maart: bezoek beurs InfoSec
- 02 april: Cybersecurity in het basisonderwijs
- 9 september: Informatieveiligheid, privacy en het gebruik van sociale media
- 15 september: gebruik van de BiZagi Software
- 18 oktober: 15j KlasCement
- 24 oktober: Security Congress Belnet
- van 9 tot 13 december: Visit - Bordeaux (zie 12.2)
- 20 december: Ethical Hacking basis

3.6. Aanbevelingen

Vorming directeurs

Gezien de technische en juridische evolutie binnen de informatiebeveiliging is het aangewezen om dit aspect verplicht op te nemen in de opleidingsmodules voor directeurs en andere kaderleden.

4. Beheer van bedrijfsmiddelen

4.1. Procesbeheer

Processen werden verder geanalyseerd en worden omgezet in een workflow zoals de behandeling van vragen en klachten, de briefwisseling en de facturatie. Jammer genoeg worden ze niet altijd gebruikt (zoals de vragen en klachten). In verband met de briefwisseling worden inbreuken vastgesteld op de vertrouwelijkheid van de informatie (inscannen van persoonlijke briefwisseling, doorsturen naar verkeerde personen, e.d.).

4.2. Archiefbeheer

In het kader van de nieuwe huisvesting werden in samenwerking met de archivaris procedures opgesteld voor het bewaren en vernietigen van papieren documenten.

4.3. GO-SQL databank

Er zijn nog steeds toepassingen die gebruikmaken van de oude Microsoft-SQL databank. Dit vormt nog steeds het grootste risico op datalekken in onze organisatie. De externe audit van 2014 heeft dit nogmaals bevestigd (zie 11.5). Jammer genoeg kunnen we deze databank niet afsluiten zolang er nog toepassingen zijn die deze gegevens gebruiken.
Deze toepassingen worden systematisch vervangen en maken dan gebruik van de nieuwe databank, die goed beveiligd is.

4.4. Kennisknooppunt

Het kennisknooppunt heeft als taak gegevens op te zoeken, te ordenen, te analyseren en te verrijken en ter beschikking te stellen van het onderwijsveld en de centrale diensten. Er wordt zowel gewerkt met gestructureerde als met ongestructureerde gegevens die gevoelige informatie kunnen bevatten. De processen werden in kaart gebracht en er worden procedures uitgewerkt om dit op een veilige manier te beheersen.

4.5. Beheer van fysieke bedrijfsmiddelen

Al onze IT-systemen (terminals, laptops, smartphones) worden geregistreerd in een centraal systeem om het beheer ervan te vergemakkelijken.

4.6. Classificatie van documenten

Alhoewel er een classificatie is afgesproken in de beleidsverklaring en in de metadata van ons documentbeheersysteem, wordt ze in de praktijk niet toegepast.

4.7. Aanbevelingen

- ***Verbeterproject rond het verwerken van de briefwisseling.***
- ***Zo vlug mogelijk de nieuwe databank in dienst nemen.***
- ***Classificatie opnemen in de metadata (workflow) en in de lay-out van documenten.***

5. Toegangsbeveiliging

5.1. Single Sign On-project

5.1.1. Algemeen

Er wordt verder gewerkt aan dit project met een product van Microsoft, namelijk Forefront Identity Manager (FIM). In een eerste fase zal dit gebruikt worden in de centrale diensten, na de rationalisatie van de Active Directory.
Tevens moeten we onderzoeken of we niet op een veiliger manier kunnen inloggen dan alleen met een wachtwoord, in een eerste fase voor de telewerkers als ze buitenshuis werken.

Voor applicaties waar beperkte toegang mogelijk moet zijn, moeten rollen gedefinieerd worden. Het toekennen van deze rollen aan personen moet opgevolgd worden om fouten te vermijden. Dit is een groot probleem.

5.1.2. Elektronisch kandideren tijdelijken (EKT)

Sinds 2014 moeten de kandidaten inloggen via het FedICT-portaal met de elektronische identiteitsaart of het federaal token, zoals opgelegd door de Commissie voor de Bescherming van de Private Levenssfeer.

