M·IT SERVICES

QUICKSCAN
RAPPORTAGE

WWW.MITSERVICES.NL

Contactpersoon:

Quickscan uitgevoerd door: Marcel Martens

Quickscan uitgevoerd op: 1 februari 2024

Bijzonderheden:
Met name geïnteresseerd hoe ze hun klanten kunnen helpen bij Cybersecurity vraagstukken.

Back-up systemen en processen

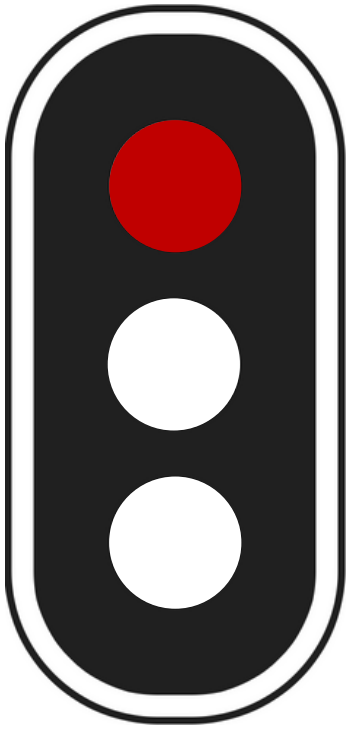
	Gevaar	Risico	In orde
Veiligheid back-up systeem	■		
Retentietijd back-up	■		
Veilig en makkelijk herstelbaar	■		
Data verloren in het verleden		■	
Veiligheid back-up cloud-oplossing	■		

Verbeterpunten

Er is momenteel geen back-up naar een externe provider. Wij adviseren het volgende:

- Advies is om een back-up met retentietijd aan te houden met bijvoorbeeld de volgende bewaarmomenten: 14 dagen, 5 weken, 12 maanden, 7 jaren. Dit zorgt ervoor dat je 38 momenten terug in de tijd kunt.
- Er wordt geen back-up gemaakt van Microsoft 365 (e-mail). Het advies is om hier dagelijks een back-up van te maken.
- Zorg voor een automatische online back-up van al je data, mail en cloudoplossingen.

Risicofactor



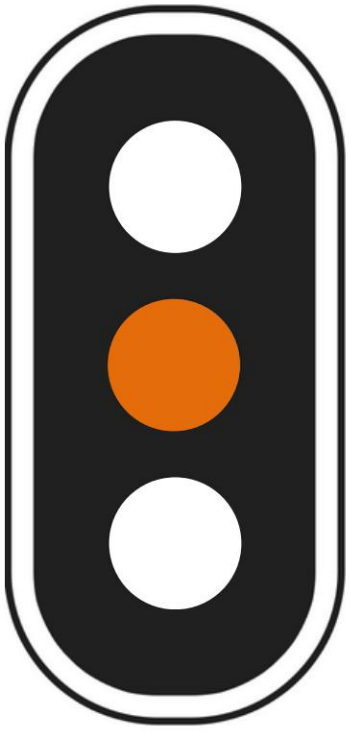
Beveiliging en rechten

	Gevaar	Risico	In orde
Veiligheid accountbeveiliging		■	
Overleefbaarheid onderneming			■
Beleid gebruikersrechten		■	
Netwerkbeveiliging extern		■	
Wachtwoord en toegang beveiliging	■		

Verbeterpunten

- Maak gebruik van een password manager zoals https://www.mindyourpass.io voor het opslaan van wachtwoorden. Zo kan ook niemand bij wachtwoorden van collega's.
- Benader de toegang tot data op basis van "least-security", wat heeft de medewerker minimaal nodig om zijn/haar werkt te kunnen doen. Review deze ook regelmatig zodat men niet bij onnodig veel data kan.
- Zorg voor een plan dat fysiek in de kast ligt over wat te doen bij een cyberincident. Hier kun je een template downloaden: https://www.mitservices.nl/wat-te-doen-bij-een-cyberincident
- Zorg dat er een apart gasten wifi netwerk is waar men niet onderling met elkaar kan communiceren.

