



Wie man Eindringlinge aussperrt

Sicherheit So schützt man sich vor Datenverlust, wenn das Handy gestohlen wird oder verlorengeht

Von unserem Online-Chef
Marcus Schwarze

Das Handy nimmt mehr und mehr persönliche Daten auf. Umso schlimmer, wenn man es verliert oder es gestohlen wird. Mit unseren Tipps hält sich der Verlust in Grenzen.

1 Codesperre einrichten: Der einfachste Schutz ist die Absicherung durch ein Kennwort oder eine PIN, also eine vierstellige Nummer. Dabei lässt sich hinterlegen, nach wie vielen Minuten die Codesperre aktiviert werden soll – beispielsweise nach fünf Minuten. Auf dem iPhone kann man zudem einstellen, dass die Daten nach zehn Falscheingaben gelöscht werden sollen. So hat ein bössartiger Finder schon einmal eine gewichtige Hürde zu überwinden, falls er an die Daten gelangen möchte.

2 Handydaten auslesen: Notieren Sie sich die eindeutige Seriennummer Ihres Telefons. Dabei handelt es sich um die „IMEI“, die „International Mobile Station Equipment Identity“ – eine 15-stellige Nummer, die weltweit jedes Handy eindeutig kennzeichnet. Auch diese Nummer finden Sie leicht in den Einstellungen des Geräts.

3 Sicherheitskopien anlegen: Nutzer eines iPhones oder Android-Handys sollten das Gerät regelmäßig mit dem Computer verbinden und die Daten synchronisieren. Dabei werden Kontakte, Kalenderdaten und Notizen abgeglichen, ebenso lassen sich die Einstellungen für Mail-Postfächer (ohne die E-Mails selbst), heruntergeladene Apps und zumeist auch deren Inhalte, Klingeltöne, Musik,

Filme, Bücher und Fotos mit dem Rechner synchronisieren. Am PC braucht man fürs iPhone das Programm iTunes, für Android beispielsweise die Software Kies oder MyPhoneExplorer. Darin lässt sich festlegen, wohin die Daten auf dem PC gesichert werden sollen. Auf dem iPhone sollte man auch festlegen, dass das Back-up (die Sicherheitskopie) verschlüsselt ab-

gespeichert wird. Dann ist sie mit einem Passwort abgesichert. Geht das Handy verloren, kann man die Daten so gut wie vollständig auf ein neues Gerät übertragen.

4 Verlorenes Handy orten oder löschen: Geht das Handy verloren, gibt es eine nützliche Funktion zum Wiederfinden. So kann man auf www.icloud.com nachschauen, wo sich das verloren gegangene iPhone befindet – der Ort wird auf einer Landkarte an-

gezeigt, und bei Bedarf kann man es einen Ton abspielen lassen. Auch gelingt über diesen Dienst von Apple das Fernlöschen. Voraussetzung für all das ist, dass man das Handy dafür einmalig einrichtet. Das geht auf dem iPhone unter Einstellungen iCloud. Auch für Android gibt es solche Dienste, beispielsweise die Software „Android Lost“.

5 Software aktuell halten: So lästig es ist: Updates sind stets notwendig, um bekannt gewordene Sicherheitslücken zu schließen. Das gilt für das Betriebssystem des Handys ebenso wie für die darauf aufgespielten Apps. Faustregel: Alle zwei Wochen sollten System und Apps auf den neuesten Stand aktualisiert werden.

6 Sicherheitssoftware: Auf dem iPhone werden Apps von Apple streng geprüft, bei Android ist die Prüfung deutlich laxer. Bössartige Software kann auf beiden Geräten aufgespielt werden. Doch während für den PC Schutzprogramme Pflicht sind, gibt es etwas Ver-

gleichbares fürs iPhone nicht. Wohl aber für Android: Die Zeitschrift „ComputerBild“ nannte vor Kurzem das Programm „Mobile Security“ von Bitdefender besonders empfehlenswert. Es kostet 7,95 Euro im Jahr. Eine gleichnamige kostenlose Software von Avast wurde mit geringen Abstrichen ebenfalls empfohlen. Fürs iPhone gibt es nichts Vergleichbares.

7 Unverschlüsseltes WLAN meiden: Im Urlaub und unterwegs bekommt man gelegentlich die Nutzung eines WLAN angeboten. Wenn dieses jedoch unverschlüsselt agiert, kann der Betreiber Ihre übertragenen Daten mitlesen. Dies sollte man vermeiden.

8 Buchführung über Dienste und Passwörter: Sicherheit am Handy hat auch damit zu tun, für die unterschiedlichen Dienste und Apps unterschiedliche Passwörter zu verwenden. Das wird zwar un bequem in der Handhabung, ist aber hilfreich, wenn einmal einer der Dienste ein Sicherheitsleck hat. In der Praxis hat es sich bewährt, ein Textdokument mit allen Diensten, Nutzernamen und Kennwörtern anzulegen – vorausgesetzt dieses Dokument lässt sich mit einem extra Kennwort verschlüsseln. Entweder vertraut man dafür einem Dienst wie Google Drive, oder man benutzt einen separaten Passwortmanager. Die Billigmethode ist eine E-Mail im eigenen Entwürfe-Ordner des Mailpostfaches, in der die Daten abgelegt werden.

