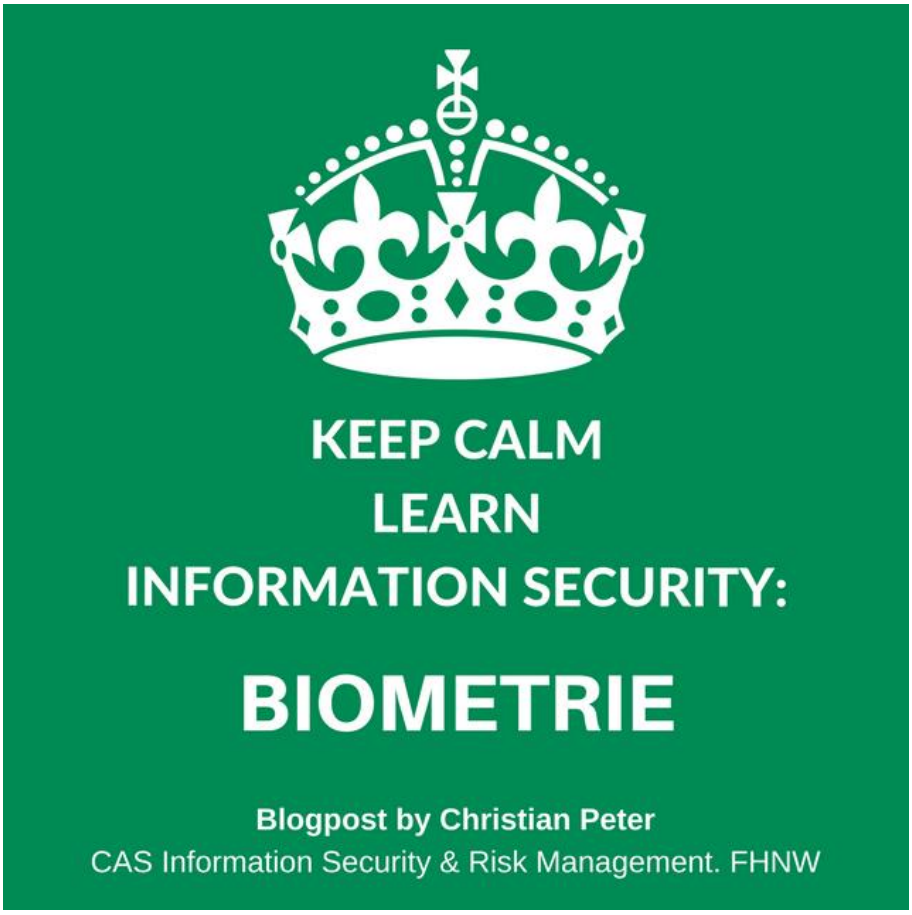
Wirtschaftsinformatik reloaded.
Neues aus dem IWI der Hochschule für Wirtschaft FHNW

CAS Information Security & Risk Management 2017: Taugt die Biometrie als Türöffner?

Posted on 5. Dezember 2017 by danielhertig



Back-to-School: Aus dem Klassenzimmer des CAS Information Security & Risk Management. Basis für diesen Lehrgang ist das BSI-Grundschutzhandbuch, und die Teilnehmenden bereiten sich begleitend auf die CISSP-Prüfung vor. Somit ist es ein Teil des 15-tägigen Lehrgangs, ein CISSP- oder BSI-Fachthema als Blogpost aufzubereiten:

Information Security: Taugt die Biometrie als Türöffner?

Das Handy mit dem Fingerabdruck oder per Gesichtserkennung entriegeln, die Haustüre mit dem Venenscanner öffnen, sich mit anderen biometrischen Daten (Stimm- und Sprecherkennung, Irismuster, Gang oder dem Rhythmus einer Tastenkombination) authentifizieren, ist schon seit längerem nicht nur James Bond oder anderen Superhelden oder Bösewichten beim Zutritt zu ihren Geheimbasen vorbehalten.

