Beveiliging in macOS

Overzicht voor IT

macOS is ontworpen met een geïntegreerde benadering van hardware, software en voorzieningen die op alle fronten veilig is en die configuratie, implementatie en beheer vergemakkelijkt. macOS omvat de belangrijkste beveiligingstechnologie die een IT-professional nodig heeft voor optimale bescherming van bedrijfsgegevens en integratie in beveiligde bedrijfsnetwerken. Apple heeft met certificeringsinstanties samengewerkt om te waarborgen dat aan de nieuwste vereisten voor beveiligingscertificering wordt voldaan. In dit overzicht worden een aantal van de beveiligingsfeatures toegelicht.

De volgende onderwerpen komen aan bod:

- **Systeembeveiliging:** De geïntegreerde en veilige software die de basis vormt van macOS.
- **Versleuteling en gegevensbescherming:** De architectuur en structuur die ervoor zorgen dat gegevens ook veilig zijn wanneer het device zoekraakt of gestolen wordt.
- **App-beveiliging:** De systemen die de Mac beschermen tegen malware en zorgen dat apps veilig kunnen worden gebruikt zonder de integriteit van het platform in gevaar te brengen.
- **Identiteitscontrole en digitale ondertekening:** De voorzieningen in macOS voor het beheer van verificatiegegevens en ondersteuning van standaardtechnologieën zoals smartcards en S/MIME.
- **Netwerkbeveiliging:** Standaardnetwerkprotocollen die ervoor zorgen dat tijdens de overdracht van gegevens een identiteitscontrole wordt uitgevoerd en dat gegevens worden versleuteld.
- **Devicebeheer:** Methoden voor het beheren van Apple devices, het voorkomen van ongeoorloofd gebruik en het inschakelen van wissen op afstand als een device zoekraakt of gestolen wordt.

Voor meer informatie over de implementatie en het beheer van macOS raadpleegt u de macOS-implementatiehandleiding op help.apple.com/deployment/macos.

Voor meer informatie over de beveiligingsfeatures van Apple voorzieningen die niet in dit document worden besproken, raadpleegt u de handleiding ‘iOS-beveiliging’ op www.apple.com/nl/business/docs/iOS_Security_Guide.pdf.

Systeembeveiliging

De systeembeveiliging van macOS is zo ontworpen dat de software en hardware in alle kernonderdelen van elke Mac beveiligd zijn. Deze architectuur speelt in de beveiliging van macOS een centrale rol, maar staat het gebruiksgemak van het device nooit in de weg.

UNIX

Het kernel, die het hart vormt van macOS, is gebaseerd op de Berkeley Software Distribution (BSD) en de Mach-microkernel. BSD biedt bestandssysteem- en netwerkvoorzieningen, een gebruikers- en groepsidentificatieschema en allerlei andere fundamentele voorzieningen. BSD legt ook toegangsbeperkingen op voor bestanden en systeembronnen op basis van gebruikers- en groeps-ID's.

Mach biedt voorzieningen voor geheugen- en threadbeheer, hardware-abstractie en communicatie tussen processen. Mach-poorten vertegenwoordigen taken en andere bronnen, en Mach regelt de toegang hiertoe door te bepalen welke taken een bericht naar de poorten kunnen sturen. BSD-beveiligingsbeleid en Mach-toegangsrechten vormen de basis van de beveiliging in macOS, en zijn van essentieel belang voor de lokale beveiliging.

De veiligheid van het gehele besturingssysteem staat of valt met de beveiliging van de kernel. Codeondertekening beschermt de kernel en kernelextensies van derden, evenals andere systeembibliotheken en uitvoerbare bestanden die door Apple zijn ontwikkeld.

Toegangsrechtenmodel

Een belangrijk aspect van de beveiliging van Mac is het toekennen of weigeren van toegangsrechten. Een toegangsrecht is de mogelijkheid om een specifieke bewerking uit te voeren, bijvoorbeeld het verkrijgen van toegang tot gegevens of het uitvoeren van code. Toegangsrechten worden toegekend op het niveau van mappen, submappen, bestanden en apps, maar ook voor specifieke gegevens in bestanden, appfunctionaliteit en beheersfuncties. De toegangsrechten van apps en systeemonderdelen worden afgelezen uit de digitale handtekening.

In macOS worden de toegangsrechten op een groot aantal niveaus geregeld, waaronder het Mach- en BSD-gedeelte van de kernel. Om rechten te beheren voor apps die netwerkvoorzieningen gebruiken, maakt macOS gebruik van netwerkprotocollen.

Verplichte toegangscontrole

macOS gebruikt ook verplichte toegangscontrole in de vorm van beleid waarmee beveiligingsbeperkingen worden ingesteld. Het beleid wordt geconfigureerd door de ontwikkelaar en het is altijd actief. Deze benadering verschilt van toegangscontrole waarbij gebruikers beveiligingsbeleid kunnen deactiveren afhankelijk van hun voorkeuren. Verplichte toegangscontroles zijn niet zichtbaar voor gebruikers, maar zijn de onderliggende technologie die diverse belangrijke features mogelijk maakt. Bijvoorbeeld sandboxing, ouderlijk toezicht, beheerde voorkeuren, extensies en System Integrity Protection.

System Integrity Protection

OS X 10.11 en hoger bevat System Integrity Protection. Dit is beveiliging op systeemniveau die onderdelen op bepaalde belangrijke systeemlocaties alleen-lezen maakt en voorkomt dat deze onderdelen worden uitgevoerd of gewijzigd door middel van schadelijke code. System Integrity Protection is een computerspecifieke instelling die standaard is ingeschakeld bij een upgrade naar OS X 10.11. Als u deze uitschakelt, is geen enkele partitie op het fysieke opslagdevice nog beveiligd. macOS past dit beveiligingsbeleid toe op elk proces dat op het systeem wordt uitgevoerd, ongeacht of dit proces in een sandbox wordt uitgevoerd of met beheerdersbevoegdheden.

