Bernd Lorenz

Sorgfaltspflichten im Umgang mit Passwörtern

Viele Dienste im Internet verlangen für die Benutzung ein Passwort. Im Umgang mit Passwörtern treffen sowohl die Nutzer als auch die Diensteanbieter Sorgfaltspflichten. Der Beitrag geht der Frage nach, welche Sorgfaltspflichten bestehen. Dazu werden die gängigen Angriffsmethoden und die daraus folgenden Sicherheitsvorkehrungen dargestellt.

1 Einleitung

Ein fahrlässiger Umgang mit Passwörtern kann dazu führen, dass Cracker in einen Dienst im Internet eindringen und Schaden anrichten. Die Brisanz dieses Problems zeigt sich in einer repräsentativen Umfrage der BITKOM: So sollen im Jahr 2012 Zugangsdaten von 8,5 Millionen Internetnutzern ausspioniert worden sein.[1] Bspw. können Cracker beim Online-Banking Geld von fremden Konten abheben. Den Schaden hat gemäß § 675u BGB erst einmal das Kreditinstitut. Der Kunde kann aber gemäß § 675v Abs. 2 BGB zum Schadensersatz verpflichtet sein, wenn er seine Sorgfaltspflichten im Umgang mit Passwörtern verletzt hat. Weiterhin kann ein Arbeitgeber einen Schadensersatzanspruch gegen seinen Arbeitnehmer haben, wenn dieser nicht sorgfältig mit Passwörtern für den Server oder Programme des Betriebs umgeht und so Daten abhandenkommen.

Durch die Verwendung unsicherer Passwörter besteht für die Nutzer auch die Gefahr des Identitätsmissbrauchs.[2] Unter dem Identitätsmissbrauch versteht man das unbefugte Agieren einer Person unter einer Identität.[3] Beim Identitätsmissbrauch übernehmen Cracker die Identität des Nutzers, um dessen Account für Vermögensdelikte oder eine Rufschädigung zu missbrauchen.[4]

Für die Frage der Haftung kommt es maßgeblich darauf an, ob Sorgfaltspflichten im Umgang mit Passwörtern verletzt wurden. Sorgfaltspflichten spielen im Rahmen der Fahrlässigkeit eine zentrale Rolle. Nach § 276 Abs. 2 BGB handelt fahrlässig, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. Wer Sorgfaltspflichten nicht beachtet, haftet für den daraus entstandenen Schaden oder ihn trifft ein Mitverschulden nach § 254 BGB. Insofern stellt sich die Frage, welche Sorgfaltspflichten im Umgang mit Passwörtern bestehen.

1 Presseinformation des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. vom 17.9.2012, URL: http://www.bitkom.org/de/presse/8477_73455.aspx.

2 *Kossel* c`t 24/2012, 132.

3 *Borges/Schwenk/Stuckenberg/Wegener*, Identitätsdiebstahl und Identitätsmissbrauch im Internet, 2011, S. 9 f.

4 Wikipedia, „Identitätsdiebstahl", URL: http://de.wikipedia.org/wiki/Identitätsdiebstahl, abgerufen am 26.1.2013.

RA Dr. Bernd Lorenz

Fachanwalt für IT-Recht, Urheber- und Medienrecht und betrieblicher Datenschutzbeauftragter bei Schulz Tegtmeyer Sozien in Essen

E-Mail: lorenz@st-sozien.de

2 Angriffsmethoden

Die Sorgfaltspflichten im Umgang mit Passwörtern stehen im Zusammenhang mit den Angriffsmethoden der Cracker. Wenn man die Angriffsmethoden der Cracker kennt, kann man daraus Sicherheitsstandards und Sorgfaltspflichten ableiten. Es soll deshalb zunächst ein Blick auf die gängigen Angriffsmethoden geworfen werden. Um an ein Passwort zu gelangen, gibt es im Wesentlichen zwei Möglichkeiten: Angreifer versuchen das Passwort auszuspähen oder versuchen das Passwort durch Ausprobieren zu erraten.

Schadsoftware

Durch Schadsoftware (Malware) wie ein Trojanisches Pferd können Passwörter ausspioniert werden.[5] Dazu wird den Nutzern bspw. eine kostenlose Software im Internet angeboten, die ein Trojanisches Pferd enthält.[6] Es gibt verschiedene Erscheinungsformen von Trojanern:[7] Es kann sich um ein scheinbar nützliches Programm handeln, das geheime Funktionen in sich selbst birgt. Trojaner können aber auch durch den Verbund zweier eigenständiger Programme zu einer einzelnen Programmdatei entstehen. Aber auch schon durch das bloße Anschauen einer speziell präparierten Website kann ein Trojaner heruntergeladen werden (sog. Drive-by-Download[8]). Ohne dass der Nutzer aktiv ein Herunterladen initiiert hat, wird die Schadsoftware im Vorbeisurfen heruntergeladen. Dazu werden Sicherheitslücken im Browser bzw. in

5 *Mack*, IT Sicherheit, 2012, S. 63.

6 *Poguntke*, Basiswissen IT-Sicherheit, 2. Aufl. 2010, S. 168.

7 Wikipedia, „Trojanisches Pferd (Computerprogramm)", URL: http://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm), abgerufen am 26.1.2013.

8 *Eckert*, IT-Sicherheit, 7. Aufl 2012, S. 162; Schimansky/Bunte/Lwowski/*Maihold*, Bankrechts-Handbuch, 4. Aufl. 2011, § 55 Rn. 33; European Network and Information Security Agency, ENISA Threat Landscape, 2012, S. 13, URL: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport; Wikipedia, „Drive-by-Download", URL: http://de.wikipedia.org/wiki/Drive-by-Download, abgerufen am 26.1.2013.

deren Plug-ins wie Java, Adobe Reader und Adobe Flash ausgenutzt. Wenn ein Computer erst einmal mit einem Trojaner infiziert ist, kann dieser unbemerkt im Hintergrund Daten und Passwörter über eine Internetverbindung an Angreifer übermitteln. Eingesetzt werden bspw. Keylogger. Als Keylogger werden Programme bezeichnet, die die Eingaben eines Benutzers an seinem Computer mitprotokollieren.[9] Diese Programme übermitteln jeden Tastenanschlag des Benutzers an den Angreifer.[10] So kann der Angreifer Zugangsdaten von den verschiedensten Diensten einsammeln. Beim Online-Banking werden auch Trojaner eingesetzt, die nach Eingabe der persönlichen Identifikationsnummer (PIN) und der Transaktionsnummer (TAN) die Verbindung des Nutzers zum Kreditinstitut unterbrechen (sog. Abbruch-Trojaner).[11] Die abgefangenen Daten werden über das Internet an den Angreifer gesandt. Dieser kann nach Abbruch der Sitzung die Internetbanking-Anwendung selber mit den ausspionierten Daten starten und Überweisungen durchführen.

Phishing
Beim Phishing (Kurzform für Password Fishing) werden Nutzer auf gefälschte Webseiten gelenkt, auf denen das Passwort ausspioniert wird.[12] Dazu erhält der Nutzer vielfach eine E-Mail, die einen Link auf eine gefälschte Website enthält. Auf dieser gefälschten Website soll der Nutzer dann sein Passwort eingeben. Dabei landet der Nutzer auf einer speziell präparierten Webseite eines Angreifers. Diese gefälschten Webseiten sehen den echten Webseiten oftmals täuschend ähnlich. Phishing wurde früher oftmals eingesetzt, um an Kontodaten von Nutzern zu gelangen. Beim Phishing werden die Nutzer auf eine gefälschte Webseite eines Kreditinstituts geleitet und zur Eingabe ihres Passworts und verschiedener TANs aufgefordert. Nach Angaben des BSI ist Phishing kaum noch feststellbar.[13] Die Täter würden heutzutage vorwiegend mit Trojanern vorgehen.

