yubico

FALLSTUDIE

HYATT®

Branche

Gastgewerbe

Vorteile

Phishing-resistente MFA für alle PII- und Karteninhaberdaten

Nahtlose Mitarbeiterauthentifizierung

Verbessertes Gasterlebnis

Protokolle

FIDO2

OTP

Produkte

YubiKey 5 NFC USB-A für Front-of-House-Mitarbeiter mit Kundenkontakt

YubiKey 5C Nano für Wissensarbeiter

YubiKey Lightning, wenn gewünscht

Informationen zur Bereitstellung

Aktuell: Für verschiedene Gruppen und Organisationen innerhalb der Hyatt-Gruppe bereitgestellt

Ziel: Passwortlose Authentifizierung für alle 170.000 Hyatt-Kollegen

Hyatt Hotels nutzt die passwortlose Authentifizierung zur Reduzierung von Risiken und Verbesserung des Gasterlebnisses

Phishing-resistente MFA verhindert Authentifizierungsmüdigkeit und sorgt für ein nahtloses Gasterlebnis

Yubico und Microsoft bieten starke Identitäts-, Endpoint- und Zugriffskontrollen für die globalen Betriebsabläufe von Hyatt

Die Hyatt Hotels Corporation ist mit rund 1.500 Hotels und All-Inclusive-Hotels in 70 Ländern eine der weltweit bekanntesten und angesehensten Hotelmarken. Da die Gruppe weltweit so viele Hotels und Mitarbeiter umfasst, ist es eine gewaltige Aufgabe, diese vor einer ständig wachsenden Liste von Cyberrisiken zu schützen – ganz zu schweigen von der Notwendigkeit, dass sich alle Mitarbeiter authentifizieren, bevor sie auf die Hyatt-Tools und -Anwendungen zugreifen können.

Art Chernobrov, Director of Identity, Access, and Endpoints, und sein Team aus 15 Mitarbeitern sind für die Verwaltung der Identitäten aller 200.000 Mitarbeiter im Unternehmen sowie der über 50.000 Endgeräte weltweit verantwortlich. Eine der größten Herausforderungen für Hotelbetreiber weltweit besteht darin, den Zugriff auf eine Art und Weise zu ermöglichen, die sowohl Sicherheit als auch Benutzerfreundlichkeit bietet.

Hyatt hat in den letzten zehn Jahren eng mit Microsoft zusammengearbeitet und Produkte wie Office 365 und Azure Active Directory (AD) Premium für das Identitäts- und Zugriffsmanagement eingeführt. Chernobrov arbeitete eng mit Microsoft zusammen, um sicherzustellen, dass die Identitätsplattform den komplexen Anforderungen von Hyatt gerecht wird. Dazu zählte auch die Notwendigkeit einer längeren Liste vertrauenswürdiger Standorte, um Franchisestandorte und dynamische Verwaltungseinheiten zu unterstützen und so die dezentrale Verwaltung häufiger Aufgaben wie das Zurücksetzen von Passwörtern zu ermöglichen.

> “Wir machen große Fortschritte beim Schutz der Sicherheit unserer Gäste und Kollegen, indem wir für alle Anwendungen, die sowohl personenbezogene Daten als auch Karteninhaberdaten offenlegen können, Phishing-resistente MFA-Methoden vorschreiben.“

Art Chernobrov
Hyatt Hotels Corporation
Director of Identity, Access, and Endpoints

Eine Lösung, die eine Brücke zwischen alten und modernen Anwendungen bildet

YubiKey unterstützt:

WebAuthn/FIDO2

FIDO

U2F

OTP

OpenPGP 3

Smart Card-Authentifizierung

Veraltete MFA verfehlt die Erwartungen an Sicherheit und Benutzerfreundlichkeit

Obwohl Microsoft alle Voraussetzungen für die Zugriffsbereitstellung und die Identitätsverwaltung erfüllte, war die Implementierung der Multi-Faktor-Authentifizierung (MFA) von Hyatt nicht bei allen Benutzern willkommen.

