Zugriffskontrolle ist nur der Anfang

_Durch KI generiertes Bild. Prompts: Riesenauge, das aus einem Baum vor einem Bürogebäude herauswächst, städtische Umgebung, digitale Kunst.

Fachartikel

_Marc Bütikofer, Head of Innovation Security Solutions, Airlock
_Michael Doujak, Product Manager, Airlock
Ergon Informatik

Erschienen im SMART insights 2023 Magazin

ergon smart people – smart software®

Klassische Zugangskontrolle reicht im Online-Business nicht mehr aus. Erst Continuous Adaptive Trust schafft die Flexibilität, die Unternehmen heute benötigen: entweder, um die IT-Sicherheit zu erhöhen oder um die User Experience zu verbessern.

Wer Zugriff auf ein Digitalangebot bekommen möchte, muss sich authentisieren. Passwörter sind ein wichtiges Element jeder IT-Sicherheitsinfrastruktur. Doch ein Passwort allein ist nicht mehr sicher genug. Deshalb haben sich Multifaktor-Authentifizierung (MFA) und Passkeys als Standard etabliert. Das Smartphone begünstigt diesen Ansatz. Es ist jederzeit griffbereit und ermöglicht eine nutzerfreundliche MFA. Das Problem: Hacker verwenden immer häufiger Methoden, die erst dann greifen, wenn User die MFA-Hürde erfolgreich überwunden haben.

Einmalige Zugriffsberechtigung reicht nicht mehr aus

Die risikobasierte Authentifizierung ist eine Antwort darauf. Sie hält Anmeldevorgänge sicher und bietet möglichst hohe Benutzerfreundlichkeit. Anhand von verschiedenen Signalen wird beurteilt, ob ein Authentifizierungsversuch plausibel ist. Solche Signale können der IP-Adressbereich oder der Ort sein, an dem der Zugriff erfolgt ist. Die risikobasierte Authentifizierung greift jedoch nur während des Log-ins. Sie schützt nicht vor Attacken während einer laufenden Online-Session. Sie bietet keinen ausreichenden Schutz vor Man-in-the-Middle-Angriffen, bei denen sich ein Hacker unbemerkt in die Kommunikation zwischen zwei oder mehreren Partnern einschleicht. Dem entgegenwirken kann Continuous Adaptive Trust (CAT), wie Gartner das Prinzip nennt. Die Risikoanalyse erfolgt nicht nur während des Log-ins, sondern kontinuierlich. Hierbei kann künstliche Intelligenz helfen. Maschinelles Lernen eignet sich gut, um Anomalien im Verhalten einer laufenden Session zu erkennen.

Die Schutzvorkehrungen und Legitimationen beim Online-Zugriff lassen sich mit dem Strassenverkehr vergleichen: Um ein Fahrzeug zu lenken, braucht es einen Führerausweis. Beim Online-Zugriff ist es die Authentifizierung mittels Passwort. Für Lastwagen ist eine zusätzliche Prüfung erforderlich.

«Continuous Adaptive Trust ist ein Paradigmenwechsel in der IT-Sicherheit.»
_Marc Bütikofer, Head of Innovation Security Solutions, Airlock

«Multifaktor-Authentifizierung allein genügt heute nicht mehr.»
_Michael Doujak, Product Manager, Airlock

Ähnlich wie bei der MFA. Ab 75 Jahren ist alle zwei Jahre eine medizinische Untersuchung obligatorisch. Das kommt der risikobasierten Authentifizierung gleich. Trotz aller Massnahmen überwachen Ordnungsbehörden die Verkehrssicherheit kontinuierlich. Etwa durch Geschwindigkeitskontrollen. Bei Online-Zugängen übernimmt CAT diese Rolle.

Vertrauensniveau wird permanent überprüft
CAT prüft nicht nur die Legitimation von Usern im Rahmen des Identity- und Access-Managements, sondern bewertet immer wieder die Signale der Risikosensoren: Ändern sich der Browser oder die IP-Adresse? Verändern sich die typischen Mausbewegungen oder Tastatureingaben? Als Risikosensoren eignen sich bestehende Komponenten, wie Security-Gateways, besonders gut. Sie überwachen den gesamten Austausch zwischen User und Applikation.

