jamf

WHITEPAPER

Cyber Security: ein Leitfaden

Unternehmens- und Benutzerdaten unterliegen ständig der Gefahr von Hackerangriffen. Dieser Leitfaden von Jamf, dem Experten für die Verwaltung von Apple Geräten, zeigt Ihnen, wie Sie Ihre Organisation vor den häufigsten Hackerangriffen schützen.

Weitere Informationen über die Sicherheitsfunktionen von Jamf Pro sowie Sicherheitsempfehlungen finden Sie unter: **https://www.jamf.com/de/sicherheit**

Weshalb ist Cybersicherheit so wichtig?

Die Sicherheit von Unternehmensdaten und -geräten bekommt angesichts der wachsenden Anzahl und dem zunehmenden Einfluss von Sicherheitsrisiken immer mehr Aufmerksamkeit. Wir glauben, dass ein Unternehmen in puncto Cybersicherheit immer nur so gut gerüstet sein kann, wie es die vom Unternehmen genutzte Software zulässt. Sicherheitslücken können den Datenschutz, vertrauliche Unternehmensdaten, die Benutzererfahrung und vieles mehr gefährden. Hackerangriffe jeglicher Art sorgen für eine Unterbrechung des normalen Geschäftsbetriebs, die solange andauert, bis die Sicherheitslücke geschlossen ist. Zur Behebung von Sicherheitsrisiken müssen wertvolle Zeit und Ressourcen eingesetzt werden, obwohl solche Probleme schon im Vorfeld hätten verhindert werden können. Daher sollte jede IT-Abteilung den folgenden Punkten Priorität einräumen: Verschlüsselung der Geräte, die sich im Besitz des Unternehmens bzw. der Benutzer befinden, die darauf gespeicherten Daten, Einhaltung der Compliance der Geräte und Daten sowie die generelle Absicherung von Geräten und Daten.

Weshalb sollte mein Unternehmen aktiv Maßnahmen zum Schutz der Cybersicherheit ergreifen?

Die überwiegende Mehrheit aller Hackerangriffe ist mit einem versuchten Einbruch vergleichbar. Hacker schauen, ob sich eine geschlossene Tür einfach öffnen lässt. Die Einrichtung eines Sicherheitsplans mindert dieses Risiko. Durch die Befolgung der Empfehlungen aus dem Leitfaden ergeben sich folgende Vorteile:

- Ihre Kunden können sicher sein, dass sich Ihr Unternehmen für die Absicherung der technischen Infrastruktur und der Daten Ihrer Kunden gegen Hackerangriffe einsetzt.
- Sie können Neukunden gewinnen, denen die Cybersicherheit ein ernstes Anliegen ist.
- Sie können Aufträge staatlicher Stellen erhalten, für die eine Zertifizierungen im Bereich Cybersicherheit Voraussetzung sind.

Welche Angriffe können wir verhindern?

In Ihrem Sicherheitsplan sollten die gängigsten Bedrohungen aus dem Internet berücksichtigt werden, insbesondere Angriffe, bei denen allgemein verfügbare Tools eingesetzt werden und wenig Know-how erforderlich ist. Im Zentrum Ihrer Bemühungen sollten folgende Aspekte stehen:

- Hackerangriffe: Ausnutzung bekannter Sicherheitslücken von Internet-Geräten mithilfe allgemein verfügbarer Tools und Techniken
- Phishing: Versuche, Benutzer per E-Mail oder auf andere Weise zur Installation oder Ausführung einer Schadanwendung zu verleiten
- Erraten von Passwörtern: manuelle oder automatische Versuche, mithilfe gehackter Passwörter über das Internet in ein System einzudringen

Wie kann Jamf Unterstützung leisten?

Ganz gleich, wie ausgeprägt Ihre Sicherheitsbemühungen gemäß Best Practice Leitlinien sind, Jamf kann Sie immer unterstützen. Jamf Pro und Jamf Connect verfügen über integrierte Funktionen, mit denen praktisch alle Best Practice Leitlinien umgesetzt werden können.

Wenn die Sicherheit von Apple Geräten für Sie Neuland ist und Sie sich über die Grundlagen informieren möchten, empfehlen wir Ihnen unser E-Book **Einführung in die Sicherheit von Apple Geräten**.

Best Practice # 1: Firewalls

Stellen Sie sicher, dass über das Internet nur sichere und notwendige Netzwerkdienste zugänglich sind.

