LEITFADEN FÜR KÄUFER:

SO WÄHLEN SIE DIE RICHTIGE MFA-LÖSUNG

Evaluierung und erste Schritte mit modernen MFA-Lösungen

Ping Identity.

NEUE FUNKTIONEN

Universelle Authentifizierungslösungen sind ein Relikt der Vergangenheit und auch die Zeiten, als Hard Token als Standard für eine starke Authentifizierung galten, sind vorbei. Zwar sind gestohlene Anmeldedaten immer noch das stärkste Argument für die Einführung einer Multifaktor-Authentifizierungslösung (MFA), doch was die Implementierungs- und Authentifizierungsmethoden, Endpunkt-Visibilität, unterstützten Anwendungen und Verwaltungsfunktionen angeht, hat sich inzwischen vieles getan.

Mit den zunehmenden Einsatzmöglichkeiten von MFA werden Innovationen in diesem kritischen Sicherheitsbereich noch weiter vorangetrieben. Die moderne MFA geht über den herkömmlichen Ansatz hinaus – der auf „etwas, was man weiß, etwas, was man hat, und etwas, was man ist" basiert – und bietet auch biometrische, standortbasierte und andere kontextbezogene Faktoren. Auf diese Weise können Sie für jeden Benutzer und zu jedem Zeitpunkt die geeignete Authentifizierungsmethode und das passende Level auswählen.

NEUE ERWARTUNGEN

Ihre Anwendungen befinden sich zunehmend außerhalb der Firewall und Ihre Sicherheitsanforderungen – darunter Zugriffsmöglichkeiten für Kunden und Partner – werden immer komplexer. Um diesen Anforderungen gerecht zu werden und Ihr Unternehmen wirksam zu schützen, reicht eine Ein- oder Zweifaktor-Authentifizierung nicht mehr aus.

Mit modernen MFA-Lösungen können Sie Ihre Sicherheitsmaßnahmen entsprechend dem jeweiligen Kontext heraufstufen und das kostspielige Risiko gestohlener Anmeldedaten senken – und gleichzeitig eine reibungslose Benutzererfahrung bieten. Wenn Sie MFA für Partner und Kunden implementieren, gibt es Dutzende neuer Anforderungen und Aspekte zu berücksichtigen. Gestalten Sie den Authentifizierungsprozess zu unpraktisch, kompliziert oder unsicher, kann es passieren, dass Sie Ihre Anwender ganz verlieren. Es gibt also vieles zu bedenken und es ist nicht immer einfach, die beste Option für Ihr Unternehmen zu finden. Mit diesem Leitfaden unterstützen wir Sie dabei, die richtigen Entscheidungen für Ihre Organisation und Ihre Benutzer zu treffen.

NEUE ZIELE

SCHNELLERE DIGITALE TRANSFORMATION

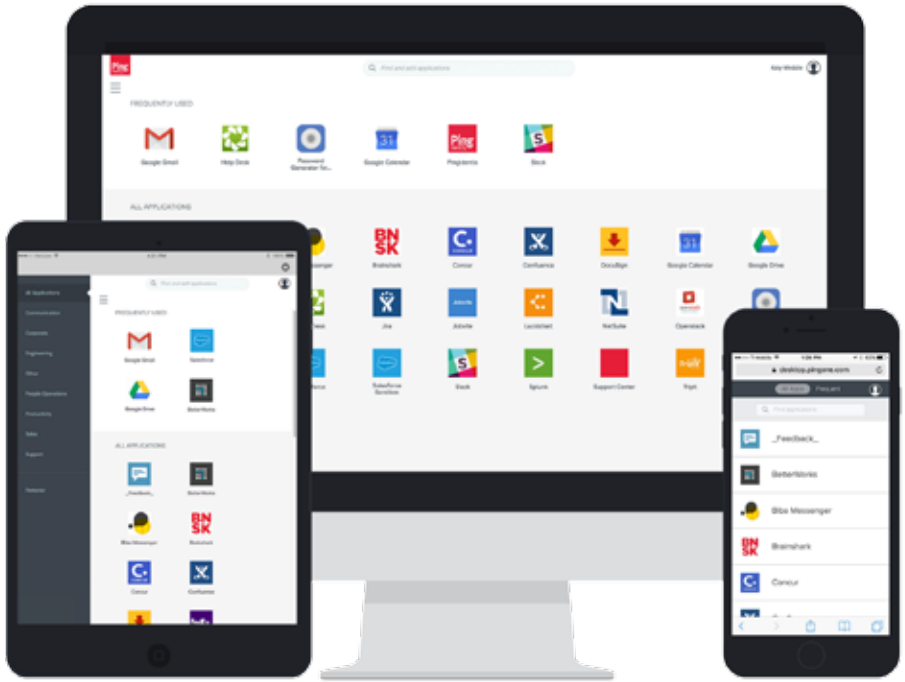
Eine vor kurzem durchgeführte Befragung von 200 IT-Entscheidern kommt zum Schluss, dass die Nutzung mobiler Anwendungen durch Mitarbeiter die häufigste Digital-Transformation-Initiative ist, die umfassend und aktiv umgesetzt wird. Mit der richtigen MFA-Lösung profitieren Ihre Anwender von einer nahtlosen, reibungslosen Benutzererfahrung und bekommen den erwarteten mobilen Zugriff auf all ihre Anwendungen – egal ob lokal oder in der Cloud gehostet. Wenn Benutzer jederzeit und überall Zugriff auf die nötigen Informationen und Analysen haben, können Unternehmen intelligenter agieren, Mehrwert schaffen und sich Wettbewerbsvorteile sichern.

