****

**Security baselines**

Security Nederland

**Versiebeheer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Datum** | **Auteur** | **Omschrijving** |
| 0.1 | Concept | 1-7-2023 | Stijn Hoogervorst (NWO), Edwin Hubers (UvA), Paul Leeraert (AUMC), Jeffeny Hoogervorst (TiU), Abdul Altawekji (SURF), Henry Meutstege (Saxion) | Bron |
| 0.2 | Concept | 7-7-2023 | Ludo Cuijpers, MBO Digitaal  Henk Links, MBO Digitaal | Aanvulling Security Baselines met NBA controls en Accountables |
|  |  |  |  |  |

**IT audit beoordeling is meegenomen in dit document omdat dit een SURF werkgroep document is. Separate audit is ook beschikbaar.**

**Vastgesteld door Security Nederland:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
|  |  |  |  |

**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).

[Inleiding 3](#_Toc144979124)

[Doel SURF security baseline 3](#_Toc144979125)

[Over de SURF security baseline 3](#_Toc144979126)

[Security baseline binnen vendor riskmanagement 3](#_Toc144979127)

[Aanvullingen MBO Digitaal 3](#_Toc144979128)

[IT audit beoordeling 10](#_Toc144979129)

# Inleiding[[1]](#footnote-2)

De SURF security baseline – als onderdeel van de dienst SURFaudit - is ontwikkeld om verschillende partijen binnen onderwijs en onderzoek te voorzien van een concrete set van maatregelen om een systeem of dienst te beveiligen. Hierdoor kunnen proces- en systeemeigenaren beter invulling geven aan hun verantwoordelijkheden op het gebied van informatiebeveiliging. Projectmanagers hebben hiermee duidelijke doelen om naartoe te werken en weten welke richtlijnen en best practices ze moeten volgen. Deze baseline voorziet leveranciers ook van duidelijke en gestandaardiseerde eisen voor beveiligingsmaatregelen, waardoor zij makkelijker kunnen voldoen aan de eisen van verschillende instellingen. Het is de bedoeling dat de SURF security baseline in de toekomst de Handreiking Beveiligingsmaatregelen van het SURF Juridisch Normenkader (Cloud)services [1] gaat vervangen.

## Doel SURF security baseline

Het doel van de security baseline is om een gestandaardiseerde set van beveiligingsmaatregelen te creëren voor onderwijs en onderzoek. Deze set bevat meer dan 100 maatregelen die geschikt zijn voor verschillende beveiligingsniveaus (laag, midden en hoog) van systemen, gegevens en processen. De set van maatregelen is concreet en gericht op praktische toepassing. Instellingen kunnen deze maatregelen intern gebruiken voor de ontwikkeling en bescherming van hun eigen IT-infrastructuur en in hun inkoopprocessen.

## Over de SURF security baseline

De baseline is een combinatie van maatregelen uit meerdere bekende en bewezen standaarden, zoals CIS controls v7.1 en ISO 27002:2017. Maar ook aangescherpt met maatregelen uit andere kaders die in onze sector worden gebruikt, zoals de STITCH controls en het certificeringsschema informatiebeveiliging en privacy ROSA v3.0. Deze maatregelen zijn vervolgens door een groep deskundigen van de hieronder genoemde instellingen één voor één beoordeeld en meerdere malen herzien. Dit met als doel om ze geschikt te maken voor de sector onderwijs en onderzoek en de samenhang tussen de verschillende maatregelen te waarborgen.

## Security baseline binnen vendor riskmanagement

In 2022 zijn instellingen in samenwerking met SURF gestart met het project Vendor Riskmanagement. Het project onderzoekt hoe we op basis van risicoclassificaties kunnen beoordelen of leveranciers voldoende beveiligingsmaatregelen hebben genomen, om de security van hun diensten en applicaties te waarborgen. De security baseline bevat de vereisten waaraan leveranciers moeten voldoen. Momenteel werken wij uit hoe wij gaan toetsen of de beveiliging van ingekochte applicaties en systemen adequaat is, en hoe wij de resultaten van deze toetsen kunnen delen onder instellingen.

