Nulmeting CIS Controls

WinSecure

Versie: 2.0

Publicatiedatum: 13-06-2023

Inhoud

Inleiding 3
1. Inventarisatie en controle van bedrijfseigendommen 4
2. Inventarisatie en controle van software-assets 6
3. Gegevensbescherming 8
4. Veilige configuratie van bedrijfsmiddelen en software 12
5. Accountbeheer 16
6. Beheer van toegangscontrole 18
7. Continue Vulnerability Management 21
8. Beheer van auditlogs 23
9. Bescherming van e-mail en webbrowsers 26
10. Bescherming tegen malware 28
11. Gegevensherstel 30
12. Beheer van de netwerkinfrastructuur 32
13. Netwerkbewaking en -verdediging 34
14. Security awareness en vaardigheidstraining 37
15. Beheer van dienstverleners 40
16. Beveiliging van applicaties/ software 43
17. Beheer van incidenten 50
18. Pentesten 54

Inleiding

Dit document is een nulmeting omtrent cybersecurity. Deze is gebaseerd op de punten zoals benoemd in de CIS Controls, versie 8. De CIS Controls zijn een internationale standaard op het gebied van cybersecurity. De CIS Controls kunt u downloaden via de website van CIS.

De CIS Controls zijn opgesplitst in drie 'Implementatiegroepen' (IG's). IG1 is de basis cyberhygiëne waaraan elk bedrijf eigenlijk zou moeten voldoen. IG2 is een uitgebreidere versie van IG1 (IG1 dient dan ook aan voldaan te worden). Deze is van toepassing op bedrijven die IT-infrastructuur beheren en daardoor logischerwijs aan strengere basisregels zouden moeten voldoen. IG3 is van toepassing op bedrijven die cybersecuritydiensten verlenen. Deze implementatiegroepen worden ook in dit document aangehouden. Dit betekent dat de checklist op maat gemaakt is voor elke branche, en dat hierdoor u zelf kunt kiezen welke implementatiegroep u wilt checken. Kijk voor meer informatie over de IG's op de website van CIS.
Na het uitvoeren van deze nulmeting heeft u inzicht op welke vlakken uw cybersecurity beter kan, of juist heel goed is.

Leeswijzer

Elke categorie is voorzien van een rationale: een gedachte waarom u aan deze categorie zou moeten voldoen. Er zijn achttien categorieën, in overeenstemming met de CIS Controls.

Elke subcategorie is voorzien van een kleur: groen is voor IG1, oranje is IG2 en blauw is IG3. Wilt u bijvoorbeeld voldoen aan IG2, dan doet u de nulmeting van alle groene (IG1) en oranje (IG2) onderdelen. Elke subcategorie is voorzien van vragen die u kunt stellen om te checken of u voldoet aan de vereisten van de subcategorie. De vereisten staan onder de kop 'criteria'. Door het stellen van deze vragen, en ze te beantwoorden krijgt u inzicht in uw cybersecurity-volwassenheid.

1. Inventarisatie en controle van bedrijfseigendommen

Rationale:

Het actief beheren (inventariseren, volgen en corrigeren) van alle bedrijfsmiddelen die fysiek, virtueel en op afstand met de infrastructuur zijn verbonden. Dit geldt ook voor/binnen cloudomgevingen.
Een inventaris is nodig om alle bedrijfsmiddelen die binnen de onderneming moeten worden bewaakt en beschermd, nauwkeurig te kennen. Dit ondersteunt ook de identificatie van onbevoegde en onbeheerde activa die moeten worden verwijderd of hersteld.

Bedrijfsmiddelen:

- *End-user apparatuur; PC's, laptops, mobiele apparatuur;*
- *Netwerkapparaten;*
- *Niet-computers/internet of things (IoT)-apparaten;*
- *Servers.*

1.1 Stel een gedetailleerde inventaris op met bedrijfseigendommen en houdt deze bij

Vragen:

- Is er een asset inventory/ inventaris van bedrijfseigendommen?
- Indien aanwezig, hoe vaak wordt deze geüpdatet?
- Wat wordt er genoteerd?

Criteria:

- Er is een inventaris.
  - De inventaris wordt bijgewerkt wanneer er nieuwe apparaten zijn en wanneer apparaten van eigenaar verwisselen.
  - De inventaris wordt ten minste tweemaal per jaar gecontroleerd.
  - Ten minste komen de volgende onderdelen voor in de inventarislijst: MAC-adres, apparaatnaam, type, eigenaar, eventueel IP of andere identificerende kenmerken.

1.2 Verwijder ongewenste eigendommen/ systemen

Vragen:

- Wordt er gecheckt op ongewenste systemen in het netwerk?
  - Zo ja, op welke manier?
- Hoeveel tijd zit er tussen de scans?

Criteria:

- Er wordt gecheckt op ongewenste systemen in het netwerk.
- Er wordt elke week gescand op ongewenste systemen.
- Na de vondst van ongewenste systemen worden deze in quarantaine geplaatst of van het netwerk verwijderd.

1.3 Gebruik een active asset discovery tool

Vragen:

- Wordt er gebruikgemaakt van een active asset discovery tool? Zo ja, welke?
- Wordt deze tool automatisch of handmatig gebruikt?
- Hoe vaak scant deze tool op aanwezige assets?

Criteria:

- Er wordt gebruikgemaakt van een active asset discovery tool.
- Gevonden apparaten worden handmatig of automatisch toegevoegd aan de inventory.
- Er wordt elke dag (of vaker) een scan uitgevoerd.

1.4 Gebruik DHCP-logging om de inventaris met bedrijfseigendommen te updaten

Vragen:

- Worden DHCP-logs bewaard/bijgehouden?
- Zo ja, worden deze gebruikt om de inventaris te updaten?
- Met welke frequentie worden deze logs gebruikt om de inventaris te updaten?

Criteria:

- DHCP-logs worden gebruikt om de inventaris te updaten.
- De inventaris wordt elke week bijgewerkt op basis van de DHCP-logs.

1.5 Gebruik een passive asset discovery tool

Vragen:

- Wordt er gebruikgemaakt van een passive asset discovery tool?
- Zo ja, welke tool(s)?
- Hoe wordt deze tool gebruikt? Automatisch of handmatig?

Criteria:

- Er wordt gebruikgemaakt van een passive asset discovery tool.
- Gevonden apparaten worden handmatig of automatisch toegevoegd aan de inventory.
- Er wordt elke dag ten minste één scan uitgevoerd.

2. Inventarisatie en controle van software-assets

Rationale: *Het activeren, bijhouden en corrigeren van alle software (besturingssystemen en toepassingen) op het netwerk, zodat alleen geautoriseerde software kan worden geïnstalleerd en uitgevoerd. Niet-geautoriseerde en onbeheerde software wordt hierbij gevonden, waardoor deze niet kan worden geïnstalleerd of uitgevoerd.*

2.1 Stel een inventaris op met software en houdt deze bij

Vragen:

- Welke softwarepakketten worden gebruikt?
  - Vraag hier naar de:
    - Titel
    - Uitgever
    - Eerste installatiedatum/ gebruiksdatum
    - Het bedrijfsdoel
- Wordt de software nog steeds gebruikt?

Criteria:

- Er is een lijst met gebruikte softwarepakketten.
- Bij de gebruikte softwarepakketten wordt de titel, uitgever, eerste installatiedatum/ gebruiksdatum en het bedrijfsdoel benoemd.

2.2 Check of software in de inventaris ondersteund wordt

Vragen:

- Wordt het gebruikte softwarepakket ondersteund?
  - Ja?
  - Nee?
    - Is het softwarepakket noodzakelijk?
    - Wat is het doel van het softwarepakket?
    - Zijn er andere mogelijkheden om hetzelfde doel te behalen?

Criteria:

- Opgestelde lijst met ondersteunde en niet ondersteunde software.

2.3 Verwijder niet-goedgekeurde software

Vragen:

- Is er een lijst met niet-goedgekeurde softwarepakketten?
- Zijn de niet-goedgekeurde softwarepakketten verwijderd?
  - Ja
  - Nee?
    - Waarom zijn deze softwarepakketten nog aanwezig?
    - Wat is het doel van dit softwarepakket?
- Wordt dit ook elke maand gecontroleerd?

Criteria:

- Er zijn geen niet-goedgekeurde softwarepakketten aanwezig.

2.4 Gebruik automatische software-inventarisatie tools

Vragen:

- Wordt er gebruikgemaakt van een automatische software-inventarisatie tool?
- Zo ja, welke tool?

Criteria:

- Er wordt gebruik gemaakt van een automatische software-inventarisatie tool.
- De tool neemt documentatie van geïnstalleerde software mee.
- Versienummers zijn terug te vinden in de lijst.

2.5 Gebruik een whitelist voor geautoriseerde software

Vragen:

- Is er een lijst met de toegestane softwarepakketten?
- Wordt het softwarepakket procesmatig gecontroleerd voordat het op de lijst wordt gezet?
- Wordt dit periodiek gecontroleerd?

Criteria:

- Er worden technische controles, zoals het toestaan van toepassingen, gebruikt om ervoor te zorgen dat alleen geautoriseerde software kan worden uitgevoerd of geopend.
- Deze whitelist wordt tweemaal per jaar of vaker opnieuw beoordeeld.

2.6 Gebruik een whitelist voor geautoriseerde libraries

Denk hierbij aan specifieke .dll-, .ocx-, .so- enz. bestanden, die ingeladen worden in systeemprocessen.

Vragen:

- Is er een lijst met de toegestane libraries?
- Wordt dit periodiek gecontroleerd?

Criteria:

- Er worden technische controles gebruikt om ervoor te zorgen dat alleen geautoriseerde libraries, zoals specifieke .dll-, .ocx-, .so-, enz. bestanden, in een systeemproces mogen worden geladen.
- Het laden van niet-geautoriseerde bibliotheken in een systeemproces worden geblokkeerd.
- Deze whitelist wordt ten minste tweemaal per jaar opnieuw beoordeeld.

2.7 Gebruik een whitelist voor geautoriseerde scripts

Vragen:

- Is er een lijst met de toegestane scripts?
- Wordt dit periodiek gecontroleerd?

Criteria:

- Er worden technische controles, zoals digitale handtekeningen en versiebeheer, gebruikt om ervoor te zorgen dat alleen geautoriseerde scripts, zoals specifieke .ps1-, .py-, enz. bestanden, mogen worden uitgevoerd.
- De uitvoering van niet-geautoriseerde scripts wordt geblokkeerd.
- De whitelist wordt ten minste tweemaal per jaar opnieuw beoordeeld.

3. Gegevensbescherming

Rationale: *Processen en technische controles ontwikkelen om gegevens te identificeren, te classificeren, veilig te behandelen, te bewaren en te verwijderen.*

3.1 Een gegevensbeheerproces opzetten en onderhouden

Vragen:

- Wordt er gebruikgemaakt van gegevensbeheerproces?
- Welke gegevens worden er opgeslagen?
- Is dit proces ook gedocumenteerd?
- Wordt er gebruikgemaakt van software voor gegevensbeheer?
- Wanneer wordt het gegevensbeheerproces bijgewerkt?

Criteria:

- Er is een gegevensbeheerproces, wat voldoende toegelicht kan worden.
- Het gegevensbeheerproces is (voldoende) gedocumenteerd.
- Het gegevensbeheerproces benoemt de volgende punten:
  - De gevoeligheid van gegevens.
  - De eigenaar van gegevens.
  - De behandeling van gegevens.
  - Limieten voor het bewaren van gegevens en verwijderingsvereisten, op basis van de normen voor gevoeligheid en bewaren voor de onderneming.
- Het gegevensbeheerproces wordt tenminste jaarlijks bijgewerkt, of bij grote veranderingen.

