

## ***Schutz gegen Existenz bedrohenden Datendiebstahl: Benutzererkennung mit Tastatur***



***Langjährige Forschung „für die Katz“***

***„Bei uns passiert schon nichts!“***

***Gesetze zwingen zur Veröffentlichung von Datenverlusten***

***Wie sieht wirksamer Schutz gegen Passwortdiebstahl heute aus?***

**37 Prozent der deutschen Unternehmen in Deutschland waren laut KPMG in den letzten drei Jahren Opfer von Wirtschaftskriminalität.**

Diese nimmt besonders im Internet signifikant zu, wie die KPMG herausfand. Insbesondere mittelständische Unternehmen sind davon betroffen.

**Der höchste Wert jedes Unternehmens ist das Wissen, das es erarbeitet und erworben hat: Sowohl Produktentwicklungen als auch Lösungen, Strategien etc. Das wird vielfach unterschätzt. Dieses Wissen ist stark gefährdet durch Datendiebstahl. Passwörter sind kein Schutz mehr. Sie werden auf Bestellung geknackt. Das dauert selbst bei komplizierten Passwörtern nur ein paar Stunden und ist erwiesenermaßen eine große Gefahr.**

Ein namhaftes mittelständisches Unternehmen hatte jahrelang mit hohem zeitlichem Aufwand eine Fertigungsanlage mit hohem Potenzial für einen neuen Markt entwickelt: Geheimsache. Kurz vor Anmeldung seines Patentbesitzes erfuhr der Inhaber, dass dieses Patent bereits weltweit angemeldet sei. Nachforschungen ergaben, dass exakt seine Berechnungen, Zeichnungen, Unterlagen etc. mit marginalen Änderungen von einem chinesischen Unternehmen eingereicht worden waren... Studien des Ponemon Institutes ergaben einen durchschnittlichen Schaden bei Datenverlust von über zwei Millionen Euro. Meist zögern Unternehmen bereits bei 10.000 Euro Investitionen für IT-Sicherheit. Die Meinung „Bei uns passiert schon nichts!“ kann fatal enden.

Die meisten Geschädigten scheuen sich, ihren Verlust publik zu machen: Der zusätzliche Imageverlust wäre immens. Mit der Novelle des Bundesdatenschutzgesetzes wurden die Auflagen für Unternehmen noch strenger: Bei Verlust von Kundendaten muss die Information entweder persönlich oder durch Pressemeldungen erfolgen – unter Androhung hoher Strafgebühren.

Daten effektiv zu schützen und dabei die Kosten nicht aus den Augen zu verlieren, das ist die Herausforderung jedes IT-Sicherheitsbeauftragten. Eine Authentifizierung muss ebenso sicher wie komfortabel und vor allem kostengünstig sein.

## Verschiedene Verfahren im Vergleich

### Token und Smartcard

Sie bieten zusätzliche Sicherheit. Große Unternehmen klagen jedoch zunehmend über den gravierenden Produktivitätsausfall durch vergessene Hardware. Eine Gefahr liegt im Verlust bzw. der bewussten Weitergabe, da Personenbindung nicht garantiert ist. Nicht zu unterschätzen: Der logistische Aufwand zur Installation an den Arbeitsplätzen und beim Versand. Hohe Kosten ergeben sich sowohl in der Anschaffung als auch bei Verwaltung und Wiederbeschaffung.

### Fingerprint

Das Verfahren ist einfach zu handhaben, erfordert jedoch, um effektiv zu sein, eine sehr hochwertige Software. Der Vorteil von Biometrien liegt normalerweise in der Personenbindung. Gegen die Fälschung eines Fingerabdrucks, die auch im Internet sehr gut beschrieben ist, ist man jedoch nicht gefeit. Nicht für jeden ist die Methode anwendbar. Die Abhängigkeit von der Hardware bedeutet eine Einschränkung, wenn man sich an flexiblen Einsatzorten einloggen möchte.

### *Die Zukunft der Authentisierung*

*Nutzer muss sich  
kein Passwort merken*

*Einzigartige Merkmale beim Tippen  
machen die Methode sicher*

*Wer errät die PIN Ihrer Kredit-  
karte? Der hat vielleicht zufällig  
auch Ihr Tippverhalten*

### Tippverhaltensbiometrie

Das Tippverhalten jedes Menschen ist so einzigartig wie seine Handschrift. Auf dieser Erkenntnis beruht die Tippverhaltensbiometrie zur Verifizierung des Benutzers. Das bedeutet: Keine Passwörter mehr. Der kurze Satz zum Login steht für alle sichtbar auf dem Bildschirm. Die relativ junge Maßnahme erfüllt alle Anforderungen für eine sichere Nutzererkennung.



**Sie ist so sicher wie die PIN Ihrer Kreditkarte.** Die Wahrscheinlichkeit, dass jemand anderer Ihr Tippverhalten „knackt“, ist so hoch wie das Erraten Ihrer Kreditkarten-PIN-Nummer.