CAT prüft laufend, ob das einmal erteilte Vertrauen weiterhin gerechtfertigt ist. Der Vorteil: Sicherheit und User Experience stehen in Einklang. Die IT-Security kämpft immer wieder mit dem Problem, dass ein Mehr an Sicherheitsmassnahmen häufig ein Weniger an Benutzerfreundlichkeit nach sich zieht. Ein prominentes Beispiel für diesen Balanceakt war die mangelnde Akzeptanz der SuisseID, die 2019 eingestellt wurde. Nicht zu verwechseln mit der Nachfolgerin, der heutigen SwissID. Problematisch bei der SuisseID war unter anderem der komplexe Registrierungsprozess: Passkopien, persönliches Erscheinen, Auszug aus dem Handelsregister, Unterschriften, technisch anspruchsvolle Nutzung am Computer mit Lesegerät und Treiber. Die Nutzung der SwissID ist weniger umständlich und ein Smartphone reicht aus.

CAT sorgt für bessere Sicherheit ohne Kompromisse bei der Benutzerfreundlichkeit. Ist das Risikoniveau hoch, ist eine erneute Authentifizierung nötig. Ist es gering, kann ein Unternehmen auf eine erneute Authentifizierung verzichten und damit die User Experience verbessern. Entscheidend ist, die richtige Balance zu finden.

Ein vermeidbarer IT-Sicherheitsvorfall
Wie fehlende Balance zu einem Sicherheitsproblem führen kann, verdeutlicht folgender Fall: Bei einem Schweizer Unternehmen war ein Angreifer in der Lage, die laufende Online-Session eines Users zu übernehmen. In der Session konnte die unbefugte Person ein neues Mobiltelefon für eine Zwei-Faktor-Authentifizierung hinterlegen. Eine zusätzliche Validierung fand nicht statt. Von da an galt sie automatisch als voll authentisiert. Sie konnte anschliessend das Passwort des gekaperten Accounts zurücksetzen und erlangte die vollständige Kontrolle. Zwar gab es weitere Sicherheitsmassnahmen, etwa ein System zur automatischen Betrugsprävention. Doch der Angreifer konnte dank des übernommenen Accounts die Kontrollen problemlos meistern, die das System auslöste. Mit CAT hätte dieser Angriff höchstwahrscheinlich verhindert werden können. Denn man hätte gleichzeitig alle Risikosensoren täuschen müssen.