3.2 Een gegevensinventaris opstellen en onderhouden

Vragen:

- Is er een gegevensinventaris?
- Wordt de gegevensinventaris gebruikt tijdens het gegevensbeheerproces?
- Wordt er gebruikgemaakt van software voor een gegevensinventaris?
- Welke gegevens bevat de inventaris? (Gevoeligheid, opslaglocatie, toegang enzovoorts)
- Wanneer wordt de gegevensinventaris bijgewerkt?

Criteria:

- Er is een gegevensinventaris.
- De gegevensinventaris wordt gebruikt in het kader van het gegevensbeheerproces.
- De gegevensinventaris wordt ten minste éénmaal per jaar bijgewerkt, waarbij gevoelige gegevens prioriteit hebben binnen dit proces.
- De gegevensinventaris bevat ten minste alle gevoelige gegevens.

3.3 Lijsten voor gegevenstoegang configureren

Vragen:

- Op welke locaties worden gegevens opgeslagen (lokaal, extern, cloud, databases, applicaties)?
- Welke permissiestructuur wordt er aangehouden?
- Wie hebben er allemaal toegang tot persoonsgegevens/gevoelige data?

Criteria:

- Er is een duidelijk beeld op welke locatie gegevens opgeslagen worden.
- Er is een duidelijke permissiestructuur.
- Toegang tot persoonsgegevens/gevoelige data is need-to-know.

3.4 Gegevensbewaring afdwingen

Vragen:

- Bevat het gegevensbeheerproces een bewaarbeleid?
- Wat bevat het gegevens-bewaarbeleid?

Criteria:

- Er is een gegevens-bewaarbeleid.
- Het gegevens-bewaarbeleid bevat een minimum- en maximum bewaartermijn.

3.5 Gegevens veilig verwijderen

Vragen:

- Bevat het gegevensbeheerproces een beleid voor veilig verwijderen?
- Wordt ervoor gezorgd dat het verwijderingsproces en de verwijderingsmethode in overeenstemming zijn met de gevoeligheid van de gegevens?

Criteria:

- Er is een beleid voor veilig verwijderen in het gegevensbeheerproces.
- De verwijderactie is in overeenstemming met de gevoeligheid van de gegevens.

3.6 Versleutel gegevens op apparaten van eindgebruikers

Vragen:

- Worden (gevoelige) gegevens versleuteld op de apparaten van eindgebruikers (Bitlocker/FileVault/dm-crypt)?

Criteria:

- Gevoelige gegevens worden versleuteld op de apparaten van eindgebruikers.

3.7 Een dataclassificatieschema opstellen en onderhouden

Vragen:

- Wordt er gebruikgemaakt van een (algemeen) classificatieschema voor gegevens?
- Welke classificaties bevat het classificatieschema?
- Hoe vaak wordt het classificatieschema bijgewerkt?

Criteria:

- Er wordt actief gebruikgemaakt van een classificatieschema voor gegevens.
- Het classificatieschema bevat meerdere classificaties.
- Het classificatieschema wordt ten minste jaarlijks bijgewerkt en wanneer er belangrijke veranderingen zijn.

3.8 Gegevensstromen documenteren

Vragen:

- Is er documentatie over gegevensstromen?
- Bevat deze documentatie ook gegevensstromen van leveranciers/serviceproviders?
- Is de gegevensstromen documentatie in lijn met het gegevensbeheerproces?
- Hoe vaak wordt deze documentatie bijgewerkt?

Criteria:

- Er is documentatie over gegevensstromen.
- Documentatie over gegevensstromen bevat ook gegevensstromen van leveranciers/serviceproviders.
- De documentatie van gegevensstromen is in lijn met het gegevensbeheerproces.
- De documentatie van gegevensstromen wordt ten minste jaarlijks bijgewerkt en wanneer er belangrijke veranderingen zijn.

3.9 Versleutel gegevens op verwijderbare media

Vragen:

- Worden gegevens versleuteld op verwijderbare media (Bitlocker/FileVault/dm-crypt)?

Criteria:

- Gegevens worden versleuteld op verwijderbare media.

3.10 Gevoelige gegevens op het netwerk versleutelen

Vragen:

- Worden gevoelige gegevens versleuteld onderweg (TLS/SSH/andere encryptie)?

Criteria:

- Gevoelige gegevens worden versleuteld onderweg (TLS/SSH/andere encryptie).

3.11 Gevoelige gegevens op harde schijven versleutelen

Vragen:

- Worden (gevoelige) gegevens versleuteld op harde schijven?
- Worden (gevoelige) gegevens versleuteld op servers?
- Worden (gevoelige) gegevens versleuteld op toepassingen?
- Worden (gevoelige) gegevens versleuteld op databases?

Criteria:

- (Gevoelige) gegevens worden versleuteld op harde schijven, servers, toepassingen en databases. Dit is de minimumeis. Voor geavanceerde beveiliging dient ook client-side encryptie toegepast te worden.

3.12 Segmenteren van gegevensverwerking en -opslag op basis van gevoeligheid

Vragen:

- Wordt er gebruikgemaakt van segmentatie voor gegevens?
- Waarop worden gegevens gesegmenteerd tijdens de opslag en verwerking?

Criteria:

- Gegevens worden opgeslagen en verwerkt op basis van gevoeligheid.
- Gevoelige gegevens worden niet verwerkt op bedrijfsmiddelen die bedoeld zijn voor minder gevoelige gegevens.

3.13 Preventie van gegevensverlies

Vragen:

- Op welke manier wordt er preventief gewerkt aan het vermijden van gegevensverlies?
- Wordt er een geautomatiseerde tool/ host-based Data Loss Prevention tool gebruikt?
- Waar vindt Data Loss Prevention plaats?
- Werkt een DLP-tool ook de inventaris van gevoelige gegevens bij?

Criteria:

- Er wordt een geautomatiseerde tool of host-based Data Loss Prevention tool gebruikt.
- Data Loss Prevention vindt plaats op alle bedrijfsmiddelen, inclusief middelen bij een externe dienstverlener.
- De Data Loss Prevention tool werkt de inventaris van gevoelige gegevens bij.

3.14 Toegang tot gevoelige gegevens vastleggen

Vragen:

- Wordt er gebruikgemaakt van access logs voor gevoelige gegevens?
- Wat wordt er bijgehouden in de access logs van gevoelige gegevens?

Criteria:

- Toegang tot gevoelige gegevens wordt gelogd, inclusief alle andere handelingen zoals wijzigingen en verwijdering.

4. Veilige configuratie van bedrijfsmiddelen en software

Rationale:

De veilige configuratie van bedrijfsmiddelen (eindgebruikersapparaten, waaronder draagbare en mobiele apparaten; netwerkapparaten; niet-computing/IoT-apparaten; en servers) en software (besturingssystemen en toepassingen) vaststellen en onderhouden.

4.1 Een veilig configuratieproces opzetten en onderhouden

Vragen:

- Is er een bestaand proces voor het installeren/ configureren van draagbare mobiele apparaten?
- Is er een bestaand proces voor het installeren/ configureren van niet-computing/ IoT apparaten?
- Is er een bestaand proces voor het installeren/ configureren van servers?
- Is er een bestaand proces voor het installeren/ configureren van software(toepassingen)?
- Is er een bestaand proces voor het installeren/ configureren van besturingssystemen?
- Wordt de documentatie periodiek gecontroleerd?
- Wordt de documentatie ook bijgewerkt wanneer er aanpassingen zijn?

Criteria:

- Er is een bestaand configuratieproces voor draagbare mobiele apparaten.
- Er is een bestaand configuratieproces voor niet-computing/ IoT apparaten.
- Er is een bestaand configuratieproces voor servers.
- Er is een bestaand configuratieproces voor software(toepassingen).
- Er is een bestaand configuratieproces voor besturingssysteem.
- Er wordt ten minste éénmaal per jaar gecontroleerd of de documentatie nog juist is.

4.2 Een veilig configuratieproces voor netwerkinfrastructuur opzetten en onderhouden

Vragen:

- Is er een bestaand proces voor het installeren/ configureren van netwerkapparaten?
- Is er een bestaand proces voor het onderhouden van netwerkapparaten?
- Wordt er jaarlijks geëvalueerd of de documentatie nog juist is?
- Wordt de documentatie ook bijgewerkt wanneer deze niet meer up-to-date is?

Criteria:

- Er is een bestaand proces voor het installeren/ configureren van netwerkapparaten.
- Er is een bestaand proces voor het onderhouden van netwerkapparaten?
- Er wordt ten minste éénmaal per jaar gecontroleerd of de documentatie nog juist is.

4.3 Automatische sessievergrendeling op bedrijfsmiddelen configureren

Vragen:

- Is er automatische sessievergrendeling ingesteld op draagbare mobiele apparaten?
- Is er automatische sessievergrendeling ingesteld op niet-computing/ IoT apparaten?
- Is er automatische sessievergrendeling ingesteld op servers?
- Is er automatische sessievergrendeling ingesteld op fysieke apparaten?
- Op hoeveel minuten is de timer ingesteld voordat de sessie wordt vergrendeld op besturingssystemen?
- Op hoeveel minuten is de timer ingesteld voordat de sessie wordt vergrendeld op mobiele eindgebruikersapparaten?

Criteria:

- Er wordt gebruikgemaakt van sessievergrendeling op draagbare mobiele apparaten.
- Er wordt gebruikgemaakt van sessievergrendeling op niet-computing/ IoT-apparaten.
- Er wordt gebruikgemaakt van sessievergrendeling op servers.
- Er wordt een sessievergrendelingstimer ingesteld op maximaal 15 minuten voor algemene besturingssystemen.
- Er wordt een sessievergrendelingstimer ingesteld op maximaal twee minuten voor mobiele eindgebruikersapparaten.

4.4 Een firewall op servers implementeren en beheren

Vragen:

- Wordt er gebruikgemaakt van een firewall op servers?
- Bestaat er een beheerproces voor firewalls op servers?
- Hoe worden logbestanden van firewalls opgeslagen?

Criteria:

- Alle servers zijn voorzien van een firewalloplossing.
- De firewalls worden beheerd en de logbestanden worden op een centraal punt opgeslagen.

4.5 Implementeren en beheren van een firewall op eindgebruikersapparaten

Vragen:

- Wordt er gebruikgemaakt van een host-gebaseerde firewall?
- Wordt er gebruikgemaakt van poort-filtering op eindgebruikersapparaten?
- Wordt er gebruikgemaakt van een poort-filtering tool?
- Zo ja,
    - Heeft deze tool ook een default-deny regel die al het verkeer blokkeert, behalve de poorten die expliciet zijn toegestaan?

Criteria:

- Er wordt gebruikgemaakt van een host-gebaseerde firewall.
- Er wordt gebruikgemaakt van poort-filtering op eindgebruikersapparaten.
- Er wordt gebruikgemaakt van een poort-filtering tool.
    - Ook heeft deze tool een default-deny regel die al het verkeer blokkeert behalve de poorten die expliciet toegestaan zijn.

4.6 Veilig beheer van bedrijfsmiddelen en software

Vragen:

- Wordt configuratiebeheer en versiebeheer gedaan met behulp van veilige protocollen?
    - Voorbeeld: SSH/HTTPS en geen Telnet/HTTP.

Criteria:

- Er worden alleen veilige connecties gebruikt voor veilig beheer van software en systemen, indien mogelijk.

4.7 Standaardaccounts op bedrijfsmiddelen en software beheren

Vragen:

- Zijn er configuratieprocessen opgesteld voor standaardaccounts (zoals: root, admin- en serviceaccounts)?
- Wordt er ook periodiek gekeken of deze accounts nog worden gebruikt?
- Worden deze accounts ook uitgeschakeld?
- Worden deze accounts verwijderd?