Pharming
Das Pharming ist eine Weiterentwicklung des Phishings. Beim Pharming werden DNS-Abfragen von Browsern manipuliert, um die Nutzer so auf gefälschte Webseiten zu lenken.[14] Wenn eine Adresse im Browser eingegeben wird, ermittelt dieser über das Domain Name System (DNS) den entsprechenden Server, mit dem er die Verbindung aufbauen soll. Wenn dem Browser eine falsche IP-Adresse und damit ein falscher Server mitgeteilt wird, ist es möglich, den Nutzer auf eine gefälschte Webseite umzulenken (sog. DNS-Spoofing[15]). Dann kann auf der gefälschten Webseite sein Passwort abgefragt werden. Es bestehen zwei Vorgehensweisen: Entweder werden DNS-Server manipuliert oder die Rechner der Nutzer werden mit Hilfe eines Schadprogramms manipuliert.

Cross-Site-Scripting
Auch die Website des Diensteanbieters selbst kann Ziel von Angriffen sein. Mittels Cross-Site-Scripting (XSS) schleusen Angreifer eigenen Code in eine Webseite des Diensteanbieters ein.[16] Hierzu wird regelmäßig die Skriptsprache JavaScript verwandt. Durch den eingeschleusten Code besteht die Möglichkeit, dass die auf der echten Seite eingegebenen Passwörter an den Angreifer übermittelt werden.[17]

Dumpster Diving
Beim Dumpster Diving (auch Bin Diving) durchsuchen Angreifer den Müll von Unternehmen, um so an Zugangsdaten zu gelangen.[18] Dabei nutzen sie den Umstand aus, dass es besonders in großen Unternehmen schwierig ist, den Einsatz von Aktenvernichtern lückenlos zu kontrollieren. So gelangen gelegentlich ungeschrederte Zugangsdaten in den Müll.

Social Engineering
Als Social Engineering (auch Social Hacking) werden zwischenmenschliche Beeinflussungen bezeichnet mit dem Ziel, bei Personen ein bestimmtes Verhalten hervorzurufen wie z.B. die Preisgabe von vertraulichen Informationen.[19] Beim Social Engineering versuchen Angreifer durch Beeinflussung oder Manipulation von Menschen, Sicherheitsregeln und -barrieren zu umgehen.[20] So rufen Angreifer unter falschen Namen bei einem Nutzer an und versuchen unter einem Vorwand an die Zugangsdaten zu gelangen. Menschen sind vielfach von Natur aus hilfsbereit. Das nutzen Angreifer aus, um mit erfundenen Geschichten an Zugangsdaten zu gelangen. Bspw. wird vorgetäuscht, dass ein neuer Mitarbeiter die Zugangsdaten braucht.[21] Beliebt ist es auch, sich als Systemadministrator auszugeben, der die Zugangsdaten für administrative Arbeiten benötigt.[22] Gelegentlich werden auch Mitarbeiter bestochen, um Zugangsdaten auszuhändigen.[23]

Vishing
Beim Vishing (Kurzform für Voice Phishing) handelt es sich um automatisierte Telefonanrufe, in denen versucht wird, an Zu-

9 *Borges* NJW 2005, 3313 [3314]; Langenbucher/Bliesener/Spindler/*Herresthal*, Bankrechts-Kommentar, 3. Aufl. 2013, 5. Kap. § 675l Rn. 66; Wikipedia, „Keylogger", URL: http://de.wikipedia.org/wiki/Keylogger, abgerufen am 26.1.2013.

10 *Kübeck*, Web-Sicherheit, 2011, S. 41.

11 Albrecht/Karahan/Lenenbach/*Koch*, Fachanwaltshandbuch Bank- und Kapitalmarktrecht, 2010, § 25 Rn. 221; *van Gelder*, in: Habersack/Joeres/Krämer, Entwicklungsrichtlinien im Bank- und Kapitalmarktrecht, 2009, S. 55 [60]; Fischer/Klanten/*Koch*, Bankrecht, 4. Aufl. 2010, Rn. 10.468; Raiffeisenbank Sonnenwald eG, URL: http://www.rb-sonnenwald.de/homepage/sicherheit_neu/phishing_warnung.html.

12 Assies/Beule/Heise/Strube/*Richter*, Handbuch des Fachanwalts Bank- und Kapitalmarktrecht, 3. Aufl. 2012, Kap. 3 Rn. 316 ff.; *Borges* NJW 2005, 3313 [3313 f.]; *van Gelder*, s.o. Fn. 11, S. 55 [58 ff.]; *Janowicz*, Sicherheit im Internet, 3. Aufl. 2007, S. 172 f., S. 253 ff.; *Karper* DuD 2006, 215 [215]; *Kübeck*, s.o Fn. 10, S. 36; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 55 Rn. 30; *Poguntke*, s.o. Fn. 6, S. 233; Wikipedia, „Phishing", URL: http://de.wikipedia.org/wiki/Phishing, abgerufen am 26.1.2013.

13 Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2011, S. 14, URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lageberichte2011.pdf?__blob=publicationFile.

14 Assies/Beule/Heise/Strube/*Richter*, s.o. Fn. 12, Kap. 3 Rn. 320 ff.; *Borges* NJW 2005, 3313 [3314]; *van Gelder*, s.o. Fn. 11, S. 55 [60]; Fischer/Klanten/*Koch*, s.o. Fn. 11, Rn. 10.472; *Karper* DuD 2006, 215 [215 f.]; *Janowicz*, s.o. Fn. 12, S. 262; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 55 Rn. 31; Wikipedia, „Pharming (Internet)", URL: http://de.wikipedia.org/wiki/Pharming_(Internet), abgerufen am 26.1.2013.

15 *Borges/Schwenk/Stuckenberg/Wegener*, s.o. Fn. 3, S. 23 f.; *Recknagel*, Vertrag und Haftung beim Internet-Banking, 2005, S. 48 f.; *Werner*, Verkehrspflichten privater IT-Nutzer in Bezug auf die Verbreitung von Schadsoftware, 2010, S. 72 ff.; Wikipedia, „DNS-Spoofing", URL: http://de.wikipedia.org/wiki/DNS-Spoofing, abgerufen am 26.1.2013.

16 *Eckert*, s.o. Fn. 8, S. 174 ff.; *Poguntke*, s.o. Fn. 6, S. 267; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 55 Rn. 35; Wikipedia „Cross-Site-Scripting", URL: http://de.wikipedia.org/wiki/Cross-Site-Scripting, abgerufen am 26.1.2013.

17 *Schmidt*, heiseSecurity 2007, URL: http://www.heise.de/security/artikel/Passwortklau-fuer-Dummies-270910.html.

18 *Kübeck*, s.o. Fn. 10, S. 76.

19 Wikipedia, „Social Engineering (Sicherheit)", URL: http://de.wikipedia.org/wiki/Social_Engineering_(Sicherheit), abgerufen am 26.1.2013.

20 *Lipski*, Social Engineering, 2009, S. 7.

21 *Kübeck*, s.o. Fn. 10, S. 34.

22 *Eckert*, s.o. Fn. 8, S. 26.

23 *Kübeck*, s.o. Fn. 10., S. 76.

gangsdaten zu gelangen.[24] Dabei werden die niedrigen Kosten der Internettelefonie ausgenutzt. In den Telefonanrufen wird versucht, die Angerufenen zur Preisgabe von Passwörtern zu bewegen. Eine andere Variante ist es durch Spam die Nutzer zum Anruf einer Telefonnummer zu bewegen. Beim Rückruf werden über eine Bandansage persönliche Daten abgefragt.

