**Afbeelding met Lettertype, Graphics, schermopname, tekst

Automatisch gegenereerde beschrijving**

**Roadmap**

Security Nederland

**Versiebeheer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Datum** | **Auteur** | **Omschrijving** |
| 0.1 | Concept | 5-9-2023 | Ludo Cuijpers  Leo Jaarsma  Henk Links  Sebastiaan van Trigt | Basisdocument |
|  |  |  |  |  |

**Vastgesteld door Security Nederland:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| 1.0 |  |  | College van Bestuur |

**Sommige rechten voorbehouden**

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en MBO Raad geen aansprakelijkheid voor eventuele fouten of onvolkomenheden.



Creative commons

MBO Raad 4.0 Nederland

(CC BY 4.0) **Copyright**

De gebruiker mag:

Het werk kopiëren, verspreiden en doorgeven

Remixen – afgeleide werken maken

Onder de volgende voorwaarde:

Naamsvermelding – De gebruiker dient bij het werk de naam van MBO Raad te vermelden (maar niet zodanig dat de indruk gewekt wordt dat zij daarmee instemt met uw werk of uw gebruik van het werk).

[Risico inventarisatie op basis van Cyberdreigingsbeeld 3](#_Toc144898198)

[Samenvatting 3](#_Toc144898199)

[Dreigingen en kwetsbaarheden permanent aanwezig 3](#_Toc144898200)

[Weerbaarheid blijft aandachtspunt 3](#_Toc144898201)

[Incidenten beter gedetecteerd maar nog niet altijd gedeeld 3](#_Toc144898202)

[Risicobeheer nog in de kinderschoenen 3](#_Toc144898203)

[Dashboard sectoraal beeld 2022 4](#_Toc144898204)

[Risicobeeld 2022 4](#_Toc144898205)

[Incidentbeeld in 2022 5](#_Toc144898206)

[Risicobeheer 5](#_Toc144898207)

[Ketenafhankelijkheid 5](#_Toc144898208)

[Capaciteitstekort 6](#_Toc144898209)

[Onveilig gedrag en gebrek aan awareness 6](#_Toc144898210)

[DPIA’s van verschillende applicaties 7](#_Toc144898211)

[Te mitigeren risico’s vanaf 2023 7](#_Toc144898212)

[2. Roadmap 2024 en 2025 8](#_Toc144898213)

# Risico inventarisatie op basis van Cyberdreigingsbeeld[[1]](#footnote-2)

## **Samenvatting**

Dreigingen en kwetsbaarheden permanent aanwezig

De laatste jaren verandert het beeld over dreigingen en kwetsbaarheden weinig. Ze worden vooral veroorzaakt door statelijke actoren, cybercriminelen, (h)acktivisten en mensen binnen organisaties die onbedoeld incidenten veroorzaken. Het aantal incidenten blijft nog steeds stijgen. Ook worden er steeds meer kwetsbaarheden gevonden in systemen en applicaties en blijven DDoS-aanvallen, phishing-mails en ransomware-aanvallen aan de orde van de dag.

Weerbaarheid blijft aandachtspunt

De professionaliteit van kwaadwillenden ontwikkelt zich vaak sneller dan de snelheid waarmee instellingen hun weerbaarheid kunnen verbeteren. De snelheid waarmee nieuwe aanvalstechnieken worden ontwikkeld is aanzienlijk en zorgt voor permanente uitdaging om bij te blijven. De metingen die SURF uitvoert op procesvolwassenheid, internetveiligheid en awareness, laten zien dat weerbaarheid een aandachtspunt blijft. Het besef groeit dat niet alleen de interne processen en systemen op orde moeten zijn, maar dat ook het menselijk handelen en processen voor samenwerkingsverbanden, ketenpartners en leveranciers aan passende richtlijnen moeten voldoen.

Incidenten beter gedetecteerd maar nog niet altijd gedeeld

Instellingen worden beter in het detecteren van incidenten, zeker nu steeds meer instellingen monitoring en detectie inrichten of uitbesteden. Toch nemen instellingen tijdens een incident niet altijd contact op met SURFcert. Niet alleen kan SURFcert ondersteuning bieden, maar kunnen zij ook de (technische) informatie over het incident delen om andere instellingen voor eenzelfde lot te behoeden.

