EXPERTENTIPP

USER UND SECURITY IM EINKLANG

> Die Integration des Mac ist eine gute Gelegenheit, Security-Anforderungen auf den Prüfstand zu stellen. Die Richtlinien sollten direkt auch die Sicherheitsanforderungen an die Nutzung von iPhones, iPads oder Cloud-Diensten berücksichtigen – sofern diese noch nicht ganzheitlich umgesetzt sind. Ein Blick aufs Ganze ist also mehr als ratsam.

Andreas Harsdorff, Senior Consultant bei Computacenter

Damit Ihre User mit ihrem Mac vollumfänglich und produktiv arbeiten können, ist es notwendig, deren Identität zu verifizieren und gleichzeitig die Sicherheitsrichtlinien Ihres Unternehmens umzusetzen. Je nach Unternehmen und Branche sind diese völlig verschieden. Wir zeigen Ihnen, wie Sie alle sicherheitsrelevanten Funktionen von macOS optimal nutzen und dennoch im Einklang mit einer ansprechenden Usability Mehrwerte für Ihre Benutzer:innen generieren können.

SICHERHEITSANALYSE BEIM KUNDEN

Im ersten Schritt empfiehlt sich eine umfassende Betrachtung der Sicherheitsanforderungen an den künftigen Mac-Client. Häufig werden sie aus sehr alten Sicherheitsrichtlinien für Windows-Clients abgeleitet. Dabei wird übersehen, dass bereits bei der Einführung von mobilen Apple-Geräten wie iPhones und iPads, bei der Transformation diverser Dienste in die Cloud und für den Betrieb von Windows-11-Clients viele neue Ansätze implementiert wurden oder noch zu implementieren sind. Basierend auf Anforderungen, die aus den Themen Zero Trust Client oder mobiles Arbeiten entstanden sind.

Daher betrachten wir bei einem Mac-Pilotprojekt auch die weiteren Transformationsprojekte, die für die Umsetzung der Sicherheitsanforderungen relevant sein könnten und beziehen diese – soweit möglich – in den Piloten mit ein. Typische Themen sind Conditional Access, Data Lost Prevention (DLP), Netz- und Contentfilter für sicheres Surfen – alles Dinge, die typischerweise in Mobility-Projekten bereits eine Rolle gespielt haben.

Letztendlich muss die sicherheitsspezifische Konfiguration eines Macs im Piloten definiert werden. Um eine strukturierte Vorgehensweise zu gewährleisten, nutzen wir – in enger Abstimmung mit Ihren Sicherheitsverantwortlichen – das Cybersecurity Framework (CSF) der US-Bundesbehörde für Standards und Technologie (NIST) oder die CIS-Benchmarks des Center for Internet Security.

Im Rahmen eines Workshops gehen wir alle Punkte mit Ihnen durch und stellen bedarfsweise Ihr Sicherheitsbedürfnis und die von Benutzer:innen erwartete

Apple-typische Usability gegenüber. Das sind sicherheitsrelevante Informationen zu Apple-Technologien wie Touch-ID, AirDrop, Sidecar oder Handover. Wir diskutieren aber auch prozessuale Aspekte, beispielsweise zur Nutzung einer privaten oder gemanagten Apple-ID. Ziel ist es, Sie anschließend in der Lage zu versetzen, relevante Sicherheitsrisiken für den Mac-Betrieb ganzheitlich einzuschätzen und angemessene Lösungen für Ihre User zu definieren. Darüber hinaus ergibt sich für Sie ein konkretes Bild, in welchen Punkten sich die Mac-Plattform von anderen Plattformen unterscheidet.

Andreas Harsdorff, Senior Consultant bei Computacenter

Fragen Sie unseren Experten

Sie wollen es genauer wissen? Dann wenden Sie sich gerne an unseren Experten **andreas.harsdorff@computacenter.com**

TYPISCHE SICHERHEITSANFORDERUNGEN

Es gibt einige Sicherheitsanforderungen, die stets im Fokus stehen – ganz unabhängig von Unternehmen und Branche. Wir haben sie alle im Blick und stets die passende Antwort parat:

Compliance-Anforderungen erfüllen: Damit User auf alle benötigten Dienste zugreifen können, legen wir gemeinsam mit Ihnen genau fest, welche allgemeinen Voraussetzungen der Mac erfüllen muss. Im Rahmen des Software Managements für Applikationen und macOS lässt sich beispielsweise definieren, welche Voraussetzungen beim Patch-Stand gelten müssen, um den Client für bestimmte Dienste zuzulassen.

Kontrolle bei der Software-Installation: In puncto Software-Installation ist es beim Mac möglich, Betriebssystem-Richtlinien festzulegen. Sie lassen beispielsweise nur zu, dass Software von Apple-zertifizierten Entwickler:innen installiert und ausgeführt werden kann.