9 Dubiose Quellen meiden: Vermeiden Sie auf dem Handy die Installation von Software aus dubiosen Quellen. Fürs iPhone ist die Gefahr nicht ganz so gravierend, auf Android-Systemen aber kann man Software auch aus anderen Stores als dem von Google installieren. In den Einstellungen von Android-Handys kann man festlegen, dass die „Installation aus unbekannten Quellen“ deaktiviert ist.

10 Verschlüsselte Ordner: Für Profis bieten sich verschlüsselte Dateicontainer auch fürs Handy an. Truecrypt ist eine Anwendung, die am PC verschlüsselte Ordner anlegt. Diese kann man über Dienste wie Dropbox auch aufs Handy übertragen. Um den Ordner dort zu öffnen, braucht man eine Anwendung wie Disk Decipher. Allerdings ist die Handhabung solcher verschlüsselten Container alles andere als simpel. Und die Integration ins Handysystem ist nicht leicht. Hier haben die Handyhersteller noch viel Arbeit zu erledigen.

Kolumne



Marcus Schwarze
über fehlerfreies
Arbeiten am Computer

Der Faktor Mensch ist unberechenbar

Der Unterschied zwischen einer richtigen und einer misslungenen Sache besteht manchmal aus nur wenigen Buchstaben. Da drückt man statt der Datei „Dreyer-an-Merkel-zu-NSA-final.docx“ die Datei „Dreyer-an-Merkel-zu-NSA.docx“ aus, schon nimmt das Unheil seinen Lauf. Die Chefin unterschreibt vertrauensvoll einen Entwurf eines diktierten Schreibens statt die korrigierte Fassung, und ein paar Tage später steht in den Zeitungen und Onlinediensten die peinliche Posse eines vor Rechtschreibfehlern strotzenden Briefes der Ministerpräsidentin an die Bundeskanzlerin.



Natürlich darf so etwas auf ministerpräsidiälem Briefpapier nicht passieren. Doch steht ein Kapitel namens „Versionierung von Word-Dokumenten“ auch nicht im Lehrplan heutiger Abiturienten, Studenten, Pressesprecher oder Journalisten. Im Lehrplan einer Büroleitung vielleicht? Selbst die in bester Sekretariatsorganisation geschulten Büromitarbeiter können nichts ausrichten, wenn der Vorgesetzte oder andere Kreativkräfte an allen Geflogenheiten vorbei ihre Gedanken stets als Mail von unterwegs auf dem Tablet-PC mit samt falschen Anführungszeichen, zu kurzen Gedankenstrichen und anderen Fehlern einbringen. So sind die Menschen. In der Praxis arbeitet man auch 30 Jahre nach der Erfindung von Textverarbeitungsprogrammen vielfach mit hin- und hergesandten E-Mails neuer und alter Versionen eines Dokuments. Man liest isolierte Korrekturhinweise zu Absätzen und Formulierungen. Im eigentlichen Dokument sorgen sie für Verschlimmbesserungen. Übers Handy schaltet sich womöglich der in CC (per Kopie) ins Benehmen gesetzte Fachkollege hinzu, per iPad von der Autobahn gibt vielleicht die Chefin selbst noch ihren vermeintlich verbesserten Senf hinzu. Der eigentliche Akt des Schreibens und Abschickens verliert seinen Autor, seinen Absendeort, sein geistiges Zentrum. Das Internet und die moderne Büroorganisation verheißen uns Fortschritt und neues Denken, neue Arbeitsweisen und Zeitersparnis. Es heißt aber auch Unklarheit, Sprunghaftigkeit, Chaos und Zeitvergeudung. Um wirklich voranzukommen, werden sich am Ende auch der Chef und die Chefin in die großen und kleinen Computerprobleme der Mitarbeiter hineinendenken müssen. Dabei werden sie feststellen, dass selbst modernste Herstellungsprogramme mitsamt Rechtschreib- und Grammatikprüfung für ein altbackenes Ding namens Text noch immer einen Faktor unberücksichtigt lassen: den Faktor Mensch. Der ist mit seinen guten und schlechten Launen, seiner spontanen Unberechenbarkeit und manchen krawalligen Einfällen noch lange nicht auf eine kalte „Prozessigkeit“ eingestellt, wie sie nur in Computersystemen vorkommen kann. Und das ist auch gut so. Was zählt, sind die Inhalte. Worum ging es noch mal in dem Schreiben? Darum, dass Geheimdienste selbst verschlüsselte Dokumente auswerten können. Fangen wir doch erst einmal mit den unverschlüsselten an und machen die richtig; ohne dass sie jemand mitlesen kann.

