Sikkerhetsfunksjoner i macOS

Oversikt for IT-avdelingen

Apple designet macOS med en integrert tilnærming til maskinvare, programvare og tjenester som sørger for sikkerhet fra grunnen av, og som gjør det enkelt å konfigurere, rulle ut og administrere datamaskinene. macOS inneholder de viktigste sikkerhetsteknologiene IT-avdelingen trenger for å beskytte bedriftsdata og integrere systemet i sikre bedriftsnettverksmiljøer. Apple har også samarbeidet med standardiseringsorganer for å sikre samsvar med de nyeste sikkerhetssertifiseringene. Denne oversikten gir en kort beskrivelse av enkelte av disse funksjonene.

Dette dokumentet er delt inn i følgende emneområder:

- **Systemsikkerhet:** Den integrerte og sikre programvaren som utgjør ryggraden i macOS.
- **Kryptering og databeskyttelse:** Arkitekturen og designen som beskytter brukernes data hvis enheten blir stjålet eller kommer på avveier.
- **Appsikkerhet:** Systemene som beskytter Macen fra ondsinnet programvare og gjør at appene kan kjøres på en sikker måte, uten å gå på bekostning av plattformintegriteten.
- **Autentisering og digital signering:** Funksjonaliteten som er innebygd i macOS for administrering av påloggingsinformasjon og støtte for teknologier av bransjestandard som smartkort og S/MIME.
- **Nettverkssikkerhet:** Nettverksprotokoller av bransjestandard som gir sikker autentisering og kryptering av data under overføring.
- **Enhetskontroller:** Metoder som muliggjør administrering av Apple-enheter, forhindrer uautorisert bruk og gjør at man kan fjernslette enheter hvis de kommer på avveier eller blir stjålet.

Hvis du vil ha mer informasjon om utrulling og administrering av Apple-enheter, kan du lese veiledningen «macOS – Håndbok for utrulling» på help.apple.com/deployment/macos.

Hvis du vil ha mer informasjon om sikkerhetsfunksjoner for Apple-tjenester som ikke er omtalt her, kan du lese dokumentet om iOS-sikkerhet på www.apple.com/no/business/docs/iOS_Security_Guide.pdf.

Systemsikkerhet

Systemsikkerheten i macOS er utformet slik at både programvare og maskinvare sikres i alle kjernekomponenter i alle Macer. Denne strukturen er avgjørende for sikkerheten i macOS, men påvirker aldri brukervennligheten.

UNIX

macOS-kjernen – hjertet i operativsystemet – er basert på Berkeley Software Distribution (BSD) og Mach-mikrokjernen. BSD gir grunnleggende tjenester for filsystem- og nettverkstjenester, et identifiseringssystem for brukere og grupper og mange andre grunnleggende funksjonaliteter. BSD pålegger også tilgangsbegrensninger for filer og systemressurser basert på bruker- og gruppe-ID-er.

Mach har funksjoner for håndtering av minne, trådkontroll, maskinvareabstraksjon og interprosesskommunikasjon. Mach-porter representerer oppgaver og andre ressurser, og Mach kontrollerer tilgang til portene ved å styre hvilke oppgaver som kan sende meldinger til dem. BSD-sikkerhetsreglene og Mach-tilgangstillatelsene utgjør grunnlaget i sikkerhetsarkitekturen til macOS, og er av kritisk betydning for håndheving av sikkerhet lokalt.

Sikkerheten for kjernen er avgjørende for sikkerheten til operativsystemet i sin helhet. Kodesignering beskytter kjernen og kjerneutvidelser fra tredjeparter samt andre systembiblioteker og kjørbare filer utviklet av Apple.

Brukertillatelsemodell

Et viktig aspekt ved sikkerheten for Macer er det å godkjenne eller avvise tilgangstillatelser (også kalt tilgangsrettigheter). Tillatelser er evnen til å kunne utføre bestemte operasjoner, for eksempel å få tilgang til data eller kjøre kode. Tillatelser gis for følgende nivåer: mapper, undermapper, filer og apper samt for spesifikke data i filer, appmuligheter og administrative funksjoner. Digitale signaturer identifiserer tilgangsrettighetene til apper og systemkomponenter.

macOS styrer tillatelser på mange nivåer, inkludert for Mach- og BSD-komponentene i kjernen. macOS bruker nettverksprotokoller til å kontrollere tillatelser for nettverksbaserte apper.

Obligatoriske tilgangskontroller

macOS bruker også obligatoriske tilgangskontroller – regler som angir sikkerhetsbegrensninger som er opprettet av utvikleren, og som ikke kan overstyres. Denne tilnærmingen skiller seg fra diskresjonære tilgangskontroller, som tillater at brukerne overstyrer sikkerhetsregler etter eget ønske. Obligatoriske tilgangskontroller er ikke synlige for brukerne, men de utgjør den underliggende teknologien som muliggjør flere viktige funksjoner, inkludert sandboxing eller kjøring i testmiljø, foreldrekontroller, administrerte valg, utvidelser og Systembeskyttelse-funksjonen.

Systembeskyttelse

OS X 10.11 og nyere versjoner inkluderer beskyttelse på systemnivå, kalt Systembeskyttelse, som begrenser komponenter i bestemte kritiske filsystemlokasjoner i den forstand at de gjøres skrivebeskyttet, for å forhindre at ondsinnet kode kjører eller modifiserer dem. Systembeskyttelse er en datamaskinspesifikk innstilling som er aktivert som standard når du oppgraderer til OS X 10.11. Ved deaktivering fjernes beskyttelsen for alle partisjoner på den fysiske lagringsenheten. macOS bruker denne sikkerhetsregelen på alle prosessene som kjører på systemet, uavhengig av om den kjører i testmiljø (sandboxed) eller med administrative privilegier.

