yubico

WHITEPAPER ZUM GESUNDHEITSWESEN: JANUAR 2021

Starke Authentifizierung mit dem YubiKey: Best Practices für den Gesundheitssektor

Warum starke Authentifizierung im Gesundheitswesen unerlässlich ist

Seit Anfang 2020 hat das Gesundheitswesen eine bedeutende digitale Transformation durchlaufen. Ob es um Fernarbeit geht, um den zunehmenden Einsatz von E-Gesundheitsleistungen wie elektronischen Rezepten, Telemedizin und elektronischen Zahlungen oder sogar um virtuelle Zusammenarbeit bei der Forschung an wichtigen Medikamenten und Impfstoffen: Einrichtungen des Gesundheitswesens verändern sich, um die Ergebnisse für die Patienten zu verbessern.

Gleichzeitig nimmt auch im Gesundheitssektor die Zahl der Cyberangriffe zu. Am 20. Mai 2020 veröffentlichten das United States Department of Homeland Security (DHS), die Cybersecurity and Infrastructure Security Agency (CISA) und das britische National Cyber Security Centre (NCSC) eine gemeinsame Warnung vor APT (Advanced Persistent Threat)-Gruppen, die groß angelegte Password-Spraying-Kampagnen gegen Einrichtungen des Gesundheitswesens, Pharmaunternehmen und medizinische Forschungseinrichtungen durchführen.[1] Einige Zeit später, am 28. Oktober 2020, veröffentlichten die CISA, das Federal Bureau of Investigation (FBI) und das Department of Health and Human Services (HHS) eine Warnung vor erhöhten, akuten Cyberbedrohungen, insbesondere Ransomware, für Krankenhäuser und Gesundheitsdienstleister in den USA.[2]

Credential-Phishing-Angriffe, der Hauptvektor für Kontoübernahmen, können eine Vielzahl schädlicher Auswirkungen haben. Zum Beispiel können Anmeldedaten missbraucht werden, um Ransomware zu verbreiten und unbefugt auf digitale Gesundheitssysteme und -daten zuzugreifen, so etwa Patientenakten, personenbezogene Informationen und Kreditkartendaten. Jede erfolgreiche Kontoübernahme kann dazu führen, dass Branchenvorschriften wie der Health Insurance Portability and Accountability Act (HIPAA) oder die Bestimmungen für die elektronische Verschreibung kontrollierter Substanzen (Electronic Prescriptions for Controlled Substances, EPCS) verletzt werden, was erhebliche Bußgelder nach sich ziehen kann.

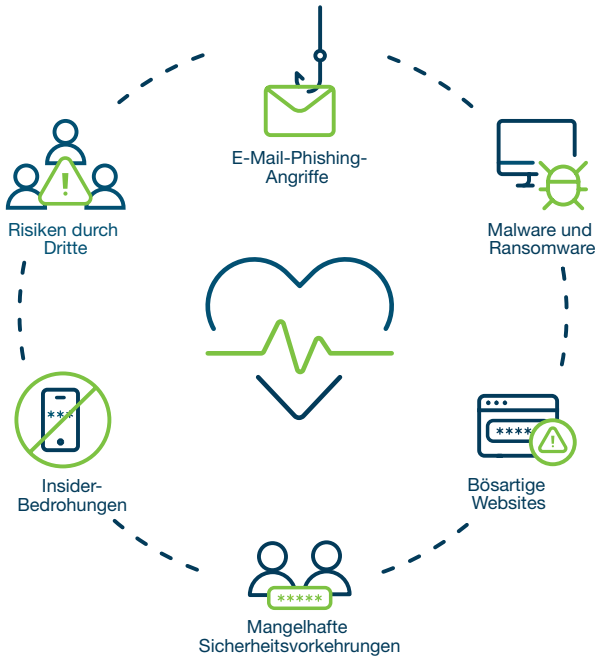
[1] https://us-cert.cisa.gov/ncas/alerts/AA20126

[2] https://us-cert.cisa.gov/ncas/current-activity/2020/10/28/ransomware-activity-targeting-healthcare-and-public-health-sector

Weitverbreitete Cyberbedrohungen und Schwachstellen im Gesundheitssektor

Gängige Cyberbedrohungen und Schwachstellen in Einrichtungen des Gesundheitswesens können die Übernahme von Konten ermöglichen, falls keine starke Authentifizierung implementiert ist.

