63349

11/2014
August

SekretärinnenSERVICE

Erfolgsideen für Büromanagement und Chefassistenz

Schwerpunktausgabe: Datenschutz

EDITORIAL

Irene Fischer Farzan, Herausgeberin und Management-Assistentin

Das gläserne Office

Liebe Leserin,

seit Edward Snowden die Abhörpraktiken des Amerikanischen Geheimdienstes publik gemacht hat, ist jedem Internetnutzer bewusst, wie transparent wir als Privatpersonen, Bürger oder auch als Unternehmen sind. Datenkraken wie Facebook oder Google verfolgen unsere Spur im Internet minutiös. Sie analysieren unser Surfverhalten, wer mit welchen Personen vernetzt ist, in welchen Online-Shops wir was einkaufen, wie wir unsere Freizeit verbringen und welche Ansichten wir vertreten. Das Internet weiß längst mehr über uns als wir selbst. Hinzu kommt, dass laufend neue Sicherheitslücken bei Cloud-Lösungen, sozialen Netzwerken oder bei der Datenübermittlung bekannt werden. Ja, selbst die Anbieter von Sicherheits- und Verschlüsselungssoftware, die uns eigentlich vor unliebsamen Eindringlingen schützen sollten, sind vor Hackerangriffen nicht gefeit. Wer sich im Internet bewegt, muss damit rechnen, bespitzelt zu werden. Lesen Sie in dieser Ausgabe, wie Sie sich – soweit es geht – gegen die Überwachung schützen können.

Ihre
Irene Fischer Farzan

*Nach vier Jahren Bank- und über 15 Jahren Sekretariatserfahrung ist unsere Herausgeberin **Irene Fischer Farzan** heute Assistentin des Teilbereichsleiters eines großen Energiekonzerns.*

Datensicherheit

Datenschutz am Arbeitsplatz

Opfer von Daten- oder Identitätsdiebstahl kann jeder werden. Bei zu sorglosem Umgang mit schützenswerten Daten kann deshalb auch jeder Mitarbeiter seine Firma in Schwierigkeiten bringen. Datenschutz und Datensicherheit beginnen sprichwörtlich an jedem einzelnen Arbeitsplatz.

In der Bundesrepublik Deutschland sind der Schutz und der Umgang mit personenbezogenen Daten im Rahmen des Bundesdatenschutzgesetzes (BDSG) geregelt. Dem BDSG untersteht jede Einrichtung, die personenbezogene Daten verarbeitet oder speichert – also auch Ihr Unternehmen. Personenbezogene Daten sind Informationen, die einer bestimmten natürlichen Person **zugeordnet sind** oder zugeordnet **werden können**. Etwa: „Klaus Müller hat grüne Augen, besitzt ein Konto mit der Nummer 123456 bei der Sparkasse Musterstadt und hat seine Rechnungen in den vergangenen 12 Monaten nicht pünktlich bezahlt."

Eine Teilmenge der personenbezogenen Daten sieht der Gesetzgeber als **besonders schützenswert** an, nämlich **Gesundheitsdaten, Informationen über die rassische oder ethnische Herkunft, politische, religiöse, gewerkschaftliche oder sexuelle Orientierung** (§ 3 Abs. 9 BDSG). Ihre Verarbeitung ist an strengere Voraussetzungen gebunden als die Verarbeitung sonstiger personenbezogener Daten.

Grundsatz der Datensparsamkeit

Ein wichtiger Begriff, der in diesem Zusammenhang immer wieder fällt, ist die Datensparsamkeit. Darunter wird verstanden, dass für die Verarbeitung von Daten **nur so viele personenbezogene Daten** abgefragt und verarbeitet werden, wie für die Durchführung der konkreten Aufgabe **erforderlich** sind. Um die Bestellung eines Kunden abwickeln zu können, benötigen Sie die Bankverbindung. Die Abfrage und Verarbeitung dieser Daten ist also zulässig. Dagegen benötigen Sie keinerlei Angaben zum Familienstand.

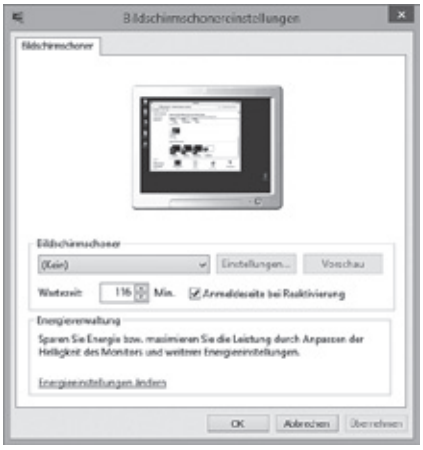
Korrekter Umgang mit Daten

Das BDSG hat direkte Auswirkungen auf jeden einzelnen Arbeitsplatz, an dem personenbezogene Daten verarbeitet und gespeichert werden. Folgende Grundsätze sind einzuhalten:

- **Zutrittskontrolle:** Nur dazu berechtigte Personen dürfen auf Systeme zugreifen, auf denen personenbezogene Daten verarbeitet werden.
- **Zugangskontrolle:** Unbefugte dürfen das System nicht benutzen können. (Schutz ist etwa die passwortgeschützte Anmeldung am PC.) (☛ Abb. 1)
- **Weitergabekontrolle:** Daten dürfen nicht während der Übertragung oder des Transports unbemerkt verändert, gelöscht, kopiert oder gelesen werden.
- **Eingabekontrolle:** Es muss nachgewiesen werden können, vom **wem** Daten eingegeben, bearbeitet oder entfernt worden sind.
- **Verfügbarkeitskontrolle:** Personenbezogene Daten müssen gegen die

INHALT

zufällige Zerstörung oder Verlust geschützt werden.



☛ **Abb. 01:** Unter Windows sollten Sie in den Einstellungen des Bildschirmschoners aktivieren, dass beim Beenden des Schoners das Passwort eingegeben werden muss.

- **Zugriffskontrolle:** Es muss sichergestellt sein, dass nur die personenbezogenen Daten eingesehen und verarbeitet werden können, auf die eine befugte Person Zugriff haben muss. (Der Sachbearbeiter von Sachgebiet 1 darf nicht ohne Begründung solche Daten aus Sachgebiet 2 ansehen.)

Was bedeutet das im Alltag?