Hvis du vil ha mer informasjon om disse skrivebeskyttede delene av filsystemet, kan du lese Apples kundestøtteartikkel med tittelen «Om Systembeskyttelse på Mac» på support.apple.com/HT204899.

Kjerneutvidelser

macOS inneholder en mekanisme for kjerneutvidelser som muliggjør dynamisk innlasting av kode til kjernen, uten behov for rekompilering eller å måtte koble på nytt. Siden disse kjerneutvidelsene (KEXT) gir både modularitet og dynamisk innlasting, er de et naturlig valg for enhver relativt frittstående tjeneste som krever tilgang til interne kjernegrensesnitt, som eksempelvis enhetsdrivere for maskinvare eller VPN-apper.

For å ivareta sikkerheten på Macen kreves brukersamtykke for å laste kjerneutvidelser som ble installert med eller etter installering av macOS High Sierra. Dette er kjent som brukergodkjent lasting av kjerneutvidelser. Alle brukere kan godkjenne kjerneutvidelser, også om de ikke har administratortilgang.

Kjerneutvidelser krever ikke autorisering hvis de:

- ble installert på Macen før den ble oppgradert til macOS High Sierra
- erstatter tidligere godkjente utvidelser
- har tillatelse til å lastes inn uten brukergodkjenning ved å bruke `spctl`-kommandoen, som er tilgjengelig ved oppstart fra partisjonen for macOS-gjenoppretting
- har tillatelse til å lastes inn via en MDM-konfigurasjon. Fra og med macOS High Sierra 10.13.2 kan du bruke MDM til å spesifisere en liste med kjerneutvidelser som blir lastet inn uten brukergodkjenning. Dette alternativet krever en Mac som kjører High Sierra 10.13.2 og som er registrert i en MDM-løsning, enten via enhetsregistreringsprogrammet (DEP) eller via brukergodkjent MDM-registrering

Hvis du vil ha mer informasjon om kjerneutvidelser, kan du lese Apples kundestøtteartikkel med tittelen «Prepare for changes to kernel extensions in macOS High Sierra» på support.apple.com/HT208019.

Firmwarepassord

macOS har støtte for bruk av passord til å forhindre utilsiktede endringer i maskinvareinnstillingene på et bestemt system. Dette firmwarepassordet brukes til å forhindre:

- oppstart fra et ikke-autorisert systemvolum
- endring av oppstartsprosessen, for eksempel oppstart til modus for én bruker
- uautorisert tilgang til macOS-gjenoppretting
- direkte minnetilgang (DMA) via grensesnitt som Thunderbolt
- måldiskmodus, som krever DMA

Merk: Apples T2-chip i iMac Pro forhindrer brukere fra å kunne tilbakestille maskinvarepassordet, selv om de skulle få fysisk tilgang til Macen. På Macer som ikke har T2-chip, må ytterligere tiltak iverksettes for å forhindre at brukerne kan få fysisk tilgang til Macens indre.

Internett-gjenoppretting

Mac-datamaskiner prøver automatisk å starte opp fra macOS-gjenoppretting over internett hvis de ikke lykkes med oppstart via det innebygde systemet for gjenoppretting. Når dette skjer, kommer det opp en roterende globus i stedet for en Apple-logo under oppstart. Internett-gjenoppretting gjør det mulig for brukeren å installere den nyeste versjonen av macOS eller versjonen Macen opprinnelig ble levert med, på nytt.

macOS-oppdateringer distribueres gjennom App Store og gjennomføres med macOS-installerer, som bruker kodesignaturer til å verifisere integriteten og autentisiteten av installeringsprogrammet og pakkene før installering.

På samme måte fungerer Internett-gjenoppretting som den autoritative kilden for operativsystemet den enkelte Macen ble levert med.

Hvis du vil ha mer informasjon om macOS-gjenoppretting, kan du lese Apples kundestøtteartikkel med tittelen «Om macOS-gjenoppretting» på support.apple.com/HT201314.

Kryptering og databeskyttelse

Apple File System

Apple File System (APFS) er et nytt og moderne filsystem for macOS, iOS, tvOS og watchOS. Det er optimalisert for slash-/SSD-lagring, og har funksjoner for sikker kryptering, kopiering ved skriving-metadata, plassdeling, kloning av filer og kataloger, øyeblikksbilder, rask katalogskalering, atomiske primitiver for sikker lagring og forbedrede filsystemgrunnlag samt en unik kopiering ved skriving-utforming som bruker I/O-oppsamling til å gi maksimal ytelse og datapålitelighet.

APFS reserverer diskplass ved behov. Når en enkelt APFS-beholder har flere volumer, deles den tilgjengelige plassen i beholderen. Dette kan fordeles til hvilke som helst av de enkelte volumene etter behov. Hvert volum bruker bare en del av den overordnede beholderen, så den tilgjengelige plassen er den totale størrelsen av beholdere minus plassen som brukes av alle volumene i beholderen.

For macOS High Sierra må en gyldig APFS-beholder inneholde minst tre volumer, der de to første er skjult for brukeren:

- Forhåndsoppstartsvolumet: Inneholder dataene som trengs for å starte opp hvert av systemvolumene i beholderen.
- Gjenopprettingsvolumet: Inneholder Gjenopprettingsdisken.
- Systemvolumet: Inneholder macOS og Bruker-mappen.