Password Sniffing
Passwörter können durch Password Sniffing ausspioniert werden. Unter Sniffing versteht man das Abhören des Netzwerkverkehrs während einer Kommunikation. Beim Password Sniffing werden Zugangsdaten aus dem abgehörten Netzwerkverkehr extrahiert.[25] Dazu werden Programme eingesetzt (sog. Sniffer), die den Netzwerkverkehr mitlesen und aufzeichnen können.[26] Wenn Passwörter mit einer herkömmlichen E-Mail versandt werden, besteht die Gefahr, dass Dritte die E-Mail mitlesen können, da herkömmliche E-Mails unverschlüsselt übertragen werden. Wenn Passwörter auf einer Webseite eingegeben werden, die keine verschlüsselte Verbindung anbietet, besteht ebenfalls die Gefahr, dass die Passwörter mitgelesen werden. Schließlich besteht bei einem unverschlüsselten WLAN die Gefahr, dass Angreifer, die sich in der näheren Umgebung befinden, den Netzwerkverkehr mitlesen.[27] Mit WLAN-Sniffern lassen sich drahtlose WLAN-Netzwerke auffinden und abhören.[28]

Ausspähen der Terminaleingabe
Möglich ist es auch, dass Angreifer die Eingabe am Terminal ausspähen, indem sie dabei zusehen, wie der Nutzer sein Passwort eingibt. Das Risiko, dass bei der Eingabe am eigenen Computer jemand über die Schulter schaut, ist verhältnismäßig gering.[29] Es kommt allerdings häufiger vor, dass die PIN an Geldautomaten ausspioniert wird[30] (sog. Skimming[31]). Dabei wird durch eine versteckte Mini-Kamera oberhalb der Tastatur oder in der Decke (z.B. in Rauchmeldern) die Tastatur des Geldautomaten gefilmt.

Brute-Force-Attacken
Bei Brute-Force-Attacken werden alle möglichen Zugangsdaten einfach der Reihe nach ausprobiert.[32] Dieser Angriff setzt auf die pure Rechengewalt von Computern.[33] Mit leistungsfähiger Hardware ist es oftmals möglich nach einigen Stunden des Ausprobierens auf gültige Zugangsdaten zu stoßen.[34]

Bei Wörterbuchattacken werden Wörter aus einer Liste ausprobiert.[35] Eine Reihe von Nutzern benutzen leicht zu merkende Wörter oder Namen als Passwort. Bei dieser Methode werden dann die sich aus der jeweiligen Sprache ergebenden sinnvollen Wörter durchprobiert. Manche Nutzer sind dazu übergegangen, die Wörter ein wenig abzuwandeln und bspw. noch Zahlen anzuhängen. Aber auch diese Verschleierungsversuche können spielend durch eine Variation der Wörter geknackt werden.[36]

Zurücksetzen von Passwörtern
Es gibt noch eine ganz andere Möglichkeit als das Ausspionieren oder Erraten von Passwörtern. Angreifer setzen Passwörter von Nutzern zurück.[37] Da es immer wieder Nutzer gibt, die ihr Passwort vergessen haben, bieten die Diensteanbieter die Möglichkeit an, ein neues Passwort zu vergeben. Wenn der Angreifer die Sicherheitsabfragen für das neue Passwort umgehen kann, hat er die Möglichkeit ein neues Passwort für die Benutzerkennung zu erhalten und mit dem neuen Passwort den Dienst zu benutzen. Dies wird allerdings nach einer gewissen Zeit auffallen, weil der eigentlich Berechtigte sich wegen des geänderten Passworts nicht mehr einloggen kann.

Mehrfach verwendete Passwörter
Oftmals verwenden Nutzer für verschiedene Dienste im Internet oder Programme dasselbe Passwort. Dabei besteht die Gefahr, dass wenn bei einer Anwendung das Passwort ausspioniert wird, der Angreifer das Passwort auch bei anderen Anwendungen benutzen kann.[38] Das einmal erlangte Passwort kann der Angreifer nämlich auch bei anderen Anwendungen ausprobieren. Besonders problematisch ist es, wenn das Passwort für den E-Mail-Dienst geknackt wird. Eine Reihe von Diensten im Internet verwendet als Benutzerkennung die E-Mail-Adresse des Nutzers. Wenn der Angreifer im Besitz der E-Mail-Adresse und des Passworts ist, kann er sich auch bei anderen Diensten einloggen, wenn das Passwort bei diesen Diensten identisch ist.

3 Sorgfaltspflichten

Im Folgenden sollen die Sicherheitsstandards dargestellt werden, die einzuhalten sind, um Angriffen vorzubeugen und sie abzuwehren. Eine Pflicht zur Einhaltung von Sicherheitsstandards kann sich im Verhältnis zwischen Diensteanbietern und Nutzern aus § 241 Abs. 2 BGB ergeben.[39] Danach hat jeder Teil Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Teils zu nehmen. Zu den vertraglichen Schutzpflichten gehört es auch, den anderen Teil vor vermeidbaren Schäden zu bewahren.[40] Vor allen Dingen Diensteanbieter sind verpflichtet, ihre Nutzer vor vermeidbaren Angriffen zu schützen. Aber auch die Nutzer selber dürfen die einfachsten Sicherheitsregeln nicht außer Acht las-

24 Assies/Beule/Heise/Strube/*Richter*, s.o. Fn. 12, Kap. 3 Rn. 319; Wikipedia, „Vishing", URL: http://de.wikipedia.org/wiki/Vishing, abgerufen am 26.1.2013.
25 *Kübeck*, s.o. Fn. 10, S. 79.
26 *Mack*, s.o. Fn. 5, S. 16 ff., Wikipedia, „Sniffer", URL: http://de.wikipedia.org/wiki/Sniffing, abgerufen am 3.10.2012.
27 *Eckert*, s.o. Fn. 8, S. 887 f.; *Kübeck*, s.o. Fn. 10, S. 79, 153.
28 Wikipedia, „WLAN-Sniffer", URL: http://de.wikipedia.org/wiki/WLAN-Sniffer, abgerufen am 26.1.2013.
29 *Eckert*, s.o. Fn. 8, S. 211.
30 Bundeskriminalamt, Zahlungskartenkriminalität Bundeslagebild 2011, S. 7 f., URL: http://www.bka.de/nn_233148/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaet__node.html?__nnn=true; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 54 Rn. 122.
31 Wikipedia, „Skimming", URL: http://de.wikipedia.org/wiki/Skimming_(Betrug), abgerufen am 26.1.2013.
32 *Kübeck*, s.o. Fn. 10, S. 76; Wikipedia, „Brute-Force-Methode", URL: http://de.wikipedia.org/wiki/Brute_force, abgerufen am 26.1.2013.
33 *Poguntke*, s.o. Fn. 6, S. 115 f.
34 *Kübeck*, s.o. Fn. 10, S. 76.
35 *Kübeck*, s.o. Fn. 10, S. 77, Wikipedia, „Wörterbuchangriff" URL: http://de.wikipedia.org/wiki/Wörterbuchangriff, abgerufen am 26.1.2013.
36 *Kübeck*, s.o. Fn. 10, S. 77; *Rütten* c't 2/2009, 86.
37 *Bager/Bleich* c`t 24/2012, 136 [137]; *Kübeck*, s.o. Fn. 10, S. 79.
38 *Kübeck*, s.o. Fn. 10, S. 78.
39 Erman/*Graf v. Westphalen*, Bürgerliches Gesetzbuch, 13. Aufl. 2011, § 675l Rn. 19; *Kind/Werner* CR 2006, 353 [354].
40 OLG Hamm, Urteil vom 29.8.2012 – 12 U 52/12, juris Rn. 21; OLG Saarbrücken, Urteil vom 18.10.2011 – 4 U 400/10, NJW-RR 2012, 152 [153]; OLG Stuttgart, Urteil vom 3.11.2010 – 3 U 109/10, NJW-RR 2011, 606 [607]; Palandt/*Grüneberg*, Bürgerliches Gesetzbuch, 72. Aufl. 2013, § 241 Rn. 7.

sen. Wer die ihm zumutbaren Sicherheitsstandards nicht einhält, verletzt seine Sorgfaltspflichten.

