Das größte und gleichzeitig bekannteste soziale Netzwerk ist mit über einer Milliarde Mitgliedern zweifelsohne Facebook. So viele Vorteile die verschiedenen Online-Communitys bieten – Vernetzung, Ablenkung, Informationen –, so viele problematische Aspekte kann es bei ihrer Nutzung geben. Die meisten davon betreffen den Bereich des Datenschutzes oder der Cyberkriminalität (z. B. Identitätsdiebstahl, Cybermobbing). Die gute Nachricht ist aber, dass die Plattformen immer mehr dem Wunsch und dem Bedürfnis der Nutzerinnen und Nutzer nach mehr Privatsphäre und Kontrolle über ihre eigenen Daten folgen.

Soziale Netzwerke & Dating-Plattformen

Soziale Netzwerke gibt es in allen Farben und Formen und alle funktionieren sie nach einem ähnlichen Prinzip: Bei der Registrierung wird ein – unterschiedlich umfangreiches – Profil erstellt, mit welchem das Netzwerk genutzt wird. Die wichtigsten Angaben sind ein selbst gewählter ***NICKNAME***, ein Foto und weitere persönliche Informationen: Für die Registrierung ist üblicherweise die Angabe des ***KLARNAMENS***, des Geburtsdatums, des Geschlechts und einer gültigen E-Mail-Adresse notwendig. Ist schließlich ein Profil erstellt, gibt es die Möglichkeit, sich auf unterschiedliche Arten mit anderen Userinnen und Usern zu vernetzen. Dies fällt von Netzwerk zu Netzwerk verschieden aus: Bei Facebook können Freundinnen und Freunde hinzugefügt werden („geaddet"), bei Instagram werden selbst geschossene Fotos mit verschiedenen Fotofiltern belegt und geteilt, bei Tumblr werden die Blogs von ausgewählten Mitgliedern verfolgt („gefollowet").

Nutzerinnen und Nutzer sollten sich aber bewusst sein, dass viele dieser Social-Media-Plattformen werbefinanziert sind. Die Nutzung der verschiedenen Netzwerke und anderer Dienste ist nur auf den ersten Blick kostenlos, gezahlt wird mit den eigenen Daten.

Die meisten sozialen Netzwerke können grob in zwei Kategorien unterteilt werden: die eher öffentlichen Netzwerke und die eher privaten Netzwerke. Während bei den Netzwerken der ersten Kategorie (Twitter, Instagram, Tumblr oder Vine) alle Inhalte mehr oder minder komplett öffentlich verbreitet werden, geht es bei Netzwerken der zweiten Kategorie (Snapchat, Messenger-Apps wie WhatsApp, Telegram oder Line) darum, Inhalte nur mit ausgewählten Mitgliedern (friends, followern etc.) zu teilen. Der große Unterschied liegt somit in der Öffentlichkeit des geposteten Inhalts und der Möglichkeit des Zugriffs durch Userinnen und User, die nicht registrierte Mitglieder dieses Online-Dienstes sind. Bei öffentlichen Netzwerken müssen sich die Nutzerinnen und Nutzer bewusst sein, dass die geposteten Inhalte grundsätzlich allen zugänglich sind, außer sie verschicken diese als Privatnachrichten. Facebook ist beispielsweise ein Hybrid-Dienst, der von privaten Nachrichten über komplett öffentliche Postings alles anbietet.

?

Klarname:

Auch Engl. „Realname", ist der tatsächliche Name einer Person, der auch in amtlichen Dokumenten geführt wird.

Nickname:

Name der eigenen virtuellen Identität, im realen Leben mit einem Spitznamen zu vergleichen.

