Technische QuickScan (APK voor het mbo)

IBPDOC30

GEBRUIKERSGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Verantwoording

Opdrachtgever:

Kennisnet / saMBO-ICT

Auteurs

Leo Bakker	(Kennisnet)
Ludo Cuijpers	(saMBO-ICT)
Robbin van den Dobbelsteen	(KZA)
Albert Hankel	(SURFnet)
Bart van den Heuvel	(SURFibo)
Frank van den Hurk	(Quarantainenet BV)
Alf Moens	(SURFnet)
Lloyd Verheijen	(Routz group)
Jan Visser	(PricewaterhouseCoopers Advisory N.V)
Ralph Wagter	(M&I/Partners)

April 2015

Sommige rechten voorbehouden

Inhoudsopgave

1. Inleiding

Het is zinvol om jaarlijks een test te organiseren waarbij de technische staat van het netwerk tegen het licht wordt gehouden. Een dergelijke test kan door de MBO instelling zelf worden gedaan, waarbij het eventueel mogelijk is om een extern bedrijf de uitkomsten te laten beoordelen. Uiteraard kan er ook voor gekozen worden om de gehele test uit te besteden. **Het is niet meer dan een eerste inventarisatie en beoordeling van de technische omgeving.** Er licht geen normenkader of beoordelingskader aan ten grondslag.

1.1 Keuze uit 2 mogelijkheden

De MBO instelling kan kiezen uit een tweetal testen. De eerste test kent een technische insteek en de tweede test een technische plus risico insteek. Er is een overlap tussen het ISO 27002 normenkader en de testen. Dit hoeft niet bezwaarlijk te zijn, omdat hierdoor de volledigheid van beide testen gewaarborgd wordt. In hoofdstuk 4 is aangegeven welke statements uit het MBO Toetsingskader ten minste van belang zijn voor een vlekkeloze technische werking. Deze statements zijn met de kleur rood in de eerste klom aangegeven.

1.2 Model cybersecurity

De beide testen gaan er van uit dat er maatregelen genomen zijn bij een security incident. Hieronder een korte toelichting van een mogelijke inrichting van een dergelijk proces (preventie, detectie en respons).

Drie aandachtsgebieden voor effectieve maatregelen.

Preventie

Preventie begint met governance en organisatie. Het gaat naast technische maatregelen onder andere om het beleggen van de verantwoordelijkheid voor cybercrime in de organisatie en om bewustwordingstrainingen voor belangrijke medewerkers.

Detectie

Een organisatie kan door het monitoren van kritieke gebeurtenissen en centrale veiligheidsincidenten en -gebeurtenissen de technologische detectiemaatregelen versterken. Monitoring en data mining vormen samen een uitstekend instrument om vreemde patronen in het gegevensverkeer op het spoor te komen, te signaleren waar de aanvallen zich concentreren en de systeemprestaties te observeren.

Respons

Bij respons gaat het om het in werking stellen van een plan zodra zich een aanval voordoet. Bij een aanval moet de organisatie alle getroffen technologie direct buiten werking kunnen stellen. Bij de ontwikkeling van een respons- en herstelplan doet een organisatie er goed aan (informatie)beveiliging te zien als een continu proces en niet als eenmalige oplossing.

	Preventie	Detectie	Respons
Beheer en Organisatie	Toewijzen van verantwoordelijkheden voor Cybercrime Verzorgen van training beveiligingsbewustzijn	Borgen van 24 x 7 stand-by crisis organisaties	Inzetten van forensische analyse vaardigheden
Processen	Uitvoeren cybercrime respons test (simulatie) Uitvoeren periodieke scans en penetratietesten	Uitvoeren procedures voor opvolging van incidenten	Uitvoeren cybercrime respons plan
Technologie	Realiseren van adequate Desktopbeveiliging Realiseren van netwerksegmentatie	Implementeren logging van kritieke processen Implementeren centraal monitoren van beveiligingsincidenten	Stoppen of verbreken van aangevallen IT-diensten