FileVault

Alle Macer er utstyrt med innebygd krypteringsfunksjonalitet, kalt FileVault, som sikrer data som ikke er i bruk. FileVault bruker XTS-AES-128-kryptering av data for å sikre data på Macen som ikke er i bruk. Dette kan brukes til å gi fullstendig volumbeskyttelse av interne og eksterne lagringsenheter. Hvis en bruker skriver inn en Apple ID og passordet ved kjøring av Oppsettsassistenten, foreslår assistenten å aktivere FileVault og oppbevare nøkkelen for gjenoppretting i iCloud.

Brukere som aktiverer FileVault på Mac, bes om å oppgi gyldig påloggings-informasjon før oppstartsprosessen fortsetter, blant annet for å få tilgang til spesialiserte oppstartsmoduser som eksempelvis Måldiskmodus. Uten gyldig påloggingsinformasjon eller nøkkel for gjenoppretting forblir hele volumet kryptert og beskyttet mot uautorisert tilgang, selv om den fysiske lagringsenheten fjernes og kobles til en annen datamaskin.

For å beskytte data i bedriftsmiljøer bør IT-avdelingen definere og pålegge bruken av FileVault-konfigurasjonsregler via MDM. Organisasjoner har flere alternativer for administrering av krypterte volumer, inkludert bedriftsspesifikke gjenopprettingsnøkler, personlige gjenopprettingsnøkler (som eventuelt kan deponeres ved å lagres i selve MDM-løsningen), eller en kombinasjon av disse alternativene. Nøkkelrotering kan også angis som en regel i MDM.

Krypterte diskfiler

I macOS fungerer krypterte diskfiler som sikre beholdere der brukerne kan lagre eller overføre sensitive dokumenter og andre filer. Krypterte diskfiler opprettes med Diskverktøy, som du finner i /Programmer/Verktøy/. Diskfiler kan krypteres med enten 128-bits eller 256-bits AES-kryptering. Siden en aktivert diskfil

behandles som et lokalt volum koblet til en Mac, kan brukerne kopiere, flytte og åpne filer og mapper som er lagret på den. Som med FileVault krypteres og dekrypteres innholdet i diskfiler i sanntid. Med krypterte diskfiler kan brukere utveksle dokumenter, filer og mapper på en sikker måte ved å lagre en kryptert diskfil på et uttakbart medium, sende den som vedlegg til en e-postmelding eller lagre den på en ekstern tjener.

ISO 27001- og 27018-sertifisering

Apple har fått ISO 27001- og ISO 27018-sertifisering for ledelsessystemet for informasjonssikkerhet (ISMS) for infrastrukturen, utviklingen og operasjonene som støtter følgende produkter og tjenester: Apple School Manager, iCloud, iMessage, FaceTime, administrerte Apple ID-er og iTunes U, i samsvar med Statement of Applicability v 2.1, datert 11. juli 2017. Apples samsvar med ISO-standarden er sertifisert av British Standards Institution (BSI). For å se ISO 27001- og ISO 27018-sertifikatene kan du gå til BSI-nettsiden:

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Kryptografisk validering (FIPS 140-2)

Krypteringsmodulene i macOS har blitt godkjent med hensyn til samsvar med amerikanske Federal Information Processing Standards (FIPS) 140-2 Level 1 for hver nye oppgradering siden OS X 10.6. Ved større oppgraderinger sender Apple modulene til CMVP for ny godkjenning når operativsystemet for Mac slippes. Dette programmet sikrer integriteten til krypteringen i Apple-apper og tredjepartsapper som bruker krypteringstjenestene og godkjente algoritmer i macOS på riktig måte. Alle Apples sertifikater for samsvar med FIPS 140-2 kan finnes på CMVP-siden. CMVP viser oppdaterte godkjenningsstatuser for krypteringsmoduler i to separate lister, avhengig av nåværende status, på: csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Common Criteria-sertifisering (ISO 15408)

Apple har tidligere oppnådd macOS-sertifiseringer i henhold til Common Criteria Certification-programmet, og skal nå gjennomgå en ny evaluering av macOS High Sierra opp mot Operating System Protection Profile (PP_OSv4.1). Apple kommer til å fortsette å evaluere og søke om sertifiseringer knyttet til nye og oppdaterte versjoner av Collaborative Protective Profiles (cPP) som er tilgjengelig i dag. Apple har tatt en aktiv rolle i International Technical Community (ITC) med hensyn til å utvikle cPP-er med fokus på å evaluere essensiell sikkerhetsteknologi for mobilenheter.

Sikkerhetssertifiseringer, programmer og veiledning

Apple har samarbeidet med myndigheter over hele verden om å utvikle veiledninger med instruksjoner og anbefalinger for et sikrere miljø for enheter, kjent som «device hardening» for høyrisikomiljøer. Disse veiledningene gir definert og grundig gjennomgått informasjon om hvordan innebygde funksjoner bør konfigureres og brukes i macOS, for høyest mulig sikkerhet.

Hvis du vil se den nyeste informasjonen om sikkerhetssertifikater, valideringer og veiledninger knyttet til macOS, kan du lese Apples kundestøtteartikkel «Produktsikkerhetssertifiseringer, valideringer og veiledning for macOS» på support.apple.com/HT201159.

Appsikkerhet

macOS kommer med innebygd funksjonalitet for å sikre at bare pålitelige apper installeres, og for å beskytte mot skadelig programvare. For å sikre at legitime apper ikke kan tukles med, har macOS også et lagdelt system som holder apper atskilt ved kjøring og appsignering.

Gatekeeper

macOS har en funksjon som heter Gatekeeper som kontrollerer hvilke kilder apper kan installeres fra. Gatekeeper gjør det mulig for brukere og virksomheter å angi et påkrevet sikkerhetsnivå for installering av apper.