Risicofactor



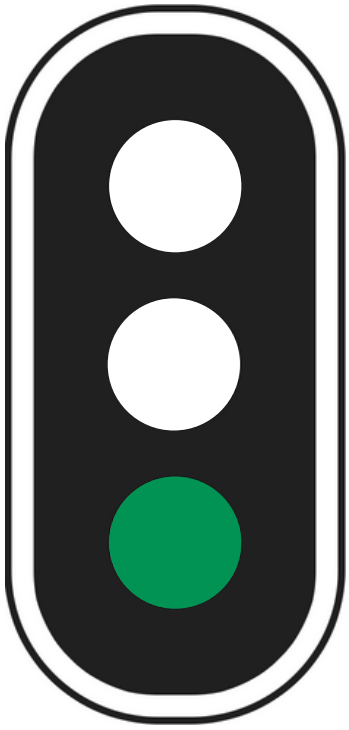
Werkplekbeheer

	Gevaar	Risico	In orde
Inventarisatie hardware eigendom	☐	■	☐
Hardware in beheer van IT	☐	☐	■
Beveiligingspatches up-to-date	☐	☐	■
Hardware werkt zoals gewenst	☐	☐	■
Werklekken voldoen aan ARBO	☐	☐	■

Verbeterpunten

- Zorg voor een overzicht van alle bedrijfsmiddelen en wie wat in gebruik heeft. Dan kun je sneller schakelen in geval van een calamiteit.
- Controleer met regelmaat of alle werkplekken up-to-date zijn.
- Zorg voor duidelijke bruikleenovereenkomsten met daarin opgenomen dat ze voor zakelijke doeleinden gebruikt worden en dat ze op eerste verzoek ingeleverd moeten worden.
- Middels Microsoft Intune kun je ook de bedrijfsgegevens op privé telefoons van medewerkers veilig stellen en indien nodig op afstand verwijderen.

Risicofactor

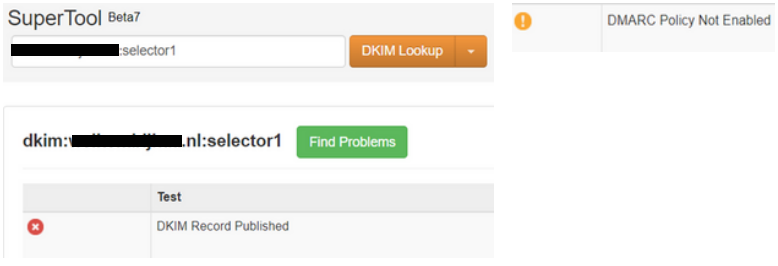


Software en Cloud

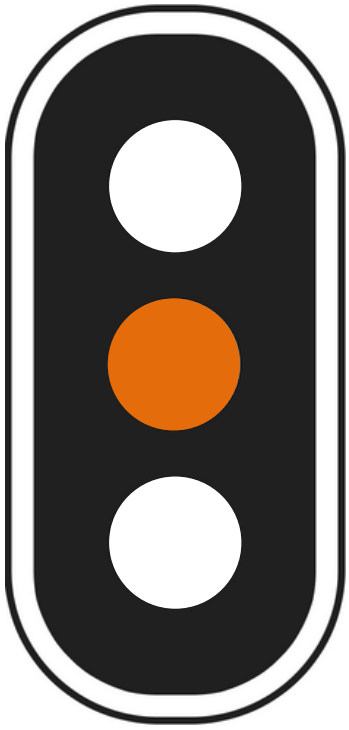
	Gevaar	Risico	In orde
E-mail hosting	☐	■	☐
Veiligheid softwarepakketten	☐	■	☐
Overzicht licenties en software	☐	■	☐
Beheer en overzicht abonnementen	☐	■	☐
Automatische updates software	☐	☐	■

Verbeterpunten

- DMARC policy niet ingesteld.
- DKIM records zijn niet aanwezig.
- Zorg voor tweestpasverificatie bij alle bedrijfsappilicaties. Ook de portals van leveranciers.
- Vraag naar het back-up en recovery protocol van de belangrijkste software leveranciers (Portals).
- Zorg voor een duidelijk overzicht van alle lopende abonnementen zodat je deze periodiek kunt evalueren.