1.3 Aanvullende informatie

- De Secure Software Foundation heeft het Framework Secure Software ontwikkeld. Een recent Nederlands product met goede handreikingen.
- Toevoeging aan 3.2 Technische Veiligheid: geen enkele pentest kan achteraf een vervanger zijn voor een goed ontwikkelproces, waarin "secure coding"-practices worden toegepast. Een pentest gaat vaak alleen in op de OWASP top 10, er zijn natuurlijk veel meer kwetsbaarheden te onderkennen.
- Voor meer diepgang wordt verwezen naar de ICT-Beveiligingsrichtlijnen van het NCSC (hier komt een nieuwe versie van) en The Standard of Good Practice for Information Security van het IS

2. APK keuring technische omgeving (TEST 1)

2.1 Algemeen (overlap met toetsingskader mbo)

- Wat is jullie beleid met betrekking tot de ICT security van de netwerkinfrastructuur? (bijvoorbeeld logische/fysieke scheiding van netwerken, welke netwerken moeten gescheiden zijn etc.)
- Voeren jullie zelf risicoanalyses uit op de inrichting van de infrastructuur: (wijze van) segmentering van het netwerk, authenticatie van interne/externe gebruikers, te gebruiken beveiligingsmaatregelen zoals encryptie en detectie?
- Hoe vaak testen jullie zelf de security omgeving en hoe weet je dat 'veilig' echt 'veilig' is?
- Met welke methoden scannen jullie zelf de kwetsbaarheden van buiten en/of binnen af?
- Laten jullie door externe partijen penetratietests uitgevoerd op het interne netwerk/externe netwerk/web applicaties?
- Wanneer is jullie laatste security probleem in het ICT-landschap (de centrale ICT-faciliteiten van de instelling) geweest?
- Welke componenten zijn er binnen jullie ICT netwerkinfrastructuur zwak ten opzichte van de rest?
- Worden medewerkers regelmatig "bijgespijkerd" en blijven zij geïnformeerd over de laatste ontwikkelingen (bedreigingen, aanvalsmethoden, bedreigingen) op "security" gebied?
- Heb je afspraken over het gebruik van het netwerk en internet, bijvoorbeeld in een ICT reglement of een acceptable use policy?

2.2 Procedures (overlap met toetsingskader mbo)

- Is er een proces voor de snelle en adequate afhandeling van 'security incidenten' inclusief ingerichte organisatie/verantwoordelijkheden (CSIRT: Computer Security Incident Response Team)?
- Hoe handel je wijzigingen in de infrastructuur (vervanging/implementatie van componenten, maar ook wijzigingen in de configuratie) af? Is daar een vaste procedure voor?
- Hoe hebben jullie de user provisioning ingeregeld? Zijn er formele indienst-/uitdienstprocedures? Gebruik jullie interne of externe directories? Zijn er periodieke controles op autorisaties?
- Is er een proces voor "hardening" (Hardening is het proces waarbij overbodige functies in besturingssystemen uitgeschakeld worden en/of van het systeem verwijderd worden. En daarnaast door zodanige waarden toekennen aan beveiligingsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat. Het gaat hierbij ook om het verwijderen van niet gebruikte of onnodige gebruikers accounts, en tevens het wijzigen van standaard wachtwoorden die op sommige systemen aanwezig kunnen zijn.)van relevante delen van de infrastructuur (bijvoorbeeld firewalls/reverse proxies, netwerkcomponenten, DNS-servers, applicatieservers etc.) en periodieke controle op autorisaties ingericht?
- Is er een proces voor "patch management" van de relevante delen van de infrastructuur ingericht?
- Op welke manieren authentiseren jullie gebruikers?
  Opmerking: Voldoet de kwaliteit van wachtwoorden etc. aan 'best practices'
- Wat gebeurt er buiten kantoortijd met signalen rondom informatiebeveiliging?

