

|  |
| --- |
| **Cyberverzekering –vragenformulier Ransomware** |

Dit (aanvullende) vragenformulier is van toepassing op de AIG Cyberverzekering. Waar in dit formulier **Verzekeringnemer** wordt gebruikt omvat dit de gehele organisatie die de dekking aanvraagt en alle dochterondernemingen. Wanneer het formulier gebruikt wordt voor het aanvragen van een nieuwe verzekering dient **Verzekeringnemer** als kandidaat-verzekeringnemer (incl. alle dochterondernemingen) gelezen te worden.

|  |  |
| --- | --- |
| **Verzekeringnemer** (holding niveau) |  |
| Omzet |  |
| Website |  |

***Invulinstructie:***

*De antwoordkolom staat alleen een antwoord toe met "ja", tenzij in de vraag specifiek om een "invulling" of een specifiek getal wordt gevraagd. Wanneer* ***Verzekeringnemer*** *het antwoord blanco laat, wordt dit geïnterpreteerd als "nee" of "niet ingericht", tenzij er een antwoord is die specifiek "nee", "onbekend", of "geen van bovenstaande" inhoudt. Na iedere sectie zijn er toelichtingsmogelijkheden waarin de* ***Verzekeringnemer*** *desgewenst aanvullende toelichting kan geven. (Aanvullende toelichtingen zijn beperkt tot 1000 tekens; indien meer ruimte nodig is, gelieve dan een afzonderlijk document als bijlage toe te voegen)*

*De onderstaande vragen zijn van belang voor de acceptatie van de dekking voor* ***Verzekeringnemer****. Deze dient te worden ingevuld door, of met de hulp van, de perso(o)n(en) die verantwoordelijk is (zijn) voor de beveiliging van de informatiesystemen van* ***Verzekeringnemer****. Indien informatiebeveiliging is uitbesteed aan een derde partij (bijv. een managed security provider), wordt ervan uitgegaan dat* ***Verzekeringnemer*** *zijn antwoorden heeft geverifieerd bij deze derde partij voordat dit formulier is ingediend.*

