yubico

Die Anforderungen der Cyber-Versicherungen erhöhen die Sicherheitsstandards

Die entscheidende Bedeutung der Phishing-resistenten MFA für die Gewährleistung höchster Sicherheit

Die Evolution der Cyber-Versicherung und steigende Prämien

Als 1995 die erste Cyber-Versicherungspolice auf den Markt kam, wussten außer IT-Insidern nur wenige, welche Risiken und Kosten eine Katastrophe im digitalen Raum wirklich mit sich bringt. Heute ist das anders. Mittlerweile sind Cyber-Attacken allgegenwärtig, raffiniert, öffentlichkeitswirksam und in vielen Fällen verheerend. Es vergeht kaum eine Woche, in dem nicht ein großer Angriff für Schlagzeilen sorgt und die Erwartungen an die Cybersicherheit neu definiert. Mit dem jüngsten Aufkommen von Erpressersoftware (Ransomware) stand noch nie so viel auf dem Spiel wie heute – Cyber-kriminalität verursachte allein im Jahr 2021 Verluste in Höhe von 6 Billionen US-Dollar, bei einem Wachstum von 15 % von Jahr zu Jahr.

Die Folge war, wenig überraschend, eine gestiegene Nachfrage nach Cyber-Versicherungen. Doch ebenso wie die Unternehmen damit kämpfen, ihre IT-Anlagen vor den sich ständig wandelnden Angriffen zu schützen, haben auch Versicherungsunternehmen Schwierigkeiten, Cyber-Risiken effektiv zu versichern. Einige sehen die potenziellen Verluste als zu groß an und bieten keine Cyber-Versicherungen mehr an. Die verbleibenden Versicherer haben die Prämien in vielen Fällen um 150 bis 300 % erhöht.

Höhere Prämien gleichen das Risiko für die Anbieter von Cyber-Versicherungen zwar aus, aber nur unwesentlich. Damit Cyber-Versicherungen in einer Welt mit explodierenden Cyber-Risiken zu einem rentablen Produkt werden können, muss die Wahrscheinlichkeit erfolgreicher Angriffe drastisch sinken. Früher, 1995, als der Ausfall von Hardware das größte Risiko darstellte, konnte jede Person mit einem digitalen Impulsgeber und einer Kreditkarte eine Police abschließen. Heute müssen Unternehmen jedoch nachweisen, dass sie die Mindeststandards für Cybersicherheit einhalten und Cyberhygiene und Widerstands-fähigkeit ernst nehmen. Der Abschluss einer Versicherung (egal zu welchem Preis) ist davon abhängig. Deshalb muss jedes Unternehmen, das eine Cyber-Versicherung abschließen oder behalten will, seine eigene Sicherheitslage überprüfen und möglicherweise verbessern.

Bloße Mindestsicherheit reicht für den Abschluss einer Cyber-Versicherung nicht mehr aus

Jeder Versicherungsanbieter legt seine eigenen Bedingungen für die Gewährung von Cyber-Versicherungsschutz fest, aber die große Mehrheit erwartet, dass Versicherungsnehmer mindestens über E-Mail-Sicherheitskontrollen, Endpunkt-Erkennungs- und Reaktionstools, Virenschutz der nächsten Generation sowie Backup- und Wiederherstellungsfunktionen verfügen. So wichtig diese Punkte auch sein mögen, die Cyber-Versicherungsbranche betrachtet die Multi-Faktor-Authentifizierung (MFA) als den wichtigsten Schutzfaktor. Tatsächlich kann es sein, dass der Abschluss einer Cyber-Versicherung ohne MFA unmöglich ist.

Diese neuen und verschärften Sicherheitsanforderungen sind vollkommen gerechtfertigt. Keine andere Sicherheitskontrolle trägt mehr zur Verringerung des Risikos im digitalen Raum bei als MFA, denn sie vermindert nicht nur die mit einer sich entwickelnden Cyber-Bedrohungslandschaft verbundenen Gefahren, sondern kann auch die mit schlechtem Nutzer-verhalten und Fehlern verbundenen Risiken minimieren. Ohne MFA sind private Konten und sensible Anlagen sehr anfällig für Angriffe, unabhängig davon, welche anderen Schutzmaßnahmen vorhanden sind. Indem sie zusätzliche Authentifizierungs-ebenen verlangen, können Unternehmen Phishing- und Erpressersoftware-Angriffe stoppen, was ausreicht, um die vielen Hacker abzuschrecken, die den Weg des geringsten Widerstands suchen. Für die wenigen hartnäckigen Angreifer stellt die Überwindung von zwei oder mehr Authentifizierungsebenen ein gewaltiges Hindernis dar.

