BEST PRACTICES:

ZTNA

Zero-Trust-Netzwerkzugriff

Diese Best-Practice-Grundsätze von ZTNA sollten immer im Vordergrund stehen:

- → Gewährung des Zugangs nach dem Prinzip der geringsten Privilegien.
- → Überprüfen Sie die Identität mit MFA und Cloud IdPs.
- → Legen Sie Compliance-Anforderungen für die Verwaltung und Sicherung von Benutzer*innen, Geräten und mehr fest.
- → Niemals vertrauenswürdig, immer verifizierbar für eine kontinuierliche Überprüfung auch nach dem ersten Zugriff.

Wenn Sie gerade erst mit modernen Identitäts- und Zugangslösungen beginnen, lesen Sie weiter, um zu erfahren, wie Sie die Weichen für Ihre moderne Identitäts- und Zugangsstrategie stellen können.

jamf

Sie gehen in Ihre Bank, um eine Abhebung vorzunehmen. Ihre Identität wird anhand Ihrer Kontonummer und Ihres Personalausweises überprüft; wenn Ihr Name auf dem Konto steht, erhalten Sie Zugang zu diesem Konto, und nur zu diesem Konto. Stellen Sie sich vor, Sie geben Ihren Ausweis ab, und der Kassierer führt Sie direkt in den Tresorraum, wo Sie den gesamten Inhalt mitnehmen können. Klingt verrückt, oder? Warum also sollten Sie das mit Ihrem Netzwerk-Zugang tun?

Ein VPN (virtuelles privates Netzwerk) gibt Benutzer*innen Zugang zu Ihrem gesamten Netzwerk, unabhängig davon, ob sie einen ganzheitlichen Zugang benötigen oder nicht; dies stellt ein Risiko für Ihre Daten dar. **Zero Trust Network Access (ZTNA) verschließt den Tresor Ihrer Unternehmensdaten, indem es nur den Zugriff auf die von den Mitarbeiter*innen benötigten Ressourcen mit den geringsten Rechten ermöglicht und die Identität von Benutzer*innen und Geräten für jede App streng überprüft.** Außerdem werden die Bandbreitenanforderungen an Ihr Netzwerk reduziert und die Privatsphäre der Benutzer*innen durch Split-Tunneling gewahrt. Mit anderen Worten: VPN muss weg.

Wie funktioniert also ZTNA? Im Grunde genommen geht es darum, etwas zu wissen:

1. **Identität:** Wer sind Sie, sind Sie derjenige, der Sie vorgeben zu sein, und haben Sie eine Genehmigung?
2. **Sicherheit:** Ist Ihr Gerät sicher?
3. **Kontext:** Beantragen Sie nur Zugang zu den Ressourcen, die Sie benötigen?

Die Einführung einer erfolgreichen ZTNA-Technologie muss diese Fragen beantworten. Bei der ZTNA müssen sowohl der Nutzer/die Nutzerin als auch sein Gerät ihre Identität nachweisen. Das Gerät muss ein bekanntes und autorisiertes Gerät sein. Dies kann erreicht werden, indem das an einen bestimmten Benutzer/eine bestimmte Benutzerin gebundene Gerät in Ihrer Geräteverwaltungs-Lösung registriert wird. Der Benutzer/die Benutzerin muss auch korrekte Anmeldedaten und Antworten für die Multi-Faktor-Authentifizierung ihres Cloud Identity Providers angeben.

Trotz der Identitätsüberprüfung ist es wichtig sicherzustellen, dass die Geräte sicher sind, um weitere Risiken beim Versuch, auf Unternehmensressourcen zuzugreifen, zu minimieren. Das bedeutet, dass die Geräte Ihren Sicherheitsrichtlinien entsprechen und mit den neuesten Patches für Betriebssysteme und Schwachstellen ausgestattet sein sollten.

Nach Überprüfung der Identität und Sicherheit erhalten die Benutzer*innen Zugang zu den von ihnen benötigten Apps. In der ZTNA-Architektur können die Benutzer*innen nur das sehen, wozu sie eine Zugangsberechtigung haben. Um dies zu erreichen, werden jedem Benutzer/jeder Benutzerin nur vorab genehmigte Apps zur Verfügung gestellt. Auf diese Weise wissen Sie, dass Benutzer*innen, die auf diese Apps zugreifen wollen, bereits über eine Genehmigung verfügen sollten.

Jamf übernimmt all das für Sie: Geräteverwaltung, App-Bereitstellung, Integration mit Cloud Identity Anbietern, Software-Updates, Endpunktschutz und vieles mehr. Weitere Informationen über die nahtlose Bereitstellung von ZTNA finden Sie in unserem E-Book Zero Trust-Netzwerkzugriff für Einsteiger.

Möchten Sie Ihre Daten mit ZTNA sichern? Weitere Informationen darüber, wie Sie dies und mehr mit Jamf 's Trusted Access erreichen können.

jamf

www.jamf.com/de/

© 2002-2023 Jamf, LLC. Alle Rechte vorbehalten.