2.3 Techniek dreigingen extern

- Welke firewalls worden gebruikt om het verkeer vanaf buitenaf tegen te houden?
- Is er een Demilitariseerde Zone ingericht waarin uitsluitend componenten staan die toegang moeten hebben tot het publieke netwerk (en geen productiegegevens)?
  Opmerking: Ook productiegegevens kunnen in de DMZ toegestaan zijn, zoals de activiteitenkalender.
- Zijn er maatregelen ingericht tegen Denial-of-Service aanvallen?
- Hoe houden jullie controle over verkeer buiten en binnen de Cloud? Weten jullie welke cloud diensten gebruikt worden? Voor primair proces? Voor persoonlijk gebruik? Welke afspraken zijn daar over?

2.4 Techniek dreigingen intern

- Zijn er afspraken over het gebruik van mobiele apparatuur?
- Hoe "open" staat jullie wireless omgeving? Voor iedereen toegankelijk of niet? Maken jullie gebruik van 802.1x en/of andere methoden voor netwerktoegangscontrole?
- Hoe "open" staat jullie bedrade netwerk? Voor iedereen toegankelijk of niet? Maken jullie gebruik van 802.1x en/of andere methoden voor netwerktoegangscontrole?
- Hoe wordt geborgd dat besmette werkplekken worden gedetecteerd? Worden er naast anti-virus nog andere technieken ingezet? Hoe rapporteren of zien jullie momenteel het vreemde / afwijkende / verdachte verkeer?
- Welke opvolging wordt er gegeven op gedetecteerd vreemd/afwijkend/verdacht verkeer? Zijn hiervoor technische maatregelen ingericht?
- Zijn de essentiële verbindingen (bijvoorbeeld voor beheer) voldoende beveiligd? Van welke encrypties maken jullie gebruik?
- Hoe is jullie dat center ingericht? In house of out house? Welke fysieke beveiligingsmaatregelen zijn hierbij genomen?
- Zijn er maatregelen genomen tegen Single-Points-of-Failure (SPOFs) door essentiële componenten (bijvoorbeeld core switches) dubbel uit te voeren?
- Worden interne verkeerstromen ook onderling gefilterd?

2.5 Aanvullende dumps en scans

- Dump van de AD (Microsoft omgeving) om deze te analyseren. Hieruit haal je:
  - Wachtwoordbeleid, en of dit consequent wordt toegepast;
  - Aantal beheerders en andere accounts met additionele privileges.
- MSBA rapportage (Microsoft omgeving) om patch management van het OS te valideren, een kleine steekproef is voldoende.
- Liefst een basale kwetsbaarhedenscan van 2-3 interne en externe systemen, bijvoorbeeld met openvas oid (thermometer gehalte).
- Liefst een NIST-scan voor controleren hardening maatregelen. Aan deze tooling zijn enige out-of-pocket kosten verbonden.

2.6 Correctie en herstel

- Welke back up tooling wordt er gebruikt, worden alle servers hierin meegenomen?
- Zijn er voor de netwerkcomponenten zoals de firewall, etc. ook back ups van de configs?
- Wordt de DMZ ook gebackuped?
- Is de back up gescheiden opgezet van het productienetwerk?
- Hoe rapporteer je over de RPO-RTO (zijn deze bekend bij het management)?

3. APK keuring technische omgeving (TEST 2)

3.1 Inrichting

De ontwikkelingen op het gebied van informatiebeveiliging volgen elkaar op de voet. Bedrijven en organisaties kunnen niet meer om informatiebeveiliging heen, maar weten vaak niet waar ze staan of waar ze moeten beginnen. Vooral op technisch vlak is hier soms veel onduidelijkheid over. Daarom is het waardevol hier snel inzicht in te kunnen krijgen door middel van een overzicht van aandachtsgebieden waar direct eventuele GAP's met het huidige beleid duidelijk worden.
Om dit te realiseren zijn op basis van best-practices en normenkaders (o.a. ISO27001, BSIMM) een aantal onderwerpen gekozen. te weten:

- Backup & Restore;
- Security Testing;
- Secure Coding;
- Scheiding van systemen;
- Logging;
- Security incidents;
- Authenticatie;
- Communicatie;
- Opslag;
- Toegang;
- Updates & Patches;
- Procesinrichting;

Met behulp van een aantal korte vragen wordt ieder onderwerp onderzocht. Op basis daarvan kan worden bepaald huidige inrichting voldoet aan de gestelde norm.

3.2 Technische veiligheid

Met de nog steeds toenemende digitalisering en ontsluiting naar het internet wordt het belang van veilige systemen steeds groter. Wanneer een organisatie intern voldoet aan informatiebeveiligingsnormen geeft dit een bepaalde mate van zekerheid van de veiligheid. Toch zijn er zaken die niet afgevangen kunnen worden door middel van organisatorische inrichting. Hierbij gaat het met name om kwetsbaarheden in al dan niet zelf ontwikkelde software. Zelfs wanneer een ontwikkelafdeling zeer hoge standaarden op het gebied van informatiebeveiliging hanteert kunnen er kwetsbaarheden bestaan in een applicatie. Dit is inherent aan de complexiteit van software.
Om inzicht te krijgen in kwetsbaarheden in software of onderliggende platformen wordt een zogeheten quick scan penetratietest uitgevoerd. Hierbij wordt op basis van veel voorkomende kwetsbaarheden en fouten de applicatie getest op veiligheid en fouten. Dit kan gedeeltelijk geautomatiseerd wat in zeer korte tijd een goed eerste beeld geeft van de veiligheid van de applicatie. Indien hieruit opvallende bevindingen komen kan ervoor gekozen worden om een uitgebreidere en handmatige penetratietest uit te voeren welke een grotere mate van zekerheid over de veiligheid van het systeem kan geven.

3.3 Technische Cybersecurity APK

3.3.1 Back up & Restore

	Vraag	Risico
1-1	Van welke systemen worden back-ups gemaakt? **Antwoord:**	Indien geen back-ups gemaakt worden kan gegevensverlies optreden bij incidenten of hardware failure
1-2	Wat voor soort back-ups zijn dit? (Full, incremental, snapshots) **Antwoord:**	Incremental back-ups en snapshots kunnen een systeem niet volledig herstellen
1-3	Wat is de frequentie van deze back-ups? **Antwoord:**	Weinig back-ups zorgen mogelijk voor groter verlies van data
1-4	Welke systemen worden NIET geback-upt? **Antwoord:**	Deze systemen kunnen volledig verloren gaan
1-5	Waarom niet? **Antwoord:**	-
1-6	Worden er volledige restore tests uitgevoerd van alle geback-upte systemen? **Antwoord:**	Het is mogelijk dat er fouten zitten in het restore proces of in de gebruikte programmatuur
1-7	Wat is de frequentie van deze restore tests? **Antwoord:**	

3.3.2 Security Testing

	Vraag	Risico
2-1	Worden er periodieke penetratietesten uitgevoerd? **Antwoord:**	Bedrijf heeft geen inzicht in kwetsbaarheden van applicaties en systemen
2-2	Welke systemen worden er getest? **Antwoord:**	Bedrijf heeft geen inzicht in kwetsbaarheden van applicaties en systemen
2-3	Wordt dit gedaan door wisselende partijen? **Antwoord:**	Verschillende partijen gebruiken verschillende benaderingen met als gevolg mogelijk groter inzicht in de veiligheid van de applicatie
2-4	Worden her testen uitgevoerd van eerdere penetratiestesten? **Antwoord:**	Hierdoor wordt opvolging van bevindingen gecontroleerd
2-5	Worden bevindingen altijd opgevolgd? **Antwoord:**	Onvoldoende opvolging kan leiden tot blijvende en/of ondergeschoven kwetsbaarheden