Datenschutz & Privatsphäre

Ob die Teilnahme an sozialen Netzwerken empfehlenswert ist oder nicht, müssen Userinnen und User für sich selbst entscheiden. Manche Menschen verweigern sich Online-Communitys, oftmals, weil sie ihre Daten nicht an die Unternehmen weitergeben wollen oder Angst haben, dass diese missbraucht werden. Auf der anderen Seite gibt es Menschen, die ihr ganzes Leben öffentlich führen: einen Blog über ihre Weltreise betreiben, Fotos von Partys teilen oder aktiv Content posten – und das alles unter ihrem echten Namen. Zwischen Verweigerung und Online-Exhibitionismus gibt es aber auch die Möglichkeit, soziale Netzwerke zu nutzen, ohne das komplette Leben offenzulegen. Viele Nutzerinnen und Nutzer machen von den Communitys Gebrauch, um sich mit anderen zu vernetzen und sich zu informieren, ohne selbst allzu viel preiszugeben. Gemeinhin werden Nutzerinnen und Nutzer, die überwiegend passiv – also nur lesend – teilnehmen, als ***„LURKER“*** bezeichnet.

Besonders die etablierten sozialen Netzwerke erkennen die Datenschutzbedürfnisse ihrer Userinnen und User an und bessern auch regelmäßig nach. Diesbezüglich werden verschiedene Möglichkeiten zum Schutz der Privatsphäre geboten, beispielsweise die Einschränkung des Zugriffs auf ein Profil. Bei vielen sozialen Netzwerken sind die Profile standardmäßig auf „öffentlich“ gestellt, sodass sie über Suchmaschinen gefunden werden können. So können selbst nicht registrierte Userinnen und User ein Profil (oder Teile davon) finden und einsehen. Prinzipiell ist es daher zu empfehlen, das eigene Profil auf „nicht öffentlich“ umzustellen. Es ist dann nur für jene Mitglieder sichtbar, die vorher als Kontakt bestätigt wurden.

Trotz aller Sicherheitsvorkehrungen sollten sich Userinnen und User immer des Risikos bewusst sein, dass sie ihre Daten einem Online-Dienst anvertrauen. Nicht alle Dienste sind so privat, wie sie auf den ersten Blick erscheinen. In der Vergangenheit kamen bei einigen Dienstanbietern immer wieder Sicherheitslücken zutage, die Angriffsfläche für Hackings und Datenklau boten. Ebenso sollten Nutzerinnen und Nutzer berücksichtigen, dass auch bei Postings mit illegalen Inhalten rechtliche Schritte folgen können. Das Internet ist kein rechtsfreier Raum und Tatbestände wie Verhetzung, Rufschädigung, Erpressung oder Stalking sind auch online rechtswidrig. Gerade in jüngster Zeit häufen sich Verurteilungen in Zusammenhang mit rechtswidrigen Postings in sozialen Netzwerken.

Lurker:
(„to lurk“, Engl. lauern, schleichen.) Userinnen und User von sozialen Netzwerken, die nur passiv am Online-Geschehen teilnehmen und kaum aktiv Content produzieren.

Facebook:
Einstellungen > Privatsphäre

Twitter:
Sicherheit und Datenschutz > Privatsphäre

Ask.fm:
Datenschutz

Instagram:
Profil > Privatsphärenschutz

Hasspostings:
Postings mit Inhalten, die unter strafrechtliche Tatbestände wie Verhetzung, Rufschädigung, Ehrenbeleidigung oder üble Nachrede fallen.

Kapitel „Cybercrime“:
S. 68

Facebook

Facebook bietet seinen Userinnen und Usern verschiedene Vorkehrungen, um genau kontrollieren zu können, wer welche Daten einsehen und mitlesen kann. Eine neue Funktion, die Nutzerinnen und Nutzern dabei helfen soll, ist der „blaue Sicherheitsdinosaurier". Mit diesem Sicherheitscheck können die wichtigsten Einstellungen in drei kurzen Schritten vorgenommen werden.

Ganz grundlegend können Mitglieder selbst entscheiden, welche ihrer persönlichen Daten für andere sichtbar sind (Geburtsdatum, Kontaktinformation etc.), ebenso ihre Fotos und Postings. Diese sollten unbedingt auf den Freundeskreis eingeschränkt werden.