> Eine der Herausforderungen, über die Geschäftsführer und Eigentümer unserer Hotels berichten, ist die Anzahl der Anmeldungen, die sie vornehmen müssen. Ihre Frustration rührt vor allem von den Herausforderungen und vom notwendigen Zeitaufwand her, die mit der Anmeldung bei den verschiedenen Anwendungen in Verbindung stehen – vom Gastreservierungssystem über POS-Systeme bis hin zu Gastabwicklungssystemen.“

Damals nutzte Hyatt die mobile MFA, wobei Einmalpasswörter (OTP) per SMS-Nachrichten zur Authentifizierung bei Apps oder zur erneuten Authentifizierung in zufälligen Intervallen gesendet wurden. Aufgrund der hohen Anzahl an Eingabeaufforderungen gewöhnten sich die Benutzer daran, für jede Eingabeaufforderung „Genehmigen“ zu wählen, wodurch die mobile MFA ein einfaches Ziel für Phishing- und Man-in-the-Middle-Angriffe (MitM) wurde. Tatsächlich konnte jeder Sicherheitsvorfall, den Hyatt je hatte, auf eine versehentlich genehmigte MFA-Anfrage zurückgeführt werden.

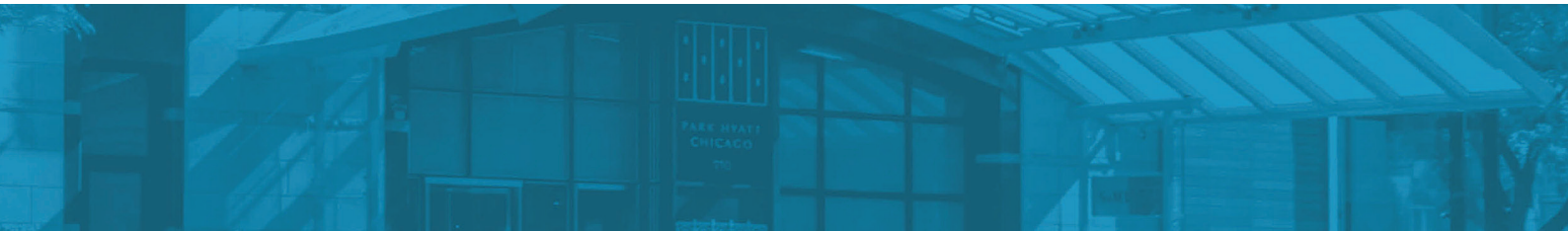
Moderne MFA, die eine starke Phishing-Resistenz bietet und sich leicht in eine Microsoft-Umgebung integrieren lässt

Als Microsoft eine Lösung für diese Authentifizierungsprobleme bei Hyatt vorstellte, war Hyatt für Vorschläge offen. Diese Lösung? Der YubiKey. Der YubiKey ist ein Hardware-Sicherheitsschlüssel, der starke Phishing-resistente Multiprotokoll-Fähigkeiten bietet, um den Zugriff auf Computer, Netzwerke und Hunderte von Online-Diensten zu sichern. Der YubiKey unterstützt WebAuthn/FIDO2, FIDO U2F, Einmalkennwort (OTP), OpenPGP 3 und Smart Card-Authentifizierung und ist eine Lösung, die eine Brücke zwischen älteren und modernen Anwendungen bildet und die passwortlose Authentifizierungserfahrung bietet, die jetzt die Empfehlung für alle Azure AD-Clients ist.

> Die Sicherheit der Daten unserer Gäste hat für unser Unternehmen oberste Priorität. Unsere Gäste sollen wissen, dass wir bei ihrem Hyatt-Aufenthalt unser Möglichstes und Bestes tun, um diese Informationen so sicher wie möglich zu halten.“

Hyatt unternimmt wichtige Schritte, um die Sicherheit von Gästen und Kollegen zu schützen, indem das Unternehmen Phishing-resistente MFA-Methoden für alle Anwendungen, die sowohl personenbezogene Daten als auch Karteninhaberdaten offenlegen, vorschreibt. Der YubiKey wird auch von Kollegen im Callcenter und Treueprogramm verwendet, die entweder in auf mobilen Zugang beschränkten Umgebungen oder auf Remote-Basis in unsicheren Netzwerken arbeiten, sowie für den Zugriff auf Systeme zur Verwaltung privilegierter Zugriffe (Privileged Access Management, PAM) und zur Planung von Unternehmensressourcen (Enterprise Resource Planning, ERP).

