Multimodale biometrische Erkennung

Sicherheit durch Kombination

Die Authentifizierung mit Usernamen und Passwort ist anfällig. Soll die digitale Transformation erfolgreich sein, braucht man jedoch neue und vor allem sichere Methoden, um die digitale Identität zu schützen. Die Lösung ist eine Kombination von verschiedenen Authentifizierungsverfahren.

Von Miki Mitric, NEVIS

Es mag eines der frühesten Beispiele multimodaler Authentifizierung sein, das Homer am Ende der Odyssee verwendet: Der Titelheld, nach 20 Jahren heimgekehrt, wird von seiner Frau Penelope auf zwei Arten geprüft, bevor sie glauben will, dass er ihr verschollener Gatte ist: Wenn er stark genug ist, seinen mächtigen Bogen zu spannen und wenn er weiß, warum das eheliche Bett unverrückbar um einen Baum herum gebaut ist. Von den drei Faktoren der Authentifizierung werden hier zwei angewandt: „etwas, das man ist“ und „etwas, das man weiß“. Die Sage zeigt ein Problem auf, das auch in der biometrischen Authentifizierung von Bedeutung ist: Wie erkennt man einen Menschen, der sich naturgemäß jeden Tag ein wenig verändert? Die Lösung liegt in der multimodalen Erkennung.

Was ist das digitale Ich wert?

Je mehr Bereiche des Lebens die digitale Transformation berührt, desto häufiger kann das physische Ich durch eine digitale Identität ersetzt werden. War früher für eine Überweisung der Gang zur Bank nötig, so geschieht das heute per Onlinebanking orts- und zeitunabhängig. Wer die Log-in- und TAN-Daten sowie das Endgerät besitzt, kann an unserer Stelle über unser Geld verfügen.

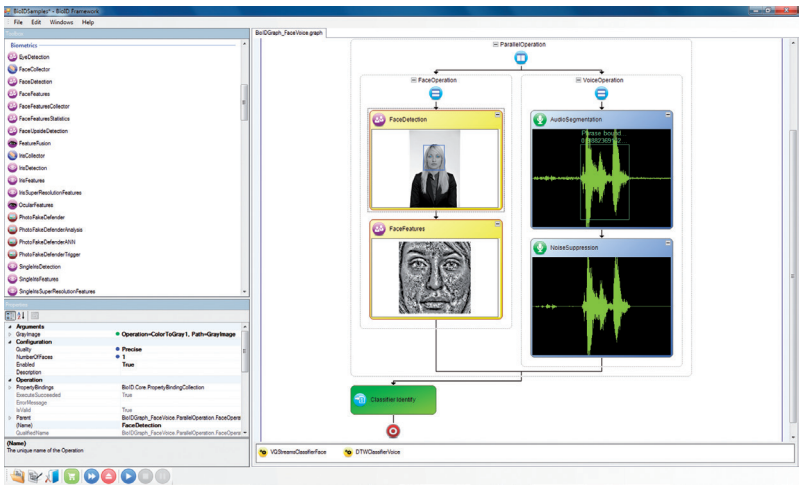
Die herkömmliche Kombination von Usernamen und Passwort ist anfällig: Einfache Passwörter mit langer Lebensdauer erhöhen die Gefahr, dass sie bereits ausgespäht wurden. Komplizierte Passwörter, die häufig geändert werden müssen, überfordern den Anwender. Laut einer Studie des Ponemon Instituts fordert jeder dritte User heute einmal im Monat ein vergessenes Passwort an.

Soll die digitale Transformation – und mit ihr das Internet of Things (IoT) – ein Erfolg werden, braucht man neue Methoden, um die digitale Identität zu schützen.

Qualitäten des virtuellen Butlers

Wie muss ein System gestaltet sein, das die Aspekte der Sicherheit mit der Nutzerfreundlichkeit ideal kombiniert? Die Antwort ist nicht, eine Art der Authentifizierung, wie Usernamen und Passwort, durch eine andere zu ersetzen. Weder ein Iris- oder Venenscan noch die Stimmerkennung oder eine andere Methode lösen allein die Herausforderung. Vielmehr muss ein ausgefeiltes System die Identität des Anwenders verifizieren. Dieses System ist die Grundlage für eine Kombination von verschiedenen Authentifizierungsverfahren.

Dazu müssen spezialisierte Partner zusammenarbeiten, um Best-of-Breed-Komponenten der Authentifizierung zu einem zuverlässigen Assistenten zu vereinen. Der Assistent kennt die Person, ihre Vorlieben und Gewohnheiten und die ihres Arbeitgebers. Dieser digitale Butler, wie ihn etwa das Partner-



Kombinierte Gesichts- und Stimmerkennung. Bild: BioID

Ecosystem von NEVIS bietet, muss eine Reihe von Eigenschaften aufweisen:

_____ Lernfähigkeit: Zu Beginn seines Dienstes muss er den Anwender in allen relevanten Dimensionen kennenlernen. Personen- und Kontaktdaten, die Geräte, Dienste und Plattformen, die er nutzt, aber auch die nötigen biometrischen Daten wie Aussehen und Tippmuster, Stimme, Venen- oder Irismuster. Ferner darf das System auf dem gelernten Stand nicht stehen bleiben. Der digitale Butler muss sein Erkennungsmuster regelmäßig aktualisieren.

