ICT Beveiligingsplan 2020

Versie 2.1

Versiebeheer

Versie	Datum	Omschrijving	Auteur
0.1	16-09-2019	Beschrijving IST situatie	HV
0.2	18-11-2019	Beschrijving Maatregelen	HV
0.3	03-12-2019	Kosten indicaties	HV-Diverse leveranciers
0.4	05-12-2019	Besproken Afdelingshoofd	HV-MW
0.5	10-12-2019	Integratie BIO	PD
1.0	11-12-2019	Versie voor overleg Fin	HV
2.0	13-12-2019	Aanpassingen	GdJ HV
2.1	10-02-2020	Verschuivingen budget	GdJ

Inhoud

Inleiding

Digitaal werken is binnen onze organisatie steeds belangrijker. Data moet ten alle tijde en overal beschikbaar zijn. De organisatie kan geen enkel moment meer zonder geautomatiseerde systemen. Echter, digitaal werken heeft ook een keerzijde. De gemeente heeft veel gevoelige (lees: zeer interessante) data. Namen, adressen, bsn nummers, vertrouwelijke adviezen zijn stuk voor stuk voor verschillende groepen, om verschillende redenen, zeer interessant.

Deze informatie dient dus zeer goed beveiligd te worden. Om de beveiliging goed op orde te hebben, is alleen een wachtwoord al lang niet meer voldoende. Ook op systeemniveau zijn maatregelen noodzakelijk.

Bewustwording bij de gebruikers is een essentieel onderdeel. Na een aantal jaarlijkse verplichte penetratie testen is gebleken dat de gebruiker de zwakste schakel is. De meeste risico's ligt dus bij de eindgebruiker. Denk hierbij aan Mail Phishing, maar ook het verlies van datadragers, het gebruik van zwakke wachtwoorden etc….

Om de data zo optimaal mogelijk te beveiligen zijn er een aantal maatregelen absoluut noodzakelijk. Niet voor niets wordt momenteel geadviseerd om minimaal 10% van het complete IT-budget te reserveren voor data beveiliging. Momenteel worden de reguliere budgetten gebruikt maar die komen onder druk te staan.

Dit plan geeft een overzicht van de huidige situatie, de gewenste situatie en de gevolgen hiervan (zowel financieel als voor de gebruikers). Daarnaast biedt dit plan inzicht in de huidige risico's, en de maatregelen die we hiertegen kunnen treffen.

Natuurlijk is het een illusie dat het 100% veilig is. Het is wel de bedoeling dat we het ongenode gasten zo moeilijk mogelijk maken.

Relatie met BIO

In 2020 wijzigt het normenkader van de BIG (Baseline Informatieveiligheid Gemeenten) naar de BIO (Baseline Informatieveiligheid Overheid). Via een implementatieplan doorloopt de gemeente daarbij allereerst een GAP-analyse. Daarin wordt geïnventariseerd welke (verplichte) maatregelen nog niet ingevuld zijn. Op basis van een risico-analyse worden de maatregelen door de organisatie geprioriteerd. De uitkomsten van deze inventarisatie zullen input leveren voor het Informatiebeveiligingsplan voor de middellange termijn (periode 2020-2022).
De GAP-analyse die in het kader van de BIO al heeft plaatsgevonden in 2019 bij het cluster Automatisering en heeft al een aantal 'quick wins' opgeleverd. De voornaamste maatregelen hiervan zijn in dit ICT Beveiligingsplan 2020 opgenomen.
De structurele maatregelen die de BIO vereist, worden in de loop van 2020 via het Implementatieplan BIO bekend. De uitwerking daarvan volgt in een komend Informatiebeveiligingsplan of zal indien noodzakelijk tussentijds worden ingepast.

Huidige stand van zaken

Werkplek

De werkplekken binnen de Gemeente Montferland zijn in 2019 vervangen. Hiermee zijn de Pc's uitgerust met de laatste software (Windows 10 en Office 2016). De werkplek is altijd up to date qua beveiligings updates. Elke 2e dinsdag van de maand komt Microsoft met de beveiligingsupdates. Deze updates worden altijd zo snel mogelijk (eerst bij een aantal test gebruikers) doorgevoerd. Beleid is dat alle updates altijd geïnstalleerd moeten worden, wat betekent dat de software hierop aangepast moet worden. Dat is altijd een bron van discussie.

