Samen aanjagen van vernieuwing

Handreiking cybersecurity configuraties in netwerken

Voorkomen van de top 10 misconfiguraties

Auteur(s): Security Expertise Centrum, MBO-Digitaal
Versie: 1.1
Datum: 15 januari 2024
Kenmerk: Handreiking cybersecurity configuraties in netwerken

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

De National Security Agency (NSA) en Cybersecurity and Infrastructure Security Agency (CISA) hebben begin oktober 2023 een top 10 van de meest voorkomende misconfiguraties in netwerken gepubliceerd[1]. Hiernaast is onze vertaling van deze top 10 weergegeven. De publicatie door NSA en CISA is voor ons aanleiding geweest om deze handreiking te maken specifiek gericht op onze sector.

1.2 Doelstelling

Met deze handreiking bieden we instellingen een praktisch hulpmiddel om de top 10 misconfiguraties te voorkomen of op te lossen. In Bjlage 1 is een mapping naar het SURFaudit Toetsingskader en zijn verwijzingen opgenomen naar de SURF Security Baseline en relevante SURF dienstverlening.

1.3 Doelgroep

Dit document is primair bedoeld voor netwerk- en systeembeheerders om hen te ondersteunen in het beveiligen van netwerken, maar uiteraard kunnen ook IBP'ers het gebruiken om hun netwerken te (laten) onderzoeken op de genoemde misconfiguraties. Instellingen worden geadviseerd om dit document te gebruiken om de meest voorkomende misconfiguraties in netwerken te voorkomen.

1.4 Disclaimer

Deze handreiking en de hierin beschreven maatregelen bieden geen garantie veilig te zijn, maar dragen gezamenlijk wel bij aan het voorkomen, tijdig detecteren en beperken van de impact van cyberaanvallen en menselijke fouten.

Klik op één van de misconfiguraties in de figuur hiernaast en navigeer direct naar het betreffende onderwerp.

Figuur 1:
Top 10 misconfiguraties

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

2 Misconfiguratie 1: Standaard configuraties

Standaard configuraties in systemen, services en applicaties kunnen leiden tot ongeautoriseerde toegang of andere ongewenste activiteiten, zoals malware infecties of data exfiltratie. Twee aspecten van standaard misconfiguraties zijn uitgelicht: standaard verificatiegegevens (credentials) en standaard permissies en configuraties.

Standaard credentials zijn bijvoorbeeld online vindbaar en cybercriminelen kunnen daar daarom makkelijk misbruik van maken wanneer die niet aangepast, verwijderd of geblokkeerd worden.

2.1 Tips

- ☐ Zorg ervoor dat in wijzigings- en inkoopprocessen is opgenomen dat standaard configuraties worden aangepast vóór de implementatie in productie omgevingen.
- ☐ Maak gebruik van de hardening[2] standaarden van de leverancier of CIS Benchmarks, NIST's National Checklist Program (NCP) en Security Technical Implementation Guides (STIGs).
- ☐ Maak gebruik van de SURFaudit Azure policy template om te voldoen aan security best practices voor Platform-as-a-Service (PaaS) en Infrastructure-as-a-Service (IaaS) diensten binnen Microsoft Azure (waaronder Windows, Linux, Docker, Kubernetes).
- ☐ Zorg ervoor dat standaard gebruikersnamen en wachtwoorden in hardware, software en services aangepast, verwijderd of uitgeschakeld worden. Testen op het gebruik van standaard credentials kan met behulp van de OWASP richtlijnen.
- ☐ Schakel Active Directory Certificate Services (ADCS) uit of zorg voor veilige implementatie ervan door:
    - Te verifiëren of Extended Protection for Authentication (EPA) voor Client Authority Web Enrollment is ingeschakeld.
    - 'Vereis SSL' in te schakelen op de ADCS server.
    - New Technology LAN Manager (NTLM) uit te schakelen op de ADCS server[3][4].
    - Subject Alternative Name (SAN) uit te schakelen voor User Principal Name (UPN) mapping. Smart card authenticatie kan in plaats daarvan het attribuut altSecurityIdentities gebruiken.
    - Je kunt ook Locksmith gebruiken om veelvoorkomende misconfiguraties in ADCS te detecteren en (automatisch) op te lossen.
- ☐ Review alle permissies van de ADCS templates op servers:
    - Beperk de inschrijvingsrechten tot de gebruikers of groepen die dit nodig hebben.
    - Schakel de CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT vlag uit.
    - Verwijder de FullControl, WriteDacl en Write permissies uit voor groepen met lage privileges zoals domein users.
- ☐ Schakel Link-Local Multicast Name Resolution (LLMNR) en NetBIOS uit als het niet noodzakelijk is (in de group policy of in lokale beveiligingsinstellingen).
- ☐ Verifieer of Server Message Block (SMB) signing voor zowel de SMB client als server op alle systemen is ingeschakeld.