## Aanvullingen MBO Digitaal

De Security Baseline is vertaald en aangevuld met de NBA control en de accountable.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Baseline item** (Engels) | **Baseline item** (Nederlands) | **Verwijzing (bijv. NBA)** | **Accountable** |
| 1. | SB.1.001 Acceptable use policy | Verantwoord netwerkgebruik | Document: Verantwoord netwerkgebruik | CvB en OR |
| 2. | SB.1.002 Governance of Processes and System | Governance van processen en systemen | 1.2 (GO.02) Beleid  2.1 (OR.01) Eigenaarschap  9.1 (DM.01) Data (en systeem) eigenaarschap  9.2 (DM.02) Classificatie  9.3 (DM.03) Beveiligingseisen voor Datamanagement | CvB  CvB  Hoofd HRM  Hoofd HRM  Hoofd HRM |
| 3. | SB.1.004 Asset inventory | Inventarisatie van bedrijfsmiddelen | 5.1 (CO.01) Identificatie en onderhoud van configuratie-items | Hoofd IT |
| 4. | SB.1.005 Asset registration | Registratie van activa | 5.2 (CO.02) Configuratiedatabase en baseline | Hoofd IT |
| 5. | SB.1.006 Detection of assets | Detectie van activa | 5.2 (CO.02) Configuratiedatabase en baseline **niveau 4** | Hoofd IT |
| 6. | SB.1.008 Patch management | Patchbeheer | 11.6 (SM.06) Patchmanagement | Hoofd IT |
| 7. | SB.1.009 Emergency updates | Noodupdates | 7.3 (CH.03) Noodaanpassingen | Hoofd IT |
| 8. | SB.1.011 Security in projects and changes | Beveiliging in projecten en wijzigingen | 7.1 (CH.01) Normen en procedures voor aanpassingen  7.2 (CH.02) Impact assessment, prioriteren en autoriseren | Hoofd IT  Hoofd IT |
| 9. | SB.1.014 Domain reservations | Domein reserveringen | Aanvullend beleid | Hoofd IT |
| 10. | SB.1.015 Software Bill-of-Materials | Software stuklijst | 15.5 (SC.05) Aanbesteding  ***NIEUWE CONTROL*** | Hoofd Inkoop |
| 11. | SB.1.016 Supplier Security Management | Leveranciersbeveiligingsbeheer | 15.5 (SC.05) Aanbesteding  ***NIEUWE CONTROL*** | Hoofd Inkoop |
| 12. | SB.2.001 Backup procedure | Back-up procedure | 13.2 (OP.02) Procedure voor back-up en herstel | Hoofd IT |
| 13. | SB.2.002 Datacenter uptime | Uptime van datacenter | 15.5 (SC.05) Aanbesteding  ***NIEUWE CONTROL*** | Hoofd Inkoop |
| 14. | SB.2.003 Offline backup | Offline back-up | 14.3 (BC-03) Offsite back-upopslag | Hoofd Facilitair |
| 15. | SB.3.001 Encrypted connections | Versleutelde verbindingen | 11.10 (SM.10) Cryptographic Key Management | Hoofd IT |
| 16. | SB.3.002 Email forwarding | E-mail doorsturen | Document: Verantwoord netwerkgebruik | CvB en OR |
| 17. | SB.3.003 Technical email security | Technische e-mailbeveiliging | 11.12 (SM.12) Beheersing van malware-aanvallen | Hoofd IT |
| 18. | SB.3.004 Warnings on external communication | Waarschuwingen voor externe communicatie | 11.12 (SM.12) Beheersing van malware-aanvallen | Hoofd IT |
| 19. | SB.3.005 Organizational mails | Organisatorische mails | 11.12 (SM.12) Beheersing van malware-aanvallen | Hoofd IT |
| 20. | SB.4.001 Incident response procedure | Incident response procedure | 6.1 (IM.01) Incident management  6.2 (IM.02) Incident escalatie  6.3 (IM.03) Incidenterespons op (cyber) beveiligingsincidenten | Hoofd IT  Hoofd IT  Hoofd It |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Baseline item** (Engels) | **Baseline item** (Nederlands) | **Verwijzing (bijv. NBA)** | **Accountable** |
| 21. | SB.4.002 Disaster Recovery Plan | Noodherstelplan | 14.1 (BC.01) Bedrijfscontinuïteitsplanning  14.5 (BC.05) Crisismanagement | Hoofd Facilitair  Hoofd IT |
| 22. | SB.4.003 Business continuity management | Beheer van bedrijfscontinuïteit | 14.2 (BC.02) Testen van Disaster recovery  14.5 (BC.05) Crisismanagement | Hoofd Facilitair  Hoofd IT |
| 23. | SB.4.004 CSIRT | CSIRT | 6.3 (IM.03) Incidenterespons op (cyber) beveiligingsincidenten  11.6 (SM.06) Patchmanagement | Hoofd IT  Hoofd IT |
| 24. | SB.4.007 Communicating about incidents | Communiceren over incidenten | 6.1 (IM.01) Incident management  6.3 (IM.03) Incidenterespons op (cyber) beveiligingsincidenten | Hoofd IT  Hoofd IT |