Serie



Schritt für Schritt ins Internet

Unsere Serie für Einsteiger

Teil 11: Mit dem iPad ins Netz
Teil 12: Passwörter
Teil 13: Verschlüsselungen
Teil 14: Datenverlust

Kompakt

Viele Onlinehändler verlangen Gebühr bei Rechnungskauf

Bestellung Für Kunden lohnt sich ein genaues Hinsehen – Zahlungsfristen sind recht unterschiedlich

Wer im Internet per Rechnung bezahlt, ist zwar gut vor Betrügern geschützt. Viele Händler verlangen für diese Zahlungsweise aber eine Gebühr. Darauf weist die Verbraucherzentrale Nordrhein-Westfalen nach einer Stichprobe bei 100 Onlineshops hin. Gut ein Drittel von ihnen lässt sich den Rechnungskauf bezahlen. Üblich sind dabei Summen von 2 bis 3 Euro, manche Händler nehmen aber auch bis zu 9 Euro. Anderswo hängt die Höhe der Gebühr vom Wert der gekauften Ware ab. Vor allem bei teuren Bestellungen werden dann schnell zweistellige Beträge fällig. Hinzu kommen weitere Schikanen für Rechnungskäufer: So bieten

einige Händler die Möglichkeit erst an, wenn der Kunde schon einmal ohne Probleme bei Lieferung und Bezahlung etwas bestellt hat. Andere begrenzen für Neukunden den maximalen Warenwert beim Rechnungskauf, wieder andere tun das sogar bei Stammkunden: Mehr als 150 oder 250 Euro dürfen per Rechnung gekaufte Waren dann nicht kosten. Zahlen müssen Kunden beim Rechnungskauf in der Regel innerhalb von 14 Tagen: 40 der 100 geprüften Händler setzten diese Frist. Weitere 30 sind großzügiger und geben Verbrauchern sogar einen Monat Zeit. Die restlichen Kandidaten wollen spätestens nach zehn Tagen Geld auf dem Konto sehen.

Laden im Flugmodus

■ **Smartphone.** Wer sein Smartphone im Turbo-Modus aufladen möchte, hängt es ausgeschaltet an die Steckdose. Das kommt aber nicht immer infrage – etwa wenn man Anrufe erwartet oder eine Anwendung nutzen möchte. Wer aber eine gewisse Zeit auf Anrufe, SMS und Datenverbindungen verzichten kann, versetzt das Handy einfach in den Flugmodus. Dann sind alle stromhungrigen Datenverbindungen gekappt, und das Gerät lädt noch einmal schneller, ohne dass es nach Ende des Ladens wieder hochgefahren werden muss.

Text im Foto finden

■ **Skydrive.** Die automatische Texterkennung in Fotos ist seit Ende August Teil von Microsofts Onlinespeicher Skydrive. Direkt neben einem hochgeladenen Bild werden die extrahierten Wörter oder Sätze angezeigt. Mit Windows 8.1 findet Skydrive Text in Fotos auch über die Suche, teilt das Unternehmen mit. Ein An-

wendungsbeispiel von Microsoft: Hat jemand etwa einmal eine Speisekarte abfotografiert, erinnert sich aber später nicht mehr genau an das Gericht, das ihn begeistert hat, gibt er einfach den Namen des Restaurants in die Suche ein und findet so das gesuchte Foto mit der Karte.

Anhang nicht öffnen

■ **Trojaner.** Verbraucher müssen derzeit mit besonders vielen Trojaner-E-Mails rechnen. In den Anhängen vieler verseuchter Mails finden sich etwa fingierte Rechnungen im Zip-Format, die den neugierigen Empfänger zum Öffnen verleiten sollen, warnt die

Verbraucherzentrale Rheinland-Pfalz. Oft handelt es sich auch um frei erfundene Schreiben, die vermeintlich von Rechtsanwälden oder Bezahldiensten stammen. Den Anhang sollte man aber keinesfalls öffnen, sondern die Mails direkt löschen, um sich keine Schadsoftware auf den Rechner zu holen.

Falsche Mitarbeiter

■ **Anrufer.** Betrüger, die sich am Telefon als Mitarbeiter von Microsoft ausgeben, gibt es schon seit einiger Zeit. Sie ängstigen ihre Opfer etwa mit einer vermeintlichen Virusinfektion und drängen ihnen eine „Fernwartung“ gegen Gebühr auf. Nun haben die Anrufer eine neue Masche: Sie lassen ihre unwissenden Opfer selbst Schadsoftware installieren, warnt das Internet Storm Center (ISC), das derartige Netz-attacken überwacht. In der harmloseren Variante nervt das Programm so lange, bis die Opfer eine geforderte „Service-Gebühr“ bezahlen. Im schlimmeren Fall sperrt die Software den Rechner, bis der Nutzer zahlt.