Criteria:

- Er zijn configuratieprocessen opgesteld betreffende standaardaccounts.
- Er wordt periodiek gekeken of de standaardaccounts gebruikt worden.
- Wanneer de standaardaccounts niet worden gebruikt, worden deze uitgeschakeld.
- Wanneer accounts niet meer worden gebruikt, wordt het account verwijderd.

4.8 Onnodige diensten op bedrijfsmiddelen en software verwijderen of uitschakelen

Benodigd:

Lijst van alle geautoriseerde softwarepakketten die momenteel worden gebruikt.

Vragen:

- Wordt er periodiek gekeken of onnodige diensten en/of software geïnstalleerd is op de bedrijfsmiddelen?
    - Worden onnodige diensten en/of software verwijderd of uitgeschakeld?

Criteria:

- Er wordt periodiek gekeken of onnodige diensten en/of software geïnstalleerd zijn op de bedrijfsmiddelen.
- De onnodige diensten en/of software wordt verwijderd indien nodig.

4.9 Vertrouwde DNS-servers configureren op bedrijfsmiddelen

Vragen:

- Wordt er gebruikgemaakt van een ‘vertrouwde’ DNS op alle systemen?

Criteria:

- Er is op alle bedrijfsmiddelen een vertrouwde DNS-server geconfigureerd.

4.10 Automatische vergrendeling op draagbare apparaten van eindgebruikers afdwingen

Vragen

- Zijn er policies ingesteld over een maximaal aantal inlogpogingen?
    - Worden laptops vergrendeld wanneer de maximale inlogpogingen van twintig zijn bereikt?
    - Worden smartphones en tablets vergrendeld wanneer de maximale inlogpogingen van tien zijn bereikt?
- Worden de accounts vergrendeld na het overschrijden van deze inlogpogingen?
- Worden er applicaties gebruikt om aan deze eisen te voldoen op mobiele apparaten?

Criteria:

- Er zijn policies ingesteld over de maximale aantal inlogpogingen.
    - Voor laptops maximaal twintig pogingen.
    - Voor smartphones en tablets maximaal tien pogingen.

4.11 Remote Wipe Capability afdwingen op draagbare eindgebruikersapparaten

Vragen:

- Is het mogelijk om apparaten op afstand te ‘wipen’ indien nodig wanneer het apparaat verloren of als gestolen wordt geacht?
- Is er een regeling opgesteld voor het ‘wipen’ van apparaten van werknemers die stoppen met de huidige werkzaamheden?
    - Zo ja, wat is die regeling en de aanpak?

Criteria:

- Het is mogelijk om apparaten op afstand te ‘wipen’.
- Er is een regeling opgesteld voor het ’wipen’ van apparaten.
    - Dit geldt voor verloren apparaten.
    - Dit geldt voor gestolen apparaten.
    - Dit geldt voor apparaten van werknemers die niet langer in dienst zijn.

4.12 Scheid werk en privé op mobiele eindgebruikersapparaten

Vragen:

- Bestaat de mogelijkheid tot een gescheiden werk- en privéomgeving op draagbare mobiele apparaten (Enterprise workspaces)?
    - Wat zijn die mogelijkheden?

Criteria:

- De mogelijkheid voor gescheiden werk- en privéomgeving is aanwezig voor draagbare mobiele apparaten.

5. Accountbeheer

Rationale:

Gebruikt processen en hulpmiddelen om autorisatie aan credentials voor gebruikersaccounts, waaronder beheerdersaccounts, en serviceaccounts toe te wijzen en te beheren voor bedrijfsmiddelen en software.

5.1 Een inventaris van accounts opstellen en bijhouden

Vragen:

- Heeft u een inventaris van alle accounts die in de onderneming worden beheerd? (Voor de inventaris gelden gebruikersaccounts evenals beheerderaccounts).
    - Wordt daarbij ook de volgende gegevens opgeslagen, zie onderstaande lijst:
        - Naam
        - Gebruikersnaam
        - Start- en stopdatum
        - Naam van de afdeling

Criteria:

- Er is een inventaris van alle accounts in het bedrijf, dit omvat gebruikers- en beheerderaccounts.
- De inventaris bevat ten minste de volgende attributen: naam persoon, de gebruikersnaam, start-/stopdatum en de naam van de afdeling.
- Accounts worden gevalideerd, minimaal elk kwartaal of vaker.

5.2 Unieke wachtwoorden gebruiken

Vragen:

- Is er een beleid opgezet over het creëren van wachtwoorden?
    - Denk hierbij aan wachtwoorden van minimaal acht karakters (bij accounts die gebruikmaken van MFA).
    - Voor accounts die geen gebruik maken van MFA, moeten er minstens veertien karakters worden gebruikt.
- Hoelang moeten wachtwoorden zijn in het bedrijf?

Criteria:

- Wachtwoorden herhalen wordt niet toegestaan.
- Wachtwoorden zijn minimaal acht karakters lang met MFA, zonder MFA 12 karakters.

5.3 Inactieve accounts uitschakelen

Vragen:

- Wat is het beleid voor inactieve accounts?

Criteria:

- Inactieve accounts worden verwijderd of gedeactiveerd na 45 dagen inactiviteit, als dit ondersteund wordt.

5.4 Beperk beheerdersrechten tot specifieke beheerdersaccounts

Vragen:

- Worden beheeraccounts gebruikt voor beheerderstaken en algemene taken uitgevoerd door normale werkaccounts?
- Worden op de beheeraccounts alleen beheertaken uitgevoerd en geen algemene taken?

Criteria:

- Speciale beheerdersrechten staan alleen op de bijbehorende accounts die (alleen) daarvoor gebruikt voor worden.
- Algemene taken worden alleen gedaan op niet beheerdersaccounts.

5.5 Maak en onderhoud een inventaris van serviceaccounts

Denk aan accounts voor Exchange, SharePoint, SQL server en IIS

Vragen:

- Is er een inventaris van alle dienstaccounts?
- Welke attributen bevat de inventaris?
- Wordt de inventaris ook nagekeken?
    - Zo ja, hoe vaak?

Criteria:

- Er is een inventaris van service-accounts.
- In de inventaris staan minimaal: de verantwoordelijke van de afdeling, de datum van herzien en het doel van het account.
- De inventaris van dienstaccounts wordt minimaal elk kwartaal herzien.

5.6 Accountbeheer centraliseren

Vragen:

- Worden accounts centraal beheerd? (Denk hierbij aan het opzetten van SSO of een AD).

Criteria:

- Alle accounts (gebruikeraccounts/ beheeraccounts)
- Er is een centrale directory of identity service voor alle accounts.

6. Beheer van toegangscontrole

Rationale:

Gebruik processen en hulpmiddelen voor het creëren, toewijzen, beheren en intrekken van toegangsreferenties en -rechten voor gebruikers-, beheerders- en dienstaccounts voor bedrijfsmiddelen en software.

6.1 Een proces voor het verlenen van toegang opzetten

Vragen:

- Is er een proces bij de indienstneming van een nieuwe medewerker?
- Is er een proces voor het veranderen van een rol van een medewerker?

Criteria:

- Er is een proces voor het verlenen van toegang tot bedrijfsmiddelen bij indiensttreding.
- Er is een proces voor het verlenen van rechten.
- Er is een proces voor het veranderen van een rol van een gebruiker.

6.2 Een proces voor het intrekken van toegang opzetten

Het uitschakelen van accounts, in plaats van het verwijderen van accounts, kan nodig zijn om logs te behouden.

Vragen:

- Is er een proces voor het deactiveren van accounts als een medewerker weg gaat?
- Is er een proces voor het veranderen van de rechten als een medewerker een nieuwe rol krijgt?

Criteria:

- Er is een proces voor het intrekken van toegang tot bedrijfsmiddelen.
    - De accounts worden onmiddellijk gedeactiveerd bij het beëindigen van het dienstverband.
    - De rechten worden direct ingetrokken (en nieuwe rechten worden toegekend in geval van rol verandering).

6.3 MFA vereisen voor extern benaderbare toepassingen

Vragen:

- Wordt er gebruikgemaakt van MFA bij extern benaderbare bedrijfsapplicaties (waar het kan)?
- Wordt er gebruikgemaakt van een SSO-provider of MFA via een directoryservice?

Criteria:

- Bij externe bedrijfsapplicaties of diensten van derden wordt er gebruikt gemaakt van MFA, indien ondersteund.
  Of
- Er wordt gebruikgemaakt van MFA via een directoryservice of een SSO-provider.

6.4 MFA vereisen voor netwerktoegang op afstand

Vragen:

- Word MFA afgedwongen voor netwerktoegang op afstand?
    - Bijvoorbeeld: VPN

Criteria:

- Er wordt MFA afgedwongen voor netwerktoegang op afstand.

6.5 MFA vereisen voor administratieve toegang

Vragen:

- Word er gebruikgemaakt van MFA voor toegang bij administratieve accounts?

Criteria:

- Er wordt gebruikgemaakt van MFA bij administratieve toegangsaccounts.
    - Indien ondersteund: op alle bedrijfsmiddelen.
    - Ongeacht op-premise of extern.

6.6 Een inventaris van verificatie- en autorisatiesystemen opstellen en bijhouden

Vragen:

- Is er een inventaris van de authenticatie- en autorisatiesystemen van de onderneming? Denk ook aan systemen die gehost worden door externe bedrijven.
    - Zo ja, hoe vaak wordt het herzien en geüpdatet?

Criteria:

- Er is een inventaris van authenticatie- en autorisatiesystemen van de onderneming
    - Met inbegrip van systemen in het bedrijf maar ook die bij een externe dienstverlener worden gehost.
- Herzie en update de inventaris minstens jaarlijks.

6.7 Toegangscontrole centraliseren

Vragen:

- Is er een centraal punt voor toegangscontrole voor alle bedrijfsmiddelen?

Criteria:

- Centraal punt voor toegangscontrole voor alle bedrijfsmiddelen via een directory service of SSO-provider, indien ondersteund.

6.8 Rol gebaseerde toegangscontrole definiëren en onderhouden

Vragen:

- Is er een rol gebaseerde toegangscontrole gedefinieerd?
    - Zo ja, wordt dit beleid ook herzien en gevalideerd of alles nog klopt?

Criteria:

- Er wordt rol gebaseerde toegangscontrole toegepast door het bepalen en documenteren van de toegangsrechten die elke rol heeft binnen de onderneming om zijn taken succesvol uit te kunnen voeren.
- Dit wordt minimaal jaarlijks herzien en gevalideerd.

7. Continue Vulnerability Management

Rationale:

Een plan ontwikkelen om voortdurend de kwetsbaarheden van alle bedrijfsmiddelen binnen de infrastructuur van de onderneming te beoordelen en te volgen, om de kansen voor aanvallers te beperken. Openbare en particuliere bronnen voor nieuwe informatie over bedreigingen en kwetsbaarheden in de gaten houden.

7.1 Opzetten en onderhouden van een proces voor het beheer van kwetsbaarheden

Vragen:

- Is er een gedocumenteerd proces voor het beheer van kwetsbaarheden van bedrijfsmiddelen?
    - Zo ja, hoe vaak wordt dit herzien?

Criteria:

- Er is een gedocumenteerd proces van beheer over kwetsbaarheden van bedrijfsmiddelen.
- Documentatie wordt jaarlijks herzien en bewerkt waar nodig.
- Bij een belangrijke verandering in de onderneming wordt het document eerder herzien.

7.2 Opzetten en onderhouden van een herstelproces

Vragen:

- Is er een risico gebaseerde herstelstrategie opgesteld/gedocumenteerd in een herstelproces?
    - Wordt dit ook minstens één keer per maand herzien en geüpdatet?

Criteria:

- Er is een risico gebaseerde herstelstrategie opgesteld en gedocumenteerd.
- Het document wordt minstens één keer per maand herzien en geüpdatet.