- **E-Mail-Phishing-Angriffe:**
  Angreifer schicken scheinbar legitime, in Wahrheit aber bösartige E-Mails an Benutzer, um an deren Benutzernamen und Kennwörter zu gelangen. Spear-Phishing-Mails, die oft sehr effektiv sind, sind stark auf die jeweilige Zielperson zugeschnitten.
- **Malware und Ransomware:**
  Die Abwehrmaßnahmen gegen gängige Mechanismen zur Malware-Verbreitung, wie etwa das Filtern von E-Mail-Anhängen, sind besser geworden. Deshalb setzen Cyberkriminelle heute zunehmend auf Phishing und Kontoübernahmen als ersten Schritt in mehrstufigen Angriffen. Die Angreifer nutzen Malware, einschließlich Ransomware, um einzelne Geräte, Server oder sogar ganze Netzwerke zu übernehmen und Daten, Benutzernachweise etc. zu stehlen. Bei einem Ransomware-Angriff wird den Benutzern in der Regel der Zugriff auf ihr System oder ihre Dateien verwehrt, bis Lösegeld gezahlt oder Anmeldedaten preisgegeben wurden.
- **Bösartige Websites:**
  Cyberkriminelle richten Websites ein, die seriösen Sites ähneln, um dort Malware zu verbergen und Benutzernamen und Kennwörter zu stehlen, die dann für E-Mail-Phishing-Angriffe genutzt werden können.
- **Mangelhafte Sicherheitsvorkehrungen:**
  Durch schlechte Sicherheitshygiene können Mitarbeiter ein Unternehmen anfällig für Angriffe machen. Dazu gehört beispielsweise die Verwendung schwacher Passwörter, die gemeinsame Nutzung von Passwörtern und die Verwendung des gleichen Passworts für mehrere Konten – eventuell auch private.
- **Insider-Bedrohungen:**
  Der Verizon Data Breach Investigations Report 2020 führt interne Akteure als die zweithäufigste Ursache für Sicherheitsverletzungen im Gesundheitswesen an (48 %). Damit liegen sie nicht weit hinter den externen Bedrohungsakteuren (51 %).[3] In Bereichen wie Callcentern, in denen den Mitarbeitern der Zugang zu hochsensiblen Daten anvertraut wird, stellen Insider-Bedrohungen ein erhebliches Risiko dar. Keinesfalls dürfen Mobilgeräte zur Authentifizierung in solchen Umgebungen verwendet werden, in denen geschützte Gesundheits- oder personenbezogene Daten mit einer Kamera erfasst und an böswillige Akteure verkauft werden könnten.
- **Risiken durch Dritte:**
  Viele Gesundheitsdienstleister lagern Services wie Catering, Gehaltsabrechnungen und Webentwicklung an Dritt- und sogar Viertanbieter aus. Diese Dienstleister haben oft Zugang zu gemeinsam genutzten sensiblen Daten, die anfällig für Angriffe sein können, wenn sie nicht richtig abgesichert werden.



[3] 2020 Verizon Data Breach Investigations Report

Was ist starke Authentifizierung?