3.3.3 Secure Coding		
	Vraag	**Risico**
3-1	Worden er risicoanalyses uitgevoerd bij het opstarten van een project? **Antwoord:**	Het is onduidelijk welke risico's gelopen worden tijdens en bij go-live van het project
3-2	Welke personen zijn hierbij betrokken / verantwoordelijk? **Antwoord:**	Er dienen security experts bij betrokken te zijn
3-3	Wordt er gebruik gemaakt van secure coding guidelines? (OWASP) **Antwoord:**	De applicatie loopt groter risico op kwetsbaarheden met hogere herstelkosten
3-4	Wordt er gebruik gemaakt van andere best practices/guidlines? (ASVS) **Antwoord:**	De applicatie loopt groter risico op kwetsbaarheden met hogere herstelkosten
3.3.4 Scheiding van systemen		
	Vraag	**Risico**
4-1	Zijn alle systemen, applicaties, DB's, interfaces, etc. duidelijk in kaart? **Antwoord:**	Onvoldoende zicht op applicatielandschap kan leiden tot outdated systemen
4-2	Is er een duidelijke scheiding tussen OTAP? (fysiek/logisch) **Antwoord:**	In geval van calamiteiten worden niet alle omgevingen aangetast.
4-3	Is functiescheiding hierop van toepassing? **Antwoord:**	Er kunnen ongecontroleerde wijzigingen worden doorgevoerd
4-4	Wordt er bij architectuur rekening gehouden met scheiding van systemen? (Webserver, applicatieserver, DB-server, etc.) **Antwoord:**	Zonder scheiding is het aanvalsoppervlak groter en mogelijke impact van inbraak groter
4-5	Word er gebruik gemaakt van een DMZ? **Antwoord:**	Zonder scheiding is het aanvalsoppervlak groter en mogelijke impact van inbraak groter
4-6	Word er gebruik gemaakt van Reverse proxy's? **Antwoord:**	
3.3.5 Logging		
	Vraag	**Risico**
5-1	Op welke systemen wordt logging toegepast? **Antwoord:**	In geval van incidenten kan niet worden teruggegrepen op logging
5-2	hoe uitgebreid is deze logging? **Antwoord:**	In geval van incidenten kan te weinig (nuttige) informatie worden gevonden
5-3	Wie heeft toegang tot de logging? **Antwoord:**	Ongeautoriseerde toegang kan leiden tot wijzigen/verwijderen van logging

5-4	Wordt de logging actief gemonitord? **Antwoord:**	Onregelmatigheden worden niet op tijd opgemerkt
5-5	Wordt de logging periodiek gecheckt op onregelmatigheden? **Antwoord:**	Onregelmatigheden worden niet op tijd opgemerkt

3.3.6 Security incidenten

	Vraag	**Risico**
6-1	Is er een centraal aanspreekpunt voor het melden van security incidenten? **Antwoord:**	Security incidenten worden niet gemeld
6-2	Hoe is de opvolging hiervan geregeld? **Antwoord:**	Security incidenten blijven bestaan, motivatie tot melden verdwijnt
6-3	Hebben klanten en/of buitenstaanders de mogelijkheid security kwetsbaarheden te melden? **Antwoord:**	Kwetsbaarheden worden op andere oncontroleerbare manieren bekend
6-4	Zo ja, hoe vind de opvolging hiervan plaats? **Antwoord:**	Security incidenten blijven bestaan, motivatie tot melden verdwijnt
6-5	Zo nee, hoe wordt omgegaan wanneer dit wel gebeurt? **Antwoord:**	Security incidenten blijven bestaan, motivatie tot melden verdwijnt