1. **Passwortschutz für Ihren Computer**
   Wenn auf Ihrem Computer Daten mit Personenbezug verarbeitet werden, sollte unter Windows die **Tastenkombination „Windows-L“** zu Ihrem alltäglichen Begleiter werden, und zwar immer dann, wenn Sie Ihren Arbeitsplatz verlassen. Denn mit diesem Tastenkürzel **sperren Sie Ihre Arbeitsstation**. Weiterarbeiten können Sie erst, nachdem Sie erfolgreich das **Passwort eingegeben** haben, mit dem Sie sich auch sonst anmelden.
2. **Verschlüsselung von E-Mails**
   Wenn Sie personenbezogene Daten weitergeben müssen (zum Beispiel per E-Mail), dürfen Sie diese nicht einfach unmittelbar versenden. Denn das BDSG fordert ja, dass bei der Übermittlung solche Daten nicht in falsche Hände geraten oder gar manipuliert werden können. Sie sollten also solche Daten stets **vor dem Versand verschlüsseln**.
3. **Unwiderrufliches Löschen**
   Werden die schützenswerten Daten nicht mehr benötigt, müssen Sie diese so **vernichten**, dass sie **nicht durch unbefugte Dritte wiederhergestellt** werden können. Einfaches Löschen auf dem PC erfüllt diese Forderung nicht!
4. **Aktuelle Schutzprogramme**
   Ein wichtiger Schutz vor Datendiebstahl und Manipulationen besteht im **Schutz des eigenen Systems** durch aktuelle **Virenscanner** und andere **Schutzprogramme**. Besonders aufpassen sollten Sie aber immer dann, wenn Sie externe Datenträger wie USB-Sticks an Ihrem System anschließen. Denn grundsätzlich kann jeder externe Datenträger auch ein Spionageprogramm enthalten. ●

Passwortschutz

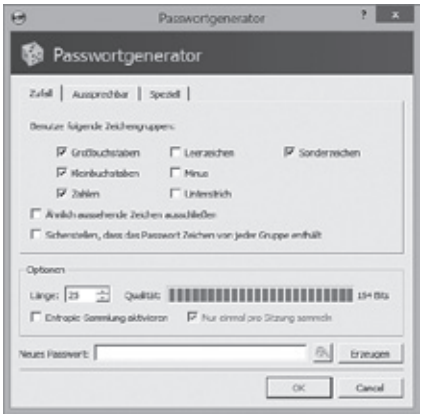
Sicherheit beginnt mit sicheren Passwörtern

Mit einem Passwort sichern Sie den Zugang zu Ihrem Computer, dem Netzwerk, Online-Diensten oder auch Dateien ab. Passwörter begegnen uns täglich, und groß ist die Versuchung, stets das gleiche Passwort zu verwenden. Lesen Sie in diesem Beitrag, wie ein sicheres Passwort sein sollte und wie Sie Ihr individuelles System dafür schaffen.

Ein sicheres Passwort besteht aus **mindestens 11 Stellen**, in denen **große** und **kleine Buchstaben**, **Ziffern** und **Sonderzeichen** vorkommen. Einfache Schulmathematik führt zu dieser Erkenntnis. Jede Stelle des Passworts kann aus 62 verschiedenen Zeichen bestehen (26 Buchstaben in großer und 26 in kleiner Schreibung plus 10 Sonderzeichen). Da jedes dieser Zeichen erneut an jeder Stelle auftauchen darf, ergeben sich rechnerisch 62^11 Kombinationsmöglichkeiten: 5,20365607 x 10^19. Selbst leistungsstarke Rechensysteme sind beim Errechnen und Ausprobieren (2 Mrd. Kombinationen in der Sekunde) damit 800 Jahre beschäftigt.

Hinweis: Diese rechnerische Sicherheit schützt natürlich nicht davor, dass bereits beim Ausprobieren die erste Möglichkeit zum Treffer führt. Die Wahrscheinlichkeit dafür ist aber gering. Sichere Passwörter besitzen einen Nachteil. Sie sind **schwer zu merken**, weswegen viele Anwender es sich dann doch wieder einfacher machen und kurze Passwörter vergeben oder (falls das durch die Vorgaben des Systems ausgeschlossen ist) sich das Passwort aufschreiben (☛ Abb. 2).

Geben Sie keinesfalls der Versuchung nach, für jedes System, das Sie verwenden, das gleiche Passwort zu benutzen! Gelangt es einmal in falsche Hände, stehen einem Angreifer dann gleich alle diese Systeme offen.



☛ **Abb. 02:** Ein Passwortmanager kann Ihnen beim Anlegen eines Passworts helfen.

Merkhilfen

Zwei Mittel helfen Ihnen dabei, sich Passwörter besser merken zu können:

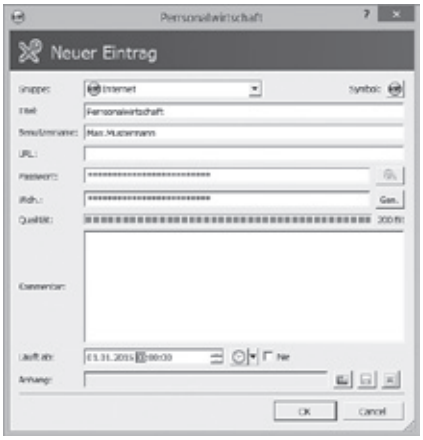
- ein System für das Finden und Merken oder
- der Einsatz einer Software (ein Passwortmanager).

Für ein **eigenes System** benötigen Sie ein etwas kürzeres, aber zugleich sicheres Passwort, das zum Beispiel aus

8 Stellen besteht. Zum Beispiel **„1MtfbwY9“**. Das sieht jetzt schon schwer zu merken aus. Wenn Sie wissen, wie das Passwort entstanden ist, allerdings nicht. Es handelt sich um die **Zahl 19**, deren Ziffern am Anfang und am Ende platziert werden. Die Buchstaben ergeben sich aus dem englischen **„May the force be with you“**, wobei eben das erste und letzte Wort mit dem Großbuchstaben abgekürzt werden.