Die Sicherheitsbranche geht zunehmend zu einem Zero-Trust-Sicherheitsmodell über, bei dem nichts von vornherein als vertrauenswürdig gilt, weder innerhalb noch außerhalb des Perimeters. Stattdessen muss jede Verbindung erst überprüft werden, bevor Zugriff gewährt wird, was die Authentifizierung zu einer Schlüsselkomponente jeder Zero-Trust-Architektur macht. In den USA schreiben EPCS-Bestimmungen auf Bundesebene und in verschiedenen Staaten Zwei-Faktor-Authentifizierung und starke Zugangskontrollen vor, um Sicherheitsrisiken zu minimieren. Und wenngleich HIPAA bei seiner Verabschiedung keine vergleichbare Vorschrift enthielt, ist eine starke Authentifizierung angesichts der heutigen Bedrohungslage unabdingbar geworden, um die in dem Gesetz geforderten „angemessenen und geeigneten Sicherheitsmaßnahmen“ zu realisieren. Dennoch verwenden viele Unternehmen immer noch schwache, veraltete Authentifizierungsmechanismen wie Benutzername/Passwort oder Authentifizierung per SMS/E-Mail. Andere setzen intern sicherere Alternativen wie etwa Smartcards mit NFC-Lesegeräten ein, die aber den Anforderungen der heutigen mobilen Mitarbeiter an die Portabilität nicht entsprechen, sodass diese außerhalb des Unternehmens potenziell ungeschützt sind. Im Gesundheitswesen wiederum haben die häufig komplexen und alten Infrastrukturen in Kombination mit Technologien für Telearbeit dazu geführt, dass die Nutzung von Zwei-Faktor-Authentifizierung (2FA) und Multi-Faktor-Authentifizierung (MFA) variiert.

Doch was genau ist starke Authentifizierung und wie kann sie vor Kontoübernahmen schützen?

Eine starke Authentifizierung hat zwei wesentliche Eigenschaften:

- Sie verlässt sich nie ausschließlich auf Shared Secrets-basierte Verfahren oder Protokolle (symmetrische Schlüssel), wie etwa Passwörter, Einmalpasswörter, SMS-Codes und Wiederherstellungsfragen.
- Sie wehrt Credential Phishing, Man-in-the-Middle-Angriffe (MitM) und Impersonation-Angriffe zuverlässig ab. Bei einer starken Authentifizierung wird davon ausgegangen, dass manche Angriffe bis zum Endnutzer durchkommen werden; das Authentifizierungsverfahren verhindert dann, dass der Angriff gelingt.

Von den verschiedenen Authentifizierungsprotokollen gewährleisten nur Smartcard-Verfahren und die modernen Protokolle FIDO U2F und FIDO2/WebAuthn wirklich eine starke Authentifizierung. Zudem sollte auch die Benutzerfreundlichkeit und Skalierbarkeit von MFA-Lösungen bedacht werden. Schlechte Benutzererfahrungen und geringe Portabilität und Skalierbarkeit können zu mangelnder Akzeptanz führen und die Kosten in die Höhe treiben.

Nicht alle Authentifizierungen sind gleichwertig

Benutzername und Passwort	Grundlegende 2FA-Authentifizierung: SMS, E-Mail, Mobiltelefon	YubiKey: Starke Authentifizierung
Überall im Einsatz	Nicht ausreichend auf Sicherheitsanforderungen zugeschnitten	Optimal auf Sicherheitsanforderungen zugeschnitten
Bekannte Usability-Lücken	Nutzt vorhandene Technologie-Stacks, die anfällig für Netzwerk- und Software-Angriffe sind	Keine Netzwerkverbindung, Datenspeicherung oder Client-Software erforderlich
Verwaltung teuer und aufwändig	Häufiges Ziel für Credential Phishing	Hochgradig Phishing-resistent
Häufiges Ziel für Credential Phishing		

Mehr Sicherheit und Benutzerfreundlichkeit mit dem YubiKey

Um das Risiko von Phishing-Angriffen zu verringern und Kontoübernahmen zu unterbinden, stellt Yubico den YubiKey bereit – einen Hardware-Sicherheitsschlüssel, der eine starke, skalierbare Multi-Faktor-Authentifizierung ermöglicht. In einer unabhängigen Untersuchung war der YubiKey die einzige Lösung, die Kontoübernahmen zu 100 % verhinderte.[4] Der YubiKey unterstützt zahlreiche Authentifizierungsprotokolle, darunter OTP, OpenPGP und starke Authentifizierungsstandards wie Smartcard-Verfahren, FIDO U2F und FIDO2/WebAuthn. Dadurch gewährleistet er höhere Sicherheit als Benutzernamen/Passwörter und mobilbasierte Authentifikatoren sowie hervorragende Portabilität und Benutzerfreundlichkeit. Zudem senkt der YubiKey den Verwaltungsaufwand, da er mehr Plattformen unterstützt als herkömmliche Smartcard-Lösungen.