|  |
| --- |
| **Data beveiliging & bedrijfscontinuiteit** |

|  |  |  |
| --- | --- | --- |
|  | Vraag | Antwoord |
| DS/BC #1 | *Selecteer één antwoord:* Hoe gecentraliseerd is het IT-beveiligingsprogramma van **Verzekeringnemer**? |  |
| IT-beveiliging wordt centraal beheerd en het beleid geldt voor alle activiteiten. Uitzonderingen worden uitsluitend per systeem gemaakt (in tegenstelling tot per activiteit/juridische entiteit). |  |
| IT-beveiliging wordt centraal beheerd, maar er worden uitzonderingen gemaakt voor bepaalde operationele/juridische entiteiten. De controls zijn van toepassing op meer dan of gelijk aan 98% van alle werkstations (o.a. desktops/laptops). |  |
| IT-beveiliging wordt centraal beheerd maar er worden uitzonderingen gemaakt voor bepaalde operationele/juridische entiteiten. De controls zijn van toepassing op minder dan 98% van alle werkstations (o.a. desktops/laptops). |  |
| IT-beveiliging is decentraal, maar de controls zijn van toepassing op meer dan of gelijk aan 98% van alle werkstations (o.a. desktops/laptops). |  |
| IT-beveiliging is decentraal, maar de controls zijn van toepassing op meer dan 50% maar minder dan 98% van alle werkstations (o.a. desktops/laptops). |  |
| IT-beveiliging wordt beheerd door afzonderlijke juridische entiteiten of operationele eenheden. De controls zijn gebaseerd op een onderzoek bij alle entiteiten en operationele eenheden. |  |
| Anders (beschrijf in de opmerkingen aan het einde van dit onderdeel ‘Data Security & Business Continuity’. |  |
| Onbekend. |  |
| DS/BC # 2 | *Selecteer alles wat van toepassing is:* Met betrekking tot het beheer van **Verzekeringnemer** van de systemen (hardware en software) geldt het volgende: |  |
| Er is een inventarisatie van alle hardware systemen - inclusief end-user devices, (netwerk), apparaten, IoT-apparaten en servers - met vermelding van het netwerkadres (indien statisch), het MAC adres en het merk&type van machine met de gegevens van de eindgebruiker. Deze lijst wordt tweejaarlijks geactualiseerd. |  |
| Er is een inventarisatie van alle hardware systemen – inclusief end-user devices, (netwerk)apparaten, IoT-apparaten en servers - met vermelding van het netwerkadres (indien statisch), het MAC adres en het merk&type van machine met de gegevens van de eindgebruiker. Deze lijst wordt jaarlijks geactualiseerd. |  |
| Er is een proces om dagelijks hardware systemen die aangesloten zijn op het netwerk te traceren en identificeren. |  |
| Er is een proces om wekelijks de hardware systemen die aangesloten zijn op het netwerk te traceren en identificeren. |  |
| Er is een proces om inventarisatie van alle hardware systemen wekelijks bij te werken op basis van discovery tools of IP Address Management (IPAM)-software. |  |
| Er is een lijst van alle licensed software die geïnstalleerd is op systemen, en deze wordt ten minste twee keer per jaar bijgewerkt. |  |
| Er is een proces om ervoor te zorgen dat alle software ofwel wordt ondersteund ofwel dat er een gedocumenteerde uitzondering daarop bestaat met schadebeperkende maatregelen. |  |
| Geen van bovenstaande/onbekend. |  |
| DS/BC # 3 | *Selecteer alles wat van toepassing is:* Met betrekking tot het beheer van **Verzekeringnemer** van kritieke systemen geldt het volgende:  *"kritieke systemen" zijn systemen die essentieel zijn voor het succes en de operatie, met inbegrip van, maar niet beperkt tot, toepassingen die de productie ondersteunen, toepassingen die bedrijfskritieke en/of gevoelige data opslaan, en core technologiediensten zoals directory services, documentbeheer en e-mail.* |  |
| Er is een lijst van alle data opslagplaatsen - met vermelding van de data owner, het systeem waarop de data is opgeslagen, de gevoeligheid, de bewaartermijnen en de vereisten voor verwijdering - voor ten minste alle gevoelige data, en dit wordt ten minste jaarlijks bijgewerkt. |  |
| Alle "kritieke systemen" zijn gedefinieerd en gedocumenteerd. |  |
| Er is een proces om actief "kritieke systemen" te identificeren en de lijst van "kritieke systemen" ten minste elk kwartaal bij te werken. |  |
| "Kritieke systemen" zijn gerangschikt naar belangrijkheid voor de bedrijfsvoering. |  |
| Geen van bovenstaande/onbekend. |  |
| DS/BC # 4 | Wat is de "Recovery Time Objective" (RTO) voor "kritieke systemen"? "RTO" is de hoeveelheid tijd waarin "kritieke systemen" naar verwachting door een organisatie kunnen worden hersteld na een incident/onderbreking. |  |
| < 5 uur |  |
| 5-12 uur |  |
| 12-24 uur |  |
| 1-7 dagen |  |
| > 7 dagen |  |
| RTO Is onbekend |  |
| DS/BC # 5 | *Selecteer alles wat van toepassing is:* Met betrekking tot de disaster recovery mogelijkheden van **Verzekeringnemer** geldt het volgende: |  |
| Er bestaat een proces voor het maken van back-ups (ook al is het niet gedocumenteerd en/of ad hoc). |  |
| Er is eengedocumenteerd disaster recovery beleid en deze maakt gebruik van wekelijks - of vaker - geautomatiseerde back-ups en standaarden op basis van de risicoclassificatie van de data. |  |
| Minstens elk kwartaal is er een restore test om verschillende kritieke systemen en data tijdig te herstellen in lijn met de Recovery Time Objective (RTO). |  |
| Geen van bovenstaande/onbekend. |  |
| DS/BC # 6 | *Selecteer alles wat van toepassing is:* Ten aanzien van de back-up mogelijkheden van **Verzekeringnemer** geldt het volgende: |  |
| De back-upstrategie bevat offline back-ups die onsite worden opgeslagen. |  |
| De back-upstrategie bevat offline back-ups die offsite zijn opgeslagen. |  |
| De back-upstrategie bevat regelmatige onsite back-ups. |  |
| De back-upstrategie bevat regelmatige offsite back-ups (Cloud, Continuity of Operations Site). |  |
| Deback-ups zijn geïsoleerd en gescheiden van het productiedomein (toegankelijk via een verificatiemechanisme buiten Active Directory om of zijn anderszins beschikbaar, zelfs als het productiedomein is gecompromitteerd) of ze zijn immutable/ onveranderlijk. |  |
| Geen van bovenstaande/onbekend. |  |
| DS/BC # 7 | *Selecteer alles wat van toepassing is:* Met betrekking tot het beleid van **Verzekeringnemer** om encryptie toe te passen om data te beschermen geldt het volgende: |  |
| Alle data op draagbare apparaten - met inbegrip van telefoons, tablets en laptops - is versleuteld (met volledige schijfversleuteling of versleuteling per bestand). |  |
| Alle werkstations (o.a. desktops/laptops) die gevoelige data bevatten, hebben volledige schijfversleuteling. |  |
| Alle verwijderbare media - USB-sticks, CD's, enz. - zijn versleuteld. |  |
| Alle gevoelige data ‘at rest’ is versleuteld (op de storage layer of de applicatie layer). |  |
| Geen van bovenstaande/onbekend. |  |
| DS/BC # 8 | *Selecteer alles wat van toepassing is:* Met betrekking tot het monitoren van **Verzekeringnemer** van de "kritieke systemen" geldt het volgende: |  |
| Er is een "Security Operations Center" (SOC) in de vorm van interne service en/of een externe Managed Security Service Provider ("MSSP") voor het monitoren van security event alerts, inclusief alerts over "kritieke systemen". |  |
| HetSOC en/of de MSSPkrijgtten minste elk kwartaal een bijgewerkte lijst van "kritieke systemen". |  |
| HetSOC en/of de MSSPmaakt gebruik van een SIEM-oplossing (Security Information and Event Monitoring) om de logs van "kritieke systemen" te automatiseren. |  |
| Geen van bovenstaande/onbekend. |  |

|  |  |  |
| --- | --- | --- |
|  | Aanvullende toelichting op deze sectie: |  |
|  |  |