| 25. | SB.5.001 Encrypted data storage | Versleutelde gegevensopslag | 11.10 (SM.10) Cryptographic Key Management | Hoofd IT |
| 26. | SB.5.002 Data Storage Encryption: own managed key | Data Storage Encryption: eigen beheerde sleutel | 11.10 (SM.10) Cryptographic Key Management | Hoofd IT |
| 27. | SB.5.003 Certificate Management Registration | Registratie voor certificaatbeheer | 11.10 (SM.10) Cryptographic Key Management | Hoofd IT |
| 28. | SB.6.001 Authorized data distribution | Geautoriseerde gegevensdistributie | 11.13 (SM.13) Bescherming van beveiliginstechnologie | Hoofd IT |
| 29. | SB.6.003 Remote Wipe of Organizational Data | Op afstand wissen van organisatiegegevens | 11.3 (SM.03) Mobiele apparaten en telewerken | Hoofd IT |
| 30. | SB.6.004 Administrator Data Access | Toegang tot beheerdersgegevens | 10.3 (ID.03) Super Users | Hoofd IT |
| 31. | SB.6.006 Data Exfiltration Detection and Prevention | Detectie en preventie van gegevensexfiltratie | Document: Verantwoord netwerkgebruik | CvB en OR |
| 32. | SB.6.007 Printing Data-Leakage Prevention | Preventie van gegevenslekken bij afdrukken | Aanvullend beleid | Hoofd IT |
| 33. | SB.6.008 Organizational Data Deletion | Verwijdering van organisatorische gegevens | 9.4 (DM.04) Inrichting van opslag en retentie | Hoofd HRM |
| 34. | SB.6.010 Data handling procedure | Procedure voor gegevensverwerking | 11.3 (SM.03) Mobiele apparaten en telewerken | Hoofd IT |
| 35. | SB.6.012 Retention periods | Bewaartermijnen | 9.4 (DM.04) Inrichting van opslag en retentie | Hoofd HRM |
| 36. | SB.7.001 Scripts and Executables | Scripts en uitvoerbare bestanden | Document: Verantwoord netwerkgebruik | CvB en OR |
| 37. | SB.7.002 Anti-Malware protection | Anti-malware bescherming | 11.12 (SM.12) Beheersing van malware-aanvallen | Hoofd IT |
| 38. | SB.7.003 Local privileged accounts | Lokale geprivilegieerde accounts | Aanvullend beleid |  |
| 39. | SB.7.004 Memory protection | Geheugenbescherming | Aanvullend beleid |  |
| 40. | SB.7.005 Screen lock | Schermvergrendeling | 10.1 (ID.01) Toegangsrechten | Hoofd Studentenzaken |
| 41. | SB.7.006 Public workspace security | Beveiliging van openbare werkruimten | Aanvullend beleid |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Baseline item** (Engels) | **Baseline item** (Nederlands) | **Verwijzing (bijv. NBA)** | **Accountable** |
| 42. | SB.8.002 Operating procedures for Secure usage of IT service | Operationele procedures voor veilig gebruik van IT-service | 4.5 (HR.05) Kennisdeling | Hoofd HRM |
| 43. | SB.8.004 Identification | Identificatie | 4.1 (HR.)01 Werving, incl. Indiensttreding proces | Hoofd HRM |
| 44. | SB.8.005 Background Check | Antecedentenonderzoek | 4.1 (HR.)01 Werving, incl. Indiensttreding proces | Hoofd HRM |
| 45. | SB.8.006 External visitors to non-public spaces | Externe bezoekers van niet-openbare ruimtes | 12.2 (PH.02) Beheer van fysieke toegangsrechten | Hoofd Facilitair |
| 46. | SB.8.007 Staged warning model | Geënsceneerd waarschuwingsmodel | 6.3 (IM.03) Incidentrespons op (cyber) beveiligingsincidenten **niveau 4** | Hoofd IT |
| 47. | SB.8.008 Non-Disclosure Agreements | Geheimhoudingsovereenkomsten | NDA document | Hoofd HRM |
| 48. | SB.8.009 Team capacity monitoring | Bewaking van de teamcapaciteit | 1.3 (GO.03) Planning / Roadmap | CvB |
| 49. | SB.8.010 Secure behavior | Veilig gedrag | 4.6 (HR.06) Veiligheidsbewustzijn | Hoof HRM |
| 50. | SB.9.001 Authentication through organizational identity | Verificatie via organisatie-identiteit | 10.1 (ID.01) Toegangsrechten  10.2 (ID.02) Administratie van toegangsrechten | Hoofd HRM |
| 51. | SB.9.002 Account lock-out | Account lock-out | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 52. | SB.9.003 Defining user management | Gebruikersbeheer definiëren | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 53. | SB.9.004 Review of Permissions | Controle van machtigingen | 10.5 (ID.05) Periodieke beoordeling van toegangsrechten | Hoofd Hrm |