Når Gatekeeper-innstillingen er satt til det strengeste sikkerhetsnivået, kan brukerne kun installere signerte apper fra App Store. Standardinnstillingen lar brukere installere apper fra App Store og apper som har en unik utvikler-ID-signatur. Denne signaturen indikerer at appen har blitt signert av et sertifikat utstedt av Apple, og at den ikke har blitt modifisert siden. Gatekeeper kan også deaktiveres helt og holdent med en Terminal-kommando.

I tillegg bruker Gatekeeper i enkelte tilfeller banerandomisering, blant annet i tilfeller der apper lastes inn direkte fra en usignert diskfil eller fra stedet de ble lastet ned til og automatisk dearkivert fra. Banerandomisering gjør apper tilgjengelige fra en uspesifisert plassering i filsystemet med kun lesetilgang før innlasting. Hvis de lastes inn fra en slik plassering med kun lesetilgang, forhindrer det appene fra å kunne få tilgang til kode eller innhold via relative baner, men det forhindrer dem også fra å oppdatere seg på egen hånd. Hvis Finder brukes for å flytte en app til eksempelvis Programmer-mappen, brukes ikke lenger banerandomisering.

Den viktigste sikkerhetsfordelen ved standardbeskyttelsesmodellen er at den gir bred beskyttelse av hele økosystemet. Hvis en som lager skadelig programvare skulle få tilgang til å signere med en utvikler-ID og bruke denne til å spre skadelig programvare, kan Apple raskt komme på banen og trekke tilbake signeringssertifikatet. Dermed kan ikke den skadelige programvaren lenger spres. Slike beskyttelsesfunksjoner tar vekk grunnlaget for det økonomiske potensialet ved å implementere skadelig programvare på den enkelte Macen, og gir et bredt beskyttelsesnivå for alle brukerne.

Brukerne kan midlertidig overstyre disse innstillingene for å installere apper etter eget forgodtbefinnende. Organisasjoner kan bruke MDM-løsningen sin til å etablere og påkreve bruk av Gatekeeper-innstillinger, samt til å legge til sertifikater til macOS-klareringspolicyen for evaluering av kodesignering.

XProtect

macOS inkluderer innebygd teknologi for signaturbasert deteksjon av skadelig programvare. Apple holder utkikk etter nye utgaver og infeksjoner av skadelig programvare, og oppdaterer XProtect-signaturer automatisk – uavhengig av systemoppdateringer – for å bidra til å beskytte Mac-systemer mot å bli infisert av skadelig programvare. XProtect oppdager og blokkerer automatisk installering av kjent skadelig programvare.

Verktøy for å fjerne skadelig programvare

Hvis det likevel skulle hende at en Mac blir infisert av skadelig programvare, inneholder macOS også teknologi for å fjerne denne. I tillegg til å holde utkikk etter aktivitet fra skadelig programvare i økosystemet for å kunne inndra utvikler-ID-er ved behov, samt for å sende ut XProtect-oppdateringer,

sender Apple også ut oppdateringer til macOS for å fjerne skadelig programvare fra eventuelle berørte systemer som er konfigurert til å motta automatiske sikkerhetsoppdateringer. Når verktøyet for fjerning av skadelig programvare får oppdatert informasjon, fjernes den skadelige programvaren neste gang maskinen startes på nytt. Verktøyet for fjerning av skadelig programvare starter ikke Macen på nytt automatisk.

Automatisk sikkerhetsoppdatering

Apple sender automatisk ut oppdateringer til XProtect og verktøyet for fjerning av skadelig programvare. Som standard sjekker macOS daglig om det har kommet slike oppdateringer. Hvis du vil ha mer informasjon om automatiske sikkerhetsoppdateringer, kan du lese Apples kundestøtteartikkel «Mac App Store: Automatiske sikkerhetsoppdateringer» på support.apple.com/HT204536.

Beskyttelse ved kjøring

Systemfiler, ressurser og kjernen er skjermet fra brukerens appområde. Alle apper fra App Store kjøres i et testmiljø for å begrense tilgangen til data i andre apper. Hvis en app fra App Store trenger tilgang til data fra en annen app, kan dette kun gjøres ved å gå via API-ene og tjenestene i macOS.

Obligatorisk appkodesignering

Alle apper i App Store signeres av Apple for å sikre at de ikke har blitt modifisert eller tuklet med. Apple signerer alle apper som skal brukes på Apple-enheter. Mange apper som distribueres utenfor App Store, er signert av utviklere med et Apple-utstedt utvikler-ID-sertifikat (kombinert med en privat nøkkel) for å kunne kjøre med standardinnstillingene for Gateway.

Apper som ikke er distribuert via App Store, er vanligvis også signert med et Apple-utstedt utviklersertifikat. Dette gjør at man kan validere at appen er ekte, og ikke har blitt tuklet med. Apper som er utviklet internt, skal også signeres med en utvikler-ID utstedt av Apple, slik at integriteten kan bekreftes.

Obligatoriske tilgangskontroller (Mandatory Access Controls – MAC) krever kodesignering for å slå på rettigheter som beskyttes av systemet. For eksempel må apper som krever tilgang gjennom brannmuren, være kodesignert med den aktuelle MAC-rettigheten.

Autentisering og digital signering

For å muliggjøre enkel og sikker lagring av brukeres påloggingsinformasjon og digitale identiteter, har macOS Nøkkelring-funksjonen og andre verktøy for å støtte teknologier for autentisering og digital signering som smartkort og S/MIME.