Risicofactor



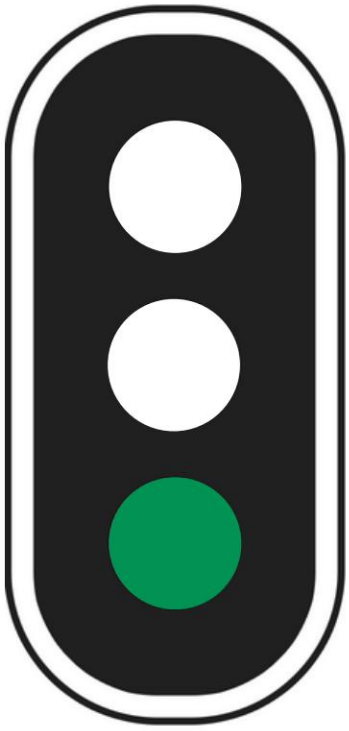
Internet en Wi-Fi

	Gevaar	Risico	In orde
Internetprovider en contracten		■	
Snelheid internetverbindings			■
Netwerkbeheer en VPN gebruik			■
Netwerkdekking kantoor			■
Netwerksegmentatie			■

Verbeterpunten

- Gedeelde internetverbinding met [redacted] Hiermee heb je mogelijk een afhankelijkheid. Advies is om een eigen verbinding te gebruiken.
- Zorg voor een separaat gasten netwerk.

Risicofactor

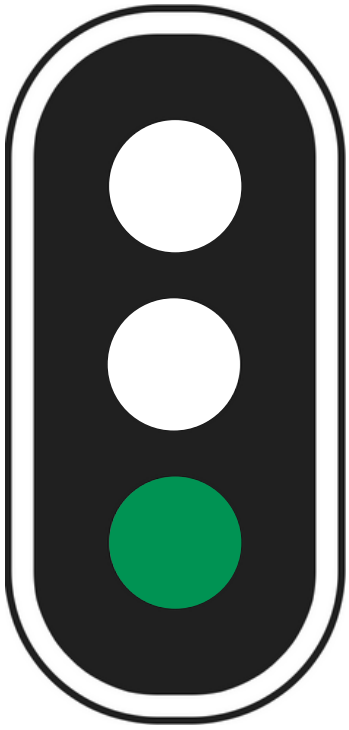


Hardware kantoor

	Gevaar	Risico	In orde
Hardware vergaderkamers	☐	☐	■
Welkomschermen en displays	☐	☐	☐
Narrowcasting	☐	☐	☐
Conferenceschermen	☐	☐	■
Calls en streaming apparatuur	☐	☐	■

Verbeterpunten

Risicofactor



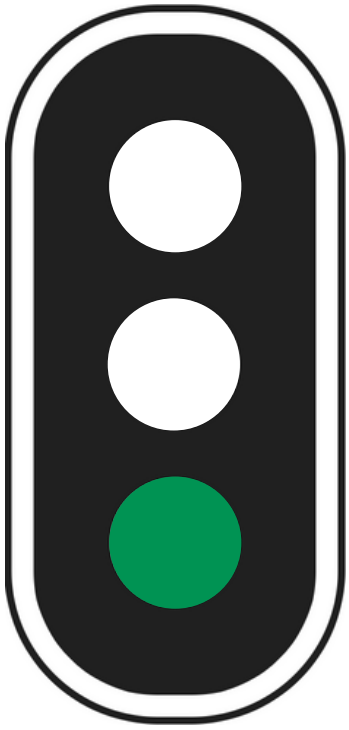
Communicatie en telefonie

	Gevaar	Risico	In orde
Telefonieprovider en contract	☐	☐	■
Apart netwerk	☐	☐	■
VOIP oplossing	☐	☐	■
Mobiele abonnementen en telefoons	☐	■	☐
Conferencetools en hardware	☐	☐	■

Verbeterpunten

- Middels VAMO is het goed geregeld echter niet alle telefoons zijn eigendom van het bedrijf, dus zorg ervoor da je bedrijfsgegevens op afstand kunt wissen indien nodig.

