IT SECURITY KOMPAS

SecKompas Nederland B.V.

Datum: 22 september 2020
Versie: 2020.1 start-pakket

Managementsamenvatting

Cyberaanvallen worden steeds intelligenter. Gerichte aanvallen verschuiven van grotere bedrijven naar het MKB. Het is niet de vraag of je gehackt wordt maar wanneer! Aanvallen veroorzaken (herstel)kosten en remmen de groei en innovatiekracht af. Ook de reputatieschade is vaak groot. Voldoende beveiliging is dus noodzakelijk. Dat geldt ook voor een optimale inzet van de beschikbare middelen. Dit onafhankelijke rapport geeft je het inzicht en handvatten om een concreet actieplan op te stellen en het securityniveau stapsgewijs te verhogen. Dit rapport geeft tevens antwoord op de vraag: wat is de zwakste schakel?

Securityniveau

Op basis van de aangeleverde informatie past het securityprofiel[1] **Beheerd** bij SecKompas Nederland B.V..

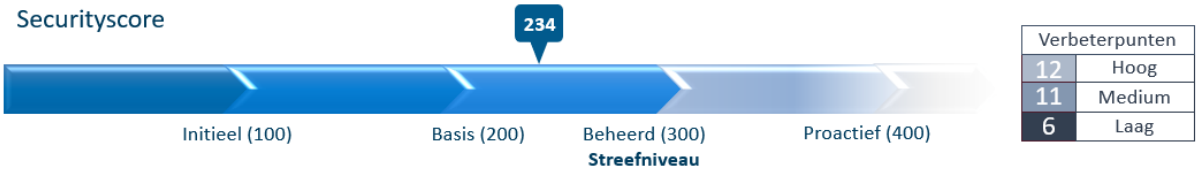
Dit securityniveau is het streefniveau waarop de waardering in dit rapport gebaseerd is.
Op basis hiervan kan SecKompas een effectief actieplan maken dat past bij haar mogelijkheden, prioriteiten en het beschikbare budget, te beginnen bij de zwakste schakel(s).

Het securityniveau **Beheerd** geeft bescherming tegen bekende en meerdere onbekende bedreigingen. Dit niveau is geschikt voor bedrijven met bedrijfskritische processen en privacygevoelige of vertrouwelijke gegevens. Deze organisaties zijn geen specifiek doel maar wel een interessante prooi voor cybercriminelen.

De securityscore van een organisatie is een berekende score over de verschillende domeinen, thema's en elementen. 163 security gerelateerde elementen worden in de berekening van de score meegenomen. De score behorende bij het niveau Beheerd is 300. Dit is het streefniveau.

Securityniveau SecKompas.

Onderstaande grafiek toont de securityscore en het aantal verbeterpunten met een hoge, medium en lage prioriteit. Het is niet mogelijk om het streefniveau te bereiken zolang er verbeterpunten met een hoge of medium prioriteit zijn.

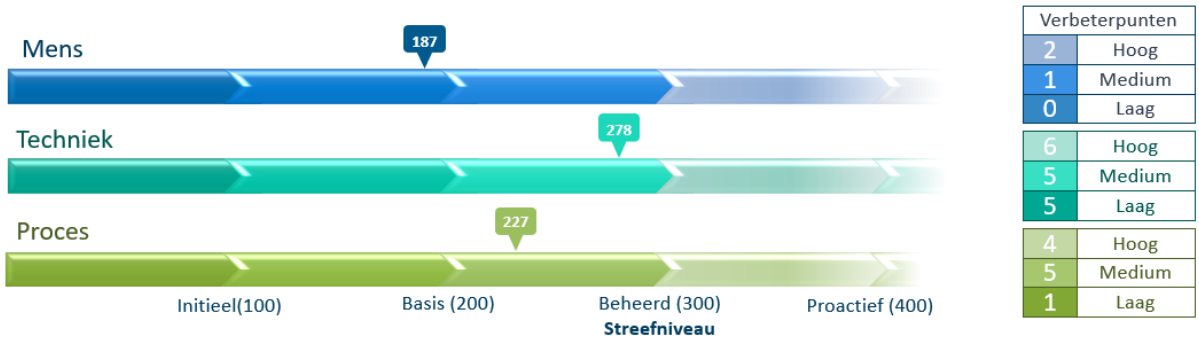


Met een securityscore van **234** en **29** verbeterpunten is het securityniveau van SecKompas **goed** te noemen. Er zijn een aantal verbeterpunten met een hoge en medium prioriteit. Deze elementen moeten aangepakt worden om het streefniveau te halen.

De securityscore en de bevindingen vormen een goed uitgangspunt voor groei naar een nog veiliger IT-landschap. De impact is het grootste wanneer als eerste de zwakste schakels – de verbeterpunten met een hoge prioriteit – aangepakt worden. Het streefniveau is behaald zodra er geen aandachts- en verbeterpunten meer zijn met een hoge en medium prioriteit.

[1] Uitleg over de verschillende securityniveaus vind je in bijlage 1.

De securityonderwerpen zijn verdeeld in 3 domeinen: Mens, Techniek en Proces.
Alle drie de domeinen zijn belangrijk. Je kunt alles nog zo goed beveiligen maar als iemand de deur openhoudt staan de techniek buitenspel.
Het aantal controle elementen verschilt per domein. Er is geen verband tussen de securityscores en verbeterpunten per domein.
Onderstaande grafiek geeft de securityscore en de verbeterpunten voor deze 3 domeinen aan.



Positieve bevindingen
SecKompas scoort goed op de volgende thema's:

- Back-up
- Mail security
- Hostprotectie
- Monitoring
- Access Control

Aandachts- en verbeterpunten
De volgende thema's hebben zeker extra aandacht nodig:

- Multi-Factor-Authenticatie (MFA) voor cloud-gebruikers
- Firewall/UTM
- Patchmanagement van netwerk devices, randapparaten en IoT/OT devices
- Patchmanagement van applicaties
- Bewustzijn binnen de organisatie
- *Alleen de 5 belangrijkste aandachts- en verbeterpunten zijn in het start-pakket uitgewerkt. Bij het de pakketten Compleet en Elite worden alle aandachts- en verbeterpunten uitgewerkt om het streefniveau te halen.*

Globale kostenindicatie

De kosten voor de implementatie van de verbeterpunten zijn afhankelijk van de bestaande infrastructuur. Op basis van de kennis en ervaring van het panel krijg je een ruwe kostenindicatie van de verbeterpunten. Deze indicatie geeft voor de meeste organisaties een goede inschatting.

