Samen aanjagen van vernieuwing

Handreiking security baselines

SM.01 SURFaudit Toetsingskader Informatiebeveiliging

Auteur(s): Ry Boxem & Mick Deben
Versie: 1.0
Datum: 6 mei 2025
Kenmerk: Handreiking security baselines

Inhoudsopgave

1 Inleiding

Verschillende instellingen hebben kenbaar gemaakt dat zij het statement SM.01 Security baselines uit het SURFaudit Toetsingskader Informatiebeveiliging lastig te interpreteren vinden. Dit is dan ook de aanleiding geweest om deze handreiking op te stellen. Het doel is om instellingen te ondersteunen in het beheersen van risico's en het bereiken van het gewenste volwassenheidsniveau voor dit betreffende statement. Aanvullend daarop geven we voorbeelden van bewijslast ten behoeve van interne en externe verantwoording.

Wat zegt het SURFaudit Toetsingskader over SM.01 Security Baselines?

Risico: Afwezige of onjuiste beveiligingsbaselines kunnen leiden tot een afwijkende of inconsistente implementatie van beveiligingsparameters, wat uiteindelijk leidt tot ongeautoriseerde toegang of verstoring van IT-services.

Beheersdoelstelling: beveiligingsbaselines en richtlijnen voor IT-infrastructuur worden gebruikt om het risico van ongeoorloofde toegang tot IT-middelen te beperken. Beveiligingsbaselines worden formeel vastgesteld, 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.

Wat is vereist voor het derde volwassenheidsniveau?

- Beveiligingsbaselines zijn gedefinieerd, goedgekeurd door senior management en gecommuniceerd aan verantwoordelijk IT-personeel.
- De geïmplementeerde beveiligingsinstellingen voor IT-middelen worden periodiek gecontroleerd op overeenstemming met de beveiligingsbaselines.
- Resultaten worden gedocumenteerd, afwijkingen worden gedocumenteerd en goedgekeurd (of gecorrigeerd).
- Voor nieuwe IT-infrastructuur componenten en projectmanagement processen wordt implementatie van beveiligingsbaselines afgedwongen.
- In hoeverre aan de baseline wordt voldaan wordt periodiek gerapporteerd aan senior management.

Let op: security baselines dienen met en door IT-personeel gedefinieerd te worden en kunnen vervolgens door senior management goedgekeurd worden. Andersom is onlogisch en onrealistisch, aangezien senior management daar over het algemeen geen gedegen uitspraken over kan doen.

Scope
Concreet betekent dit statement dat security baselines toegepast moeten worden voor alle I(o)T-gerelateerde hardware, middleware, firmware en software, zoals bijvoorbeeld netwerkapparaten, printers, camerasystemen, toegangscontrolesystemen, mobiele apparaten, firmware, slimme apparaten, wearables, enzovoort.

2 Security baselines

2.1 Wat is een security baseline?

Definitie van NIST[1]: “Security baselines zijn vooraf gedefinieerde sets van maatregelen die specifiek zijn samengesteld om de beschermingsbehoeften van groepen en organisaties te behartigen. De security baselines dienen als uitgangspunt voor de bescherming van de privacy van individuen, informatie en informatiesystemen en kunnen op maat worden gemaakt, waarbij rekening gehouden wordt met de missie en bedrijfsfuncties van de organisatie, dreigingsinformatie en de omgeving waarin de organisatie opereert”. Een security baseline is dus een minimaal niveau van beveiliging dat standaard in een bepaalde context toegepast wordt. Voor IT-middelen gaat het is het doel het realiseren van veilige configuraties door middel van hardening[2], oftewel het realiseren van een ‘known good’ configuratie.

2.2 Hoe bepaal je security baselines?

Risicogebaseerd natuurlijk! Security baselines zijn eigenlijk altijd maatwerk, er bestaat simpelweg geen one-size fits all. Dit komt door verschillende factoren zoals het dreigingslandschap, gebruikte technologie, de organisatorische doelstellingen, wetgeving, etc. Het blindelings overnemen van security baselines wordt afgeraden. Kijk altijd kritisch naar de security baseline om te voorkomen dat dingen stuk gemaakt worden voor jouw specifieke situatie. Heel pragmatisch kun je jezelf de volgende vraag stellen: *welke functionaliteiten heeft het systeem minimaal nodig voor het beoogde doeleinde?* Hanteer dit als uitgangspunt en schakel overige zaken uit of blokkeer ze. Dit verkleint het aanvalsoppervlak aanzienlijk waardoor de kansen tot misbruik voor aanvallers afnemen. Afhankelijk van de geïdentificeerde risico’s kunnen er aanvullende of compenserende maatregelen, zoals monitoring, van toepassing zijn boven op de security baseline.

