MSBFS 2020:7 och Sunet Drive

På denna sida dokumenterar vi hur Sunet Drive uppfyller MSBs riktlinjer för säkerhetsåtgärder i informationssystem för statliga myndigheter.

Paragraf	MSBFS 2020:7 Text	Sunet	Kundens eget arbete	Referenser
Kapitel 2				
2	Myndigheten ska bedriva omvärldsbevakning för att underlätta identifiering och hantering av hot mot och sårbarheter i myndighetens informationssystem.	Detta arbete sker kontinuerligt inom ramen för Sunet SOC för samtliga Sunet-tjänster	Detta måste sker för komponenter där kunden tar ansvar för drift och underhåll, t.ex. SAML-inloggningen eller node-specifika anpassningar.	
3	Myndigheten ska genomföra riskbedömning för enskilda informationssystem och myndighetens produktionsmiljö i sin helhet.	Detta arbete sker kontinuerligt inom ramen för Sunet SOC för samtliga Sunet-tjänster	Kunden kan genomföra en riskbedömning och avstämmer det med sina processer.	
4	Myndigheten ska upprätthålla uppdaterad dokumentation över 1. hård- och mjukvara som används i varje enskilt informationssystem, 2. beroenden mellan olika interna informationssystem respektive beroenden av informationssystem hos externa aktörer, 3. vilka informationssystem som behandlar information som har behov av utökat skydd, och 4. vilka informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag.	Detta ingår i Sunet arbete med samtliga tjänster.	Vissa av dessa krav handlar om värdering av skyddsvärd information som i samtliga fall ligger på kundens ansvar.	
Kapitel 3				
1	Myndigheten ska, vid utveckling, anskaffning eller utkontraktering av informationssystem, identifiera krav på säkerhet avseende 1. uppdelning i nätverkssegment, 2. filtrering av nätverkstrafik, 3. behörigheter, digitala identiteter och autentisering, 4. kryptering, 5. säkerhetskonfigurering, 6. säkerhetstester och granskningar, 7. ändringshantering, uppgradering och uppdatering, 8. robust och korrekt tid, 9. säkerhetskopiering, 10. säkerhetsloggning och tillhörande analys, 11. övervakning av nätverkstrafik, 12. övervakning av informationssystem inklusive säkerhetsfunktioner, 13. skydd mot skadlig kod, 14. skydd av utrustning, 15. redundans och återställning, 16. kontinuitet under fredstida krissituation samt inför och vid höjd beredskap, 17. arkivering, och 18. avveckling. Myndigheten ska dokumentera vilka säkerhetsåtgärder som valts för att möta respektive krav.	Alla Sunet-tjänster designas med dessa principer som utgångspunkt. Specifikt: • Alla tjänster designas utifrån principen "defence in depth" vilket bla betyder att brandväggar och nätverksfiltrering sker på flera nivåer i en tjänst. Sunet drive använder både OpenStack security groups såväl som hostbrandväggar som skapas automatiskt av vårt CM-system. • Digitala identiteter hanteras mha integration med SAML. En gemensam redundant SAML2SAML-proxy baserad på SATOSA används för att ansluta såväl SWAMID som andra eID till tjänten. • Sunet Drive erbjuder access till nextcloud API (via sk API-nycklar) som kan användas för att provisionera och de-provisionera identiteter. • Sunet Drive har stöd för kryptering av filer. Alla hemligheter eller andra uppgifter med skyddsvärde (tex databaslösenord) lagras i krypterad form i infrastrukturen. Access sker integrerat med vårt CM-system. • Alla Sunet system synkroniserar tid med PTS tidsservrar. • Alla konfigurationsförändringar är spårbara och säkerställs via digitala signaturer i vårt CM. • Säkerhetskopiering av systemets infrastruktur utom fil-data sker via Sunet BaaS. • Loggning sker till Sunet loggningsinfrastruktur och kan på kundens initiativ även omdirigeras till kundens eget logghanteringssystem via syslog. • Övervakning av nätverkstrafik och loggar sker som del av Sunets driftsarbete. Detta inkluderar hantering av DDoS-attacker. • Allt säkerhetsarbete i Sunet sker med fokus på förebyggande arbete. Detta inkluderar omvärldsbevakning i syfte att fånga upp och motverka aktuella attacker. Detta arbete tillämpas på samtliga Sunet-tjänster. Sunets tjänster etableras i datacenter med högsta säkerhetsklassning.	• Deprovisionering av identiteter sker på kundens initiativ mha API. • Användning av netcloud inbyggda stöd för kryptering sker på initiativ från kunden. • Konfiguration av separat logghantering ingår inte i tjänsten. Det finns planer på att etablera en loggtjänst i Sunet. För närvarande hänvisar vi till den inbyggda logghanteringen i nextcloud.	https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/logging_configuration.html
2	Myndigheten ska, innan driftsättning och inför förändring som kan påverka säkerheten i informationssystemen, 1. genom säkerhetstester och granskning kontrollera att valda säkerhetsåtgärder är tillräckliga för att möta identifierade krav på säkerhet, och 2. verifiera att det finns nödvändig dokumentation för drift och förvaltning.	• Detta arbete sker inom ramen för Sunets interna process för överlämning till Drift.	• Kunden kan utföra egna tester i test- och produktionsmiljön.	