[2] Niet gebruikte functies in hardware en software uitzetten of weghalen. En de rechten van andere functies waar mogelijk beperken. Zo verkleint men het aanvalsoppervlak en daarmee het risico van aanvallen.

[3] https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain

[4] https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-incoming-ntlm-traffic

3 Misconfiguratie 2: Standaard permissies

Standaard configuraties in systemen, services en applicaties kunnen leiden tot ongeautoriseerde toegang of andere ongewenste activiteiten, zoals malware infecties of data exfiltratie. Twee aspecten van standaard misconfiguraties zijn uitgelicht: standaard verificatiegegevens (credentials) en standaard permissies en configuraties.

3.1 Tips

- ☐ Pas het least privilege principe toe op alle accounts, dit betekent dat uitsluitend de rechten die noodzakelijk zijn worden toegekend.
- ☐ Limiteer de mogelijkheid waarmee gebruikers aanvullende accounts kunnen creëren.
- ☐ Verricht regelmatig een controle op beheer- en serviceaccounts en verwijder inactieve of onnodige accounts.
- ☐ Beperk het gebruik van geprivilegieerde accounts voor reguliere taken[5][6].
- ☐ Implementeer tijd-gebaseerde (just-in-time) conditionele toegang voor geprivilegieerde accounts7.
- ☐ Beperk het bereik van domeingebruikers zodat ze zich niet in de lokale beheerdersgroep op meerdere systemen kunnen bevinden[8].
- ☐ Voer indien mogelijk services zonder beheeraccounts uit.
- ☐ Configureer serviceaccounts alleen met de machtigingen die nodig zijn voor de services die ze beheren (least privilege).
- ☐ Schakel ongebruikte services uit en implementeer een Access Control List (ACL) om services te beschermen.
- ☐ Controleer regelmatig de uitgegeven rechten en corrigeer ze indien nodig.
- ☐ Stel account lock-out in om de kans op misbruik te verkleinen:
    - wanneer een account langer dan 45 dagen inactief is geweest;
    - op de uitdienstdatum van de betreffende persoon;
    - bij het meermaals invoeren van onjuiste credentials (bijv. 15 minuten blokkeren na 3 onjuiste pogingen en 1 seconde vertraging tussen pogingen) om veelgebruikte aanvallen zoals brute force, password spraying en -guessing tegen te gaan.
- ☐ Maak onderscheid tussen de verschillende beveiligingsniveaus binnen het IT-landschap voor geprivilegieerde toegang, waarbij in ieder geval een logisch onderscheid wordt gemaakt tussen endpoints, netwerktoegangslaag, netwerkkern, serverbeheerder en domeinbeheerder.

[5] https://media.defense.gov/2019/Sep/09/2002180330/-1/-1/0/Defend%20Privileges%20and%20Accounts%20-%20Copy.pdf

[6] https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

[7] https://joshua-lucas.com/posts/just-in-time-conditional-access-with-azure-ad-pim/

[8] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

4 Misconfiguratie 3: Ontoereikend monitoren van het netwerk

Alle leden van SURF nemen in de basisvergoeding SURFinternet, eduroam, eduroam Visitor Access en SURFcert af. Het netwerk van SURF wordt 24x7 proactief gemonitord en beschermd door SURFcert tegen cyberdreigingen zoals DDoS-aanvallen. Aanvullend daarop moeten instellingen ervoor zorgen dat zij zelf ook het interne netwerk (kunnen) monitoren.