| 54. | SB.9.008 Password Complexity | Complexiteit van wachtwoorden | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 55. | SB.9.009 PIN and biometrics | PIN en biometrie | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 56. | SB.9.010 Password Visibility | Zichtbaarheid van wachtwoorden | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 57. | SB.9.011 Multi-Factor Authentication | Meervoudige verificatie | 10.1 (ID.01) Toegangsrechten  11.2 (SM.02) Authenticatie-mechanismes | Hoofd HRM  Hoofd IT |
| 58. | SB.9.012 Session Timeout | Time-out voor sessie | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 59. | SB.9.013 Digital identities | Digitale identiteiten | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 60. | SB.9.014 Least Privilege | Minste privilege | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 61. | SB.9.015 Joiner/Mover/Leaver | Joiner/Changer/Leaver | 4.4 (HR.04) Verandering of beëindiging van functie  10.1 (ID.01) Toegangsrechten | Hoofd HRM  Hoofd HRM |
| 62. | SB.9.016 Authorization Matrix | Autorisatiematrix | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 63. | SB.10.001 Privilege account monitoring | Bewaking van privilege-accounts | 10.3 (ID.03) Super Users | Hoofd HRM |
| 64. | SB.10.002 Account monitoring | Account monitoring | 11.2 (SM.02) Authenticatie-mechanismes | Hoofd IT |
| 65. | SB.10.003 Session and Identity monitoring | Sessie- en identiteitsbewaking | Aanvullend beleid |  |
| 66. | SB.10.004 Logging events | Gebeurtenissen vastleggen | 11.4 (SM.04) Logging | Hoofd IT |
| 67. | SB.10.005 Monitoring scripts and executables | Scripts en uitvoerbare bestanden controleren | 11.4 (SM.04) Logging | Hoofd IT |
| 68. | SB.10.006 Mutation and Data Access Logs | Logboeken voor mutaties en gegevenstoegang | 11.4 (SM.04) Logging | Hoofd IT |
| **Nr.** | **Baseline item** (Engels) | **Baseline item** (Nederlands) | **Verwijzing (bijv. NBA)** | **Accountable** |
| 69. | SB.10.007 Access and authentication attempts | Toegangs- en verificatiepogingen | 11.4 (SM.04) Logging | Hoofd IT |
| 70. | SB.10.008 Risk Monitoring | Risk Monitoring | 11.4 (SM.04) Logging | Hoofd IT |
| 71. | SB.10.009 Password Monitoring | Wachtwoordcontrole | 11.4 (SM.04) Logging | Hoofd IT |
| 72. | SB.10.011 Network Intrusion Detection and Prevention Systems | Netwerkinbraakdetectie- en preventiesystemen | 11.4 (SM.04) Logging | Hoofd IT |
| 73. | SB.11.001 Network Access Control | Netwerktoegangsbeheer | 11.4 (SM.04) Logging | Hoofd IT |
| 74. | SB.11.002 Block malicious sources | Blokkeer kwaadaardige bronnen | 11.4 (SM.04) Logging | Hoofd IT |
| 75. | SB.11.003 Networking Hardware | Netwerkhardware | 11.8 (SM.08) Beschikbaarheid en bescherming van infrastructuur | Hoofd IT |
| 76. | SB.11.004 Network Segmentation and zoning | Netwerksegmentatie en zonering | 11.8 (SM.08) Beschikbaarheid en bescherming van infrastructuur | Hoofd IT |
| 77. | SB.11.005 DMZ | DMZ | 11.8 (SM.08) Beschikbaarheid en bescherming van infrastructuur | Hoofd IT |
| 78. | SB.11.006 Firewall Rule Management | Beheer van firewallregels | 11.11 (SM.11) Network Security | Hoofd IT |
| 79. | SB.11.007 DDoS Network Protections | DDoS-netwerkbeveiliging | 11.4 (SM.04) Logging  11.8 (SM.08) Beschikbaarheid en bescherming van infrastructuur | Hoofd IT |
| 80. | SB.12.001 Access to technical areas | Toegang tot technische ruimtes | 12.1 (PH.01) Fysieke beveili-gingsmaatregelen | Hoofd IT |
| 81. | SB.12.002 Emergency Power | Noodstroom | 11.8 (SM.08) Beschikbaarheid en bescherming van infrastructuur | Hoofd IT |
| 82. | SB.13.001 Segmenting authentication domains | Verificatiedomeinen segmenteren | 11.11 (SM.11) Network Security | Hoofd IT |
| 83. | SB.13.002 Access to admin interfaces | Toegang tot beheerinterfaces | Aanvullend beleid |  |
| 84. | SB.13.003 Privileged Access | Geprivilegieerde toegang | 10.3 (ID.03) Super Users | Hoofd HRM |
| 85. | SB.13.004 Service Accounts | Service-accounts | Aanvullend beleid |  |