Für alle, die eine Cyber-Versicherung abschließen möchten, hat die Einrichtung von MFA in der gesamten Organisation oberste Priorität. Und während die vermeintlich schnellste, billigste oder einfachste Lösung, wie SMS oder mobile (App,-) Authentifizierung, ausreichend erscheinen mag, sehen Versicherungsanbieter dies vielleicht anders. Sie wünschen sich Unternehmen, die am besten gegen Angriffe abgesichert sind, vor allem, da die Versicherer immer risikoscheuer werden. Deshalb ist die beste Lösung für MFA diejenige, die den besten Schutz bietet, jetzt und für die Zukunft. Jede andere Lösung erhöht nur das Risiko für das Unternehmen und den Versicherungsanbieter - daher werden weniger gute Lösungen für den Abschluss oder die Aufrechterhaltung einer Cyber-Versicherung zunehmend inakzeptabel.

Phishing-resistente MFA ist wichtiger als je zuvor

Mehrfache Faktoren in der Authentifizierung sind immer sicherer als ein einzelner Faktor. Allerdings sind einige Formen der MFA deutlich unsicherer als andere. So sind zum Beispiel MFA-Produkte, die ein Einmal-Passwort (OTP) an die Telefon- oder E-Mail-Adresse einer Person senden, zwar sicherer als Passwörter an sich, aber immer noch anfällig für Phishing-Angriffe. Ein Hacker muss eine Person nur dazu bringen, sich auf einer gefälschten Website, die der echten Website gleicht, zu authentifizieren und kann dort die Benutzerdaten und MFA-Codes sammeln. Sobald Hacker diese Informationen besitzen, können sie sich ganz einfach anmelden und ihren Angriff unter dem Deckmantel eines autorisierten Benutzers fortsetzen, was die Aufdeckung so lange hinauszögern kann, bis es zu spät ist und massive Probleme auftreten.

Phishing-resistente MFA funktioniert anders. Anstatt zur Authentifizierung von Nutzer/innen etwas heranzuziehen, „was sie wissen“, wie z. B. ein Einmalpasswort (OTP), werden Nutzer/innen durch etwas authentifiziert, „das sie haben“, wie z. B. einen Sicherheitsschlüssel, den sie in den USB-Anschluss ihres

Geräts stecken. Es ist nahezu unmöglich, die Geheimnisse eines hardwarebasierten Sicherheitsschlüssels aus der Ferne zu entschlüsseln, während SMS-Codes und andere Methoden leicht durch Fern- und Man-in-the-Middle-Angriffe abgefangen werden können, wie zahlreiche aktuelle Vorfälle in den Nachrichten zeigen. Daher ist eine wirklich Phishing-resistente MFA ein Ansatz, der extrem schwer zu knacken ist, so dass Unternehmen und ihre Cyber-Versicherer beruhigt sein können, dass nur die richtigen Nutzer/innen Zugang zu sensiblen Ressourcen erhalten.

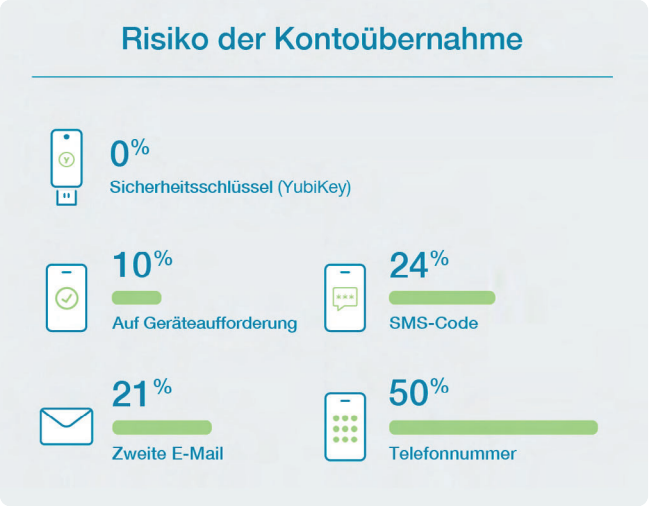
Alle US-Bundesbehörden wurden vor Kurzem verpflichtet, eine Phishing-resistente MFA einzuführen und auch für staatliche und lokale Behörden sowie für den privaten Sektor wird dies zunehmend zur Pflicht. Um wirklich Phishing-resistent zu sein, werden diese Organisationen zudem dazu angehalten, MFA auf der Grundlage von FIDO/WebAuthn oder Smart Card/PIV-Protokoll einzuführen. Alle anderen Methoden sind nicht Phishing-resistent und bleiben hinter dem akzeptablen Standard für sicherheitsbewusste Organisationen zurück. Unternehmen, die diesen modernen Sicherheitsansatz anwenden, sind erheblich weniger anfällig für erfolgreiche Cyberangriffe. Daher gehören sie nicht nur zu den bevorzugten Kandidaten für Cyber-Versicherungen bei möglicherweise niedrigeren Versicherungsprämien, sondern sie sind auch am besten gegen finanzielle, rechtliche und rufschädigende Folgen abgesichert, die keine noch so gute Versicherung beheben kann.