4.1 Tips

- ☐ Zorg voor een actueel en zo volledig mogelijk inventaris van bedrijfsmiddelen (CMDB) voor onder andere apparatuur voor eindgebruikers zoals laptops, tablets en smartphones, netwerkapparaten, printers, Internet of Things (IoT), Operational Technology (OT) en (web)servers. Leg voor iedere registratie vast: naam en omschrijving, MAC-adres, IP-adres (indien statisch), machine naam, eigenaar, beheer (intern/extern), leverancier (incl. contactpersoon), fysieke locatie (indien mogelijk), BIV-classificatie[9] en de herstelprioriteit[10].
- ☐ Gebruik ter ondersteuning daarvan actieve en passieve tools om bedrijfsmiddelen te identificeren, bijvoorbeeld via Dynamic Host Configuration Protocol (DHCP) logging op alle DHCP-servers of IP-adres management tools of via Microsoft Defender for endpoint.
- ☐ Controleer regelmatig het gebruik van applicaties en services, met in het bijzonder administratieve activiteit, ACL's en hun permissies.
- ☐ Definieer wat 'normaal' gedrag in het netwerk is (netwerkverkeer, -prestaties, activiteit host applicaties en gebruikersgedrag) en adresseer afwijkend gedrag, bijvoorbeeld met Microsoft Defender for endpoint en SURFsoc.
- ☐ Zorg ervoor dat logbestanden centraal geaggregeerd en gecorreleerd worden (SIEM), bijvoorbeeld met SURFsoc of Microsoft Sentinel.
- ☐ Scan proactief naar misconfiguraties zoals open shares met tools zoals nfsscanner en smbscanner.
- ☐ Implementeer een Netwerk Intrusion Detection System (NIDS) zoals Azure Network Watcher, Snort of Suricata.

Op de wiki-pagina van SCIRT vind je meer informatie en een verzameling van handige tools. SCIRT is een SURF community die zich bezighoudt met operationele informatiebeveiliging.

[9] Beschikbaarheid, integriteit en vertrouwelijkheid.

[10] Recovery Time Objective (RTO) oftewel de acceptabele periode van verstoring.

5 Misconfiguratie 4: Onvoldoende netwerksegmentatie

Brandcompartimenten zorgen ervoor dat een brand niet eenvoudig kan overslaan naar andere compartimenten. Ditzelfde geldt ook voor netwerksegmenten. Als een aanvaller eenmaal binnen is, moet hij niet direct in staat zijn om kritieke systemen te benaderen. Netwerksegmentatie deelt het netwerk op in logische compartimenten waardoor de mate van controle en beveiliging toeneemt. Netwerken kunnen zowel fysiek (air-gapped) als virtueel (bijv. subnets en VLAN's) gescheiden worden.

5.1 Tips

- ☐ Isoleer kritieke systemen, functies en middelen in netwerksegmenten (VLAN's), zoals werkstations, BYOD/gasten, servers, printers, telefonie, IoT en air-gap OT[11].
- ☐ Scheid de security-functie van de rest en volg het privileged access model van Microsoft (E5 licentie benodigd).
- ☐ Positioneer publiek toegankelijke systemen en uitgaande proxies tussen firewalls in Demilitarized Zones (DMZ).
- ☐ Implementeer zero-trust principes in het netwerk en hanteer strike filtering tussen segmenten, systemen en applicaties[12].
- ☐ Implementeer meerdere lagen van (virtuele) next-generation firewalls (bij voorkeur van verschillende leveranciers en/of SURFfirewall) om inkomend en uitgaand verkeer te beperken en om het interne verkeer tussen segmenten te kunnen monitoren.
- ☐ Configureer ACLs op infrastructuur apparatuur (switches, routers, firewalls) om de toegang daartoe en tussen segmenten te beperken tot het strikt noodzakelijke (deny-by-default) en voor het reguleren van inkomende- en uitgaande informatiestromen.
- ☐ Zorg ervoor dat server- en applicatie-infrastructuur niet gedeeld wordt (productie scheiden van IT-infrastructuur).
- ☐ Overweeg microsegmentatie om op systeemniveau segmentatie toe te kunnen passen.
- ☐ Verwijder achterdeuren in het netwerk om te voorkomen dat aanvallers via gecompromitteerde apparaten en accounts eenvoudig lateraal kunnen bewegen naar andere segmenten. Voorbeelden hiervan zijn aan het internet blootgestelde management interfaces, redundante accounts of services, accounts voor leveranciers en onveilige API's.
- ☐ Implementeer port-based Network Access Control (802.1x) om te voorkomen dat ongeautoriseerde apparatuur toegang verkrijgt tot het interne netwerk.