Naast de updates zijn er op de werkplek ook andere beveiligingsmaatregelen getroffen. Zo kan een eindgebruiker niet zelfstandig software installeren. Deze maatregel zorgt ervoor dat alle software, welke binnen de organisatie gebruikt wordt, via Automatisering is gecheckt en geïnstalleerd. Daarnaast krijgen we op deze manier geen onbetrouwbare/illegale software binnen.

Een gebruiker heeft op het netwerk alleen de rechten die hij/zij nodig heeft. Dat wil zeggen dat iemand vanuit een standaard werkplek, niet ergens terecht kan komen, waar eventueel schade kan worden veroorzaakt.

Tevens zijn alle werkplekken voorzien van een goede virusscanner (Sophos) die automatisch voorzien wordt van de laatste updates.

Internet

Het internet is natuurlijk een belangrijke informatiebron. Op het internet kun je alles vinden. Echter, ook de schadelijke software is op het internet te vinden.

Om dit te beveiligen hebben we tussen de werkplek en het internet een firewall (3 stuks). Deze firewalls zorgen ervoor dat twijfelachtige sites geblokkeerd worden. Ook sites die gehost worden in bepaalde landen worden geblokkeerd. Op de firewall wordt actief beheer uitgevoerd om zo uitzonderingen toe te voegen. (Wat toegelaten wordt, is beoordeeld)

Naast het internet, hebben we ook een dubbel uitgevoerde Gemnet verbinding. Dit is een beveiligde verbinding waarop een aantal diensten (zoals iBurgerzaken, DigiD, eHerkenning) op draaien. De routering van en naar de Gemnet omgeving wordt geregeld op de Firewall.

Het internet is verder niet voor de eindgebruikers beperkt.

Mail

Naast het internet is mail een potentieel risico. Denk hierbij aan Phishing, RansomWare, SPAM-mailtjes. Om de mail te beveiligen hebben we een aantal maatregelen getroffen die ervoor zorgen dat we zo min mogelijk kwetsbaar zijn.

Het grootste voordeel wat de organisatie heeft, is dat we met GroupWise werken. Omdat deze mail applicatie niet bijzonder populair is, worden er weinig virussen voor geschreven. Nadeel is wel dat GroupWise moeilijk integreert met andere applicaties.

Inkomend

Voordat een mailtje binnenkomt, moet deze eerst door een aantal spam filters heen.

1. Gemnet Spam filter → dit is de eerste check. Het grootste aantal mailtjes welke niet helemaal zuiver zijn, wordt hier tegen gehouden.

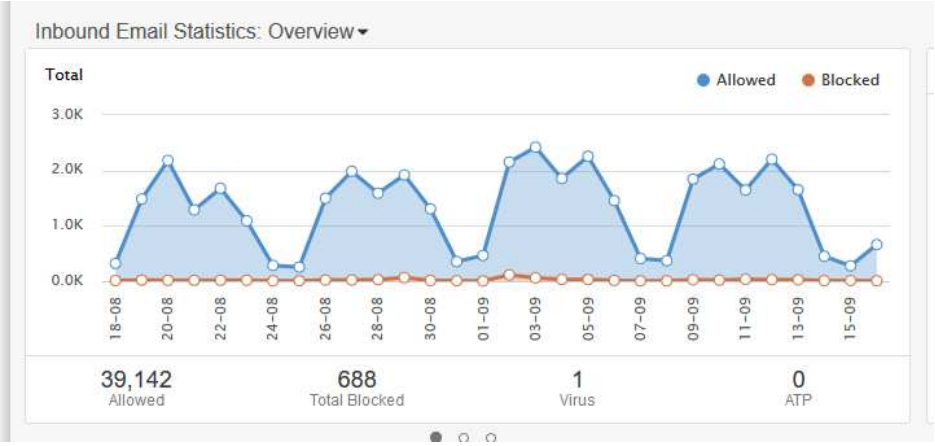
   Overzicht aantal mails van sep 2018 – sep 2019