GERINGERES RISIKO VON SICHERHEITS-LÜCKEN

Gestohlene Anmeldedaten und Brute-Force-Angriffe sind nach wie vor das stärkste Argument für MFA. Betrachtet man die enormen Kosten einer typischen Sicherheitslücke – von den Umsatzverlusten und Imageschäden ganz zu schweigen –, hat eine Risikominimierung enorme geschäftliche Vorteile. Da Organisationen auch immer mehr persönliche Daten von Kunden und Partnern verwalten, sind die Anmeldedaten von Mitarbeitern nicht mehr länger das einzige Ziel von Cyberkriminellen.

NIEDRIGERE KOSTEN

Unternehmen, die auf moderne Lösungen umsteigen, weil sie MFA als nötig erachten oder an Richtlinien gebunden sind, profitieren von deutlich niedrigeren Kosten als mit den veralteten, Hardware-basierten Token-Lösungen. Darüber hinaus ermöglichen es einige MFA-Lösungen, je nach Risiko einer bestimmten Aktivität die Anforderungen kontextbezogen hoch- oder herabzustufen. Das gibt Ihnen die Flexibilität, strenge Kontrollen nur bei entsprechendem Risiko einzusetzen, so dass Sie die Kosten für die Weiterleitung von Einmalpasswörtern per SMS, Anruf oder Push-Methoden reduzieren können. Und schließlich wird die Investition in eine MFA-Lösung normalerweise mit einer deutlichen Kostenreduzierung in Form eines geringeren Helpdesk-Aufwands und mehr Endbenutzer-Produktivität kompensiert.



SO WÄHLEN SIE DEN RICHTIGEN ANBIETER UND DIE PASSENDE LÖSUNG

Auf der Suche nach geeigneten Anbietern können Sie sich bei Branchenverbänden, in Fachzeitschriften und bei Kollegen informieren. Auch unabhängige Experten wie die führenden Analysten Gartner, Forrester und KuppingerCole berichten regelmäßig über MFA-Trends, -Technologien und -Lösungsanbieter.

Anschließend sollten Sie jeden dieser Anbieter persönlich kontaktieren und prüfen, ob sie Ihre Anforderungen erfüllen. Dazu können Sie z. B. Präsentationen, Demonstrationen und andere Supportmaterialien wie Whitepaper, E-Books, Datenblätter etc. anfordern. Das können Sie so formell (oder informell) handhaben, wie es in Ihrer Organisation üblich ist. Wichtig ist auf jeden Fall, dass Sie Ihre Ziele und Anforderungen klar und deutlich mitteilen.

Neue Funktionen, Erwartungen und Ziele legen die Messlatte für MFA-Anbieter ständig höher. Die unten aufgeführten Anforderungen bzw. die damit verbundenen Funktionen erheben keinen Anspruch auf Vollständigkeit, bieten aber einen guten Ausgangspunkt, um die besten Anbieter in die engere Auswahl zu nehmen.