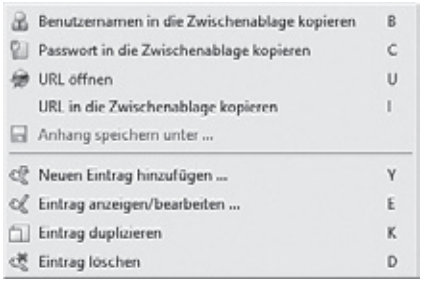
Dieses kurze Passwort bildet nun die **Grundlage für alle weiteren Zugangsbeschränkungen**. Die Grundlage wird jetzt ergänzt mit Buchstaben, die sich ebenfalls aus einer Regel herleiten. Zum Beispiel, dass Sie dem Passwort die ersten drei Buchstaben des Namens eines Dienstes oder einer Anwendung voranstellen. Sie wollen sich bei **Yahoo** einloggen? Dann ergibt sich das Passwort: „**yah1MtfbwY9“**. Sie benötigen ein Passwort für die **Personalwirtschaft** in Ihrem Unternehmen? Das Passwort lautet dann also **„per1MtfbwY9“**. Statt einer Reihe von schwierigen Ziffern- und Buchstabenkombinationen müssen Sie sich **nur einige wenige Regeln** merken. Das ist viel einfacher, oder?

Passwort-Manager werden in Hülle und Fülle sowohl für Windows als auch den Mac angeboten. Eine gute Figur auf bei-



☛ **Abb. 03:** In KeePassX hinterlegen Sie Benutzernamen, Passwort und URL.

den Plattformen macht **KeePassX** (https://www.keepassx.org/), das den großen Vorteil besitzt, **kostenlos** genutzt werden zu können und noch dazu als **Open Source** vertrieben wird. Programmierer und Administratoren mit



☛ **Abb. 04:** Über das Kontextmenü eines Eintrags übergeben Sie die Daten dann in die Zwischenablage und von dort in die Anmeldefelder des Angebots.

entsprechenden Kenntnissen können sich also den Quellcode des Programms ansehen, um eventuelle **Sicherheitslücken aufzuspüren** (☛ Abb. 3).

Sobald Sie im Internet Explorer oder einem anderen Browser ein Passwort eingeben, fragt Sie das Programm, ob Sie die **Zugangsdaten speichern** wollen. Sie sparen sich damit natürlich etwas Zeit, aber jedem Angreifer ist bekannt, wo die Anwendungen diese Daten speichern. **Verzichten Sie also darauf** genauso wie auf den Einsatz der von den Betriebssystemen (zum Beispiel Mac) angebotenen Passwort-Safes (☛ Abb. 4).

Quote

Nichts ist sicherer als ein langes Passwort, das ausschließlich in Ihrem Kopf steckt.

Praxis-Tipp

Im Falle von Krankheit oder Urlauben müssen sich Kollegen auch vertreten können. Keine gute Idee ist es, wenn im Falle eines Falles einfach das jeweilige Passwort dem anderen verraten wird. Besser ist es, **gegenseitige Stellvertretungsregeln** zu finden und **über die Administratoren** im System hinterlegen zu lassen. ●

Datensicherheit

So löschen Sie Daten sicher!

Dokumente auf modernen Computern landen zunächst in einem Papierkorb. Erst wenn dieser geleert wird, sind die Daten auch gelöscht. Oder etwa doch nicht? Lesen Sie in diesem Artikel, warum einfaches Löschen nicht ausreicht.

Das BDSG geht davon aus, dass die Sicherheit der personenbezogenen Daten auch **über den Zeitpunkt der letzten Nutzung** hinaus besteht. Werden die Informationen zu einem Kunden nicht mehr benötigt, dürfen schützenswerte Daten nicht in die Hände von Unbefugten gelangen. Es muss Ihnen also gelingen, die Daten so zu löschen, dass diese **nicht wiederhergestellt** oder gestohlen werden können. Dieses sichere Löschen gelingt mit den einfachen Bordmitteln der Betriebssysteme nicht. Legen Sie ein Element in den Papierkorb, ist es physikalisch noch vollständig lesbar auf der Festplatte vorhanden. Die Datei wird lediglich in ein bestimmtes Verzeichnis des Computers verschoben. Entleeren Sie den Papierkorb, verschwindet die Datei aus diesem Verzeichnis. Doch der Inhalt kann **problemlos wiederhergestellt** werden.

Was passiert beim Löschen?

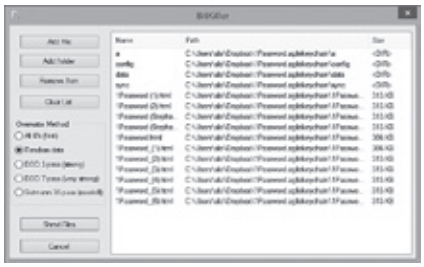
Damit der Computer eine Datei findet, muss das Betriebssystem in einer Art Inhaltsverzeichnis nachsehen, wo sich die einzelnen **Bruchstücke der Datei** befinden. Technisch bedingt setzt sich der Brief, den Sie in Word geschrieben haben, physikalisch aus einer Reihe von kleineren Informationen zusammen, die **verstreut auf der Festplatte** liegen. Wird der Papierkorb gelöscht, entfernt das Betriebssystem im Dateisystem lediglich den **Eintrag der Datei im Inhaltsverzeichnis**. Die einzelnen Bruchstücke sind immer noch auf der Festplatte vorhanden. Nur der Platz wird so vorgemerkt, dass dort **im Laufe der Zeit neue Inhalte** gespeichert werden können. Wann die ursprüngliche Datei überschrieben wird, können Sie

allerdings nicht steuern. Um wirklich sicher zu sein, dass Dokumente auf der Festplatte nicht mehr zu rekonstruieren sind, müssen gelöschte Dateien **mit neuen Daten überschrieben** werden.

Achtung! In immer mehr Computern arbeiten sogenannte **SSD-Festplatten**. Diese bestehen vereinfacht aus „Speicherchips" und funktionieren **ohne Magnetismus**. Um ihre Vorteile in Sachen Geschwindigkeit voll auszuspielen, setzen die Platten auf ein völlig anderes Speichermanagement. Um solche Datenträger vollständig und sicher zu löschen, ist **Spezialwerkzeug notwendig**. Die nachfolgenden Erläuterungen gehen davon aus, dass Sie **lediglich Dokumente** auf den Festplatten löschen wollen. Wenn es um das sichere Löschen sowohl der Daten als auch des **Betriebssystems** geht (etwa weil das Gerät ausgemustert werden soll), sollte dies **vom Administrator erledigt** werden. Er verfügt über das Spezialwerkzeug dafür.