| 86. | SB.13.005 Separate Accounts for Privileged Access | Afzonderlijke accounts voor geprivilegieerde toegang | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 87. | SB.13.006 Session Management for Privileged Access | Sessiebeheer voor geprivilegieerde toegang | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 88. | SB.13.007 Break Glass Procedure | Noodprocedure | 10.4 (ID.04) Noodtoegang (enveloppocedure/breek-het-glasprocedure) | Hoofd HRM |
| 89. | SB.13.008 MFA for Privileged Access | MFA voor geprivilegieerde toegang | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 90. | SB.14.001 DTAP | OTAP | 7.6 (CH.06) Promotie naar productie | Hoofd IT |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr.** | **Baseline item** (Engels) | **Baseline item** (Nederlands) | **Verwijzing (bijv. NBA)** | **Accountable** |
| 91. | SB.14.002 Testing Data | Testgegevens | 7.4 (CH.04) Testomgeving  7.5 (CH.05) Testen van aanpassingen | Hoofd IT  Hoofd IT |
| 92. | SB.14.003 Rollback Procedure | Terugdraaiprocedure | 7.4 (CH.04) Testomgeving  7.5 (CH.05) Testen van aanpassingen | Hoofd IT  Hoofd IT |
| 93. | SB.14.004 Configuration Files | Configuratiebestanden | 7.4 (CH.04) Testomgeving  7.5 (CH.05) Testen van aanpassingen | Hoofd IT  Hoofd IT |
| 94. | SB.14.005 Input and Output Filtering | Invoer- en uitvoerfiltering | 7.4 (CH.04) Testomgeving  7.5 (CH.05) Testen van aanpassingen | Hoofd IT  Hoofd IT |
| 95. | SB.14.006 Web Application Security | Beveiliging van webtoepassingen | 8.1 (SD.01) Methodiek voor veilige softwareontwikkeling en -implementatie | Hoofd IT |
| 96. | SB.14.007 Mobile Applications | Mobiele applicaties | 8.1 (SD.01) Methodiek voor veilige softwareontwikkeling en -implementatie | Hoofd IT |
| 97. | SB.14.008 Application (D)DoS Protection | Toepassing (D)DoS-bescherming | 7.4 (CH.04) Testomgeving  7.5 (CH.05) Testen van aanpassingen | Hoofd IT  Hoofd IT |
| 98. | SB.14.009 Malware Scanning | Malware scannen | 11.12 (SM.12) Beheersing van malware-aanvallen | Hoofd IT |
| 99. | SB.14.010 Third Party Apps and Libraries | Third Party Apps en bibliotheken | 15.5 (SC.05) Aanbesteding  ***NIEUWE CONTROL*** | Hoofd Inkoop |
| 100. | SB.16.001 Baseline configuration | Baseline configuratie | 15.5 (SC.05) Aanbesteding  ***NIEUWE CONTROL***  11.11 (SM.11) Network Security | Hoofd Inkoop  Hoofd IT |
| 101. | SB.16.002 Hardening Validation | Hardening validatie | Aanvullend beleid |  |
| 102. | SB.16.003 Unintended Information Disclosure | Onbedoelde openbaarmaking van informatie | Document: Verantwoord netwerkgebruik | CvB en OR |
| 103. | SB.16.004 Default Passwords changed | Standaardwachtwoorden gewijzigd | 10.1 (ID.01) Toegangsrechten | Hoofd HRM |
| 104. | SB.16.005 Service Hardening | Service Hardening | 15.2 (SC.02) Service Level Management | Hoofd Inkoop |
| 105. | SB.16.006 Server and Application Infrastructure Not Shared | Server- en toepassingsinfrastructuur niet gedeeld | 15.2 (SC.02) Service Level Management | Hoofd Inkoop |
| 106. | SB.18.001 Vulnerability Registration and Resolution | Registratie en oplossing van kwetsbaarheden | 11.6 (SM.06) Patchmanagement  11.7 (SM.07) Threat en Vulnerability Management | Hoofd IT  Hoofd IT |
| 107. | SB.18.002 Coordinated Vulnerability Disclosure Policy | Gecoördineerd beleid voor het vrijgeven van kwetsbaarheden | Responsible Disclosure (onderdeel Verantwoord Netwerkbebruik) | Hoofd IT  Hoofd IT |
| 108. | SB.18.003 Automated Vulnerability Scanning | Geautomatiseerde kwetsbaarheidsscans | 11.6 (SM.06) Patchmanagement  11.7 (SM.07) Threat en Vulnerability Management | Hoofd IT  Hoofd IT |
| 109. | SB.18.004 Automated Application Vulnerability Scanning | Geautomatiseerde kwetsbaarheidsscans voor toepassingen | 11.6 (SM.06) Patchmanagement  11.7 (SM.07) Threat en Vulnerability Management | Hoofd IT  Hoofd IT |
| **Nr.** | **Baseline item** (Engels) | **Baseline item** (Nederlands) | **Verwijzing (bijv. NBA)** | **Accountable** |
| 110. | SB.18.005 Penetration Testing | Penetratie testen | 11.5 (SM.05) Testen van, inspectie van en toezicht op beveiliging | Hoofd IT |