Zugriffsmöglichkeiten auf das System: Data-Loss-Prevention-Software (DLP) bietet umfassende Endpoint-Sicherheit. Sie ermöglicht es, sensible Daten zu schützen sowie alle Aktionen zu überwachen, die diese Informationen betreffen. Weiterhin lässt sich über das Management Framework festlegen, welche Systemeinstellungen und Konfigurationen User selbst durchführen bzw. nicht verändern können. Gemanagte App-Settings können z.B. die Nutzung privater Cloud-Dienste verhindern. Auch hier gilt es, Ihre User primär vor Fehlbedienungen zu schützen, aber nicht durch zu restriktive Reglementierung in ihrer Arbeit zu behindern. Oder schlimmer: Sie in „kreative" Eigenlösungen zu drängen, die ein Risiko für einen ungewollten Datenverlust darstellen können.

Admin-Rechte definieren: Die Admin-Rechte auf dem Mac lassen sich genau festlegen, sodass User bestimmte Aktivitäten durchführen können – oder auch nicht. Zudem ist es einfach möglich, bestimmten Nutzer:innen temporäre Admin-Rechte zuzuweisen, damit sie eine bestimmte Software nach Rücksprache mit den Sicherheitsverantwortlichen selbst installieren oder Einstellungen des Systems anpassen können. Hier ist es möglich, die Handlungen von einzelnen Anwender:innen mitzuloggen. Bei einem Sicherheitsvorfall könnte hierüber rückwirkend forensisch festgestellt werden, welche Aktionen damit in einem kausalen Zusammenhang standen.

Das Gewähren temporärer Adminrechte hat sich auch bei Computacenter im Mac-Betrieb durchgesetzt. User tragen das Risiko, dass sie durch ihre Operationen als Admin den Rechner so verändern, dass er nicht mehr als compliant bewertet wird und sie deshalb daran gehindert werden, auf tätigkeitsrelevante Daten zuzugreifen. Für die Benutzer:innen ist ein solcher Vorfall transparent und sie können den „alten Zustand" wiederherstellen – oder das Managementsystem stellt ihn automatisch wieder her.nierten Weg anzubieten, den sie sich intuitiv selber erschließen können.

Sicherer Datenaustausch: Der Austausch von Dateien zwischen macOS- bzw. iOS-Geräten geht via AirDrop ganz einfach. Diese Funktion lässt sich jedoch auch komplett ausschalten. Einige Unternehmen ziehen das in Erwägung, um für eine höhere Sicherheit zu sorgen. Hier stellt sich jedoch die Frage: Ist es wirklich sicherer, solche Funktion auszuschalten? Treibt man User damit nicht dahin, Daten – wenn erforderlich – beispielsweise über einen privaten Webmail-Client zu übertragen? Die deutlich bessere Option ist es, Anwender:innen stets einen definierten Weg anzubieten, den sie sich intuitiv selber erschließen können.

BALANCE ZWISCHEN SICHERHEIT UND USER EXPERIENCE

Die Gewährleistung von Sicherheit und gleichzeitigem Mac-Feeling stellt eine wichtige Aufgabe für Unternehmen dar, um den Nutzer:innen ein reibungsloses und produktives Arbeiten mit ihren Mac-Geräten zu ermöglichen. Eine umfassende Sicherheitsanalyse, bei der sowohl kundenspezifische als auch technische Aspekte berücksichtigt werden, ist der erste Schritt, um die Sicherheitsrichtlinien des Unternehmens erfolgreich umzusetzen. Indem Sie in Ihrem Unternehmen Sicherheit und User Experience in Einklang bringen, schöpfen Sie das volle Potenzial Ihrer Mac-Geräte aus und gewährleisten den Schutz Ihrer sensiblen Daten.

DER MAC – EINE SICHERE KISTE

Hard- und Software für den Mac basiert auf fortschrittlichen Technologien, die reibungslos zusammenarbeiten – damit Applikationen sicherer laufen und die Daten geschützt sind.

- Automatische Einrichtung von macOS-Benachrichtigung, wenn Updates verfügbar sind oder automatische Ausführung von Updates, wenn der Mac nicht verwendet wird
- Macs mit Apple Silicon Chip mit integrierter Secure Enclave bieten einen hohen Schutz des Anmeldepasswortes, verschlüsseln Daten automatisch und ermöglichen eine Verschlüsselung auf Dateiebene.
- Integration von Endpoint-Security-Software nach Branchenstandard, um Malware zu blocken und zu entfernen.
- App Review ermöglicht es, Apps aus dem App Store und aus dem Internet einfach zu installieren, ohne sich Gedanken über die Sicherheit machen zu müssen.
- Zugriffsbestätigungen sind erforderlich, damit Apps auf Dokumente auf dem Mac zugreifen dürfen. Gleiches gilt für den Zugriff einer App auf Kamera oder Mikrofon.
- FileVault 2 verschlüsselt die komplette Festplatte auf dem Mac und schützt Daten mit XTSAES-128Bit-Verschlüsselung.
- Integrierte Technologie für Datenschutz in Safari sorgt dafür, dass Daten online geschützt bleiben.
- Safari nutzt den iCloud-Schlüsselbund, um Passwörter sicher auf allen Geräten zu speichern.
- „Wo ist?"-App hilft Nutzer:innen, einen verlorenen Mac zu finden – auch wenn er offline oder im Ruhezustand ist.