3.1 Wahl von Benutzernamen und Passwörtern

Passwörter müssen über eine ausreichende Länge verfügen, damit sie sicher sind. Bei zu kurzen Passwörtern besteht die Gefahr, dass diese schnell durch Brute-Force-Attacken ermittelt werden können. Die Empfehlung des BSI geht dahin, dass Passwörter aus mindestens 8 Zeichen bestehen müssen.[41] Besteht ein Passwort aus 8 Zeichen, dann gibt es ca. 18,5 Billiarden Kombinationsmöglichkeiten. Das ergibt sich daraus, dass es auf einer deutschsprachigen Tastatur 108 verschiedene Zeichen gibt. Selbst wenn der Angreifer die Möglichkeit hat, eine Milliarde Passwörter pro Sekunde auszuprobieren, würde er immer noch ca. 214 Tage benötigen, um alle Kombinationsmöglichkeiten durchzuprobieren.

Wenn ein Passwort nach mehreren Falscheingaben gesperrt wird, können auch kürzere Passwörter ausreichen. Das BSI hält 6 Zeichen für ausreichend, wenn nur Ziffern verwendet können, und das Passwort nach mehreren Falscheingaben dauerhaft oder für eine längere Zeit gesperrt wird.[42]

Grundsätzlich wird man von einer Verletzung der Sorgfaltspflicht des Diensteanbieters ausgehen müssen, wenn dieser nicht sicherstellt, dass die Passwörter seiner Nutzer eine ausreichende Länge haben. Diensteanbieter haben es technisch sicherzustellen, dass die Nutzer keine zu kurzen Passwörter eingeben können. Im Hinblick auf die leichte Angreifbarkeit von Internetdiensten sollten bei Internetdiensten stets achtstellige Passwörter als Mindestlänge vorgesehen werden.[43]

Um Wörterbuchangriffe abzuwehren, darf ein Passwort nicht aus Wörtern oder Namen bestehen. Am sichersten ist es, eine Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen zu verwenden (z.B. g#79K+Rf). Es stellt eine Sorgfaltspflichtverletzung des Nutzers darf, wenn er einfach zu erratende Passwörter wie z.B. seinen Vornamen oder seinen Vornamen mit Geburtsdatum verwendet (z.B. Peter62).

Diensteanbieter im Internet müssen die Nutzer auf die Grundregeln für die Verwendung von sicheren Passwörtern hinweisen und die Passwörter ggf. auf ihre Qualität überprüfen. Mittels spezieller Programme (sog. Password Checker) lässt sich automatisch überprüfen, ob ein Passwort sicher ist. Viele unbedarfte Nutzer verwenden einfach zu erratende Passwörter. Insofern trifft die Diensteanbieter eine Hinweis- und Kontrollpflicht bezüglich der von den Nutzern verwandten Passwörter.

Die Sicherheit kann noch erhöht werden, wenn die Nutzer bei verschiedenen Diensten verschiedene Benutzernamen wählen.[44] So kann verhindert werden, dass ein Angreifer, der einen Benutzernamen kennt, diesen bei anderen Diensten verwendet, um Passwörter auszuprobieren. Kennt der Angreifer den Benutzernamen bei einem Dienst schon nicht, kann er auch keine Passwörter ausprobieren. Allerdings gibt es keine Pflicht verschiedene Benutzernamen zu verwenden. Hierbei handelt es sich nur um eine zusätzliche Sicherheitsmaßnahme.

3.2 Aufbewahren von Passwörtern

Da Passwörter für verschiedene Dienste nicht mehrfach verwandt werden dürfen, ergibt sich eine Vielzahl von Passwörtern, die ein Nutzer zu verwenden hat: das Passwort bzw. die Passwörter für E-Mail-Dienste, das Online-Banking, soziale Netzwerke, Auktionsplattformen, Onlineshops, den Router, das WLAN, Video-on-Demand-Dienste, die PIN für die Bank- und Kreditkarte, für das Handy, für den elektronischen Personalausweis usw. Ein durchschnittlicher Nutzer wird auf mindestens 20 verschiedene Passwörter kommen. Bei einer intensiven Nutzung des Internets können es auch schnell weitaus mehr werden. Bei der Vielzahl der Passwörter ist es aufgrund der dargestellten Anforderungen an ein sicheres Passwort nicht möglich, sämtliche Passwörter auswendig zu lernen und zu behalten. Teilweise wird deshalb empfohlen ein Grundpasswort zu wählen und dies jedes Mal abzuwandeln, indem man ein paar Stellen des Passworts verändert (z.B. a8+tku64, a8+tkgMD, a8+tk2D3 usw.).[45] Bei der Vielzahl der Passwörter wird es jedoch auch nicht möglich sein, sich sämtliche Passwörter zu merken. Aus diesem Grunde kann von den Nutzern nicht verlangt werden, dass sie sämtliche Passwörter auswendig kennen.[46]

Keine Sorgfaltspflichtverletzung liegt vor, wenn der Nutzer sich seine Passwörter aufschreibt und an einem sicheren Ort aufbewahrt. Diesbezüglich sieht § 675l S. 1 BGB für Zahlungsdienste vor, dass der Zahler alle zumutbaren Vorkehrungen treffen muss, um die personalisierten Sicherheitsmerkmale vor unbefugtem Zugriff zu schützen. Die Vorschrift gilt unmittelbar nur für Zahlungsdienste. Der Begriff des Zahlungsdienstes bestimmt sich gemäß § 675c Abs. 3 BGB nach § 1 Abs. 2, 10 ZAG. Zahlungsdienste stellen bspw. das Online-Banking,[47] PayPal,[48] SOFORT Überweisung,[49] ClickandBuy[50] oder andere Online-Zahlungsdienste[51] dar. Die im E-Commerce vielfach angebotene Möglichkeit eines Diensteanbieters, dass der Rechnungsbetrag per Lastschrift abgebucht wird, ist kein Zahlungsdienst. Die Abbuchung vom Konto des Kunden führt nämlich nicht der Diensteanbieter, sondern dessen Kreditinstitut durch. Eine Ausführung von Zahlungsvorgängen i.S.d. § 1 Abs. 2 Nr. 2 ZAG liegt nicht bei einer bloßen Unterstützung der Übermittlung des Zahlungsauftrags oder der Einreichung einer Lastschrift bei einer Inkassostelle vor, wenn der Diensteanbieter nicht selber ein multilaterales Verrechnungssystem betreibt.[52] § 675l S. 1 BGB gilt folglich für den E-Com-

41 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, 12. Ergl. 2011, M2.11, URL: https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf.

42 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, 12. Ergl. 2011, M2.11, URL: https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf.

43 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Sicheres Surfen im Internet – so schützen Sie sich!, 2010 S. 10, URL: http://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/SicheresSurfen.pdf?__blob=publicationFile; a.A. *Rütten* c`t 2/2009, 86 [86] mindestens 10 Zeichen.

44 *Bager/Bleich* c't 24/2012, 136 [137].

45 *Bager/Bleich* c't 24/2012, 136 [137]; *Rütten* c`t 2/2009, 86; *Rütten* c`t 4/2010, 168.

46 Bamberger/Roth/*Schmalenbach*, Kommentar zum Bürgerlichen Gesetzbuch, 3. Aufl. 2012, § 675l Rn. 4; Erman/*Graf v. Westphalen*, s.o. Fn. 39, § 675l Rn. 5; Langenbucher/Bliesener/Spindler/*Langenbucher*, s.o. Fn. 9, 3. Kap. § 675l Rn. 6; Langenbucher/Bliesener/Spindler/*Herresthal*, s.o. Fn. 9, 5. Kap. § 675l Rn. 12; Palandt/*Sprau*, s.o. Fn. 40, § 675l Rn. 2; *Redeker*, IT-Recht, 5. Aufl. 2012, Rn. 880; Säcker/Rixecker/Oetker/*Casper*, Münchener Kommentar zum Bürgerlichen Gesetzbuch, 6. Aufl. 2012, § 675l Rn. 12 f.; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 54 Rn. 75, § 55 Rn. 115.