Maten	Waarde	Berekening
Spam ratio (van alle berichten)	22,90%	Herkende spamberichten / Totaal gefilterde berichten

Maten	Benodigde bandbreedte	Telling van berichten
Geen spamberichten	277,16 GiB	509532
Onduidelijke berichten	1,61 GiB	4431
Spamberichten geblokkeerd	2,51 GiB	157169
Virussen geblokkeerd	43,16 MiB	217
Op witte lijst geplaatst	1,11 GiB	14305
Op zwarte lijst geplaatst	551,57 MiB	603
Totaal aantallen	**282,96 GiB**	**686257**

2. Barracuda Cloud Control → Hier worden allen linkjes en bijlage(n) van een mailtje gecheckt op virus en juistheid.

   Overzicht gescande mail 18-08 – 15-09



3. Barracuda Spam Filter → dit is de laatste check, voordat het mailtje aan de gebruiker afgeleverd wordt.

   Overzicht totaal gescande mail (2,5 jaar)

Email Statistics [inbound] Help

	TOTAL	DAY	HOUR
Blocked	46,070	17	0
Blocked: Virus	7	0	0
Rate Controlled	8,465	0	0
Quarantined	0	0	0
Allowed: Tagged	398	0	0
Allowed	1,453,019	654	9
Total Received	1,507,959	671	9

Uitgaand

Voor de uitgaande mail hebben we de optie om gevoelige mails te versturen. Dat is Secure Mail van KPN. Hiermee wordt de mail niet rechtstreeks naar de ontvanger gestuurd, maar naar een portal binnen KPN. De ontvanger moet zich hier dan aanmelden om de mail te kunnen lezen en/of te reageren.

Netwerk

Het netwerk in de gemeente is onderverdeeld in segmenten (VLANS). Ook de 2 dislocaties (Gemeentewerf en Gouden Handen, gekoppeld middels een dark fiber glasvezelverbinding) hebben een eigen stukje netwerk. Dat maakt het voor indringers erg lastig.

Het bedrade netwerk zit achter de fysieke toegangscontrole. Dus niet te gebruiken voor mensen die geen toegang hebben tot het pand. Bij de maatregelen zult u een advies hierover aantreffen.

Het WLAN (Wifi) is verdeeld in 2 versies. De geautoriseerde/beheerde apparaten krijgen toegang tot het medewerkers netwerk. Ongeautoriseerde apparaten mogen alleengebruik maken van het WLAN Gasten netwerk (kaal internet).

Mobiele devices

Ook op de mobiele devices kan data van de gemeente staan. Dat is de reden dat ook deze devices beveiligd worden. De gemeente maakt geen gebruik van bring Your Own Device (BYOD). Dat maakt de beveiliging een stukje makkelijker. Op elke iPhone/iPad zit het profiel van de gemeente. Dit zorgt voor de beveiliging, het verplichte wachtwoord, op afstand kunnen leegmaken van het device, na 5 foutieve pogingen het device leegmaken. De oplossing hiervoor is Mobile Device Management.

De laptops, die op de afdelingen liggen tbv het flexwerken, zijn alleen maar binnen het gemeentehuis te gebruiken. Deze zijn niet geschikt om thuis mee te werken.

Voor presentaties buitenshuis worden speciale standalone laptops gebruikt worden. Hier staat geen data op…

Daarnaast wordt er door de afdeling OW gebruik gemaakt van Dura Books. Hier worden situaties gelijk ingetekend en gebruik gemaakt van het intern beschikbare kaartmateriaal. Men werkt dus ook buiten direct met de data van binnen, wat als voordeel heeft dat de data maar 1 keer gemuteerd hoeft te worden.

De afdeling Zorg gebruikt voor de huisbezoeken Ultrabooks. Deze zijn uitgerust met een thuiswerk optie en een Sim kaartje. Dat betekent dat er tijdens een keukentafel gesprek gelijk de afspraken vastgelegd kunnen worden. Deze kunnen dan worden voorzien met een handtekening, zodat ook hier een optimaal resultaat behaald wordt.