3	Myndighetens arbete med utveckling och tester som kan påverka informationssäkerheten i produktionsmiljön ska ske i en från produktionsmiljön avskild del av it-miljön.	• Sunet Drive har en separat test- och utvecklingsmiljö.		
4	Myndigheten ska identifiera och hantera behovet av en utbildningsmiljö som är avskild från produktionsmiljön.	• Något behov av separat utbildningsmiljö för Sunet Drive har inte identifierats.		
Kapitel 4				
1	Myndigheten ska förhindra spridning av incidenter och minska konsekvenser av angrepp genom att placera informationssystem med olika funktioner i separata nätverkssegment i sin produktionsmiljö.	• I Sunet Drive implementeras detta dels genom OpenStack security groups. Se även punkten om säkerhetsarbete ovan. • Sunet Drive implementerar en "global scale" arkitektur där enskilda noder kör på separata virtuella maskiner.		

2	Myndigheten ska filtrera nätverkstrafiken så att endast nödvändiga dataflöden förekommer mellan olika nätverkssegment.	• I Sunet Drive implementeras detta dels genom OpenStack security groups. Se även punkten om säkerhetsarbete ovan.		
3	Myndigheten ska säkerställa att endast behöriga användare och informationssystem har åtkomst till it-miljön och utforma sin behörighetshantering på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver.		• Detta krav ligger i huvusak på kundens ansvar och möjliggörs av tekniska funktioner i nextcloud.	https://docs.nextcloud.com/server/latest/admin_manual/configuration_user/index.html
4	Digitala identiteter som ger systemadministrativ behörighet ska endast användas för systemadministration och tilldelas restriktivt.	• Sunet delar upp ansvar för olika säkerhetskritiska administrativa åtgärder på olika grupper.		
5	Flerfaktorsautentisering ska användas vid 1. egen och inhyrd personals åtkomst till produktionsmiljön via externt nätverk, 2. systemadministrativ åtkomst till informationssystem, och 3. åtkomst till informationssystem som behandlar information som bedömts ha behov av utökat skydd.	• Sunet CM-system kräver digitala signaturer med hårdvarubaserade multifator-tokens (MFA) för samtliga förändringar. Dessa förändringar spåras och valideras av samtliga ingående system. • Access till nextcloud kan konfigureras så att MFA alltid krävs. Det pågår arbete med att identifiera möjliga utvecklingsprojekt som gör det enklare att styra åtkomst på en mer detaljerad nivå i nextcloud baserad på sk förtroendenivåer.	• Kunden har möjlighet att använda antingen MFA i nextcloud, via eduID eller via egen IdP.	https://apps.nextcloud.com/apps/twofactor_u2f https://apps.nextcloud.com/apps/twofactor_totp
6	Myndigheten ska ha interna regler för hantering av autentiseringsuppgifter med krav på 1. längd och komplexitet, 2. när byte ska ske, 3. hur distribution ska ske, och 4. hur autentiseringsuppgifterna ska skyddas.	• Hantering av identiteter är i huvudsak en fråga för lärosätet eftersom Sunet Drive använder SAML för all identitetshantering. • Lokala konton i nextcloud som används för administration ska använda U2F eller TOTP.	• Dessa regler hanteras i huvudsak inom SWAMID och genom dokumentation av lärosätets regler för lösenords- och inloggningshantering.	
7	Myndigheten ska identifiera och hantera behovet av kryptering för att skydda information mot obehörig åtkomst och obehörig förändring vid överföring och lagring.	• Sunet Drive har stöd för kryptering av filer via inbyggda funktioner i nextcloud.	• Användning av nextcloud egna funktioner för kryptering kräver etablerade processer hos kunden för hantering och arkivering av kryptonycklar.	https://docs.nextcloud.com/server/latest/admin_manual/configuration_files/encryption_configuration.html
8	Myndigheten ska använda Domain Name System Security Extensions (DNSSEC) avseende samtliga domännamn som myndigheten registrerat i domännamnssystemet (DNS).	• Sunet Drive såväl som alla andra Sunet-zoner är signerade.		