47 Ellenberger/Findeisen/Nobbe/*Frey*, Kommentar zum Zahlungsverkehrsrecht, 2010, § 675l BGB Rn. 4.

48 URL: https://www.paypal.com.

49 URL: https://www.payment-network.com.

50 URL: http://www.clickandbuy.com.

51 LG Köln, Urteil vom 29.9.2011 – 81 O 91/11, MMR 2011, 815.

52 Bundesanstalt für Finanzdienstleistungsaufsicht, Merkblatt – Hinweise zu dem Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz – ZAG) vom 22.12.2011, Nr. 2 b), URL: http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html.

merce nur eingeschränkt. Gleichwohl erscheint es aber geboten, die Vorschrift auf andere Zugangsberechtigungen analog anzuwenden. Voraussetzung einer analogen Anwendung ist eine planwidrige Regelungslücke bei vergleichbarer Interessenlage.[53] Der Gesetzgeber hat den Umgang mit Zugangsberechtigungen nur für Zahlungsdienste geregelt, sodass eine Regelungslücke besteht. Diese ist auch planwidrig, da der Gesetzgeber es offenbar übersehen hat, eine entsprechende Regelung für andere Zugangsberechtigungen zu schaffen. Schließlich besteht eine vergleichbare Interessenlage. Die Vorschrift des § 675l BGB dient dem Schutz vor Missbrauch von Zahlungsauthentifizierungsinstrumenten. Bei anderen Zugangsberechtigungen besteht gleichermaßen ein Bedürfnis Diensteanbieter vor Missbrauch zu schützen.

Das Aufbewahren einer Bank- oder Kreditkarte zusammen mit der PIN ist in jedem Fall grob fahrlässig.[54] Aus diesem Grunde scheidet das Portmonee zur Aufbewahrung der PIN für die Bank- oder Kreditkarte aus. Grundsätzlich zulässig ist es aber, andere Passwörter auf einem Zettel in einem Portmonee aufzubewahren. In einem solchen Fall muss der Nutzer sorgfältig auf sein Portmonee achten. Lässt jemand sein Portmonee in einem anderen Personen zugänglichen Raum, in einem Fahrzeug oder in einem Einkaufswagen liegen, liegt hierin ein grob fahrlässiges Verhalten.[55] Keine Fahrlässigkeit wird dagegen regelmäßig anzunehmen sein, wenn jemandem das Portmonee aus der Hosentasche oder der eigenen Wohnung gestohlen wird. In einem solchen Fall handelt der Nutzer dann nicht fahrlässig, wenn Dritte die Zugangsberechtigungen nicht in einem Zugriff erlangen können.[56] Fahrlässigkeit liegt deshalb nicht vor, wenn sich der Nutzer nur die Passwörter ohne zusätzliche Angaben wie die Benutzerkennung, den Link zu dem Dienst, den Namen des Dienstes oder Programms aufgeschrieben hat. Wenn der Zettel in einem solchen Fall abhandenkommt, ist der Angreifer zwar im Besitz der Passwörter. Er kennt aber den Dienst und die Benutzerkennung nicht, zu dem das Passwort gehört. Damit wird es dem Angreifer erheblich erschwert, das Passwort einzusetzen. Er wird erst zusätzliche aufwändige Recherchen anstellen müssen. Das gibt dem Nutzer ausreichend Zeit, seine Passwörter nach dem Abhandenkommen des Zettels zu ändern.

Passwörter können auch auf dem Computer abgespeichert werden. Dies sollte aber immer verschlüsselt geschehen, da die Passwörter sonst mittels eines Schadprogramms ausgelesen werden können. Es gibt auch Programme, in denen man all seine Passwörter hinterlegen kann.[57] Man braucht sich dann nur noch das Passwort für ein Programm (sog. Master-Passwort) zu merken.

3.3 Ändern des Passworts

Es können bestimmte Situationen auftreten, in denen der Nutzer verpflichtet ist, sein Passwort zu ändern. Zunächst einmal trifft den Nutzer eine solche Pflicht immer dann, wenn er befürchten muss, dass das Passwort Dritten offenbart wurde.[58] Hierfür genügt schon der Verdacht der Offenbarung, auch wenn noch kein konkreter Missbrauch des Passworts eingetreten ist. Ferner ist der Nutzer zur Änderung seiner Passwörter verpflichtet, wenn sein Computer mit einem Schadprogramm infiziert wurde. Nach dem Entfernen des Schadprogramms hat er unverzüglich alle Passwörter zu ändern, da die Gefahr besteht, dass diese in fremde Hände gelangt sein könnten. Weiterhin übersenden einige Internetdienste bspw. nach einer Anmeldung Passwörter per E-Mail. Herkömmliche E-Mails sind unverschlüsselt und können von Dritten mitgelesen werden. Aus diesem Grunde trifft den Nutzer die Pflicht, per E-Mail versandte Passwörter umgehend zu ändern. Etwas anderes mag nur für Passwörter gelten, die per De-Mail oder E-Postbrief versandt werden. Beide Dienste versenden nur verschlüsselte Nachrichten.

Zu den Sorgfaltspflichten der Nutzer gehört es auch Passwörter ohne konkreten Verdacht des Missbrauchs regelmäßig zu ändern.[59] Wie schon in der Einleitung festgestellt wurde, besteht eine erhebliche Gefahr, dass Passwörter ausspioniert werden. Dabei besteht die Möglichkeit, dass Passwörter ausspioniert werden, ohne dass der Nutzer davon überhaupt Kenntnis erlangt. Das Missbrauchsrisiko kann der Nutzer deshalb nur durch ein regelmäßiges Ändern von Passwörtern minimieren. Die Empfehlungen des BSI und der BITKOM gehen dahin, Passwörter alle drei Monate zu ändern.[60] Bei der Vielzahl der von den Nutzern verwandten verschiedenen Passwörter dürfte dies jedoch einen unzumutbaren Aufwand darstellen. Es ist den Nutzern unzumutbar alle drei Monate 20 oder mehr Passwörter zu ändern. Ausreichend ist es, wenn die Nutzer ihre Passwörter alle ein bis zwei Jahre ändern.[61] Eine Sorgfaltspflichtverletzung eines Nutzers wird man erst dann annehmen können, wenn dieser über einen längeren Zeitraum von ein bis zwei Jahren seine Passwörter nicht ändert. Die Diensteanbieter haben die Nutzer auf die Änderung ihrer Passwörter hinzuweisen und ggf. daran zu erinnern.

Eine andere Frage ist es, ob Passwörter auch für Dienste geändert werden müssen, die der Nutzer nur selten oder nicht mehr benutzt. Bspw. ist es denkbar, dass ein Nutzer sich für einen Dienst im Internet anmeldet, diesen aber dann nicht mehr benutzt. Eine Pflicht des Nutzers Passwörter für nicht benutzte Dienste zu ändern oder eine Löschung des Accounts zu beantragen, gibt es nicht. Allerdings wird man von einer Pflicht des Diensteanbieters ausgehen müssen, den Account nach einer jahrelangen Nichtbenutzung zu deaktivieren. Wenn ein Nutzer einen Account zwei Jahre nicht benutzt hat, ist es Sache des Diensteanbieters den Nutzer vor Missbrauch zu schützen, indem er den Account deaktiviert.

3.4 Zusätzliche Sicherheitsabfragen

Wenn das Passwort mehrfach falsch eingegeben wurde, hat der Diensteanbieter durch zusätzliche Sicherheitsabfragen sicherzustellen, dass es sich nicht um eine Brute-Force-Attacke handelt.

53 *Schmalz*, Methodenlehre für das juristische Studium, 4. Aufl. 1998, Rn. 383 ff.

54 BGH, Urteil vom 5.10.2004 – XI ZR 210/03, NJW 2004, 3623 [3623]; OLG Frankfurt, Urteil vom 19.11.1996 – 17 U 69/96, OLGR Frankfurt, 1997, 6; Ellenberger/Findeisen/Nobbe/*Frey*, s.o. Fn. 47, § 675l BGB Rn. 14.

55 OLG Düsseldorf, Teilurteil vom 26.10.2007 – 16 U 160/04, BKR 2008, 41 [41 f.]; MüKo-BGB/*Casper*, s.o. Fn. 46, § 675l Rn. 10.