Nøkkelringarkitektur

macOS har en oppbevaringsfunksjon kalt Nøkkelring. Den lagrer brukernavn og passord, inkludert digitale identiteter, krypteringsnøkler og sikre notater på en sikker og praktisk måte. Man får tilgang til den ved å åpne Nøkkelringtilgang-appen i /Programmer/Verktøy/. Ved å bruke nøkkelringen elimineres behovet for å skrive inn eller huske påloggingsinformasjonen for hver eneste ressurs. En innledende standardnøkkelring opprettes for hver Mac-bruker, men brukerne kan også opprette andre nøkkelringer for spesifikke formål.

I tillegg til brukernøkkelringer bruker macOS en rekke nøkkelringer på systemnivå som opprettholder autentiseringselementer som ikke er brukerspesifikke,

eksempelvis påloggingsdetaljer for nettverk og PKI-sertifikater (Public Key Infrastructure). En av disse, nøkkelringen Systemrøtter, kan ikke endres. Den lagrer internett-PKI-rotsertifikater for å tilrettelegge for oppgaver som bruk av nettbanktjenester og netthandel. På samme måte kan du rulle ut interne CA-sertifikater til administrerte Mac-datamaskiner for å bistå i godkjenning av interne nettsider og tjenester.

Rammeverk for sikker autentisering

Nøkkelringdata partisjoneres og beskyttes med tilgangskontrollister, slik at påloggingsinformasjon som lagres av tredjepartsapper, ikke er tilgjengelig for apper med ulik identitet, med mindre brukeren uttrykkelig godtar dem. Denne beskyttelsen danner mekanismen for å sikre autentiserings- og påloggingsinformasjonen på Apple-enheter på tvers av flere apper og tjenester i organisasjonen.

Touch ID

Mac-systemer med en Touch ID-sensor kan låses opp med et fingeravtrykk. Touch ID fjerner ikke behovet for et passord, som fortsatt kreves for å logge inn etter oppstart eller omstart av Macen, eller hvis man har logget ut av den. Når brukeren er pålogget, kan vedkommende bruke Touch ID til autentisering hver gang man blir bedt om å oppgi passord.

Brukerne kan også bruke Touch ID til å låse opp passordbeskyttede notater i Notater-appen, Passord-panelet i Safari-innstillingene samt mange valgpaneler i Systemvalg. Av sikkerhetsårsaker må brukerne skrive inn et passord i stedet for å bruke Touch ID for å kunne låse opp Sikkerhet og personvern-panelet i Systemvalg. Hvis FileVault er slått på, må brukere også skrive inn et passord for å administrere valgene for Brukere og grupper. Hvis flere brukere skal dele på den samme Macen, kan de bruke Touch ID for å bytte mellom kontoer.

Hvis du vil ha mer informasjon om Touch ID og sikkerhetsfunksjoner og -aspekter ved denne funksjonen, kan du lese Apples kundestøtteartikkel «Om avansert sikkerhetsteknologi med Touch ID» på support.apple.com/HT204587.

Automatisk opplåsing med Apple Watch

Brukere med Apple Watch kan bruke den til å låse opp Macen deres automatisk. Med Bluetooth Low Energy (BLE) og «peer-to-peer»-Wi-Fi kan Apple Watch brukes til sikker opplåsing av Mac hvis man er i nærheten av enheten. For å kunne gjøre dette kreves det at brukeren har en iCloud-konto med tofaktorautentisering konfigurert.

Hvis du vil ha mer informasjon om protokollen og om kontinuitets- og Handoff-funksjoner, kan du lese «iOS-sikkerhet» på https://www.apple.com/no/business/docs/iOS_Security_Guide.pdf.

Smartkort

macOS Sierra og nyere versjoner kommer med integrert støtte for PIV-kort (Personal Identity Verification). Disse kortene brukes i utstrakt grad i kommersielle og offentlige organisasjoner for tofaktorautentisering, digital signering og kryptering.

Smartkort inneholder en eller flere digitale identiteter som har et par med offentlige og private nøkler og et tilknyttet sertifikat. Ved å låse opp et smartkort med den tilhørende PIN-koden får man tilgang til de private nøklene som brukes til autentisering, kryptering og signering. Sertifikatet avgjør hva

en nøkkel kan brukes til, hvilke attributter som er knyttet til den, samt hvorvidt det er godkjent (signert) av en CA.

Smartkort kan brukes til tofaktorautentisering. De to faktorene som kreves for å låse opp et kort, er «noe du har» (et kort) og «noe du vet» (PIN-koden). macOS Sierra og nyere versjoner har integrert støtte for autentisering av påloggingsvinduet og klientsertifikater og via smartkort for nettsider i Safari. Systemet støtter også Kerberos-autentisering med bruk av nøkkelpar (PKINIT) for Single Sign On til Kerberos-støttede tjenester.

Hvis du vil ha mer informasjon om utrulling av smartkort, kan du lese «macOS – Håndbok for utrulling» på help.apple.com/deployment/macos.

Digital signering og kryptering

i Mail-appen kan brukerne sende meldinger som er kryptert og digitalt signert. Mail oppdager automatisk passende RFC 822-e-postadresseemner som skiller mellom store og små bokstaver, eller alternative emnenavn på sertifikater for digital signering og krypteringssertifikater på tilknyttede PIV-tokener i kompatible smartkort. Hvis en konfigurert e-postkonto samsvarer med e-postadressen på et digitalt signerings- eller krypteringssertifikat på et vedlagt PIV-token, viser Mail automatisk signeringsknappen i verktøylinjen på et nytt meldingsvindu.
Hvis Mail har mottakerens e-postkrypteringssertifikat, eller kan finne det i den globale adresselisten i Microsoft Exchange, vises et symbol med en opplåst hengelås i verktøylinjen for den nye meldingen. Et låst hengelåssymbol indikerer at meldingen sendes i kryptert form med mottakerens offentlige nøkkel.