Risicobeheer nog in de kinderschoenen

Er zijn nog maar weinig instellingen die risico gebaseerd werken. Risico eigenaarschap is nog beperkt ingebed bij het hogere management. Functionarissen die risico-eigenaren moeten ondersteunen zijn vaak nog niet goed in positie gebracht en worden gehinderd door capaciteitsproblemen. Toch zien we dat bestuurders steeds meer betrokken zijn en in de hele sector worden verbeterprogramma’s uitgevoerd.

## Dashboard sectoraal beeld 2022

Risicobeeld 2022

Ten opzichte van het vorige dreigingsbeeld valt op dat dit jaar geen van de risicocategorieën als ‘zeer hoog’ wordt ingeschat. Daarnaast zijn er twee nieuwe categorieën toegevoegd: Onveilig gedrag en gebrek aan awareness en Capaciteitstekort.

Afbeelding met tekst, schermopname, nummer, Lettertype

Automatisch gegenereerde beschrijving

Incidentbeeld in 2022

In 2022 hebben er incidenten plaatsgevonden in alle risicocategorieën uit het Cyberdreigingsbeeld van 2021-2022

Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving

## Risicobeheer

Het algemene beeld voor heel Nederland is helder in de Nederlandse Cybersecurity Strategie: ‘Risicomanagement staat nog in de kinderschoenen’. Risicobeheer blijkt vaak organisatorisch complex te zijn, ook in onze sector. We zien dit terug in de SURFaudit benchmark, het instrument waarmee de compliance wordt gemeten tegen het SURFaudit toetsingskader informatiebeveiliging. De benchmark scores laten zien dat het volwassenheidsniveau van risicobeheer en governance bij de deelnemende leden nog niet op het geambieerde volwassenheidsniveau 3 is. Het volwassenheidsniveau van het domein risicobeheer is al twee metingen op rij de laagste van alle vijftien deelgebieden van het toetsingskader. Instellingen die bij risicobeheer op niveau 2 zijn, hebben wel beleid en processen voor (informatiebeveiliging)risicobeheer, maar gebruiken die voornamelijk bij grote projecten of als reactie op problemen. Informatie- en privacy risicobeoordeling op basis van organisatiedoelstellingen gebeurt op beperkte schaal. Daarbij is het eigenaarschap van risico’s slechts gedeeltelijk toegewezen aan senior managers.

Uit de survey blijkt dat bestuurders van de meeste instellingen met regelmaat rapportages over informatiebeveiliging en privacy ontvangen. Bij bijna de helft van de instellingen vindt daarbij elk kwartaal een dialoog plaats tussen het college van bestuur en de rapporterende functionaris. Er is weinig uniformiteit in de rapportagevormen: de respondenten van de survey rapporteren elk op hun eigen wijze aan verschillende gremia.

## **Ketenafhankelijkheid**

De categorie Ketenafhankelijkheid heette vorige jaar Afhankelijkheid van clouddiensten. We hebben de naam aangepast om een bredere lading te dekken. Respondenten gaven aan dat zij niet alleen met cloud-leveranciers, maar ook met andere leveranciers uitdagingen ervaren. Bovendien is het van belang om ook de risico’s bij samenwerkingen met partnerorganisaties te beheersen. Organisaties zijn digitaal verbonden en verweven, ook met samenwerkingspartners, leveranciers en overheden. Wanneer een van de partijen wordt getroffen door een incident, kan dat gevolgen hebben voor meerdere organisaties. En die gevolgen kunnen zich uitstrekken buiten informatiebeveiliging: toen in 2022 een leverancier van toegangspassen was getroffen door een incident, was dat niet alleen een datalek, maar was er ook een mogelijke impact op de fysieke beveiliging

## Capaciteitstekort

We hebben deze categorie dit jaar toegevoegd omdat het tekort aan mensen en kennis in de survey veelvuldig werd genoemd als een hoog tot zeer hoog urgent risico, dat ook andere risicocategorieën beïnvloedt: maar liefst 81% van de respondenten in de survey gaf aan dat hun instelling onvoldoende mensen heeft om informatiebeveiligings- en privacytaken uit te voeren. Tijdelijke inhuur van professionals lijkt dit probleem niet op te lossen omdat ook ict-dienstverleners kampen met personeelstekorten. Vacatures voor informatiebeveiliging en privacy zijn lastig te vervullen. Het probleem is niet beperkt tot informatieveiligheid, maar betreft de hele ict-sector. Door gebrek aan goed geschoolde en ervaren medewerkers kunnen instellingen niet groeien in weerbaarheid en cybervolwassenheid.