Zusätzlich können die Online-Freundinnen und -Freunde in Untergruppen sortiert werden; hier können Nutzerinnen und Nutzer für jeden angelegten Personenkreis („Liste") eigene Regeln erstellen und so zum Beispiel festlegen, dass die Arbeitskolleginnen und -kollegen nicht die Urlaubsfotos sehen, die Familienmitglieder aber schon. Auch gibt es mit der Profilvorschau die Möglichkeit zu überprüfen, wie das eigene Profil aus der Sicht eines anderen Mitglieds aussieht.

Facebook bietet viele verschiedene Anwendungen an (Spiele, Quiz etc.). Diese werden von Drittanbietern betrieben. Um diese Anwendungen nutzen zu können, wird der Zugriff auf die Nutzerdaten verlangt. Teilweise können Drittanbieter auch über Freundinnen und Freunde an die eigenen Daten gelangen. Es empfiehlt sich dringend, diese Option einzuschränken und auch bei den eigenen Anwendungen regelmäßig „auszumisten". Zuletzt sollten Nutzerinnen und Nutzer von Facebook die Markierungsfunktion deaktivieren, sodass sie nicht mehr in Fotos oder Beiträgen markiert – also verlinkt – werden können („getagget").
Zu guter Letzt ein Tipp, der nicht die Sicherheit, aber vielleicht die Nerven schützt: das Blockieren von Spielen und Anwendungen. Keine lästigen Spieleeinladungen von anderen Facebook-Userinnen und -Usern mehr!

Die wichtigsten fünf Tipps für mehr Privatsphäre auf Facebook:

- → ***Sichtbarkeit:*** *Postings und Fotos sollten nicht für die Öffentlichkeit freigeschaltet werden; Gruppen für verschiedene Inhalte verwenden (z. B. Familie, Arbeit etc.).*
- → ***Persönliche Informationen:*** *Möglichst wenige persönliche Informationen*

YouTube:
beim eigenen Kanal das hochgeladene Video auswählen, Upload bearbeiten > Datenschutzeinstellungen

Xing:
Einstellungen > Privatsphäre

Vine:
Profil bearbeiten > Einstellungen > Dein Content

Linkedin:
Konto & Einstellungen > Datenschutz & Einstellungen > Prüfen

Sicherheits-Check auf Facebook:
Privatsphäre-Verknüpfungen > Überprüfung der Privatsphäre

Facebook: Einstellungen > Chronik und Markierungen > Anzeigen aus der Sicht von > Person, aus deren Sicht das eigene Profil angezeigt werden soll, auswählen.

preisgeben, Adresse- und Kontaktdaten sollten tunlichst nicht veröffentlicht werden; zumindest eine leichte Abwandlung des eigenen Klarnamens sollte verwendet werden (z. B. Kathi Müller statt Katharina Müller).

- → ***Anwendungen blockieren:*** *Drittanbieter verlangen Zugriff auf persönliche Daten und können diese auch über die eigenen Freundinnen und Freunde sammeln – diese Möglichkeit sollte unbedingt deaktiviert werden.*
- → ***Suchmaschinen:*** *Das Profil auf „privat" schalten, sodass es nicht in den Ergebnissen von Suchmaschinen auftaucht.*
- → ***Profilvorschau nutzen:*** *Das Profil aus der Sicht von befreundeten Nutzerinnen und Nutzern ansehen, um sicherzugehen, dass nur die gewünschten Informationen einsehbar sind.*

Facebook: Einstellungen > Apps > Von anderen Nutzern verwendete Apps > alle Optionen abwählen