Die folgenden Schritte sollten regelmäßig durchgeführt werden:

- Passwörter sollten regelmäßig geändert werden. Es sollten nur schwer zu erratende, komplexe Passwörter verwendet werden.
- Der Zugriff auf die administrative Schnittstelle aus dem Internet muss verhindert werden, falls diese nicht durch einen der folgenden Kontrollmechanismen geschützt ist:
  - Zwei Faktor Authentifizierung, beispielsweise durch einmalige Tokens
  - IP-Whitelist, die den Zugriff nur einer kleinen Auswahl vertrauenswürdiger Adressen gewährt
- Nicht authentifizierte eintreffende Verbindungen werden standardmäßig gesperrt.
- Firewall Regeln für eintreffende Verbindungen sind von einem dazu befugten Mitarbeiter freizugeben und zu dokumentieren.
- Großzügige Firewall Regeln müssen sofort entfernt bzw. deaktiviert werden.
- Für Geräte, die in nicht vertrauenswürdigen Netzwerken wie etwa öffentlichen WLAN-Hotspots eingesetzt werden, muss eine hostbasierte Firewall verwendet werden.

Best Practices für Firewalls mit Jamf umsetzen

Wir begleiten Sie auf diesem Weg! Jamf Pro bietet Einstellungen, die diese Best Practices in der Sicherheits- und Datenschutz-Payload eines Jamf Pro Konfigurationsprofils realisieren, welches auf alle verwalteten Macs gepusht wird:

- Firewall aktivieren
- Alle eintreffenden Verbindungen wie beispielsweise Dateifreigabe, Bildschirmfreigabe, Messages Bonjour und Sharing von Musikdateien per iTunes sperren
- Eintreffende Verbindungen über das Dropdown-Menü für Verbindungseinstellungen bei bestimmten Apps kontrollieren. Dabei wird vor der Freigabe der App der Name der App, die Bundle-ID und die Verbindungseinstellung angefordert.
- Tarnmodus aktivieren: Zugriffsversuche auf den Computer aus dem Netzwerk durch ICMP-Testanwendungen wie z. B. Ping ignorieren
- Verwaltete Geräte so konfigurieren, dass automatisch eine Verbindung zu einem VPN hergestellt wird, wenn bestimmte Bedingungen gegeben sind. Dies sorgt für einen sichereren Netzwerkzugang.

Darüber hinaus vereinfacht Jamf Connect Nutzern eines Cloud Identity Service die Bereitstellung von Apple Produkten im Rahmen eines entsprechenden Workflows, der auch eine mehrstufige Authentifizierung umfasst.

Weiterführende technische Informationen zur Anwendungsfirewall und deren Konfiguration mit Jamf Pro finden Sie in den folgenden Informationsquellen für Entwickler:

Developer Configuration Profile Reference von Apple, Abschnitt „Firewall Payload“

Apple KB - OS X: Informationen zur Programm-Firewall

Jamf Pro Administrator’s Guide, Abschnitt „Computer Configuration Profiles“

jamf | CONNECT

Weiterführende Informationen finden Sie hier auf Jamf Connect:

https://www.jamf.com/de/ressourcen/produktdokumentation/jamf-connect-umdenken-bei-der-provisionierung-und-identitatsverwaltung/

Best Practice # 2: Sichere Konfiguration

Stellen Sie sicher, dass über das Internet nur sichere und notwendige Netzwerkdienste zugänglich sind.

Best Practices für Macs und Netzwerkgeräte

Die folgenden Schritte sollten in Unternehmen regelmäßig durchgeführt werden:

- Unnötige Benutzeraccounts entfernen und deaktivieren
- Standardpasswörter bzw. leicht zu erratende Passwörter ändern
- Unnötige Software entfernen bzw. deaktivieren
- Automatisch ausgeführte Funktionen deaktivieren, welche die Ausführung von Dateien ohne Benutzerautorisierung gestatten
- Zugriff auf vertrauliche Daten aus dem Internet authentifizieren lassen

Best Practices für Macs und Netzwerke mit Jamf umsetzen

Jamf Pro kann Administratoren bei der Umsetzung dieser Best Practices mithilfe von Konfigurationsprofilen, Richtlinien und Skripten unterstützen, mit denen Funktionen deaktiviert bzw. Probleme gemeldet oder schnell behoben werden können. Beispiele:

- Um einen Gast-Account permanent zu deaktivieren, kann der Jamf Administrator allen verwalteten Geräten ein Konfigurationsprofil mit dem Anmeldefenster als Payload bereitstellen.
- Administratoren können mithilfe von intelligenten Gruppen und mit einem Skript-Payload bestimmte Benutzergruppen sperren. Jamf Nation, die größte Online-Community von Apple Administratoren und Jamf Benutzern, enthält eine Fülle von Informationen, Beispielskripten und Tipps von anderen Benutzern zur Fehlerbehebung.
- Automatisierte Berichte liefern Administratoren bei Bedarf Informationen über lokale Benutzeraccounts; Einstellungen für die benutzerinitiierte Registrierung können unter „Globales Management“ oder nachträglich über die Management Account Payload festgelegt werden.
- Administratoren können Bluetooth deaktivieren und bestimmte Apps einschränken bzw. sperren.
- Bei der Konfiguration von Registrierungseinstellungen kann der Jamf Administrator mithilfe der Option für die benutzerinitiierte Registrierung zufallsgenerierte Passwörter aktivieren oder die Verwendung komplexer Passwörter vorschreiben.

Weitere Informationen zur Verwaltung von Account-Passwörtern mit Jamf Pro finden Sie in den folgenden technischen Informationsquellen:

Jamf Pro Administrator’s Guide, Abschnitt „Administering the Management Account“

Jamf Pro Administrator’s Guide, Abschnitt „Administering Local Accounts“

Jamf Pro Administrator’s Guide, Abschnitt „User-Initiated Enrolment Settings“

Best Practices für die passwortgestützte Authentifizierung

Diese Best Practice schützt gegen das automatisierte Ermitteln von Passwörtern, indem mindestens eine der folgenden Methoden eingesetzt wird:

- Sperrung des Accounts nach zu vielen Fehlversuchen
- Beschränkung der Anzahl der Anmeldeversuche innerhalb eines bestimmten Zeitraums
- Vorgaben für Länge und Komplexität des Passworts
- Verwendung einer Passwortrichtlinie, die den Benutzern die Nutzung sicherer, geschützter Passwörter klar verständlich erläutert

Best Practices für die passwortgestützte Authentifizierung mit Jamf umsetzen

Jamf Pro bietet die Möglichkeit, all diese Einstellungen in einem Konfigurationsprofil vorzunehmen. Jamf Pro Administratoren können auch Blacklists mit gängigen, leicht zu erratenden Passwörter erstellen. Mit Jamf Connect und Jamf Pro können die Benutzer die Vorteile der Single Sign-on Authentifizierung und der mehrstufigen Authentifizierung nutzen, was für noch besseren Passwortschutz sorgt.

Auch lokale Accounts mit NoMAD und mobile Accounts mit Active Directory werden unterstützt: Jamf Connect funktioniert problemlos mit NoMAD. Dies ermöglicht eine noch sicherere Nutzung.

Informationen über das Zusammenspiel dieser Komponenten finden Sie in dieser übersichtlichen Infografik: **https://www.jamf.com/resources/infographics/understanding-macos-catalina-and-jamf-connect/**

Best Practice # 3: Kontrolle des Benutzerzugangs

Unternehmen sollten sicherstellen, dass Benutzeraccounts nur autorisierten Personen zugewiesen werden und dass Anwendungen, Computer und Netzwerke nur für Benutzer zugänglich sind, die diese Ressourcen tatsächlich benötigen.

Infolgedessen sollten Unternehmen auf folgende Punkte achten:

- Festgelegtes Verfahren zur Erstellung und Freigabe von Benutzeraccounts verwenden
- Benutzer vor Gewährung des Zugangs zu Anwendungen bzw. Geräten authentifizieren
- Benutzeraccounts entfernen bzw. deaktivieren, wenn diese nicht mehr benötigt werden
- Administrator-Accounts nur zum Durchführen von administrativen Aufgaben nutzen
- Spezielle Zugangsberechtigungen entfernen bzw. deaktivieren, wenn diese nicht mehr benötigt werden

Best Practices für die Zugangskontrolle mit Jamf umsetzen

Für die Umsetzung dieser Punkte können die in Jamf für die Systemeinstellungen verfügbaren Einschränkungen genutzt werden, die mithilfe eines Konfigurationsprofils, mit einer Payload für Einschränkungen oder ganz einfach durch das Löschen von nicht mehr benötigten Administrator-Zugängen realisiert werden. Die korrekt konfigurierte Option **Self Service** gewährleistet, dass Benutzer keinen Zugang zu Bereichen bzw. Apps haben, die sie für Ihre Arbeit nicht benötigen.

Zum Entfernen von Benutzern und Accounts implementieren die Administratoren eine einfache Richtlinie, mit der die Zugriffsberechtigungen, Accounts bzw. Benutzer entfernt werden.