Meldingsbasert S/MIME-kryptering

macOS har støtte for meldingsbasert S/MIME. Dette betyr at S/MIME-brukere kan velge å alltid signere og kryptere meldinger som standard, eller velge å signere og kryptere enkeltmeldinger.

Identiteter som brukes med S/MIME, kan leveres til Apple-enheter med en konfigurasjonsprofil, en MDM-løsning, Simple Certificate Enrollment Protocol (SCEP) eller Microsoft Active Directory-sertifikattjenester.

Nettverkssikkerhet

I tillegg til de innebygde sikkerhetsløsningene Apple bruker til å beskytte data som er lagret på Mac-datamaskiner, finnes det mange løsninger for nettverkssikkerhet som organisasjoner kan ta i bruk for å sikre informasjonen mens den overføres til eller fra Macen.

Mobilbrukere må ha tilgang til bedriftsnettverk fra hele verden, så det er viktig å sikre at de er godkjente, og at dataene er beskyttet under overføringen. macOS bruker – og gir utviklertilgang til – standard nettverksprotokoller for autentisert, autorisert og kryptert kommunikasjon. For å oppfylle disse sikkerhetskravene integrerer macOS velprøvde teknologier og de nyeste standardene for Wi-Fi-datanettverk.

TLS

macOS støtter Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2) og DTLS. Det støtter både AES-128 og AES-256, og foretrekker chiffreringspakker med «perfect forward secrecy». Safari, Kalender, Mail og andre internettapper tar disse mekanismene i bruk automatisk for å opprette en kryptert kommunikasjonskanal mellom enheten og nettverkstjenestene.

Avanserte API-er (som CFNetwork) gjør det enkelt for utviklere å integrere TLS i appene sine, mens API-er på lavere nivå (som SecureTransport) gir detaljert kontroll. CFNetwork tillater ikke bruk av SSLv3, og apper som bruker WebKit (som Safari), forbys å opprette en SSLv3-kobling.

Fra og med macOS High Sierra og iOS 11 tillates ikke lenger SHA-1-sertifikater for TSL-koblinger, med mindre de er godkjent av brukeren. Sertifikater med RSA-nøkler som er kortere enn 2048 bits, tillates heller ikke. Symmetriske RC4-chiffreringspakker er avviklet i macOS Sierra og iOS 10. Som standard har ikke TLS-klienter eller tjenere som har implementert SecureTransport API-er, aktivert RC4-chiffreringspakker, og de kan ikke kobles til når RC4 er den eneste tilgjengelige chiffreringspakken. Av sikkerhetsårsaker bør tjenester og apper som krever RC4, oppgraderes til å bruke moderne og sikrere chiffreringspakken.

App Transport Security

App Transport Security etablerer standardkrav til tilkoblinger, slik at apper følger anbefalt praksis for sikker tilkobling ved bruk av NSURLConnection-, CFURL- eller NSURLSession-API-er. Som standard begrenser App Transport Security chiffreringsutvalget til å kun omfatte pakker med Forward Secrecy, spesifikt ECDHE_ECDSA_AES og ECDHE_RSA_AES i GCM- eller CBC-modus. Apper kan deaktivere Forward Secrecy-kravet etter domene. I så fall legges RSA_AES til settet med tilgjengelige chifre.

Tjenere må ha støtte for TLS 1.2 og Forward Secrecy, og sertifikater må være gyldige og signert med SHA-256 eller bedre med minimum en 2048-bits RSA-nøkkel eller 256-bits elliptisk kurve-nøkkel.

Nettverkforbindelser som ikke oppfyller disse kravene, vil mislykkes med mindre appen overstyrer App Transport Security-funksjonen. Ugyldige sertifikater resulterer alltid i feil, og ingen forbindelse opprettes. App Transport Security brukes automatisk på apper som er kompilert for macOS 10.11 eller nyere.

VPN

Sikrede nettverkstjenester som tjenester for virtuelle private nettverk (VPN), krever som regel minimalt med konfigurering for å fungere med macOS. Mac-datamaskiner fungerer med VPN-tjenere som støtter følgende protokoller og autentiseringsmetoder:

- IKEv2/IPSec med autentisering med «delt hemmelighet», RSA-sertifikater, ECDSA-sertifikater, EAP-MSCHAPv2 eller EAP-TLS
- SSL VPN ved bruk av den aktuelle klientappen fra App Store
- Cisco IPSec med brukerautentisering via passord, RSA SecurID eller CRYPTOCard, og maskinautentisering med «delt hemmelighet» og sertifikater
- L2TP/IPSec med brukerautentisering via MS-CHAPV2-passord, RSA SecurID eller CRYPTOCard, og maskinautentisering med «delt hemmelighet»

I tillegg til VPN-løsninger fra tredjeparter støtter macOS følgende:

- **VPN etter behov** for nettverk som bruker sertifikatbasert autentisering. IT-retningslinjer spesifiserer hvilke domener som krever en VPN-forbindelse, ved å bruke en VPN-konfigurasjonsprofil.
- **VPN per app** for langt mer spesifikke VPN-tilkoblinger. MDM kan spesifisere en forbindelse for hver enkelt administrerte app og spesifikke domener i Safari. Dette gjør at sikre data alltid overføres til og fra bedriftsnettverket, men at brukerens personlige informasjon ikke overføres.