Facebook: Einstellungen > Chronik und Markierungen

Anwendungen blockieren: Einstellungen > Blockieren > Anwendungen blockieren

Kontaktbörsen & Dating-Portale

„Drum prüfe, wer sich ewig bindet": Online-Dating-Plattformen sind die Kontaktanzeigen der digitalen Welt. Hatten sie früher ein negatives Image und waren lediglich ein Nischenprodukt, so sind sie heute in der breiten Öffentlichkeit angelangt und werden stark genutzt. Online-Dating scheint in unserer vernetzten Welt immer mehr die Partnersuche der Zukunft zu sein. Mittlerweile sind Dating-Plattformen ein umsatzstarkes Geschäft, so verzeichnete beispielsweise das größte Portal im deutschsprachigen Raum, Parship, im Jahr 2013 über 50 Mio. Euro Umsatz.

Weitere Tipps für Sicherheitseinstellungen auf Facebook und in anderen Netzwerken:

www.saferinternet.at/privatsphaere-leitfaeden

Besonders mobile Dating-Apps boomen derzeit. Die bekanntesten Beispiele sind Tinder und Lovoo. Diese basieren auf dem Prinzip der standortbezogenen Dienste, die unter Zuhilfenahme von positionsabhängigen Daten arbeiten ***(„GEOSOCIAL NETWORKING")*** – also beispielsweise Singles in geografischer Nähe anzeigen.

Geosocial Networking:

Soziale Netzwerke, die mit standortbezogenen Daten arbeiten.

Im (Online-)Geschäft mit der Liebe gibt es spezialisierte Plattformen für besondere Zielgruppen. So können zum Beispiel Singles in geografischer Nähe, für Seitensprünge oder speziell Singles mit hohem Bildungshintergrund gesucht werden. Auch Plattformen, die sich an Minderjährige richten, gibt es mittlerweile nicht wenige.
Beim Online-Dating gilt wie im echten Leben: lieber Vorsicht als Nachsicht. Denn viele Dating-Plattformen locken mit Gratismitgliedschaften (***„FREEMIUM"***), jedoch sind nur sehr wenige Funktionen bei diesen Gratisprofilen inkludiert (beispielsweise ist die Kontaktaufnahme mit anderen Mitgliedern blockiert). Dadurch wollen die Plattformen Userinnen und User zu den vollen und oftmals kostenpflichtigen Mitgliedschaften drängen. Nicht

Teenager & Dating-Plattformen:

Siehe Kapitel „Kinder und Medien", S. 91

selten finden sich in den Geschäftsbedingungen solcher Plattformen lange Laufzeiten für die Mitgliedschaft, kostenpflichtige Abos oder Klauseln zur automatischen Verlängerung. Daher sollten unbedingt die AGB, aber speziell die E-Mails, die im Zuge der Registrierung von den Plattformen versandt werden, aufmerksam gelesen werden. Oftmals sind in diesen Hinweise auf Laufzeiten oder Kosten enthalten.

Immer wieder werden die undurchsichtigen Vertragsbedingungen bei Online-Partnerbörsen oder deren zweifelhafte Praxis im Hinblick auf Widerruf und Kündigung von Verbraucher- und Konsumentenschutz kritisiert. So ist bei manchen Plattformen eine Kündigung auch dann nicht möglich, wenn die Userinnen und User bereits die „große Liebe" über die Plattform gefunden haben.

Manche Plattformen arbeiten auch mit „Köderkontakten". Hier werden neue Mitglieder von fiktiven oder eigens für solche Dienste engagierten Mitgliedern kontaktiert (sogenannten ***„DATE-BAITS"***), die sie in ein Abo locken oder zu einer Verlängerung der Mitgliedschaft motivieren sollen.

Versteckte AGB

Einige wenige Social-Media- und Dating-Plattformen machen sich durch extremere Werbemaßnahmen unbeliebt: Userinnen und User erhalten E-Mail-Einladungen zum Plattform-Beitritt von ihren eigenen Bekannten oder bekommen Benachrichtigungen, dass ihnen eben jene Bekannte über diese Plattform Nachrichten geschickt hätten. Geübte Nutzerinnen und Nutzer erkennen diese E-Mails auf den ersten Blick als Spam und Ködernachricht, doch nicht wenige fallen auf diesen Trick herein und melden sich bei der Plattform an, um die angeblich dort abrufbaren Nachrichten lesen zu können – und hier beginnt der Teufelskreis.

