yubico

abtis sichert die digitale Zukunft von Kunden mit YubiKeys

Schutz der IT-Lieferkette durch Phishing-resistente MFA

Fallstudie

[abtis]
DIGITALE ZUKUNFT

Branche
- IT-Dienste

Vorteile
- Passwortlose Authentifizierung
- Sichert die Remote-Anmeldung
- Schützt die IT-Lieferkette
- Reibungslose User Experience

Protokolle
- FIDO2

Produkte
- YubiKey 5C NFC

Informationen zur Bereitstellun
- Unternehmensweite Einführung
- Schutz von Microsoft-Lösunge

Die digitale Zukunft der Kunden gestalten und Produktivität von überall aus ermöglichen

abtis ist ein IT-Dienstleister mit Sitz in Pforzheim, der sich auf Microsoft-Lösungen spezialisiert hat. Der moderne Arbeitsplatz ist zunehmend auf Cloud-Dienste angewiesen, ein Trend, der sich während der Pandemie noch verschärft hat, da viele Mitarbeiter zur Remote-Arbeit gewechselt sind. abtis hat eine klare Mission: die digitale Zukunft seiner Kunden zu gestalten und ihren Übergang zur Digitalisierung zu ermöglichen, damit Mitarbeiter von überall aus und selbst unterwegs problemlos arbeiten können. Neue Arbeitsweisen bringen neue Herausforderungen mit sich. Dazu gehört auch die Gewissheit, dass alle in der Cloud gespeicherten Daten sicher sind. Um Risiken zu minimieren, legt abtis den Schwerpunkt auf die Aufrechterhaltung eines starken Cybersicherheitsteams und die Bereitstellung der richtigen Tools.

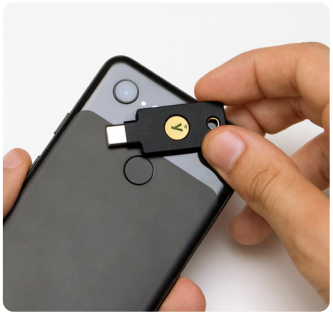
Sebastian Thum ist Senior SOC Analyst bei abtis. Er gehört zum Cyber Defense Operations Center des Unternehmens und reagiert auf Cybersicherheitsvorfälle, die bei Kunden auftreten. Das Center ist auch der erste Kontakt bei internen Cybersicherheitsproblemen. Als IT-Dienstleister mit Verantwortung für die kritische Infrastruktur seiner Kunden, bildet abtis einen Bestandteil der IT-Lieferketten dieser Kunden. Die jüngste NIS2-Richtlinie schreibt vor, dass das Risikomanagement in den kommenden Jahren durch digitale Dienstleister in der EU zunehmend reguliert wird. abtis ist dafür bereits gut vorbereitet. „Wir überwachen konstant, wo Risiken bestehen“, erklärt Thum. „Um unsere Kunden zu schützen, müssen wir auch auf unsere eigene Sicherheit achten. Wir legen größten Wert darauf, einen sehr hohen Sicherheitsstandard beizubehalten.“

Wachsender Bedarf an starker, Phishing-resistenter MFA

Als Experte für Cybersicherheit ist Thum sich der globalen Sicherheitstrends sehr bewusst. „Wenn wir über die globale Bedrohungslage sprechen“, so Thum, „müssen wir zwangsläufig auch das Thema Zero Trust einbeziehen. Es gibt nun drei wichtige Aspekte, über die man Bescheid wissen sollte. Erstens: die Identität. Diese können wir am effektivsten mit einem zweiten Authentifizierungsfaktor schützen. Zweitens müssen wir auch auf die Geräte achten, die wir verwenden, egal ob wir zu Hause, im Zug oder anderswo arbeiten. Zu guter Letzt haben wir natürlich die Daten. Dank Cloud-Systemen können wir von überall aus auf unsere Daten zugreifen, und daher müssen wir diese Daten angemessen schützen. Genau das sind die Ziele von Angreifern: Sie wollen Identitäten übernehmen, auf Geräte zugreifen und Unternehmensressourcen in Form von Daten abgreifen.“