Authenticatie

Authenticatie blijft een aandachtspunt. Het traditionele naam en wachtwoord is niet veilig gebleken. Diverse pen tests hebben dit uitgewezen. Een simpel wachtwoord (is minder dan 14 posities) is eenvoudig te kraken. Intern hebben we natuurlijk altijd de fysieke toegangsbeveiliging… Maar dat alleen is niet voldoende. Onder de maatregelen zullen we een goed alternatief beschrijven.

De diensten die vanaf buiten te benaderen zijn (webmail, CorsaNxT, Filr) zijn beter beveiligd. We zijn bezig om deze diensten achter een VPN (beveiligd netwerk, met 2weg authenticatie) te plaatsen.

Thuis werken

Voor een groot aantal gebruikers is het mogelijk om thuis te kunnen werken. Deze omgeving is natuurlijk extra beveiligd, maar vormt altijd een risico. Het aanmelden gebeurt middels een 2 weg authenticatie (naam, wachtwoord en token). Na aanmelding krijgt men ook alleen de beschikking over de applicaties waar zij voor geautoriseerd zijn. Het risico betreft dat er geen controle is wie er eventueel mee kan kijken. Dat is en blijft de verantwoordelijkheid van de medewerker.

GGI Veilig

GGI veilig is een initiatief van de VNG om gemeentes te ontzorgen in verband met de beveiligingsvraagstukken. GGI Veilig bevat een drietal percelen, waarbinnen de gemeente een richting gegeven wordt naar bepaalde beveiligingsoplossingen.

Perceel 1

SIEM/SOC: Het monitoren en grip op het netwerk is essentieel. Dit perceel voorziet daarin. Er wordt een platform geleverd, waarop ook de meldingen en bedreigingen die in den lande bekend zijn.

Perceel 2

Aanvullende security product/dienstverlening. In dit perceel zitten een aantal diensten en producten die direct met beveiligingsmaatregelen te maken heeft. Te denken valt aan de aanschaf van een nieuwe Firewall of een Spam filter voor de mail. Indien de gemeente voornemens is om iets van deze producten te vervangen/aan te schaffen, zullen we dit uit de shortlist van de leveranciers van dit perceel moeten doen.

Perceel 3

Security Expertise Services. In dit perceel zit de aanvullende dienstverlening. Onder ander de beveiligingsaudits, jaarlijkse Pentest en overige inhuur is hier geregeld. Ook hier geldt een shortlist van bedrijven, waaruit je verplicht bent om te kiezen.

De belangrijkste reden voor de gemeente om mee te doen met GGI veilig is perceel 1. Dit perceel voorziet in de behoefte om grip te krijgen op het netwerk, en biedt de mogelijkheid om proactief te reageren op beveiligings-risico's.

Maatregelen

Om de data beveiliging op een hoger niveau te tillen, zijn er een aantal maatregelen nodig. De maatregelen zullen zowel financieel als functioneel gevolgen hebben. Een aantal noodzakelijke zaken, zullen op korte termijn uitgevoerd moeten worden.

Authenticatie

De traditionele beveiliging zoals daar zijn het standaard naam en wachtwoord is eigenlijk niet meer voldoende. Het wachtwoord is in de huidige vorm niet echt veilig te noemen.

Een eerste stap is het extra beveiligen van de diensten van de gemeente die buiten beschikbaar zijn.

Thuiswerken: is middels een token (dus 2 weg authenticatie) beschikbaar. Deze dienst voldoet technisch aan de huidige beveiligingseisen. Qua bewustwording en gebruik zijn er nog stappen te maken.

Webmail/GroupWise Webaccess: Deze diensten zijn via onder meer via de iPad/iPhone beschikbaar. Ze zijn te benaderen via standaard naam en wachtwoord. Dit is per definitie niet veilig.

MicroFocus Filr: Met de komst van iBabs wordt deze app minder gebruikt, maar het blijft een risico dat je met alleen naam en wachtwoord overal bij je bestanden kunt. Ook hier zal een vorm van 2 weg authenticatie moeten plaats gaan vinden.