Denn in den AGB zum Datenschutz schreibt eine dieser Plattformen, dass ein Tool zum Import der privaten Kontakte angeboten wird. Dieses Tool ist fixer Bestandteil des Anmeldeprozederes, allerdings nicht sehr benutzerfreundlich, sodass viele unbeabsichtigt dem Import ihrer Adressbücher zustimmen. Daraufhin beginnt die Plattform, an alle Kontakte aus den Adressbüchern E-Mails mit Einladungen und Erinnerungen zu schicken. Die AGB enthalten zusätzlich eine Klausel, in der festgehalten ist, dass das Mitglied durch den – wenn auch unbeabsichtigten – Import der Kontakte zustimmt, dass das Netzwerk diesen Kontakten Einladungen und anderes zuschicken darf.

?

Freemium:

(Kombination aus „free", Engl. gratis, und „premium", Engl. Belohnung.) Geschäftsmodell, bei dem Basisprodukte oder -funktionen kostenlos sind, die Vollversion bzw. deren Freischaltung ist jedoch kostenpflichtig.

?

Date-Baits:

(Engl. Date-Köder.) Von Dating-Plattformen engagierte Personen, die Mitglieder in eine (kostenpflichtige) Mitgliedschaft locken sollen.

Ausstieg & digitale Leichen

www.justdelete.me:
Informiert über die Möglichkeiten, Konten bei verschiedenen Online-Diensten zu löschen.

Irgendwann kommt der Punkt, an dem Userinnen und User die sozialen Netzwerke oder Online-Communitys verlassen möchten oder diese einfach nicht mehr nutzen. Ist das der Fall, sollte unbedingt der Account deaktiviert und gelöscht werden. Somit werden nicht nur unnötige „digitale Leichen" verhindert, sondern auch die Daten beim jeweiligen Dienst gelöscht.
Ein angelegtes Profil oder Konto zu löschen, ist von Plattform zu Plattform unterschiedlich einfach oder kompliziert. Manche der Online-Dienste stellen Kontaktformulare bereit, andere haben „Lösch-Buttons". Wiederum andere machen es registrierten Userinnen und Usern möglichst schwer, indem sie die Kontolöschfunktionen gut verstecken und auf den ersten Blick nicht auffindbar machen. Die Absicht hierbei ist, die Userinnen und User zum Aufgeben zu bewegen. Schließlich werben die Online-Dienste mit ihren hohen Mitgliederzahlen nicht nur neue Mitglieder an, sondern können dadurch auch die Werbeeinnahmen erhöhen. Üblicherweise können die Informationen über die Löschung aber in den FAQ oder in den AGB gefunden werden. Ist dies nicht der Fall, kann eine kurze Internetsuche nach dem Namen des Online-Dienstes und den Begriffen „Konto" und „löschen" gut weiterhelfen. Die Wahrscheinlichkeit ist groß, dass viele andere Mitglieder diese Frage bereits gestellt und beantwortet bekommen haben. Ansonsten ist die Webseite justdelete.me eine gute Anlaufstelle. Hier werden Informationen über die verschiedenen Löschabläufe der beliebtesten Online-Dienste gesammelt.

