

Neben den bereits genannten Sicherheitseigenschaften erfüllt der PasswordSitter weitere vorteilhafte Eigenschaften:

- ++ Unterstützung verschiedener Passwortregeln und Politiken
- ++ Effizienter Passwortwechsel
- ++ Verschlüsselte lokale Ablage von Profildaten

### Schutz, der sich lohnt

Laut der jährlichen Safenet-Umfrage schreiben 50 Prozent aller beruflichen Computernutzer ihre Passwörter auf und rund ein Drittel verrät die eigenen Geheimnisse auch Kollegen. Viele Menschen wählen schwache Passwörter wie den Namen des Ehepartners oder verwenden kurzerhand für alle Zwecke das gleiche Passwort. All dies stellt ein erhebliches Sicherheitsrisiko für Unternehmen dar, das sich mit dem PasswordSitter beseitigen lässt. Außerdem steigert das Programm die Unternehmenssicherheit, weil es besonders starke Passwörter erzeugt. Dadurch, dass man sich als Benutzer nur noch ein Master-Passwort merken muss, wird das

Problem mit vergessenen Passwörtern entschärft und als Unternehmen kann man sich Helpdesk-Kosten sowie Kosten durch unproduktive Wartezeiten sparen.

### Zielgruppen – Anwendungsfelder

Die Verwertungsmöglichkeiten des PasswordSitters sind vielseitig. Unternehmen können ihn beispielsweise als Dienst anbieten, in existierende Anwendungen und Dienste einbetten oder firmenintern nutzen. Letzteres eignet sich insbesondere für Unternehmen, die über viele Mitarbeiter verfügen oder über zahlreiche unternehmensinterne passwortgeschützte Anwendungen verfügen. Unternehmen, die vom PasswordSitter profitieren können, lassen sich in folgende Kategorien einordnen:

- ++ Unternehmen als Endanwender
- ++ IT-Dienstleister
- ++ Software-Hersteller
- ++ Portalbetreiber



PasswordSi<sup>++</sup>er

Webbasiertes Passwort-Management:  
einfach, sicher, flexibel

#### Fraunhofer-Institut für Sichere Informationstechnologie SIT

Ansprechpartner:

Dr. Markus Schneider  
Rheinstraße 75  
64295 Darmstadt

Telefon: +49 (0) 6151 / 869-337  
Fax: +49 (0) 6151 / 869-224  
E-Mail: markus.schneider@sit.fraunhofer.de

Dipl.-Inform. Ruben Wolf  
Rheinstraße 75  
64295 Darmstadt

Telefon: +49 (0) 6151 / 869-60177  
Fax: +49 (0) 6151 / 869-224  
E-Mail: ruben.wolf@sit.fraunhofer.de

Web: www.sit.fraunhofer.de  
www.sit.passwordsitter.de



Die Passwort-Abfrage ist in der Praxis noch immer die am weitesten verbreitete Methode der Identitätsprüfung – sowohl in der lokalen Computerumgebung als auch im Internet. Ob E-Mail, Online-Auktionen oder Zugriff auf Netzwerk-Ressourcen, überall sind Zugangsdaten und Kennwörter gefragt. Die steigende Zahl der zu merkenden und regelmäßig zu ändernden Passwörter überfordert jedoch viele Nutzer, insbesondere wenn komplexe Passwortregeln zu befolgen sind.

Der PasswordSitter vom Fraunhofer-Institut SIT löst dieses Problem. Er sorgt für starke Passwörter und liefert sie sicher auf jedes Gerät. Der PasswordSitter ermöglicht Unternehmen, ihre Mitarbeiter zu entlasten, die Helpdesk-Kosten zu senken, Produktivitätsausfälle zu vermeiden und die Sicherheit des eigenen Unternehmens deutlich zu erhöhen.

### Mit Sicherheit flexibel

Weil sich kein Mensch viele komplizierte Passwörter merken kann, nutzen Anwender Hilfsmittel: Sie speichern ihre Passwörter auf dem eigenen Rechner oder auf spezieller Hardware wie USB-Sticks, legen sie verschlüsselt auf irgendwelchen Servern ab, notieren sich ihre Passwörter auf Zetteln oder verwenden einfach ein einziges Passwort für verschiedene Zugänge. Diese Methoden haben gravierende Mängel, was Sicherheit, Benutzerfreundlichkeit und Flexibilität angeht. Merkzettel und USB-Sticks kann man verlieren, auf Festplatte gespeicherte Passwörter stehen nicht auf allen Geräten zur Verfügung.