De benodigde investeringen om de verbeterpunten aan te pakken, blijven **beperkt**. In enkele gevallen is het waarschijnlijk noodzakelijk om de apparatuur te vervangen. Om voor SecKompas tot een exacte kostenindicatie te komen moeten de verbeterpunten op de bestaande infrastructuur geprojecteerd worden.

1. Inleiding

IT-security is voor elke organisatie belangrijk en wordt steeds belangrijker. De cijfers bewijzen dat jaar op jaar. Elke organisatie is – in meer of mindere mate – doelwit voor cyberaanvallen. Vraag jezelf niet af of je te maken krijgt met een security incident maar wanneer.

Hoe wapen je je tegen cybercriminaliteit? Allereerst is het cruciaal om technische maatregelen te nemen. Daarnaast is het zaak om de rol van de mens en het proces kritisch te bekijken. Bij security incidenten is de mens (lees de medewerker) steeds vaker het initiële doelwit. En dat is niet voor niets. De maatregelen in de domeinen Mens, Techniek en Proces moeten in balans zijn. Het heeft geen zin om op technisch vlak alle mogelijke maatregelen te treffen en geen aandacht te besteden aan het domein Mens.
Of zoals de beroemde hacker Kevin Mitnick zegt: 'Hoe goed beveiligd een fort ook is, als iemand de poort openhoudt, staan alle technische maatregelen buiten spel.'

Het meeste effect krijg je door de zwakste schakels aan te pakken. Daarom moeten die inzichtelijk zijn. Je kunt je niet met één maatregel beschermen tegen een cyberaanval. Het is de combinatie van maatregelen die zorgt voor een adequate beveiliging.

Het is belangrijk dat het securityniveau past bij SecKompas. Hoe afhankelijk ben je van IT? Zijn er veel bedrijfskritische processen die bij verstoring de continuïteit in gevaar brengen? Heb je veel privacygevoelige of vertrouwelijke gegevens? Hoeveel data mag je maximaal kwijt zijn? Hoe groot is je budget? Al deze vragen zijn van belang. Verandert jouw organisatie, dan verandert het noodzakelijke securityniveau.
Beschik je over een goed inzicht in het huidige en het gewenste securityniveau? Op basis van dit inzicht bepaal je welke acties nodig zijn om de IT-beveiliging op het niveau te brengen dat past bij jouw organisatie.

IT-security is zo sterk als de zwakste schakel. Het IT Security Kompas:

- geeft een volledig **inzicht** in het huidige niveau van jouw IT security weerbaarheid;
- geeft bruikbare verbeterpunten om direct een onderbouwd **actieplan** te maken;
- geeft input om het beschikbare **budget** optimaal in te zetten en de weerbaarheid te verhogen;
- maakt de **voortgang** inzichtelijk;
- geeft concrete, heldere handvatten om in **gesprek** te gaan met de interne IT-afdeling of de IT-partner over IT-security.

Het model van dit kompas zorgt voor een advies dat breed toepasbaar is. Het geeft je de handvatten om je security op een hoger plan te brengen. Sommige aandachts- of verbeterpunten staan misschien al op je netvlies of zijn voor SecKompas niet relevant. Bespreek dit rapport daarom met je collega's en IT-partner(s). Zo kun je een effectief en realiseerbaar actie- of projectplan maken, dat volledig afgestemd is op het gewenste securityniveau, de organisatie én het beschikbare budget.

Het IT Securitykompas kijkt naar de inzet van technische en administratieve maatregelen. Niet naar de werkelijke configuratie van die maatregelen. Specialisten kunnen deze configuraties inhoudelijk goed beoordelen. Of vraag het IT Security Kompas wat ze hierin kunnen betekenen.

2. IT-security streefniveau

De mate van afhankelijkheid van IT bepaalt het securityprofiel voor jouw organisatie. Wanneer komt de continuïteit van de organisatie in gevaar? Wat is het maximale dataverlies en hoe lang mag de hersteltijd bij een maximaal incident zijn? Het is belangrijk om deze informatie (snel) paraat te hebben. Dat hoeft niet ingewikkeld te zijn. Ga pragmatische te werk. Een begin heb je al gemaakt tijdens het invullen van de vragenlijst.

Binnen het IT Security kompas zijn 5 verschillende security profielen gedefinieerd: Initieel, Basis, Beheerd, Proactief en Adaptief. De beschrijving van de niveaus vind je in bijlage 1.

Het IT Security Kompas combineert de aangeleverde informatie met de praktijkervaring van het IT Security panel[2] en de beschikbare statistische informatie. Zo ontstaat het streefniveau. Als de uitgangspunten zwaarder of minder zwaarwegend zijn, wijzigt het streefniveau.
Onderstaande factoren zijn bepalend voor het streefniveau van SecKompas:

Branche:	3 - Industrie
Aantal werknemers:	250-999
Aantal IT-medewerkers:	5 - 9
Omzet:	>100mio
Afhankelijkheid IT:	bovengemiddeld
Privacygevoelige gegevens:	hoog
Vertrouwelijke gegevens:	gemiddeld
R&D-activiteiten:	geen

Het streefniveau voor SecKompas is vastgesteld op **Beheerd.**

Het securityniveau Beheerd heeft een score van 300. De score is opgebouwd uit 163 elementen. SecKompas voldoet aan het streefniveau als er geen aandachts- en verbeterpunten meer zijn met een hoge en medium prioriteit. In dit rapport staan alleen de 5 belangrijkste aandachts- en verbeterpunten. Elementen die al voldoen aan het streefniveau, zijn ook niet in dit rapport opgenomen.

[2] Het Panel bestaat uit 3 IT-security specialisten. Samen goed voor 75 jaar ervaring in IT-security.