9	Myndigheten ska ha interna regler för kryptering med krav på 1. hantering av krypteringsnycklar, 2. godkännande och förvaltning av krypteringslösningar, och 3. hur krypteringsalgoritmer, krypteringsprotokoll och nyckellängder ska väljas.	• Sunet Drive har stöd för kryptering av filer via inbyggda funktioner i nextcloud.	• Användning av nextcloud egna funktioner för kryptering kräver etablerade processer hos kunden för hantering och arkivering av kryptonycklar.	https://docs.nextcloud.com/server/latest/admin_manual/configuration_files/encryption_configuration.html
10	Myndigheten ska, för att skydda informationssystem mot obehörig åtkomst, 1. byta ut förinställda autentiseringsuppgifter, 2. stänga av, ta bort eller blockera systemfunktioner som inte behövs, och 3. i övrigt anpassa konfigurationer för att uppnå avsedd säkerhet.	• Sunet genomför periodisk genomgång av samtliga identiteter med systemåtkomst. Dessa identiteter införs och rensas från samtliga Sunet-tjänster via vårt CM-system ochdessa förändringar är därmed digitalt spårbara. • Hantering av identiteter i Sunet Drive är i huvudsak en fråga för lärosätet eftersom Sunet Drive använder SAML för all identitetshantering. • Lokala konton i nextcloud som används för administration ska använda U2F eller TOTP.		
11	Myndigheten ska säkerställa att säkerhetstester och granskningar möjliggör identifiering av sårbarheter. Myndigheten ska ha interna regler för hur kontroll görs av att 1. informationssystemen är uppdaterade, 2. valda säkerhetsåtgärder är införda på korrekt sätt, och	• Processen för underhåll av samtliga Sunet-tjänster innehåller rutiner för uppdatering av tjänsten • Säkerheten i systemet baseras på ett aktivt säkerhetsarbete inom Sunet SOC • Vårt CM-system garanterar att de förändringar som införs i systemet är verifierade och säkerställda samt autentiska och utförda av behörig personal.		
12	Myndigheten ska säkerställa att förändringar i informationssystem genomförs på ett strukturerat och spårbart sätt. Myndigheten ska ha interna regler för ändringshantering med krav på 1. vilka kriterier som ska användas för att godkänna hård- och mjukvara innan installation eller användning, 2. hur risker för incidenter och avvikelser i samband med förändring i produktionsmiljön ska identifieras och hanteras, 3. hur mjukvara, utan onödigt dröjsmål, ska uppdateras till senaste version, 4. hur utbyte eller uppgradering av hård- och mjukvara som inte längre uppdateras eller stöds av leverantören ska säkerställas utan onödigt dröjsmål, och 5. hur risker ska hanteras när uppdatering eller uppgradering enligt punkt 3 och 6. inte kan genomföras.	• Sunets interna processer för förändrings- och incidenthantering samt drift uppfyller dessa krav för samtliga Sunet-tjänster.		
13	Myndigheten ska använda robust och korrekt tid spårbar till den svenska tillämpningen av koordinerad universell tid, UTC(SP), i sin produktionsmiljö.	• Samtliga Sunet-system synkroniseras mot UTC(SP) via pts NTP-servrar.		

14	Myndigheten ska, för att kunna återställa information som förlorats eller förvanskats, regelbundet säkerhetskopiera sin information.	• Se svaret på paragraf 1, kapitel 3 ovan.	• OBS att backup av fil-data inte ingår i Sunet Drive utan måste köpas separat.	
15	Säkerhetskopior ska förvaras skilda från produktionsmiljön och skyddas mot skada, obehörig åtkomst och obehörig förändring.	• Sunet Drives säkerhetskopior är placerade i ett separat datacenter som inte används för produktionsdata.		