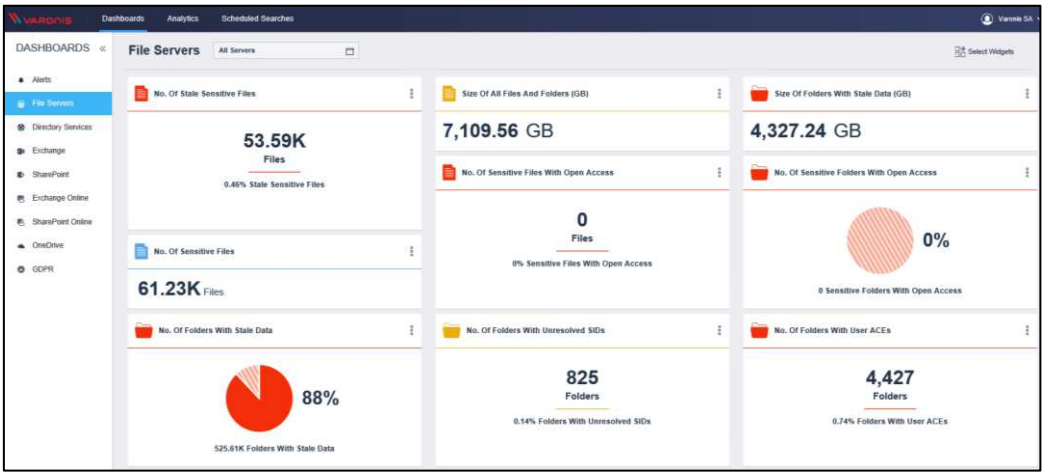
CorsaNxT: deze dienst is inmiddels in een VPN beschikbaar, en dus veilig.

Daarnaast wordt er door de informatie beveiligingsdienst (IBD) geadviseerd om 2 weg authenticatie ook binnen de organisatie toe te passen. We hebben een POC (Proof Of Concept) gedraaid om de 2 weg authenticatie via de iPhone en de huidige token te regelen. Dit krijgt in 2020 verder vervolg.

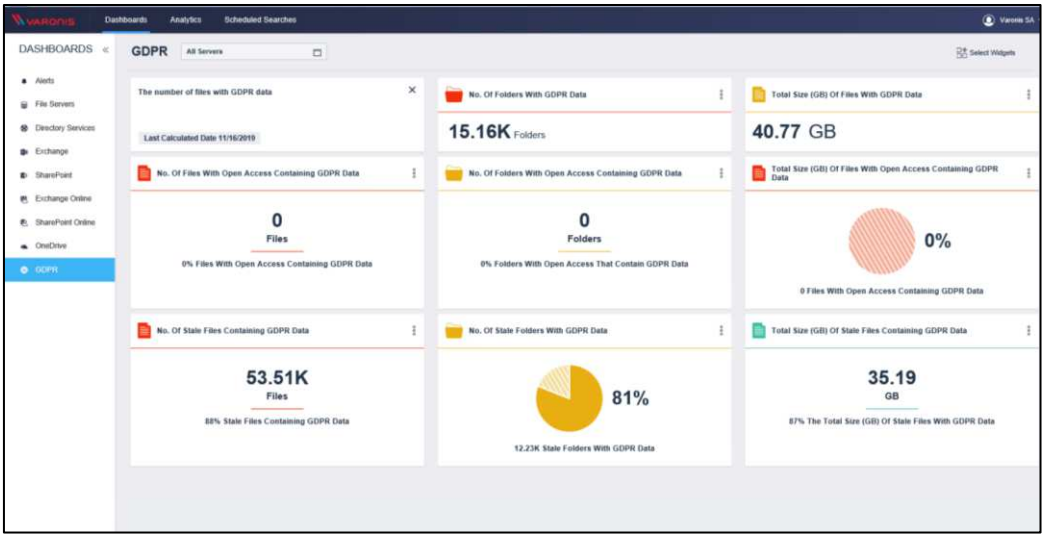
Netwerkschijven

De data op de netwerkschijf is vaak ongestructureerd. De hoeveelheid data in de Home directory's en de data in de afdelingsmappen is enorm. Het opschonen van deze data heeft eigenlijk nooit prioriteit. Maar feit blijft: Hoe minder data, hoe minder risico. Daarnaast kan er op deze locaties privacygevoelige informatie staan, waarvan niemand weet dat deze er staan. Er bestaat software die de data op de netwerkschijven scant, en precies kan filteren op privacy, rechten en gebruik. Daarnaast kan deze software gedraganalyses doen, en zo vreemd gedrag (bijv. versleutelen van bestanden) vroegtijdig signaleren.