3. Het IT Security Kompas

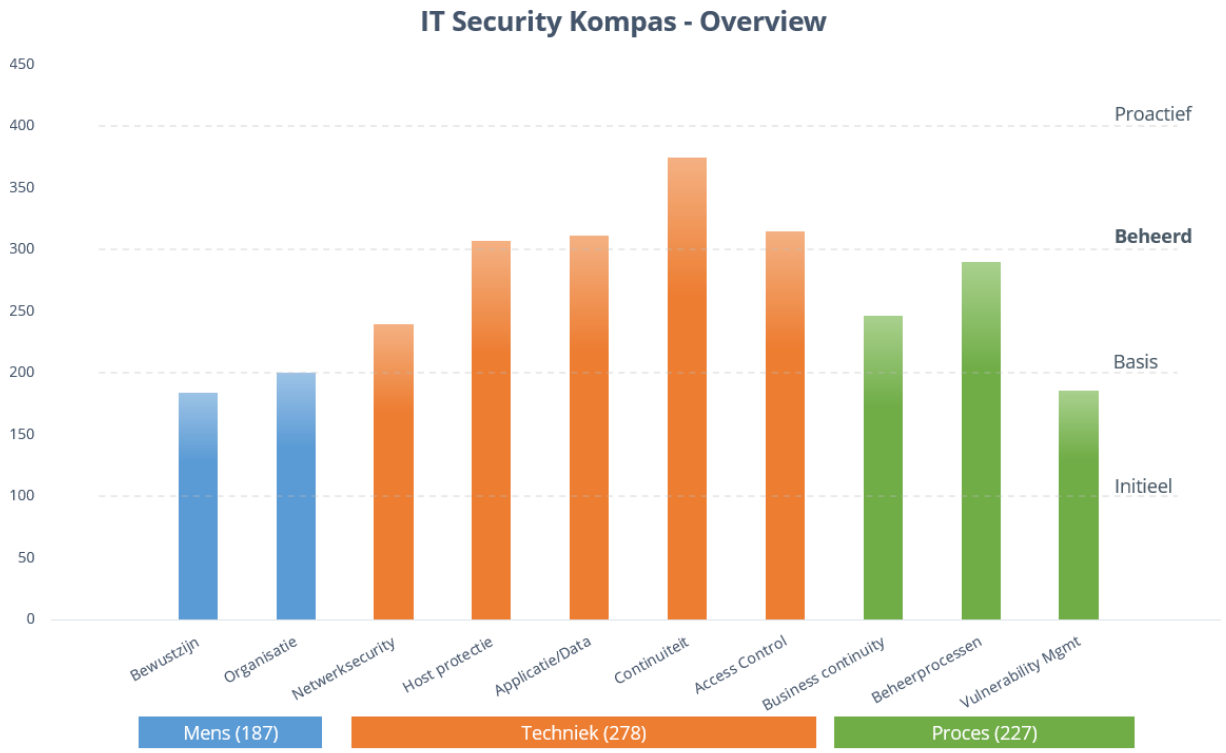
De elementen binnen het securitylandschap zijn verdeeld in 3 domeinen: Mens, Techniek en Proces. Deze domeinen worden onderverdeeld in thema's en de thema's in elementen. Het is belangrijk dat je de zwakste schakel(s) aanpakt en zo je budget optimaal inzet. Hieronder vind je de score, plus de aandachts- en verbeterpunten van de diverse thema's en elementen.

Het securitymodel is zodanig ontwikkeld dat de meeste organisatie binnen dit model passen. Op bepaalde elementen kan de nadruk iets anders liggen of kunnen details invloed hebben op de uitwerking van een element. Het is belangrijk om de verbeterpunten goed te projecteren op de bestaande omgeving van SecKompas en te bespreken met de verantwoordelijke.

Dit rapport is een momentopname, gebaseerd op het IT Security Kompas 2020.1 en de antwoorden die vertegenwoordigers van SecKompas gegeven hebben.

Het veilig ontwikkelen van applicaties is niet meegenomen in het IT Security Kompas. Hiervoor gebruikt men andere kaders en methodieken en zijn daarom niet in het model meegenomen.

3.1. Overview



Het securityniveau van SecKompas is:

- **Securityscore = 234**
- **Aantal verbeterpunten = 29**
  (Hoog=12, Medium=11, Laag=6)

Het securityniveau van SecKompas is **goed,** maar er zijn een aantal noodzakelijk verbeterpunten.

Als je de genoemde verbeterpunten aanpakt, verbeter je de weerbaarheid en krijg je een securityniveau dat past bij SecKompas. De securityscore groeit dan automatische tot boven het ideale niveau van 300.

Positieve bevindingen
SecKompas scoort goed op de volgende thema's:

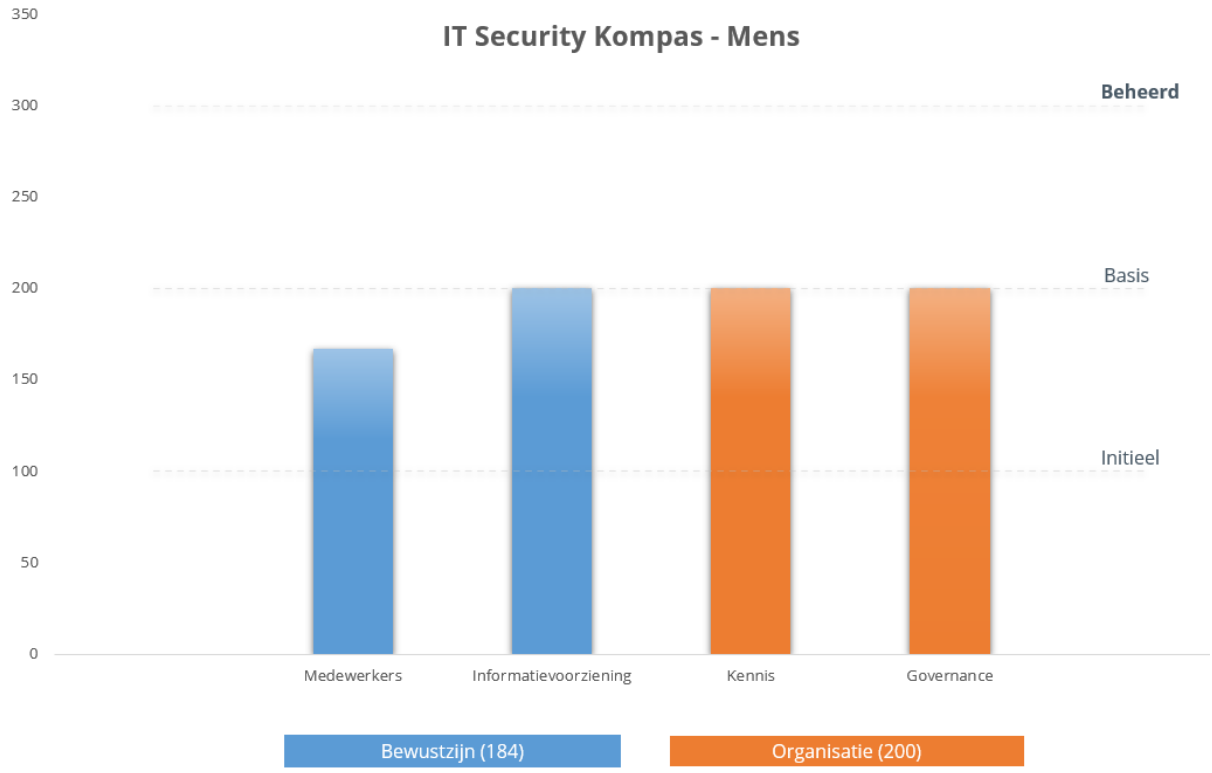
- Back-up
- Mail security
- Hostprotectie
- Monitoring
- Access Control

Aandachts- en verbeterpunten
De volgende thema's hebben zeker extra aandacht nodig:

- Multi-Factor-Authenticatie (MFA) voor cloud-gebruikers
- Firewall/UTM
- Patchmanagement van netwerk devices, randapparaten en IoT/OT devices
- Patchmanagement van applicaties
- Bewustzijn binnen de organisatie

Alleen de 5 belangrijkste aandachts- en verbeterpunten zijn in het start-pakket uitgewerkt. Bij het de pakketten Compleet en Elite worden alle aandachts- en verbeterpunten uitgewerkt om het streefniveau te halen.