7.3 Geautomatiseerd beheer van besturingssystemen

Vragen:

- Is er een patchbeheer voor besturingssystemen?
    - Gebeurt dit automatisch of handmatig?
    - Hoe vaak worden systemen geüpdatet?

Criteria:

- Besturingssystemen worden minimaal maandelijks via geautomatiseerd patchbeheer geüpdatet.

7.4 Geautomatiseerd beheer van applicatiepatches

Vragen:

- Is er een patchbeheer voor applicaties?
    - Gebeurt dit automatisch of handmatig?
    - Hoe vaak worden systemen geüpdatet?

Criteria:

- Applicaties worden minimaal maandelijks via geautomatiseerd patchbeheer geüpdatet

7.5 Uitvoeren van geautomatiseerde kwetsbaarheidsscans van interne bedrijfsmiddelen

Vragen:

- Worden er scans uitgevoerd voor kwetsbaarheden in interne bedrijfsmiddelen?
    - Zijn de scans geautomatiseerd?
    - Hoeveel tijd zit er tussen scans?
- Wordt er gebruikgemaakt van zowel geauthentiseerde als niet-geauthentiseerde SCAP-conforme tools voor het scannen van kwetsbaarheden binnen het interne netwerk.

Criteria:

- Er wordt minstens één keer per kwartaal een SCAP-conforme scan tool gebruikt om kwetsbaarheden te scannen, voor zowel geauthentiseerde als niet-geauthentiseerde scans.

7.6 Uitvoeren van geautomatiseerde kwetsbaarhedenscans van extern benaderbare bedrijfsmiddelen.

Vragen:

- Word er gescand naar kwetsbaarheden van extern blootgestelde bedrijfsmiddelen met een SCAP-conforme tool?
    - Is dit een automatisch proces?
    - Hoe vaak gebeurt dit proces?

Criteria:

- Er wordt automatisch gescand naar kwetsbaarheden van extern blootgestelde bedrijfsmiddelen met een SCAP-conforme tool.
    - Dit gebeurt maandelijks of vaker.

7.7 Herstellen van gedetecteerde kwetsbaarheden

Vragen:

- Hoe snel worden gedetecteerde kwetsbaarheden verholpen?
    - Word dit gedaan op basis van een beschreven proces?
- Wordt er ook actie ondernomen wanneer kwetsbaarheden maandelijks of vaker gedetecteerd worden in software.
    - Wordt dit ook verholpen met behulp van processen en hulpmiddelen van het herstelproces?

Criteria:

- Maandelijks of vaker gedetecteerde kwetsbaarheden in software worden verholpen door processen en hulpmiddelen op basis van het herstelproces.

8. Beheer van auditlogs

Rationale:

Verzamelen, waarschuwen, beoordelen en bewaren van auditlogs van gebeurtenissen die kunnen helpen bij het detecteren, begrijpen of herstellen van een aanval.

8.1 Opzetten en onderhouden van een proces voor het beheer van auditlogs

Vragen:

- Is er een auditlog managementproces?
  - Welke logging eisen zijn hierin opgenomen?
  - Hoe vaak wordt deze documentatie herzien?

Criteria:

- Er is een auditlog managementproces gedocumenteerd dat de logging eisen van de onderneming definieert.
- Het auditlog managementproces benoemt eisen voor het verzamelen, beoordelen en bewaren van auditlogs (van bedrijfsmiddelen).
- De documentatie wordt jaarlijks herzien of bijgewerkt, of wanneer er belangrijke changes zijn.

8.2 Verzamelen van audit logs

Vragen:

- Worden er auditlogs verzameld vanuit bedrijfsmiddelen?
- Worden deze auditlogs verzameld in compliance met het auditlog managementproces?

Criteria:

- Er worden auditlogs verzameld op (alle) bedrijfsmiddelen.
- De auditlogs worden verzameld volgens het auditlog managementproces.

8.3 Zorgen voor adequate opslag van audit logs

Vragen:

- Worden er auditlogs opgeslagen op een opslagmedium met voldoende ruimte voor (grote) logfiles?
- Voldoet de opslaglocatie aan het auditlog managementproces?

Criteria:

- Auditlogs worden opgeslagen op een opslagmedium (logbestemming) met voldoende vrije opslagruimte, volgens het auditlog managementproces.

8.4 Standaardiseer tijdsynchronisatie

Vragen:

- Wordt er een standaard tijdsbron gebruikt voor alle bedrijfsmiddelen?
- Is er een back-up voor de standaard tijdsbron?

Criteria:

- Bedrijfsmiddelen worden voorzien van dezelfde tijdsynchronisatie.

- Er wordt gebruikgemaakt van meerdere tijdsbronnen (*waar ondersteund*).

8.5 Verzamel gedetailleerde auditlogs

Vragen:

- Worden er gedetailleerde auditlogs verzameld op bedrijfsmiddelen die gevoelige gegevens bevatten?
- Wat wordt er dan gelogd?

Criteria:

- Er worden gedetailleerde auditlogs verzameld van alle bedrijfsmiddelen die gevoelige gegevens bevatten.
- De auditlogs bevatten ten minste: gebeurtenisbron, datum, gebruikersnaam, tijdstempel, bronadressen, bestemmingsadressen (en andere nuttige elementen voor forensisch onderzoek).

8.6 Verzamelen van DNS query auditlogs

Vragen:

- Worden er DNS query auditlogs verzameld van bedrijfsmiddelen (zo ja, welke)?

Criteria:

- DNS query auditlogs worden verzameld van bedrijfsmiddelen, waar nodig en ondersteund.

8.7 Verzamelen van URL request auditlogs

Vragen:

- Worden er URL request auditlogs verzameld van bedrijfsmiddelen (zo ja, welke)?

Criteria:

- URL request auditlogs worden verzameld van bedrijfsmiddelen, waar nodig en ondersteund.

8.8 Verzamelen van Command-Line (CLI) auditlogs

Vragen:

- Worden er CLI (PowerShell/BASH) auditlogs verzameld van bedrijfsmiddelen (zo ja, welke)?

Criteria:

- CLI-auditlogs worden verzameld van bedrijfsmiddelen, waar nodig en ondersteund.

8.9 Centraliseer auditlogs

Vragen:

- Worden er auditlogs verzameld op een centrale locatie?

Criteria:

- Er worden auditlogs verzameld op een centrale locatie.
- De auditlogs worden verzameld volgens het auditlog managementproces.

8.10 Auditlogs bewaren

Vragen:

- Worden auditlogs opgeslagen?
    - Hoe lang worden auditlogs bewaard?

Criteria:

- Auditlogs worden ten minste 90 dagen bewaard.

8.11 Audit logs controleren

Vragen:

- Worden auditlogs ook periodiek gecontroleerd? (handmatig/ logcorrelation tool/ SIEM).
- Hoe vaak worden deze auditlogs gecontroleerd?

Criteria:

- Auditlogs worden, ten minste wekelijks, gecontroleerd om zo abnormale gebeurtenissen op te kunnen sporen.

8.12 Logs van serviceproviders verzamelen

Vragen:

- Worden auditlogs van serviceproviders verzameld?
- Wat wordt er gelogd?

Criteria:

- Er worden auditlogs van serviceproviders verzameld.
- Er worden bijvoorbeeld authenticatie- en autorisatie-events, events voor het creëren en verwijderen van gegevens en/of events voor gebruikersbeheer gelogd.

9. Bescherming van e-mail en webbrowsers

Rationale:

Betere bescherming en detectie van bedreigingen vanuit e-mail- en webbrowsers, aangezien dit kansen zijn voor aanvallers om menselijk gedrag te manipuleren via directe betrokkenheid.

9.1 Ervoor zorgen dat alleen volledig ondersteunde browsers en e-mailclients worden gebruikt.

Vragen:

- Wordt ervoor gezorgd dat alleen ondersteunde browsers gebruikt (kunnen) worden?
- Wordt de browser periodiek geüpdatet?
- Wordt ervoor gezorgd dat alleen ondersteunde e-mailclients gebruikt (kunnen) worden?
- Is de mail client up to date?

Criteria:

- Er wordt voor gezorgd dat alleen volledig ondersteunde browsers en e-mailclients in de onderneming mogen worden gebruikt.
- Alleen de nieuwste versie van de door de leverancier geleverde browsers en e-mailclients mag worden gebruikt.

9.2 DNS-filterdiensten gebruiken

Vragen:

- Is op alle apparaten standaard een DNS-filterdienst geconfigureerd om de toegang tot kwaadaardige domeinen te blokkeren?

Criteria:

- Op alle apparaten zijn de DNS-filterdienst instellingen geconfigureerd.

9.3 Netwerk gebaseerde URL-filters onderhouden en afdwingen

Vragen:

- Zijn er network-based URL-filters ingesteld op alle bedrijfsmiddelen?

Criteria:

- Network-based URL-filters worden gehandhaafd om de verbinding van bedrijfsmiddelen met potentieel schadelijke of niet-goedgekeurde websites te beperken.
- De URL-filters worden periodiek geüpdatet.
  Voorbeeld: filtering op basis van categorie, filtering op basis van reputatie of door het gebruik van blokkadelijsten.
- Filters worden afgedwongen voor alle bedrijfsmiddelen.

9.4 Onnodige of onbevoegde uitbreidingen van browsers en e-mailclients beperken

Vragen:

- Vind er management plaats op het gebied van plugins/add-ons voor browsers en e-mailclients?

Criteria:

- Beperk, door het verwijderen of uitschakelen, alle ongeautoriseerde of onnodige plugins, extensies en add-on toepassingen van browsers of e-mailclients.

9.5 DMARC implementeren

Vragen:

- Wordt er gebruikgemaakt van een DMARC-beleid?
- Wordt er gebruikgemaakt van SPF?
- Wordt er gebruikgemaakt van DKIM?

Criteria:

- Er wordt gebruikgemaakt van een DMARC-beleid.
- Er wordt gebruikgemaakt van SPF.
- Er wordt gebruikgemaakt van DKIM.

9.6 Onnodige bestandstypen blokkeren

Vragen:

- Worden onnodige bestandstypes geblokkeerd in de mailomgeving?

Criteria:

- Onnodige bestandstypes worden geblokkeerd in de mailomgeving.

9.7 Anti-malwarebescherming voor mailservers implementeren en onderhouden

Vragen:

- Is er anti-malwarebescherming voor mailservers geïmplementeerd?
- Wordt deze ook onderhouden?

Criteria:

- Er is anti-malwarebescherming geconfigureerd op de mailservers.

10. Bescherming tegen malware

Rationale:

De installatie, verspreiding en uitvoering van kwaadaardige toepassingen, code of scripts op bedrijfsmiddelen voorkomen of controleren.

10.1 Anti-Malware software implementeren en onderhouden

Vragen:

- Wordt op apparaten gebruikgemaakt van anti-malware software?
  - Wordt deze software regelmatig onderhouden (updates)?

Criteria:

- Anti-malware software is geïmplementeerd op alle bedrijfsmiddelen.
- De anti-malware software wordt regelmatig gecontroleerd op updates.

10.2 Automatische updates van anti-malwarehandtekeningen configureren

Vragen:

- Zijn automatische updates ingeschakeld voor anti-malware handtekeningbestanden?

Criteria:

- Automatische updates zijn geconfigureerd voor de anti-malware handtekeningbestanden op alle bedrijfsmiddelen.

10.3 Autorun en Autoplay uitschakelen voor verwijderbare media

Vragen:

- Staat Autoplay uitgeschakeld voor verwijderbare media? (USB etc.)

Criteria:

- Automatisch starten en automatisch afspelen van verwijderbare media is uitgeschakeld.