|  |
| --- |
| **Identity, Credential, and Access Management (ICAM)** |

|  |  |  |
| --- | --- | --- |
|  | Vraag | Antwoord |
| ICA # 1 | *Selecteer alles wat van toepassing is:* Welke van de volgende programma's gebruikt **Verzekeringnemer** voor directory services, identity providers (IdP), federation en/of rechten beheer? |  |
| Microsoft Active Directory (Active Directory) |  |
| Azure Active Directory (Azure AD) |  |
| Okta |  |
| Ping |  |
| Active Directory Federation Services |  |
| Google Workspaces |  |
| Anders (details gewenst - vermeld ze onderstaand) |  |
| *Indien andere, vermeld hier met een toelichting* |  |
| Geen van bovenstaande/ onbekend. |  |
| ICA # 2 | *Selecteer één antwoord:* Wat wordt er gebruikt voor het merendeel van de gebruikers van **Verzekeringnemer**? |  |
| Microsoft Active Directory (Active Directory) |  |
| Azure Active Directory (Azure AD) |  |
| Active Directory en Azure AD (Active Directory is dominant) |  |
| Azure AD en Active Directory (Azure AD is dominant) |  |
| Een Identity Provider ("IdP"; e.g., Okta of Ping) |  |
| Cloud-based (e.g., Google Workspaces) |  |
| Anders (details gewenst - vermeld ze onderstaand) |  |
| *Indien andere, vermeld hier met een toelichting* |  |
| Geen van bovenstaande/ onbekend. |  |
| ICA # 3 | *Selecteer alles wat van toepassing is:* Met betrekking tot het beheer van accounts van **Verzekeringnemer** geldt het volgende: |  |
| Er wordt een lijst bijgehouden van alle gebruiker en admin accounts. |  |
| Deze lijst van accounts bevat de naam van de persoon, de gebruikersnaam, de start- en einddatum en de afdeling. |  |
| Alle actieve accounts worden ten minste jaarlijks gevalideerd. |  |
| Alle actieve accounts worden ten minste eens per kwartaal gevalideerd. |  |
| Geen van bovenstaande. |  |
| ICA # 4 | *Selecteer alles wat van toepassing is:* Met betrekking tot het beleid en de technische maatregelen van **Verzekeringnemer** inzake wachtwoorden geldt het volgende: |  |
| Gebruikers worden gewezen op de risico's van hergebruik van wachtwoorden en voert een beleid om dat tegen te gaan. |  |
| Er is een oplossing geïmplementeerd om te voorkomen dat gebruikers veelgebruikte en bekende wachtwoorden instellen, zelfs als deze voldoen aan de complexiteitseisen (zoals "1q2w3e4r5t" en "Passw0rd! "). |  |
| Er wordt een wachtwoordmanager ter beschikking gesteld aan de werknemers. |  |
| Er is een oplossing geïmplementeerd om voor alle aan het ‘Domain’ gekoppelde computers verschillende, willekeurige wachtwoorden in te stellen voor lokale administrator accounts (d.w.z. oplossing voor wachtwoorden voor local admins - referentie: https://support.microsoft.com/en-us/topic/microsoft-security-advisory-local-administrator-password-solution-laps-now-available-may-1-2015-404369c3-ea1e-80ff-1e14-5caafb832f53). |  |
| Geen van bovenstaande. |  |
| ICA # 5 | *Selecteer alles wat van toepassing is:* Met betrekking tot de wijze waarop **Verzekeringnemer** “Domain Administrator Accounts" beschermt geldt het volgende :  *"Domain Administrator Accounts" zijn gebruikersaccounts - met uitzondering van "serviceaccounts" - die informatie kunnen bewerken in de omgeving die gebruikt wordt voor directory services, identity providers (IdP), federation en/of rights management enz. In een Active Directory-omgeving omvat dit Enterprise-admins, domain-admins en de groepen (domain)beheerders; in Azure AD omvat dit Global Admins, Hybrid Identity Adminis en Privileged Role Administrators).* |  |
| Administrators hebben een separate en uniek account voor admin taken (los van reguliere accounts voor dagelijkse toegang, e-mail, enz.). |  |
| "Domain Administrator Accounts" vereisen multi-factor authenticatie (MFA). |  |
| "Domain Administrator Accounts" worden beheerd en gecontroleerd via "just-in-time"-toegang, zijn tijdsgebonden en vereisen goedkeuringen om “privilege access” te verlenen. |  |
| "Domain Administrator Accounts" worden opgeslagen in een wachtwoordkluis die vereist dat de gebruiker de inloggegevens “uitcheckt” (wat daarna wordt geroteerd). |  |
| "Domain Administrator Accounts" worden niet alleen in een wachtwoordkluis bewaard, maar zijn daarnaast ook onzichtbaar voor de admin accounts wanneer zij worden "uitgecheckt", en de toegang wordt bijgehouden via een sessie manager. |  |
| "Domain Administrator Accounts" kunnen alleen gebruikt worden op computers die geen toegang hebben tot internet of e-mail en uitsluitend worden gebruikt voor het beheer van kritieke systemen (incl. authenticatie servers/ Domain controllers). |  |
| Er is een logboek van het gebruik van "Domain Administrator Accounts" gedurende ten minste de afgelopen dertig dagen. |  |
| Geen van bovenstaande/onbekend. |  |
| ICA # 6 | *Selecteer één antwoord:* op welke wijze laat **Verzekeringnemer** de werknemers op afstand (remote access) inloggen op het netwerk? |  |
| Alleen een geldige gebruikersnaam en wachtwoord (single factor authenticatie). |  |
| Multi-factor authenticatie (MFA) wordt gebruikt voor sommige connecties op afstand maar niet voor alles. |  |
| Multi-factor authenticatie (MFA) is conform beleid vereist voor alle connecties op afstand, alle uitzonderingen hierop worden bijgehouden. |  |
| Er wordtgeen toegang op afstand aan werknemers geboden. |  |
| ICA # 7 | *Selecteer één antwoord:* op welke wijze laat **Verzekeringnemer** derden op afstand (remote access) inloggen op het netwerk? |  |
| Alleen een geldige gebruikersnaam en wachtwoord (single factor authenticatie). |  |
| Multi-factor authenticatie (MFA) wordt gebruikt voor sommige connecties op afstand maar niet voor alles. |  |
| Multi-factor authenticatie (MFA) is conform beleid vereist voor alle connecties op afstand, alle uitzonderingen hierop worden bijgehouden. |  |
| Er wordtgeen toegang op afstand aan derden geboden. |  |
| ICA # 8 | *Selecteer één antwoord:* op welke wijze loggen zowel werknemers als derden in op kritieke SaaS/3rd party applicaties? |  |