16	Myndigheten ska, för att säkerställa spårbarhet i informationssystem, logga följande säkerhetsrelaterade händelser: 1. Obehörig åtkomst och försök till obehörig åtkomst till it-miljö och enskilda informationssystem. 2. Förändringar av konfigurationer och säkerhetsfunktioner som förutsätter priviligierade rättigheter. 3. Förändringar av behörighet för användare och informationssystem. 4. Åtkomst till information som bedömts ha behov av utökat skydd.	• Sunet CM-system ger en digitalt signerad spårbarhet av samtliga förändringar av alla Sunet-tjänster. • Åtkomst av data i Sunet Drive sker med hjälp av de inbyggda loggfunktionerna i nextloud. • Loggar kan skickas vidare till valfritt externt system via syslog	• Kunden ansvarar för att använda de funktioner som finns i nextcloud logghantering i syfte att övervaka och upptäcka åtkomst till och förändring av data som inte ligger i linje med kundens policy, alternativt omdirigera loggning till ett eget system och där genomföra analysen. • Sunet har planer på att erbjuda en loggtjänst i framtiden som kommer erbjuda de tekniska möjlighet som krävs för att etablera rutiner för att övervaka åtkomst.	https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/logging_configuration.html
17	Myndigheten ska analysera innehållet i säkerhetsloggarna för att upptäcka och hantera incidenter och avvikelser. Säkerhetsloggarna ska 1. möjliggöra utredning av intrång, tekniska fel och brister i säkerheten, 2. utformas på ett sätt som möjliggör jämförbarhet mellan olika loggar, och 3. vara tillgängliga för analys under fastställd bevarandetid. Myndigheten ska dokumentera hur säkerhetsloggarna ska användas samt var loggningsuppgifter hämtas och lagras, hur de skyddas och hur länge de ska bevaras.	• Se ovan.		
18	Myndigheten ska identifiera och hantera behovet av intrångsdetektering och intrångsskydd.	• Säkerhetsarbetet i Sunet SOC inkluderar arbete med passiv och aktiv intrångsdetektering för samtliga Sunet-tjänster. • Nextcloud har inbyggd intrångsdetekteringen och skydd mot "brute force"		https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/bruteforce_configuration.html
19	Myndigheten ska identifiera och hantera behovet av realtidsövervakning av informationssystem.	• Samtliga Sunet-tjänster övervakas 247 av Sunet Driftsgrupp (NOC)		
20	Myndigheten ska använda mjukvara som ger skydd mot skadlig kod. För informationssystem där sådan mjukvara inte finns tillgänglig ska andra åtgärder vidtas som ger motsvarande skydd.	• Sunet Drive samt alla ingående komponenter är baserat helt på öppen källkod. Arbetet med skydd mot skadlig kod sker på flera nivåer inklusive ingående OpenSource projekt. • Filer som lagras i Sunet Drive kan scannas med antivirusmotorn ClamAV.	• Kontroll av klienters patchnivå (sk endpoint assessment) ingår inte i tjänsten idag. Denna funktion kan komma att utveklas eller kan evt utvecklas av kund mha nextcloud APIer.	https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/antivirus_configuration.html
21	Myndigheten ska skydda den utrustning som informationssystem består av mot skador och obehörig åtkomst, genom att 1. placera centrala servrar och central nätverksutrustning i särskilda itutrymmen, 2. tilldela behörighet till särskilda it-utrymmen restriktivt, 3. identifiera och hantera behovet av övervakning och larm i särskilda itutrymmen, 4. registrera tillträde till särskilda it-utrymmen på individnivå och spara dokumentationen under fastställd bevarandetid, och 5. ha interna regler för hur mobil utrustning ska skyddas.	• Samtliga Sunet-tjänster placeras i datacenter som uppfyller högt ställda IT-säkerhetskrav. I flera fall använder Sunet datacenter som är nationella skyddsobjekt. • Dessa datacenter uppfyller samtliga av MSB uppställda krav inklusive krav på registrering och övervakning av åtkomst.		
22	Myndigheten ska, för att säkerställa tillgänglighet till information och informationssystem vid incidenter och avvikelser, 1. ha interna regler för återställning av produktionsmiljön i sin helhet och för enskilda informationssystem, 2. öva återställning av informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och 3. placera centrala servrar och central nätverksutrustning som skapar redundant funktion i olika särskilda it-utrymmen.	• Sunet driftsrutiner säkerställer uppfyllelse av dessa krav.		
Kapitel 5				
1	De myndigheter som har ett särskilt ansvar för krisberedskapen enligt 10 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap ska, utöver vad som framgår av kapitel 2 – 4 i dessa föreskrifter, 1. använda flerfaktorsautentisering och realtidsövervakning för informationssystem som är centrala för myndighetens förmåga att utföra sitt uppdrag, och 2. en gång per kvartal verifiera förmågan till återställning av dessa system.	• Sunet Drive omfattas inte av detta.		

2	Myndigheten ska, en gång per kvartal, kontrollera funktionen hos informationssystem som ska användas för informationsdelning under fredstida krissituationer.	• Sunet Drive omfattas inte av detta.		