YubiKeys – Phishing-resistente MFA, die Ihnen eine gute Ausgangsposition für die neuen Ansprüche von Cyber-Versicherungen verschafft

Yubico ist seit über einem Jahrzehnt führend und Wegbereiter auf dem Gebiet der leistungsstarken Authentifizierung. Unser bekanntestes Produkt, der YubiKey, wird von vielen Sicherheitsexperten und Cyber-Versicherungsanbietern gleichermaßen als die beste Lösung der Branche angesehen.

> Die Rolle von Yubico in der Branche ist einzigartig. Die von Yubico heute angebotenen Lösungen repräsentieren die nächste Generation in der Identitätssicherheit. Der Rest der Welt muss zu Yubico aufschließen und nicht umgekehrt.
>
> Steve Brasen, Research Director, Enterprise Management Associates

Moderne Sicherheit: Die Zeit und umfangreiche Studien haben bewiesen, dass Phishing und andere Strategien zur Kontoübernahme mithilfe von YubiKeys bereits im Ansatz unterbunden werden. YubiKeys unterstützen auf einem einzigen Sicherheitsschlüssel mehrere Authentifizierungsprotokolle, z. B. ältere Authentifizierungsprotokolle wie OTP, aber auch moderne Sicherheitsprotokolle, die echten Phishing-Schutz bieten, wie FIDO U2F und FIDO2/WebAuthn sowie Smart Card/PIV. Durch die Unterstützung mehrerer Protokolle verbessern YubiKeys die Sicherheitslage von Organisationen unabhängig davon, wo sich diese auf ihrer Authentifizierungsreise befinden, und über eine Vielzahl von älteren lokalen und modernen Cloud-Infrastrukturen hinweg.



Forschung von Google, NYU und UCSD auf der Grundlage von 350.000 realen Hijacking-Versuchen. Die angezeigten Ergebnisse beziehen sich auf gezielte Angriffe.

Schnelle und einfache Benutzererfahrung: Die Einfachheit der YubiKeys ist ein weiteres wichtiges Alleinstellungsmerkmal. Für YubiKeys muss keine Client-Software installiert werden und sie benötigen weder Batterien noch eine Mobilfunkverbindung. Benutzer können sie einfach in einen USB-Anschluss stecken und die Taste berühren oder Tap&Go mit Nahfeldkommunikation (NFC) zur sicheren Authentifizierung nutzen. Mithilfe der Selbstbedienungsfunktionen können Unternehmen ihren Benutzern schnell und einfach die Möglichkeit geben, den eigenen YubiKey selbst einzurichten, ohne dass die IT-Abteilung eingeschaltet werden muss oder ein Besuch im Büro erforderlich ist. Phishing-resistente MFA lässt sich in wenigen Minuten einrichten und der YubiKey funktioniert mühelos auf Laptops, Tablets und Smartphones. Je nach den Anforderungen und Richtlinien des Unternehmens für den Zugriff auf bestimmte Systeme kann er sogar als Smartcard verwendet werden.

Finanzielle, rechtliche und rufschädigende Risiken verringern: Es wird erwartet, dass sich die Kosten der weltweiten Cyberkriminalität bis 2025 auf 10,5 Billionen Dollar belaufen werden, obwohl Unternehmen Hunderte von Milliarden Dollar zur Stärkung ihrer Cybersicherheit aufwenden. YubiKeys bieten Ihnen den stärksten Schutz gegen Phishing, mithilfe von speziell entwickelten Hardware-Sicherheitsschlüsseln, die Ihr Unternehmen und die Benutzer und Benutzerinnen schützen, indem sie moderne Cyber-Risiken umgehen.

Zusammenfassung:

Eine Panne im Bereich der Cybersicherheit kann katastrophale Folgen für das betroffene Unternehmen haben. Sie führt zu Ausfallzeiten und entgangenen Chancen und hat auch erhebliche Auswirkungen auf die Anbieter von Cyber-Versicherungen. Schützen Sie sich und verschaffen Sie sich die beste Ausgangsposition, indem Sie einen MFA-Ansatz in Erwägung ziehen, der sowohl den aktuellen Bedrohungen standhält als auch zukunftssicher die immer ausgefeilteren Bedrohungen bewältigen kann. YubiKeys sichern eine breite Palette von Umgebungen ab und bieten den nötigen Komfort für die Unterstützung der heutigen modernen Beschäftigten am Arbeitsplatz, in Fernarbeit oder in einem hybriden Modell. Außerdem bieten YubiKeys einen konsistenten, robusten und Phishing-resistenten MFA-Ansatz für die modernen Arbeitsweisen von Unternehmen und ihren Benutzern.

Über Yubico Als Erfinder des YubiKey macht Yubico sicheres Login mit Phishing-resistenter MFA-Technologie sehr einfach. Yubico setzt globale Standards für den plattformübergreifenden sicheren Zugang zu Anwendungen und Endgeräten und ist einer der Hauptentwickler und Mitgestalter von offenen Authentifizierungsstandards wie FIDO2 (WebAuthn) und FIDO U2F. Weitere Informationen finden Sie hier: www.yubico.com.

Yubico AB
Kungsgatan 44, 2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054
USA