Voor meer informatie over deze alleen-lezen gedeelten van het bestandssysteem raadpleegt u het Apple Support-artikel 'Over System Integrity Protection op een Mac' op support.apple.com/HT204899.

Kernelextensies

macOS bevat een kernelextensiemechanisme om dynamisch code in de kernel te kunnen laden zonder opnieuw te hoeven compileren of koppelen. Omdat deze kernelextensies (KEXT's) modulair werken en dynamisch worden geladen, zijn ze een logische keuze voor relatief op zichzelf staande voorzieningen die geen toegang nodig hebben tot interne kernelinterfaces, zoals hardwaredevicedrivers of VPN-apps.

Om de beveiliging op de Mac te verbeteren, is toestemming van de gebruiker nodig om kernelextensies te laden die zijn geïnstalleerd met of na de installatie van macOS High Sierra. Dit wordt ook wel het laden van door de gebruiker goedgekeurde kernelextensies genoemd. Elke gebruiker, ook al heeft deze geen beheerdersbevoegdheden, kan een kernelextensie goedkeuren.

Voor kernelextensies is geen autorisatie vereist als ze:

- Op de Mac zijn geïnstalleerd vóór de upgrade naar macOS High Sierra.
- Eerder goedgekeurde extensies vervangen.
- Geladen mogen worden zonder toestemming van de gebruiker, door middel van het commando `spctl` dat beschikbaar is bij opstarten vanuit de macOS-herstelpartitie.
- Mogen worden geladen via een MDM-configuratie (Mobile Device Management). Vanaf macOS High Sierra 10.13.2 kunt u MDM gebruiken om aan te geven welke kernelextensies kunnen worden geladen zonder toestemming van de gebruiker. Deze optie vereist een Mac met macOS High Sierra 10.13.2 die is aangemeld bij MDM via het Device Enrollment Program (DEP) of via een door de gebruiker goedgekeurde MDM-aanmelding.

Voor meer informatie over kernelextensies raadpleegt u het Apple Support-artikel 'Voorbereidingen treffen voor wijzigingen in kernelextensies in macOS High Sierra' op support.apple.com/HT208019.

Firmwarewachtwoord

macOS ondersteunt het gebruik van een wachtwoord om onbedoelde wijzigingen van firmware-instellingen op een bepaald systeem te vermijden. Dit firmware-wachtwoord wordt gebruikt om de volgende zaken te voorkomen:

- Opstarten vanaf een niet-geautoriseerd systeemvolume
- Aanpassing van het opstartproces, zoals opstarten in de modus voor één gebruiker
- Ongeautoriseerde toegang tot macOS Recovery
- Direct toegang tot het geheugen (DMA) via interfaces zoals Thunderbolt
- Doelschijfmodus, waarvoor DMA vereist is

Opmerking: De Apple T2-chip in iMac Pro voorkomt dat gebruikers het firmwarewachtwoord kunnen herstellen, zelfs als ze fysiek toegang hebben tot de Mac. Op een Mac zonder T2-chip zijn extra voorzorgsmaatregelen nodig om te voorkomen dat gebruikers fysiek toegang krijgen tot het binnenste van de Mac.

Internetherstel

Mac-computers proberen automatisch op te starten vanuit macOS Recovery via het internet als ze niet kunnen opstarten vanuit het ingebouwde herstelsysteem. Als dit gebeurt, ziet u tijdens het opstarten een ronddraaiende wereldbol in plaats van het Apple logo. Met internetherstel kunnen gebruikers de nieuwste versie van macOS opnieuw installeren of de versie die bij aankoop op hun Mac stond.

macOS-updates worden verspreid via de App Store en uitgevoerd door het macOS-installatieprogramma, dat codehandtekeningen gebruikt om de integriteit en authenticiteit van het installatieprogramma en de bijbehorende pakketten te waarborgen voorafgaand aan installatie. Op dezelfde manier is de internetherstelvoorziening de geautoriseerde bron voor het besturingssysteem dat oorspronkelijk met een bepaalde Mac is geleverd.

Voor meer informatie over macOS Recovery raadpleegt u het Apple Support-artikel 'Over macOS Recovery' op support.apple.com/HT201314.

Versleuteling en beveiliging van gegevens

Apple File System

Apple File System (APFS) is een nieuw, modern bestandssysteem voor macOS, iOS, tvOS en watchOS. Het is geoptimaliseerd voor Flash/SSD-opslag, bevat features voor sterke versleuteling, copy-on-write metadata, space sharing, klonen voor bestanden en directory's, snapshots, fast directory sizing, atomic safe-save primitives en verbeterde bestandssysteemfuncties, en een uniek copy-on-write-design dat gebruikmaakt van I/O-coalescing om zowel maximale prestaties als betrouwbaarheid van gegevens te waarborgen.

APFS wijst op aanvraag schijfruimte toe. Als één APFS-container meerdere volumes heeft, wordt de vrije ruimte van de container gedeeld en kan deze naar behoefte aan een willekeurig afzonderlijk volume worden toegewezen. Elk volume gebruikt maar een deel van de hele container, dus de beschikbare ruimte is de totale grootte van de container, minus de gebruikte ruimte in alle volumes in de container.

Voor macOS High Sierra moet een geldige APFS-container ten minste drie volumes bevatten, waarvan de eerste twee verborgen zijn voor de gebruiker:

- Prebootvolume: Bevat gegevens die benodigd zijn voor het opstarten van elk systeemvolume in de container.
- Herstelvolume: Bevat de herstelschijf.
- Systeemvolume: Bevat macOS en de gebruikersmap.

FileVault

Elke Mac bevat de ingebouwde versleutelingsfunctie FileVault om alle aanwezige gegevens te beveiligen. FileVault gebruikt XTS-AES-128 gegevensversleuteling om op een Mac aanwezige gegevens te beveiligen. Deze versleuteling kan worden toegepast op hele volumes op interne en externe opslagdevices. Als een gebruiker tijdens de configuratie-assistent een Apple ID en wachtwoord invoert, verschijnt een suggestie om FileVault in te schakelen en de herstelsleutel in iCloud te bewaren.