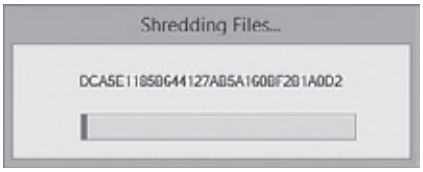
Sicheres Löschen unter Windows

Es erscheint etwas unverständlich, aber Windows verfügt über **kein eingebautes Werkzeug**, mit dessen Hilfe Sie Dokumente sicher entfernen können. Glücklicherweise werden im Internet zahlreiche Programme kostenlos angeboten. Eine solche Anwendung, die Sie nicht einmal installieren müssen, ist **BitKiller**. Besuchen Sie die Seite http://sourceforge.net/projects/bitkiller/. Klicken Sie dort auf „Download". Damit übertragen Sie ein **ZIP-Archiv**, das drei Dateien enthält. Sie benötigen lediglich **die Anwendung**. Diese bewegen Sie mit der Maus aus dem Archiv in einen Ordner Ihres Systems oder auf den Desktop. Mit Doppelklick starten Sie die App (☛ Abb. 5).



☛ **Abb. 05:** Sie ziehen die Dateien, die Sie löschen wollen, einfach in BitKiller hinein.

Ziehen Sie aus dem Explorer die zu löschenden Dateien **in das Programmfenster** statt in den Papierkorb. Entscheiden Sie sich dann für eine der angebotenen **Methoden zum Überschreiben** der Dateien. „DOD3" dürfte ein guter Kompromiss zwischen Geschwindigkeit und Sicherheit sein. Drücken Sie danach auf „Shred Files". Bestätigen Sie die Sicherheitsabfrage – und schon entfernen Sie die Dokumente sicher (☛ Abb. 6).



☛ **Abb. 06:** Je nach gewählter Methode kann das sichere Löschen dann einen Moment dauern. Die Software zeigt Ihnen aber genau an, wann der Vorgang beendet ist.

Sicheres Löschen auf dem Mac

Auch auf dem Mac landen alle Dateien, die Sie löschen, zunächst im Papierkorb. Dieser lässt sich sicher löschen, die Elemente werden dabei mehrfach überschrieben. Das Löschen dauert nur unwesentlich länger. Legen Sie die Dokumente, die Sie löschen wollen, wie gewohnt **in den Papierkorb**. Klicken Sie diesen dann mit der **rechten Maustaste und gedrückter Taste cmd** an. Im Kontextmenü erscheint so das Kommando „Papierkorb sicher entleeren". Der Mac fragt zur Sicherheit noch einmal nach. Bestätigen Sie, werden die sensiblen Daten entfernt. ●

Mobile Geräte

Datensicherheit auf mobilen Geräten

Smartphones, Tablets und Phablets sind ungeheuer praktische Geräte und aus dem Arbeitsalltag in vielen Unternehmen schlicht nicht mehr wegzudenken. Lesen Sie in diesem Beitrag, wie Sie dort den Datenschutz verbessern.

In immer mehr Unternehmen nutzen gerade die Mitarbeiter im Außendienst häufiger Smartphones mit großen Displays oder auch den Tablet-PC wie das iPad. So praktisch die Geräte sind, bedeuten sie immer auch ein Risiko für den Datenschutz und die Datensicherheit von personenbezogenen Daten.

Und dies auch gleich unter zwei Gesichtspunkten:

- Lokale gespeicherte Dateien geraten schnell in die Hände von unbefugten Dritten. Nämlich dann, wenn das Gerät verloren geht oder gestohlen wird.
- Immer wieder sorgen Programme (Apps) für die mobilen Begleiter für Schlagzeilen, weil sie, ohne den Nutzer zu informieren, Informationen vom Gerät an einen Server übermitteln.

Damit ist auch die Stoßrichtung vorgegeben, um die Sicherheit eines mobilen Geräts zu erhöhen.

Bessere Sicherheit bei Apps

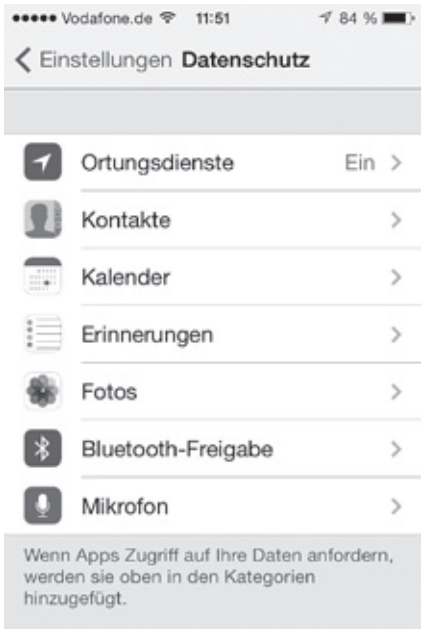
Wie bei einem klassischen PC gibt es auch bei der Nutzung von Smartphones und Tablets **zwei Maximen**, die Sie beachten müssen. Dazu gehört, dass Sie Apps **nur aus offiziellen Quellen** installieren dürfen. Nur Anwendungen, die in Play- und App-Store angeboten werden, dürfen auf dem Gerät landen. Zum anderen sollten Sie darauf achten, dass die Geräte stets **auf dem neuesten Stand** gehalten werden. Bieten die Hersteller ein **Update des Betriebssystems** an, richten Sie dies möglichst bald ein. Auch die Apps sollten stets **auf dem neuesten Stand** gehalten werden. Denn in beiden Fällen werden immer auch **Sicherheitslücken in der Software** geschlossen.

Prüfen Sie bereits während der Installation sowie bei bereits genutzten Apps, **welche Informationen** und Daten das Programm abfragt. **Hinterfragen Sie**

jeweils die Übermittlung von Daten an einen Server und den Zugriff auf das interne Adressbuch.

Datenschutz-Einstellungen

Auf einem Apple-Gerät (iPhone oder iPad) wechseln Sie in die „Einstellungen". Tippen Sie dort auf „Datenschutz" (☛ Abb. 7).



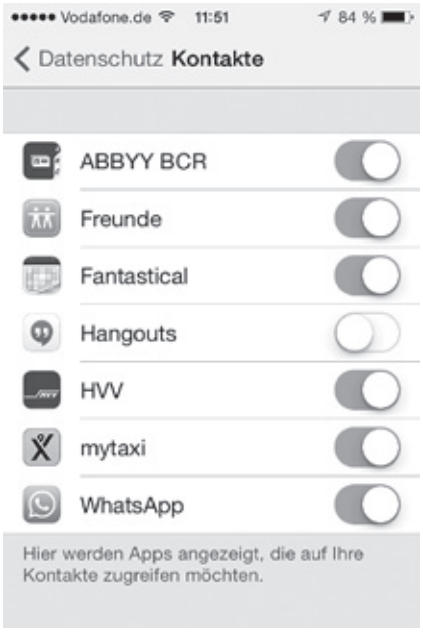
☛ **Abb. 07:** Unter iOS gehen Sie in den Abschnitt Datenschutz.