Het is raadzaam om gebruik te maken van security baselines die actief worden ontwikkeld en onderhouden door de cybersecurity community. De security baselines van het Center for Internet Security (CIS), ook wel CIS benchmarks[3] genoemd, worden aanbevolen. Deze worden actief onderhouden en in diverse formaten beschikbaar gesteld, zoals bijvoorbeeld XML. De documentatie van CIS benchmarks is erg goed waardoor het eenvoudig is om de aanbevelingen te reproduceren en om de rationale en impact van maatregelen te begrijpen (zie onderstaand voorbeeld). Via SURF is het voor leden mogelijk om de CIS SecureSuite aan te schaffen onder aantrekkelijke voorwaarden.

2.1.1.3.2.1.1 (L1) Ensure 'Allow Trusted Locations on the network' is set to 'Disabled' Fail

Description:

This policy setting controls whether trusted locations on the network can be used. Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe by the application opening the file.

The recommended state for this setting is: `Disabled` .

Rationale:

Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm the user's computers or data.

Remediation:

To establish the recommended state via configuration profiles, set the following Settings Catalog path to `Disabled` .

`Microsoft Access 2016\Application Settings\Security\Trust Center\Trusted Locations\Allow Trusted Locations on the network`

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. These custom locations added by users are ignored but not removed. Trusted locations added that specify a network location are also ignored.

Assessment:
Show Assessment Evidence

Show Rule Result XML

References:

CIS Critical Security Controls V8.0:

- **Not Explicitly Mapped:** -- More
  >

Back to Summary

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

[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://www.cisecurity.org/cis-benchmarks

2.3 Hoe onderhoud je security baselines?

Een belangrijk aandachtspunt is het realiseren van een relatie tussen het wijzigingsproces en het onderhouden van security baselines. Updates, upgrades, patches, hotfixes, enzovoort kunnen namelijk negatieve impact hebben op security baselines. Hoe weet je of de security baseline nog steeds naar behoren werkt na het doorvoeren van een wijziging? Het doornemen van de release notes geeft geen zekerheid, maar verificatie van de security baseline wel, bijvoorbeeld met CIS Secure Suite. Identificeer hiaten, los ze op en stel de security baseline eventueel bij ('golden image').

2.4 Welke security baselines zijn er?

Gelukkig zijn er al diverse (verzamelingen van) security baselines ontwikkeld door diverse organisaties en instellingen. De meest gebruikte baselines voor onderwijsinstellingen zijn de:

- SURF Security Baseline;
- Center for Internet Security Controls (CIS);
- Microsoft Security Baseline.

De SURF security baseline (SSB) voorziet instellingen van een set concrete maatregelen om systemen en diensten te beveiligen. Omdat de maatregelen gekoppeld zijn aan het SURFaudit toetsingskader, stelt de SBB instellingen in staat om snel praktisch invulling te geven aan de controls op het gebied van technische weerbaarheid. De voordelen van CIS en Microsoft daarentegen is dat er voor beide ook benchmark tooling beschikbaar is die op een systeem uitgevoerd kan worden waar (voor dat systeem) dan een rapportage uit komt die aangeeft waar er wel en niet wordt voldaan aan de baseline.

Er zijn veel meer security baselines, ook toegespitst op bijvoorbeeld IoT, OT en Firmware. Zie bijlage 1 voor een overzicht van de meest voorkomende baselines met bijbehorende links.

2.5 Het maken van een keuze, en prioriteren

De verschillende baselines in bijlage 1 bieden een goed vertrekpunt voor het realiseren van security baselines. Het blijft echter belangrijk om altijd kritisch door de lijst van aanbevelingen te lopen en op basis van een risico-afweging te bepalen of aanbevelingen wel of niet overgenomen worden.