Een gebruiker die FileVault inschakelt op een Mac, wordt gevraagd geldige inloggegevens op te geven voordat het opstarten wordt voortgezet en om toegang te krijgen tot speciale opstartmodi, zoals de doelschijfmodus. Zonder geldige inloggegevens of een herstelsleutel blijft het hele volume versleuteld en wordt het beschermd tegen ongeautoriseerde toegang, zelfs als het fysieke opslagdevice wordt verwijderd en op een andere computer wordt aangesloten.

Om gegevens te beveiligen in een onderneming, moet het IT-team FileVault-configuratiebeleid definiëren en toepassen via MDM. Organisaties hebben verschillende opties voor het beheren van versleutelde volumes, waaronder herstelsleutels voor de hele organisatie, persoonlijke herstelsleutels (die eventueel

met MDM kunnen worden bewaard voor escrow), of een combinatie van beide. In MDM kan ook worden ingesteld dat sleutels moeten worden geroteerd.

Versleutelde schijfkopieën

In macOS doen versleutelde schijfkopieën dienst als beveiligde containers waarin gebruikers vertrouwelijke documenten en andere bestanden kunnen bewaren of versturen. Versleutelde schijfkopieën worden gemaakt met Schijfhulpprogramma, in /Programma's/Hulpprogramma's. Schijfkopieën kunnen worden versleuteld met 128-bits of 256-bits AES-versleuteling. Omdat een geactiveerde schijfkopie wordt behandeld als een lokaal volume dat op een Mac is aangesloten, kunnen gebruikers bestanden, en mappen die hierop worden bewaard, kopiëren, verplaatsen en openen. Zoals bij FileVault wordt de inhoud van een schijfkopie in real time versleuteld en ontsleuteld. Bij versleutelde schijfkopieën kunnen gebruikers veilig documenten, bestanden en mappen uitwisselen door een versleutelde schijfkopie te bewaren op verwisselbare media, ze als e-mailbijlage te versturen of ze op een externe server te bewaren.

Certificering ISO 27001 en 27018

Apple is gecertificeerd volgens ISO 27001 en ISO 27018 voor het Information Security Management System (ISMS) voor de infrastructuur, ontwikkeling en activiteiten die de volgende producten en voorzieningen ondersteunen: Apple School Manager, iCloud, iMessage, FaceTime, beheerde Apple ID's en iTunes U, in overeenstemming met de Statement of Applicability versie 2.1, van 11 juli 2017. Certificering voor naleving van de ISO-norm is aan Apple verleend door de British Standards Institution (BSI). Voor de nalevingscertificaten voor ISO 27001 en ISO 27018 raadpleegt u de website van het BSI:

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

Cryptografische validatie (FIPS 140-2)

De cryptografische modules in macOS zijn herhaaldelijk gevalideerd voor naleving van U.S. Federal Information Processing Standards (FIPS) 140-2 Level 1 voor OS X 10.6 en hoger. Zoals bij elke grote release stuurt Apple de modules naar CMVP voor hernieuwde validatie zodra het Mac-besturingssysteem wordt uitgebracht. Dit programma valideert de integriteit van cryptografische bewerkingen voor apps van Apple en apps van andere aanbieders, die op correcte wijze gebruikmaken van de cryptografische voorzieningen en goedgekeurde algoritmen van macOS. Alle nalevingscertificaten van FIPS 140-2 voor Apple zijn te vinden op de aanbiederpagina van CMVP. CMVP vermeldt de validatiestatus van cryptografische modules in twee afzonderlijke lijsten afhankelijk van hun huidige status, op csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Common Criteria Certification (ISO 15408)

Apple heeft al eerder macOS-certificeringen verkregen binnen het Common Criteria Certification-programma en evalueert macOS High Sierra op basis van het Operating System Protection Profile (PP_OSv4.1). Apple blijft evalueren en certificering nastreven op basis van nieuwe en bijgewerkte versies van de Collaborative Protection Profiles (cPPs) die nu beschikbaar zijn. Apple heeft

geholpen bij het ontwikkelen van cPP's voor het evalueren van beveiligingsmethoden voor mobiele technologie.

Certificering, programma's en richtlijnen voor beveiliging

Apple werkt samen met overheden overal ter wereld om handleidingen te ontwikkelen met instructies en aanbevelingen voor het beheren van een veilige omgeving, ook wel 'device hardening' genoemd voor omgevingen met een hoog risico. Deze handleidingen bevatten uitgebreid gescreende informatie over de configuratie en het gebruik van ingebouwde features in macOS voor verbeterde beveiliging.

Raadpleeg voor de nieuwste informatie over beveiligingscertificeringen, validaties en richtlijnen voor macOS het Apple Support-artikel 'Beveiligingscertificering van producten, validaties en richtlijnen voor macOS' op support.apple.com/HT201159.

Beveiliging van apps

macOS bevat ingebouwde technologieën die ervoor zorgen dat alleen vertrouwde apps kunnen worden geïnstalleerd en die de nodige bescherming bieden tegen malware. Om te voorkomen dat er gerommeld wordt met legitieme apps, biedt macOS ook een laagsgewijze benadering van app-runtimebeveiliging en -ondertekening.

Gatekeeper

Om de bronnen te controleren van waaruit apps kunnen worden geïnstalleerd, bevat macOS de feature Gatekeeper. Met Gatekeeper kunnen gebruikers en organisaties een vereist beveiligingsniveau instellen voor het installeren van apps.

Met de strengste instellingen van Gatekeeper kunnen gebruikers alleen ondertekende apps uit de App Store installeren. Met de standaardinstellingen kunnen gebruikers apps installeren uit de App Store en apps die zijn ondertekend met een geldige ontwikkelaars-ID. Deze handtekening geeft aan dat de apps zijn ondertekend door een certificaat dat is uitgegeven door Apple, en dat de apps sindsdien niet zijn aangepast. Gatekeeper kan desgewenst ook volledig worden uitgeschakeld via een Terminal-commando.