Im nachfolgenden Dialog werden verschiedene Bereiche des Systems aufgelistet wie Kontakte, Erinnerungen, Freigaben etc. Nach der Auswahl eines solchen Punktes sehen Sie exakt, welche Anwendung auf den Bereich zugreift bzw. zugreifen will. Mittels der Schieberegler passen Sie den Zugriff einfach an. Besonders kritisch sollten Sie dabei auch Freigaben prüfen, die die Übertragung von Daten auf das Gerät erlauben (Bluetooth). Deaktivieren Sie hier besser und sehen danach, ob die App noch funktioniert (☛ Abb. 8).

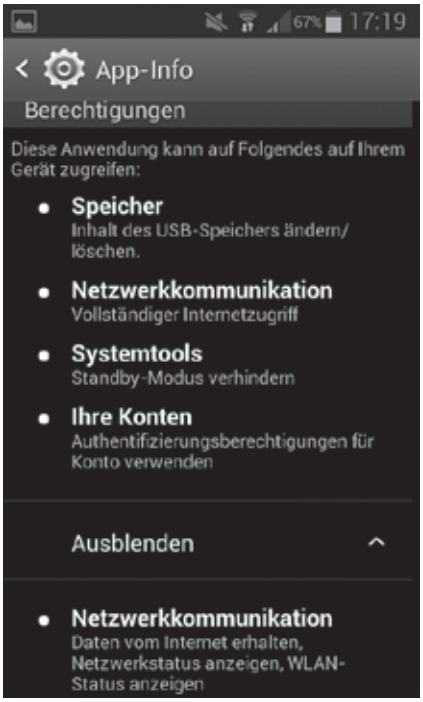
Für Geräte mit Android gibt es kostenlos im Playstore die App „Permission Manager". Diese listet Ihnen alle installierten Anwendungen auf (☛ Abb. 9). Nach Auswahl einer App wechseln Sie zu den Details und können dort jeden Zugriff einzeln bearbeiten (☛ Abb. 10).

Zugriffsschutz

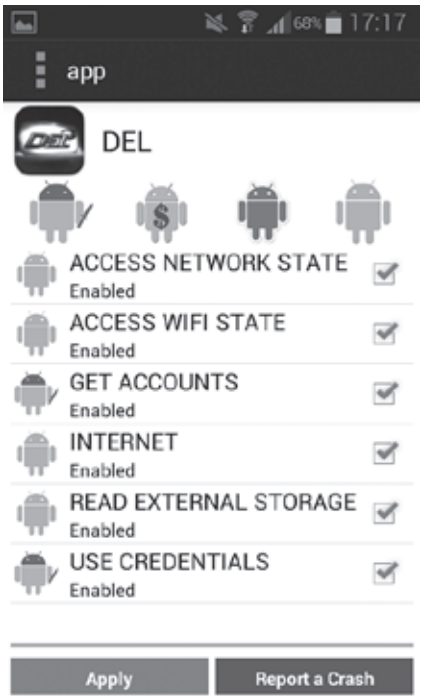
Wenn Sie keine Maßnahmen ergreifen, kann jeder, der das Gerät in die Hände bekommt, Programme starten und Daten einsehen. Dazu gehören dann eben auch spezielle Anwendungen, die vielleicht nur in Ihrem Unternehmen eingesetzt werden. Deswegen sollten Sie Ihr Gerät unbedingt vor fremdem Zugriff schützen.



☛ **Abb. 08:** Zu jeder Rubrik sehen Sie, welche App auf die gespeicherten Informationen zugreifen will.



☛ **Abb. 09:** Beim Installieren einer Android-App werden Sie gefragt, ob Sie den Zugriff auf bestimmte Infos zulassen wollen.



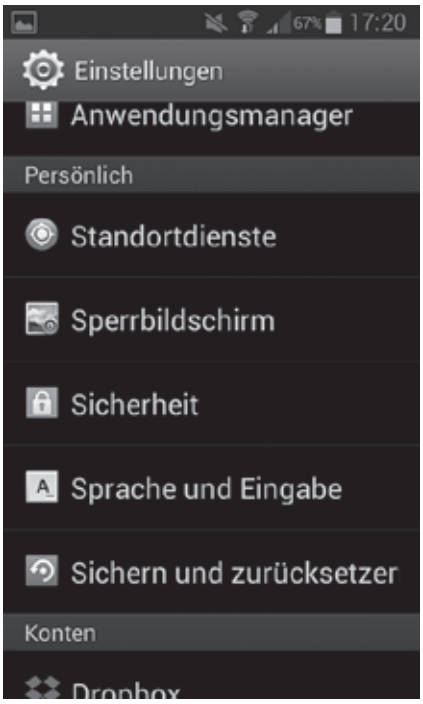
☛ **Abb. 10:** Permission Manager heißt die App, mit der Sie gezielt die einzelnen Berechtigungen einer App unter Android bearbeiten.

Auf dem iPad oder iPhone:

Rufen Sie die **Einstellungen** des Geräts auf. Wechseln Sie in den Abschnitt „Allgemein". Dort finden Sie den Bereich **„Automatische Sperre"**. Wählen Sie dort einen nicht zu kleinen, aber auch nicht zu großen Wert. Eine Mi-

Impressum
Herausgeber: WEKA MEDIA GmbH & Co. KG, Römerstraße 4, 86438 Kissing
Tel: 08233 23 7850, Fax: 08233 23 7860
E-Mail: service@weka.de,
Internet: www.weka.de
Persönlich haftende Gesellschafterin: WEKA MEDIA Beteiligungs-GmbH, Sitz in Kissing
Geschäftsführung: Stephan Behrens, Michael Bruns, Werner Pehland
Redaktion: Angela von Lerber (Chefredakteurin, V.i.S.d.P.), Irene Fischer Farzan (Herausgeberin), Michaela Timeus (Objektleitung), Stephan Lamprecht (Fachautor), Anschrift siehe oben
Layout/Satz: contentsign, Altenahr
Druck: Druckkultur GmbH, München