_____ Anpassungsfähigkeit und Intelligenz: Nicht jeder Anlass erfordert das gleiche Maß an Sicherheit. Der digitale Butler sollte den „Level of Assurance", also das geforderte Niveau der Authentifizierung, entsprechend wählen. Genauso anpassungsfähig sollte er auch bei Abweichungen von den gespeicherten Authentifizierungsmustern sein. Schlägt die Stimmerkennung aufgrund einer Erkältung fehl, ist das kein Grund für einen Alarm. Versucht sich aber jemand mit einem unbekannten Endgerät zu ungewohnter Uhrzeit von einem weit entfernten Ort einzuloggen, ist ein Versagen der Stimmerkennung durchaus ein Grund, weitere Beweise der Identität einzufordern.

_____ Wachsamkeit und schnelle Reaktion: Je mehr Merkmale bei einer versuchten Authentifizierung von den bekannten Mustern abweichen, desto misstrauischer wird der digitale Butler und desto strengere Kriterien sollte er anlegen. Erreicht der „Risk Score" ein bestimmtes Maß, sollte das System sofort überprüfen, ob hinter der beobachteten Unregelmäßigkeit ein Betrugsversuch steckt und den Zugriff gegebenenfalls verhindern.

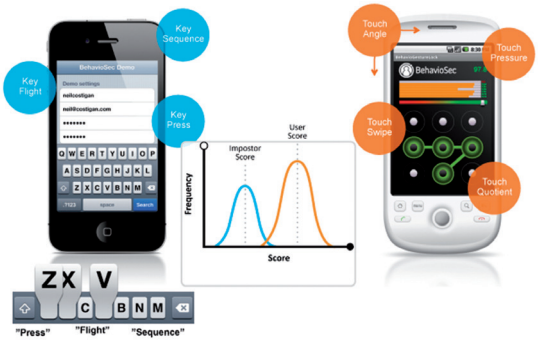
_____ Bequeme Anwendung: Sicherheitsmaßnahmen, die für den Anwender aufwändig sind, verleiten ihn dazu, sie zu umgehen. Viele biometrische Verfahren wie die Gesichtserkennung oder die Analyse des Tippverhaltens erfordern nur eine geringe Beteiligung des Menschen und eignen sich deshalb gut zur alltäglichen Authentifizierung.

_____ Vertrauenswürdigkeit bei Datenschutz und Transparenz: Weil die digitale Identität so wichtig ist, muss der Anwender wissen, ob und wann sie angewendet wird und zu welchem Zweck. Ebenso müssen die verwendeten Daten ihrerseits sicher und der Zugriff darauf muss klar geregelt und transparent sein.

Diese Kombination aus kontextbasierter, mehrmodaler Authentifizierung, der intelligenten Erkennung von Abweichungen und der Reaktion darauf, bieten Plattformen wie die NEVIS Security Suite des Schweizer Software-Hauses AdNovum. In der Schweiz schützt sie bereits 80 Prozent aller Onlinebanking-Transaktionen. Die Security-Suite vereint die Best-of-Breed-Expertise von Technologiepartnern wie BioID oder Behaviosec. Dabei sind die Partner Spezialisten in einzelnen biometrischen Disziplinen:

_____ Die Gesichtserkennungs-Lösung der Firma BioID setzt die Kamera des Smartphones ein, um Banking-Transaktionen abzusichern. Dieser zusätzliche Aufwand ist für den Anwender kaum höher als eine TAN-Eingabe und macht ihn auf sehr natürliche Art und Weise eindeutig identifizierbar. Die patentierte Lebenderkennung schützt zusätzlich gegen Manipulationen mit Fotos oder Videos. Wichtig ist dabei, dass nicht ein komplettes Bild des Anwenders zu seiner Authentifizierung gespeichert wird, sondern ein „Template". Das ist eine bereinigte und reduzierte Datendarstellung biometrischer Merkmale. Dieser Vorgang ist nicht umkehrbar. Aus dem Template kann kein Bild des Menschen errechnet werden.

_____ Auch das Verhalten einer Person macht ihn eindeutig erkennbar und kann als eine zusätzliche Sicherheitsebene verwendet werden. Je nachdem, welches Gerät eingesetzt wird, erfasst und analysiert die Technologie von Behaviosec die Dynamik von Tastatur-Eingaben, Maus-Bewegungen, Touch-Gesten oder wie etwa ein Smartphone gehalten wird. Diese Verhaltensweisen sind bei jedem Nutzer einzigartig. Ohne zusätzlichen Aufwand ist die Lösung für den Nutzer transparent und erhöht die Sicherheit signifikant: Username und Passwort funktionieren nicht nur wie gewohnt als simpler Schutzmechanismus. Die Art und Weise, wie der autorisierte Inhaber sie eingibt, stellt seine Identität sicher.



Analyse des Tippverhaltens anhand von Werten wie Anschlagdruck und Geschwindigkeit.

Fazit

Der digitale Butler wird als Begleiter und Garant unserer digitalen Identität ein zentrales Element werden. Er setzt – anders als herkömmliche Systeme mit starren Mechanismen – bei der Authentifizierung auf intelligente, kontextinformierte Methoden.

Schon Penelope hat ihren Gatten durch eine multimodale Authentifizierung herausgefordert, sich als derjenige auszuweisen, der er vorgibt, zu sein. Auch nach 2.700 Jahren müssen wir sicher sein, dass wir als User zuverlässig erkannt werden und der Zugang zu unserem digitalen Ich nicht von Fremden missbraucht wird. ■