Der YubiKey ist eine hochgradig portable Root of Trust, die mit zahlreichen Geräten wie Desktops, Laptops, Mobiltelefonen, Tablets und Notebooks kompatibel ist und keine Batterie oder Internetverbindung erfordert. Er lässt sich auch zur starken Authentifizierung bei jedem USB- oder NFC-fähigen System oder Gerät im Gesundheitswesen verwenden. Damit eignet sich der YubiKey ideal zum Schutz der Infrastrukturen im Gesundheitswesen und der Computersysteme, die das medizinische Personal nutzt.

Der YubiKey ermöglicht starke Authentifizierung für alle:

- Mitarbeiter des Gesundheitswesens und klinisches Personal wie Ärzte und Pfleger können sich durch einfaches Antippen schnell und sicher bei EHR-Systemen, gemeinsam genutzten Workstations und E-Rezept-Anwendungen anmelden, um auf Patientenakten zuzugreifen und produktiver zu arbeiten – auch aus der Ferne.
- Gesundheitsdienstleister können die Einhaltung von Branchenvorschriften gewährleisten, IT-Kosten für die Passwortverwaltung einsparen und mehr Patienten schneller versorgen. So lässt sich auch die geschäftliche Effizienz verbessern.
- Die Patienten erhalten sicheren Zugriff auf ihre Online-Gesundheitsdaten und elektronischen Rezepte und haben die Gewissheit, dass ihre personenbezogenen Informationen und Gesundheitsdaten vor Cyberkriminellen geschützt sind.

[4] https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Best Practices für starke Authentifizierung mit dem YubiKey

1. Einhaltung von HIPAA, HITECH und EPCS

HIPAA schreibt angemessene Maßnahmen zur Absicherung elektronischer geschützter Gesundheitsdaten (ePHI) vor. Wenn ePHI-Daten verlorengehen, gestohlen oder unbefugt eingesehen werden, muss die betroffene Einrichtung ein Bußgeld zahlen. Auch ist jede Datenverletzung gemäß dem Health Information Technology for Economic and Clinical Health Act (HITECH) meldepflichtig. EPCS erfordert eine Bestätigung der Identität des Leistungserbringers und eine Identitätsprüfung bei der Rezeptausstellung.

Gemäß den Bestimmungen der Drug Enforcement Agency (DEA) muss jeder US-Bundesstaat, der eine elektronische Ausstellung von Rezepten gestattet, die DEA-Richtlinien für EPCS befolgen – auch dann, wenn der Bundesstaat selbst Vorschriften dazu erlassen hat. Die DEA-Richtlinien zur elektronischen Verschreibung kontrollierter Substanzen besagen, dass alle Hardware-Geräte, die zur Authentifizierung verwendet werden, den Federal Information Processing Standard (FIPS) 140-2 Security Level 1 erfüllen müssen.

YubiKeys sind FIPS 140-2-validiert und entsprechen dem höchsten Sicherheitsniveau (Authentication Assurance Level 3, AAL3) der NIST SP800-63B-Empfehlungen. Die Verwendung von YubiKeys für starke MFA hilft Gesundheitseinrichtungen, den EPCS-Anforderungen für die Ausstellung elektronischer Rezepte gerecht zu werden. Außerdem können Gesundheitseinrichtungen YubiKeys auch für starke Zugriffskontrollen und die Authentifizierung bei Systemen verwenden, auf denen Patientendaten und ePHI gespeichert sind, um so HIPAA-konform zu bleiben.

2. Schutz elektronischer Patientendatensysteme

Einrichtungen des Gesundheitswesens, die elektronische Patientendatensysteme oder andere elektronische Technologien zur Erfassung und Nutzung von ePHI einsetzen, müssen die HIPAA-Sicherheitsregel und „Meaningful Use“-Vorgaben einhalten. Darüber hinaus ist der Schutz der Privatsphäre der Patienten und die Absicherung ihrer elektronisch gespeicherten Gesundheitsdaten eine Kernanforderung der Medicare- und Medicaid EHR Incentive-Programme in den USA. Diese Schutzmaßnahmen sind unerlässlich, gleich, ob das Patientendatensystem auf einem Server vor Ort installiert ist oder von einem Cloud Service Provider (CSP) gehostet wird.