5.2. Project “Loop niet te koop met jouw wachtwoord”

In september 2013 werd de campagne rond veilige wachtwoorden opgestart. Begin 2014 werd ze door de aanspreekpunten geëvalueerd. De ondersteuning van de communicatiedienst was niet optimaal; de campagne verloor daardoor aan kracht. Daarom werd de actie terug opgestart in maart-april 2014.
Op het einde van 2014 werden we geconfronteerd met een aantal reportages in de media over leerlingen die wachtwoorden van leerkrachten misbruiken (cf. “Hacking op school”).

5.3. Aanbevelingen

5.3.1. Wachtwoorden en alternatieven

Leerkrachten en personeel zijn zich nog te weinig bewust van het belang van een veilig wachtwoord. De campagne moet geregeld herhaald worden om effectief te zijn (cf. de BOB-campagnes).
Smartschool biedt nu al de mogelijkheid om, naast het ingeven van een wachtwoord, een bijkomende beveiliging in te bouwen in de vorm van een code (via de smartphone) of een USB-stick. Dit zou verplicht moeten worden voor alle leerkrachten die gebruikmaken van het leerlingvolgsysteem en/of de toets- en puntenmodule (“Score”).
Dezelfde soort beveiliging moet gevraagd worden aan alle producenten van schoolsoftware die persoonsgegevens verwerken, zoals de administratieve schoolpakketten en vooral ook de CLB-toepassing LARS.
Voor de centrale diensten moet er een strenger beleid rond wachtwoorden komen. Er wordt te veel gebruikgemaakt van gemakkelijke wachtwoorden. Voor telewerkers is dubbele authenticatie aangewezen.

5.3.2. Single Sign on

Door FIM te koppelen aan het toegangsbeheer van Smartschool, kunnen we de rollen beheersbaar maken.

6. Cryptografie

De nieuwe kritische toepassingen maken gebruik van beveiligde internetverbinding (https). Dit is van groot belang voor de telewerkers van de centrale diensten.

7. Fysieke beveiliging

7.1. Nieuwe huisvesting

In het kader van de nieuwe huisvesting werd ook gedacht aan de informatieveiligheid op het vlak van toegangscontrole en indeling van de ruimtes.

Het gebouw werd ingedeeld in diverse zones: publieke (gelijkvloerse verdieping), semipublieke (leslokalen en vergaderzalen) en bureauruimtes waar in principe enkel personeel komt. Er werd een controlesysteem met badges geïnstalleerd, maar dat wordt tot nu toe niet gebruikt. Dit heeft als gevolg dat bezoekers gemakkelijk de controle aan het onthaal kunnen omzeilen (zeker bij grote toevloed) en bijna overal binnen kunnen.

7.2. Beveiliging serverpark

Onze servers staan niet meer in het Huis van het GO! maar worden gehost in een beveiligde omgeving die aan alle moderne eisen voldoet.
Deze site is ontdubbeld zodanig dat onderbrekingen tot een minimum beperkt worden.
De fysieke toegang tot de site wordt constant gemonitord. Wie toegang wil krijgen moet goedgekeurd worden door de IVC en de in- en uitgangen worden geregistreerd en automatisch doorgemaild naar de IVC.

7.3. Aanbevelingen

7.3.1. Toegangscontrole

Het management moet overwegen om de toegangscontrole te activeren, na een evaluatie van de risico's.

8. Operationele processen

8.1. ISO 27001 certificatie

8.1.1. Centrale diensten

In het meerjarenplan 2014 -2017 staat dat men gaat voor certificatie van de centrale ICT-dienst, conform de ISO 27001 norm (informatieveiligheid). Dit werd in juli door de directieraad bevestigd. Er werd een offerte voor consultancy uitgeschreven. De opdracht werd gegund en het project is in november opgestart.

8.1.2. Scholengroepen

Via de lerende netwerken werden de scholengroepen geïnformeerd over de acties die de overheid vraagt (zie 2.1 en 2.2). Om de beginsituatie te bepalen, wordt in de loop van 2015 een risicoanalyse uitgevoerd, gebaseerd op de ISO-normen.

Het CVO van Antwerpen heeft zijn ISO27001 certificaat gehaald.

8.2. Netwerkbeveiliging

8.2.1. 'Virtual desktop interface' (VDI)

Het in gebruik nemen van het Huis van het GO! ging ook gepaard met de installatie van een vernieuwd serverpark en een andere aanpak. Er wordt nu gewerkt met VDI. Dit wil zeggen dat men via de browser verbinding maakt met de server waarop alle programma's geïnstalleerd staan. Dit maakt de beveiliging veel efficiënter, vermits alle software op één centrale plaats staat.