Erscheinungsweise monatlich.
ISSN: 1861-6933

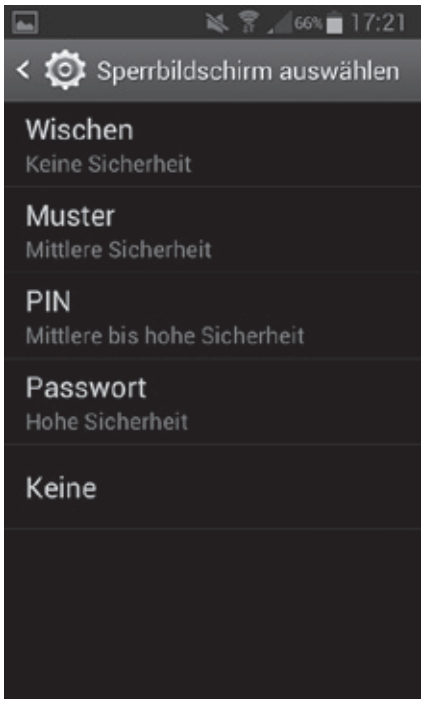


☛ **Abb. 11:** In den Einstellungen von Android finden Sie auch den Eintrag Sperrbildschirm.

nute dürfte etwas knapp bemessen sein, denn bereits nach 60 Sekunden Inaktivität wäre dann der Zugriff gesperrt. Tippen Sie auf **„Code-Sperre"** und aktivieren Sie im nachfolgenden Dialog den Zugriffsschutz. Sie müssen dort einen Code eintragen. Nutzen Sie einen möglichst langen Zahlenschlüssel, so ist die Sicherheit größer als beim „Einfachen Code", der nur aus vier Ziffern besteht.

Auf einem Android-System:

Dann müssen Sie hier ebenfalls in die Einstellungen gehen. In der Rubrik „Persönlich" tippen Sie auf „Sperrbildschirm". Tippen Sie dort erneut auf „Sperrbildschirm", können Sie die Art der Sperre definieren. Wischen und Muster sind weniger gut geeignet. Sie sollten also wenigstens eine PIN oder noch besser ein Passwort verwenden (☛ Abb. 11) (☛ Abb. 12).



☛ **Abb. 12:** Entscheiden Sie sich besser für die Eingabe eines Codes oder Passworts.

Cloud

Datensicherheit in der Cloud

Fehlt die Verbindung zum globalen Datennetz, stehen heute in praktisch jedem Unternehmen die Räder still. Doch die Vernetzung – und damit die Öffnung der Firmennetzwerke nach außen – erleichtert auch Datendieben, Hackern und Wirtschaftsspionen die Arbeit. In diesem Artikel geht es um die Datensicherheit in der Cloud.

Um personenbezogene Daten nicht unnötigen Risiken auszusetzen, sollten Sie folgende Aspekte beachten:

Synchronisierungsdienste

Es gibt eine ganze Reihe von Diensten, die den **Austausch von Dateien** zwischen verschiedenen Computern und Geräten ermöglichen. Legen Sie eine Datei in das vom Programm überwachte Verzeichnis auf Ihrem Computer, steht das Dokument binnen weniger Minuten auch auf anderen Rechnern oder sogar Ihrem Smartphone zur Verfügung. **Dropbox**, **Google Drive** oder auch **OneDrive von Microsoft** sind die bekanntesten Beispiele.

Das Problem an den Diensten: Sie haben ihre Server in aller Regel **im Ausland** stehen. Der Gesetzgeber verbietet aber die Weitergabe und Verarbeitung von **personenbezogenen Daten** im Ausland, zumindest ohne die **Zustimmung der Betroffenen**. Und damit ist die Nutzung solcher Dienste streng genommen **nicht erlaubt**. Ein Beispiel: Sie synchronisieren eine Excel-Datei, in der sich die Adressen und Namen von Kunden sowie Bankinformationen befinden. Sie müssten jetzt eigentlich jeden Kunden einzeln fragen, ob Sie seinen Datensatz auf einen Rechner im Ausland übertragen dürfen. Ein Ding der Unmöglichkeit. Daraus ergibt sich, dass Sie Dropbox & Co. nur für Dateien **ohne personenbezogene Inhalte** verwenden dürfen.

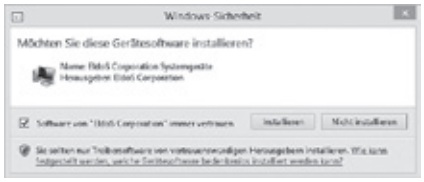
Online-Festplatten verschlüsseln

Online-Festplatten (auch ohne automatischen Datenabgleich) sind in den vergangenen Monaten in die Schlagzeilen geraten. Offensichtlich werden (zumindest auf Systemen, die in den USA stehen) **routinemäßig Daten gelesen** und von amerikanischen Sicherheitsbehörden geprüft. Das ist ein klarer Verstoß gegen das deutsche Datenschutzrecht. Wenn Sie auf die praktischen Dienste nicht verzichten wollen, bleibt Ihnen nur, die gespeicherten **Informationen zu verschlüsseln**. Nachdem das seit Jahren bewährte Programm TrueCrypt unter dem Verdacht steht, nicht mehr sicher zu sein, fehlt auf dem Markt eine leicht bedienbare (und vor allen Dingen kostenfreie) Software zur Datenverschlüsselung. Als Alternative bietet sich das Programm **Boxcryptor** (www.boxcryptor.com) an. Allerdings ist dessen Einsatz nur auf privat genutzten Computern kostenlos möglich. Im Firmeneinsatz werden **72 Euro pro Jahr** fällig. Besuchen Sie die Seite des Herstellers und laden sich die aktuelle Version auf Ihren Rechner. Starten Sie die Installation anschließend mit einem Doppelklick.

Dazu zwei Hinweise

Im Laufe des Setups werden Sie gebeten, das „EFS" von Windows auszuschalten. Dieser Bitte können Sie einfach entsprechen. **Außerdem möchte das Setup ei-**

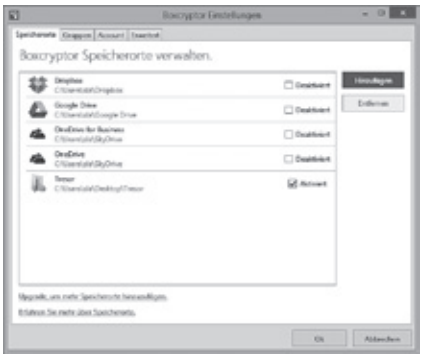
nen weiteren (externen) Programmbestandteil installieren. Dazu blendet Windows einen Sicherheitshinweis ein (☛ Abb. 13).