Wenn YubiKeys zur starken MFA bei EHR-Systemen eingesetzt werden und so eine zusätzliche Verifizierungsebene für Benutzeridentitäten geschaffen wird, haben nur autorisierte Personen Zugang zu Systemen mit ePHI, wie in HIPAA 164.308(a) (4)(ii)(B) vorgeschrieben. Ärzte und anderes medizinisches Personal müssen nur durch Tippen/Berühren des YubiKeys die Benutzeranwesenheit bestätigen und können dann von ihren eigenen Geräten oder sogar von gemeinsam genutzten Geräten/Workstations sicher auf EHR-Anwendungen zugreifen. Diese Überprüfung der Benutzerpräsenz stellt sicher, dass nicht etwa ein entfernter Angreifer oder Malware versucht, sich anzumelden.

3. Sicherer Fernzugriff auf Patientendaten

Viele Mitarbeiter im Gesundheitswesen arbeiten seit Anfang 2020 aufgrund von COVID-19 im Homeoffice, müssen aber trotzdem weiter auf Systeme und Daten zugreifen können, so etwa Datenbanken von Klinikern und Forschern, Testergebnisse, Finanzdaten, organisatorische Daten, Bildarchive, Pathologiebilder und mehr.

Multi-Faktor-Authentifizierung sollte in einer verteilten oder dezentralen Arbeitsumgebung eine der wichtigsten Anforderungen sein. Der YubiKey bietet eine benutzerfreundliche, langlebige und multifunktionale Lösung für alle Mitarbeiter, unabhängig von ihrem Gerätetyp, Betriebssystem oder Standort. YubiKeys eignen sich zur MFA für Identitätsmanagementsysteme (IAM) und Identitätsanbieter (IdPs) wie Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, PingID und RSA SecurID® Suite. In Kombination mit IAM-Lösungen und IdPs lässt sich der YubiKey auch für Single Sign-on (SSO) bei anderen geschäftskritischen Messaging- oder Videokonferenz-Apps wie Microsoft Teams, Google Hangouts und Zoom verwenden.

Viele Einrichtungen des Gesundheitswesens nutzen für Remote-Mitarbeiter Virtual Desktop Infrastructure (VDI) wie Citrix und VMware. Der Zugriff darauf kann mit dem YubiKey abgesichert werden.

Des Weiteren können YubiKeys auch eingesetzt werden, um einen sicheren VPN-Zugang zum Netzwerk eines Gesundheitsdienstleisters zu bieten. Pulse Secure und Cisco AnyConnect lassen sich so konfigurieren, dass ein YubiKey als Smartcard (PIV) für den Fernzugriff verwendet werden kann. Andere VPN-Anwendungen, die native Unterstützung für YubiKeys bieten, nutzen die OTP-Funktionen (Einmalpasswort).

Zu den weiteren Best Practices für sichere Remote-Zugriffe gehört es, die Smartcard-Funktionalität des YubiKeys zu nutzen und mit einem YubiKey plus PIN den Zugriff auf einen Computer abzusichern sowie die Authentifizierung für Passwort-Manager zu verstärken.

4. Sicherer Zugang für Call-Center-Mitarbeiter

Callcenter-Mitarbeiter haben Zugang zu sensiblen elektronischen Gesundheitsdaten (EHI), Kontoinformationen, Gesundheits- und Zahlungsdaten und damit Zugriffs-möglichkeiten, die unbedingt abgesichert werden müssen. Die Verwendung mobil-telefonbasierter Authentifikatoren ist in Callcentern aufgrund von Sicherheits-, Produktivitäts- und Compliance-Risiken besonders problematisch. Wenn Callcenter-Mitarbeiter mobile Geräte für 2FA nutzen, könnten sie in der Lage sein, mit der Kamera heimlich sensible Daten zu erfassen – für Einrichtungen des Gesundheitswesens ein enormes Risiko.