## **Onveilig gedrag en gebrek aan awareness**

De meerderheid van cyberincidenten vindt plaats als gevolg van onbedoeld onveilig handelen door mensen. Dit beeld is niet uniek voor onze sector. Voor veel mensen is het nog geen routine om basale cybersecuritymaatregelen toe te passen, of om daarbij hulp te vragen. Van medewerkers en studenten wordt verwacht dat zij weten hoe zij met ict moeten omgaan, terwijl niet iedereen daarin een basisniveau heeft. Bovendien kan hoge werkdruk leiden tot vergissingen. Uit de reacties van de respondenten bleek dat bepaalde soorten vergissingen binnen hun organisatie herhaaldelijk de oorzaak waren van incidenten:

• Fouten met het versturen van e-mails, waarbij persoonsgegevens bij de verkeerde ontvanger terecht komen.

• Klikken op linkjes in phishingmails en vervolgens accountgegevens invoeren op een malafide website.

• Een drive met documenten delen met personen die daartoe geen toegang nodig hebben.

• Het delen van inloggegevens.

• Onvoldoende kennis van autorisaties in een samenwerkingsomgeving.

• Vergissingen van ict-beheerders bij wijzigingen in systemen waardoor de autorisaties veranderen.

• Buiten de procedures om ict inkopen, waardoor de basismaatregelen voor privacy en informatiebeveiliging niet zijn geborgd.

De respondenten van de survey zijn het ermee eens dat structurele aandacht voor security en privacy onontbeerlijk is om een weerbare organisatie te zijn, en dat medewerkers hier een belangrijke rol in spelen. Een aantal respondenten geeft aan dat security en privacy nu te vrijblijvende thema’s zijn. Zij pleiten daarom voor het invoeren van bijvoorbeeld verplichte awareness trainingen en phishingtesten. De respondenten zien dit als een stok achter de deur; zij zijn zich ervan bewust dat collega's mogelijk minder gemotiveerd zijn door werkdruk, onduidelijke regels en gebrek aan interesse. Door awareness-activiteiten verplicht te maken, wordt voor de instelling ook duidelijk welke investering er van medewerkers verwacht wordt

## DPIA’s van verschillende applicaties

De bevindingen en aanbevelingen van de SIS (Studenten Informatie Systeem) en HR-applicaties geven aan de autorisatieprocedures niet op orde zijn. Deze aanbeveling sluit aan bij het 2e beschreven risico binnen het Cyberdreigingsbeeld (2. Identiteitsfraude).

Een ander risico, ook aangeven door de Onderwijsinspectie, zijn de bewaartermijnen.

Governance wordt meegenomen als 1e risico, immers een sluitende en werkbare governance is de voorwaarde om de overige risico’s te mitigeren. Nogmaals governance is de basis voor de mitigatie van de benoemde risico’s.

## Te mitigeren risico’s vanaf 2023

De volgende 5 risico’s zullen vanaf 2023 gemitigeerd worden:

De aanpak om te komen tot een laag risico wordt hieronder globaal beschreven. De bijlagen beschrijven de details.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **R1**  **Governance** | **R2**  **Ransomware** | **R3**  **Ketenafhankelijkheid** | **R4**  **Identiteitsfraude** | **R5**  **Bewaartermijnen** |
| 1 Strategie / Visie | **Governance** | **Governance** | **Governance** | **Governance** |
| 2 IBP Beleid | 1 Scholing | 1 Scholing | 1 Scholing | 1 Scholing |
| 3 Architectuur MORA/HORA | 2 Duidelijke afspraken met gebruikers | 2 Duidelijke afspraken met gebruikers | 2 Duidelijke afspraken met gebruikers | 2 Duidelijke afspraken met gebruikers |
| 4 Eigenaarschap | 3 Registreren van incidenten van gebruikers en SURFcert | 3 Inkoop als proceseigenaar benoemen | 3 Document voor Identity and Access Management (IAM) | 3 Veilig opslaan data |
| 5 Risk Management | 4 Implementeren van technische weerbaarheid (MFA, SOC SIEM, etc.) | 4 Uitvoeren van (pen-) testen en audits door SURF op kernapplicaties | 4 Toepassen van IAM door leidinggevenden en beheerders | 4 Classificatie van data |
| 6 Roadmap | 5 Implementeren en testen van Business Continuïteit (deelname OZON / NOZON) |  |  | 5 Verwijderen van data op basis van afspraken binnen de mbo sector (DSP) |