10.4 Automatisch scannen van verwijderbare media door Anti-Malware te configureren

Vragen:

- Is er automatische anti-malware scanning voor verwijderbare media aanwezig?

Criteria:

- Anti-malware software is geconfigureerd om automatisch verwijderbare media te scannen.

10.5 Anti-exploitatiefuncties inschakelen

Vragen:

- Hebben alle bedrijfsmiddelen (en software) anti-exploitatiefuncties ingeschakeld?
  Voorbeeld: Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) of Apple® System Integrity Protection (SIP) en Gatekeeper™.

Criteria:

- Waar mogelijk zijn anti-exploitatiefuncties ingeschakeld op bedrijfsmiddelen en software.
  Voorbeeld: Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) of Apple® System Integrity Protection (SIP) en Gatekeeper™.

10.6 Anti-Malware software centraal beheren

Vragen:

- Wordt de anti-malware software centraal beheerd?

Criteria:

- Anti-malware software wordt centraal beheerd.

10.7 Behavior-based anti-malware software gebruiken

Vragen:

- Wordt er behavior-based anti-malware software gebruikt op alle systemen?

Criteria:

- Er wordt gebruikgemaakt van behavior-based anti-malware software gebruiken.

11. Gegevensherstel

Rationale: *Vaststellen en handhaven van praktijken voor gegevensherstel die toereikend zijn om de bedrijfsmiddelen binnen de reikwijdte van het incident en de vertrouwde staat te herstellen.*

11.1 Een proces voor gegevensherstel opzetten en onderhouden

Vragen:

- Is er een proces voor gegevensherstel?
- Wat omvat dit proces?
- Hoe vaak wordt de documentatie van dit proces bijgewerkt?

Criteria:

- Er is een proces voor gegevensherstel opgezet (en wordt onderhouden).
- Het proces bevat: de omvang van gegevensherstelactiviteiten, herstelprioriteiten en de beveiliging van back-upgegevens.
- De documentatie wordt minimaal jaarlijks herzien en bijgewerkt, of bij belangrijke veranderingen.

11.2 Geautomatiseerde back-ups uitvoeren

Vragen:

- Worden er geautomatiseerd back-ups uitgevoerd van bedrijfsmiddelen?

Criteria:

- Automatische back-ups uitvoeren van bedrijfsmiddelen.
- Back-ups worden wekelijks of vaker uitgevoerd, afhankelijk van de gevoeligheid van de gegevens.

11.3 Bescherm back-up gegevens

Vragen:

- Worden herstelgegevens beschermd?
- Wordt er gebruikgemaakt van encryptie voor back-ups?
- Wordt er gebruikgemaakt van scheiding van gegevens?

Criteria:

- Herstelgegevens worden beschermd met gelijkwaardige controles als de oorspronkelijke gegevens.
- Er wordt gebruikgemaakt van encryptie en/of scheiding van gegevens.

11.4 Een geïsoleerde kopie van back-ups maken en onderhouden

Vragen:

- Zijn er geïsoleerde kopieën van de back-ups aanwezig?

Criteria:

- Er is een geïsoleerde instantie van herstelgegevens gecreëerd en wordt onderhouden.
  Voorbeeld: versiebeheer van back-up bestemmingen via offline, cloud, of off-site systemen of diensten.

11.5 Testen van back-ups

Vragen:

- Hoe vaak worden back-ups getest?
- Op welke wijze worden back-ups getest?

Criteria:

- Elk kwartaal, of vaker, wordt het herstel van de back-up getest door een steekproef van bedrijfsmiddelen binnen het bereik.

12. Beheer van de netwerkinfrastructuur

Rationale: *Netwerkapparatuur opzetten, implementeren en actief beheren (opsporen, rapporteren, corrigeren) om te voorkomen dat aanvallers misbruik maken van kwetsbare netwerkdiensten en toegangspunten.*

12.1 Ervoor zorgen dat de netwerkinfrastructuur up-to-date is

Vragen:

- Wordt netwerkinfrastructuur up-to-date gehouden?
- Hoe vaak wordt deze geüpdatet?

Criteria:

- De netwerkinfrastructuur wordt up-to-date gehouden.
  Voorbeeld: gebruikmaken van de laatste stabiele release van software en/of het gebruik van momenteel ondersteunde network-as-a-service (NaaS) aanbiedingen.
- Softwareversies worden maandelijks of vaker gecontroleerd om de softwareondersteuning te garanderen.

12.2 Een veilige netwerkarchitectuur opzetten en onderhouden

Vragen:

- Hoe wordt de veiligheid van de netwerkarchitectuur gegarandeerd?

Criteria:

- Er is een veilige netwerkarchitectuur opgezet en deze wordt onderhouden.
  Een veilige netwerkarchitectuur moet minimaal gericht zijn op segmentatie, minimale privileges en beschikbaarheid.

12.3 Veilig beheren van de netwerkinfrastructuur

Vragen:

- Is de netwerkinfrastructuur (goed) beveiligd door gebruik te maken van veilige protocollen en versies?

Criteria:

- De netwerkinfrastructuur is beveiligd.
  Voorbeelden van implementaties zijn versie-gecontroleerde infrastructuur-als-code en het gebruik van veilige netwerkprotocollen, zoals SSH en HTTPS.

12.4 Architectuurschema('s) opstellen en onderhouden

Vragen:

- Zijn er architectuurdiagrammen en/of documentatie over netwerksystemen?
- Hoe vaak wordt deze documentatie herzien?

Criteria:

- Er zijn architectuurdiagrammen en/of andere documentatie over netwerksystemen.

- Documentatie en diagrammen worden jaarlijks herzien/geactualiseerd, of bij belangrijke changes.

12.5 Centraliseren van netwerkauthenticatie, -autorisatie en -auditing (AAA)

Vragen:

- Is netwerkauthenticatie, -autorisatie en -auditing gecentraliseerd?

Criteria:

- Netwerkauthenticatie, -autorisatie en -auditing (AAA) is gecentraliseerd.

12.6 Gebruik van veilige netwerkbeheer- en communicatieprotocollen

Vragen:

- Wordt er gebruikgemaakt van veilige netwerkbeheer- en communicatieprotocollen zoals WPA2 (Enterprise), WPA3 en/of 802.1X?

Criteria:

- Veilige netwerkbeheer- en communicatieprotocollen worden gebruikt.
  Denk bijvoorbeeld aan 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise of hoger.

12.7 Ervoor zorgen dat externe apparaten een VPN gebruiken en verbinding maken met de AAA-infrastructuur van de onderneming.

Vragen:

- Maken gebruikers gebruik van een VPN voor externe toegang?
- Moeten gebruikers zich authentiseren via de AAA-infrastructuur van de onderneming?

Criteria:

- Er wordt geëist dat gebruikers zich authentiseren bij de, door de onderneming beheerde, VPN- en authenticatiediensten alvorens toegang te krijgen tot bedrijfsmiddelen op eindgebruikersapparaten.

12.8 Dedicated computers voor alle administratieve werkzaamheden

Vragen:

- Worden er speciale computers gebruikt voor administratieve werkzaamheden?
- Zijn deze speciale computers gescheiden van het primaire netwerk?
- Zijn deze speciale computers afgesloten van het internet?

Criteria:

- Er worden speciale computers gebruikt (en onderhouden), fysiek of logisch gescheiden, voor alle administratieve taken of taken die administratieve toegang vereisen.
- De computers worden gescheiden van het primaire netwerk van de onderneming en mogen geen toegang hebben tot het internet.

13. Netwerkbewaking en -verdediging

Rationale: *Maak gebruik van processen en hulpmiddelen voor het opzetten en onderhouden van uitgebreide netwerkbewaking en verdediging tegen veiligheidsbedreigingen in de netwerkinfrastructuur en het gebruikersbestand van de onderneming.*

13.1 Bij securityevents centraal waarschuwen

Vragen:

- Word er gebruikgemaakt van een SIEM?
    - Staan in de SIEM ook door de leverancier ook gedefinieerde event correlatie-waarschuwingen in?
    - **Zo niet,** word er gebruikgemaakt van een ander soort centrale logboekanalyse?

Criteria:

- Waarschuwingen voor beveiligingsgebeurtenissen in alle bedrijfsmiddelen voor logboekcorrelatie en -analyse worden gecentraliseerd.
- Best-practice implementatie is het gebruik van een SIEM, met door de leverancier gedefinieerde event correlatie-waarschuwingen.
- Een platform voor logboekanalyse dat is geconfigureerd met voor de beveiliging relevante correlatiemeldingen voldoet ook aan deze waarborg (bij afwezigheid van een SIEM).

13.2 Gebruik een host-based oplossing voor inbraakdetectie

Vragen:

- Is er inbraakdetectie op host-niveau?

Criteria:

- Er is een hostgebaseerde oplossing geïmplementeerd voor inbraakdetectie op bedrijfsmiddelen, waar nodig en/of ondersteund.

13.3 Gebruik inbraakdetectiesystemen in het netwerk

Vragen:

- Wordt er gebruikgemaakt van een inbraakdetectiesysteem in het netwerk?

Criteria:

- Gebruik van een oplossing voor netwerkintrusiedetectie op bedrijfsmiddelen, indien van toepassing.
  Voorbeeld: het gebruik van een Network Intrusion Detection System (NIDS) of een gelijkwaardige cloud serviceprovider (CSP) dienst.

13.4 Filteren van verkeer tussen netwerksegmenten

Vragen:

- Worden netwerken gesegmenteerd?
- Wordt verkeer tussen segmenten gefilterd?

Criteria:

- Filtreren van verkeer tussen netwerksegmenten, waar nodig.

13.5 Beheer van toegangscontrole voor externe activa

Vragen:

- Word er toegangscontrole uitgevoerd op externe verbindingen?
    - Zo ja, wat voor soort beveiliging?

Criteria:

- Beheer van toegangscontrole voor middelen die op afstand verbinding maken met bedrijfsmiddelen.
- Bepaal de hoeveelheid toegang tot bedrijfsmiddelen op basis van:
    - up-to-date anti-malware software geïnstalleerd.
    - Configuratie volgens/ in overeenstemming met het beveiligde configuratieproces van de onderneming.
    - Dat het besturingssysteem en de toepassingen up-to-date zijn.

13.6 Verzamelen van logbestanden over netwerkverkeer

Vragen:

- Hoe wordt het netwerkverkeer gemonitord?

Criteria:

- Logboeken van netwerkverkeer en/of netwerkverkeer verzamelen om te beoordelen
- Waarschuwen op basis van gegevens/logs van netwerkapparaten.

13.7 Inzet van een hostgebaseerde inbraakpreventieoplossing

Vragen:

- Wordt er gebruikgemaakt van een host-based intrusion prevention-oplossing op bedrijfsmiddelen?
    - *Denk aan: EDR-client of IPS-agent.*

Criteria:

- Inzetten van een host-based intrusion prevention-oplossing op bedrijfsmiddelen, waar nodig en/of ondersteund.
    - *Voorbeeld: een EDR-client (Endpoint Detection and Response) of een host-gebaseerde IPS-agent.*

13.8 Inzet van een netwerkinbraakpreventieoplossing

Vragen:

- Wordt er gebruikgemaakt van netwerkinbraakpreventie?
    - *Denk aan: NIPS of een vergelijkbare CSP-dienst*

Criteria:

- Implementeren van een oplossing voor netwerkinbraakpreventie, indien van toepassing.
    - *Voorbeeld: een Network Intrusion Prevention System (NIPS) of een gelijkwaardige CSP-dienst.*

13.9 Gebruik van toegangscontrole op poortniveau

Vragen:

- Is er toegangscontrole op poortniveau?
    - Zo ja, wat voor?