Het kritisch analyseren van security baselines is tijdrovend dus waar begin je? Ook hierbij geldt dat risicogebaseerd werken de voorkeur heeft. Begin met edge devices die direct vanaf het internet benaderbaar zijn en vervolgens met kritieke systemen in het interne netwerk. Breid de dekkingsgraad van security baselines op deze manier steeds verder uit naar minder belangrijke systemen. Eventuele uitzonderingen op security baselines kun je volgens de procedure afwijkingen registreren en monitoren.

2.6 Formele goedkeuring

Voor het formeel laten goedkeuren van security baselines is het belangrijk dat de gevolgen van technische configuraties in begrijpbare taal aan het management worden uitgelegd. Het is hierbij belangrijk om het verschil tussen de gewenste situatie (SOLL) ten opzichte van de huidige situatie (IST) duidelijk te maken. Dit kan bijvoorbeeld door het scannen van een bestaand systeem ten

opzichte van een security baseline waaruit blijkt wat de gap daartussen is (zie figuur). Vervolgens kun je per wijziging toelichten wat de impact is, bijvoorbeeld door de rationale van de CIS Benchmarks te raadplegen. Wijzigingen die veel impact hebben op eindgebruikers zijn de belangrijkste beslispunten voor het management. Denk hierbij aan het ontnemen van de mogelijkheid tot het gebruik van USB-randapparatuur of het zelfstandig kunnen installeren van software. Probeer in het advies aan het management de nadruk op deze impactvolle wijzigingen te leggen.

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Computer Configuration	**0**	**18**	**0**	**0**	**0**	**0**	**0.0**	**18.0**	**0%**
1.1 Administrative Templates	0	2	0	0	0	0	0.0	2.0	0%
1.1.1 MS Security Guide	0	2	0	0	0	0	0.0	2.0	0%
1.2 Microsoft Office 2016 (Machine)	0	16	0	0	0	0	0.0	16.0	0%
1.2.1 Customize	0	0	0	0	0	0	0.0	0.0	0%
1.2.2 Global Options	0	0	0	0	0	0	0.0	0.0	0%
1.2.3 Licensing Settings	0	0	0	0	0	0	0.0	0.0	0%
1.2.4 Miscellaneous	0	0	0	0	0	0	0.0	0.0	0%
1.2.5 Security Settings	0	14	0	0	0	0	0.0	14.0	0%
1.2.5.1 IE Security	0	14	0	0	0	0	0.0	14.0	0%
1.2.6 Updates	0	2	0	0	0	0	0.0	2.0	0%
2 User Configuration	**9**	**199**	**0**	**0**	**0**	**0**	**9.0**	**208.0**	**4%**
2.1 Microsoft Access 2016	0	8	0	0	0	0	0.0	8.0	0%
2.1.1 Application Settings	0	5	0	0	0	0	0.0	5.0	0%
2.1.1.1 General	0	0	0	0	0	0	0.0	0.0	0%
2.1.1.2 International	0	0	0	0	0	0	0.0	0.0	0%
2.1.1.3 Security	0	4	0	0	0	0	0.0	4.0	0%
2.1.1.3.1 Cryptography	0	0	0	0	0	0	0.0	0.0	0%
2.1.1.3.2 Trust Center	0	4	0	0	0	0	0.0	4.0	0%
2.1.1.3.2.1 Trusted Locations	0	1	0	0	0	0	0.0	1.0	0%
2.1.1.4 Web Options...	0	1	0	0	0	0	0.0	1.0	0%
2.1.1.4.1 General	0	1	0	0	0	0	0.0	1.0	0%
2.1.2 Customizable Error Messages	0	0	0	0	0	0	0.0	0.0	0%

2.7 Security baselines in een breder perspectief

SM.01 heeft uitsluitend betrekking op IT-middelen, maar security baselines kun je in breder perspectief toepassen. Door risicogebaseerd classificatie toe te passen kun je security baselines ontwikkelen die verder gaan dan IT-middelen. Dit kan bijvoorbeeld door per onderwerp een classificatieschema (beschikbaarheid, integriteit, vertrouwelijkheid) uit te werken waarbij per classificatieniveau de security baseline bepaald wordt. Zie hieronder een voorbeelduitwerking op een aantal onderwerpen. Dergelijke security baselines kun je dus ook ontwikkelen voor niet-technische thema's zoals screening, fysieke beveiliging en risicomanagement.