| Alleen een geldige gebruikersnaam en wachtwoord (single factor authenticatie). |  |
| Multi-factor authenticatie (MFA) wordt gebruikt voor sommige connecties op afstand maar niet voor alles |  |
| Multi-factor authenticatie (MFA) is conform beleid vereist voor alle connecties op kritieke SaaS/3rd party applicaties, alle uitzonderingen hierop worden bijgehouden. |  |
| Er wordt geen gebruik gemaakt van kritieke SaaS/3rd party applicaties. |  |
| ICA # 9 | *Selecteer alles wat van toepassing is:* Met betrekking tot de wijze waarop **Verzekeringnemer** “privileged”“Service Accounts" beschermt geldt het volgende:  *"Service Accounts" zijn accounts die worden gebruikt voor het uitvoeren van applicaties en andere processen; zij worden doorgaans niet gebruikt door personen met uitzondering van het oplossen van problemen.*  *"Privileged" betekent dat men verhoogde rechten heeft, in een Active Directory-omgeving omvat dit onder meer Enterprise-admins, Domain-admins en (domein-)administrators.* |  |
| Er is een lijst (of inventaris) van alle "Privileged" "Service Accounts" en deze wordt ten minste elk kwartaal bijgewerkt. |  |
| "Privileged" "Service Accounts" hebben wachtwoorden van ten minste 25 tekens. |  |
| "Privileged" "Service Accounts" wachtwoorden worden ten minste jaarlijks vervangen (rotated). |  |
| "Privileged" "Service Accounts" wachtwoorden worden ten minste eenmaal per kwartaal vervangen (rotated). |  |
| "Service Accounts" zijn zo geclassificeerd dat verschillende accounts worden gebruikt voor interactie met werkstations, servers en authenticatie servers, zelfs voor dezelfde service. |  |
| Er bestaat een proces om jaarlijks de huidige vereisten voor elke dienst die is verbonden met "Privileged" "Service Accounts" te toetsen om na te gaan of de dienst nog steeds de machtigingen vereist die de "Service Account" heeft (en die machtigingen af te schalen indien dat niet het geval is). |  |
| Geen van bovenstaande/Onbekend. |  |
| ICA # 10 | *Selecteer één antwoord:* Het Authenticator Assurance Level (AAL) dat het beste de Multi-factor authenticatie (MFA) toepassing van **Verzekeringnemer** weergeeft:  *NIST Special Publication 800-63B beschrijft de Authenticator Assurance Levels (AAL).* |  |
| AAL1 |  |
| AAL2 |  |
| AAL3 |  |
| Onbekend. |  |
| ICA # 11 | Geef het aantal actieve accounts op die **Verzekeringnemer** heeft voor de onderstaande categorieën. De opgave van accounts mogen geen inactieve accounts omvatten, maar zal wel alle ‘nested’ accounts moeten bevatten binnen alle domeinen. |  |
| Het aantal "Domain Administrator Accounts": |  |
| Het aantal "Privileged" "Services Accounts":  *"Privileged" betekent dat het account verhoogde rechten heeft, in een*  *Active Directory-omgeving omvat dit onder meer Enterprise-admins,*  *Domain admins en (domein-)administrators.* |  |
| OPMERKING: Voor elk "Privileged" "Service Account", kan de tabel onderaan dit formulier ingevuld te worden om meer details te geven over: naam van het account, de rechten die het account heeft, de software die het ondersteund, bij welke hosts het service account inlogt en waarom de toegekende rechten benodigd zijn. |  |
| ICA # 12 | *Selecteer één antwoord:* Wat beschrijft het beste de manier van ‘access controls’ op de werkstations (o.a. desktops/laptops) van gebruikers?  Wanneer een ‘endpoint privilege manager’ of een soortgelijke toepassing wordt gebruikt om gebruikers tijdelijk admin toegang te verlenen voor specifieke activiteiten, mag dat in het kader van deze vraag niet als "admin toegang" worden beschouwd. |  |
| De gewone, dagelijkse accounts van werknemers zijn geen local admins en/of hebben geen admin toegang tot de werkstations. |  |
| Het beleid is dat werknemers niet standaard in de Administrators groep zitten en geen lokale admin toegang hebben; alle uitzonderingen op het beleid worden gedocumenteerd. |  |
| Sommige werknemers maken deel uit van de Administrators groep of hebben lokale admin toegang. |  |
| Onbekend. |  |
| ICA # 13 | *Selecteer één antwoord:* Wat beschrijft het beste de manier van ‘access controls’ van gebruikers op servers die zijn aangesloten op het netwerk?  Deze vraag ziet toe op de gewone, dagelijkse accounts van werknemers en niet op separate accounts voor admin taken die naast de dagelijkse accounts worden gebruikt. |  |
| De gewone, dagelijkse accounts van werknemers zijn geen local admins en/of hebben geen admin toegang tot de servers. |  |
| Het beleid is dat werknemers niet standaard in de Administrators groep zitten en geen lokale admin toegang hebben; alle uitzonderingen op het beleid worden gedocumenteerd. |  |
| Sommige werknemers maken deel uit van de Administrators groep of hebben lokale admin toegang. |  |
| Onbekend. |  |
| ICA # 14 | Hoeveel gebruikers hebben permanente Admin (privileged) toegang tot andere servers en/of werkstations dan van henzelf?  Gebruikers die inloggegevens ‘uitchecken’ hoeven niet te worden meegenomen. Onderaan deze rubriek kan een aanvullende toelichting worden gegeven) |  |
| Vul een aantal in: |  |
| ICA # 15 | Worden beveiliging logs van alle Domain Controllers in een SIEM oplossing geladen voor analyse? |  |
| Ja |  |
| Nee – er is geen SIEM of er worden geen logs in de SIEM geladen |  |
| Niet van toepassing – er wordt geen gebruik gemaakt van directory services, IdP, rights management. |  |
| ICA # 16 | *Selecteer alles wat van toepassing is:* Welk Audit beleid is er van toepassing op Domain Controllers? |  |
| *Audit Credential Validation* (Failure) |  |
| *Audit Process Creation* (Success) |  |
| *Audit Security Group Management* (Success and Failure) |  |
| *Audit User Account Management* (Success and Failure) |  |
| *Audit Other Account Management Events* (Success and Failure*)* |  |
| *Audit Sensitive Privilege Use* (Success and Failure) |  |
| *Audit Logon* (Success and Failure) |  |
| *Audit Special Logon* (Success) |  |
| Geen van bovenstaande/ onbekend. |  |
| Niet van toepassing (er wordt geen gebruik gemaakt van Active Directory). |  |