3.2. De Mens.



Het securityniveau van het domein Mens is:

- **Securityscore = 187**
- **Aantal verbeterpunten = 3**
  (Hoog=2, Medium=1, Laag=0)

Het menselijke aspect is even belangrijk als ondergewaardeerd. Je kunt diverse technische en procedurele maatregelen treffen om de negatieve impact van het menselijk handelen te beperken. Focus op alleen technische en administratieve maatregelen is te beperkt. Het menselijke aspect is bij SecKompas nog **onvoldoende** meegenomen. Aandacht voor IT-security binnen de gehele organisatie is hierbij het sleutelwoord. Door continue aandacht te besteden aan IT-security wordt de gehele organisatie veilig en informatiebewust.

Bewustzijn

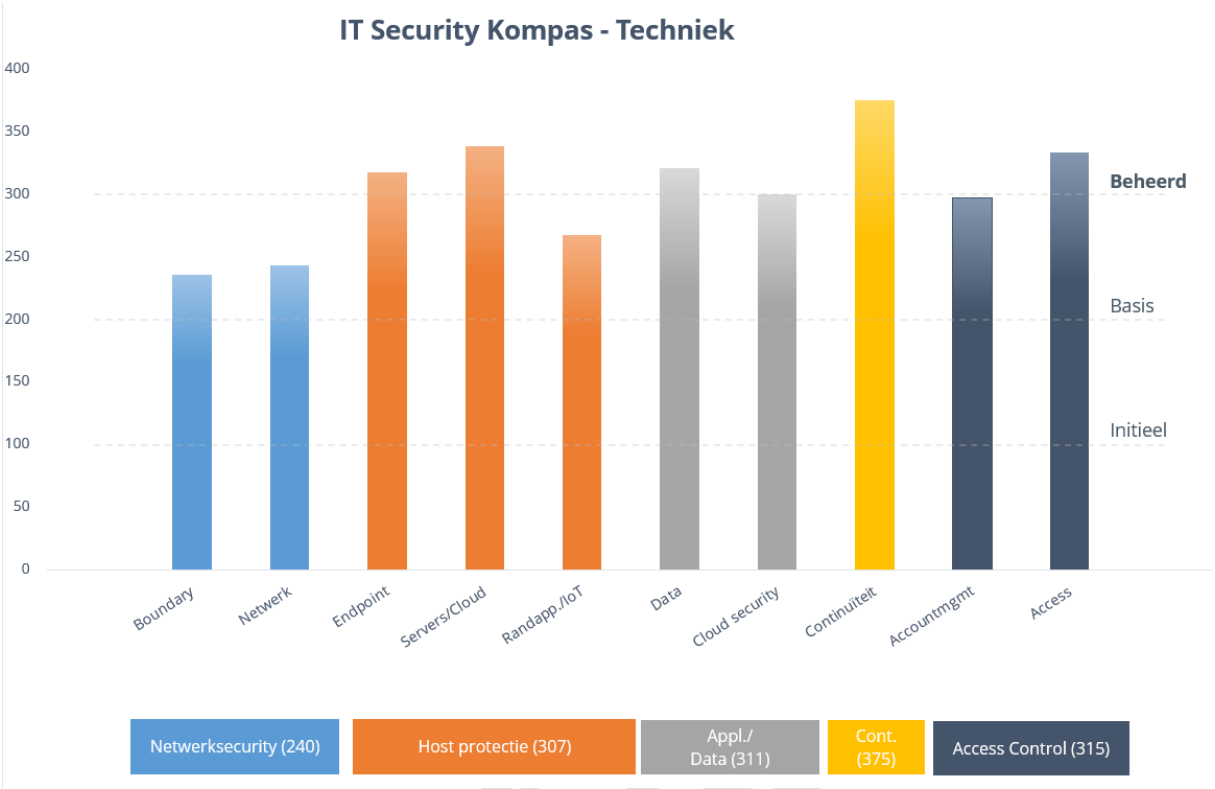
Iedereen binnen de organisatie moet zich bewust zijn van de gevaren die verborgen zijn in het IT-landschap en op Internet in het bijzonder. Bij ongeveer 85% van alle succesvolle inbraakpogingen is de mens een belangrijke factor, bewust of onbewust.

Binnen het thema bewustzijn zijn de volgende elementen onderbelicht.

Verbeterpunt:	Bewustzijn binnen de organisatie
Prioriteit:	**Hoog.**
Belang:	Iedereen binnen de organisatie moet zich bewust zijn van de gevaren op de verschillende gebieden binnen IT-security namelijk cybersecurity, informatiebeveiliging en privacy. Dit bereik je alleen door hier aandacht aan te besteden. Op alle niveaus binnen de organisatie. Technische maatregelen hebben geen zin wanneer een medewerker zijn inloggegevens aan een cybercrimineel geeft of een bankrekeningnummer van een crediteur wijzigt naar het bankrekeningnummer van criminele organisatie.
Aanpak:	Communiceer regelmatig over de gevaren van cybercriminaliteit met het management, binnen de IT-afdeling en organisatie breed. Check eventueel het bewustzijn door bijvoorbeeld een phishing simulatie. Benoem cybercriminaliteit in de verschillende afdelingsoverleggen of in een organisatiebrede bijeenkomst. Bekijk alle procedures vanuit het oogpunt van cybersecurity, Informatiebeveiliging en privacy. Creëer een structurele aanpak door een awareness programma op te stellen. Schakel eventueel een externe partij in om te ondersteunen.
Kostenindicatie:	Laag.

Bij de 5 belangrijkste aandachts- en verbeterpunten staan verder geen punten in het thema Bewustzijn en Organisatie.