Op de wiki-pagina van SCIRT vind je meer informatie en een verzameling van handige tools. SCIRT is een SURF community die zich bezighoudt met operationele informatiebeveiliging.

[11] https://github.com/sergiomarotco/Network-segmentation-cheat-sheet

[12] https://learn.microsoft.com/en-us/security/zero-trust/deploy/networks

6 Misconfiguratie 5: Slecht patchmanagement

Patches verhelpen bekende kwetsbaarheden en schromen om een patch (tijdig) door te voeren stelt een aanvaller in staat om bekende kwetsbaarheden te misbruiken. Hoe erg dat is hangt af van de ernst van de kwetsbaarheid. Een goed patchmanagementproces is daarom noodzakelijk om de kans op misbruik te verkleinen.

6.1 Tips

- ☐ Stel een Software- en Hardware Bill of Materials (SBOM/HBOM)[13] op of verzoek een leverancier om die aan te leveren aangezien de effectiviteit van patch management daarop leunt.
- ☐ Neem in de basis altijd de adviezen van leveranciers en SURFcert voor het verhelpen van kwetsbaarheden over.
- ☐ Prioriteer het verhelpen van kwetsbaarheden eventueel op basis van het Common Vulnerability Scoring System (CVSS) en overige factoren.
- ☐ Automatiseer het updateproces zoveel mogelijk om menselijke fouten en missers te voorkomen, bijvoorbeeld via Azure Automation update management en Windows Server Update Services (WSUS).
- ☐ Patch ook de Basic Input/Output System (BIOS) en overige firmware.
- ☐ Waar patchen niet mogelijk (bijv. legacy[14]) of wenselijk (bijv. compatibiliteit) is, dienen compenserende maatregelen getroffen te worden zoals virtualisatie, segmentatie, isolatie of aanvullende monitoring.
- ☐ Voorkom waar mogelijk het gebruik van legacy systemen. Als dat niet mogelijk of wenselijk is, pas dan de self-assessmentmethode van het Nationaal Cyber Security Centrum (NCSC) toe om inzicht te verkrijgen in de risico's en mogelijkheden om deze in te dammen of zelf weg te nemen.

[13] SBOM/HBOM is een lijst van welke versie van componenten in de soft- en hardware zit.

[14] Systemen die niet meer onderhouden worden door de leverancier.

7 Misconfiguratie 6: Omzeilen van toegangscontroles

Toegangscontroles (access control) zijn bedoeld om te voorkomen dat ongeautoriseerde personen toegang krijgen tot systemen en informatie. Met toegangscontrole bewijs je wie je zegt dat je bent en er zijn drie smaken: 1) iets dat je weet (zoals een wachtwoord), 2) iets dat je hebt (zoals een hardtoken), en 3) iets dat je bent (zoals een vingerafdruk). Het kunnen omzeilen van toegangscontroles, bijvoorbeeld via pass-the-hash of hergebruik van sessiecookies, kan verregaande gevolgen hebben. Het is daarom noodzakelijk om naast sterke toegangscontroles ook andere maatregelen te treffen, zie ook Misconfiguratie 7.

7.1 Tips

- ☐ Gebruik Kerberos voor authenticatie in Windows omgevingen met AES-encryptie, gebruik sterke en lange wachtwoorden voor serviceaccounts (>25 karakters) en overweeg het gebruik van Group Managed Service Accounts voor het beheren daarvan.
- ☐ Volg de security best practices van Microsoft voor het veilig configureren van Kerberos.
- ☐ Beperk de toegang tot de hash van het KRBTGT wachtwoord en verander deze iedere 180 dagen om kerberoasting aanvallen tegen te gaan.
- ☐ Zorg ervoor dat authenticatie zoveel mogelijk via Single-Sign-On (SSO) verloopt, bij voorkeur via SURFconext. Zorg ervoor dat voor externe systemen waar geen SSO mogelijk is unieke credentials en MFA gebruikt worden om initiële toegang en laterale beweging te bemoeilijken.
- ☐ Leg User Account Control (UAC) restricties op.
- ☐ Sta communicatie tussen werkstations niet toe en leidt verkeer altijd om via een server om laterale beweging te voorkomen, bijvoorbeeld met behulp van firewall, Group Policy of micro-segmentatie.
- ☐ Gebruik geprivilegieerde accounts alleen op systemen die dat vereisen (dus niet voor reguliere zaken zoals het lezen van mails of browsen op het internet).
- ☐ Overweeg het gebruik van speciale werkstations voor geprivilegieerde accounts (PAW).