|  |  |  |
| --- | --- | --- |
|  | Aanvullende toelichting op deze sectie: |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Security Monitoring en Incident Response** | | |
|  | Vraag | Antwoord |
| SMIR # 1 | *Selecteer één antwoord:* Als het gaat om monitoring van de output van de beveiligingstools middels een SOC (Security Operations Center) geldt het volgende: |  |
| Er is geen personeel dat zich bezighoudt met monitoring en bewaken van beveiligingsoperaties (Security Operations Center). |  |
| Er is een Security Operation Center (SOC), maar dit is niet 24/7 (intern of extern). |  |
| Er is een 24/7 Security Operation Center (SOC) die wordt uitgevoerd door een derde partij (zoals een Managed Security Services Provider). |  |
| Er is een 24/7 interne Security Operations Center (SOC). |  |
| SMIR # 2 | *Selecteer alles wat van toepassing is*: Met betrekking tot het monitoren van het netwerk geldt het volgende: |  |
| Er wordt gebruikt een Security Information and Event Management (SIEM) oplossing om de output van meerdere beveiligingsoplossingen te analyseren |  |
| Het netwerkverkeer wordt gemonitord op abnormale of mogelijk verdachte dataoverdrachten. |  |
| Er wordt gecontroleerd op problemen met de prestaties en opslagcapaciteit (zoals hoog memory- of processor gebruik, of geen vrije schijfruimte). |  |
| Er wordt gebruik gemaakt van tools om gegevensverlies te monitoren (DLP) en deze bevindt zich in de blokkeermodus. |  |
| Er wordt gebruik gemaakt van tools om gegevensverlies te monitoren (DLP) en deze bevindt zich niet in de blokkeermodus. |  |
| Geen van bovenstaande/onbekend. |  |
| SMIR # 3 | Wat is de gemiddelde tijd om beveiligingsincidenten van werkstations (desktops en laptops) te onderzoeken en te verhelpen kijkende naar het recente kwartaal? |  |
| <30 minuten |  |
| 30 minuten-2 uur |  |
| 2-8 uur |  |
| 8 uur – 3 dagen |  |
| > 3 dagen |  |
| Dit wordt niet bijgehouden |  |
| SMIR # 4 | Welk percentage van de (kritieke) systemen worden gelogd en doorgestuurd naar de SIEM oplossing? |  |
| 0-30% |  |
| 31-50% |  |
| 51-70% |  |
| >= 71% |  |
| Dit wordt niet bijgehouden |  |
| Niet van toepassing (Geen SIEM) |  |
| SMIR # 5 | Hoelang worden deze logs bewaard in de SIEM oplossing? |  |
| Korter dan 30 dagen |  |
| 30-50 dagen |  |
| 60-90 dagen |  |
| 90 dagen of meer |  |
| Dit wordt niet bijgehouden |  |
| Niet van toepassing (geen SIEM) |  |
| SMIR # 6 | *Geef alles aan wat van toepassing is:* op het verifiëren van de efficiëntie van de beveiligingsmaatregelen: |  |
| Verzekeringnemer gebruikt Breach and Attack Simulation (BAS) software om de effectiviteit van beveiligingsmaatregelen na te gaan. |  |
| Er is een intern "red team" die beveiligingsmaatregelen en respons test of minimaal eenmaal per jaar een expert die een penetratietests uitvoert op de interne systemen. |  |
| Er is het afgelopen jaar een externe partij ingeschakeld om bedreigingen te simuleren en de beveiligingsmaatregelen te testen (penetratietest). |  |
| Geen van bovenstaande/onbekend. |  |
| SMIR # 7 | *Selecteer alles wat van toepassing is:* Met betrekking tot het incident response plan en de procedures van V**erzekeringnemer** geldt het volgende: |  |
| Er is een gedocumenteerd incident response plan. |  |
| Het incident response plan bevat een draaiboek specifiek voor ransomware incidenten |  |
| Het incident responsplan bevat een draaiboek specifiek voor ransomware incidenten bij derden (zoals onafhankelijke contractanten, leveranciers, dienstverleners of klanten) |  |
| Het incident response plan bevat een proces voor contact met toezichthouders in het geval dat een ransomware incident is bevestigd. |  |
| Het incident response plan bevat een proces voor het hervatten van de operationele werkzaamheden na herstel via een back-up. |  |
| Geen van bovenstaande/onbekend. |  |
| SMIR # 8 | Is er een gedocumenteerd proces om te reageren op phishing-campagnes (al dan niet specifiek gericht tegen **Verzekeringnemer** of haar werknemers)? |  |
| Ja |  |
| Nee |  |