**Roadmap 2024-2025 wordt voortdurend gevolgd in de ISMS.**

# 2. Roadmap 2024 en 2025

Deze stap plot de NBA statements op de cyberdreigingsrisico’s. Bovendien wordt een volwassenheidsniveau aangegeven. Voorbeeld statement 11.4, Logging, vermeldt SIEM op niveau 5, vandaar dat dit statement als mitigerende maatregel op volwassenheidsniveau 5 gerealiseerd moet worden.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2 Ransomware** | **R3 Cloud computing** | **R4 Identiteitsfraude** | **R5 Bewaartermijnen** | **Kosten INDICATIEF** | **Q1 2024** | **Q2-2024** | **Q3-2024** | **Q4-2024** | **2025** | **Accountable (eigenaar)** | **Responsible (uitvoerder)** |
| **G01 Strategie** | 1.1 Strategie | **1** | **4** | **4** | **4** | **4** |  | ❸ |  |  | ❹ |  | College van Bestuur | Security officer |
| **G02 Beleid** | 1.2 Beleid | **2** | **4** | **4** | **4** | **4** |  | ❸ |  |  | ❹ |  | College van Bestuur | Security officer |
| **G03 Architectuur** | 1.4 Architectuur | **3** | **4** | **4** | **4** | **4** |  | ❷ |  | ❸ |  |  | College van Bestuur | Security officer |
| **G04 Eigenaarschap** | 2.1 Eigenaarschap, rollen, verantwoording en verantw. | **4** | **3** | **3** | **3** | **3** |  | ❷ | ❸ |  | ❹ |  | College van Bestuur | Security officer |
| 2.2 Functiescheiding | **5** | **3** | **3** | **3** | **3** |  | ❷ |  |  | ❸ |  | College van Bestuur | Security officer |
| **G05 Risk Management** | 3.1 Informatie risicomanagementframework | **6** | **3** | **3** | **3** | **3** |  | ❷ | ❸ |  |  |  | College van Bestuur | Security officer |
| 3.2 Risicobeoordeling | **7** | **3** | **3** | **3** | **3** |  | ❷ | ❸ |  |  |  | College van Bestuur | Security officer |
| 3.3 Plan voor behandeling en beperking van risico's | **8** | **3** | **3** | **3** | **3** |  | ❷ | ❸ |  |  |  | College van Bestuur | Security officer |
| **G06 Roadmap** | 1.3 Planning / Roadmap | **9** | **4** | **4** | **4** | **4** |  | ❷ |  | ❸ |  |  | College van Bestuur | Security officer |
| **G07 Assurance** | 1.5 Onafhankelijke toetsing | **10** | **4** | **4** | **4** | **4** |  | ❷ |  |  | ❸ | ❹ | College van Bestuur | Internal IT auditor |
| **P08 Human Resources** | 4.1 Werving | **11** |  |  |  |  |  | ❷ |  |  | ❸ |  | Hoofd HRM | Medewerker HRM |
| 4.2 Certificering, training en scholing | **12** |  |  |  |  |  | ❷ |  |  | ❸ |  | Hoofd HRM | Hoofd ICT |
| 4.3 Afhankelijkheid van individuen | **13** |  |  |  |  |  | ❷ |  |  | ❸ |  | Hoofd HRM | Hoofd ICT |
| 4.4 Verandering of beëindiging van functie | **14** |  |  |  |  |  | ❷ |  |  | ❸ |  | Hoofd HRM | Medewerker HRM |
| 4.5 Kennisdeling | **15** |  |  |  |  |  | ❷ |  |  | ❸ |  | Hoofd HRM | Hoofd ICT |
| 4.6 Veiligheidsbewustzijn | **16** | **4** | **4** | **4** | **4** | **2K** | ❷ |  |  | ❸ |  | Hoofd HRM | Medewerker HRM |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2 Ransomware** | **R3 Cloud computing** | **R4 Identiteitsfraude** | **R5 Bewaartermijnen** | **Kosten INDICATIEF** | **Q1 2024** | **Q2-2024** | **Q3-2024** | **Q4-2024** | **2025** | **Accountable (eigenaar)** | **Responsible (uitvoerder)** |
| **P09 ITIL** | 5.1 Identificatie en onderhoud van configuratie-items | **17** |  | **3** |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 5.2 Configuratiedatabase en baseline | **18** | **3** | **3** |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 6.1 Incident management | **19** | **3** |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 6.2 Incident escalatie | **20** | **3** |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 6.3 Incidentrespons op (cyber) beveiligingsincidenten | **21** | **3** |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 6.4 Probleemmanagement | **22** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 7.1 Normen en procedures voor aanpassingen | **23** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 7.2 Impact assessment, prioriteren en autoriseren | **24** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 7.3 Noodaanpassingen | **25** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 7.4 Testomgeving | **26** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 7.5 Testen van aanpassingen | **27** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 7.6 Promotie naar productie | **28** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Medewerder ITIL processen |
| 12.1 Fysieke beveiligingsmaatregelen | **29** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Hoofd Facilitair |
| 12.2 Beheer van fysieke toegangsrechten | **30** |  |  |  |  |  | ❸ |  |  |  |  | Hoofd ICT | Hoofd Facilitair |
| **P10 Data Management** | 8.1 Methodiek voor veilige softwareontwikkeling/implem. | **31** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd HRM | Security officer |
| 8.2 Toegang tot productieomgeving door ontwikkelaars | **32** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd HRM | Security officer |
| 8.3 Data conversie en/of migratie | **33** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd HRM | Externe projectleider |
| 9.1 Data (en systeem) eigenaarschap | **34** |  |  |  | **3** |  | ❷ | ❸ |  |  |  | Hoofd HRM | Security officer |