3.3.7 Authenticatie

	Vraag	**Risico**
7-1	Worden sterke wachtwoorden voor alle applicaties en systemen afgedwongen? **Antwoord:**	Zwakke wachtwoorden zijn gemakkelijker te kraken
7-2	Wordt gebruik gemaakt van 2factor authenticatie voor gevoelige of kritieke systemen? **Antwoord:**	Wachtwoorden zijn mogelijk eenvouding af te kijken, raden of kraken
7-3	Zijn interne systemen afgeschermd van buiten? **Antwoord:**	Aanvalsoppervlak van organisatie is groot
7-4	Wordt ip restrictie toegepast? **Antwoord:**	Aanvalsoppervlak van organisatie is groot
7-5	Wordt er gebruik gemaakt van VPN? **Antwoord:**	VPN kan een veilige manier van werken op afstand zijn
7-6	Hoe is de toegang hiertoe geregeld? **Antwoord:**	In geval van compromittering leidt ruime toegang tot grotere impact
7-7	Welke applicaties/servers/etc. zijn er te benaderen via de VPN? **Antwoord:**	Aanvalsoppervlak van organisatie is groot
7-8	Wordt er gebruik gemaakt van 2fa voor de VPN? **Antwoord:**	Wachtwoorden zijn mogelijk eenvoudig af te kijken, raden of kraken

3.3.8 Communicatie		
	Vraag	**Risico**
8-1	Wordt er voor alle systemen gebruik gemaakt van HTTPS? **Antwoord:**	Oversleutelde verbinding is mogelijk uit te lezen; identiteit van website kan niet geverifieerd worden
3.3.9 Opslag		
	Vraag	**Risico**
9-1	Zijn systemen versleuteld? (BitLocker) **Antwoord:**	Oversleutelde systemen kunnen eenvouding worden uitgelezen
9-2	Is het toegestaan gevoelige data op te slaan op lokale harde schijf? **Antwoord:**	Lokaal opgeslagen data is eenvoudig uit te lezen (oplossing: BitLocker)
9-3	Wordt er gebruik gemaakt van onversleutelde USB-sticks? **Antwoord:**	Oversleutelde USB sticks met gevoelige informatie zijn zeer eenvoudig uit te lezen en er is grote kans op verlies of diefstal
9-4	Wordt er gebruik gemaakt van cloud-opslag? **Antwoord:**	Cloud opslag kan onderhevig zijn aan andere wetgeving en mogelijke verlies van data betekenen bij calamiteiten leverende partij
9-5	Wordt hiervoor gebruik gemaakt van 2fa? **Antwoord:**	Wachtwoorden zijn mogelijk eenvouding af te kijken, raden of kraken
9-6	Wordt opslag die kapot is of aan het einde van de levensduur door een specialistisch bedrijf verwijderd? **Antwoord:**	Oversleutelde systemen kunnen eenvoudig worden uitgelezen
3.3.10 Toegang		
	Vraag	**Risico**
10-1	Is toegang tot server ruimtes beperkt? **Antwoord:**	ongeautoriseerde toegang tot of wijzigingen van systemen
10-2	Zijn USB poorten afgeschermd? **Antwoord:**	Besmette USB sticks kunnen systemen infecteren en gegevens stelen
10-3	Is het mogelijk gebruik te maken van UTP kabels om op het netwerk te komen met willekeurige apparaten? **Antwoord:**	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-4	Wordt er gebruik gemaakt van MAC whitelisting? **Antwoord:**	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-5	Is er beveiligde Wifi aanwezig? **Antwoord:**	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-6	Is er een scheiding tussen interne en gasten wifi? **Antwoord:**	Ongeautoriseerde apparaten krijgen toegang tot netwerk
10-7	Is er filtering actief op het netwerk (ports, websites) **Antwoord:**	Ongeautoriseerde apparaten krijgen toegang tot netwerk

10-8	Wordt er gebruik gemaakt van IPS/IDS **Antwoord:**	geen monitoring op mogelijke aanvallen
10-9	Zo ja, vind hier actieve monitoring op plaats? **Antwoord:**	te late reactie op mogelijke aanvallen