Gatekeeper past daarnaast in sommige gevallen randomisering van paden toe, bijvoorbeeld wanneer apps rechtstreeks worden geopend vanaf een niet-ondertekende schijfkopie of vanaf de locatie waarnaar ze zijn gedownload en automatisch uitgepakt. Randomisering van paden maakt apps beschikbaar vanaf een niet nader opgegeven alleen-lezen locatie in het bestandssysteem voordat ze worden geopend. Zo wordt voorkomen dat apps met behulp van relatieve paden toegang kunnen krijgen tot code of materiaal, maar dit voorkomt ook dat apps automatisch worden bijgewerkt als ze vanaf deze alleen-lezen locatie worden geopend. Als de Finder wordt gebruikt om een app bijvoorbeeld naar de map Programma's te verplaatsen, wordt randomisering van het pad niet langer toegepast.

Het belangrijkste veiligheidsvoordeel van het standaardbeveiligingsmodel is dat het gehele ecosysteem wordt beschermd. Stel dat een uitgever van malware erin slaagt een ontwikkelaar-ID te stelen of anderszins te bemachtigen. En stel dat deze wordt gebruikt om malware te verspreiden. Dan kan Apple snel reageren door het handtekeningcertificaat in te trekken. Zo wordt verdere verspreiding van de malware voorkomen. Het is aan dergelijke maatregelen te danken dat de meeste malwarecampagnes nauwelijks vat hebben op de Mac en zijn gebruikers.

Gebruikers kunnen deze instellingen tijdelijk negeren om apps naar keuze te installeren. Organisaties kunnen hun MDM-oplossing gebruiken om Gatekeeper-instellingen vast te leggen en af te dwingen. Ze kunnen hiermee ook certificaten toevoegen aan het macOS-vertrouwensbeleid voor het evalueren van codeondertekening.

XProtect

macOS bevat ingebouwde technologie voor op handtekeningen gebaseerde detectie van malware. Apple controleert op nieuwe malwarebesmettingen en -families, en werkt de XProtect-handtekeningen automatisch bij (onafhankelijk van systeemupdates) om Mac-systemen tegen malware te beschermen. XProtect detecteert en blokkeert automatisch de installatie van als zodanig bekende malware.

Tool voor verwijderen van malware

Mocht er malware op een Mac terechtkomen, dan bevat macOS ook technologie om een besmetting op te lossen. Er wordt niet alleen gecontroleerd op malware-activiteit in het ecosysteem om ontwikkelaar-ID's (indien van toepassing) te kunnen intrekken en XProtect-updates uit te geven. Apple brengt ook macOS-updates uit om malware te verwijderen van getroffen systemen die zijn ingesteld op het ontvangen van automatische beveiligingsupdates. Zodra de tool voor het verwijderen van malware bijgewerkte informatie ontvangt, wordt malware verwijderd bij de volgende keer opstarten. De Mac wordt niet automatisch opnieuw opgestart.

Automatische beveiligingsupdates

Apple geeft de updates voor XProtect en de tool voor het verwijderen van malware automatisch uit. macOS controleert standaard dagelijks op deze updates. Voor meer informatie over automatische beveiligingsupdates raadpleegt u het Apple Support-artikel 'Mac App Store: automatische beveiligingsupdates' op support.apple.com/HT204536.

Runtimebeveiliging

Systeembestanden, bronnen en de kernel worden beschermd vanuit de appruimte van een gebruiker. Alle apps uit de App Store worden in een aparte sandbox geplaatst om te voorkomen dat ze toegang hebben tot gegevens die door andere apps worden bewaard. Als een app uit de App Store toegang nodig heeft tot gegevens uit een andere app, kan dit alleen door middel van de API's en voorzieningen van macOS.

Verplichte ondertekening van appcode

Alle apps uit de App Store worden ondertekend door Apple om te waarborgen dat er niet mee is geknoeid en dat ze niet zijn aangepast. Apple ondertekent alle apps die standaard bij Apple devices worden geleverd. Veel apps die buiten de App Store worden verspreid, worden ondertekend door de ontwikkelaar met behulp van een door Apple uitgegeven ontwikkelaars-ID-certificaat (in combinatie met een privésleutel) om te worden uitgevoerd met standaard-Gatekeeper-instellingen.

Apps van buiten de App Store worden normaliter ook ondertekend met een door Apple uitgegeven ontwikkelaarscertificaat. Zo kunt u verifiëren of de app authentiek is en dat er niet mee is geknoeid. Ook apps die intern worden ontwikkeld, moeten worden ondertekend met een door Apple uitgegeven Apple ID, zodat u de integriteit van deze apps kunt controleren.

Voor verplichte toegangscontrole is codeondertekening vereist om door het systeem beveiligde rechten in te schakelen. Van apps die bijvoorbeeld toegang nodig hebben door de firewall, moeten zijn ondertekend met de daarvoor benodigde rechten voor verplichte toegangscontrole.

Identiteitscontrole en digitale ondertekening

Voor het handig en veilig bewaren van inloggegevens en digitale identiteitsgegevens van gebruikers, bevat macOS Sleutelhanger en andere tools die technologie ondersteunen voor authenticatie en digitale ondertekening, zoals smartcards en S/MIME.

Sleutelhanger

In Sleutelhanger in macOS kunnen op een handige, veilige manier gebruikersnamen en wachtwoorden worden bewaard, waaronder digitale identiteitsgegevens, coderingssleutels en beveiligde notities. Sleutelhanger is toegankelijk via de app Sleutelhangertoegang in/Programma's/Hulpprogramma's. Als een sleutelhanger wordt gebruikt, is het niet meer nodig om voor elk onderdeel inloggegevens in te voeren (en te onthouden). Voor elke Mac-gebruiker wordt in eerste instantie één standaardsleutelhanger aangemaakt, maar gebruikers kunnen zelf ook extra sleutelhangers aanmaken voor specifieke doeleinden.