3.3. Techniek.



Het securityniveau van het domein Techniek is:

- **Securityscore = 278**
- **Aantal verbeterpunten = 16**
  (Hoog=6, Medium=5, Laag=5)

De techniek waarborgt een eerste, geautomatiseerde bescherming van je gegevens en infrastructuur tegen aanvallen van cybercriminelen. Verder helpt de techniek ook bij bedreigingen die ontstaan door bewust of onbewust foutief handelen van medewerkers.
De inzet van techniek voor de vertrouwelijkheid, integriteit en beschikbaarheid van de data en infrastructuur is **goed**. Enkele (zeer) belangrijke categorieën vereisen verbetering. De te verwachten kosten van de meeste verbeterpunten zijn laag. Voor sommige verbeterpunten kunnen de investeringen aanzienlijk zijn. Dit is sterk afhankelijk van de bestaande infrastructuur.

Netwerksecurity

Betere afscherming van interne systemen én beperking van interne verspreiding van malware (zoals ransomware) vraagt om aanscherping van de volgende technische maatregelen.

Verbeterpunt:	Firewall/UTM.
Prioriteit:	**Hoog.**
Belang:	Het is zeer belangrijk om het netwerkverkeer tussen interne netwerk, de DMZ én het Internet van elkaar te scheiden en het netwerkverkeer tussen deze netwerken goed te controleren. Koppel ook andere belangrijke netwerken zoals het server-VLAN of het IoT-VLAN aan de firewall of nog beter, een aparte interne FW.

	Cybercriminelen liften graag mee op bestaande verbindingen van en naar interne devices. Daarom is het essentieel om de inhoud van het netwerkverkeer te inspecteren. Het verkeer moet inhoudelijk gecontroleerd worden op bekende en onbekende bedreigingen zoals malware, ransomware en andere geavanceerde aanvallen. Hiervoor zijn minimaal advanced malware inspection en advanced threat prevention nodig. Inspecteer ook het SSL-verkeer. Meer dan 75% van het internetverkeer is tegenwoordig versleuteld, dikwijls met SSL. Op de firewall is zichtbaarheid nog wel belangrijker dan op andere systemen. Zorg daarom dat je altijd kunt inzicht hebt in de events en in het geblokkeerde en doorgelaten sessies.
Aanpak:	Zorg voor een goede scheiding tussen het internet, de DMZ én het interne netwerk d.m.v. een goede firewall. Bescherm ook belangrijke interne netwerken aan een firewall. Zet minimaal advanced malware inspection en advanced threat Prevention aan. Inspecteer ook het encrypted verkeer door SSL-interception. Log alle belangrijke gebeurtenissen én detailinformatie over geaccepteerde en geblokkeerde sessies op een centrale locatie.
Kostenindicatie:	Hoog: De kosten zijn sterk afhankelijk van de uitbreidingsmogelijkheden van de FW, UTM of de managed firewall dienst. Eventueel moet de FW/UTM vervangen worden.

Goed beschermd: voor mailverkeer zijn de juiste securitymaatregelen getroffen.

Bij de 5 belangrijkste aandachts- en verbeterpunten staan verder geen punten in het thema netwerkprotectie.

Hostprotectie

De mobiliteit van de medewerkers neemt toe. Daarom wordt host protectie op laptops en mobile devices (telefoons en tablets) steeds belangrijker. Deze trend zien we al langer, maar heeft door de coronacrisis een extra boost gekregen. De afscherming verplaatst zich daardoor steeds meer van de buitenkant van het netwerk, het endpoint. De bescherming van servers blijft onverminderd belangrijk.

We zien ook dat steeds meer aanvallen gericht zijn op randapparaten, IoT (Internet of Things) en OT (Operational Technology, aansturing van industriële apparatuur). Door de beperkte capaciteit en upgrade-mogelijkheden vormen die devices een gemakkelijke prooi voor hackers. Deze aanvalsmethode groeit sterk. De aanwezigheid van IoT-devices is niet altijd bekend bij de IT-afdeling, met alle gevaren van dien.
Bij de 5 belangrijkste aandachts- en verbeterpunten staan geen punten in het thema hostprotectie.

Applicatie- en Datasecurity

Incidenten zijn nooit helemaal te voorkomen. Incidenten ontstaan door securitybedreigingen, maar ook door menselijk en technisch falen. Er ontstaat direct een gevaar voor een verminderde beschikbaarheid van data en systemen en dus een gevaar voor de continuïteit van SecKompas.
Bij de 5 belangrijkste aandachts- en verbeterpunten staan geen punten in het thema Applicatie- en datasecurity.

Continuïteit

De maatregelen binnen het thema continuïteit zijn erop gericht om de beschikbaarheid te optimaliseren. Hiervoor zijn een aantal elementen belangrijk namelijk het zo snel mogelijk ontdekken van een storing, het minimaliseren van het aantal storingen, een goede, adequate analyse van een incident en het zo snel mogelijk herstellen van de productieomgeving.

Er zijn een aantal aandachts- en verbeterpunten. Die worden in dit rapport niet uitgewerkt. Bij het pakket Compleet en Elite zijn deze punten wel volledig uitgewerkt.

Access control.

De identiteit (authenticatie) en rechten (autorisatie) van gebruikers is een zeer belangrijk thema. Dat bepaalt tot welke systemen en data een gebruiker toegang krijgt. Personen die niet gerechtigd of getraind zijn om systemen of data te benaderen, brengen de vertrouwelijkheid, integriteit én beschikbaarheid van systemen en data in gevaar. Daarom is belangrijk om het gebruik van accounts goed te controleren.

Toegang tot de cloud.
In de cloud speelt access control een nog belangrijkere rol. Inlogpogingen blijven niet beperkt tot het interne netwerk. De gehele internetgemeenschap kan met op het internet verkrijgbare tools proberen toegang te krijgen tot jouw cloud-omgeving. Dit geldt voor zowel SaaS-, PaaS- als IaaS-omgevingen. Multi-factor authenticatie (MFA) zorgt voor een extra authenticatieslag met “iets wat je hebt”, een token. Een belangrijke uitbreiding op “iets wat je weet”, namelijk gebruikersnaam en wachtwoord. MFA beschermt niet alleen tegen diefstal van wachtwoorden maar ook tegen brute-force-attacks of social engineering.