Die Verifizierung geht in der Regel schneller und bequemer als viele Alternativen (Iris- und Retina-Erkennung mal ausgenommen). Biometrische Merkmale sind vermeintlich einzigartig und untrennbar mit ihrem Träger verknüpft. Anders als Passwörter oder Hardware-Token können sie nicht vergessen, verloren oder verlegt werden. Die Biometrie gilt als innovative Methode zur Authentifizierung und hat noch immer einen gewissen futuristischen Touch.

Auch die Anbieter von Biometrie-Lösungen freuen sich. Das weltweite Marktvolumen für Biometrie-Lösungen wird auf aktuell fünf Milliarden US-Dollar geschätzt. Bis 2020 soll es auf 33 Milliarden US-Dollar ansteigen.

Positiv ins Feld geführt wird der Umstand, dass biometrische Daten im Gegensatz zu vielen anderen Authentifizierungsmassnahmen vermeintlich unauflöslich mit einer konkreten Person verbunden sind, nicht verloren gehen und eine lange Gültigkeit haben. Bei den biometrischen Verfahren lassen sich die physiologischen (körperliche Eigenheiten) von den verhaltensbezogenen (typische Verhaltensweisen und Aktionen) unterscheiden. Hauptqualitätsmerkmal der biometrischen Erkennung ist, dass ein Merkmal eindeutig mit einer Person verknüpft ist. Die Authentifizierung erfolgt über den Vergleich der Daten der biometrisch erfassten Person mit vorhandenen und zuvor hinterlegten Referenzdaten. Bei Übereinstimmung ist die Person verifiziert und der Zugang öffnet sich. So einfach ist es. Daher ist die Biometrie auch sehr beliebt. Zweidrittel der Europäer wünschen sich die Biometrie als Authentifikation für ihre Geldzahlung (zusammen mit einer Karte).

Ist dieses Vertrauen berechtigt?

Der Chaos Computer Club kopierte 2008 den Fingerabdruck von Wolfgang Schäuble, 2014 denjenigen von Ursula von der Leyen. Auch veröffentlichte er eine Iris-Attrappe von Kanzlerin Angela Merkel. Hochauflösende Kameras und 3D-Drucker machen es möglich. Auch über die Reaktivierung von Fettrückständen auf einem Fingerabdruck-Scanner – so genannten Latenzbildern – gelang es bereits Fingerabdrücke zu duplizieren.

Selbst beim Venenscanner wurde 2014 gezeigt, dass sich dieser anhand eines einfachen Ausdrucks der Aufnahme eines Venenscanners täuschen lässt. Auch die komplexesten Verfahren der Stimmenerkennung können mittlerweile überlistet werden. Ende letzten Jahres stellte Adobe ein Programm vor, das Wörter in einzelne Laute zerlegt und auf Basis von lediglich zwanzig Minuten Tonaufnahme jede Stimme täuschend echt imitiert. Das gesprochene Wort könnte dank dieser innovativen Technik als biometrisches Merkmal jede Relevanz verlieren.

Zudem muss die Fehlerquote im Auge behalten werden. Eine Genauigkeit von 98 Prozent klingt nur für Laien gut. Betreten jedoch 10.000 Mitarbeitende eines grossen Unternehmens tagtäglich das Firmengelände und authentifizieren sich biometrisch, scheitern jeden Tag 200 Personen an der Zugangskontrolle und starten ihre Arbeit verspätet. Es gibt bei diesem Authentifizierungsverfahren sowohl das Problem der Falschzurückweisungsrate (FRR, 2% beim Fingerabdruck, 7% bei der Stimmerkennung, 0,4% bei der Gesichtserkennung, nach 1,5 Jahren jedoch bereits 43%), bei welcher der valide Benutzer nicht erkannt wird, als auch das Problem der Falschakzeptanzrate (FAR, 0,7% beim Fingerabdruck, 1% bei der Stimmerkennung, 2% bei der Gesichtserkennung), bei welcher ein unberechtigter Benutzer autorisiert wird. Da beide Werte miteinander korrelieren, bedeutet dies, je kleiner die FAR wird, desto höher wird die FRR.

