

# Gesicht und Sprache statt Passwörter

Mit BiometrySSO bringt der Schweizer Hersteller Biometry.com eine biometrische Single-Sign-on-Lösung für den Einzelanwender auf den Markt.

VON URS BINDER

## IN KÜRZE

- BiometrySSO bietet biometrische Authentifizierung für Windows- und Web-Anwendungen.
- Die Software kombiniert Gesicht- und Stimmerkennung.
- Hardware-seitig werden nur Webcam und Mikrofon benötigt.
- Die Passwörter werden in einer Datenbank verschlüsselt gespeichert und bei der Anmeldung automatisch eingefügt.

Der durchschnittliche Computernutzer muss sich heute bei einer Unzahl von Anwendungen anmelden, sei es auf dem eigenen System, bei Applikationen im Rechenzentrum seines Arbeitgebers oder bei Web-Anwendungen. Für jede Anwendung kommt idealerweise eine eigene User-ID/Passwort-Kombination zum Einsatz, die der Nutzer aus dem Gedächtnis abzurufen hat – eine unrealistische Forderung: In der Praxis wird man sich entweder einige wenige oder gar nur eine Kombination für alle Logins merken, oder man notiert die Passwörter und legt die Notiz an einem vermeintlich sicheren Ort ab.

### Single-Sign-on tut Not

Vernünftiger und auch bequemer ist eine Single-Sign-on-Lösung (SSO), die im Stil von «Sesam, öffne dich» mit einer einzigen Authentifizierungskombination sämtliche Anwendungen zugänglich macht. Solche Lösungen sind in manchen Unternehmensnetzwerken implementiert. Auf dem Heim-PC oder dem Notebook dagegen gibt es im allgemeinen keine bequeme Authentifizierungsmöglichkeit – es sei denn, das Gerät ist mit einem Fingerabdruckleser und entsprechender SSO-Software ausgestattet, was meist nicht der Fall ist.

Hier springt die Windows-Software BiometrySSO von der Schweizer Software-Schmiede Biometry.com in die Bresche. Das Programm ermöglicht über eine Passwortdatenbank und mehrere parallele biometrische Erkennungsverfahren den Zugang zu allen Anwendungen, die mit einem Passwortschutz

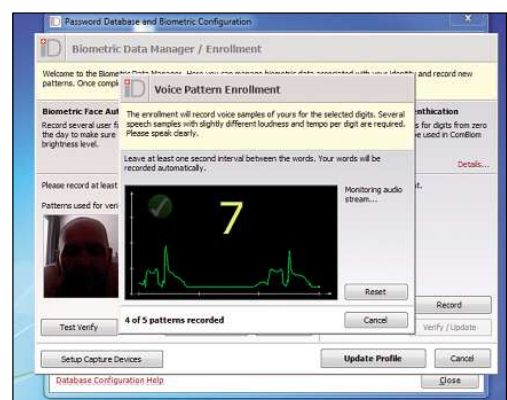
arbeiten. Ausserdem prüft die Software auf Wunsch regelmässig, ob der angemeldete User auch wirklich noch vor dem Computer sitzt und sperrt im Bedarfsfall alle zuvor per Single-Sign-on geöffneten Anwendungen.

### Zuerst registrieren

Nach der Installation fragt BiometrySSO zuallererst, wo die Passwortdatenbank abgelegt werden soll. Zusätzlich zur aktiven Datenbank lässt sich dabei eine Backup-Datei spezifizieren, in der die erfassten Authentifizierungsmerkmale laufend zweitgesichert werden. Nach dem Einrichten der Passwortdatenbank erfolgt die Registrierung des Nutzers: BiometrySSO arbeitet mit Gesicht- und/oder Stimmerkennung – die Software benötigt also einen Computer, der mit einer Webcam und einem Mikrofon ausgerüstet ist.

Die Registrierung der Gesichtsm Merkmale sollte möglichst mehrmals unter verschiedenen Lichtverhältnissen erfolgen, damit die Authentifizierung später ohne Probleme über die Bühne geht. Im Test hatten wir zu Beginn nur eine Aufnahme bei relativ schlechter Beleuchtung gemacht. BiometrySSO hatte danach deutliche Schwierigkeiten, das Gesicht wieder zu erkennen. Nach einer weiteren Aufnahme bei Tageslicht funktionierte die Erkennung dann problemlos.