# IT audit beoordeling

|  |  |
| --- | --- |
| **Risico**: | Afwezige of onjuiste beveiligings-baselines kunnen leiden tot een afwijkende of inconsistente implementatie van beveiligingsparameters, wat uiteindelijk leidt tot ongeautoriseerde toegang of verstoring van IT-services. |
| **Doelstelling**: | Beveiligingsbaselines en richtlijnen voor IT-infrastructuur zijn vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. Beveiligingsbaselines worden formeel vastgelegd, periodiek geactualiseerd en goedgekeurd door het senior management. Verantwoordelijk IT-personeel wordt hiervan op de hoogte gesteld. Geïmplementeerde beveiligingsinstellingen voor IT-middelen worden periodiek beoordeeld op naleving van beveiligingsbaselines. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd. |

**Volwassenheidsniveaus**

|  |  |
| --- | --- |
| **1** | 1. Er zijn geen beveiligingsbaselines. |
| **2** | 1. Er zijn beveiligingsbaselines gedefinieerd voor belangrijkste IT-infrastructuurcomponenten. 2. Beveiligingsbaselines worden ad-hoc geïmplementeerd en afwijkingen van de baselines worden niet gedocumenteerd. |
| **3** | 1. Beveiligingsbaselines zijn gedefinieerd, goedgekeurd door het senior management en gecommuniceerd naar verantwoordelijk IT-personeel. 2. *Zie document NBADOC- P12 Security Baselines 14-8-2023, versiebeheer* 3. De geïmplementeerde beveiligingsinstellingen voor IT-middelen worden periodiek gecontroleerd op overeenstemming met de beveiligingsbaselines.   *Beoordeling opgenomen in de roadmap.*   1. Resultaten worden gedocumenteerd, afwijkingen worden gedocumenteerd en goedgekeurd (of gecorrigeerd).   *Zie verslag beoordeling Security Baselines*   1. Voor nieuwe IT infrastructuur componenten en projectmanagement processen wordt implementatie van beveiligingsbaselines afgedwongen.   *Onderdeel van Control 70, Aanbesteding.*   1. In hoeverre aan de baseline wordt voldaan wordt periodiek gerapporteerd aan het senior management.   *Kwartaalrapportage vanaf Q4-2023 beschikbaar.* |
| **4** | 1. Beveiligingsbaselines worden periodiek geëvalueerd en geactualiseerd (indien nodig). |
| **5** | 1. Het bewaken van de mate waarin aan de beveiligingsbaselines wordt voldaan, wordt gedaan door middel van continuous monitoring/audittools. *(CIS compliance)* 2. Afwijkingen van de baselines worden real-time gerapporteerd en indien nodig gecorrigeerd. |

1. Bron: SURF [↑](#footnote-ref-2)