3.3.11 Updates & Patches

	Vraag	**Risico**
11-1	Is er patch management actief? **Antwoord:**	Geen actuele versies met mogelijk bekende kwetsbaarheden
11-2	Worden applicaties en systemen altijd voorzien van de laatste security updates? **Antwoord:**	Geen actuele versies met mogelijk bekende kwetsbaarheden
11-3	Blijven applicatiebeheerders op de hoogte van 0-day kwetsbaarheden of andere bekende kwetsbaarheden? **Antwoord:**	Mogelijk onveilige systemen
11-4	Worden er maatregelen genomen wanneer kwetsbaarheden van toepassing zijn? **Antwoord:**	Mogelijk onveilige systemen

4. Technische audit statements (rood)

4.1 Cluster beleid en organisatie

Nr.	ISO27002	Statement
1.1	5.1.1.1	Beleidsregels voor informatiebeveiliging: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd en goedgekeurd door het bestuur.
1.2	5.1.1.2	Beleidsregels voor informatiebeveiliging: Het door het bestuur vastgestelde Informatiebeveiligingsbeleid wordt gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
1.3	5.1.2	Beoordeling van het Informatiebeveiligingsbeleid: Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
1.4	6.1.1	Taken en verantwoordelijkheden informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen
1.5	6.1.5	Informatiebeveiliging in projectbeheer: Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.
1.6	6.2.1.1	Beleid voor mobiele apparatuur: Er dient beleid te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.
1.7	8.2.1	Classificatie van informatie: Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
1.8	8.2.2	Informatie labelen: Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
1.9	10.1.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld.
1.10	10.1.1.2	Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van crypto grafische beheersmaatregelen wordt geïmplementeerd.
1.11	11.2.5	Verwijdering van bedrijfsmiddelen: Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.
1.12	13.2.1	Beleid en procedures voor informatietransport: Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
1.13	13.2.2	Overeenkomsten over informatietransport: Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.
1.14	14.1.1	Analyse en specificatie van informatiebeveiligingseisen: De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.
1.17	16.1.1	Verantwoordelijkheden en procedures: Er zijn leidinggevende en -procedures vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
1.19	18.1.3	Beschermen van registraties: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.
1.20	18.1.4	Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.
1.21	6.1.2	Scheiding van taken: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

4.2 Cluster personeel, studenten en gasten

Nr.	ISO27002	Statement
2.1	7.1.2	**Arbeidsvoorwaarden**: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.
2.2	7.2.2	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging:** Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
2.3	9.2.6	**Toegangsrechten intrekken of aanpassen:** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
2.4	11.2.9	**'Clear desk'- en 'clear screen'-beleid**: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.
2.5	13.2.4	**Vertrouwelijkheids- of geheimhoudingsovereenkomst:** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.
2.6	16.1.3	**Rapportage van zwakke plekken in de informatiebeveiliging:** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.
2.7	7.1.1	**Screening**: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.

4.3 Ruimten en apparatuur

Nr.	ISO27002	Statement
3.1	6.2.1.2	**Beleid voor mobiele apparatuur:** Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.
3.2	8.3.2	**Verwijderen van media:** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
3.3	11.1.1	**Fysieke beveiligingszone:** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
3.4	11.1.2	**Fysieke toegangsbeveiliging:** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
3.5	11.1.3	**Kantoren, ruimten en faciliteiten beveiligen:** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.
3.6	11.1.4	**Beschermen tegen bedreigingen van buitenaf:** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
3.7	11.1.5	**Werken in beveiligde gebieden:** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
3.8	11.1.6	**Laad- en loslocatie:** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.
3.9	11.2.1	**Plaatsing en bescherming van apparatuur:** Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.
3.10	11.2.2	**Nutsvoorzieningen:** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.
3.11	11.2.3	**Beveiliging van bekabeling:** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.
3.12	11.2.4	**Onderhoud van apparatuur:** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
3.13	11.2.6	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein:** Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.
3.14	11.2.7	**Veilig verwijderen of hergebruiken van apparatuur:** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
3.15	12.4.4	**Kloksynchronisatie:** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.

