

BIJLAGE 12 INFORMATIEBEVEILIGINGSCOMPETENTIES KANTOORAUTOMATISERING-BEHEERPARTIJ

1. Basiskennis van IT security

Beschrijving: Het begrijpen van de fundamenteën van IT-beveiliging, inclusief de principes van vertrouwelijkheid, integriteit en beschikbaarheid (CIA).

Bepaling: Evalueren via certificeringen zoals CompTIA Security+ of basisopleiding in informatiebeveiliging.

2. Netwerkbeveiliging

Beschrijving: Kennis van netwerkarchitecturen, (web application)/(nextgen) firewalls, intrusion detection/prevention systems (IDS/IPS), VPN's en koppelen met en van relevante Cloudproducten en Security Operations Centum(s).

Bepaling: Toetsen door praktische tests en evaluaties van de vaardigheden in het configureren en beheren van netwerkbeveiligingsapparatuur.

3. Identiteits- en Toegangsbeheer (IAM)

Beschrijving: Beheer van gebruikersidentiteiten, authenticatie en toegangscontrole, inclusief het implementeren van rolgebaseerde toegang.

Bepaling: Analyse van ervaring met IAM-tools en het ontwikkelen van procedurele documentatie.

4. Gegevensbescherming en Encryptie

Beschrijving: Begrip van dataclassificatie, gegevensversleuteling en technieken voor gegevensbescherming.

Bepaling: Beoordelen door praktische ervaring in het implementeren van gegevensbeveiligingsmaatregelen.

5. Incident Response en Beheer

Beschrijving: Vaardigheden in het herkennen, onderzoeken en reageren op beveiligingsincidenten.

Bepaling: Evalueren via simulaties van incidenten en de ontwikkeling van procedures voor incidentrespons.

6. Veiligheid van Applicaties

Beschrijving: Kennis van softwarebeveiligingsprincipes, zoals codebeoordeling en het identificeren van kwetsbaarheden in web- en bedrijfsapplicaties.

Bepaling: Opleiding of ervaring in het testen van applicaties op beveiligingslekken (bijv. OWASP).

7. Compliance en Regelgeving

Beschrijving: Inzicht in relevante wet- en regelgeving, zoals GDPR, ISO 27001 en specifieke sectorvoorschriften.

Bepaling: Toetsen van kennis via training en het deelnemen aan compliance-audits.

8. Beleid en Procedures

Beschrijving: Ontwikkelen, implementeren en handhaven van beveiligingsbeleid en procedures voor Kantoorautomatisering.

Bepaling: Beoordelen van eerdere bijdragen aan het opstellen van beveiligingsrichtlijnen en -procedures.

9. Training en Bewustwording

Beschrijving: Vermogen om beveiligingsbewustzijn en training aan te bieden aan andere werknemers.

Bepaling: Toetsen via het ontwikkelen van trainingsprogramma's en het organiseren van workshops.

10. Monitoring en Evaluatie

Beschrijving: Competenties in het monitoren van systemen, loganalyse en het evalueren van beveiligingsmaatregelen.

Bepaling: Beoordelen door praktische ervaring met monitoringtools en rapportage.

Bepalingsmethodiek

Evaluatie van Huidige Vaardigheden: Voer een vaardighedeninventarisatie uit om het huidige niveau van competenties vast te stellen.

Opleidingsbehoefte Analyse: Beoordeel welke aanvullende trainingen of certificeringen nodig zijn op basis van de inventarisatie.

Praktische Toetsing: Organiseer tests of simulaties om vaardigheden in een realistischer scenario te beoordelen.

Feedback en Rapportage: Verzamel feedback van teamleden en leidinggevenden over de effectiviteit van de huidige bekendheid met beveiligingsprotocollen.

11. Risicobeheer

Beschrijving: Het vermogen om risico's te identificeren, te evalueren en te beheren met betrekking tot informatiesystemen. Dit omvat het uitvoeren van risicoanalyses en het ontwikkelen van strategieën om risico's te mitigeren.

Bepaling: inzage geven in het Information Security Management System (ISMS) en overleggen van risicoanalysemethodiek en (actuele) risicoanalyses.