Criteria:

- Toegangscontrole op poortniveau wordt gebruikt.
    - Toegangscontrole op poortniveau maakt gebruik van 802.1x of soortgelijke protocollen voor netwerktoegangscontrole, zoals certificaten, en kan authenticatie van gebruikers en/of apparaten omvatten.

13.10 Filteren van de applicatielaag

Vragen:

- Is er een filter op applicatie niveau?
    - *Bijvoorbeeld: filterproxy, firewall of gateway.*

Criteria:

- Filtering op de toepassingslaag uitgevoerd.
    - *Voorbeeld: een filterproxy, firewall of gateway.*

13.11 Drempels voor beveiligingswaarschuwingen afstemmen

Vragen:

- Hoe vaak worden de alarmdrempels voor beveiligingsgebeurtenissen afgestemd?

Criteria:

- De alarmdrempels voor beveiligingsgebeurtenissen worden maandelijks of vaker afgesteld.

14. Security awareness en vaardigheidstraining

Rationale: *Een security awareness programma opzetten en onderhouden om het gedrag van het personeel zodanig te beïnvloeden dat het zich bewust is van de beveiliging en over de juiste vaardigheden beschikt om de risico's van cyberbeveiliging voor de onderneming te beperken.*

14.1 Een security awareness programma opzetten en onderhouden

Vragen:

- Is er een security awareness programma?
    - Hoe vaak wordt er training gegeven?
    - Wanneer wordt deze bijgewerkt?
    - Wordt deze ingezet bij de training van (nieuwe) medewerkers?

Criteria:

- Er is een security awareness programma.
    - Training wordt ten minste jaarlijks gegeven en bij in diensttreding.
    - Minstens jaarlijk herzien/ bijwerken (actualiseren), of bij belangrijke events.

14.2 Personeelsleden opleiden in het herkennen van social engineering-aanvallen

Vragen:

- Worden werknemers geleerd social-engineering aanvallen te herkennen?

Criteria:

- Werknemers wordt geleerd social-engineering aanvallen te herkennen, zoals phishing, pre-texting en tailgating.

14.3 Werknemers opleiden in best-practices op het gebied van authenticatie

Vragen:

- Wordt het personeel getraind in best practices op het gebied van authenticatie?

Criteria:

- Personeelsleden worden getraind over beste praktijken op het gebied van authenticatie. *Voorbeelden van onderwerpen zijn MFA, samenstelling van wachtwoorden en credential management.*

14.4 Opleiding van personeel over best-practices inzake gegevensverwerking

Vragen:

- Wordt het personeel getraind in het identificeren en correct opslaan, overdragen, archiveren en vernietigen van gevoelige gegevens?
- Wordt het personeel getraind in het “clean screen/desk” principe?
- Wordt het personeel getraind in het veilig opslaan van gegevens en bedrijfsmiddelen?

Criteria:

- Personeelsleden worden getraind over het identificeren en correct opslaan, overdragen, archiveren en vernietigen van gevoelige gegevens.
- Medewerkers worden getraind over best practices omtrent het “clean screen/desk” principe, *zoals het vergrendelen van hun scherm wanneer ze hun bedrijfsmiddelen verlaten, het wissen van fysieke en virtuele whiteboards aan het einde van vergaderingen en het veilig opslaan van gegevens en bedrijfsmiddelen.*

14.5 Train het personeel over de oorzaken van onbedoelde datalekken

Vragen:

- Wordt het personeel getraind om zich bewust te zijn van de oorzaken van onbedoelde gegevensblootstelling, zoals het verkeerd afleveren van gevoelige gegevens of het publiceren van gegevens aan een onbedoeld publiek?

Criteria:

- Personeelsleden worden getraind om zich bewust te zijn van de oorzaken van onbedoelde gegevensblootstelling, zoals het verkeerd afleveren van gevoelige gegevens, het verliezen van een draagbaar eindgebruikersapparaat of het publiceren van gegevens aan een onbedoeld publiek.

14.6 Train het personeel over het herkennen en melden van beveiligingsincidenten

Vragen:

- Wordt het personeel getraind in het herkennen van potentiële beveiligingsincidenten?
- Wordt het personeel getraind in het correct melden van beveiligingsincidenten?

Criteria:

- Het trainen van personeel om een potentieel incident te kunnen herkennen en een dergelijk incident te kunnen melden.

14.7 Train het personeel over het identificeren en rapporteren van ontbrekende beveiligingsupdates voor hun bedrijfsmiddelen

Vragen:

- Wordt het personeel opgeleid om te begrijpen hoe verouderde softwarepatches of storingen in geautomatiseerde processen en hulpmiddelen kunnen worden geverifieerd en gemeld?
- Is het een onderdeel van deze training het melden van storingen in geautomatiseerde processen en hulpmiddelen aan IT-personeel?

Criteria:

- Het personeel wordt opgeleid om te begrijpen hoe verouderde softwarepatches of storingen in geautomatiseerde processen en hulpmiddelen kunnen worden geverifieerd en gemeld.
- Onderdeel van deze training is het melden van storingen in geautomatiseerde processen en hulpmiddelen aan IT-personeel.

14.8 Leid het personeel op over de gevaren van verbinding met onveilige netwerken. Leid personeel op over de gevaren van verzending van bedrijfsgegevens via onveilige netwerken

Vragen:

- Wordt het personeel getraind over de gevaren van verbinding met en overdracht van gegevens via onveilige netwerken voor bedrijfsactiviteiten?
- *Als de onderneming werknemers op afstand heeft:* Bevat de training richtlijnen om ervoor te zorgen dat alle gebruikers hun thuisnetwerkinfrastructuur veilig configureren?

Criteria:

- Het personeel wordt getraind over de gevaren van verbinding met en overdracht van gegevens via onveilige netwerken voor bedrijfsactiviteiten.
- *Als de onderneming werknemers op afstand heeft:* De training bevat richtlijnen om ervoor te zorgen dat alle gebruikers hun thuisnetwerkinfrastructuur veilig configureren.

14.9 Uitvoering van rol specifieke training in security awareness en -vaardigheden

Vragen:

- Wordt er rol specifieke training in security awareness en -vaardigheden gegeven?
  Voorbeeld: cursussen voor veilig systeembeheer voor IT-professionals, OWASP® Top 10-bewustzijn en preventie van kwetsbaarheden voor ontwikkelaars van webtoepassingen, en geavanceerde social engineering-training voor prominente functies.

Criteria:

- Er wordt rol specifieke training in security awareness en -vaardigheden gegeven.
  Voorbeeld: cursussen voor veilig systeembeheer voor IT-professionals, OWASP® Top 10-bewustzijn en preventie van kwetsbaarheden voor ontwikkelaars van webtoepassingen, en geavanceerde social engineering-training voor prominente functies.

15. Beheer van dienstverleners

Rationale: *Een proces ontwikkelen om dienstverleners te evalueren die over gevoelige gegevens beschikken of verantwoordelijk zijn voor kritieke IT-platforms of -processen van een onderneming, om ervoor te zorgen dat deze dienstverleners deze platforms en gegevens naar behoren beschermen.*

15.1 Een inventaris van dienstverleners opstellen en bijhouden

Vragen:

- Heeft u een inventaris van alle dienstverleners die uw organisatie gebruikt?
- Wordt deze inventaris regelmatig bijgewerkt en onderhouden?

Criteria:

- Alle dienstverleners zijn geïdentificeerd en geregistreerd in een centrale inventaris.
- Informatie over elke dienstverlener, inclusief classificatie, contactgegevens, bedrijfscontact en diensten die zij leveren zijn up-to-date.
- De inventaris wordt jaarlijks gecontroleerd en bijwerkt wanneer nodig.

15.2 Opstellen en onderhouden van een beleid voor het beheer van dienstverleners

Vragen:

- Heeft uw organisatie een beleid voor het beheer van dienstverleners?
- Wat bevat dit beleid?
- Wordt dit beleid regelmatig geëvalueerd en bijgewerkt?

Criteria:

- Een (schriftelijk) beleid voor het beheer van dienstverleners is opgesteld.
- Het beleid wordt minimaal jaarlijks bijgewerkt.
- Het beleid heeft betrekking op de classificatie, inventarisatie, beoordeling, monitoring en beëindiging van de overeenkomst van dienstverleners.

15.3 Classificeren van dienstverleners

Vragen:

- Worden dienstverleners geclassificeerd op basis van risiconiveau?
- Hoe vaak wordt deze classificatie bijgewerkt?

Criteria:

- De classificatie van een dienstverlener omvat een of meer kenmerken, zoals gevoeligheid van de gegevens, gegevensvolume, beschikbaarheidseisen, toepasselijke regelgeving, inherent risico en beperkt risico.
- Classificaties worden jaarlijks bijgewerkt en herzien, of wanneer zich belangrijke veranderingen in de onderneming voordoen.

15.4 Ervoor zorgen dat contracten met dienstverleners beveiligingsvereisten bevatten

Vragen:

- Worden beveiligingsvereisten opgenomen in alle contracten met dienstverleners?
- Wordt er gecontroleerd of deze beveiligingsvereisten worden nageleefd?

Criteria:

- Contracten met dienstverleners bevatten beveiligingsvereisten.
  Voorbeeld: minimumeisen voor beveiligingsprogramma's, kennisgeving van beveiligingsincidenten en/of inbreuken op gegevens, eisen inzake gegevensversleuteling en verbintenissen inzake gegevensverwijdering.
- Deze beveiligingseisen moeten in overeenstemming zijn met het beleid van de onderneming inzake het beheer van dienstverleners.
- De contracten met dienstverleners worden jaarlijks beoordeeld om er zeker van te zijn dat de beveiligingsvereisten niet ontbreken.

15.5 Dienstverleners beoordelen

Vragen:

- Worden dienstverleners beoordeeld op basis van hun beveiligingspraktijken (en is hier een schriftelijk beleid voor)?
- Welke standaard wordt bij deze beoordeling gebruikt?
- Hoe vaak worden dienstverleners beoordeeld?

Criteria:

- Dienstverleners worden beoordeeld overeenkomstig het beleid van de onderneming inzake het beheer van dienstverleners.
- De reikwijdte van de beoordeling kan variëren op basis van de classificatie(s), en kan bestaan uit een beoordeling van gestandaardiseerde beoordelingsrapporten, zoals Service Organization Control 2 (SOC 2) en Payment Card Industry (PCI) Attestation of Compliance (AoC), aangepaste vragenlijsten, of andere passende rigoureuze processen.
- Dienstverleners worden minimaal jaarlijks of bij nieuwe en vernieuwde contracten opnieuw beoordeeld.

15.6 Toezicht houden op dienstverleners

Vragen:

- Wordt er regelmatig toezicht gehouden op dienstverleners (en is hier een schriftelijk beleid voor)?
- Worden eventuele tekortkomingen geïdentificeerd en aangepakt?

Criteria:

- Er wordt toezicht gehouden op dienstverleners overeenkomstig het beleid van de onderneming inzake het beheer van dienstverleners.
  Voorbeeld: periodieke herbeoordeling van de naleving door dienstverleners, het controleren van release notes van dienstverleners en dark web monitoring.

15.7 Dienstverleners veilig ‘buiten bedrijf’ stellen

Vragen:

- Worden dienstverleners veilig ‘buiten bedrijf’ gesteld als hun diensten niet langer nodig zijn?
- Is hier een schriftelijk beleid voor?

Criteria:

- De overeenkomst met dienstverleners wordt veilig beëindigd.
  Voorbeeld: deactiveren van gebruikers en dienstaccounts, het beëindigen van gegevensstromen en het veilig verwijderen van bedrijfsgegevens in de systemen van dienstverleners.
- Voor het bovenstaande is een schriftelijk beleid/procedure.