Naast sleutelhangers voor gebruikers heeft macOS een aantal sleutelhangers op systeemniveau waarmee niet-gebruikersspecifieke gegevens voor identiteitscontrole worden bijgehouden, bijvoorbeeld inloggegevens voor netwerken en identiteitsgegevens voor de infrastructuur voor publieke sleutels (PKI). Een van deze sleutelhangers, System Roots, kan niet worden gewijzigd en wordt gebruikt om root-CA-certificaten voor PKI op te slaan voor veelvoorkomende activiteiten op internet, zoals online bankieren en e-commerce. Op dezelfde manier kunt u intern aangemaakte CA-certificaten implementeren op beheerde Mac-computers voor de validatie van interne sites en voorzieningen.

Beveiligd framework voor identiteitscontrole

Sleutelhangers worden in partities verdeeld en beveiligd met toegangscontrolelijsten, zodat inloggegevens die worden bewaard door apps van andere aanbieders, alleen toegankelijk zijn voor apps met andere identiteiten als de gebruiker hier expliciet toestemming voor geeft. Dit beveiligingsmechanisme beschermt de inloggegevens voor identiteitscontroles op Apple devices voor uiteenlopende apps en voorzieningen binnen een bedrijf.

Touch ID

Mac-systemen met een Touch ID-sensor kunnen met een vingerafdruk worden ontgrendeld. Ondanks Touch ID is een wachtwoord nog steeds nodig, om in te loggen na (opnieuw) opstarten of na het uitloggen bij een Mac. Als gebruikers zijn aangemeld, kunnen ze zich gemakkelijk legitimeren met Touch ID wanneer om een wachtwoord wordt gevraagd.

Gebruikers kunnen Touch ID ook gebruiken voor het ontgrendelen van beveiligde notities in de Notities-app, het wachtwoordenvenster in de voorkeuren van Safari en diverse andere voorkeurenvensters in Systeemvoorkeuren. Voor extra veiligheid moeten gebruikers een wachtwoord invoeren om het paneel 'Beveiliging en privacy' in Systeemvoorkeuren te openen. Hiervoor kunnen ze hun Touch ID niet gebruiken. Als FileVault is ingeschakeld, moeten gebruikers ook een wachtwoord invoeren om het paneel 'Gebruikers en groepen' in Systeemvoorkeuren te openen. Als meerdere gebruikers op dezelfde Mac werken, kunnen ze met behulp van hun Touch ID van account wisselen.

Voor meer informatie over Touch ID en de bijbehorende beveiliging raadpleegt u het Apple Support-artikel 'Over de geavanceerde beveiligingstechnologie Touch ID' op support.apple.com/HT204587.

Ontgrendel je Mac met Apple Watch

Gebruikers kunnen met hun Apple Watch automatisch hun Mac ontgrendelen. Via Bluetooth Low Energy (BLE) en peer-to-peer wifi kan Apple Watch veilig een Mac ontgrendelen, nadat is vastgesteld dat de devices zich bij elkaar in de buurt bevinden. Hiervoor moet een iCloud-account met tweestapsverificatie zijn geconfigureerd.

Voor meer informatie over het protocol en de features Continuïteit en Handoff raadpleegt u de handleiding 'iOS-beveiliging' op www.apple.com/nl/business/docs/iOS_Security_Guide.pdf.

Smartcards

macOS Sierra en hoger ondersteunen kaarten voor persoonlijke identiteitsverificatie (PIV-kaarten). Deze kaarten worden op grote schaal gebruikt bij bedrijven en overheidsinstanties voor tweestapsverificatie, digitale ondertekening en versleuteling.

Smartcards omvatten een of meer digitale identiteiten met een openbare en privésleutel evenals een bijbehorend certificaat. Als gebruikers de smartcard ontgrendelen met de PIN-code, krijgen ze toegang tot de privésleutels die worden gebruikt voor identiteitscontrole, versleuteling en ondertekening. Het certificaat bepaalt waarvoor een sleutel kan worden gebruikt, welke kenmerken eraan zijn gekoppeld en of de sleutel wordt gevalideerd (ondertekend) door een certificaatautoriteit.

Smartcards kunnen worden gebruikt voor tweestapsverificatie. De twee zaken die nodig zijn om een kaart te ontgrendelen zijn 'iets wat u hebt' (de kaart) en 'iets wat u weet' (de PIN-code). macOS Sierra en hoger bieden standaard ondersteuning voor smartcards als legitimatiemiddel in het inlogvenster en voor op een clientcertificaat gebaseerde identiteitscontrole voor websites in Safari. macOS ondersteunt ook Kerberos-identiteitscontrole met sleutelparen (PKINIT) voor eenmalige aanmelding bij voorzieningen die Kerberos gebruiken.

Voor meer informatie over de implementatie van smartcards met macOS, raadpleegt u de implementatiehandleiding voor macOS op help.apple.com/deployment/macos.

Digitale ondertekening en versleuteling

In de Mail-app kunnen gebruikers berichten verzenden die digitaal worden ondertekend en versleuteld. Bij compatibele smartcards detecteert Mail automatisch de naam en alternatieve naam van eigenaars van e-mailadressen met hoofdlettergevoelige RFC 822-indeling in digitale ondertekenings- en versleutelingscertificaten van PIV-tokens. Als een geconfigureerde e-mailaccount overeenkomt met een e-mailadres in een certificaat voor digitale ondertekening of versleuteling in een bijgevoegde PIV-token, geeft Mail automatisch de ondertekenknop weer in de knoppenbalk van het venster voor een nieuw bericht. Als Mail het e-mailversleutelingscertificaat voor de ontvanger heeft of dit certificaat kan vinden in de Global Address List (GAL) van Microsoft Exchange, verschijnt een geopend slot in de knoppenbalk van het nieuwe bericht. Een gesloten slot geeft aan dat het bericht wordt versleuteld met de openbare sleutel van de ontvanger.