Om hoeveel data gaat het?



Hoeveel privacygevoelige data staat op het netwerk?



Monitor

Grip op het netwerk. Dat is essentieel. Natuurlijk hebben we een groot aantal beveiligingsmaatregelen getroffen, maar het is heel lastig om een compleet beeld te krijgen. Vooral omdat de maatregelen allen afzonderlijk goed hun werk doen, maar je mist het complete overzicht

Controles

Controleren van de activiteiten op het netwerk. Welke accounts worden niet gebruikt, welke datastromen zijn ongebruikelijk. Maar ook de controles op de firewallregels zullen periodiek moeten plaatsvinden.

Updates

Het up to date houden van alle software is essentieel. Kwaadwillenden maken vaak gebruik van bestaande kwetsbaarheden binnen softwarepakketten. De softwareontwikkelaars hebben hiervoor meestal al een fix voor gemaakt. Het is dus zaak om zo snel mogelijk deze fix/patch te installeren. Aandachtspunt hierbij is wel dat deze updates altijd buiten werktijd geplaatst moeten worden, wat dus extra resources vraagt.

Fysiek Netwerk

Het hardenen van het netwerk is ook belangrijk. De Wifi is beveiligd met een sterk wachtwoord. Echter, als iemand een eigen laptop aansluit op de bekabeling, dan mag men gewoon internetten. Dat zou, in een uitzonderlijk geval, kunnen betekenen dat men op het netwerk kan. De maatregelen die we hier kunnen treffen, is dat alleen door de gemeente geautoriseerde apparaten, toegang krijgen tot het netwerk.

Opschonen en centrale opslag

Zoals al eerder gemeld is het belangrijk om structuur in de data aan te brengen. Minder data betekent minder risico. Ook zijn er dan minder back-up faciliteiten nodig. Het opschonen van de data is echt een gebruikers actie. Dit moet een onderdeel worden van de bewustwording.
Daarnaast zal veel belangrijke informatie, welke nu nog verspreid staat in de diverse home directories, centraal moeten worden opgeslagen in het DMS. Dit is vaak archiefwaardig materiaal. Daarmee is ook gelijk de wettelijke vernietiging geregeld.

Reguliere testing

Jaarlijks dient er een Pentest op het netwerk plaats te vinden. De test wordt uitgevoerd door een Ethical Hacker die de kwetsbaarheden binnen het netwerk, maar ook van de gebruikers, onderzoekt. Uit dit onderzoek komt een lijst met maatregelen, die zeer waardevol is om de omgeving zo veilig mogelijk te maken. Daarnaast wordt dit in de diverse audits ook vereist.

Doorlopende vulnerability check

Een pentest vindt jaarlijks plaats. Dat zijn natuurlijk moment opnames. Kwetsbaarheden ontstaan dagelijks en de impact hiervan is moeilijk te bepalen. Eigenlijk wil je bij het ontstaan van een kwetsbaarheid dit weten en de impact kunnen bepalen. Ook hierbij is het zaak dat je geïnformeerd wordt, bij het bekend worden van de kwetsbaarheid. Daarnaast geeft de software wel een blauwdruk van hoe we qua beveiliging er voor staan.
Een aparte toepassing binnen deze oplossing is het zelf versturen van phishing mails. Zo kunnen we de alertheid van de medewerkers testen en daar ook op acteren.

Uniformiteit

Momenteel hebben we veel individuele (op zichzelf staande) oplossingen in huis. Dat is voor dit moment een logische situatie want de maatregelen zij ook heel divers en komen ook niet op hetzelfde tijdstip. Nu is het heel lastig om dan eenvoudig een compleet beeld te krijgen. Nu blijkt dat er totaaloplossingen zijn, die wel een totaalbeeld kunnen verschaffen. De vraag hierbij is altijd op welk moment kies je voor een totaaloplossing. Dat betekent een desinvestering van de huidige oplossingen.