56 BGH, Urteil vom 17.10.2000 – XI ZR 42/00, NJW 2001, 286 [287]; Herberger/Martinek/Rüßmann/Weth/*Schwintowski*, juris PraxisKommentar BGB, 6. Aufl. 2012, § 675l Rn. 9.

57 Z.B. KeePass, URL: http://keepass.info; Password Safe, URL: http://passwordsafe.sourceforge.net; SplashID, URL: http://www.splashdata.com/splashid/.

58 *Recknagel*, s.o. Fn. 15, S. 224; *Spindler*, in: Habersack/Joeres/Krämer, Entwicklungsrichtlinien im Bank- und Kapitalmarktrecht, 2009, S. 215 [230].

59 A.A. *Recknagel*, s.o. Fn. 15, S. 224 f.; *Spindler*, s.o. Fn. 58, S. 215 [230 f.]; Hellner/Steuer/*Werner*, Bankrecht und Bankpraxis, 99. Ergl. 2012, Rn. 19/71.

60 Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, 12. Ergl. 2011, M2.11, URL: https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf: Presseinformation des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. vom 28.6.2010, URL: http://www.bitkom.org/de/presse/66442_64365.aspx.

61 *Rütten* c't 4/2010, 168.

Vielfach verbreitet ist der Einbau einer Zeitverzögerung nach mehreren Falscheingaben. Durch eine Zeitverzögerung für einen neuen Versuch kann verhindert werden, dass Angreifer in kurzer Zeit große Mengen an Passwörtern ausprobieren können. Eine andere Methode, um das automatisierte Ausprobieren von Passwörtern zu verhindern, ist der Einsatz von CAPTCHAs (Abk. für Completely Automated Public Turing test to tell Computers and Humans Apart). Ein CAPTCHA beinhaltet eine von einem Menschen zu lösende Aufgabe, aus der sich ein Einmalcode ergibt.[62] Dieser Einmalcode muss zur Vorbeugung gegen automatisierte Angriffe zusätzlich eingegeben werden. Er wird vielfach in Form von Bildern auf dem Bildschirm angezeigt, damit er nicht automatisch ausgelesen werden kann. Weiterhin besteht die Möglichkeit, dass der Diensteanbieter zusätzliche Angaben abfragt, die der Nutzer zuvor hinterlegt hat. Dabei sollte es sich allerdings nicht, um einfache Angaben wie das Geburtsdatum oder den Geburtsort handeln, die sich leicht durch soziale Netzwerke ermitteln lassen. Sinnvoll erscheint es, einen Einmalcode per SMS an eine zuvor hinterlegte Mobilfunknummer zu senden oder einen Einmalcode per Briefpost zu übermitteln.

3.5 Technische Sicherheitsvorkehrungen

Zur wirkungsvollen Abwehr von Trojanern ist der Einsatz eines aktuellen Anti-Virenprogramms selbstverständlich. Der Einsatz eines aktuellen Virenscanners zählt nach heute h.M. zu den Sorgfaltspflichten des Nutzers.[63] Es gibt sogar gute kostenlose Anti-Virenprogramme.[64] Im Hinblick auf die rasante Entwicklung und Verbreitung von Schadprogrammen müssen Anti-Virenprogramme grundsätzlich täglich aktualisiert werden.[65] Der Virenscanner sollte dabei auch eine heuristische Suche unterstützen. Bei einer heuristischen Suche sucht der Virenscanner nach Funktions- und Prozessaufrufen, also verdächtigen Befehlen, die in einem normalen Programm nicht vorkommen und bzw. oder es wird das Verhalten eines Programms analysiert.[66] Durch solche Methoden lassen sich auch unbekannte Schadprogramme entdecken. Ebenso wie ein Virenscanner gehört auch der Einsatz einer Firewall zu den Sorgfaltspflichten des Nutzers.[67]

Diensteanbieter sind verpflichtet die neuste Technik einzusetzen.[68] Sie müssen Sicherheitslücken umgehend durch Updates schließen. Aber auch die Nutzer trifft bei der Verwendung ihres Betriebssystems und Browsers die Pflicht regelmäßige Updates einzuspielen.[69] Einer Infektion mit Trojanern durch Drive-by-Downloads kann man nur durch die Verwendung einer aktuellen Version des Browsers und dessen Plug-ins begegnen. Die Aktualität von Plug-ins lässt sich einfach mit dem Firefox Plug-in-Check überprüfen.[70]

Diensteanbieter und Nutzer trifft gleichermaßen die Pflicht soweit möglich Spam-Filter einzusetzen.[71] Spam-Filter können einen weiteren Schutz vor Phishing-Angriffen bieten. Verdächtige E-Mails werden von vorneherein herausgefiltert und landen in einem extra Ordner. Die Nutzer können dadurch erkennen, dass es sich um massenweise verschickte Spam-Mails handelt, die nicht von ihrer Bank bzw. ihrem Diensteanbieter stammen.

3.6 Verschlüsselung von Passwörtern

Nutzer dürfen Passwörter auf gar keinen Fall unverschlüsselt auf dem Computer speichern. Bei einer Infektion mit einem Trojaner ist es sonst möglich, dass die unverschlüsselt auf der Festplatte gespeicherten Passwörter ausgelesen werden. Bedenklich sind deshalb auch die Passwort Manager verschiedener Browser, die die Passwörter zum Teil unverschlüsselt abspeichern.[72] In dem unverschlüsselten Abspeichern von Zugangsdaten liegt eine Sorgfaltspflichtverletzung.[73] Die verschlüsselte Speicherung ist dagegen zulässig.[74] Aber auch die Diensteanbieter trifft die Pflicht die Passwörter ihrer Nutzer nur verschlüsselt in ihrer Datenbank zu speichern. In der Vergangenheit sind durch Hacker-Angriffe immer wieder massenweise Passwörter gestohlen worden.[75] Dem können Diensteanbieter vorbeugen, wenn sie Passwörter mit einem Salt

62 Vgl. *Borges/Schwenk/Stuckenberg/Wegener*, s.o. Fn. 3, S. 43 f.; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 55 Rn. 25 f.; Wikipedia, „CAPTCHA", URL: http://de.wikipedia.org/wiki/Captcha, URL: abgerufen am 26.1..2013.

63 LG Nürnberg-Fürth, Urteil vom 28.4.2008 – 10 O 11391/07, juris Rn. 36; LG Köln, Urteil vom 5.12.2007 – 9 S 195/07, MMR 2008, 259 [261]; *Blissenbach* jurisPR-BKR 4/2008 Anm. 6; *Borges/Schwenk/Stuckenberg/Wegener*, s.o. Fn. 3, S. 273 f., 284 f.; *Borges* NJW 2012, 2385 [2386]; *Dienstbach/Mühlenbrock* K&R 2008, 151 [154]; Ellenberger/Findeisen/Nobbe/*Nobbe*, s.o. Fn. 47, § 675v BGB Rn. 56 f.; Erman/*Graf v. Westphalen*, s.o. Fn. 39, § 675l Rn. 5, 20; *van Gelder*, s.o. Fn. 11, S. 55 [61, 66]; *Hossenfelder* CR 2009, 790 [793]; Langenbucher/Bliesener/Spindler/*Herresthal,* s.o. Fn. 9, 5. Kap. § 675l Rn. 11; *Mühlenbrock/Dienstbach* MMR 2008, 630 [631]; MüKo-BGB/*Casper*, s.o. Fn. 46, § 675l Rn. 18; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 55 Rn. 134; *Schulte am Hülse/Klabunde* MMR 2010, 84 [87]; *Spindler*, Verantwortlichkeit von IT-Herstellern, Nutzern und Intermediären, 2007, Rn. 295, URL: https://www.bsi.bund.de/cae/servlet/contentblob/486890/publicationFile/30962/Gutachten_pdf.pdf; *Werner* K&R 2008, 554 [555], *Werner*, s.o. Fn. 15, S. 155 ff.; a.A. *Kind/Werner* CR 2006, 353 [355].