Risicofactor

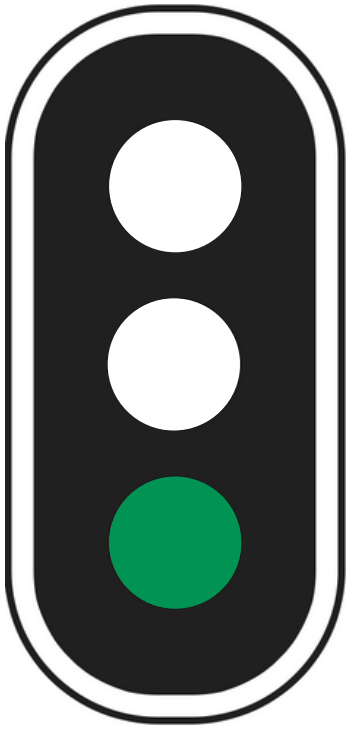


Domeinnamen en hosting

	Gevaar	Risico	In orde
Domeinnaam registratie en hosting	☐	☐	■
Contractoverzicht	☐	☐	■
WHOIS geanonimiseerd	☐	☐	■
E-mail koppelingen	☐	☐	■
Websitebeveiliging en updates	☐	☐	■

Verbeterpunten

Risicofactor



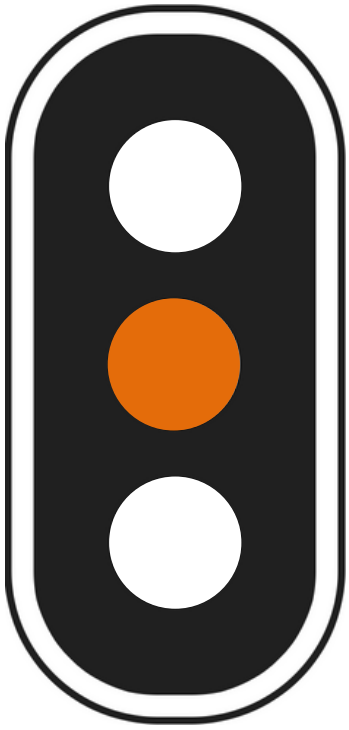
Conclusie en advies

	Gevaar	Risico	In orde
IT-beheer en beveiliging		■	
Bedrijfscontinuïteit		■	
Kostenbeheer			■
Extern beheer			■
Gebruikers en productiviteit			■

Verbeterpunten

- Gebruik Multifactor authenticatie voor bedrijfskritische toepassingen.
- Maak gebruik van Full Disk Encryptie op de werkplekken.
- Zorg voor een externe back-up met een duidelijk retentiebeleid.
- Zorg voor een herstelplan en test dit regelmatig.
- Momenteel gebruik je jaarlijkse licenties. Als er regelmatig personele wisselingen zijn ben je flexibeler met maandelijkse licenties. Deze zijn iets duurder maar ben je wel flexibeler. Daarnaast vindt ik € 92,40 per jaar aan licentiebeheer vrij fors voor het aantal gebruikers. De kosten voor jullie Microsoft licenties bedragen € 763,20 per jaar.

Risicofactor



Conclusie en advies

Complimenten voor de wijze waarop het ICT-beheer is geregeld. Afgezien van wat aandachtspunten omtrent beveiliging is dat goed op orde.
De patchkasten zagen er goed en netjes uit.

Als we inzoomen op de beveiliging en de bedrijfscontinuiteit valt er zeker winst te behalen. Door een goede back-up strategie, met een duidelijke retentie toe te passen en deze regelmatig te testen kun je vervelende situaties voorkomen.