Best Practice # 4: Schutz gegen Malware

Unternehmen sollten die Ausführung bekannter Malware und nicht vertrauenswürdiger Software sperren, um zu verhindern, dass gefährlicher Code Schäden verursacht oder auf vertrauliche Daten zugreifen kann.

Best Practices zum Schutz gegen Malware

- Virenschutz und sonstige Sicherheitssoftware muss stets auf dem aktuellsten Stand gehalten werden, und zwar entweder automatisch oder nach einem festgelegten Workflow mindestens einmal täglich.
- Die Software muss so konfiguriert werden, dass sie Dateien und Webseiten beim Zugriff automatisch prüft.
- Die Software muss Verbindungen zu betrügerischen Websites im Internet verhindern.
- Auf den Geräten sind nur freigegebene Anwendungen zugelassen.
- Sämtlicher Programmcode unbekannter Herkunft muss in einer „Sandbox“ ausgeführt werden, die den Zugriff auf andere Ressourcen ohne ausdrückliche Zustimmung des Benutzers verhindert

Best Practices gegen Malware mit Jamf umsetzen

Jamf verfügt über integrierte Sicherheitsfunktionen. Bei der Bereitstellung von Software über eine Richtlinie und dank automatischer Updates der gesamten Software können Sie sich darauf verlassen, dass der Virenschutz und die gesamte sonstige Sicherheitssoftware immer auf dem neuesten Stand sind. Wenn die in Ihrem Unternehmen eingesetzte Virenschutzsoftware Dateien beim Zugriff nicht automatisch prüft, können Sie dies mit einem Skript oder einer Richtlinie von Jamf veranlassen. Selbstverständlich sind darüber hinaus sämtliche Macs mit dem integrierten System **Xprotect** von Apple ausgestattet.

Außerdem können Administratoren mit den Konfigurationsprofilen von Jamf Pro Sicherheits- und Datenschutz-Payloads über Gatekeeper-Einstellungen festlegen, Zertifikatstransparenz-Payloads bereitstellen, Apps auf eine bestimmte Whitelist beschränken und vieles mehr.

Zusätzlich zur integrierten Sandbox von Apple, die verhindert, dass Apps wichtige Funktionen teilen, verfügen auch die Server von Jamf Cloud über eine Sandbox, die zusätzliche Sicherheit bietet. Doch damit nicht genug: Administratoren können zusätzliche Sicherheitsfunktionen zum Schutz vor Malware mithilfe eines Konfigurationsprofils für die Steuerung der persönlichen Datenschutzrichtlinie einsetzen.

Best Practice # 5: Patch-Verwaltung

Diese Best Practice gewährleistet, dass Geräte und Software nicht für bekannte Sicherheitsprobleme anfällig sind, für die Korrekturen verfügbar sind.

Für Software gilt:

- Sie muss stets auf dem aktuellen Stand gehalten werden.
- Sie muss lizenziert und supportberechtigt sein.
- Sie muss von den Geräten entfernt werden, wenn für sie kein Support mehr geleistet wird.
- Sie sollte innerhalb von 14 Tagen nach Veröffentlichung eines Updates aktualisiert werden.

Best Practices für die Patch-Verwaltung mit Jamf umsetzen

Administratoren können mit der Patch-Verwaltungsfunktion von Jamf Pro Software auf verwalteten Geräten erfassen und aktualisieren: Dank der Patch-Verwaltungsfunktion wird die Software auf verwalteten Geräten automatisch aktualisiert. Zu diesem Zweck lädt der Administrator ein entsprechendes Paket hoch, verknüpft es mit einer Patch-Version und erstellt eine Patch-Richtlinie.

Der Patch-Server von Jamf kann Softwaretitel bereitstellen. Die Kunden können wahlweise auch eine externe Patch-Quelle einbinden, die von ihnen selbst oder von einem anderen Anbieter verwaltet wird. In den Softwaretitelinformationen sind auch die unterstützten Betriebssystemversionen enthalten.

Software kann auf einfache Weise deinstalliert werden, und zwar entweder mithilfe einer Richtlinie, die für die Deinstallation konfiguriert ist, oder indem das Gerät aus dem Geltungsbereich des Datensatzes für den Mac App Store entfernt wird.

Fazit

Mit Jamf ist es sehr einfach, Best Practices für die Cybersicherheit umzusetzen und einzuhalten. Kontaktieren Sie uns noch heute und erfahren Sie, wie auch Ihr Unternehmen sich gegen Cyberangriffe schützen kann.

jamf

www.jamf.com/de

Um diese Sicherheitsfunktionen zu testen, können Sie eine **kostenlose Testversion** anfordern.