ENDBENUTZER-ANFORDERUNGEN

EVALUIERUNGSKRITERIEN	BEDEUTUNG
Unterstützt der Anbieter die Registrierung mehrerer Geräte und Authentifizierungsmethoden pro Benutzer?	Stehen mehrere Authentifizierungsmethoden zur Verfügung, können sich die Anwender authentifizieren, auch wenn sie ihr primäres Gerät nicht zur Hand haben oder sich unter normalen Umständen nicht authentifizieren können.
Unterstützt der Anbieter Authentifizierungsmethoden wie OOB-Push-Benachrichtigungen, Fingerabdruck und Einmalpasswörter mit Soft-Token?	Stehen mehrere Authentifizierungsmethoden zur Verfügung, können Unternehmen aus unterschiedlichen Authentifizierungsmethoden auswählen, um das geeignete Sicherheitslevel zu erreichen.
Stellt der Anbieter neben Mobile-Push noch andere Authentifizierungsmethoden zur Verfügung?	Einmalpasswörter, die per Desktop-Anwendung, SMS, E-Mail oder Sprachnachricht übermittelt werden, sind ideal für Benutzer, die kein Smartphone haben oder am Arbeitsplatz keine Mobilgeräte nutzen können.
Unterstützt der Anbieter anpassbare Regeln, die auf den geografischen Standort und die IP-Adresse zurückgreifen?	Passive Benutzerdaten wie geografischer Standort, Uhrzeit, IP-Adresse und Geräte-ID verbessern die Sicherheit und die Benutzererfahrung.
Stellt der Anbieter eine große Bandbreite an Endbenutzer- Selfservice-Funktionen bereit?	Selfservice-Funktionen, die dem Benutzer die Möglichkeit geben, neue Geräte zu registrieren und zwischen Authentifizierungsarten zu wählen, senken den administrativen Aufwand für das IT-Team und beschleunigen die Benutzerakzeptanz.
Stellt der Anbieter mehrere Sprach- und Ländereinstellungen bereit?	Internationale Unternehmen, die für ihre Benutzer Anwendungen und Daten global schützen möchten, müssen eine lokalisierte Benutzererfahrung bereitstellen, um MFA erfolgreich einzuführen.
Unterstützt der Anbieter Android und iOS?	Die Unterstützung mehrerer Mobilplattformen ist wichtig für die BYOD-Initiativen, die sich in Unternehmen immer mehr durchsetzen.

Ping Identity.

IT-ANFORDERUNGEN

EVALUIERUNGSKRITERIEN	BEDEUTUNG
Unterstützt der Anbieter die Integration von Windows RDP, Linux/Unix SSH etc. und kundenspezifische APIs?	MFA für Remote- und berechtigte Benutzer schützt die wichtigsten Ressourcen des Unternehmens – egal wer oder wo der Benutzer ist.
Stellt der Anbieter Out-of-the-Box-Integrationen für mehrere Serverplattformen und Web Access Management-Systeme bereit?	Für die Entwicklung und Wartung dieser Integrationen braucht es häufig mehrere IT-Administratoren und Entwickler sowie Helpdesk-Personal, das bei Verbindungsausfällen Anrufe entgegennimmt. Eine Lösung der Enterprise-Klasse sollte mit mehreren Out-of-the-Box-Integrationen Agilität ermöglichen.
Unterstützt der Anbieter Integrationen mit älteren Multifaktor-Authentifizierungslösungen?	Wenn Sie Ihre alte MFA-Lösung austauschen, erlaubt Ihnen ein zeitlich begrenzter Parallelbetrieb, stufenlos zu Ihrer neuen Lösung zu migrieren. Dies erfordert jedoch eine Integration mit dem Anbieter Ihrer alten MFA-Lösung.
Erlaubt der Anbieter webbasierten administrativen Zugriff und rollenbasierte Berechtigungen?	Unterschiedliche Vertrauensstufen ermöglichen unterschiedlich abgestufte Zugriffs- und Berechtigungsoptionen. Rollenbasierte Berechtigungen und webbasierter Zugriff für Untergruppen von Benutzern sind wichtig, um den Zugriff auf der Grundlage administrativer Berechtigungen flexibel zu gestalten.
Unterstützt der Anbieter administrative Bypasscodes?	In den seltenen Fällen, in denen sich Benutzer nicht über einen der zahlreichen Fehlereskalationsprozesse authentifizieren können, ist es wichtig, dass der Administrator eingreifen kann.
Unterstützt der Anbieter eine kryptografisch starke Aufrechterhaltung der Sitzung?	Eine sichere Kommunikation zwischen Mobilanwendung, MFA-Service und externen Anwendungen ist wichtig, um Ihre Anwendungen und sensiblen Daten effektiv zu schützen.
Stellt der Anbieter einen detaillierten Bericht von Authentifizierungsereignissen bereit?	Detaillierte Daten zu Authentifizierungsereignissen wie Evaluierung und Ergebnis, IP-Adresse und MDM-Status tragen dazu bei, die Sicherheit in Ihrem Unternehmen ständig zu verbessern.
Unterstützt der Anbieter Endpunkt-Visibilität und grundlegende Funktionen zur Fehlerbehebung?	Endpunkt-Visibilität und Fehlerbehebung werden normalerweise von Enterprise Mobility Management- und Virenschutzanbietern bereitgestellt. Doch wenn die MFA-Lösung über grundlegende Funktionen verfügt, profitieren Sie von einer zusätzlichen Schutzschicht für Ihre gefährdeten verwalteten und unverwalteten Geräte sowie von zusätzlichen Kontext-Informationen zur Benutzerauthentifizierung.
Unterstützt der Anbieter Out-of-the-Box-Integrationen mit MDM-Anbietern?	Mit diesen Integrationen können Sie die Authentifizierung entsprechend den vom MDM-Anbieter gesammelten Geräteattributen (z. B. Compliance mit den Unternehmensrichtlinien) heraufstufen oder den Zugriff blockieren.