Los van het kunnen herstellen, blijven we natuurlijk problemen liever voor. Dit kan opgelost worden door een goede werkplekbeveiliging in te zetten. Denk hierbij aan:
• Multifactor authenticatie, zeker wanneer apparatuur buiten de deur gebruikt wordt;
• Gebruik Full Disk Encryptie zodat je bij verlies van hardware geen data op straat hebt liggen;
• Endpoint Security met Cloud sandbox scanning (moderne antivirus);
• Een goede rechtenstructuur zodat medewerkers alleen bij gegevens kunnen die ze nodig hebben om hun werk te kunnen doen;
• Het gebruik van een Passwordmanager;

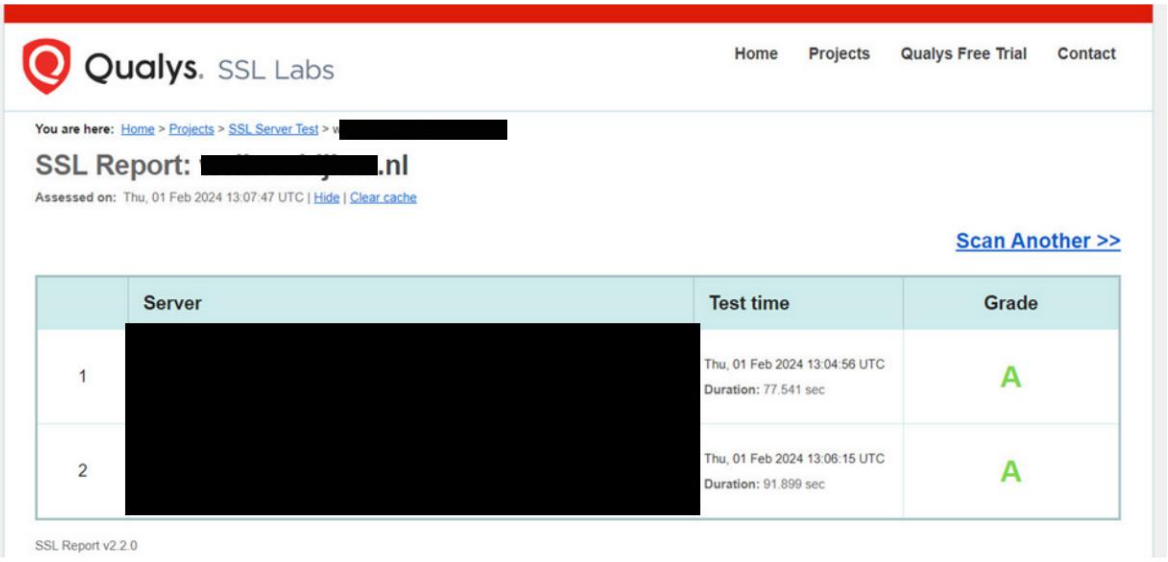
Om ervoor te zorgen dat een e-mail niet als spam gemarkeerd wordt bij de ontvanger is het zaak om je e-mail security ook goed in te regelen. Hiervoor zijn standaarden zoals DMARC, DKIM en SPF afgesproken. DMARC en DKIM staan niet goed ingesteld. Het SPF record is in orde.

Tot slot adviseren wij om een eigen internetverbinding af te sluiten om geen afhankelijkheid naar derden te hebben.

Kunnen wij jullie met een of meerdere punten helpen?
Dan horen wij dat uiteraard graag. Wij werken graag, geheel vrijblijvend een voorstel voor jullie uit.

Conclusie en advies

De website heeft momenteel een A score dat is voldoende.
Een perfecte score zou A++ zijn hiervoor kunnen zwakke Ciphers uitgeschakeld worden.



Als we een scan uitvoeren naar het publieke ip-adres van jullie internetverbinding valt het op dat er 3 poorten openstaan. Dit heeft met de Fortinet configuratie te maken.
Het is aan te raden dit regelmatig te updaten en heroverwegen of deze poorten nog noodzakelijk zijn.

Starting Nmap 7.93 (https://nmap.org) at 2024-02-01 13:23 CET
Nmap scan report for [redacted]
Host is up (0.00089s latency).
Not shown: 65531 filtered tcp ports (no-response), 1 closed tcp port (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT	STATE	SERVICE
8010/tcp	open	xmpp
8015/tcp	open	cfg-cloud
8020/tcp	open	intu-ec-svcdisc

M·IT SERVICES

Altijd Veilig in Bedrijf

WWW.MITSERVICES.NL