8 Misconfiguratie 7: Zwakke of misconfiguratie in MFA

Sommige vormen van Multifactor authenticatie (MFA) zijn niet bestendig tegen phishing aanvallen. Hierdoor is de kans aanwezig dat aanvallers door middel van social engineering technieken ongeautoriseerd toegang kunnen krijgen tot accounts en vanuit daar verdere aanvallen kunnen uitvoeren.

8.1 Tips

- ☐ Schakel NTLM en overige legacy protocollen uit om pass-the-hash aanvallen te voorkomen en gebruik Kerberos voor authenticatie in Windows omgevingen.
- ☐ Gebruik zoveel mogelijk SURFconext of Single-Sign-On (SSO) voor authenticatie voor Cloudoplossingen.
- ☐ Implementeer een phishing bestendige MFA oplossing op basis van FIDO, WebAuthn of PKI voor geprivilegieerde accounts en overweeg dit ook voor vaak geselecteerde doelwitten zoals bestuursleden en financiële medewerkers. Bijvoorbeeld via SURFsecureID.
- ☐ Schakel logging voor authenticatie in en monitor actief alle loginpogingen om afwijkende logins te detecteren en te adresseren, bijvoorbeeld met behulp van SURFsoc of Microsoft Sentinel.
- ☐ Maak gebruik van EduVPN voor veilige toegang vanaf onbetrouwbare netwerken.

9 Misconfiguratie 8: Onvoldoende toegangscontrole op netwerkschijven en -services

Gedeelde netwerkschijven en services zijn primaire doelen van aanvallers. Als de toegang onjuist geconfigureerd is kan een aanvaller ongeautoriseerd toegang krijgen tot gevoelige informatie, deze exfiltreren, versleutelen (ransomware), muteren of verwijderen. Toegang verschaft de aanvaller(s) vaak ook veel kennis over de organisatie, haar processen en IT-infrastructuur.

9.1 Tips

- ☐ Zorg voor een veilige configuratie van opslagapparatuur en netwerkschijven die uitsluitend toegang geven tot geautoriseerde gebruikers (MFA, least privilege, filtering, etc.).
- ☐ Definieer de permissies en leg deze vast in een autorisatiematrix.
- ☐ Beperk de permissies tot bestanden en directories en voorkom het aanpassen van een ACL (least privilege).
- ☐ Beperk permissies tot bestanden en mappen met private sleutels om ongeautoriseerde toegang en misbruik te voorkomen.
- ☐ Controleer de permissies regelmatig en tref indien nodig corrigerende maatregelen.
- ☐ Schakel de Windows Group Policy beveiligingsinstelling Do Not Allow Anonymous Enumeration of Security Account Manager Accounts and Shares in om het aantal gebruikers dat netwerkschijven kan enumereren te beperken. Een enumeratie-aanval stelt en hacker in staat om erachter te komen of een naam al in de database voorkomt. Hierdoor kan de hacker niet onmiddellijk inloggen, maar het geeft hem wel al de helft van de benodigde informatie.
- ☐ Scan het netwerk proactief op open shares.

Op de wiki-pagina van SCIRT vind je meer informatie en een verzameling van handige tools. SCIRT is een SURF community die zich bezighoudt met operationele informatiebeveiliging.

10 Misconfiguratie 9: Slecht beheer van credentials

Slecht beheer van credentials faciliteert dreigingsactoren in het verkrijgen van credentials voor initiële toegang tot systemen en netwerken, maar bijvoorbeeld ook voor het escaleren van rechten daarna. Dit kan mogelijk gemaakt worden door een zwak beleid voor wachtwoorden, eenvoudig te kraken of te raden wachtwoorden, het hergebruiken van wachtwoorden of het opslaan van leesbare wachtwoorden in configuratiebestanden.