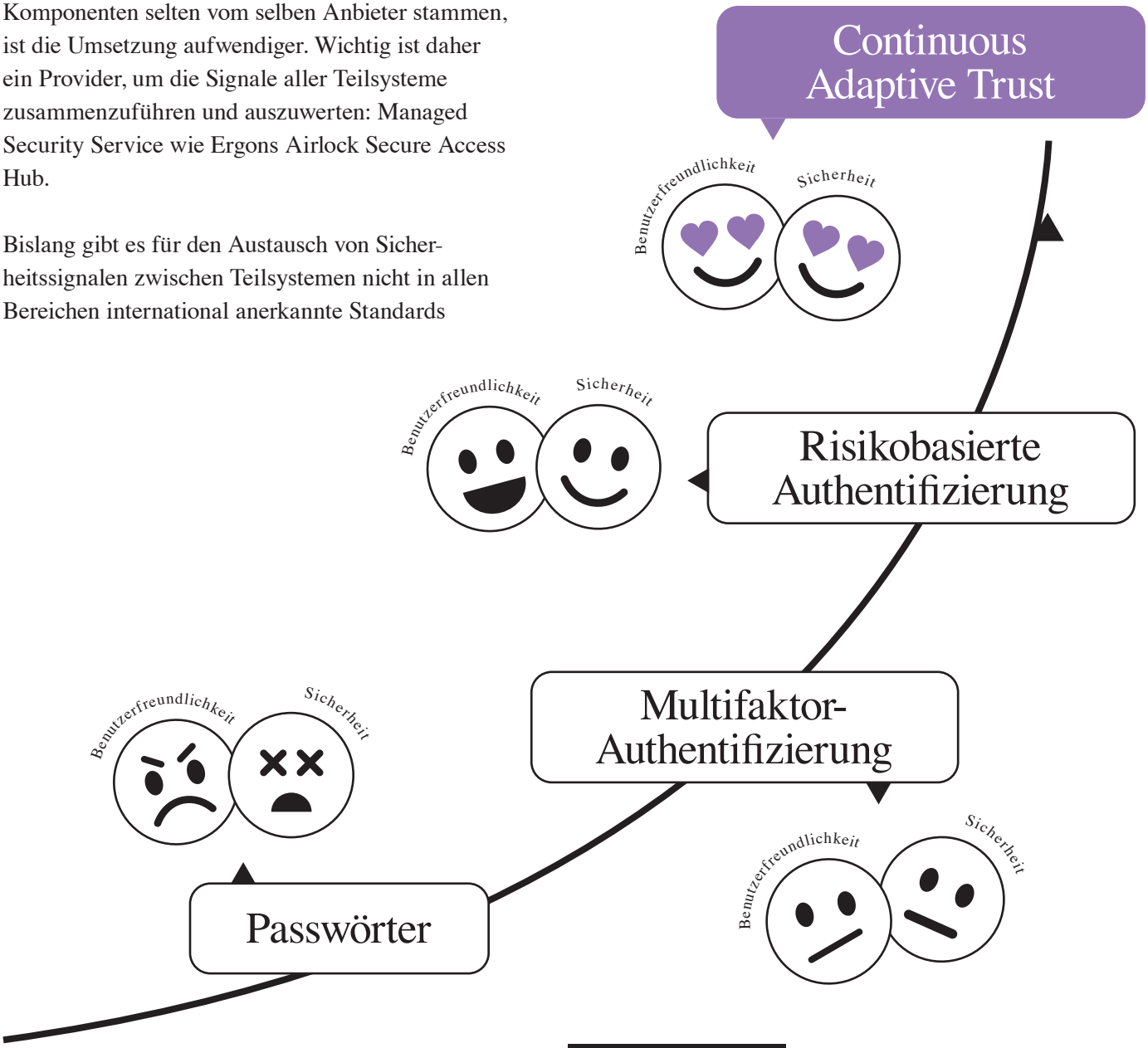
Single Sign-on macht CAT notwendiger
Besonders relevant wird CAT durch das häufig anzutreffende Prinzip «Single Sign-on». Für User ist es bequem. Sie müssen sich bei unterstützten Online-Zugängen nur einmal authentisieren, um auf verschiedene Konten zuzugreifen. Die Bestätigung der Identität und die Erteilung der Rechte erfolgen dauerhaft. CAT überprüft hingegen immer wieder, ob das Vertrauen in den User noch angemessen ist.

CAT ergänzt das Zero-Trust-Modell optimal. Bei diesem Modell gilt die Annahme, dass nichts sicher ist. Somit wird standardmässig keinem Benutzer vertraut. Es gibt einen eher starren Rahmen vor, bei dem jeder Service direkt an seinen Schnittstellen kontrolliert, ob ein Zugriff erlaubt ist. Zero Trust sorgt für viele kleine Trutzburgen, die eine Art Verteidigungswall nach aussen und innen bilden. CAT sorgt dafür, dass Kontrollen kontinuierlich erfolgen. Solange, bis eine Session dauerhaft endet.

Mehr Security oder bessere User Experience?
Bevor sich ein Unternehmen für CAT entscheidet, sollte es festlegen, ob es dadurch mehr Sicherheit

oder eine bessere User Experience erreichen will. In der technischen Umsetzung erfordert CAT die Integration von verschiedenen Komponenten. Web-Application und API-Protection (WAAP) sind notwendig, um Risikosignale zu messen. Die Anpassung des Vertrauensniveaus realisiert ein Identitäts- und Zugriffsmanagement. Da diese Komponenten selten vom selben Anbieter stammen, ist die Umsetzung aufwendiger. Wichtig ist daher ein Provider, um die Signale aller Teilsysteme zusammenzuführen und auszuwerten: Managed Security Service wie Ergons Airlock Secure Access Hub.

Bislang gibt es für den Austausch von Sicherheitssignalen zwischen Teilsystemen nicht in allen Bereichen international anerkannte Standards – oder wenigstens Quasistandards. Deshalb steckt der grösste Aufwand bei CAT in der Einführung: Alle Systeme müssen aufgesetzt, konfiguriert und die Policies neu definiert werden. Das Resultat kann sich sehen lassen: CAT wird zum Wettbewerbsvorteil. />



_Evolution der Authentifizierung