☛ Abb. 13: Wenn das Setup von Boxcryptor nachfragt, gestatten Sie die Installation des Gerätetreibers, um fortfahren zu können.

Erlauben Sie die Installation, da Sie sonst nicht weiterkommen. Läuft das Programm, müssen Sie zuerst ein **Benutzerkonto anlegen**. Das kann auf dem Server des Herstellers liegen oder lokal auf Ihrem System. Folgen Sie den Anweisungen für die Einrichtung eines Benutzerkontos und entscheiden Sie sich (zunächst) für das **kostenlose Paket**. Danach nistet sich das Programm im Systemabschnitt der Kontrollleiste ein. Klicken Sie mit der rechten Maustaste auf das Icon und wählen Sie aus dem Kontextmenü „Einstellungen". Im Register „Speicherorte" sind die bekanntesten Cloud-Anbieter bereits vorhanden. Mit einem Mausklick aktivieren Sie einen dieser Orte oder legen mit „Hinzufügen" ein anderes Verzeichnis fest, das auf Ihrem Rechner oder einem Server liegen darf. In der **kostenfreien Variante** der Software kann **stets nur einer** dieser Orte aktiv sein. Sobald Sie den Ort aktiviert haben, taucht in Ihrem Dateimanager ein **neues Laufwerk** auf. Alle Informationen, die Sie dort ablegen, werden von Boxcryptor **automatisch verschlüsselt**. Lesbar und unverschlüsselt sind die Daten nur, wenn Sie die Versionen aus diesem Laufwerk verwenden. Wenn Sie aus dem Kontextmenü von Boxcryptor die Funktion „Abmelden" verwenden oder aber das Laufwerk „Auswerfen", ist **kein Zugriff mehr** auf die Daten möglich. Auf dem Server oder lokal liegen damit **nur noch die verschlüsselten Versionen** vor.

Praktisch: Wenn Sie eine Datei direkt in den verschlüsselten Container ziehen (absichtlich oder aus Versehen), wird diese auf Wunsch automatisch verschlüsselt. Sie können die Verschlüsselung also nicht vergessen (☛ Abb. 14).



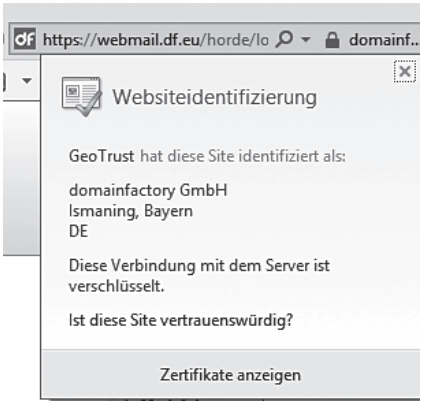
☛ Abb. 14: Boxcryptor legt mit nur einem Mausklick in den lokalen Ordnern von Standard-Cloud-Anbietern verschlüsselte Container an. Sie können aber auch ein beliebiges eigenes Verzeichnis nutzen.

Browser überprüfen!

Liegen sensible Informationen auf einem externen Server oder ungeschützt auf einem Rechner, haben Datendiebe leichtes Spiel. Es gibt neben dem Datendiebstahl aber noch eine weitere mögliche Bedrohung. Durch so genannte **Man-in-the-middle-Angriffe** könnten Informationen abgefangen und entwendet werden. Typische Szenarien sind dabei zum Beispiel das **Abfangen von Benutzernamen und Passwörtern**, damit sich der Angreifer später selbst in das System einwählen kann.

Die externe Einwahl in Kundendatenbanken oder Anwendungen des Unternehmens (zum Beispiel durch den Außendienst) sollte deshalb nach Möglichkeit **nur über eine verschlüsselte Verbindung** erfolgen. Der im World Wide Web eingesetzte Standard ist die **SSL-Verschlüsselung**. Hier kümmern sich Browser und Server automatisch um das Aushandeln der Verschlüsselung. Abgesichert wird sie durch ein **Zertifikat**, das zusichert, dass der Server, mit dem Sie kommunizieren, tatsächlich zu dem Unternehmen und der URL gehört, die Sie erwarten dürfen. Achten Sie beim Austausch sensibler Informationen per Browser also stets darauf, dass Sie eine verschlüsselte Verbindung nutzen. Und bleiben Sie vor allen Dingen gegenüber Warnhinweisen aufmerksam, die die Browser automatisch einblenden, falls Widersprüche im Zertifikat sichtbar werden (☛ Abb. 15) (☛ Abb. 16).

☛ Abb. 15: Bei einem solchen Hinweis müssen Sie vorsichtig sein



☛ Abb. 16: Mit einem Klick auf den Schlüssel blenden Sie im Internet Explorer das Fenster ein, mit dem Sie weitere Informationen erreichen.

1. Versuchen Sie beim Aufruf einer Seite immer die **sichere Verbindung** zu verwenden. Dazu geben Sie einfach **„https"** statt des gewohnten „http" ein.
2. Achten Sie auf eventuelle **Hinweise des Browsers**. Wenn Ihnen der Internet Explorer ein **Problem mit dem Zertifikat** meldet, sollten Sie sich gut überlegen, die Seite tatsächlich aufzurufen. Fragen Sie im Zweifel lieber bei Ihrem Administrator oder dem Anbieter der Seite nach, was dort los ist.
3. Wenn die **Adressleiste** des Internet Explorers **grün** wird, haben Sie erfolgreich eine abgesicherte Verbindung hergestellt, die auch durch ein gültiges Zertifikat abgesichert wird. Die Daten können also nicht abgehört werden.
4. Bei der Eingabe von besonders sensiblen Informationen, zum Beispiel Buchhaltungssystemen oder Personalwirtschaft, werden Ihnen die Anbieter meist auch noch einen **Nachweis des Zertifikats** zum Vergleich anbieten. Wenn Sie im Internet Explorer auf das Schlüsselsymbol in der Adressleiste klicken, können Sie über **„Zertifikat anzeigen"** einen separaten Dialog öffnen, über den Sie Zugriff auf die Details erhalten. Diese Daten **vergleichen** Sie dann mit der Vorlage des Dienstes. ●

Elektronische Post

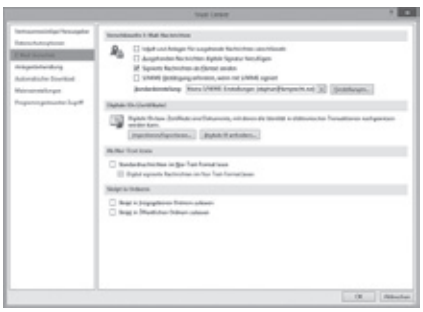
E-Mails verschlüsseln

Schnell sind per E-Mail Aufstellungen und Dateien versendet. Enthalten diese aber personenbezogene Daten, müssen Sie dafür sorgen, dass Vertrauliches auch vertraulich bleibt. So verschlüsseln Sie Ihre E-Mails.