10.1 Tips

- ☐ Dwing het gebruik van sterke wachtwoorden af.
- ☐ Monitor op uitgelekte credentials van alle domeinen van de instelling.
- ☐ Blokkeer het gebruik van bekende wachtwoorden[15].
- ☐ Gebruik een (gedeelde) wachtwoordkluis of Microsoft LAPS waarmee beheerders sterke wachtwoorden kunnen beheren, routeren en delen.
- ☐ Gebruik Microsoft Purview trainable classifiers om plaintext wachtwoorden in systemen en bestanden te detecteren.
- ☐ Implementeer Privileged Identity Management (PIM) in Microsoft 365.

[15] https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad

11 Misconfiguratie 10: Ongelimiteerd uitvoeren van code

Zodra aanvallers initiële toegang tot een systeem hebben verkregen zullen zij proberen om bepaalde programma's (code) uit te voeren om hun verdere doelen te bereiken. Zoals bijvoorbeeld het dumpen van credentials uit het geheugen of het lateraal kunnen bewegen in het netwerk.

11.1 Tips

- ☐ Zorg ervoor dat endpoint protection zoals Microsoft Defender for Endpoint draait op alle beheerde werkplekken en servers.
- ☐ Implementeer allowlisting om te voorkomen dat niet geverifieerde programma's uitgevoerd kunnen worden, zoals AppLocker of Windows Defender Application Control (WDAC).
- ☐ Blokkeer of voorkom het uitvoeren van kwetsbare drivers om het uitvoeren van code in kernel mode tegen te gaan. Valideer driver block regels in audit mode om stabiliteit te verzekeren[16].
- ☐ Beperk of blokkeer scripttalen, zoals PowerShell of Command prompt, die niet noodzakelijk zijn om kwaadaardige activiteiten te voorkomen.
- ☐ Gebruik een lijst van geautoriseerde (ondertekende) PowerShell scripts[17] om het uitvoeren van kwaadaardige scripts te beperken.
- ☐ Gebruik PowerShell om de beveiliging te verbeteren op werkplekken waar PowerShell nodig is[18].
- ☐ Blokkeer veel misbruikte bestandsextensies als deze niet noodzakelijk zijn of wijs het standaardprogramma voor het openen daarvan toe aan notepad.exe.
- ☐ Gebruik read-only containers en minimale images waar mogelijk om het uitvoeren van kwaadaardige commando's te voorkomen[19][20][21].
- ☐ Geef geen (permanente) local admin rechten uit als dat niet noodzakelijk is.
- ☐ Schakel Microsoft Office macro's volledig uit of sta alleen getekende macro's toe (standaard blokkering al aanwezig in Microsoft 365).

---

16 https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/microsoft-recommended-driver-block-rules

17 Instelling: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on Script Execution

Waarde: Allow only signed scripts

18 https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/1/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF

19 https://res.cloudinary.com/snyk/image/upload/v1551798390/Docker_Image_Security_Best_Practices_.pdf

20 https://docs.docker.com/develop/security-best-practices/

21 https://cheatsheetseries.owasp.org/cheatsheets/Kubernetes_Security_Cheat_Sheet.html#use-minimal-base-images-and-avoid-adding-unnecessary-components

Bijlage 1 Mapping Top 10 misconfiguraties

In deze bijlage zijn de Top 10 misconfiguraties in lijn gebracht (mapping) met het SURFaudit Toetsingskader. Hierbij de kanttekening dat voor de mapping gebruik is gemaakt van de thema indeling zoals die binnen het MBO wordt toegepast (Goverance, Processen en Techniek).