S/MIME per bericht

macOS ondersteunt S/MIME per bericht. Dit betekent dat S/MIME-gebruikers ervoor kunnen kiezen alle berichten altijd te ondertekenen en versleutelen, of dit per bericht in te stellen.

Identiteiten die worden gebruikt met S/MIME, kunnen worden bezorgd bij Apple devices met behulp van een configuratieprofiel, een MDM-oplossing, het Simple Certificate Enrollment Protocol (SCEP) of de Microsoft Active Directory Certificate Authority.

Netwerkbeveiliging

Naast de ingebouwde beveiligingsvoorzieningen voor gegevens die op Mac-computers worden bewaard, kunnen bedrijven ook allerlei maatregelen treffen om hun netwerk te beveiligen, zodat informatie ook veilig is als die onderweg is van en naar een Mac.

Mobiele gebruikers moeten overal ter wereld bij bedrijfsnetwerken kunnen, dus is het belangrijk om te zorgen dat ze over de nodige bevoegdheden beschikken en dat hun gegevens tijdens overdracht goed zijn beveiligd. macOS gebruikt – en biedt ontwikkelaars toegang
tot – standaardnetwerkprotocollen voor gevalideerde, geautoriseerde en versleutelde communicatie. Om deze veiligheidsdoelen te verwezenlijken, integreert macOS beproefde technologieën en de nieuwste standaarden voor wifi-netwerkverbindingen.

TLS

macOS ondersteunt Transport Layer Security (TLS 1.0, TLS 1.1 en TLS 1.2) en DTLS. macOS ondersteunt zowel AES-128 als AES-256, en geeft de voorkeur aan cipher suites met perfect forward secrecy. Safari, Agenda, Mail en andere internet-apps gebruiken automatisch dit protocol om een versleuteld communicatiekanaal te realiseren tussen het device en netwerkvoorzieningen.

Dankzij API's op hoog niveau (zoals CFNetwork) kunnen ontwikkelaars TLS opnemen in hun apps, terwijl API's op laag niveau (zoals SecureTransport) verfijnde controle mogelijk maken. CFNetwork staat geen SSLv3 toe, en apps die WebKit gebruiken (zoals Safari) mogen geen SSLv3-verbinding maken.

Vanaf macOS High Sierra en iOS 11 worden SHA-1-certificaten niet meer toegestaan voor TLS-verbindingen, tenzij deze worden vertrouwd door de gebruiker. Certificaten met RSA-sleutels die korter zijn dan 2048 bits, zijn ook niet toegestaan. De symmetrische RC4 cipher suite wordt niet meer gebruikt in macOS Sierra en iOS 10. Voor TLS-clients of -servers die zijn geïmplementeerd met SecureTransport-API's zijn RC4 cipher suites standaard niet geactiveerd. Ze kunnen geen verbinding maken als RC4 is de enige beschikbare cipher suite is. Voor optimale veiligheid moeten voorzieningen of apps die RC4 vereisen, worden bijgewerkt zodat ze nieuwere, veilige cipher suites gebruiken.

App Transport Security

App Transport Security levert standaardverbindingsvereisten zodat apps beproefde methoden volgen voor beveiligde verbindingen bij het gebruik van NSURLConnection-, CFURL- of NSURLSession-API's. App Transport Security beperkt standaard de cipherselectie tot suites die forward secrecy bieden, met name ECDHE_ECDSA_AES en ECDHE_RSA_AES in GCM- of CBC-modus. Apps kunnen de vereiste voor forward secrecy uitschakelen per domein. RSA_AES wordt dan toegevoegd aan de reeks beschikbare ciphers.

Servers moeten TLS 1.2 en forward secrecy ondersteunen. Certificaten moeten geldig en ondertekend zijn en SHA-256 of beter gebruiken, met minimaal een 2048-bits RSA-sleutel of 256-bits elliptic curve-sleutel.

Netwerkverbindingen die niet aan deze vereisten voldoen, slagen alleen als App Transport Security in de app wordt uitgeschakeld. Bij ongeldige certificaten treedt altijd een fout op en kan er geen verbinding worden gemaakt. App Transport Security wordt automatisch toegepast op apps die worden gecompileerd voor macOS 10.11 of hoger.

VPN

Veilige netwerkvoorzieningen zoals Virtual Private Networking (VPN) zijn gewoonlijk snel te configureren voor gebruik in combinatie met macOS. Mac-computers werken met VPN-servers die de volgende protocollen en methoden voor identiteitscontrole ondersteunen:

- IKEv2/IPSec met verificatie op basis van een gedeeld geheim, RSA-certificaten, ECDSA-certificaten, EAP-MSCHAPv2 of EAP-TLS
- SSL VPN met gebruik van de juiste client-app uit de App Store
- Cisco IPSec met identiteitscontrole van gebruikers via een wachtwoord, RSA SecurID of CRYPTOCard, en identiteitscontrole van devices via een gedeeld geheim en certificaten
- L2TP/IPSec met identiteitscontrole van gebruikers via een MS-CHAPV2-wachtwoord, RSA SecurID of CryptoCard, en met identiteitscontrole van devices via een gedeeld geheim

Naast VPN-oplossingen van derden ondersteunt macOS het volgende:

- **VPN op aanvraag** voor netwerken waarop identiteitscontrole op basis van certificaten plaatsvindt. IT-beleidsregels bepalen aan de hand van een VPN-configuratieprofiel welke domeinen een VPN-verbinding nodig hebben.
- **App-gebonden VPN** om gerichter VPN-verbindingen te maken. Via MDM kunnen verbindingsgegevens worden aangegeven voor elke beheerde app en specifieke domeinen in Safari. Hiermee wordt gewaarborgd dat beveiligde gegevens altijd via het bedrijfsnetwerk gaan, dit in tegenstelling tot persoonlijke gegevens van gebruikers.