VPN

De VPN (Virtueel Private Network) is de oplossing voor de oplossingen die thuis beschikbaar zijn. Denk hierbij aan Corsa, Filr en de mail. Een VPN is een beschermd (middels 2weg authenticatie) netwerk van de gemeente. Alle verkeer dat hierover gaat, is veilig. Inmiddels is Corsa alleen nog via

de VPN beschikbaar, maar dit wordt snel uitgebreid. Hiermee is het ook mogelijk om andere diensten beschikbaar te maken. Denk hierbij dan bijvoorbeeld aan de Nedbrowser en Intranet.

Internet

Momenteel vinden er geen extra maatregelen plaats voor wat betreft het gebruik van internet. Met uitzondering van het internet en email protocol. Dus men is zelf verantwoordelijk wat men op internet doet. Een andere optie is om een internet policy te maken, waarbij bepaalde acties/sites al niet beschikbaar zijn. Tot op heden is daar binnen de organisatie niet voor gekozen. Misbruik is ook nog nooit aangetoond.

Bewustwording

Zoals uit de diverse testen is gebleken, blijft de gebruiker de zwakste schakel. Het klikken op een link in een spam mailtje, het bezoeken van een malafide site, het meenemen van bestanden op een stick, het kwijtraken van een telefoon, de pc niet in de schermbeveiliging zetten. Het kan ons allemaal gebeuren, maar het kan hele nare gevolgen hebben. Het is belangrijk dat gebruikers databeveiliging “tussen de oren krijgen”. Dus is er samen met de CiSo een bewustwordingscampagne gestart. Daarnaast willen we aantonen (middels een Mystery guest) hoe het met de beveiliging is gesteld.

Resources

Binnen het cluster Automatisering zijn de resources beperkt. Er loopt een ander traject om een deel van de aanwezige formatie ruimte in te zetten op het vlak van informatie beveiliging. Aangezien dit een zwaardere functie is, moet hier ruimte voor gevonden worden. Dit traject is inmiddels op met ee ander advies gestart

Financiële consequenties en dekking

Onderstaande tabel geeft een opsomming van de maatregelen weer, met daarbij de financiële gevolgen.

Maatregel	Beschrijving oplossing	Kosten incidenteel 2020	Kosten incidenteel 2021	Kosten structureel
GGI Veilig Perceel 1	SIEM SOC (grip op het netwerk) oplossing	10.500		15.000
Authenticatie	2 weg authenticatie middels een token	14.000		1.200
Netwerkschijven	Rechten, gebruik, privacy op de ongestructureerde data			20.000
Uniformiteit	Zorg dat de componenten uitwisselbaar zijn om een compleet beeld te krijgen		83.000(incl. 2f authenticatie)	
Netwerk	Oplossing om alleen geautoriseerde apparaten toe te laten op het netwerk	30.000		
Vulnerability check	Constante (automatische) check op alle kwetsbaarheden. Incl. phishing			7.500
Pentest	Jaarlijks een test op de beveiliging.			10.000
Totaal		54.500	83.000	55.000

Voorgesteld wordt om de incidentele kosten in 2020 (€ 54.500) en in 2021 (€ 83.000) te dekken middels een onttrekking aan de Algemene Reserve.

De structurele kosten ingaande 2021 bedragen € 55.000. Conform de vastgestelde procedure zullen deze aanvullende lasten worden betrokken bij de Kadernota 2021 (nieuw beleid).

Advies

Bovenstaand document geeft aan dat we binnen de Gemeente Montferland al flink bezig zijn met de beveiliging van de IT-omgeving. Binnen de huidige kaders is de beveiliging goed op orde. Alleen zullen er een aantal maatregelen getroffen moeten worden om de beveiliging naar een hoger niveau te tillen. Deze maatregelen zullen niet altijd het werk van de gebruikers vergemakkelijken, maar het is noodzakelijk. In veel gevallen zijn we afhankelijk van het gedrag van de gebruikers, dus bewustwording is essentieel. De genoemde technische maatregelen zijn minimaal nodig om de omgeving zo veilig mogelijk te houden.