| 9.2 Classificatie | **35** |  |  |  | **3** |  | ❷ | ❸ |  |  |  | Hoofd HRM | Security officer |
| 9.3 Beveiligingseisen voor gegevensbeheer | **36** |  |  |  | **3** |  | ❷ | ❸ |  |  |  | Hoofd HRM | Security officer |
| 9.4 Inrichting van opslag en retentie | **37** |  |  |  | **3** | **50K** | ❷ |  |  |  | ❸ | Hoofd HRM | Applicatiebeheerder HRM |
| 9.5 Uitwisseling van (gevoelige) gegevens | **38** |  |  | **3** |  |  | ❷ | ❸ |  |  |  | Hoofd HRM | Security officer |
| 9.6 Verwijdering van data | **39** |  |  | **3** |  |  | ❷ | ❸ |  |  |  | Hoofd HRM | Hoofd ICT |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2 Ransomware** | **R3 Cloud computing** | **R4 Identiteitsfraude** | **R5 Bewaartermijnen** | **Kosten INDICATIEF** | **Q1 2024** | **Q2-2024** | **Q3-2024** | **Q4-2024** | **2025** | **Accountable (eigenaar)** | **Responsible (uitvoerder)** |
| **P11 IAM** | 10.1 Toegangsrechten | **40** |  |  | **3** |  |  | ❷ | ❸ |  |  |  | Hoofd Studentzaken | Applicatiebeheerder Osiris |
| 10.2 Administratie van toegangsrechten | **41** |  |  | **3** |  |  | ❷ | ❸ |  |  |  | Hoofd Studentzaken | Applicatiebeheerder Osiris |
| 10.3 Super Users | **42** |  |  | **3** |  |  | ❷ | ❸ |  |  |  | Hoofd Studentzaken | Security officer |
| 10.4 Noodtoegang (breek-het-glasprocedure) | **43** |  |  | **3** |  |  | ❷ | ❸ |  |  |  | Hoofd Studentzaken | Security officer |
| 10.5 Periodieke beoordeling van toegangsrechten | **44** |  |  | **3** |  |  | ❷ | ❸ |  |  |  | Hoofd Studentzaken | Security officer |
| **P12 Security Baselines** | 11.1 Security baselines | **45** | **4** | **4** | **4** | **4** |  | ❷ |  | ❸ |  | ❹ | College van Bestuur | Security officer |
| **P13 Business Continuity** | 14.1 Bedrijfscontinuïteitsplanning | **46** | **3** |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd Facilitair | Hoofd ICT |
| 14.2 Testen van Disaster recovery | **47** | **3** |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd Facilitair | Hoofd ICT |
| 14.3 Offsite back-upopslag | **48** | **3** |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd Facilitair | Hoofd ICT |
| 14.4 Gegevensreplicatie | **49** | **3** |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd Facilitair | Hoofd ICT |
| 14.5 Crisisbeheer | **50** | **3** |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd Facilitair | Hoofd ICT |
| **P14 Cloud Leveranciers** | 15.1 Service level overeenkomst | **51** |  | **3** |  |  |  | ❷ | ❸ |  |  |  | Hoofd Inkoop | Security officer |
| 15.2 Service level beheer | **52** |  | **3** |  |  |  | ❷ | ❸ |  |  |  | Hoofd Inkoop | Security officer |
| 15.3 Risicobeheer van leveranciers | **53** |  | **3** |  |  |  | ❷ | ❸ |  |  |  | Hoofd Inkoop | Security officer |
| 15.4 Interne beheersing bij derden | **54** |  | **3** |  |  |  | ❷ | ❸ |  |  |  | Hoofd Inkoop | Security officer |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Thema’s** | **Verwijzing naar NBA** | **#** | **R2 Ransomware** | **R3 Cloud computing** | **R4 Identiteitsfraude** | **R5 Bewaartermijnen** | **Kosten INDICATIEF** | **Q1 2024** | **Q2-2024** | **Q3-2024** | **Q4-2024** | **2025** | **Accountable**  **(eigenaar)** | **Responsible**  **(uitvoerder)** |
| **T15 MFA - Thuiswerken** | 11.2 Authenticatiemechanismes | **55** | **4** |  | **4** |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| 11.3 Mobiele apparaten en telewerken | **56** | **3** |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| **T16 SOC SIEM** | 11.4 Logging | **57** | **5** |  |  |  | **30K** | ❷ |  |  |  | **❺** | Hoofd ICT | Medewerker ICT |
| **T17 Pentesten** | 11.5 Testen van, inspectie van en toezicht op beveiliging | **58** | **3** |  |  |  | **20K** | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| **T18 Patchbeheer** | 11.6 Patchbeheer | **59** | **3** |  |  |  | **10K** | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| 11.7 Beheer van bedreigingen en kwetsbaarheden | **60** | **3** |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| **T19 Infrastructuur** | 11.8 Beschikbaarheid en bescherming van infrastructuur | **61** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| 11.9 Onderhoud van de infrastructuur | **62** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| **T20 Security Policy** | 11.10 Beheer van cryptografische sleutels | **63** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| 11.11 Network security | **64** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| 11.12 Beheersing van malware-aanvallen | **65** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| 11.13 Bescherming van beveiligingstechnologie | **66** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Security officer |
| **T21 Computer Operations** | 13.1 Job processing | **67** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| 13.2 Procedures voor back-up en herstel | **68** | **3** | **3** |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |
| 13.3 Capaciteits- en prestatiebeheer | **69** |  |  |  |  |  | ❷ | ❸ |  |  |  | Hoofd ICT | Medewerker ICT |

1. CYBERDREIGINGSBEELD 2023 ONDERWIJS EN ONDERZOEK, SURF Utrecht [↑](#footnote-ref-2)