Wifi

macOS ondersteunt standaard-wifi-protocollen, zoals WPA2 Enterprise, voor identiteitscontrole tijdens de aanmelding bij draadloze bedrijfsnetwerken. WPA2 Enterprise maakt gebruik van 128-bits AES-versleuteling en biedt gebruikers de absolute zekerheid dat hun gegevens beschermd blijven tijdens het gebruik van de wifiverbinding. Dankzij ondersteuning voor 802.1X-identiteitscontrole kunnen Mac-computers in uiteenlopende RADIUS-serveromgevingen worden geïntegreerd. Methoden voor draadloze identiteitscontrole via 802.1X zijn onder meer EAP-TLS,
EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 en LEAP.

WPA/WPA2 Enterprise-identiteitscontrole kan ook worden gebruikt in het inlogvenster van macOS, zodat de gebruiker inlogt voor identiteitscontrole bij het netwerk.

De configuratie-assistent van macOS ondersteunt 802.1X-identiteitscontrole met gebruikersnaam en wachtwoord met behulp van TTLS of PEAP.

Firewall

In macOS is een firewall ingebouwd om de Mac te beschermen tegen ongeoorloofde netwerktoegang en denial-of-service-aanvallen. De firewall kan als volgt worden geconfigureerd:

- Alle inkomende verbindingen blokkeren, ongeacht de app
- Automatisch inkomende verbindingen toestaan in ingebouwde software
- Automatisch inkomende verbindingen toestaan in gedownloade en ondertekende software
- Toegang toestaan of weigeren op basis van door de gebruiker opgegeven apps
- Voorkomen dat de Mac reageert op ICMP-aanvragen (probing en portscan)

Single Sign-On

macOS ondersteunt identiteitscontrole bij bedrijfsnetwerken met behulp van Kerberos. Apps kunnen Kerberos gebruiken om te controleren tot welke voorzieningen gebruikers toegang hebben. Kerberos kan ook worden gebruikt voor netwerkactiviteiten uiteenlopend van beveiligde Safari-sessies en identiteitscontrole voor het netwerkbestandssysteem, tot apps van derden. Identiteitscontrole op basis van certificaten (PKINIT) wordt ondersteund, hoewel de app dan een ontwikkelaars-API moet implementeren.

GSS-API SPNEGO-tokens en het HTTP Negotiate-protocol werken met op Kerberos gebaseerde gateways voor identiteitscontrole en geïntegreerde Windows-verificatiesystemen die Kerberos-tickets ondersteunen. Kerberos-ondersteuning is gebaseerd op het open-source Heimdal-project.

De volgende typen versleuteling worden ondersteund:

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

Om Kerberos te configureren haalt u tickets op met Ticket Viewer, logt u in bij een Windows Active Directory-domein of gebruikt u de commandoregeltool `kinit`.

Beveiliging van AirDrop

Mac-computers die AirDrop ondersteunen, gebruiken BLE en door Apple ontwikkelde peer-to-peer wifi-technologie om bestanden en informatie te versturen naar devices in de buurt, waaronder iOS-devices met AirDrop-functionaliteit en iOS 7 of hoger. Het wifisignaal wordt gebruikt voor rechtstreekse communicatie tussen devices zonder gebruik van de internetverbinding of een wifi-toegangspunt. Deze verbinding wordt versleuteld met TLS.

Voor meer informatie over AirDrop, AirDrop-beveiliging en overige voorzieningen van Apple raadpleegt u het gedeelte ‘Netwerkbeveiliging’ in de handleiding ‘iOS-beveiliging’ op www.apple.com/nl/business/docs/iOS_Security_Guide.pdf.

Devicebeheer

macOS ondersteunt flexibel beveiligingsbeleid en configuraties die gemakkelijk zijn af te dwingen en te beheren. Zodoende kunnen organisaties hun bedrijfsgegevens beschermen en er tegelijkertijd voor zorgen dat werknemers aan de vereisten van het bedrijf voldoen, ook als ze hun eigen persoonlijke computers gebruiken voor hun werk, bijvoorbeeld in het kader van een ‘Bring your own device’-programma (BYOD).

Organisaties kunnen gebruikmaken van wachtwoordbeveiliging, configuratieprofielen en MDM-oplossingen van andere aanbieders om grote aantallen devices te beheren en bedrijfsgegevens te beveiligen, ook wanneer medewerkers deze gegevens gebruiken op hun persoonlijke Mac.

Wachtwoordbeveiliging

Op Mac-computers met Touch ID moet het wachtwoord minimaal acht tekens lang zijn. Het is verstandig lange en complexe wachtwoorden te gebruiken, want die zijn moeilijker te achterhalen.

Beheerders kunnen het gebruik van complexe wachtwoorden en ander beleid afdwingen met behulp van MDM of door gebruikers handmatig configuratieprofielen te laten installeren. Er is een beheerderswachtwoord nodig voor het installeren van de payload met het macOS-toegangscodebeleid.

Voor meer informatie over de beleidsregels die beschikbaar zijn in MDM-instellingen, raadpleegt u help.apple.com/deployment/mdm/#/mdm4D6A472A.

Voor meer informatie over de verschillende beleidsregels vanuit het oogpunt van ontwikkelaars, raadpleegt u de naslaginformatie over configuratieprofielen (Engelstalig) op developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Opleggen van configuraties

Een configuratieprofiel is een XML-bestand waarmee een beheerder configuratie-informatie kan versturen naar Mac-computers. Als de gebruiker een configuratieprofiel verwijdert, worden ook alle bijbehorende instellingen verwijderd. Beheerders kunnen instellingen afdwingen door beleid te koppelen aan wifi- en gegevenstoegang. Een configuratieprofiel dat een e-mailconfiguratie bevat, kan bijvoorbeeld ook wachtwoordbeleid voor devices bevatten. Een gebruiker kan dan alleen bij zijn e-mail als het wachtwoord aan de vereisten van de beheerder voldoet.