Für die Stimmerkennung muss der Nutzer die Ziffern von 0 bis 9 mehrmals ins Mikrofon sprechen. Die Anzahl der Erfas-



Zuerst muss der Nutzer Gesicht und/oder Sprache registrieren. Webcam und Mikro sind Voraussetzung.

sungen lässt sich einstellen, der Hersteller empfiehlt, wie vom Programm per Default vorgegeben, jede Ziffer mindestens fünfmal nachzusprechen – möglichst mit jeweils unterschiedlicher Geschwindigkeit und Lautstärke.

### Universelle Passwortverwaltung

Hat sich der Nutzer erfolgreich registriert – in der englisch gehaltenen Oberfläche nennt sich der Vorgang «Biometric Enrollment» – steht BiometrySSO für den Praxiseinsatz bereit. Überall dort, wo eine User-ID und ein Passwort eingegeben werden müssen, präsentiert BiometrySSO im Passwortfeld einen Button mit drei Sternchen. Wird dieser angeklickt, erscheint ein Dialogfenster mit diversen Optionen. BiometrySSO zeigt hier den Inhalt der Passwortdatenbank nach Applikationen geordnet an: Wurde das Passwort für die aktuelle Anwendung bereits erfasst, lässt es sich mit einem Klick auf den entsprechenden Eintrag ins Anmeldeformular übertragen. Bei der ersten Anmeldung gibt man vor dem Klick auf den BiometrySSO-Button die User-ID und das Passwort ins Formular ein und überträgt die Angaben danach über die Option «New Record



Der Button mit den drei Sternchen weist auf die biometrischen Möglichkeiten hin.

## BIOMETRYSSO

### Fazit

Das biometrische Single-Sign-on vereinfacht die Anmeldung bei Windows- und Web-Anwendungen erheblich. Die Gesichtserkennung arbeitet schnell und gut, die Spracherkennung hat eine eher hohe Fehlerrate. Wer mit vielen Passwörtern kämpft, ist mit BiometrySSO zu einem annehmbaren Preis gut bedient, zumal keine zusätzliche Hardware nötig ist.

### Features

- Passwortdatenbank
- Zwei biometrische Authentifizierungsmethoden
- Laufende Präsenzkontrolle

### Positiv

- + Einfach zu installieren und zu bedienen
- + Schnelle Gesichtserkennung

### Negativ

- Funktioniert nicht für die Windows-Anmeldung
- Spracherkennung oft nicht erfolgreich

### Hersteller/Anbieter

Biometry.com, www.biometry.com

### Preis

Fr. 69.- pro Jahr

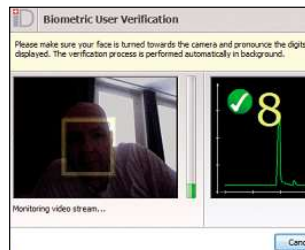
### Wertung

Funktionalität	★ ★ ★ ★ ★
Bedienung	★ ★ ★ ★ ★
Preis/Leistung	★ ★ ★ ★ ★
Gesamt	★ ★ ★ ★ ★

from User Data» in die Passwortdatenbank. Wurden die Anmeldeinformationen bereits erfasst, meldet BiometrySSO den Nutzer auf Wunsch auch vollautomatisch an – dazu dient die Option «Automate Login Data Record for the Form». Eine weitere Option heisst «Fill in but do not submit the form automatically» – Zweck selbsterklärend.

### Biometrie statt Passwordeingabe

Sobald die Passwortdatenbank für mindestens eine Anwendung bereit ist, kommen für die Anmeldung die bei der Nutzerregistrierung erfassten biometrischen Templates zum Einsatz. Die Gesichtserkennung funktioniert in der Praxis bei annehmbaren Lichtverhältnissen gut und schnell. Etwas sperriger gibt sich die Stimm- und Spracherkennung: Für eine Freigabe sind jeweils vier zufällig ausgewählte Ziffern zu sprechen. BiometrySSO erkannte im Test des öfteren eine oder mehrere Ziffern auch im wiederholten Versuch nicht, so dass wir am Schluss doch wieder aufs Passwort zurückgreifen mussten. Wir haben darauf die Stimmerkennung deaktiviert – Gesichtserkennung allein ist zwar weniger sicher, aber immer noch sicherer als ein irgendwo aufgeschriebenes oder allzu einfaches Passwort.