Sebastian Thum
Senior SOC Analyst, abtis

> “Wie die meisten Menschen heutzutage wissen, sind weder Telefonanrufe noch SMS-Nachrichten sicher. Wir mussten eine Alternative finden, die uns wirklich verlässliche Sicherheit bietet – und so kamen wir auf YubiKeys.“
>
> Sebastian Thum, Senior SOC Analyst bei abtis



> YubiKeys sind einfach zu bedienen, zuverlässig, robust und gehen nicht kaputt."
>
> Sebastian Thum
> Senior SOC Analyst bei abtis

Das Herzstück einer erfolgreichen Zero-Trust-Strategie ist eine starke Authentifizierung. Wichtig ist, dass diese nicht von Hackern umgangen werden kann und einen starken Schutz vor Phishing und anderen Methoden des Diebstahls von Zugangsdaten bietet. Bei der Arbeit mit Microsoft-Produkten muss abtis schon lange eine Multi-Faktor-Authentifizierung (MFA) verwenden, doch das Bewusstsein nahm zu, dass nicht alle MFA gleich effektiv sind. „Um ein Höchstmaß an Sicherheit zu gewährleisten, stellen wir sicher, dass wir die besten verfügbaren Produkte verwenden und die neuesten Entwicklungen stets im Blick behalten. Wir müssen immer auf dem aktuellen Stand der Technik sein. Bis vor kurzem haben wir die App Microsoft Authenticator, Telefonanrufe und SMS-Nachrichten genutzt. Es reicht nicht, einfach nur einen zweiten Faktor zu verwenden, sondern wir benötigen auch einen weiteren, der als Backup dient. Da Telefonanrufe und SMS-Nachrichten, wie die meisten Menschen inzwischen wissen, nicht sicher sind, mussten wir eine Alternative finden, die uns wirklich verlässliche Sicherheit bietet."

YubiKeys setzen neue Maßstäbe für Sicherheit bei der mobilen Authentifizierung

Bei dieser Suche stieß abtis zum ersten Mal auf YubiKeys, die Sicherheitsschlüssel von Yubico, welche auf Basis moderner Authentifizierung mehrere Protokolle unterstützen, eine Phishing-resistente MFA bieten und Kontoübernahmen verhindern. „Der größte Vorteil der YubiKeys und der Lösungen von Yubico insgesamt", so Thum, „besteht in ihrer Einfachheit. Es ist nicht schwierig, einen YubiKey anzuschließen oder anzutippen. YubiKeys sind einfach zu bedienen, zuverlässig, robust und gehen nicht kaputt. Hinzu kommt, dass viele Mitarbeiter ihre privaten Handys nicht für die Authentifizierung nutzen möchten, insbesondere wenn dies bedeutet, dass eine App installiert werden muss. Außerdem besitzt nicht jeder Mitarbeiter ein Arbeitshandy. Dies ist oft ein entscheidender Punkt für abtis-Kunden, die die Sicherheit erhöhen möchten, ohne neue Handys für ihr gesamtes Unternehmen bereitstellen zu müssen. Schließlich ist ein iPhone 14 erheblich teurer als ein YubiKey. Der Preis ist also ein gewaltiger Vorteil.

abtis hat YubiKey 5 NFCs erworben, sodass Mitarbeiter sich entweder über USB-C-Anschlüsse oder über NFC (kontaktlos) auf ihren Smartphones authentifizieren können. Die YubiKeys werden für die passwortlose FIDO-2-Authentifizierung für Computeranmeldung und SSO unter Einsatz von Microsoft Azure Active Directory mit bedingtem Zugriff verwendet. Mitarbeiter haben auch die Möglichkeit, die YubiKeys als zweiten Authentifizierungsfaktor für andere Online-Dienste, einschließlich PayPal, zu verwenden. „Mitarbeiter nutzen den YubiKey in verschiedenen Szenarien", so Thum, „einschließlich zur Remote-Arbeit und auf mobilen Geräten. Wir haben es unternehmensweit allen unseren Mitarbeitern zur Verfügung gestellt."