64 Z.B. avast! Free Antivirus, URL: http://www.avast.com/de-de/free-antivirus-download; AVG AntiVirus Free, URL: http://free.avg.com/de-de/free-antivirus-download; Avira Free Antivirus, URL: http://www.avira.com/de/avira-free-antivirus/; Windows Defender, seit Windows 8 Bestandteil des Betriebssystems, URL: http://windows.microsoft.com/de-DE/windows-8/windows-defender#1TC=t1.

65 A.A. *Blissenbach* jurisPR-BKR 4/2008 Anm. 6 wöchentlich; *Borges/Schwenk/Stuckenberg/Wegener*, s.o. Fn. 3, S. 273 f., 284 mehrfach täglich; *Dienstbach/Mühlenbrock* K&R 2008, 151 [154 f.] nicht ständig; *Hossenfelder* CR 2009, 790 [792] mindestens wöchentlich; *Meder/Blissenbach* EWiR 2008, 243 [244] wöchentlich; MüKo-BGB/*Casper*, s.o. Fn. 46, § 675l Rn. 18 regelmäßig, aber nicht täglich; *Spindler*, s.o. Fn. 63, Rn. 296, maximal wöchentlich.

66 *Lehner/Hermann* DuD 2006, 768 [769 f.]; *Werner*, s.o. Fn. 15, S. 78.

67 LG Nürnberg-Fürth, Urteil vom 28.4.2008 – 10 O 11391/07, juris Rn. 36; LG Köln, Urteil vom 5.12.2007 – 9 S 195/07, MMR 2008, 259 [261]; Assies/Beule/Heise/Strube/*Richter*, s.o. Fn. 12, Kap. 3 Rn. 356 ff.; *Blissenbach* jurisPR-BKR 4/2008 Anm. 6; Ellenberger/Findeisen/Nobbe/*Nobbe*, s.o. Fn. 47, § 675v BGB Rn. 56 f.; Erman/*Graf v. Westphalen*, s.o. Fn. 39, § 675l Rn. 20; *Hossenfelder* CR 2009, 790 [793]; Langenbucher/Bliesener/Spindler/*Herresthal,* s.o. Fn. 9, 5. Kap. § 675l Rn. 11; MüKo-BGB/*Casper*, s.o. Fn. 46, § 675l Rn. 18; *Schulte am Hülse/Klabunde* MMR 2010, 84 [87]; a.A. *Erfurth* CR 2008, 604 [605]; *Kind/Werner* CR 2006, 353 [355]; *Spindler*, s.o. Fn. 63, Rn. 301; vermittelnd für vorinstallierte Firewall *Mühlenbrock/Dienstbach* MMR 2008, 630 [631]; *Werner* K&R 2008, 554 [555]; *Werner*, s.o. Fn. 15, S. 161 ff..

68 KG, Urteil vom 29.11.2010 – 26 U 159/09, MMR 2011, 338 [339 f.]; Erman/*Graf v. Westphalen*, s.o. Fn. 39, § 675l Rn. 19; Fischer/Klanten/*Koch*, s.o. Fn. 11, Rn. 10.482; *Kind/Werner* CR 2006, 353 [359]; *Spindler*, s.o. Fn. 58, S. 215 [224].

69 LG Nürnberg-Fürth, Urteil vom 28.4.2008 – 10 O 11391/07, juris Rn. 36; LG Köln, Urteil vom 5.12.2007 – 9 S 195/07, MMR 2008, 259 [261]; *Borges* NJW 2012, 2385 [2386]; *van Gelder*, s.o. Fn. 11, S. 55 [66]; *Karper* DuD 2006, 215 [217]; Langenbucher/Bliesener/Spindler/*Langenbucher*, s.o. Fn. 9, 3. Kap. § 675l Rn. 6; MüKo-BGB/*Casper*, s.o. Fn. 46, § 675l Rn. 18; *Spindler*, s.o. Fn. 63, Rn. 303 ff.; a.A. *Erfurth* CR 2008, 604 [605]; vermittelnd für automatische Updates *Mühlenbrock/Dienstbach* MMR 2008, 630 [631]; *Werner*, s.o. Fn. 15, S. 164 ff.

70 URL: https://www.mozilla.org/de/plugincheck/.

71 *Van Gelder*, s.o. Fn. 11, S. 55 [61 f.].

72 *Bager/Bleich* c't 24/2012, 136 [137]; *Eikenberg* c`t 2/2011, 150 [151].

73 *Gößmann/Bredenkamp*, in: Habersack/Joeres/Krämer, Entwicklungsrichtlinien im Bank- und Kapitalmarktrecht, 2009, S. 93 [112]; *Lenz/Schmidt*, Die elektronische Signatur, 2. Aufl. 2004, S. 121; Hellner/Steuer/*Werner*, s.o. Fn. 59, Rn. 19/65 f., 19/126.

74 Langenbucher/Bliesener/Spindler/*Langenbucher*, s.o. Fn. 9, 3. Kap. § 675l Rn. 6; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 55 Rn. 116.

75 Zeit Online vom 12.7.2012, URL: http://www.zeit.de/digital/internet/2012-07/hacker-daten-yahoo.

kombinieren und daraus einen Hash generieren.[76] Gespeichert wird dann nicht das Passwort im Klartext oder ein ungesalzener Hash, sondern der gesalzene Hash, der kaum zu knacken ist.

Diensteanbieter sind verpflichtet Passwörter nur über eine gesicherte und verschlüsselte Verbindung abzufragen. Hierzu wird regelmäßig das Netzwerkprotokoll TLS (früher: SSL) eingesetzt. Nur durch Einsatz einer verschlüsselten Verbindung ist sichergestellt, dass Passwörter nicht durch Password Sniffing ausspioniert werden können. Verschlüsselte Verbindungen können die Nutzer durch den Zusatz https vor dem Domainnamen erkennen.

Nutzer haben dafür Sorge zu tragen, dass sie nur ein gesichertes und verschlüsseltes WLAN verwenden. Nur dadurch kann verhindert werden, dass in der Nachbarschaft befindliche Angreifer Passwörter ausspionieren können. Bei dem WLAN gibt es verschiedene Sicherheitsstandards. Die Sicherheitsstandards WEP und WPA gelten als veraltet und leicht knackbar.[77] Der aktuelle Sicherheitsstandard ist WPA2. Wie der BGH mit Urteil vom 12.5.2012 entschieden hat, ist ein privater Anschlussinhaber nicht verpflichtet ständig aufzurüsten und den neusten Sicherheitsstandard zu verwenden.[78] Privatpersonen müssen nur die zum Zeitpunkt des Kaufs des Routers marktüblichen Sicherungen verwenden. Dies mag als Widerspruch dazu erscheinen, dass die neuste Technik einzusetzen ist. Indes wird man von Privatpersonen nicht verlangen können, dass sie ständig die neuste Hardware kaufen. Eine solche Verpflichtung trifft nur Unternehmen. Gleichwohl sind aber auch Privatpersonen verpflichtet, regelmäßig kostenlose Sicherheitsupdates für das Betriebssystem, den Browser und dessen Plug-ins einzuspielen.

3.7 Benachrichtigung des Diensteanbieters

Es stellt sich die Frage, ob der Nutzer verpflichtet ist, die missbräuchliche Verwendung seines Accounts dem Diensteanbieter anzuzeigen. Ausdrücklich enthält § 675l S. 2 BGB eine solche Verpflichtung für Zahlungsdienste. Es erscheint sachgemäß diese Verpflichtung auf andere Zugangsberechtigungen analog anzuwenden. Zu den Voraussetzungen der Analogie sei auf die obigen Ausführungen zu § 675l S. 1 BGB verwiesen. Wenn ein Nutzer Kenntnis davon, dass sein Passwort für einen Onlineshop in falsche Hände geraten ist, hat er nicht nur das Passwort unverzüglich zu ändern, sondern auch den Shopbetreiber zu unterrichten. So wird der Shopbetreiber vor der Auslieferung von unberechtigten Bestellungen geschützt.