|  |  |  |
| --- | --- | --- |
|  | Aanvullende toelichting op deze sectie: |  |
|  |  |

|  |
| --- |
| **Risk Management** |

|  |  |  |
| --- | --- | --- |
|  | Vraag | Antwoord |
| RM # 1 | Heeft **Verzekeringnemer** een vulnerability scanning tool om kwetsbaarheden binnen "kritieke systemen" te identificeren en beheren? |  |
| Ja |  |
| Nee |  |
| RM # 2 | *Selecteer alles wat van toepassing is:* Met betrekking tot de middelen die **Verzekeringnemer** gebruikt om patches te kunnen prioriteren geldt het volgende: |  |
| Common Vulnerability Scoring System (CVSS) score. |  |
| Samenhang met de invloed van de kwetsbaarheid op "kritieke systemen". |  |
| Generieke threat intelligence (bv. dat kwaadwillenden een bepaalde kwetsbaarheid misbruiken; zoals de "Known Exploited Vulnerability Catalog" van CISA). |  |
| Specifieke threat intelligence voor **Verzekeringnemer** (inclusief informatie dat kwaadwillenden Verzekeringnemer targettenvia bepaalde kwetsbaarheden, of gegevens uit de omgeving van **Verzekeringnemer** die aangeven waar kwaadwillenden zich op richten). |  |
| Geen van bovenstaande/onbekend. |  |
| RM # 3 | Wat is de termijn waarbinnen **Verzekeringnemer** kritieke patches (met hoge prioriteit) uitvoert volgens het standaard beleid? |  |
| Binnen 24 uur |  |
| 24-72 uur |  |
| 3-7 dagen |  |
| 7-29 dagen |  |
| >= 30 dagen |  |
| Er is geen specifiek beleid gedefinieerd voor het implementeren van kritieke patches/ onbekend |  |
| RM # 4 | Kijkende naar het bovengenoemde patch target van **Verzekeringnemer**, welk percentage aan uitgevoerde kritieke patches wordt daadwerkelijk behaald binnen die termijn? |  |
| >95% |  |
| 90-95% |  |
| 80-89% |  |
| <80% |  |
| Onbekend. |  |
| RM # 5 | *Selecteer alles wat van toepassing is:* Met betrekking tot het beleid van **Verzekeringnemer** voor het gebruik van IT-systemen geldt het volgende: |  |
| Er is een "Acceptable Use Policy" (AUP) waarin de verplichtingen en beperkingen van de gebruikers worden uiteengezet. |  |
| De AUP beschrijft de gevolgen voor overtredingen van het beleid. |  |
| Het is gebruikers niet toegestaan om social-mediaplatforms te bezoeken vanaf systemen van verzekeringnemer, behalve wanneer er een specifieke zakelijke behoefte is. |  |
| Gebruikers hebben geen toegang tot persoonlijke e-mail. |  |
| Het is beheerders uitdrukkelijk verboden om via privileged accounts op het internet te surfen of toegang te krijgen tot persoonlijke e-mail. |  |
| Gebruikers en beheerders zijn verantwoordelijk voor het beveiligen van hun computer en accounts tegen veelvoorkomende risico's of problemen. |  |
| Gebruikers en beheerders zijn verplicht vermoedelijke overtredingen te melden. |  |
| Geen van bovenstaande/onbekend. |  |
| RM # 6 | *Selecteer alles wat van toepassing is:* Om risicovol en afwijkend gedrag maar ook kwaadwillende insiders te monitoren en te signaleren geldt het volgende: |  |
| Er is een insider threat programma. |  |
| Het instellen van onveilige wachtwoorden op gebruikers- of beheerdersaccounts wordt gemonitord. |  |
| Monitoring van "privileged" accounts wanneer deze toegang krijgen tot niet-geautoriseerde websites en services. |  |
| Monitoring op ongeoorloofde toegang op afstand tot "kritieke systemen". |  |
| Monitoring vanzowel gebruikers- als beheerdersaccounts op communicatie met bekende kwaadaardige websites, IP-adressen en andere bekende bronnen van threats. |  |
| Geen van bovenstaande/onbekend. |  |

|  |  |  |
| --- | --- | --- |
|  | Aanvullende toelichting op deze sectie: |  |
|  |  |

|  |
| --- |
| **Phishing Defence** |

|  |  |  |
| --- | --- | --- |
|  | Vraag | Antwoord |
| PhD # 1 | *Selecteer alles wat van toepassing is:* Hoe gaat **Verzekeringnemer** om met het reduceren van Phishing risico's? |  |
| Er wordt jaarlijks een security awareness training gegeven aan medewerkers met aandacht voor phishing. |  |
| Minimaal jaarlijksworden gesimuleerde phishing-aanvallen uitgevoerd om de awareness van medewerkers te monitoren. |  |
| De succesratio van de laatste phishing simulatie is minder dan 15% (minder dan 15% van de medewerkers heeft de betreffende link geopend). |  |
| Externe e-mails worden als zodanig gemarkeerd of getagd. |  |
| Er is een procedure om verdachte e-mails te melden aan een intern beveiligingsteam voor nader onderzoek. |  |
| Geen van bovenstaande/onbekend. |  |
| PhD # 2 | *Selecteer alles wat van toepassing is:* Met betrekking tot het blokkeren van mogelijk schadelijke websites en/of e-mails door **Verzekeringnemer** geldt het volgende: |  |
| Er is een e-mailfilteroplossing die bekende kwaadaardige bijlagen en verdachte bestandstypen blokkeert, inclusief 'executable' bestanden. |  |
| Er is een e-mailfilteroplossing die verdachte berichten blokkeert op basis van content of kenmerken van de afzender. |  |
| Er is een webfilteroplossing waardoor werknemers bekende kwaadaardige of verdachte webpagina's niet kunnen bezoeken. |  |
| Niet gecategoriseerde en nieuw geregistreerde domeinen worden geblokkeerd middels webproxy's of DNS-filters. |  |
| Er is een webfilteroplossing die bekende kwaadaardige of verdachte downloads blokkeert, inclusief 'executable' bestanden. |  |
| De e-mailfilteroplossing bevat de mogelijkheid om verdachte bijlagen in een 'sandbox' uit te voeren. |  |
| De webfiltermogelijkheden zijn voor alle systemen, ook indien deze zich niet op het bedrijfsnetwerk bevinden (systemen welke bijvoorbeeld zijn geconfigureerd om cloudbased webfilters te gebruiken of een VPN-verbinding vereisen om op het internet te surfen). |  |
| Geen van bovenstaande/onbekend. |  |

|  |  |  |
| --- | --- | --- |
|  | Aanvullende toelichting op deze sectie: |  |
|  |  |