8.2.2. Draadloos netwerk

In onze nieuwe huisvesting zijn er twee gescheiden draadloze netwerken, één voor bezoekers en een intern netwerk. Dit maakt dat ons intern netwerk extra beveiligd is.

8.2.3. Mobile Device Management

Vorig jaar werd een marktonderzoek gedaan om de mobiele toestellen (laptops, tablets en smartphones) te beveiligen. Een kleine groep gebruikers heeft dit uitgetest. De offertes werden uitgeschreven en worden begin 2015 gegund.
Alle nieuwe toestellen zullen daarmee uitgerust worden.

8.3. Nieuwe huisvesting - anders werken

Bij de inrichting van het gebouw en de nieuwe ICT-infrastructuur werd met de informatieveiligheid rekening gehouden. Bij de organisatie van het werk in het Huis van het GO! werd ook rekening gehouden met veiligheidsaspecten in de werkprocessen, bv. met het "clean desk"- principe.
Er werden richtlijnen voor het telewerken opgesteld.

8.4. Dienstencatalogus

In het kader van de reorganisatie van de centrale diensten werden de kerntaken van de ICT-dienst onderzocht en werd een dienstencatalogus opgesteld.

8.5. Kennisknooppunt

Introductie van begrippen over informatieveiligheid bij de bespreking van de kernprocessen in het kennisknooppunt

8.6. Sociale media en mediawijsheid

8.6.1. Nascholing

Samen met GO! nascholing werden verschillende navormingen voorbereid en georganiseerd (zie 3.3).

8.6.2. Samenwerking

Er werd deelgenomen aan de bespreking over het ontwikkelen van een educatieve portaalsite waar men informatie over onderwijs kan uitwisselen (KlasCement, VIAA,uitgevers …) Dit was een initiatief van het departement Onderwijs.
Op initiatief van "Iminds" werd ons advies gevraagd over het inzetten van sociale media in de ouderwerking van scholen, in samenwerking met GO! ouders.

8.6.3. School on the cloud

Adviseren en meedenken rond dit Europees project over het inzetten van digitale middelen in het onderwijs.

8.7. Aanbevelingen

8.7.1. ISO

In het kader van de ISO-certificatie, moeten de operationele processen verder geanalyseerd en vooral gedocumenteerd worden.

8.7.2. Mobile Device Management

Personeelsleden die gebruik wensen te maken van hun eigen toestellen voor professionele doelen ("Bring your own device") moeten ook over Mobile Device Management beschikken.

Mogelijke uitrol naar scholengroepen die hier belangstelling voor hebben.

9. Ontwikkeling en onderhoud / Evaluatie leveranciers

9.1. Digitaal schoolreglement

Advies over de beveiliging en ontwikkeling van het platform voor het opstellen van schoolreglementen.

9.2. Wekelijks teamoverleg

Om het ontwikkelen en bijsturen van ICT- projecten beter te laten verlopen is er nu wekelijks overleg met alle projectleiders.

9.3. Evaluatie leveranciers

Dit is een nieuwe vereiste sinds de invoering van de nieuwe ISO-norm (2013).

10. Veiligheidsincidenten

10.1. Registratie

Op dit ogenblik worden incidenten nog niet systematisch geregistreerd. Sommige worden geregistreerd door de helpdesk, andere komen rechtstreeks bij de IVC. Nu de helpdesk gebruikmaakt van een aangekochte toepassing “Topdesk”, werd uitgetest of we die toepassing ook kunnen gebruiken om veiligheidsincidenten te melden. Dit werd positief geëvalueerd en zal vanaf 2015 gebruikt worden (ook in het kader van de ISO-certificatie).