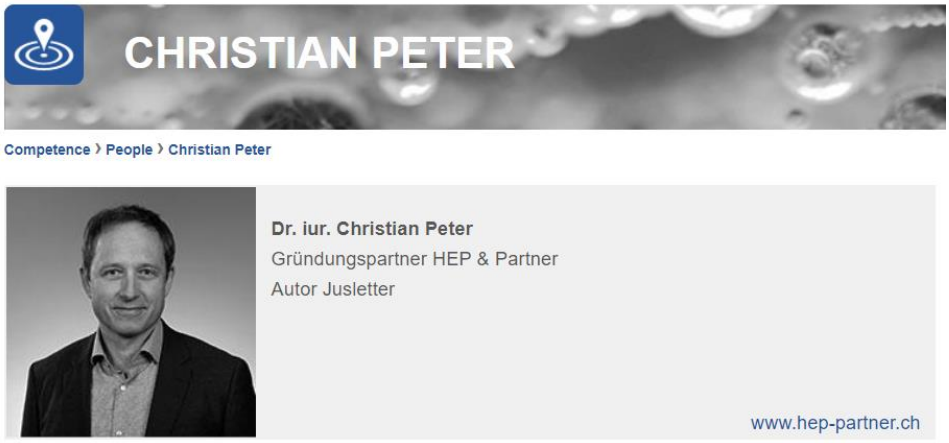
Auch können äussere Umstände wie Verschmutzung beim Scan, schlechte Belichtung bei der Gesichtserkennung, äussere Verletzungen an der Hand, Krankheiten oder aber auch nur eine Brille störend wirken und die Authentifizierung verhindern.

Dass biometrische Merkmale fest mit ihrem Träger verknüpft sind, ist zudem nicht nur positiv. Der vermeintliche Vorteil kann schnell zum Nachteil werden – nämlich dann, wenn ein Merkmal erfolgreich kopiert wurde. Anders als ein Passwort lassen sich ein gestohlener Fingerabdruck, Blutgefässmuster, die Netzhaut oder die EKG-Muster nicht „zurücksetzen“ oder ändern. Man stelle sich die Konsequenzen vor, wenn ein biometrisches Merkmal in die Hände Krimineller gelangt und im Dark Web zum Kauf angeboten wird.

Zudem ist zu bedenken, dass es auch Anwender gibt, denen es an Vertrauen mangelt und die nicht möchten, dass ihr Fingerabdruck, den sie als sehr persönlich empfinden, in den Datenbanken grosser Konzerne bereitliegen? Sollen diese gezwungen werden, die oben genannten Schwachpunkte der Biometrie zu akzeptieren und den Eingriff zu erdulden oder auf den Dienst oder den Zugang zur Arbeitsstelle verzichten? Solange die oben genannten Probleme nicht gelöst sind, wird man parallel zur Biometrie noch andere Lösungen anbieten müssen.

Für das Öffnen von Garagen oder Wohnungen oder zum Entsperren von privaten Smartphones mag der Biometrie die Zukunft gehören. Für alle anderen Bereiche gehört sie den intelligenten, mehrstufigen Sicherheitskonzepten, die sich die Vorteile verschiedener Philosophien zunutze machen. Aber auch bei diesen lässt die Erfüllung der lang ersehnten Verheissung hundertprozentiger Sicherheit weiterhin auf sich warten.

Blogpost wurde erstellt von Christian Peter im Rahmen vom CAS Information Security & Risk Management.



https://www.weblaw.ch/fr/competence/people/p/peter_christian.html

https://web.fhnw.ch/plattformen/blogs/iwi/2017/12/05/cas-information-security-risk-management-2017-taugt-die-biometrie-als-tueroeffner/#more-48404