SURFaudit toetsingskader **Top 10 misconfiguraties**	**Governance**	**Processen**	**Techniek**
1. Standaard configuraties	-	5.2, 7.1, 7.2, 10.1, 10.2, 10.3, 10.4, 10.5, 11.1	11.2, 11.3, 11.7
2. Onjuiste scheiding in privileges	2.1, 2.2	11.1	11.7, 11.8
3. Ontoereikend monitoren van het interne netwerk	-	11.1, 15.2	11.4, 11.8
4. Onvoldoende netwerksegmentatie	-	11.1	11.7, 11.8, 11.11, 11.12, 11.13
5. Slecht patch management	-	5.1, 5.2, 7.1, 7.2, 7.3	11.6, 11.7, 11.8, 11.11, 11.12
6. Omzeilen van toegangscontroles	-	10.1, 10.2, 10.3, 10.4, 10.5	11.2, 11.3, 11.7, 11.8
7. Zwakke of misconfiguraties in MFA methodes	-	10.1, 10.2, 10.3, 10.4, 10.5	11.2, 11.3, 11.7, 11.8
8. Onvoldoende toegangscontrole op netwerkschijf/service	2.1, 2.2	10.1, 10.2, 10.3, 10.4, 10.5	11.2, 11.3, 11.7, 11.8
9. Slechte hygiëne credentials	-	10.1, 10.2, 10.3, 10.4, 10.5	11.2, 11.3, 11.7, 11.8
10. Ongelimiteerde uitvoer van code	-	5.2, 11.1	11.7, 11.8

Tabel 1: Mapping Top 10 misconfiguraties aan SURFaudit Toetsingskader

Bijlage 2 Top 10 misconfiguraties in een notendop

MISCONFIGURATIE	PROBLEEM	LEID TOT
1. Standaard configuraties	- Insecure by design (out of the box) door leveranciers - Onveilige configuraties worden niet aangepast - Legacy protocollen en services worden gebruikt	- Misbruik van standaard credentials - Compromitteren van systemen - Lateraal bewegen - Relay aanvallen - Man-in-the-Middle aanvallen - Escaleren van rechten
2. Onjuiste scheiding in privileges	- Beheerders kennen meerdere rollen toe aan één account - Te veel rechten toekennen aan gebruikers en serviceaccounts - Niet noodzakelijk gebruik van geprivilegieerde accounts	- Lateraal bewegen - Escaleren van rechten - Vergroten van het aanvalsoppervlak
3. Ontoereikend monitoren van het interne netwerk	- Onvoldoende sensoren in het netwerk geplaatst - Onvoldoende logging en centrale collectie daarvan	- Onvoldoende omgevingsbewustzijn - Niet of te laat een incident detecteren - Het niet kunnen verzamelen van bewijsmateriaal
4. Onvoldoende netwerksegmentatie	- Geen of onvoldoende grenzen tussen de gebruikers, systemen en netwerken	- Lateraal bewegen - Kwetsbaarder voor ransomware aanvallen
5. Slecht patch management	- Patches worden niet regelmatig doorgevoerd - Verouderde systemen worden gebruikt zonder compenserende maatregelen	- Uitbuiten van kwetsbaarheden wat kan leiden tot bijvoorbeeld ongeautoriseerde toegang, denial of service of het kunnen uitvoeren van willekeurige code.
6. Omzeilen van toegangscontroles	- Credentials worden hergebruikt voor verschillende systemen - Onvoldoende isolatie van geprivilegieerde accounts - Geen lock-out beleid bij onjuiste loginpogingen	- Pass the hash of kerberoasting aanvallen - Escaleren van rechten - Lateraal bewegen
7. Zwakke of misconfiguraties in MFA methodes	- MFA methode is niet bestand tegen phishing aanvallen	- Pass the hash aanvallen - Ongeautoriseerde toegang
8. Onvoldoende toegangscontrole op netwerkschijven en -services	- Onjuiste configuratie van access control lists (ACL) - Credentials in leesbare tekst opslaan	- Verzamelen en exfiltreren van data - Afpersen en publiceren data - Bewerkstelligen van omgevingsbewustzijn voor aanvallers
9. Slechte hygiëne credentials	- Gebruik van zwakke wachtwoorden - Credentials in leesbare tekst opslaan	- Kraken van wachtwoorden - Pass the hash aanvallen - Escaleren van rechten - Lateraal bewegen
10. Ongelimiteerde uitvoer van code	- Het kunnen uitvoeren van niet geverifieerde software	- Uitvoeren van kwaadaardige code - Escaleren van rechten

Tabel 2: Top 10 misconfiguraties in een notendop