10.2. Bekende veiligheidsincidenten

- een leerlingbegeleider die zijn gesprekken met leerlingen opneemt
- een sniffer in een school plaatsen
- een van onze mailservers werd “geblacklisted” wegens het verspreiden van spam
- stroomonderbreking centrale diensten
- “defacement” van een schoolwebsite
- gehackte schoolwebsites (2)
- frauduleus gebruik van de loginpagina van een schoolwebsite
- configuratie van laptop gewijzigd zonder toestemming
- een van onze servers aangetast door de heartbleed- bug
- wachtwoorden op een onveilige manier doorgeven
- een e-mailaccount van de Europese Commissie misbruiken om virussen rond te sturen
- verdachte bug in applicatie over de reaffectaties; bleek een bug te zijn en geen poging tot hacken
- zonder toestemming ouders foto’s publiceren op schoolwebsite (2)
- zonder toestemming foto’s/film publiceren op Facebookpagina van een ouder (3)
- phishingmails (4)
- virusinfectie op de P-schijf
- frauduleuze vraag van een firma om gegevens van scholen in een databank te plaatsen (tegen betaling)

Er zijn ongetwijfeld nog veel incidenten gebeurd en allicht gemeld aan de helpdesk, maar die worden niet doorgegeven.

10.3. Adviezen

- Gebruik van Office 365 en Skydrive door CLB’s
- Gebruik van e-mailadressen binnen Smartschool virtuele ruimtes
- Deontologische code voor een school
- Hosting van schoolwebsites
- Gebruik van telefonie
- Omgaan met vertrouwelijke gegevens
- Hoe omgaan met een haatmail rond verbod levensbeschouwelijke kentekens
- Gebruik van beeldmateriaal op school
- Advies na klacht over het verplichte gebruik van de Eid voor kandidering tijdelijken
- Wachtwoordgebruik (3)
- E-mailadressen doorgeven bij vervanging
- Gebruik van het rijksregisternummer in een CVO
- Advies aan Telefacts over hacking op school en identiteitsdiefstal op Facebook
- Gebruik van foto’s in FMIS
- Gebruik van betalende software door leerlingen

- Advies gebruik van wachtwoorden
- Advies of een mail van het departement Onderwijs wel origineel was en geen phishing
- Advies over het gebruik van Google Earth in promotiefilmpje van een school
- Vraag naar policies over ICT-gebruik
- Advies over het gebruik van Smartschoolplatform voor vakbondsmededelingen
- Advies en uitleg over verschil in aanpak tussen Nederland en Vlaanderen in verband met het doorgeven van leerlingengegevens aan privébedrijven
- Vraag om vorming te geven in een school
- Gebruik van LARS om personeelsgegevens te registreren
- Beveiliging van laptops door MDM

10.4. **Aanbeveling**

Gebruik maken van het meldpunt om incidenten te registreren en op te volgen.

11. Continuïteitsbeheer

11.1. Huidige situatie

Vorig jaar werd begonnen met het opstellen van een Business Continuity Management plan. Ditmaal niet alleen technisch maar ook op het vlak van processen en management.

11.2. Aanbeveling

Dit BCM integreren in het ISO-traject.

12. Naleving en controle

12.1. Wettelijke en contractuele verplichtingen

In het kader van de ISO-certificatie werd een document opgesteld waarin alle wettelijke en contractuele verplichtingen zijn opgenomen. Contractuele verplichtingen worden ook geregistreerd in onze helpdesktoepassing.

12.2. Audits

In augustus werd een externe audit uitgevoerd om onze nieuwe infrastructuur te testen, zowel extern (publieke websites) als intern (VDI).
Bij deze audit was er ook een “social engineering” opdracht om via een phishingmail te proberen toegang te hebben tot onze systemen. Dit werd eerst besproken met de vakbonden.
Deze externe audit had als resultaat:

- 7 kritische zwakke punten
- 3 hoge risico’s

Een van de kritische punten is het gebruik van zwakke wachtwoorden, de andere zijn van technische aard en vertrouwelijke informatie.

13. Varia

13.1. Open data

Binnen de Vlaamse overheid streeft men ernaar om zoveel mogelijk data ter beschikking te stellen voor openbaar gebruik. Ontwikkelaars kunnen die data gebruiken om applicaties te maken ten dienste van het publiek. De IVC volgt deze werkgroep in naam van het GO!.

13.2. Trovi

We werden gecontacteerd door een firma die programmeerbare bandjes ontwikkelde om informatie door te geven via een smartphone, wanneer kinderen tijdens een activiteit verloren lopen. De beslissing om het systeem al dan niet te gebruiken ligt op het niveau van de school of de scholengroep.