Umstritten ist, ob die Anzeigepflicht bereits durch die konkrete Gefahr einer missbräuchlichen Verwendung ausgelöst wird. Eine Auffassung verweist auf den Wortlaut der Vorschrift, wonach die Anzeigepflicht nur bei einem erfolgten Missbrauch besteht.[79] Danach kann eine Anzeigepflicht nur bei einer entsprechenden vertraglichen Vereinbarung bestehen.[80] Nach zutreffender Ansicht reicht jedoch bereits eine konkrete Gefahr aus.[81] Bei einer konkreten Gefahr ist der Diensteanbieter bereits schutzwürdig, um ihn vor Schaden zu bewahren. Eine bestimmte Form ist für die Anzeige nicht vorgesehen.[82] Sie kann schriftlich, mündlich, telefonisch, per E-Mail, per Telefax oder konkludent erfolgen. Die Anzeige hat unverzüglich, d.h. gemäß § 121 Abs. 1 S. 1 BGB ohne schuldhaftes Zögern, zu erfolgen.[83]

3.8 Aufklärungs- und Warnpflichten

Diensteanbieter treffen Aufklärungs- und Warnpflichten gegenüber den Nutzern. Dies gilt insb. für das Online-Banking.[84] Diensteanbieter müssen die Nutzer auf die Verwendung sicherer Passwörter hinweisen, diese auf ihre Sicherheit überprüfen und unsichere Passwörter ggf. beanstanden. Nach einem erfolgreichen Angriff auf ihren Server müssen Diensteanbieter die Nutzer informieren und zu einer Änderung ihrer Passwörter auffordern.

3.9 Schulung von Mitarbeitern

Insb. Angriffen durch Social Engineering lässt sich in Unternehmen nur durch eine Sensibilisierung und Schulung der Mitarbeiter vorbeugen.[85] Mitarbeiter müssen für Fragen der Datensicherheit und des Datenschutzes sensibilisiert werden. Nur wenn die Mitarbeiter vorher sensibilisiert wurden, dass ein solcher Angriff passieren kann, kann man ihn auch verhindern. Dies ist nach § 4g Abs. 1 S. 1 BDSG vor allen Dingen Aufgabe des betrieblichen bzw. behördlichen Datenschutzbeauftragten.

4 Fazit

Diensteanbieter und Nutzer treffen hohe Sorgfaltspflichten im Umgang mit Passwörtern. Privatpersonen wird viel abverlangt, um einen Missbrauch von Passwörtern vorzubeugen. Wenn aber die vorgenannten Sicherheitsvorkehrungen beherzigt werden, kann man die Missbrauchsgefahr minimieren

76 *Eikenberg* c't 2/2011, 150 [150 f.]; Wikipedia, „Salt (Kryptologie)", URL: http://de.wikipedia.org/wiki/Salt_(Kryptologie), abgerufen am 25.12.2012.

77 *Barnes*, Die Hacker-Bibel: Wireless LANs, 2002, S. 196 ff., 293 ff.; *Beck/Tews*, in: Basin/Capkun/Lee, Proceedings of the second ACM conference on Wireless network security, 2009, S. 79 ff., URL: http://dl.aircrack-ng.org/breakingwepandwpa.pdf; *Cache/Wright/Liu*, Hacking Wireless Exposed, 2. Aufl. 2010, S. 88 ff.; *Eckert*, s.o. Fn. 8, S. 887 ff.; *Edney/Arbaugh*, Real 802.11 Security, 2003, S. 322 ff.; *Tews/Klein*, Attacks on Wireless LANs, 2008, S. 29 ff.; *Tews/Weinmann/Pyshkin*, in: Kim/Yung/Lee, Information Security Applications, 2007, S. 188 ff.

78 BGH, Urteil vom 12.5.2010 – I ZR 121/08, NJW 2010, 2061 Abs. 23 = JurPC Web-Dok. 114/2010 Abs. 24, URL: http://www.jurpc.de/rechtspr/20100114.htm.

79 Bamberger/Roth/*Schmalenbach*, s.o. Fn. 46, § 675l Rn. 6; Ellenberger/Findeisen/Nobbe/*Nobbe*, s.o. Fn. 47, § 675v BGB Rn. 66; Langenbucher/Bliesener/Spindler/*Langenbucher*, s.o. Fn. 9, 3. Kap. § 675l Rn. 12; Palandt/*Sprau*, s.o. Fn. 40, § 675l Rn. 7.

80 Erman/*Graf v. Westphalen*, s.o. Fn. 39, § 675l Rn. 17; Palandt/*Sprau*, s.o. Fn. 40, § 675l Rn. 7; Beispiele bei Hellner/Steuer/*Werner*, s.o. Fn. 59, Rn. 19/138.

81 Ellenberger/Findeisen/Nobbe/*Frey*, s.o. Fn. 47, § 675l BGB Rn. 19; *Karper* DuD 2006, 215 [216]; Langenbucher/Bliesener/Spindler/*Herresthal,* s.o. Fn. 9, 5. Kap. § 675l Rn. 19; MüKo-BGB/*Casper*, s.o. Fn. 46, § 675l Rn. 28; Soergel/*Werner*, Bürgerliches Gesetzbuch, 13. Aufl. 2012, § 675l Rn. 5.

82 Bamberger/Roth/*Schmalenbach*, s.o. Fn. 46, § 675l Rn. 6; Ellenberger/Findeisen/Nobbe/*Frey,* s.o. Fn. 47, § 675l BGB Rn. 21; Erman/*Graf v. Westphalen*, s.o. Fn. 39, § 675l Rn. 16; Langenbucher/Bliesener/Spindler/*Langenbucher*, s.o. Fn. 9, 3. Kap. § 675l Rn. 13; Langenbucher/Bliesener/Spindler/*Herresthal,* s.o. Fn. 9, 5. Kap. § 675l Rn. 21; MüKo-BGB/*Casper*, s.o. Fn. 46, § 675l Rn. 30; jurisPK-BGB/*Schwintowski*, s.o. Fn. 56, § 675l Rn. 4; Palandt/*Sprau*, s.o. Fn. 40, § 675l Rn. 8; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 54 Rn. 92, § 55 Rn. 151; Soergel/*Werner*, s.o. Fn. 81, § 675l Rn. 6.

83 Bamberger/Roth/*Schmalenbach*, s.o. Fn. 46, § 675l Rn. 6; Ellenberger/Findeisen/Nobbe/*Frey,* s.o. Fn. 47, § 675l BGB Rn. 20; Ellenberger/Findeisen/Nobbe/*Nobbe*, s.o. Fn. 47, § 675v BGB Rn. 71; Erman/*Graf v. Westphalen*, s.o. Fn. 39, § 675l Rn. 12, 16; Langenbucher/Bliesener/Spindler/*Langenbucher*, s.o. Fn. 9, 3. Kap. § 675l Rn. 13; Langenbucher/Bliesener/Spindler/*Herresthal,* s.o. Fn. 9, 5. Kap. § 675l Rn. 20; MüKo-BGB/*Casper*, s.o. Fn. 46, § 675l Rn. 32; Palandt/*Sprau*, s.o. Fn. 40, § 675l Rn. 7; Schimansky/Bunte/Lwowski/*Maihold*, s.o. Fn. 8, § 54 Rn. 81, § 55 Rn. 152; Soergel/*Werner*, s.o. Fn. 81, § 675l Rn. 6.

84 Albrecht/Karahan/Lenenbach/*Koch*, s.o. Fn. 11, § 25 Rn. 236; *Karper* DuD 2006, 215 [218]; *Kind/Werner* CR 2006, 353 [356 f.]; *Recknagel*, s.o. Fn. 15, S. 220 f.; *Spindler*, s.o. Fn. 58, S. 215 [226 f.].

85 *Lipski*, s.o. Fn. 20, S. 39 ff.