Anders beim PasswordSitter: Hier merkt sich der Benutzer nur noch einziges Geheimnis, das Master-Passwort. Mit dessen Hilfe erzeugt der PasswordSitter die Passwörter für die jeweiligen Dienste und Anwendungen. Hierbei berücksich-

tigt er die Passwortregeln der jeweiligen Anwendung. Verlangt ein Online-Dienst etwa, dass Passwörter mindestens zehn Zeichen lang sind und Sonderzeichen enthalten, berücksichtigt der PasswordSitter diese Anforderungen. Außerdem vereinfacht der PasswordSitter auch die Änderung von Passwörtern und unterstützt Benutzer so bei der Befolgung von Passwortpolitiken. Um die Eingabe von Zugangsinformationen zu erleichtern, kann der Nutzer auch Passwortregeln, Login-Namen und Internet-Adressen für die jeweiligen Dienste speichern.

### Einfaches Passwort-Management: jederzeit – überall

Der PasswordSitter lässt sich per Browser benutzen. Bei einer Nutzung über Internet wird das Programm als signiertes Applet geladen und ausgeführt. Dadurch ist der Nutzer nicht an einen festen Computer gebunden und kann seine Passwörter mit einem beliebigen Endgerät benutzen. Am Arbeitsplatz, zu Hause oder auch im Internet Café – mit dem PasswordSitter hat man überall Zugang zu seinen Passwörtern. So stehen die Passwörter jederzeit auf verschiedenen Computern zur Verfügung, ohne dass der Nutzer seine Passwörter abspeichern und/oder mitnehmen muss.

Die Benutzung ist denkbar einfach: Programm öffnen, Master-Passwort eingeben und per Klick den Dienst oder die Anwendung wählen, für den man das Passwort benötigt. Der PasswordSitter berechnet das jeweilige Passwort und kopiert es in die Zwischenablage des Computers, von wo aus man es bequem in das entsprechende Eingabefeld einfügen kann. Nach wenigen Sekunden wird das Passwort automatisch aus der Zwischenablage gelöscht. Auf dem jeweiligen Endgerät verbleiben so keine Spuren, mit denen sich ein Passwort rekonstruieren ließe.

### Generieren, nicht speichern!

Anders als herkömmliche Passwort-Werkzeuge speichert der PasswordSitter die Geheimnisse nirgendwo dauerhaft, sondern generiert sie stets neu. Dabei nutzt er Informationen, die an unterschiedlichen Orten verteilt sind. Nach Eingabe des Master-Passworts lädt der PasswordSitter die zur Berechnung der Passwörter erforderlichen Daten über das Internet. Hierzu zählen etwa die Passwortregeln für Dienste und Anwendungen, die auf einem Server in einer Datenbank gespeichert werden können.

Selbst wenn ein Angreifer die auf dem Server abgelegten Informationen kennt, kann er damit die Passwörter des Nutzers nicht in Erfahrung zu bringen. Zur Berechnung der Passwörter ist stets das Master-Passwort des Benutzers erforderlich, das nirgendwo gespeichert und in keiner Weise übertragen wird.

Die Generierung von Passwörtern ist auch ohne Netzzugang möglich. Hierbei liest man als Benutzer seine Profildaten von der Festplatte ein oder gibt sie von Hand ein. Dadurch werden Freiheit und Flexibilität für den Endanwender nochmals verbessert, weil er sicher sein kann, auch im Falle eines Server-Ausfalls stets an seine Passwörter zu kommen.

### Sicherheitseigenschaften

Die Berechnung der Passwörter im PasswordSitter basiert auf einem Verfahren, welches am Fraunhofer SIT entwickelt wurde und dem Patentamt zur Patentierung vorliegt. Hierzu wird AES eingesetzt, ein weltweit von Sicherheitsexperten anerkanntes und für sicher befundenes Verschlüsselungsverfahren. Die Sicherheit der Passwörter basiert auf der Geheimhaltung des Master-Passworts. Darüber hinaus garan-



tiert das im PasswordSitter eingesetzte Verfahren, dass man von einem bekannten Passwort weder auf das Master-Passwort noch auf andere Passwörter zurück schließen kann.

Ebenso ist das auf dem Server gespeicherte Benutzerprofil gegen unerlaubte Zugriffe geschützt. Hierzu dient ein spezielles Datenbank-Passwort, das der PasswordSitter aus dem Master-Passwort errechnet. Dies geschieht vollautomatisch, der Benutzer muss sich dieses Datenbank-Passwort also weder merken noch irgendwo eingeben. Die Berechnung des Datenbank-Passworts ist dabei so angelegt, dass auch der Betreiber der entsprechenden Datenbank nicht auf das Master-Passwort zurück schließen kann.

Die mit dem PasswordSitter generierten Passwörter erfüllen die Voraussetzungen an starke Passwörter. Darüber hinaus stellt der PasswordSitter sicher, dass alle Dienste und Anwendungen unterschiedliche Passwörter erhalten. Insgesamt betrachtet, kombiniert der PasswordSitter die hohe Sicherheit der lokalen Speicherung mit der Flexibilität von Serverlösungen.