UNTERNEHMENSANFORDERUNGEN

EVALUIERUNGSKRITERIEN	BEDEUTUNG
Erlaubt der Anbieter Co-Branding für die Anwendung?	Co-Branding ermöglicht eine einheitliche und vertraute Benutzererfahrung. Außerdem gibt das gewohnte Look & Feel dem Benutzer die Gewissheit, dass er sich in der Unternehmensumgebung authentifiziert.
Erlauben Technologieplattform und Preismodell des Anbieters ein einfaches Upgrade für zusätzliche Anwendungsfälle?	Unternehmen, die den Zugriff auf Anwendungen und sensible Daten schützen, handeln immer häufiger im Auftrag ihrer Partner und Kunden und weiten auch MFA auf neue Anwendungsfälle wie die Anmeldung bei Windows-Geräten aus.
Stellt der Anbieter einen Offline-MFA-Modus bereit?	Wenn bei Endbenutzern die Internetverbindung ausfällt, kann das die Produktivität der Mitarbeiter erheblich beeinträchtigen. Offline-MFA mildert die Auswirkungen eines Internetausfalls ab.
Stellt der Anbieter weitere Funktionen aus dem Identity- und Access-Management-Bereichs bereit?	Anbieter von Full-Service-IAM-Lösungen, die auf den IAM-Bereich spezialisiert sind, haben in der Regel mehr aktuelle Features, mehr Know-how und einen besseren Support.
Gilt der Anbieter als Innovationsführer, dessen Lösung auf offenen Standards wie OAuth2.0 und OpenID Connect basiert?	Innovative Anbieter bieten in der Regel die modernsten Lösungen auf dem Markt und treiben technologische Verbesserungen für die Herausforderungen von morgen voran.
Bekommen Anbieter und Lösung gute Bewertungen bei Analysten wie Gartner, IDC, Forrester und KuppingerCole?	Analysten können zuverlässige unabhängige Informationen zu Konkurrenzprodukten bieten.

ANBIETER-EVALUIERUNG UND -AUSWAHL

Nachdem Sie all Ihre Anforderungen definiert haben, sollten Sie Ihre Daten in eine passende Form bringen, um die einzelnen Anbieter auf einfache Weise zu evaluieren. Dafür eignet sich eine Sheets- oder Excel-Tabelle. Erstellen Sie am besten eine Reihe für jedes Ihrer Auswahlkriterien und ordnen Sie diese wie oben nach den wichtigsten Anforderungen.

Fügen Sie anschießend für jeden Anbieter, den Sie evaluieren möchten, eine Spalte hinzu. Sie können anhand von Punkten bewerten, wie gut die einzelnen Anbieter Ihre Kriterien erfüllen:

0 = erfüllt die Anforderung nicht
1 = erfüllt die Anforderung nur sehr eingeschränkt
2 = erfüllt die Anforderung teilweise
3 = erfüllt oder übertrifft die Anforderung

Mit diesem System können Sie jeden Anbieter mit 0–3 Punkte für jedes Ihrer Kriterien bewerten. Zählen Sie anschließend die Punkte der einzelnen Anbieter zusammen. Der Anbieter mit der höchsten Punktzahl ist auch der Anbieter, der Ihre Anforderungen am besten erfüllt.

#3140 | 07.18 | v013