Hardware-Sicherheitsschlüssel wie der YubiKey eignen sich dagegen ideal für Callcenter. Da dafür keine Mobiltelefone benötigt werden, können Callcenter sicherstellen, dass ihre Mitarbeiter keine Kunden- und Finanzdaten fotografieren können, wie etwa Kontonummern, Sozialversicherungsnummern, Kreditkarten-daten und viele andere sensible Informationen. Zudem trägt die Einschränkung der Mobiltelefon-Nutzung auch zur Verbesserung der Callcenter-Produktivität bei.

5. Schutz vernetzter medizinischer Geräte (IoMT)

Vernetzte medizinische Geräte (Geräte aus dem Internet of Medical Things, IoMT) wie Infusionspumpen, Bildgebungssysteme, Patientenmonitore, Point-of-Care-Analysatoren, Gateways und EKG-Systeme sind sehr anfällig für Hackerangriffe, wenn keine angemessenen Sicherheits- und Zugriffskontrollen implementiert werden. Medizinische Geräte sind meist mit zahlreichen Sensoren und Monitoren verbunden und können Cyberkriminellen als potenzielles Einfallstor in das IT-Netz eines Gesundheitsdienstleisters dienen. Laut dem 2018 Annual Zingbox Threat Report on Medical Devices gibt es in US-Krankenhäusern in der Regel 10-15 vernetzte Geräte pro Bett. Aufgrund ihrer langen Lebenszyklen können solche Geräte ein gravierendes Sicherheitsrisiko darstellen, wenn ihre Betriebssysteme nicht regelmäßig gepatcht oder aktualisiert werden oder die Standardpasswörter des Herstellers nicht geändert werden.[5] Der 2020 Unit 42 IoT Threat Report stellte fest, dass 83 % aller medizinischen Bildgebungsgeräte mit nicht unterstützten Betriebssystemen laufen – 56 % mehr als in 2018.[6]

YubiKeys gewährleisten starke 2FA- und MFA-Sicherheit für vernetzte medizinische Geräte, indem sie den Benutzernamen und das Passwort um eine hardwaregestützte Authentifizierungsschicht erweitern. Dies verhindert unbefugte Zugriffe auf die Geräte und hilft, Kontoübernahmen zu unterbinden, selbst wenn schwache oder vom Hersteller voreingestellte Passwörter verwendet werden.

[5] Zingbox 2018 Annual Threat Report Medical Devices

[6] 2020 Unit 42 IoT Threat Report

6. **Sicherer Patientenzugriff auf Gesundheits- und Versicherungssysteme**

   Im Gesundheitssektor sind schnelle Zugriffe unerlässlich, da eine unzureichende medizinische Versorgung schwerwiegende Folgen haben kann. Verschiedene Umstände können den Patienten jedoch den Zugang zu Versorgungsleistungen erschweren, was die Bedeutung der Telemedizin unterstreicht. Patienten möchten medizinische Leistungen dann in Anspruch nehmen können, wenn sie sie brauchen, und mit Telemedizin können Gesundheitseinrichtungen Versorgungslücken schließen, die durch geografische Barrieren entstehen. Viele kleinere Einrichtungen in ländlichen Gegenden nutzen die Telemedizin auch, um sich mit Experten in städtischen Regionen zu vernetzen, damit die Patienten für aufwändige oder spezialisierte Behandlungen keine weiten Strecken zurücklegen müssen.[7]

   Der YubiKey kann für MFA bei telemedizinischen Anwendungen, Gesundheits-Websites und Versicherungs- und Zahlungssystemen eingesetzt werden, damit die Patienten ihre Daten auf sichere Weise einsehen und nutzen können. Ein schneller und sicherer elektronischer Zugriff auf Gesundheitsinformationen erleichtert es den Menschen, fundierte Entscheidungen über ihre Gesundheitsversorgung zu treffen.