|  |
| --- |
| **Malware Beveiliging** |

|  |  |  |
| --- | --- | --- |
|  | Vraag | Antwoord |
| Mal # 1 | *Selecteer alles wat van toepassing is:* Wat is van toepassing ten aanzien van de beveiligingssoftware op de werkstations (desktops en laptops) van **Verzekeringnemer?**: |  |
| De beveiligingssoftware bevat antivirus met heuristische scan mogelijkheden. |  |
| Er wordt gebruik gemaakt van beveiligingssoftware met detectie van ongebruikelijk gedragspatronen en misbruik (exploit) bescherming. |  |
| Er wordt gebruik gemaakt van ‘endpoint threat detection and response (ETDR of EDR)’ software die het volgende doet: controleren op dreigingsindicatoren; patronen identificeren die overeenkomen met bekende dreigingen; automatisch reageren door dreigingen te verwijderen of in te perken; beveiligingspersoneel waarschuwt bij incidenten; forensische en analysemogelijkheden biedt om analisten in staat te stellen op dreigingen te reageren. |  |
| Er zijn maatregelen op werkstations geïmplementeerd om alleen de uitvoering van toegestane applicaties toe te staan. Niet-toegestane applicaties worden geblokkeerd en een lijst van toegestane applicaties wordt ten minste twee keer per jaar opnieuw beoordeeld. |  |
| **Verzekeringnemer** heeft een interne groep en/of een MSSP die toezicht houdt op de output van de beveiligingssoftware en eventuele afwijkingen onderzoekt. |  |
| Geen van bovenstaande/onbekend. |  |
| Mal # 2 | *Selecteer alles wat van toepassing is:* Met betrekking tot de hierboven genoemde beveiligingssoftware op werkstations geldt het volgende: |  |
| De beveiligingssoftware wordt op alle werkstations (desktop en laptops) gebruikt, alle uitzonderingen op het beleid worden gedocumenteerd. |  |
| De beveiligingssoftware wordt op alle servers gebruikt (hypervisor hosts uitgezonderd), alle uitzonderingen op het beleid worden gedocumenteerd. |  |
| De beveiligingssoftware wordt op alle mobiele apparaten (inclusief tablets, telefoons etc., maar met uitzondering van laptops) gebruikt, alle uitzonderingen op het beleid worden gedocumenteerd. |  |
| Geen van bovenstaande/onbekend. |  |
| Mal # 3 | *Selecteer alles wat van toepassing is:* Met betrekking tot de instellingen van de hierboven genoemde beveiligingssoftware geldt het volgende: |  |
| De software wordt ten minste dagelijks geüpdatet – indien die updates dagelijks beschikbaar zijn |  |
| De software is ingesteld zodat verdachte processen/bestanden geblokkeerd worden (i.p.v. alleen gemeld te worden). |  |
| De software is ingesteld om onbeheerde systemen te detecteren en doet dit tenminste wekelijks. |  |
| Functies die ongeautoriseerde aanpassingen tegengaan zijn ingeschakeld. |  |
| Geen van bovenstaande/onbekend. |  |
| Mal # 4 | Benoem de beveiligingssoftware (antivirus/EDR) die gebruikt wordt; wees alstublieft zo specifiek mogelijk en noem de productnamen, bijvoorbeeld: “Falcon Prevent, Insight en Overwatch” ipv “Crowdstrike” |  |
| *Beschrijf hier* |  |
| Mal # 5 | *Selecteer alles wat van toepassing is:* Met betrekking tot het beperken van genoemde ‘lateral movements’ geldt het volgende: |  |
| Het netwerk is geografisch onderverdeeld. (b.v. verkeer tussen kantoren op verschillende locaties is niet mogelijk tenzij noodzakelijk ter ondersteuning van een specifieke zakelijke behoefte.) |  |
| Het netwerk is gesegmenteerd in verschillende afdelingen of business units. (voorbeeld: netwerkverkeer tussen de bedrijfsmiddelen/ apparaten/ servers die verschillende functies ondersteunen- zoals HR en Finance - is niet mogelijk tenzij hoogst noodzakelijk) |  |
| Er zijn hostfirewall regels geïmplementeerd die het gebruik van RDP die het inloggen op werkstations voorkomt. |  |
| Alle serviceaccounts zijn ingesteld om ‘interactive logon’ te voorkomen. |  |
| Geen van bovenstaande/onbekend. |  |
| Mal # 6 | Heeft **Verzekeringnemer** in het afgelopen jaar een ransomware oefening uitgevoerd waarbij de tactieken, technieken en procedures van ransomware groepen werden gesimuleerd? |  |
| Ja |  |
| Nee |  |

|  |  |  |
| --- | --- | --- |
|  | Aanvullende toelichting op deze sectie: |  |
|  |  |

|  |
| --- |
| **Externe IT dienstverleners & Managed Service Providers (MSP)** |

|  |  |  |
| --- | --- | --- |
|  | Vraag | Antwoord |
| TP & MSP # 1 | *Selecteer alles wat van toepassing is:* Met betrekking tot externe IT dienstverleners voor het IT netwerk (inclusief remote access zoals cloud en VPN's) van **Verzekeringnemer** geldt het volgende: |  |
| **Verzekeringnemer** maakt gebruik van een Managed Service Providers (MSP) voor het beheer van (kritieke) systemen. |  |
| **Verzekeringnemer** maakt gebruik van een Managed Service Providers (MSP) voor security services. |  |
| **Verzekeringnemer** maakt gebruik van een Managed Service Providers (MSP) voor back-up en recovery. |  |
| **Verzekeringnemer** maakt gebruik van een Managed Service Providers (MSP) voor cloud transformatie. |  |
| **Verzekeringnemer** maakt gebruik van een Managed Service Providers (MSP) voor softwareontwikkeling. |  |
| Er is sprake vanpermanente toegang (“always on”) voor externe dienstverleners (zoals MSP’s) tot corporate resources (er is geen specifiek autorisatie van **Verzekeringnemer** vereist voor toegang) |  |
| Geen van bovenstaande/onbekend. |  |
| TP & MSP # 2 | Heeft **Verzekeringnemer** processen of tools om de risico's van externe dienstverleners (waaronder MSP's) te identificeren, beoordelen, beheren en reduceren? |  |
| Ja |  |
| Nee |  |

|  |  |  |
| --- | --- | --- |
|  | Aanvullende toelichting op deze sectie: |  |
|  |  |

|  |
| --- |
| **Perimeter and Internet Defense** |

|  |  |  |
| --- | --- | --- |
|  | Vraag | Antwoord |
| Perimeter # 1 | *Selecteer alles wat van toepassing is:* Met betrekking tot extern blootgestelde systemen, inclusief systemen die aan het internet zijn gekoppeld geldt het volgende: |  |
| Er wordt een lijst bijgehouden van extern blootgestelde systemen. |  |
| Er worden regelmatig kwetsbaarheidsscans uitgevoerd van extern blootgestelde systemen. |  |
| **Verzekeringnemer** heeft een Web Application Firewall (WAF), in blocking modus, voor alle extern gerichte applicaties. |  |
| Extern blootgestelde systemen worden ten minste maandelijks gescand op kwetsbaarheden. |  |
| Er wordt een externe dienst gebruikt om het aanvalsoppervlak (aan het internet gekoppelde systemen) te monitoren. |  |
| **Verzekeringnemer** deactiveert of blokkeert op extern blootgestelde systemen de poorten, diensten en protocollen waarvan bekend is dat zij de verspreiding van ransomware mogelijk maken, met inbegrip van, maar niet beperkt tot RDP, SMBv1, en SMBv2. |  |
| Deextern blootgestelde systemen zijn gesegmenteerd binnen een gedemilitariseerde zone (DMZ), en de DMZ is niet rechtstreeks routeerbaar naar het bedrijfsnetwerk. Gebruikers die toegang tot DMZ-diensten nodig hebben, worden naar het internet gerouteerd voor toegang. |  |
| **Verzekeringnemer** kan dreigingen detecteren en hierop reageren met oplossingen voor endpoint- en netwerkmonitoring. |  |
| Geen van bovenstaande/onbekend. |  |