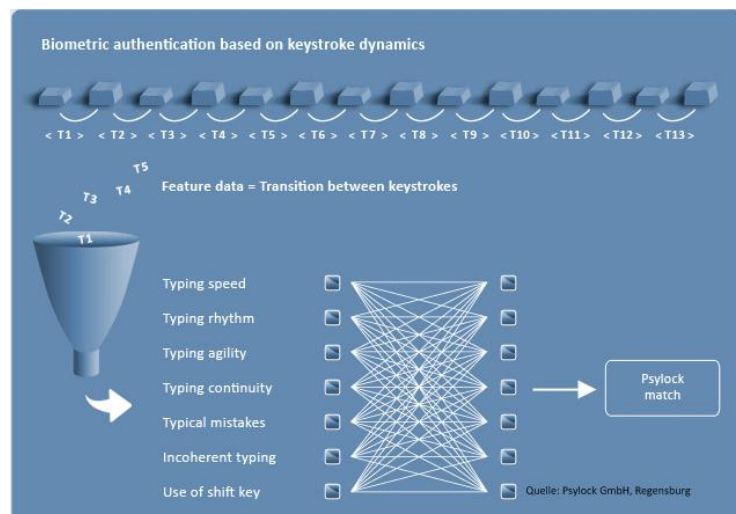


***Das Unterbewusstsein ist ausschlaggebend***

In jahrzehntelanger Forschungsarbeit wurden nicht nur sichtbare Kriterien erfasst wie Zwei- und Zehnfingersystem oder das Umschaltverhalten, sondern auch tiefer liegende Merkmale, die nicht bewusst beeinflussbar sind. So werden z. B. Überschneidungen und häufig auftretende Tippfehler bzw. Korrekturen zur Unterscheidung herangezogen.

***Hunderttausende Male erprobt***

Insgesamt sind es mindestens fünfzehn verschiedene Merkmale, die mathematisch erfasst werden und so ein klares Bild vom Tippenden ergeben. Langjährige Tests mit Hunderttausenden haben das bestätigt.



***Skalierbare Sicherheit***

Die Erkennungsleistung korreliert mit der zu tippenden Textlänge. Damit ist die Stärke des Verfahrens je nach Sicherheitsbedürfnis von hoch bis sehr hoch einstellbar. Eine willentliche Weitergabe des Tippverhaltens ist nicht möglich, da sich die charakteristischen Feinheiten im Millisekundenbereich abspielen. Dies schließt auch eine erzwungene Anwendung in einer stressbehafteten Bedrohungssituation aus.

***Angezeigten Satz tippen – sofortiges Login***

**Sie ist komfortabel.** Der Nutzer braucht sich kein Passwort merken. Er benötigt keine Zusatzhardware – jede handelsübliche Tastatur eignet sich dafür. Tippverhalten kann nicht gestohlen, verloren oder imitiert werden. Es bedeutet die Unabhängigkeit von Zusatzhardware.

***Egal, wann und wo – funktioniert immer und überall***

Weltweites Login an jedem Computer. In Zeiten mobiler Arbeitsplätze ein großes Plus.

***Keine Hardware, keine Wartung, kein Verlust, keine Beschädigung, schnelle Installation***

**Sie spart vielfach Kosten:** In der Anschaffung - es handelt sich um eine reine Softwarelösung. Sie ist schnell installiert, wartungsfrei und bedarf keiner aufwändigen Logistik. Verlust oder Beschädigung ausgeschlossen. Daraus ergibt sich gegenüber anderen Methoden eine Ersparnis bis zu 75 %.

**Somit stellt die Tippverhaltensbiometrie eine gute und sichere Alternative zu herkömmlichen Authentifizierungen dar, auch im Hinblick auf den Return-on-Invest.**

Die Psylock GmbH ist führend auf dem Sektor der Tippverhaltensbiometrie. 2007 gegründet, bündelt das Unternehmen das wissenschaftliche Know-how des Gründers Prof. Dr. Dieter Bartmann und seines Teams von hochqualifizierten Softwareentwicklern.

Das Psylock Verfahren wird seit 1993 fortlaufend weiterentwickelt und stellt heute eines der weltweit sichersten, komfortabelsten und kostengünstigsten Authentifizierungsverfahren dar. Psylock wurde bereits mehrfach national und international ausgezeichnet, (z. B. Global Security Award etc.), zuletzt mit dem „Deutschen IT-Sicherheitspreis 2008“. Diverse nationale und internationale Patente schützen die Psylock Produkte.

**Ansprechpartner PR:** Hildegard Herzog

**Psylock GmbH**

Regerstraße 4

93053 Regensburg

Tel.: +49.941.28095.102

Fax: +49.941.28095.111

E-Mail: [presse@psylock.com](mailto:presse@psylock.com)

[www.psylock.com](http://www.psylock.com)