16. Beveiliging van applicaties/ software

Rationale: *Beheren van de beveiligingslevenscyclus van intern ontwikkelde, gehoste of aangeschafte software om zwakke plekken in de beveiliging te voorkomen, op te sporen en te herstellen voordat deze van invloed kunnen zijn op de onderneming.*

16.1 Een veilig ontwikkelingsproces voor applicaties vaststellen en handhaven

Vragen:

- Is er een veilig ontwikkelingsproces voor toepassingen opgezet?
- Wordt het ontwikkelingsproces onderhouden?
- Komen in het ontwikkelingsproces zaken aan de orde zoals: normen voor een veilig applicatieontwerp, veilige codeerpraktijken, opleiding van ontwikkelaars, beheer van kwetsbaarheden, beveiliging van code van derden en procedures voor het testen van de beveiliging van applicaties?
- Wordt de documentatie regelmatig bijgewerkt?

Criteria:

- Er is een veilig ontwikkelingsproces voor toepassingen opgezet.
- Het ontwikkelingsproces wordt onderhouden.
- In het ontwikkelingsproces komen zaken aan de orde zoals: normen voor een veilig applicatieontwerp, veilige codeerpraktijken, opleiding van ontwikkelaars, beheer van kwetsbaarheden, beveiliging van code van derden en procedures voor het testen van de beveiliging van applicaties.
- De documentatie wordt jaarlijks herzien en bijgewerkt, of wanneer zich belangrijke veranderingen in de onderneming voordoen.

16.2 Een proces opzetten en onderhouden om kwetsbaarheden in de software te aanvaarden en aan te pakken

Vragen:

- Is er een proces vastgesteld om meldingen van softwarekwetsbaarheden te aanvaarden en aan te pakken, met inbegrip van een middel voor externe entiteiten om meldingen te doen?
- Omvat het proces zaken zoals: een beleid voor de behandeling van kwetsbaarheden dat het meldingsproces identificeert, de verantwoordelijke partij voor de behandeling van kwetsbaarheidsmeldingen en een proces voor intake, toewijzing, herstel en hersteltests?
- Wordt er als onderdeel van het proces een systeem gebruikt voor het traceren van kwetsbaarheden?
- Bevat het systeem een classificatie van de ernst en metrieken voor het meten van de timing voor het identificeren, analyseren en verhelpen van kwetsbaarheden?
- Wat gebeurt er met betrekking tot kwetsbaarheden in programma's van derden?
- De documentatie wordt jaarlijks herzien en bijgewerkt, of wanneer zich belangrijke veranderingen in de onderneming voordoen.

Criteria:

- Er is een proces vastgesteld om meldingen van softwarekwetsbaarheden te aanvaarden en aan te pakken, met inbegrip van een middel voor externe entiteiten om meldingen te doen.
- Het proces omvat zaken zoals: een beleid voor de behandeling van kwetsbaarheden dat het meldingsproces identificeert, de verantwoordelijke partij voor de behandeling van kwetsbaarheidsmeldingen en een proces voor intake, toewijzing, herstel en hersteltests.
- Als onderdeel van het proces wordt een systeem gebruikt voor het traceren van kwetsbaarheden, met een classificatie van de ernst ervan en metrieken voor het meten van de timing voor het identificeren, analyseren en verhelpen van kwetsbaarheden.
- De documentatie wordt jaarlijks herzien en bijgewerkt, of wanneer zich belangrijke veranderingen in de onderneming voordoen.
- Ontwikkelaars van toepassingen van derden moeten dit beschouwen als een extern beleid dat helpt verwachtingen te stellen aan externe belanghebbenden.

16.3 Analyse van de oorzaak van vulnerabilities

Vragen:

- Worden er hoofdoorzaakanalyses uitgevoerd op beveiligingskwetsbaarheden?
- Is de analyse van de hoofdoorzaak, bij de beoordeling van kwetsbaarheden, het evalueren van onderliggende problemen die leiden tot kwetsbaarheden in code, en stelt het ontwikkelingsteams in staat verder te gaan dan alleen het verhelpen van afzonderlijke kwetsbaarheden wanneer deze zich voordoen?

Criteria:

- Hoofdoorzaakanalyses worden uitgevoerd op beveiligingskwetsbaarheden.
- Bij de beoordeling van kwetsbaarheden is de analyse van de hoofdoorzaak: het evalueren van onderliggende problemen die leiden tot kwetsbaarheden in code, en stelt het ontwikkelingsteams in staat verder te gaan dan alleen het verhelpen van afzonderlijke kwetsbaarheden wanneer deze zich voordoen.

16.4 Een inventaris van softwarecomponenten (van derde partijen) opstellen en beheren

Vragen:

- Is er een bijgewerkte inventaris/“stuklijst” opgesteld van componenten van derden die bij de ontwikkeling zijn gebruikt, alsmede van componenten die in de toekomst zullen worden gebruikt?
- Bevat de inventaris alle risico's die elk onderdeel van derden kan opleveren?
- Wordt de lijst ten minste maandelijks geëvalueerd om eventuele wijzigingen of updates van deze componenten te identificeren en wordt er gecontroleerd of de component nog steeds wordt ondersteund?

Criteria:

- Er is een bijgewerkte inventaris opgesteld van componenten van derden die bij de ontwikkeling zijn gebruikt, vaak "stuklijst" genoemd, alsmede van componenten die in de toekomst zullen worden gebruikt.
- De inventaris bevat alle risico's die elk onderdeel van derden kan opleveren.
- De lijst wordt ten minste maandelijks geëvalueerd om eventuele wijzigingen of updates van deze componenten te identificeren en er wordt gecontroleerd of de component nog steeds wordt ondersteund.

16.5 Gebruik van actuele en betrouwbare softwarecomponenten van derden.

Vragen:

- Worden er actuele en vertrouwde softwarecomponenten van derden gebruikt?
- Wordt er, waar mogelijk, gekozen voor gevestigde en bewezen frameworks en bibliotheken die voldoende beveiliging bieden?
- Zijn de componenten van derden gekocht van betrouwbare bronnen en/of geëvalueerd op kwetsbaarheden vóór gebruik?

Criteria:

- Actuele en vertrouwde softwarecomponenten van derden worden gebruikt.
- Er wordt, waar mogelijk, gekozen voor gevestigde en bewezen frameworks en bibliotheken die voldoende beveiliging bieden.
- De componenten van derden zijn gekocht van betrouwbare bronnen en/of geëvalueerd op kwetsbaarheden vóór gebruik.

16.6 Opzetten en onderhouden van een classificatiesysteem en proces voor kwetsbaarheden in toepassingen.

Vragen:

- Is er een systeem en proces voor de beoordeling van de ernst van kwetsbaarheden in toepassingen ingesteld, dat het gemakkelijker maakt prioriteiten te stellen bij het verhelpen van ontdekte kwetsbaarheden?
- Omvat dit proces tenminste het vaststellen van een minimumniveau van aanvaardbare beveiliging voor het vrijgeven van code of toepassingen?
  Urgentiewaarderingen bieden een systematische manier om kwetsbaarheden te triageren die het risicobeheer verbetert en ervoor zorgt dat de ernstigste bugs het eerst worden verholpen.
- Wordt het systeem en het proces tenminste jaarlijks herzien en geactualiseerd?

Criteria:

- Er is een systeem en proces voor de beoordeling van de ernst van kwetsbaarheden in toepassingen ingesteld, dat het gemakkelijker maakt prioriteiten te stellen bij het verhelpen van ontdekte kwetsbaarheden.
- Dit proces omvat tenminste het vaststellen van een minimumniveau van aanvaardbare beveiliging voor het vrijgeven van code of toepassingen. Urgentiewaarderingen bieden een systematische manier om kwetsbaarheden te triageren die het risicobeheer verbetert en ervoor zorgt dat de ernstigste bugs het eerst worden verholpen.
- Het systeem en het proces wordt tenminste jaarlijks herzien en geactualiseerd.

16.7 Gebruik standaard configuratie templates voor hardening van de applicatie infrastructuur.

Vragen:

- Worden er standaard templates gebruikt voor componenten van de applicatie-infrastructuur?
- Welke servers/services omvatten deze standaard templates?
- Wordt er toegestaan dat intern ontwikkelde software de configuratiehardening verzwakt?

Criteria:

- Er worden standaard, door de industrie aanbevolen, hardening-configuratiesjablonen voor componenten van de applicatie-infrastructuur.
- Deze standaard templates omvatten onderliggende servers, databases en webservers, en is van toepassing op cloud containers, Platform as a Service (PaaS)-componenten en SaaS-componenten.
- Er wordt niet toegestaan dat intern ontwikkelde software de configuratiehardening verzwakt.

16.8 Scheid productie- en niet-productiesystemen

Vragen:

- Is er een duidelijke scheiding tussen productie- en niet-productiesystemen?
- Hoe wordt deze scheiding gehandhaafd?

Criteria:

- Gescheiden omgevingen voor productie- en niet-productiesystemen worden gehandhaafd.

16.9 Ontwikkelaars opleiden in concepten van applicatiebeveiliging en veilig coderen

Vragen:

- Is er een training voor softwareontwikkelaars m.b.t. het schrijven van veilige code?
- Wat omvat deze training?
- Hoe vaak wordt deze training gegeven?

Criteria:

- Er is voor gezorgd dat alle softwareontwikkelaars training krijgen in het schrijven van veilige code voor hun specifieke ontwikkelomgeving en verantwoordelijkheden.
- De training omvat algemene beveiligingsprincipes en standaardpraktijken voor applicatiebeveiliging.
- Geef ten minste jaarlijks training en ontwerp een manier om de beveiliging binnen het ontwikkelingsteam te bevorderen en een beveiligingscultuur onder de ontwikkelaars op te bouwen.

16.10 Pas veilige ontwerpprincipes toe in applicatiearchitecturen

Vragen:

- Hoe wordt veiligheid ingebouwd in de (applicatie)architecturen?

Criteria:

- Er worden veilige ontwerpbeginselen toegepast in applicatiearchitecturen.
  Tot de veilige ontwerpbeginselen behoren het concept van de minste rechten en het afdwingen van bemiddeling om elke handeling van de gebruiker te valideren, waarbij het concept van "Never trust (user)input" wordt bevorderd. Voorbeeld: ervoor zorgen dat expliciete foutcontrole wordt uitgevoerd en gedocumenteerd voor alle invoer, inclusief voor grootte, gegevenstype en aanvaardbare bereiken of formaten. Veilig ontwerp betekent ook het minimaliseren van het aanvalsoppervlak van de applicatie-infrastructuur, zoals het uitschakelen van onbeschermde poorten en diensten, het verwijderen van onnodige programma's en bestanden, en het hernoemen of verwijderen van standaard accounts.

16.11 Gebruik gekeurde modules of diensten voor componenten van de applicatiebeveiliging

Vragen:

- Wordt er gebruikgemaakt van ‘gekeurde’ modules of diensten voor beveiligingscomponenten van toepassingen?
- Hoe worden deze modules of diensten gekeurd?
- Hoe wordt de encryptie gekeurd, welke encryptie wordt standaard gebruikt?

Criteria:

- Er wordt gebruikgemaakt van doorgelichte modules of diensten voor beveiligingscomponenten van toepassingen, zoals identiteitsbeheer, encryptie, en auditing en logging.
  Het gebruik van platformfuncties voor kritieke beveiligingsfuncties vermindert de werklast van ontwikkelaars en minimaliseert de kans op ontwerp- of implementatiefouten. Moderne besturingssystemen bieden effectieve mechanismen voor identificatie, authenticatie en autorisatie en stellen die mechanismen beschikbaar voor toepassingen.
- Er wordt alleen gebruikgemaakt van gestandaardiseerde, momenteel geaccepteerde en uitvoerig beoordeelde encryptie-algoritmen.
  Besturingssystemen bieden ook mechanismen om veilige audit logs aan te maken en bij te houden.