Wenn Sie E-Mails verschlüsseln wollen, stehen **zwei verschiedene Verfahren** zur Auswahl. Diese sind leider nicht miteinander kompatibel. Damit Sie sicher Nachrichten mit dem Empfänger austauschen können, müssen Sie und der Adressat der Nachricht **das gleiche Verfahren** nutzen. Zur Auswahl stehen: S/MIME und GPG. **Hinweis:** Die genannten Programme und Zertifikate dürfen Sie nicht auf Ihrem Rechner installieren, wenn Sie bereits eine zentrale Lösung einsetzen, da sie ansonsten mit bereits eingerichteten Programmen kollidieren.

S/MIME mit Zertifikat-Erwerb

MS Outlook unterstützt S/MIME unmittelbar. Sie müssen dazu keine weitere Software erwerben. Sie erwerben lediglich ein personalisiertes Zertifikat von einer dazu autorisierten Stelle. Hierzu besuchen Sie zum Beispiel die Seite https://www.s-trust.de/bestellung/email_zertifikat/. Am Ende des Bestellprozesses wird Ihnen das Zertifikat angezeigt. In den Einstellungen von Outlook hinterlegen Sie es dann unter „Trust Center, E-Mail-Sicherheit“ (☛ Abb. 17).



☛ Abb. 17: In Outlook importieren Sie ein S/MIME Zertifikat, um über diesen Ansatz die Nachrichten zu verschlüsseln.

Das Unterschreiben und Verschlüsseln einer ausgehenden Nachricht wird unmittelbar im Editor der E-Mail erledigt. Im Register „Optionen“ sind die beiden Funktionen „Verschlüsseln“ und „Signieren“ angebracht. Drücken Sie auf „Senden“, werden die Aktionen ausgeführt. Dazu müssen Sie das Passwort, mit dem das Zertifikat gesichert ist, eintragen.

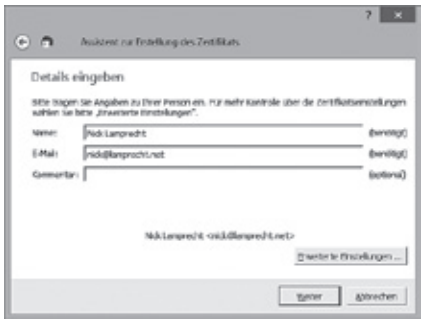
S/MIME basiert darauf, dass die Nutzer ein Zertifikat von einer **vertrauenswürdigen Stelle** erwerben (Trust Center). Die Zertifikate sind nur kostenpflichtig (ca. 30 Euro pro Jahr) zu bekommen.

GPG – flexibler und kostenlos

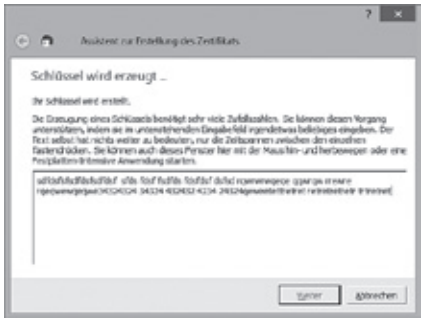
GPG basiert darauf, dass **zwei Schlüssel zur Absicherung** verwendet werden. Jeder Kommunikationsteilnehmer besitzt einen **öffentlichen** und einen **privaten** (geheimen) Schlüssel. Möchte Person A nun eine Nachricht an Person B senden, importiert A den öffentlichen Schlüssel von B in seine Software und verschlüsselt die Nachricht damit. B erhält die E-Mail und nutzt seinen geheimen und privaten Schlüssel, um die Botschaft wieder in den Klartext zu versetzen. Die **notwendige Software** finden Sie unter http://www.gpg4win.de/. Laden Sie sich das Programmpaket herunter und starten Sie die Installation mit einem Doppelklick auf die Datei. Während des Setups sollten Sie auch die **Programmkomponenten für Outlook** installieren.

Das Programm begleitet Sie durch den Prozess einer Zertifikatserstellung. Sie müssen den Namen, die E-Mail-Adresse sowie eine Passphrase eingeben. Merken Sie sich diese **unbedingt**, denn ohne diese Phrase ist später das Ver- und Entschlüsseln der Nachrichten unmöglich. Im nächsten Fenster sind zufällige Bewegungen und Eingaben vorzunehmen, damit die Schlüssel erstellt und übernommen werden (☛ Abb. 18) (☛ Abb. 19) (☛ Abb. 20).

Um eine Nachricht zu unterschreiben, gehen Sie dann so vor: Sie verfassen den Text und wechseln im Editor in das



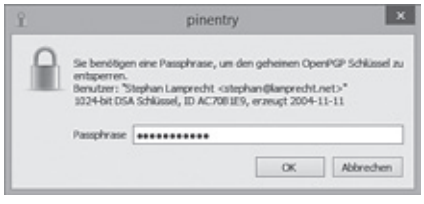
☛ Abb. 18: GPG unterstützt Sie bei der Einrichtung Ihrer Schlüssel. Dazu geben Sie zuerst den Namen und die E-Mail-Adresse ein.



☛ Abb. 19: Durch die Eingabe von zufälligen Zeichen beeinflussen Sie die Schlüsselgenerierung.

☛ Abb. 20: Geschafft! Der öffentliche und private Schlüssel sind angelegt.

Register GPGO. Dort klicken Sie auf „Signieren“ und wählen Ihren eigenen Schlüssel aus. Anschließend geben Sie Ihre Passphrase ein. Beim Verschlüsseln müssen Sie zuerst den öffentlichen **Schlüssel des Empfängers** in Ihre Schlüsselverwaltung **importieren**. Im Editor nutzen Sie dann die Funktion „Verschlüsseln“ und bestätigen den Dialog für das Zertifikat (☛ Abb. 21). ●



☛ Abb. 21: Mit der Eingabe der Passphrase greifen Sie auf Ihren Schlüssel zu.