Wie Chernobrov bemerkt: „Weder Social Engineering noch MFA-Ermüdung können an der Tatsache rütteln, dass ich ohne einen YubiKey auf dieses System nicht zugreifen kann.“ Dieselbe Logik gilt für die Lieferkette, wobei zur Identitätsüberprüfung in der gesamten Lieferkette vorab registrierte Schlüssel an Lieferanten gesendet werden.



> Ein reibungsloses Benutzererlebnis ist ein zentraler Grundsatz unserer Abteilung. Wir möchten sicherstellen, dass für unseren Endbenutzer alles so einfach und nahtlos wie möglich ist.“

Der YubiKey bietet eine nahtlose, passwortlose Authentifizierung und verbessert die Mitarbeitererfahrung

Das Gästeerlebnis hat für Hyatt oberste Priorität. Doch dieselben Werte – Menschen und Erfahrung – gelten für alle Hyatt-Kollegen. „Wir möchten mit unseren Front-of-House-Kollegen genauso umgehen, wie diese unsere Gäste behandeln“, so Chernobrov. „Wir betrachten also das Erlebnis, das wir Hyatt-Kollegen bieten können, um ihren Zugang so nahtlos und einfach wie möglich zu gestalten.“

Von dem Moment an, in dem ein Kollege seine Arbeit bei Hyatt aufnimmt, stellt das Team von Chernobrov sicher, dass er Zugriff auf die benötigten Anwendungen hat und dass sein Zugriff mit ihm verschoben wird, wenn er zwischen Hotels oder zwischen Büro und Hotel wechselt. Mit dem YubiKey und Azure AD kann Hyatt nun eine passwortlose Authentifizierung für alle Apps bereitstellen, auf die ein Benutzer für seine Rolle zugreifen muss.

Hyatt bietet den Front-of-House-Kollegen den YubiKey 5 NFC zur Unterstützung der mobilen Tap-and-Go-Authentifizierung und bietet Callcenter-Kollegen und Back-of-House-Wissensarbeitern den 5C Nano, obwohl die Benutzer Informationen erhalten, die die Wahl des Formfaktors unterstützen. Dank Videos, die den YubiKey in Aktion zeigen, war die Einführung einfach. Tatsächlich war die Einführung so einfach, dass die erwarteten Supportanrufe einfach „nie eintraten“.

> Personen, die nicht wirklich computerversiert sind, können sich so schnell und schmerzlos registrieren und ihren YubiKey dann mühelos und sofort verwenden – das ist ein leichter Sieg für uns.“

Um einen YubiKey in einem beliebigen Szenario zu verwenden, legen Kollegen einfach den Schlüssel (etwas, das sie haben) in das Gerät ein und nehmen entweder per Antippen oder PIN (etwas, das sie sind oder kennen) Zugriff, um sich bei Azure AD-Ressourcen zu authentifizieren. Der YubiKey ist nicht nur bis zu 4-mal schneller als die OTP- und SMS-basierte Authentifizierung, sondern Hyatt-Kollegen werden nach dem Aufbau der Sitzung auch nicht mehr zur wiederholten MFA aufgefordert. So können sowohl Front-of-House- als auch Callcenter-Kollegen sicher und schnell auf die Bedürfnisse ihrer Gäste eingehen.

> Unsere Benutzer waren von der nahtlosen Funktionsweise überrascht. Sie berühren zu Beginn des Tages einen YubiKey – und mehr ist nicht zu tun. Die Apps werden gestartet, und sie berühren diesen Schlüssel erst wieder, nachdem die Maschine gesperrt und neu gestartet wurde. Die Produktivität ist deutlich gestiegen. Es geht dabei nicht nur um das Thema Sicherheit, sondern auch um die Erleichterung des Endnutzeralltags.“

YubiKeys sorgen für kundenorientiertere Gasterlebnisse

Bei kundenorientierten Rollen an der Rezeption war die mobile Authentifizierung nicht nur eine unsichere Authentifizierungsmethode, sie wirkte sich unter Umständen auch auf die Wahrnehmung der von einem Kollegen gebotenen Kundenerfahrung aus.