4.4 Continuïteit

Nr.	ISO27002	Statement
4.1	12.1.2	**Wijzigingsbeheer:** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.
4.2	12.1.4	**Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.
4.3	12.2.1.1	**Beheersmaatregelen tegen malware:** Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd.
4.4	12.2.1.2	**Beheersmaatregelen tegen malware:** Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers te vergroten ten aanzien van het gevaar van virussen en dergelijke.
4.5	12.3.1.1	**Back-up van informatie:** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt.
4.6	12.3.1.2	**Back-up van informatie:** Gemaakte back ups worden regelmatig getest conform het back-up beleid.
4.7	12.5.1	**Software installeren op operationele systemen:** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.
4.8	12.6.1	**Beheer van technische kwetsbaarheden:** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.
4.9	12.6.2	**Beperkingen voor het installeren van software:** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.
4.10	14.2.6	**Beveiligde ontwikkelomgeving:** Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.
4.11	15.2.2	**Beheer van veranderingen in dienstverlening van leveranciers:** Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.
4.12	16.1.4	**Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen:** Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiliging incidenten.
4.13	16.1.5	**Respons op informatiebeveiligingsincidenten:** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
4.14	17.1.2	**Informatiebeveiligingscontinuïteit implementeren:** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.
4.15	17.2.1	**Beschikbaarheid van informatie verwerkende faciliteiten:** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

4.5 Toegangsbeveiliging en integriteit

Nr.	ISO27002	Statement
5.1	9.1.1	**Beleid voor toegangsbeveiliging:** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
5.2	9.1.2	**Toegang tot netwerken en netwerkdiensten:** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
5.3	9.2.1	**Registratie en afmelden van gebruikers:** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
5.4	9.2.2	**Gebruikers toegang verlenen:** Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
5.5	9.2.3	**Beheren van speciale toegangsrechten:** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
5.6	9.2.4	**Beheer van geheime authenticatie-informatie van gebruikers:** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.
5.7	9.3.1	**Geheime authenticatie-informatie gebruiken:** Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie informatie houden aan de praktijk van de organisatie.
5.8	9.4.1	**Beperking toegang tot informatie:** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.
5.9	9.4.2	**Beveiligde inlogprocedures:** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
5.10	10.1.2.1	**Sleutelbeheer:** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld.
5.11	10.1.2.2	**Sleutelbeheer:** Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.
5.12	12.4.2	**Beschermen van informatie in logbestanden:** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
5.13	13.1.1	**Beheersmaatregelen voor netwerken:** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
5.14	13.1.2	**Beveiliging van netwerkdiensten:** Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
5.15	13.1.3	**Scheiding in netwerken:** Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.
5.16	13.2.3	**Elektronische berichten**: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd
5.17	14.1.3	**Transacties van toepassingen beschermen:** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

4.6 Controle en logging

Nr.	ISO27002	Statement
6.1	9.2.5	**Beoordeling van toegangsrechten van gebruikers:** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
6.2	12.4.1	**Gebeurtenissen registreren:** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
6.3	12.4.3	**Logbestanden van beheerders en operators:** Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
6.4	14.2.7	**Uitbestede softwareontwikkeling:** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.
6.5	14.2.8	**Testen van systeembeveiliging:** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.
6.6	14.2.9	**Systeemacceptatietests:** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
6.7	15.2.1	**Monitoring en beoordeling van dienstverlening van leveranciers:** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.
6.8	16.1.7	**Verzamelen van bewijsmateriaal:** De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.
6.9	18.2.2	**Naleving van beveiligingsbeleid en –normen:** Het management behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.
6.10	18.2.3	**Beoordeling van technische naleving:** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.

Bijlage 1: Framework informatiebeveiliging en privacy in het mbo