Wi-Fi

macOS har støtte for Wi-Fi-protokoller av bransjestandard, inkludert WPA2 Enterprise, for å gi autentisert tilgang til trådløse bedriftsnettverk. WPA2 Enterprise bruker 128-bits AES-kryptering, som gir brukerne den beste mulige forsikringen om at dataene deres fortsatt er beskyttet når de sender og mottar informasjon over et Wi-Fi-nettverk. Med støtte for 802.1X kan Mac-datamaskiner integreres i en rekke RADIUS-autentiseringsmiljøer. Metoder for 802.1X trådløs autentisering omfatter EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 og LEAP.

WPA/WPA2 Enterprise-autentisering kan også brukes på påloggingsvinduet for macOS, slik at brukeren logger på for å autentisere seg for nettverket.

Oppsettsassistenten for macOS har støtte for 802.1X-autentisering med påloggingsinformasjon i form av brukernavn og passord som bruker TTLS eller PEAP.

Brannmur

macOS kommer med en innebygd brannmur som beskytter Macen fra nettverkstilgang- og tjenestenektangrep. Det har støtte for følgende konfigurasjoner:

- blokker alle innkommende forbindelser, uavhengig av app
- tillat automatisk at innebygd programvare mottar innkommende forbindelser
- tillat automatisk at nedlastet og signert programvare mottar innkommende forbindelser
- legg til eller nekt tilgang basert på brukerspesifiserte apper
- forhindre at Macen responderer på ICMP-probing og henvendelser om portskanning

Single Sign On

macOS har støtte for autentisering overfor bedriftsnettverk med Kerberos. Apper kan bruke Kerberos til å godkjenne brukere for tjenester de er autorisert til å få tilgang til. Kerberos kan også brukes til en rekke nettverksaktiviteter, fra sikre Safari-økter og godkjenning av nettverksfilsystemer til apper fra tredjeparter. Sertifikatsbasert autentisering (PKINIT) støttes, selv om appene må ta i bruk en utvikler-API.

GSS-API SPNEGO-tokener og HTTP Negotiate-protokollen fungerer med Kerberos-baserte autentiseringsgatewayer og systemer for Windows-integrert godkjenning som støtter Kerberos-billetter. Støtten for Kerberos er basert på åpen kildekode-prosjektet Heimdal.

Følgende krypteringstyper støttes:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

For å konfigurere Kerberos må man skaffe billetter via Kerberos-billettvisningen, logge på et Windows Active Directory-domene eller bruke `kinit`-verktøyet på kommandolinjen.

AirDrop-sikkerhet

Mac-datamaskiner som har støtte for AirDrop, bruker BLE og Apple-utviklet peer-to-peer Wi-Fi-teknologi til å sende filer og informasjon til enheter

i nærheten, inkludert iOS-enheter med AirDrop-funksjonalitet som kjører iOS 7 eller nyere versjoner. Wi-Fi-radioen brukes for å kommunisere direkte mellom enheter uten å bruke noen form for internettforbindelse eller Wi-Fi-tilgangspunkt. Denne forbindelsen er kryptert med TLS.

Hvis du vil ha mer informasjon om AirDrop, AirDrop-sikkerhet og andre Apple-tjenester, kan du lese delen om nettverkssikkerhet i «iOS-sikkerhet» på https://www.apple.com/no/business/docs/iOS_Security_Guide.pdf.

Enhetskontroller

macOS har støtte for fleksible sikkerhetsinnstillinger og -konfigurasjoner som er enkle å håndheve og administrere. Dette gjør det mulig for organisasjoner å beskytte bedriftsinformasjon og sikre at de ansatte opptrer i tråd med bedriftens krav, selv om de bruker sine egne enheter – for eksempel som en del av et BYOD-program (Bring Your Own Device – bruk din egen enhet).

Organisasjoner kan bruke ressurser som passordbeskyttelse, konfigurasjonsprofiler og MDM-løsninger fra tredjeparter for å administrere enhetsflåter og sørge for at bedriftsdata beskyttes, selv der ansatte får tilgang til denne informasjonen på deres personlige Mac-datamaskiner.

Passordbeskyttelse

På Mac-datamaskiner med Touch ID er minimumslengden for passord åtte tegn. Lange og komplekse passord anbefales alltid, siden det er vanskeligere å gjette eller rette angrep mot slike.

Administratorer kan påkreve bruk av komplekse passord og andre sikkerhetsløsninger via MDM, eller ved å kreve at brukerne manuelt installerer konfigurasjonsprofiler. Et administratorpassord kreves for nyttelastinstallasjon av macOS-passordinnstillinger.

Hvis du vil ha mer informasjon om innstillingene som er tilgjengelige i MDM-løsningen, kan du lese help.apple.com/deployment/mdm/#/mdm4D6A472A.

Hvis du vil ha mer informasjon for utviklere knyttet til hver enkelt regel, kan du lese om Configuration Profile Reference på developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Påkrevet konfigurasjon

En konfigurasjonsprofil er en XML-fil som brukes av administratorer til å distribuere konfigurasjonsinformasjon til Mac-datamaskiner. Hvis brukeren sletter en konfigurasjonsprofil, fjernes også alle reglene som er definert av denne profilen. Administratorer kan pålegge tvungen bruk av regler ved å knytte innstillinger til Wi-Fi- og datatilgang. For eksempel kan en konfigurasjonsprofil som innebærer e-postkonfigurering, også spesifisere regler for enhetspassord. Brukeren får ikke tilgang til e-postkontoen med mindre passordet oppfyller kravene administratoren har satt.

macOS-konfigurasjonsprofiler inneholder en rekke innstillinger som kan spesifiseres, inkludert:

- passordregler
- begrensninger for tilgang til funksjoner på enheten (eksempelvis at kameraet er deaktivert)
- Wi-Fi- eller VPN-innstillinger

- tjenerinnstillinger for Mail eller Exchange
- tjenesteinnstillinger for LDAP-katalogsystemer
- brannmurinnstillinger
- påloggingsinformasjon og nøkler
- programvareoppdateringer

Du finner en oppdatert liste over profiler i konfigurasjonsprofil-delen på help.apple.com/deployment/mdm/#/mdm5370d089.