Behandeling	BESCHIKBAARHEID			
	Niveau 0 (niet nodig)	Niveau 1 (belangrijk)	Niveau 2 (noodzakelijk)	Niveau 3 (essentieel)
	Minder maatregelen ←			→ Meer maatregelen
Restore	Minimaal 1x per jaar wordt een herstel-test uitgevoerd om vast te stellen of het succesvol herstellen vanaf een backup mogelijk is én binnen de maximaal aanvaardbare periode (RTO) uitgevoerd kan worden.	Minimaal 1x per halfjaar wordt een herstel-test uitgevoerd om vast te stellen of het succesvol herstellen vanaf een backup mogelijk is én binnen de maximaal aanvaardbare periode (RTO) uitgevoerd kan worden.	Minimaal 1x per kwartaal wordt een herstel-test uitgevoerd om vast te stellen of het succesvol herstellen vanaf een backup mogelijk is én binnen de maximaal aanvaardbare periode (RTO) uitgevoerd kan worden.	Minimaal 1x per maand wordt een herstel-test uitgevoerd om vast te stellen of het succesvol herstellen vanaf een backup mogelijk is én binnen de maximaal aanvaardbare periode (RTO) uitgevoerd kan worden.

Behandeling	INTEGRITEIT			
	Niveau 0 (niet nodig)	Niveau 1 (beschermd)	Niveau 2 (hoog)	Niveau 3 (absoluut)
	Minder maatregelen ←			→ Meer maatregelen
Registratie	Informatie mag buiten de bron worden opgeslagen.	Informatie mag alleen in de door I&A gefaciliteerde middelen gewijzigd worden.	Informatie mag alleen in de bron gewijzigd ('Single Point of Truth') en opgeslagen worden.	Informatie wordt alleen in de bron gewijzigd ('Single Point of Truth') en niet buiten de bron opgeslagen worden (behalve voor beschikbaarheid).

Behandeling	VERTROUWELIJKHEID			
	Niveau 0 (openbaar)	Niveau 1 (intern gebruik)	Niveau 2 (vertrouwelijk)	Niveau 3 (geheim)
	Minder maatregelen ←			→ Meer maatregelen
Toegang	Voor openbare informatie gelden geen toegangsrestricties.	De informatie mag intern vrij worden verspreid. Als medewerkers toegang verkrijgen tot interne informatie die niet voorkomt in de autorisatiematrix is dit geen informatiebeveiligingsincident. Wanneer derden hier toegang tot krijgen is dit wel het geval. Toegang tot interne informatie wordt uitsluitend verleend via Multifactor authenticatie (MFA).	Toegang wordt uitsluitend verleend op basis van de principes 'need-to-know' en 'least privilege'.[31] Als medewerkers of derden onterecht toegang krijgen tot vertrouwelijke informatie is dat een informatiebeveiligingsincident. Toegang wordt uitsluitend verleend via Multifactor authenticatie (MFA).	Toegang wordt uitsluitend verleend op basis van de principes 'need-to-know' en 'least privilege'. Als medewerkers of derden onterecht toegang krijgen tot vertrouwelijke informatie is dat een informatiebeveiligingsincident. Toegang wordt uitsluitend verleend via Multifactor authenticatie (MFA).

3 Toepassen

Na het vaststellen van de gewenste security baseline is het moment daar om ze daadwerkelijk toe te gaan passen. Dit toepassen dient gepland en weloverwogen te gebeuren. De volgende stappen zijn essentieel voor een goede implementatie.

3.1 Testen van security baselines

Voordat security baselines uitgerold worden op productiesystemen is het raadzaam om deze eerst te testen in gecontroleerde omgevingen. Zo kun je vaststellen of verwachte functies blijven werken en kun je verstoringen en toenames in incidentmeldingen beperken. Daarnaast is het zoals eerder aangegeven belangrijk om alert te zijn op verzwakkingen van de security baseline door wijzigingen. Het is raadzaam om na (majeure) wijzigingen naleving van de security baselines opnieuw te verifiëren. Zo kunnen hiaten geïdentificeerd en opgelost worden.

3.2 Automatiseren van implementatie

Automatiseren zorgt voor consistentie, het verminderen van handwerk verlaagt de kans op fouten en vergissingen. Dit is ook van toepassing op security baselines. Er zijn meerdere methodieken en tools die hierbij kunnen helpen. Er is een overzicht van alle tools en de functionele meerwaarde ervan te vinden in bijlage 2.