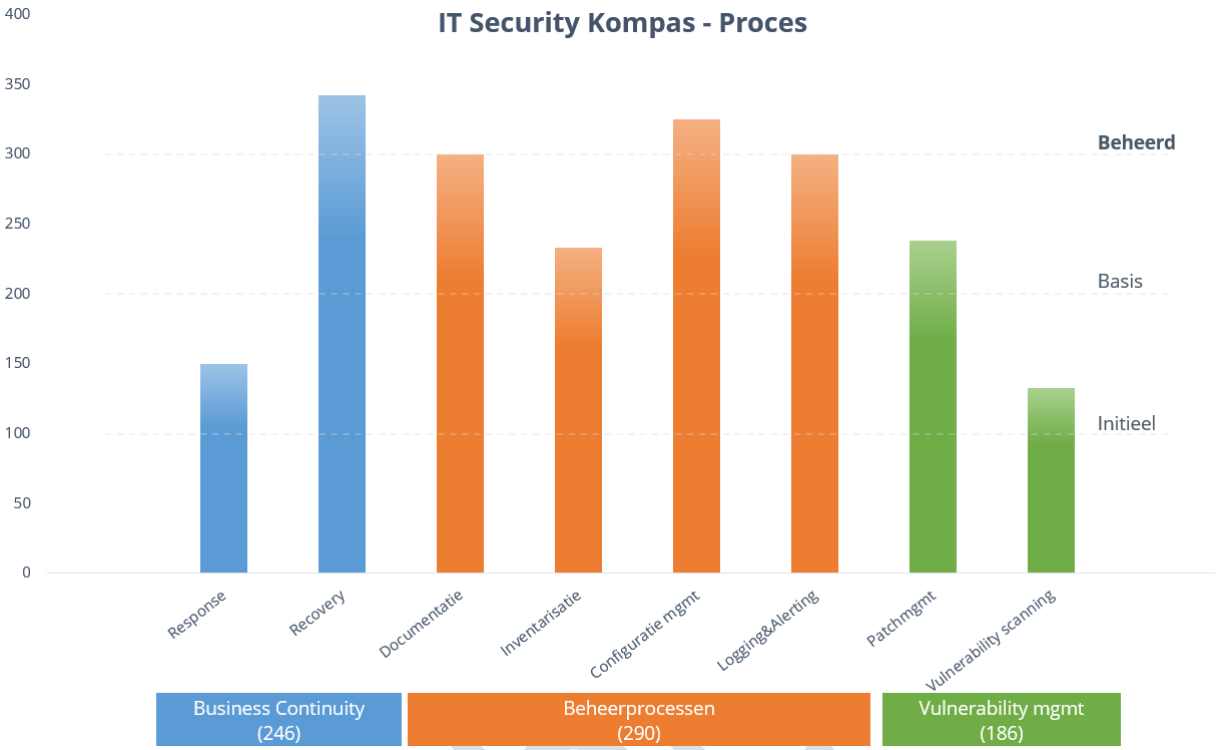
Aandachts- en verbeterpunten:

Verbeterpunt:	Multi-factor authenticatie (MFA) voor cloud-gebruikers.
Prioriteit:	**Hoog.**
Belang:	De gehele internetgemeenschap kan proberen om toegang te krijgen tot jouw account (hacken). Een wachtwoord alleen is niet voldoende. MFA beschermt niet alleen tegen diefstal van wachtwoorden maar ook tegen brute-force-attacks of social engineering.
Aanpak:	Onderzoek welke MFA-methode past bij de infrastructuur van SecKompas. Kijk ook naar de authenticatie mogelijkheden van andere omgevingen zoals bijvoorbeeld interne AD, remote access of andere cloud providers. Implementeer vervolgens MFA voor alle gebruikers.
Kostenindicatie:	Laag.

	De meeste cloud providers zien het belang van MFA in en stellen MFA gratis of tegen lage kosten ter beschikking.

Bij de 5 belangrijkste aandachts- en verbeterpunten staan geen punten in het thema Access Control.

3.4. Processen.



Het securityniveau van het domein Proces is:

- **Securityscore = 227**
- **Aantal verbeterpunten = 10**
  (Hoog=4, Medium=5, Laag=1)

Goed ingerichte processen waarborgen structuur en duidelijkheid. Bovendien zorgen ze voor standaardisatie en een hogere betrouwbaarheid. Processen worden beter wanneer je ze regelmatig evalueert. Niet alleen repeterende activiteiten moeten beschreven zijn. Ook moet beschreven zijn wat men moet doen bij calamiteiten en wie men hierbij moet betrekken. Daarmee minimaliseer je de impact van een calamiteit.
Het securityniveau van het domein Proces is **redelijk** maar een aantal processen moeten dringend verbeterd worden.

Business Continuïteit

IT-security is belangrijk om de continuïteit van jouw organisatie te waarborgen. Helaas zijn nooit alle mogelijke incidenten te voorkomen. Het is dus niet de vraag of jouw organisatie het slachtoffer wordt van een security incident maar wanneer. Bij dit thema ligt de focus op maatregelen om incidenten proactief en snel op te lossen en de impact tot een minimum te beperken. Denk hierbij aan omzetderving en imagoschade.

Bij de 5 belangrijkste aandachts- en verbeterpunten staan geen punten in het thema Business Continuiteit.

Beheerprocessen

Processen helpen mensen om hun werkzaamheden efficiënt en adequaat uit te voeren. En biedt volop mogelijkheden om te automatiseren.

Bij de 5 belangrijkste aandachts- en verbeterpunten staan geen punten in het thema beheerprocessen.

Vulnerability management

Bij de meeste succesvolle cyberaanvallen maken cybercriminelen misbruik van kwetsbaarheden waarvoor al een update beschikbaar is. Vulnerability management bestaat uit het checken op en dichten van kwetsbaarheden. Beide processen moeten voor alle type devices goed ingeregeld worden. Dus ook voor devices die op het eerste gezicht minder vatbaar zijn voor securityincidenten zoals printers of camera's.

Een goed patchmanagementproces is cruciaal om alle securitypatches, updates of upgrades binnen een acceptabel tijdsbestek te installeren. De frequentie waarop security updates beschikbaar komen, is sterk afhankelijk van het type device.

Verbeterpunt:	Patchen van netwerk devices, randapparaten en IoT/OT devices.
Prioriteit:	**Hoog.**
Belang:	Cybercriminelen hebben het steeds vaker gemunt op devices waarvoor weinig securityupdates beschikbaar komen of devices die moeilijker te upgraden zijn. Deze devices zijn om verschillende redenen interessant voor cybercriminelen. Check daarom regelmatig of er security gerelateerde updates, upgrades of patches beschikbaar zijn. In dat geval moeten de devices binnen een vooraf bepaalde tijd gepatcht worden.
Aanpak:	Hou regelmatig bij of er upgrades, updates of patches beschikbaar zijn. Wacht niet te lang met het installeren van nieuwe firmware of OS. Tip: Deze devices worden ook gebruikt als springplank naar andere belangrijke devices. Zet ze daarom in verschillende VLANs. Bijvoorbeeld door gebruik te maken van een NAC-oplossing. Zet deze VLANs vervolgens achter een firewall zodat ze beter afgeschermd zijn en patchen minder cruciaal wordt.
Kostenindicatie:	Laag.