7. **Schutz für die klinische Forschung und pharmazeutische Lieferketten**

   Die Pharmaindustrie und die klinische Forschung sind stark auf virtuelle, länder- und organisationsübergreifende Zusammenarbeit angewiesen. In der aktuellen COVID-19-Krise wird dies besonders deutlich. Zudem muss die pharmazeutische Industrie wichtige Komponenten, Materialien und Fertigprodukte im Ausland beschaffen, wie etwa eine Studie zeigt, die das Office of Technology Evaluation des US-Handelsministeriums 2011 unter dem Titel „Reliance on Foreign Sourcing in the Healthcare and Public Health (HPH) Sector: Pharmaceuticals, Medical Devices and Surgical Equipment“ veröffentlicht hat.[8] Wenn nicht jeder Mitwirkende in der klinischen Forschung und der pharmazeutischen Lieferkette zuverlässig gegen Kontoübernahmen und andere Cyberangriffe abgesichert ist, können sich ausländische Akteure und Staaten leicht Zugang zu geschützten und vertraulichen Informationen verschaffen.

   Der YubiKey ist einfach zu implementieren und macht es allen Einrichtungen leicht, eine lieferkettenübergreifende starke Authentifizierung umzusetzen. YubiKeys unterstützen moderne Protokolle wie FIDO2 und WebAuthn ebenso wie OTP, SmartCard (PIV), OpenPGP, frühere FIDO-Versionen und mehr. Da ein einziger YubiKey mit zahlreichen Anwendungen kompatibel ist, sind die Schlüssel sowohl für derzeitige Applikationen und Authentifizierungsmethoden einsetzbar als auch für erweiterte und neu aufkommende Verfahren. Die Benutzer können auch ihre SAFE-BioPharma-zertifizierten Identitätsnachweise auf dem YubiKey speichern, um zuverlässige Identitätssicherheit für Cyber-Transaktionen zu gewährleisten.

2020 hat das Gesundheitswesen neu definiert – und starke Authentifizierung unverzichtbar gemacht

COVID-19 hat die digitale Transformation im gesamten Gesundheitssektor beschleunigt und Initiativen für Telemedizin, Online-Versicherungen und -Zahlungen vorangetrieben, ebenso wie wichtige globale Kooperationen in der Arzneimittel- und Impfstoffforschung. Zugleich hat die Krise aber auch Sicherheitslücken aufgedeckt, die sich Cyberkriminelle und Staaten zunutze machen. Das Jahr 2020 hat gezeigt, dass eine starke, optimal auf Sicherheit ausgelegte Authentifizierung, die Phishing-resistent ist und Kontoübernahmen unterbindet, eine entscheidende Voraussetzung darstellt, um Vorschriften einzuhalten und sensible Gesundheitsdaten zu schützen.

Bei der Planung für die Zukunft nach der Pandemie sollten Gesundheitseinrichtungen zusehen, YubiKeys zu implementieren, um eine starke Authentifizierung zu gewährleisten, die keine Kompromisse bei der Sicherheit, Benutzerfreundlichkeit oder Skalierung erfordert.

[7] https://patientengagementhit.com/news/top-challenges-impacting-patient-access-to-healthcare

[8] https://www.fda.gov/news-events/congressional-testimony/safeguarding-pharmaceutical-supply-chains-global-economy-10302019#ftn3

yubico

Über Yubico

Yubico setzt weltweit neue Maßstäbe für den einfachen und sicheren Zugriff auf Computer, mobile Geräte, Server und Onlinekonten.

Das Kernprodukt des Unternehmens, der YubiKey, bietet per simpler Berührung effektiven hardwarebasierten Schutz für eine beliebige Zahl von IT-Systemen und Online-Diensten. Das YubiHSM, Yubicos hochportables Hardware-Sicherheitsmodul, schützt vertrauliche Daten auf Servern.

Yubico leistet einen wesentlichen Beitrag zur Entwicklung der offenen Authentifizierungsstandards FIDO2, WebAuthn und FIDO Universal 2nd Factor. Die Technologien des Unternehmens werden von 9 der 10 führenden Internet-Marken und Millionen von Nutzern in 160 Ländern genutzt und geschätzt.

Yubico wurde 2007 gegründet und ist ein Privatunternehmen mit Niederlassungen in Schweden, Großbritannien, Deutschland, den USA, Australien und Singapur. Weitere Informationen: www.yubico.com.