3.3 Rapporteren

Er zijn verschillende niveaus te onderscheiden op basis waarvan gerapporteerd wordt. Dit kan enerzijds de huidige configuratiestaat (IST) van het doelsysteem ten opzichte van de security baseline (SOLL) zijn óf de dekkingsgraad van de security baselines gezien over het totaal aantal doelsystemen. Het eerste bepaald hoe strikt de beveiliging daadwerkelijk is op het doelsysteem en het laatste ziet erop toe dat het gewenste beveiligingsniveau over de gehele linie gehandhaafd wordt. Met name het laatste is belangrijk aangezien aanvallers altijd net dat ene systeem weten te vinden waar de baseline niet op actief was.

"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."
John Lambert, Microsoft Threat Intelligence Center.

3.4 Evalueren en actualiseren

Zoals aangegeven in 2.3 is het belangrijk om de security baseline te blijven onderhouden. Dit onderhoud wordt uitgevoerd door een aantal dingen periodiek te evalueren en wanneer nodig te actualiseren. Er zijn verschillende niveaus waarop met een verschillende cadans een dergelijke evaluatie gewenst kan zijn, een mogelijk voorbeeld daarvan:

- Thema beleid: 1-3 jaar
- Richtlijn: half-< 1 jaar
- Procedure: < 1 jaar .

Uit een combinatie van de rapportage en evaluatie kan voortkomen dat voor een bepaald device de baseline moet worden geactualiseerd. Dit is dan iets wat in de procedure vastgelegd kan worden.

Bijlage 1 Overzicht security baselines

Een overzicht van de meest voorkomende baselines met bijbehorende links naar de informatie/documentatie.

IT:

- SURF security baseline
- Center for Internet Security Controls
- Center for Internet Security (CIS) Benchmarks
- NIST National Checklist Program (NCP)
- Microsoft Security Baselines
- Secure Cloud Business Applications (SCuBA)
- Awesome security hardening
- DevSec Hardening Framework
- Securing Web Application Technologies (SWAT) Checklist
- Security Technical Implementation Guides (STIGs)

IoT:

- Basisbeveiligingsmaatregelen slimme apparaten (IoT)
- Baseline Security Recommnedations for IoT
- IoT Device Cybersecurity Capability Core Baseline
- OWASP Internet of Things Top Ten
- IoT Security Verification Standard

OT:

- Configuration Hardening Assessment PowerShell Script (CHAPS)
- Stand-Alone Windows Hardening (SAWH)
- Awesome hardening
- ICS/OT Security Hardening Checklist

Firmware:

- UEFI Defensive Practices Technical Report
- UEFI Lockdown Quick Guide
- Boot Security Modes
- Hardware and Firmware Security Guidance
- Hardware Security Requirements for x86 Platforms

Bijlage 2 Ondersteunende tools

Tool	Omschrijving	Functie
Ansible[4]	Ansible is een open-source automatiseringstool waarmee je IT-taken zoals software-installaties, configuratiebeheer en het uitrollen van applicaties kunt automatiseren zonder agents.	Automatiseren van configuraties
Chef[5], Puppet[6]	Chef en Puppet zijn open-source automatiseringstools waarmee je IT-taken zoals software-installaties, configuratiebeheer en het uitrollen van applicaties kunt automatiseren met lokale agents.	Automatiseren van configuraties
Intune[7]	Intune stelt beheerders in staat om beleid toe te passen voor beveiliging, updates, toegang tot bedrijfsresources en app-distributie — allemaal zonder fysieke toegang tot de apparaten.	Afdwingen van configuraties gericht op eindgebruikers
CIS SecureSuite[8].	Een programma dat organisaties toegang biedt tot een uitgebreide set cybersecuritytools en -bronnen. Het is ontworpen om organisaties te helpen bij het implementeren en beheren van effectieve beveiligingsmaatregelen, en om te voldoen aan industriestandstandaarden aarden en eisen.	Ondersteuning implementatie en beheer baselines.
Terraform[9].	Terraform is een open-source tool waarmee je infrastructuur in de cloud kunt beheren als code (Infrastructure as Code, IaC).	Geautomatiseerde provisioning in cloud.

[4] https://docs.ansible.com/

[5] https://community.chef.io/

[6] https://www.puppet.com/

[7] https://learn.microsoft.com/en-us/intune/intune-service/protect/security-baselines-configure

[8] https://www.cisecurity.org/cis-securesuite

[9] https://developer.hashicorp.com/terraform