> Eine der Herausforderungen, denen wir als Hotelplattform gegenüberstehen, ist das visuelle Bild, das mit der Nutzung eines Mobilgeräts zur Durchführung eines MFA-Prozesses verbunden ist“, so Chernobrov. „Wenn Mitarbeiter des Gästeservice auf ihr Telefon schauen, um eine MFA-Antwort oder -Genehmigung zu geben, vermittelt dies unserer Ansicht nach nicht die Botschaft, die wir Gästen an der Rezeption weitergeben möchten.“

Wenn ein Hyatt-Mitarbeiter ein Mobiltelefon in der Hand hält, erwirkt dies den Eindruck, als ginge er seinen Privatangelegenheiten nach oder sei auf sozialen Medien aktiv. Dies war nicht das Image, das Hyatt vermitteln wollte.

> Die Verwendung eines YubiKey bietet dem Mitarbeiter nicht nur ein nahtloses Erlebnis und schützt unsere Daten, sondern ermöglicht es ihm auch, sein Mobiltelefon während der Gästebetreuung wegzulegen.“

Dank des passwortlosen Erlebnisses des YubiKeys können sich Hyatt-Kollegen nahtlos und schnell in ihrer Arbeitsumgebung authentifizieren, um die Bedürfnisse der Gäste zu erfüllen. Dies führt zu einem besseren Blickkontakt mit dem Gast und einem nahtlosen Gasterlebnis. „Wir wollen einem Gast beim Einchecken ins Hotel das Gefühl vermitteln, dass nichts zwischen der Interaktion zwischen Gast und Nutzer steht“, erklärt Chernobrov.

Die Zukunft bei Hyatt ist passwortlos

Das ultimative Ziel für Hyatt ist es, im gesamten Unternehmen vollkommen passwortlos zu agieren – angesichts der Tatsache, dass das Unternehmen mehr als 200.000 Kollegen an ca. 1.500 Standorten weltweit beschäftigt, keine geringe Leistung. Um dies zu erreichen, integriert Hyatt YubiKeys weiterhin als Teil jeder neuen No-Touch-Hardware-Implementierung sowie neben neuen Anwendungs-Rollouts oder -Upgrades. Das bedeutet, dass im Rahmen solcher Rollouts 5.000 oder 10.000 YubiKeys gleichzeitig eingesetzt werden.

Während Hyatt all seine Anwendungen durchläuft und den YubiKey für jede neue Anwendung fordert, für die unter Azure AD bisher Single Sign-On (SSO) verwendet wurde, werden irgendwann alle Anwendungen abgedeckt sein. „Das vollständige Onboarding geht blitzschnell und reibungslos vonstatten. Dann stellt sich uns die anfängliche Frage, wie wir dies bis zu 200.000 Mitarbeitern bereitstellen können, nicht mehr.“

> Der größte Vorteil, den Hyatt durch die Bereitstellung von YubiKeys erhält, besteht darin, Passwörter aus der Unternehmensumgebung auszuschließen. Was nicht da ist, kann keinen Schaden anrichten. Wir werden es wirklich zu schätzen wissen, sobald wir in der Hotelumgebung keine Passwörter mehr nutzen müssen.“

Obwohl eine vollständig passwortlose Erfahrung mit einer finanziellen Belastung einhergeht, ist der Mehrwert, den die Einführung passwortloser Authentifizierung auf der Führungsebene demonstriert hat, jedoch umso größer. „Sie wissen, dass sie Hyatt zu einem sichereren Ort für Gäste und Kollegen machen, ohne dass sie Angst vor einem problematischen Endnutzererlebnis haben müssen“, bemerkt Chernobrov. „Es ist eine Investition, die sich auszahlt.“

Weitere Informationen | yubi.co/customers | yubi.co/retail-hospitality

yubico

Über Yubico Als Erfinder des YubiKey erleichtert Yubico die sichere Anmeldung. Yubico ist nicht nur führender Anbieter globaler Standards für den sicheren Zugriff auf Computer, mobile Geräte und mehr, sondern auch Entwickler von und treibende Kraft hinter FIDO2, WebAuthn, und FIDO Universal 2nd Factor (U2F) sowie von Open Authentication Standards. Weitere Informationen finden Sie unter: www.yubico.com.