Verbeterpunt:	Patchen van applicaties.
Prioriteit:	**Hoog.**
Belang:	Cybercriminelen kijken niet naar de belangrijkheid van een applicatie. Het is meestal maar een startpunt. In de veel gevallen zijn kleine, op het oog minder belangrijke applicaties een gemakkelijk doelwit. Denk hierbij bijvoorbeeld aan PDF-readers, browsers, Java runtime of scansoftware. Die worden minder gepatcht dan wereldwijd gebruikte of bedrijfskritische applicaties.
Aanpak:	Hou regelmatig bij of er upgrades, updates of patches beschikbaar zijn. Bijvoorbeeld door informatie uit softwarecontracten of nieuwsbrieven.

	Wacht niet te lang met het installeren van nieuwe software.
Kostenindicatie:	Laag.

Bij de 5 belangrijkste aandachts- en verbeterpunten staan verder geen punten in het thema Patchmanagement.

Vulnerability scanning zorgt voor een overzicht van alle kwetsbaarheden in het netwerk en ondersteunt het patchmanagement. Niet geïnstalleerde updates of configuratiefouten worden zichtbaar. Verder controleert de vulnerability scanner welke systemen zich op het netwerk bevinden en detecteert eventuele onbekende apparaten.

Bij de 5 belangrijkste aandachts- en verbeterpunten staan geen punten in het thema Vulnerability.

4. Opvolging

Het IT Security Kompas geeft je het inzicht en de handvatten om je securityniveau op een verantwoorde en onderbouwde manier te verhogen. Misschien bevatten de verbeterpunten een aantal 'open deuren'. Ook die moet je vergrendelen. Het kost niet altijd veel tijd en geld om de aandachts- en verbeterpunten aan te pakken. Misschien lijkt het aantal verbeterpunten groot. Vergeet niet dat we de vragen projecteren op meer dan 160 elementen. Je hoeft ook niet alle punten direct aan te pakken. Veel belangrijker is het dat je bewust bent van de gevaren. Vanuit dit bewustzijn selecteer je de belangrijkste aandachts- en verbeterpunten en maak je een onderbouwd verbeterplan.

Hoe kun je dit aanpakken? De volgende stappen helpen je om je cyberweerbaarheid te verhogen.

1. Bespreek dit rapport met de operationeel betrokken medewerkers en/of IT-partner. Sommige verbeterpunten worden misschien al aangepakt, staan op de planning of zijn voor SecKompas niet relevant.
2. Maak een verbeterplan dat SMART[3] is. Zorg dat je de verbeteringen goed afstemt op jouw situatie. Houd hierbij rekening met het beschikbare budget. Registreer en onderbouw waarom je sommige aandachts- en verbeterpunten nog niet aanpakt en wat de risico's zijn. Neem deze argumenten mee in toekomstige voortgangs- en/of evaluatiegesprekken.
3. Bespreek het actieplan en/of het rapport inclusief alle opmerkingen met het management en betrek de leden in de reis naar een veilige en flexibele organisatie.
4. Evalueer periodiek de voortgang. Doorloop eventueel het IT Security Kompas om de voortgang zichtbaar te maken en nieuwe ontwikkelingen op het gebied van cybercriminaliteit mee te nemen. Bespreek de analyse met de betrokkenen en pas eventueel het verbeterplan aan. Vergeet niet het management hierbij te betrekken.

Heb je al een verbeterproces zoals PDCA (Plan-Do-Check-Act)? Neem IT-security hierin mee want het verbeteren van je veiligheidsniveau is een continu proces.

De consultants van IT Security Kompas ondersteunen je graag en zijn volledig product en leveranciers onafhankelijk. Heb je vragen, wil je ondersteuning bij het maken van het verbeterplan of wil je weten hoe een specifiek verbeterpunt aanpakt? Neem dan contact op met IT Security Kompas (info@itsecuritykompas.nl). Wij helpen SecKompas graag met het beschermen van jullie kroonjuwelen.
Op de website vind je een overzicht van alle diensten van IT Security Kompas.

Als we onze krachten bundelen en gebruikmaken van elkaars ervaringen en expertise maken we de BV Nederland maar vooral jouw organisatie veiliger.

[3] SMART = Specifiek – Meetbaar – Acceptabel – Realistisch - Tijdgebonden.

5. Prioriteitenlijst

Domein	Thema	Prio	kosten	Omschrijving
Techniek	Access control	Hoog	Laag	Multi-Factor-Authentication (MFA) voor cloud-gebruikers.
Techniek	Netwerksecurity	Hoog	Hoog	Firewall/UTM
Proces	Vulnerability mgmt	Hoog	Laag	Patchmanagement netwerkdevices, randapparaten en IoT/OT devices.
Proces	Vulnerability mgmt	Hoog	Laag	Patchmanagement van applicaties.
Mens	Bewustzijn	Hoog	Laag	Bewustzijn binnen de organisatie.

Bijlage 1: Securityprofielen

De noodzaak en het niveau waarop organisaties hun IT-security inrichten, verschilt per organisatie. Uiteraard zijn er ook overeenkomsten. Bij IT Security Kompas maken we een onderverdeling in 5 IT-security niveaus voor organisaties. Deze 5 niveaus lopen uiteen: van een niveau zonder specifieke securitymaatregelen tot een niveau waar de organisatie zich volledig bewust is van de security risico's. Welk niveaus bij jouw bedrijf past is afhankelijk van de privacy gevoeligheid, de noodzakelijke beschikbaarheid, de vertrouwelijkheid van gegevens en de mate waarin IT binnen de organisatie verweven is. Ook de eventuele maatschappelijke missie van de organisatie speelt soms een belangrijke rol. Tenslotte focussen we ons op de motivatie van cybercriminelen: geld, wraak, politieke of religieuze redenen en fun (in mindere mate).

Het niveau is een streefniveau, een niveau waar je naar toe werkt. De mogelijkheden binnen jouw organisatie en het beschikbaar gestelde budget bepalen de termijn waarbinnen het niveau bereikt wordt. Je maakt grote stappen door juiste verbeterpunten als eerste aan te pakken.

Hieronder volgt een grove beschrijving van de 5 niveaus: van een lage naar een hoge securityscore.

Initieel (securityscore 100):
Organisaties met een initieel niveau hebben geen of heel weinig aandacht voor IT-security. IT als geheel wordt ad hoc en soms chaotisch opgepakt. De organisatie heeft niet de kennis en mogelijkheden om IT structureel aan te pakken, laat staan IT-security. IT-security is volledig afhankelijk van de maatregelen die de leverancier of IT-partner standaard meelevert.