|  |  |  |
| --- | --- | --- |
|  | Aanvullende toelichting op deze sectie: |  |
|  |  |

|  |
| --- |
|  |
| **“Privileged” “Service Account” tabel (indien van toepassing)** |

Invulinstructies: Gebruik voor ieder "Privileged” “Service Account” de tabel om aan te geven:

1. naam van het account,
2. de rechten die het account heeft,
3. de software die het ondersteund,
4. bij welke hosts het service account inlogt,
5. waarom de toegekende rechten nodig zijn.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **“Privileged” “Service Accounts”** | | |  |
| **Naam van het account** | **Welke rechten heeft het account** | **Ondersteunde software** | **Welke hosts het service account inlogt** | **Reden van de toekenning van de rechten** |
| *INVULVOORBEELD*  *svc\_cyberark* | *INVULVOORBEELD*  *Domain Admin* | *INVULVOORBEELD*  *CyberArk Privileged Access Manager* | *INVULVOORBEELD*  *Solely Domain Controllers* | *INVULVOORBEELD*  *DA required to change passwords of sensitive accounts* |
|  | Choose an item. |  | Choose an item. |  |
|  | Choose an item. |  | Choose an item. |  |
|  | Choose an item. |  | Choose an item. |  |
|  | Choose an item. |  | Choose an item. |  |
|  | Choose an item. |  | Choose an item. |  |
|  | Choose an item. |  | Choose an item. |  |
|  | Choose an item. |  | Choose an item. |  |
|  | Choose an item. |  | Choose an item. |  |
|  | Choose an item. |  | Choose an item. |  |

*Dit vragenformulier is onderdeel van het aanvraagproces voor een Cyberverzekering en vormt tezamen met overige verstrekte informatie en verklaringen (a) de grondslag voor het besluit van verzekeraar omtrent het sluiten van de verzekering waaronder het bepalen van de toepasselijke verzekeringsvoorwaarden en de premie en is hiermee (b) een integraal onderdeel van de verzekeringsovereenkomst.*

*Voor dit aanvraagformulier geldt de mededelingsplicht zoals vermeld in artikel 7:928 van het Burgerlijk Wetboek, tenzij van dit regime hieronder wordt afgeweken. Als (kandidaat-) verzekeringnemer bent u verplicht de gestelde vragen in dit vragenformulier zo volledig mogelijk te beantwoorden. Dit geldt ook voor feiten en omstandigheden die betrekking hebben op een bij het sluiten van deze verzekering bekende derde, wiens belangen worden meeverzekerd. Bij de beantwoording is bovendien niet alleen de eigen wetenschap van de invuller bepalend, maar ook die van de andere belanghebbenden bij deze verzekering. Vragen waarvan u het antwoord al bij de verzekeraar bekend veronderstelt, moet u toch zo volledig mogelijk beantwoorden.*

*Indien u niet volledig aan uw mededelingsplicht heeft voldaan, kan dat ertoe leiden dat het recht op uitkering wordt beperkt of zelfs vervalt. Indien u met opzet tot misleiden van de verzekeraar heeft gehandeld of verzekeraar bij kennis omtrent de ware stand van zaken de verzekering nimmer zou hebben gesloten, heeft verzekeraar tevens het recht de verzekering op te zeggen.*

*Feiten en omstandigheden die u bekend worden nadat u dit vragenformulier heeft ingezonden, maar voordat de verzekeraar u heeft bericht over zijn definitieve beslissing om het door u ter verzekering aangeboden risico al dan niet te verzekeren, moet u alsnog aan de verzekeraar mededelen, indien deze vallen onder de vraagstelling in het vragenformulier. Dit geldt uitsluitend voor nieuwe verzekeringsovereenkomsten en niet voor verlengingen.*

*In afwijking van het bepaalde in artikel 7:928 lid 6, BW gelden ten aanzien van de mededelingsplicht voor deze verzekering bovendien de volgende uitgangspunten:*

* *een niet beantwoorde of open gelaten vraag wordt geacht ontkennend te zijn beantwoord;*
* *de slotvraag dient volledig te worden beantwoord.*

*De slotvraag wordt geacht onvolledig te zijn beantwoord, indien daarbij feiten en omstandigheden zijn verzwegen of verkeerd voorgesteld waarvan aanvrager, bijvoorbeeld op grond van de overige op het aanvraagformulier gestelde vragen en/of de aard van de aangevraagde verzekering in relatie tot hetgeen niet is opgegeven of verkeerd is voorgesteld, in redelijkheid moest begrijpen dat deze voor de beoordeling van het ter verzekering aangeboden risico van belang konden zijn.*

*Door de ondertekening van dit vragenformulier verklaart (kandidaat-) verzekeringnemer, mede gelet op de inhoud van art. 7:928 BW, dat de vragen volledig en naar waarheid zijn beantwoord om daarmee de aangevraagde verzekering te verkrijgen.*

*Ondergetekende gaat hierbij akkoord, garandeert en verklaart dat hij of zij een bevoegde vertegenwoordiger van de (kandidaat-) verzekeringnemer is en volledig gemachtigd is om namens de (kandidaat-) verzekeringnemer deze aanvraag te doen, de vragen te beantwoorden en verklaringen af te leggen.*

|  |  |
| --- | --- |
| Handtekening (kandidaat-) Verzekeringnemer | Datum: |
| Functie: |  |