Een macOS-configuratieprofiel bevat een aantal instellingen die kunnen worden vastgelegd, waaronder:

- Toegangscodebeleid
- Beperkingen voor devicefeatures (bijvoorbeeld het uitschakelen van de camera)
- Wifi- of VPN-instellingen
- Instellingen van mail- of Exchange-server
- Instellingen van LDAP-adreslijstservice
- Firewall-instellingen
- Inloggegevens en sleutels
- Software-updates

Voor een actueel overzicht van profielen raadpleegt u de lijst met payloads op help.apple.com/deployment/mdm/#/mdm5370d089.

Configuratieprofielen kunnen worden ondertekend en versleuteld om hun herkomst te controleren, hun integriteit te waarborgen en hun inhoud te beveiligen. Configuratieprofielen kunnen ook worden vergrendeld op een Mac om te voorkomen dat ze worden verwijderd, of ervoor te zorgen dat verwijderen alleen mogelijk is na het invoeren van een wachtwoord. Configuratieprofielen waarmee een Mac wordt aangemeld bij een MDM-oplossing, kunnen worden verwijderd. In dat geval worden echter ook beheerde configuratie-informatie, gegevens en apps verwijderd.

Gebruikers kunnen configuratieprofielen installeren die worden gedownload vanuit Safari, verstuurd in een e-mailbericht of draadloos verstuurd via een MDM-oplossing. Wanneer een gebruiker een Mac configureert in DEP of Apple

School Manager, wordt op de computer een profiel voor MDM-aanmelding gedownload dat automatisch wordt geïnstalleerd.

MDM

macOS ondersteunt MDM, zodat bedrijven de grootschalige implementatie van Mac, iPhone, iPad en Apple TV in hun organisatie op een veilige manier kunnen configureren en beheren. De MDM-voorzieningen zijn gebaseerd op bestaande macOS-technologie zoals configuratieprofielen, draadloze aanmelding en de Apple Push Notification-service (APNs). De APNs wordt bijvoorbeeld gebruikt om het device te activeren zodat het rechtstreeks kan communiceren met de MDM-oplossing via een beveiligde verbinding. Er wordt geen vertrouwelijke informatie via de APNs verstuurd.

Met behulp van MDM kunnen IT-teams Mac-computers aanmelden in een bedrijfsomgeving, draadloos instellingen configureren en bijwerken, naleving van de beleidsinstellingen controleren en beheerde Mac-computers ook op afstand vergrendelen of wissen.

Device-aanmelding

Device-aanmelding, dat deel uitmaakt van Apple School Manager en Apple Deployment Programs, is een snelle methode om Mac-computers te implementeren die een organisatie bij Apple zelf of bij deelnemende erkende Apple resellers heeft gekocht.

Organisaties kunnen devices automatisch aanmelden bij MDM zonder ze fysiek in handen te hoeven hebben, of de devices voorbereiden voordat ze in handen van de gebruikers komen. Na aanmelding logt de beheerder in bij de programmawebsite en koppelt hij het programma aan de MDM-oplossing. De aangeschafte computers kunnen vervolgens automatisch worden toegewezen met een MDM-oplossing. Zodra een Mac is aangemeld worden eventuele via MDM opgegeven configuraties, beperkingen of regelaars automatisch geïnstalleerd. Alle communicatie tussen computers en Apple servers wordt onderweg versleuteld met HTTPS (SSL).

Het configuratieproces voor gebruikers kan verder worden vereenvoudigd door stappen uit de configuratie-assistent te verwijderen. Gebruikers kunnen dan sneller aan de slag. De beheerder kan ook bepalen of de gebruiker het MDM-profiel van de computer mag verwijderen, en ervoor zorgen dat devicebeperkingen direct bij ingebruikname actief zijn. Zodra de computer is uitgepakt en geactiveerd, wordt deze aangemeld bij de MDM-oplossing van de organisatie. Alle beheerinstellingen, apps en boeken worden dan geïnstalleerd. Let op: device-aanmelding is niet overal beschikbaar.

Voor meer informatie met betrekking tot bedrijven raadpleegt u de Apple Deployment Programs Help (Engelstalig) op help.apple.com/deployment/business. Voor meer informatie met betrekking tot het onderwijs, raadpleegt u de Apple School Manager Help op help.apple.com/schoolmanager.

Beperkingen

Beperkingen kunnen door beheerders worden ingeschakeld – en in sommige gevallen uitgeschakeld – om te voorkomen dat gebruikers toegang hebben tot een specifieke app, voorziening of functie van het device. Beperkingen worden naar devices verstuurd in de payload voor beperkingen in een configuratieprofiel. Beperkingen kunnen worden toegepast op macOS-, iOS- en tvOS-devices.

Een actuele lijst met beschikbare beperkingen voor IT-beheerders vindt u hier: help.apple.com/deployment/mdm/#/mdm2pHf95672

Op afstand vergrendelen en wissen

Mac-computers kunnen op afstand worden gewist door een beheerder of gebruiker. Direct wissen op afstand is alleen beschikbaar als FileVault op de Mac is ingeschakeld. Wanneer een commando voor wissen op afstand wordt geactiveerd door MDM of iCloud, verschijnt een bevestiging voordat de gegevens worden gewist. Voor vergrendelen op afstand moet een toegangscode van zes cijfers voor de Mac worden ingesteld. De computer is dan pas toegankelijk als deze toegangscode wordt ingetoetst.

Privacy

Bij Apple zijn we van mening dat privacy een basisrecht is van iedereen. Daarom is elk Apple product zo ontworpen dat gegevens zoveel mogelijk op het device zelf worden verwerkt. Het verzamelen en gebruiken van gegevens wordt tot een minimum beperkt. We bieden transparantie en controle over uw informatie. En bij alles staat beveiliging centraal.

Apple heeft allerlei functies ingebouwd zodat macOS-gebruikers zelf kunnen bepalen hoe en wanneer apps hun informatie gebruiken, en welke informatie het precies betreft. Voor meer informatie raadpleegt u www.apple.com/nl/privacy.