Konfigurasjonsprofiler kan signeres og krypteres for å validere opphavet deres, sikre integriteten og beskytte innholdet i dem. Konfigurasjonsprofiler kan også låses til en Mac for å fullstendig hindre muligheten for at de fjernes, eller for å kreve at passord oppgis før de fjernes. Konfigurasjonsprofiler som innebærer at en Mac registreres for en MDM-løsning, kan fjernes – men dette vil også fjerne administrert konfigureringsinformasjon, data og apper.

Brukere kan installere konfigurasjonsprofiler som er lastet ned fra Safari, sendt i en e-postmelding eller sendt trådløst via en MDM-løsning. Når en bruker konfigurerer en Mac i DEP eller Apple School Manager, laster datamaskinen ned og installerer automatisk en profil for MDM-registrering.

MDM

macOS har støtte for MDM, noe som gjør det mulig for virksomheter å konfigurere og administrere utrulling av Mac, iPhone, iPad og Apple TV på en sikker måte i hele organisasjonen. MDM-funksjonaliteten er bygget på grunnlag av eksisterende macOS-teknologier som konfigurasjonsprofiler, trådløs registrering og Apples pushvarslingstjeneste (APN). For eksempel brukes Apples pushvarslingstjeneste til å «vekke» enheten, slik at den kan kommunisere direkte med MDM-løsningen over en sikker forbindelse. Det blir ikke overført konfidensiell eller proprietær informasjon via pushvarslinger.

Ved å bruke MDM kan IT-avdelingen registrere Mac-datamaskiner i et bedriftsmiljø, trådløst konfigurere og oppdatere innstillinger, overvåke samsvar med virksomhetens regler og til og med slette eller låse Mac-datamaskiner eksternt.

Enhetsregistrering

Enhetsregistrering, en del av Apple School Manager-programmet og Apples utrullingsprogrammer, gir en rask og sømløs måte for utrulling av Mac-datamaskiner som organisasjoner har kjøpt direkte fra Apple eller via Apple-autoriserte forhandlere som deltar i disse programmene.

Organisasjoner kan registrere datamaskiner automatisk i MDM uten å ha fysisk tilgang til datamaskinene, eller klargjøre dem før brukerne får dem. Etter registreringen logger administratorene på programnettstedet og kobler programmet til MDM-løsningen. Datamaskinene de har kjøpt, kan deretter automatisk registreres i MDM-løsningen. Etter at Macen er registrert, blir MDM-spesifikke konfigurasjoner, restriksjoner og kontroller installert automatisk. All kommunikasjon mellom datamaskinene og Apple-tjenerne krypteres med HTTPS (SSL) under sending.

Konfigurasjonsprosessen for brukerne kan forenkles ytterligere ved å ta ut enkelte av trinnene i Oppsettsassistenten, slik at brukerne kan ta enhetene i bruk etter kort tid. Administratorene kan også styre hvorvidt brukerne kan fjerne MDM-profilen fra datamaskinen, og sikre at enhetsbegrensninger er på plass fra første stund. Så snart datamaskinen er pakket ut og aktivert, registreres den i organisasjonens MDM-løsning – slik at alle administrasjonsinnstillinger,

apper og bøker installeres på et blunk. Merk at enhetsregistreringsprogrammet ikke er tilgjengelig i alle land og områder.

Hvis du vil ha mer informasjon om bruk i bedrifter, kan du lese «Hjelp for Apples distribusjonsprogrammer» på help.apple.com/deployment/business. Hvis du vil ha mer informasjon om utdanning, kan du lese «Hjelp til Apple School Manager» på help.apple.com/schoolmanager.

Restriksjoner

Restriksjoner kan aktiveres – og i visse tilfeller deaktiveres – av administratorer for å hindre brukerne fra å få tilgang til bestemte apper, tjenester eller funksjoner på en enhet. Restriksjoner sendes ut til enhetene i en Restriksjoner-nyttelast i konfigurasjonsprofilen. Restriksjoner kan brukes på macOS-, iOS- og tvOS-enheter.

En oppdatert liste over tilgjengelige restriksjonsmuligheter for IT-administratorer finnes på: help.apple.com/deployment/mdm/#/mdm2pHf95672

Fjernsletting og fjernlåsing

Mac-datamaskiner kan fjernslettes av administratoren eller brukeren. Umiddelbar fjernsletting er bare tilgjengelig hvis Macen har aktivert FileVault. Når en kommando om fjernsletting utløses i MDM eller iCloud, sender datamaskinen en bekreftelse og gjennomfører slettingen. Hvis fjernlåsing er aktivert, krever MDM-løsningen at Macen beskyttes med en sekssifret kode, som stenger ute alle brukere frem til denne koden tastes inn.

Personvern

I Apple mener vi at personvern er en grunnleggende menneskerettighet. Derfor er alle Apple-produkter utformet for å bearbeide informasjon direkte på enheten når dette er mulig, begrense innsamlingen og bruken av opplysninger, gi innsyn i og kontroll over din informasjon og bygge på et robust sikkerhetsgrunnlag.

Apple har en rekke innebygde kontroller og innstillinger som lar macOS-brukere styre når og hvordan apper bruker informasjonen deres, samt hvilken informasjon som brukes. Hvis du vil vite mer, kan du gå til www.apple.com/no/privacy.