Schnelle und erfolgreiche Bereitstellung der Hardware für die Multi-Faktor-Authentifizierung

Die Bereitstellung der YubiKeys für alle Mitarbeiter von abtis dauerte nur zwei Monate. Die YubiKeys wurden entweder per Post versandt oder vor Ort in den Büros verteilt, zusammen mit einer Schritt-für-Schritt-Anleitung zur Einrichtung der Schlüssel. Es wurde ein Datum festgelegt, zu dem alle SMS- und Telefonauthentifizierungen abgestellt wurden. Die YubiKeys mussten gleichzeitig bis zu diesem Datum eingesetzt werden, da andernfalls der Zugriff auf Konten erloschen wäre. abtis hat nicht nur seine eigenen Mitarbeiter ausgestattet – das Unternehmen ermutigte auch seine Kunden, YubiKeys zu verwenden. „Nachdem wir die YubiKeys seit mehr als einem Jahr selbst nutzen, können wir mit Fug und Recht behaupten, dass die Einführung ein voller Erfolg war", meint Thum. „Außerdem feiern wir bereits Erfolge bei Projekten, für die wir unseren Kunden YubiKeys zur Verfügung gestellt haben. Es gibt immer mehr Kunden, die diese Lösung aktiv nutzen, und man sieht immer mehr Anwendungsfälle. Am besten an der Lösung gefällt mir, dass Kunden auch ihre VPN-Lösungen mit YubiKeys schützen können. Das bietet Kunden natürlich einen großen Mehrwert.

> Der größte Vorteil der YubiKeys besteht darin, dass wir da jetzt eine Phishing-resistente MFA-Lösung haben und somit nochmal einen zusätzlichen Schutz für unsere Mitarbeiter. Es ist auch ein Kostenfaktor: Wir konnten dadurch viel Geld sparen.
>
> Sebastian Thum
> Senior SOC Analyst
> Abtis

abtis schränkt die Nutzung der YubiKeys durch die Mitarbeiter nicht ein. „Der YubiKey ist in unserem Unternehmen allgemein sehr anerkannt, und die Leute arbeiten gern damit. Wir ermutigen unsere Mitarbeiter offen, den YubiKey auch im privaten Umfeld zu nutzen“, so Thum. „Das setzen unsere Mitarbeiter auch aktiv um. Das Schöne sind die vielen Profile, die man hat. Ich kann ihn für die Arbeit verwenden, doch gleichzeitig kann ich auch persönliche Konten auf demselben YubiKey speichern. Das kommt unseren Mitarbeitern sehr zugute.“

Phishing-resistente MFA verringert das Risiko von Cyberbedrohungen erheblich

Thum ist sicher, dass die Bereitstellung von YubiKeys Cyberangriffe verhindert hat:

> Wir hören immer wieder, dass Angreifer an der Multi-Faktor-Authentifizierung vorbeikommen, weil ein unachtsamer Mitarbeiter einen Anruf entgegengenommen hat oder in der Authentifizierungs-App auf „Bestätigen“ getippt hat. Dieses Problem gibt es mit dem YubiKey nicht.
>
> Sebastian Thum, Senior SOC Analyst bei abtis

Dadurch haben abtis und seine Kunden das Sicherheitsniveau für ihre Systeme und Daten erhöht. „Man kann sagen, dass die YubiKeys unsere Sicherheit verbessert haben“, meint Thum. „Der größte Vorteil besteht darin, dass wir da jetzt eine Phishing-resistente MFA-Lösung haben und somit nochmal einen zusätzlichen Schutz für unsere Mitarbeiter. Es ist auch ein Kostenfaktor: Wir konnten viel Geld dadurch sparen, was wir auch unseren Kunden immer wieder nahelegen.

„MFA ist inzwischen keine Frage mehr – es ist unumgänglich“, so Thum. Man sollte nicht mehr überlegen, sondern es einfach umsetzen. Früher pflegte man zu sagen: „Kein Backup, selbst schuld“. Heute kann man sagen: „Keine MFA, selbst schuld“. Sie sollten eine Phishing-resistente MFA für jegliche geschäftlichen und privaten Systeme verwenden, für die es möglich ist. Mein Rat an alle ist, keine Authentifizierung mehr per Anruf oder SMS-Nachricht durchzuführen. Die Authentifizierungs-App ist zwar sicher, doch mit dem YubiKey können Sie sogar Geld sparen und benötigen keine Arbeitshandys.“