Organisaties met dit niveau hebben een zeer beperkte bescherming tegen bedreigingen van buitenaf**. Dit niveau is alleen geschikt voor zeer kleine organisaties en ZZP'ers die voor hun bedrijfsvoering niet afhankelijk zijn van IT.** Voor cybercriminelen zijn deze organisaties geen specifiek doel, maar wel een gemakkelijke prooi.

Basis (securityscore 200):
Organisaties met het niveau 'Basis' hebben geen vastgesteld beleid voor informatiebeveiliging en IT-security. De organisatie is minimaal betrokken bij de veiligheid. Prioriteiten van de IT-afdeling bepalen grotendeels de security-aanpak. Binnen de infrastructuur is beperkte aandacht besteed aan IT-security. Bovendien is er te weinig zichtbaarheid en bewustzijn om hier proactief aan te kunnen werken. De aanpak van IT-security is meer vrijblijvend en vaak een reactie op concrete security incidenten. De getroffen veiligheidsmaatregelen beschermen alleen tegen bekende aanvalstechnieken van cybercriminelen met beperkte kennis. Het is niet mogelijk om zo de veiligheid van de infrastructuur en data te waarborgen. Cruciale bedrijfsprocessen komen hierdoor in gevaar.

Het basisniveau is het minimale niveau voor bescherming tegen de meest gebruikte en bekende bedreigingen. **Deze aanpak is geschikt voor bedrijven met weinig tot geen bedrijfskritische processen en privacygevoelige of vertrouwelijke gegevens.** Cybercriminelen richten zich niet specifiek op deze organisaties. Er is wel sprake van een serieus risico.

Beheerd (securityscore 300):
Organisaties met het niveau 'Beheerd' hebben een korte-termijnbeleid voor informatiebeveiliging en IT-security. Dit beleid komt in samenspraak tussen het hoger management en het IT-

management tot stand. De IT-afdeling is zich bewust van de risico's en communiceert hierover met de directie en medewerkers van de organisatie. IT-security kent een actieve aanpak in zowel projecten als beheer. De IT-afdeling kent de getroffen maatregelen en houdt regelmatig de documentatie bij. Denk aan maatregelen die de organisatie beschermen tegen bekende en onbekende bedreigingen. Die hoeven niet specifiek op de organisatie gericht te zijn. Ook houdt de IT-afdeling systemen en applicaties up-to-date. Binnen de organisatie is de logging centraal geregeld, waardoor de gebeurtenissen in de infrastructuur zichtbaar zijn. In het geval van een security incident onderzoekt het IT-management de oorzaak en treft maatregelen.

Organisaties met dit securityniveau hebben een goede bescherming tegen de meeste bedreigingen die niet specifiek op de organisatie gericht zijn. Als informatie en systemen niet beschikbaar zijn, leidt dit niet binnen enkele dagen tot een faillissement. **Organisaties die binnen dit niveau passen hebben bedrijfskritische processen en privacygevoelige of vertrouwelijke gegevens, maar zijn geen specifiek doelwit.** Ze kunnen zich tot op zekere hoogte verweren tegen bekende en onbekende bedreigingen.

Proactief (securityscore 400):
Bij organisaties met een proactief niveau zijn de directie, het hoger management en de IT-afdeling zich sterk bewust van de bedreigingen binnen het IT-landschap. De organisatie heeft een duidelijk beleid voor de korte en lange termijn opgesteld. Voor de komende 2 jaar is er minimaal een roadmap beschikbaar. De gestructureerde aanpak van het IT-beheer is reproduceerbaar en schaalbaar. Binnen de organisatie (of ingehuurd) is veel kennis over IT-security beschikbaar. Er bestaat dus een goed inzicht is in alles wat er binnen de infrastructuur en applicaties gebeurt. De logging wordt centraal opgeslagen. Bij incidenten geven de belangrijkste systemen een signaal. De organisatie is niet alleen beschermd tegen bekende en onbekende bedreigingen. Zij is ook voorbereid op mogelijke aanvallen die specifiek op haar gericht zijn.

Het proactieve niveau geeft een goede bescherming waarbij er ook maatregelen getroffen zijn om gerichte aanvallen af te slaan. **Binnen de organisatie is er bedrijfskritische informatie die een hoge beschikbaarheid van IT-security vragen of het imago van de organisatie gemakkelijk kunnen aantasten.** Organisaties die binnen dit niveau passen, vormen een mogelijk doelwit. Ze zijn goed voorbereid op cybercriminaliteit.

Adaptief (securityscore 500):
Organisaties met het niveau 'Adaptief' zijn zich volledig bewust van de bedreigingen en risico's voor de informatie en IT binnen de organisatie. Ze hebben een duidelijk langetermijnbeleid en de informatieveiligheid speelt bij alle bedrijfsprocessen een cruciale rol. Zo staat er een duidelijk bedrijfscontinuïteitsplan op papier. Dit plan bevat informatie over de belangrijke bedrijfsprocessen, de infrastructuur en de data. De IT-security is voor zover mogelijk geautomatiseerd en wordt continu geëvalueerd en verbeterd. IT-medewerkers monitoren continu het interne verkeer binnen de organisatie en melden eventuele afwijkingen direct aan de securityspecialisten. De organisatie is beschermd tegen bekende en onbekende bedreigingen. Monitoring tooling merkt cyberaanvallen op die de security infrastructuur over het hoofd ziet.

Dit niveau van IT-security is gewenst voor organisaties die een specifiek doelwit zijn en waar de beschikbaarheid van data en processen extreem belangrijk is. Organisaties binnen dit niveau vormen een doelwit, maar zijn geen gemakkelijke prooi. Specialisten monitoren, evalueren en verbeteren immers continu de IT-security.

Disclaimer

Het model achter het IT Security Kompas en de bijbehorende adviezen is met veel zorg opgebouwd en uitgewerkt. De diepgaande kennis en de brede ervaring van de leden van het securitypanel liggen ten grondslag aan dit model en aan de adviezen. Het securitypanel beoordeelt regelmatig opnieuw (minimaal elk kwartaal) het IT Security Kompas. Het kompas is niet ontwikkeld voor een specifieke organisatie, maar juist breed toepasbaar. Met deze informatie in het achterhoofd moet je het rapport lezen. Adviezen hebben in meer of mindere mate betrekking op jouw organisatie. Het IT Security Kompas is niet verantwoordelijk voor de uiteindelijke opvolging en uitvoering van de adviezen. Het is belangrijk om dit rapport en de eventuele acties te bespreken met de uitvoerende afdelingen en personen. De kostenindicatie is afhankelijk van de al aanwezige informatie, infrastructuur en processen.