Die biometrische Erkennung ist im Gange.

### Laufende Nachkontrolle

Ist die Option «Lock SSO-activated Programs» aktiviert, prüft das Programm im Fünf-Sekunden-Intervall regelmässig via Webcam nach, ob der Nutzer tatsächlich noch vor dem Computer sitzt. Ist dies nicht der Fall, werden nach einer einstellbaren Reaktionsfrist alle ge-

öffneten Anwendungen gesperrt. Sobald das registrierte Gesicht wieder vor der Webcam erscheint, gibt BiometrySSO die gesperrten Anwendungen wieder frei. Die laufende Präsenzkontrolle, die Sperrung und die Freigabe der Anwendungen gehen vollautomatisch vor sich – es erscheint jeweils nur eine kleine Notiz auf dem Bildschirm, die den aktuellen Status meldet, zum Beispiel «Please pay attention to the camera to verify your identity».

Einen Pferdefuss hat die permanente Präsenzkontrolle: Die Kamera wird ständig durch BiometrySSO in Anspruch genommen. Benötigt man die Webcam für einen anderen Zweck, muss die Präsenzkontrolle unterbrochen und die Kamera freigegeben werden. Die Software bietet dazu eine Option im Taskleisten-Menü und einen Hotkey. Zwei weitere Hotkeys lassen sich für die Wiederaufnahme der Präsenzkontrolle und die Sperrung der geöffneten Anwendungen definieren. ■



Ist der Nutzer nicht vor der Kamera, wird gesperrt.



## TEST TICKER

**iX Oktober 2010 vergleicht Script-Editoren für die Windows Powershell.** Das Fazit für die integrierten Tools Powershell Konsole und Powershell Integrated Scripting Environment sieht nicht rosig aus: Als einzigen Vorteil werten die Tester, dass beide auf jedem System automatisch vorhanden sind, auf dem die Powershell installiert ist. «Wenig Komfort, viele Funktionen nur kommandozeilenorientiert», lautet die weitere Bewertung. Da haben die drei übrigen getesteten Tools schon mehr zu bieten: Powershell Plus überzeugt durch Script-Verwaltung mit Code-Snippets und mitgelieferte Scripts. Das kostenlose PowerGUI bietet laut dem Test insgesamt weniger Funktionen als Powershell Plus, ermöglicht aber Tabellenansichten auf Basis von Powershell-Scripts. Primalscript ist ein Universaleditor für viele Formate und Sprachen – aber

die Oberfläche passt sich nicht hinreichend der gewählten Sprache an, und einige Funktionen waren im Test nicht lauffähig. Das Fazit: Am besten ist das 145 Dollar teure Powershell Plus.

**Das deutsche Computermagazin Com!** hat in Ausgabe 11/2010 acht Security-Suiten auf Herz und Nieren geprüft und kommt zum Schluss, dass G Data Internet Security 2011 den PC am besten schützt. Das Paket habe im Test eine der besten Scan-Leistungen gezeigt (Erkennungsrate 99,86 Prozent) und aktive Malware zuverlässig entfernt. Die weitere Rangfolge präsentiert sich so: Auf dem zweiten Platz liegen ex aequo Bitdefender Internet Security 2011 und F-Secure Internet Security 2011, dahinter folgen Norton Internet Security 2011 (3), Kaspersky Internet Security 2011 und Panda

Internet Security 2011 (4) und Avira Premium Security Suite 10 (5). Das Schlusslicht bildet McAfee Internet Security 2010.

**«Viel Versprochen, wenig gehalten»** betitelt C't 22/2010 seinen Test des vom deutschen Hersteller Neofonie eigentlich als iPad-Killer geplanten Tablets WeTab. Daraus wird nun wohl nichts, denn es stecken laut dem Test zwar gute Ideen in dem Produkt, manches wurde aber unsauber umgesetzt. Als Videoplayer taugt das Gerät für Youtube in Standardauflösung. Wer mehr Funktionalität wolle, stosse auf ein dünnes App-Angebot und inkonsistente, nicht fingertaugliche Bedienkonzepte. Das Gewicht, der blickwinkelabhängige Screen und die kurze Akkulaufzeit passen laut den Testern nicht zu den Anwendungsgebieten Lesen und Couch-Surfen.