16.12 Beveiligingscontroles op codeniveau implementeren

Vragen:

- Worden er tools gebruikt om te checken of coderingspraktijken veilig zijn?

Criteria:

- Statische en dynamische analyse-instrumenten worden gebruikt tijdens de levenscyclus van toepassingen om na te gaan of veilige coderingspraktijken worden gevolgd.

16.13 Applicatiepentests uitvoeren

Vragen:

- Worden er regelmatig applicatiepentests uitgevoerd om kwetsbaarheden op te sporen?

Criteria:

- Voer penetratietests op toepassingen uit.
  Voor kritieke toepassingen zijn geauthentiseerde penetratietests beter geschikt om kwetsbaarheden in de bedrijfslogica op te sporen dan het scannen van codes en geautomatiseerde beveiligingstests. Penetratietests berusten op de vaardigheid van de tester om een applicatie handmatig te manipuleren als geauthentiseerde en niet-geauthentiseerde gebruiker.

16.14 Voer Threat Modeling uit

Vragen:

- Wordt er Threat Modeling gebruikt om de beveiliging van de applicaties te verbeteren?
- Wie voert Threat Modeling uit (heeft die persoon de juiste opleiding)?

Criteria:

- Threat Modeling wordt uitgevoerd.
  Threat Modeling is het proces van het identificeren en aanpakken van zwakke plekken in het beveiligingsontwerp van een toepassing, voordat code wordt gemaakt. Het wordt uitgevoerd door speciaal opgeleide personen die het applicatieontwerp evalueren en de beveiligingsrisico's voor elk toegangspunt en toegangsniveau inschatten. Het doel is de toepassing, architectuur en infrastructuur op een gestructureerde manier in kaart te brengen om de zwakke punten ervan te begrijpen.

17. Beheer van incidenten

Rationale: *Een programma opstellen voor het ontwikkelen en onderhouden van een responscapaciteit voor incidenten (bijv. beleid, plannen, procedures, gedefinieerde rollen, opleiding en communicatie) om een aanval voor te bereiden, op te sporen en er snel op te reageren.*

17.1 Aanwijzen van personeel voor incidentafhandeling

Vragen:

- Is er een team of individu aangewezen om beveiligingsincidenten af te handelen?
- Zijn de verantwoordelijkheden en taken van deze personen duidelijk gedefinieerd en begrepen?
- Hoe vaak wordt het beleid hiervan herzien?

Criteria:

- Er is tenminste één sleutelpersoon aangewezen, en ten minste één back-up, die het incident-afhandelingsproces van de onderneming zullen beheren.
- Het beheerpersoneel is verantwoordelijk voor de coördinatie tijdens incidenten.
- Het beheerpersoneel is verantwoordelijk voor documentatie van de reactie op incidenten.
- Het beheerpersoneel is verantwoordelijk voor het herstel van incidenten.
- Het beheerpersoneel bestaat uit interne werknemers van de onderneming, externe leveranciers of een hybride aanpak.
  Als er een externe leverancier gebruikt wordt, dan is er ten minste één persoon binnen de onderneming aangewezen om toezicht te houden op het werk van de derde partij.
- Jaarlijks wordt al het bovenstaande herzien, of wanneer zich belangrijke veranderingen in de onderneming voordoen (wijziging in het personeel bijvoorbeeld).

17.2 Vaststellen en bijhouden van contactinformatie voor het melden van beveiligingsincidenten

Vragen:

- Zijn er contactgegevens beschikbaar voor het melden van beveiligingsincidenten?
  - Van wie?
- Zijn deze contactgegevens up-to-date en hoe vaak worden deze gecontroleerd?

Criteria:

- Contactinformatie voor partijen die moeten worden geïnformeerd over beveiligingsincidenten is vastgesteld en wordt bijgehouden.
  Voorbeeld: interne medewerkers, externe verkopers, wetshandhavingsinstanties, aanbieders van cyberverzekeringen, relevante overheidsinstanties, partners van het Information Sharing and Analysis Center (ISAC) of andere belanghebbenden.
- De contacten worden jaarlijks geverifieerd om ervoor te zorgen dat de informatie up-to-date is.

17.3 Opzetten en onderhouden van een bedrijfsproces voor het melden van incidenten

Vragen:

- Is er een duidelijk proces voor het melden van beveiligingsincidenten?
- Wat omvat het proces?
- Is dit proces begrijpelijk en toegankelijk voor alle betrokkenen?
- Hoe vaak wordt dit proces geëvalueerd en bijgewerkt?

Criteria:

- Er is een bedrijfsproces vastgesteld voor het melden van beveiligingsincidenten door het personeel.
- Dit proces omvat: het tijdschema voor de rapportage, het personeel waaraan moet worden gerapporteerd, het mechanisme voor de rapportage en de minimaal te rapporteren informatie.
- De documentatie van het proces is voor alle werknemers openbaar.
- Deze documentatie en het proces wordt minimaal jaarlijks herzien, of wanneer zich belangrijke veranderingen in de onderneming voordoen.

17.4 Vaststellen en bijhouden van een Incident Response Proces

Vragen:

- Is er een gedetailleerd incident response proces vastgesteld en gedocumenteerd?
- Hoe vaak wordt dit proces geëvalueerd en bijgewerkt?

Criteria:

- Er is een gedocumenteerd incident response proces.
- Het incident response proces bevat rollen en verantwoordelijkheden, compliance eisen en een communicatieplan.
- Het proces wordt jaarlijks herzien, of wanneer zich belangrijke veranderingen in de onderneming voordoen.

17.5 Toewijzen van sleutelrollen en verantwoordelijkheden

Vragen:

- Zijn de sleutelrollen en verantwoordelijkheden binnen het incident response team duidelijk gedefinieerd?
    - Van wie?
- Hoe vaak wordt de rolverdeling en verantwoordelijkheden herzien?

Criteria:

- De belangrijkste rollen en verantwoordelijkheden voor het reageren op incidenten zijn toegewezen.
  Voorbeeld: medewerkers van juridische zaken, IT, informatiebeveiliging, faciliteiten, public relations, personeelszaken, incidentbestrijders en analisten, voor zover van toepassing.
- De rolverdeling en verantwoordelijkheden worden jaarlijks herzien, of wanneer zich belangrijke veranderingen in de onderneming voordoen.

17.6 Communicatiestrategieën definiëren voor tijdens het incident response proces

Vragen:

- Is er een duidelijke communicatiestrategie voor het incident response proces?
- Welke communicatiemogelijkheden worden er gebruikt?
- Wat wordt er gedaan als een communicatiemiddel niet werkt?
- Wanneer wordt deze strategie geëvalueerd en bijgewerkt?

Criteria:

- Bepaal welke primaire en secundaire mechanismen worden gebruikt om tijdens een beveiligingsincident te communiceren en te rapporteren.
  Voorbeeld: telefoongesprekken, e-mails of brieven.
- Er rekening mee gehouden dat bepaalde mechanismen, zoals e-mails, tijdens een beveiligingsincident kunnen worden beïnvloed.
- De communicatiestrategieën worden jaarlijks herzien, of wanneer zich belangrijke veranderingen in de onderneming voordoen.

17.7 Herhaaldelijk uitvoeren van incident response oefeningen

Vragen:

- Wordt het incident response proces regelmatig getest en geoefend?
- Wat wordt er precies getest?
- Hoe vaak wordt er getest?

Criteria:

- Routinematig worden incident response oefeningen en scenario's ingepland en uitgevoerd door belangrijk personeel dat betrokken is bij het incident response proces.
- De oefeningen testen communicatiekanalen, besluitvorming en workflows.
- Het bovenstaande gebeurt minimaal jaarlijks.

17.8 Het uitvoeren van evaluaties na een incident

Vragen:

- Wordt elk beveiligingsincident grondig geëvalueerd na afloop?
- Worden de bevindingen van deze evaluaties gebruikt om het incident response proces te verbeteren?

Criteria:

- Er wordt na elk incident een evaluatie uitgevoerd.
- De evaluatie is gestructureerd en grondig.
- Er worden maatregelen genomen op basis van de evaluatie.

17.9 Vaststellen en handhaven van drempelwaarden voor beveiligingsincidenten

Vragen:

- Zijn drempelwaarden voor beveiligingsincidenten vastgesteld en gedocumenteerd?
- Worden deze drempelwaarden regelmatig geëvalueerd en geactualiseerd om aan de veranderende bedrijfsomgeving te voldoen?

Criteria:

- Er is een formeel beleid voor het vaststellen van drempelwaarden voor beveiligingsincidenten.
- Er wordt ten minste onderscheid wordt gemaakt tussen een incident en een gebeurtenis. *Voorbeelden kunnen zijn: abnormale activiteit, beveiligingslek, zwakke plek in de beveiliging, gegevensinbreuk, privacyincident, enz.*
- Jaarlijks herzien, of wanneer zich belangrijke veranderingen in de onderneming voordoen.

18. Pentesten

Rationale: *Test de doeltreffendheid en veerkracht van bedrijfsmiddelen door zwakke plekken in controles (mensen, processen en technologie) op te sporen en uit te buiten, en de doelstellingen en acties van een aanvaller te simuleren.*

18.1 Opzetten en onderhouden van een programma voor pentesten

Vragen:

- Is er (bewijsbaar) een programma voor pentesten?
- Wordt er tijdens pentesten (hoofdzakelijk) gebruikgemaakt van externe partijen?
- Zijn de externe partijen gekwalificeerd op dit gebied?
- Welke penetratietest varianten wordt er gebruikt? (White/Gray/Black box)
- Wordt er tijdens penetratietests bedrijfs- en omgevingsverkenningen toegepast?
- Hoe vaak wordt het programma bijgehouden?

Criteria:

- Er is een programma voor pentesten.
- Er wordt tijdens de pentesten gebruikgemaakt van externe partijen.
- Externe partijen, betrokken bij een pentest, zijn hiervoor gekwalificeerd.
- Tijdens penetratietests wordt er bedrijfs- en omgevingsverkenningen toegepast.
- Het pentest programma wordt regelmatig bijgehouden en vernieuwd.

18.2 Periodieke externe penetratietests uitvoeren

Vragen:

- Hoe is het programma afgestemd op de eigenschappen van jullie organisatie?
- Wat omvat het pentestprogramma (documentatie)?

Criteria:

- Er is een programma voor pentesten.
- Het programma is afgestemd op de omvang, complexiteit en volwassenheid van de organisatie.
- Het pentestprogramma bevat de scope, controles op fysieke locaties, frequentie, beperkingen, contactpunt, herstel, interne routering van bevindingen en retrospective vereisten.

18.3 Herstellen van de bevindingen van de penetratietest

Vragen:

- Is er een beleid voor het herstellen van de bevindingen/ schade van een penetratietest?

Criteria:

- Er is een beleid voor het herstellen van de bevindingen/ schade van een penetratietest.
- Het beleid van het herstellen van bevindingen van een penetratietest is gebaseerd op de omvang en prioriteit van deze bevindingen.

18.4 Valideren van beveiligingsmaatregelen

Vragen:

- Worden beveiligingsmaatregelen na elke pentest gevalideerd?
- Zijn er al eens wijzigingen in beveiligingsmaatregelen doorgevoerd n.a.v. de resultaten van een pentest?

Criteria:

- De beveiligingsmaatregelen worden na elke pentest gevalideerd.
- Indien nodig worden regelsets en detectiemethoden aangepast om de gebruikte technieken in een test (beter) te kunnen herkennen.

18.5 Periodieke interne penetratietests uitvoeren

Vragen:

- Worden pentesten volgens de programmavereisten, periodiek uitgevoerd (Denk aan White box, Black box)?

Criteria:

- Pentesten worden ten minste jaarlijks uitgevoerd.