Manche Dienste haben keine standardisierten Verfahren und auch keine Informationen zur Kontolöschung, führen sie aber auf Anfrage beim Kundensupport durch (z. B. Ask.fm). Registrierungen bei Diensten wie Picasa oder YouTube, die über das zentrale Google-Konto laufen, können oftmals nicht einzeln gelöscht werden, da hierfür das Hauptkonto von Google gelöscht werden müsste. Bei Facebook ist der Löschvorgang etwas komplizierter. In einem ersten Schritt muss der Account unter den Kontoeinstellungen deaktiviert werden. Soll das Konto dauerhaft gelöscht werden, muss im Menüpunkt „Hilfe" nach „Wie kann ich mein Konto dauerhaft löschen?" gesucht werden. In der Erklärung findet sich ein Link, der zum Netzwerk-Ausgang führt. Allerdings wird das Konto vorerst für 14 Tage stillgelegt, sodass die Userinnen und User wiederkehren können. Erst nach dieser zweiwöchigen Frist wird das Konto dauerhaft gelöscht. Der Löschvorgang der Daten dauert anschließend noch 90 Tage.

Facebook-Konto löschen:
Account deaktivieren > unter „Hilfe" nach „Konto löschen" suchen > Link folgen

Reißen alle Stricke, gibt es noch die Möglichkeit, die eigenen Daten manuell zu löschen und die Benutzerdaten dahingehend zu ändern, dass die eigene Identität nicht mehr nachvollziehbar ist. So können nicht löschbare Daten verschleiert und unkenntlich gemacht werden.

Berufswelt und soziale Netzwerke

Das Privat- und das Berufsleben verschmelzen immer mehr, die Übergänge sind oftmals fließend. Auch nach Ende des regulären Arbeitstages beantworten Berufstätige ihre E-Mails, genauso wie während der Arbeitszeit das eine oder andere Mal etwas auf Facebook gepostet oder ein Flug für den nächsten Urlaub gebucht wird. Umso wichtiger ist es aber, den beruflichen und den privaten Internetauftritt voneinander zu trennen. Unprofessionelles Online-Verhalten kann für die berufliche Zukunft ein nicht geringes Hindernis sein, schlimmstenfalls kann es einen den zukünftigen genauso wie den aktuellen Job kosten. In diesem Zusammenhang sollten sich Arbeitnehmerinnen und -nehmer über die Richtlinien bezüglich der Verwendung des Internets am Arbeitsplatz in ihrem Unternehmen informieren. Diese Richtlinien legen genau fest, was im Unternehmen erlaubt und was ein No-Go ist.
Viele Unternehmen haben außerdem auch ***SOCIAL-MEDIA-RICHTLINIEN***. Je nach Branche und Unternehmenskultur ist es beispielsweise angebracht oder unangebracht, mit der Chefin auf Facebook befreundet zu sein oder während der Arbeitszeit den Kollegen mit der Frage anzutwittern, ob er was vom Bäcker haben will. Besonders das „Ventilieren" im Internet, also das Schimpfen über Chefs oder die werte Kollegenschaft, kann gefährlich werden und im schlimmsten Fall zu einer Verwarnung oder auch zur Kündigung führen. Arbeitnehmerinnen und Arbeitnehmer sollten sich besonders mit negativen Äußerungen oder dem Preisgeben von – durch das Geschäftsgeheimnis geschützten – internen Abläufen zurückhalten. Für Internetnutzerinnen und -nutzer in Österreich gilt österreichisches Recht, ein strafrechtlicher Tatbestand wie Ehrenbeleidigung oder ein zivilrechtlicher Tatbestand wie Kreditschädigung kann auch durch Postings in Social Media erfüllt werden.

Social-Media-Richtlinien:

Von Unternehmen erstellte Richtlinien für die Angestellten, die das Verhalten in und die Nutzung von sozialen Netzwerken während der Arbeitszeit festlegen.

Strafbare Postings:

Siehe Kapitel „Cybercrime", S.65

Bewerben & Internet

ISPA Studie „Mein Ruf im Netz“:
www.ispa.at/studien

In der ISPA Studie „Mein Ruf im Netz – Auswirkungen auf die berufliche Zukunft“ aus dem Jahr 2014 gaben die knapp 300 befragten Personalverantwortlichen an, dass sie in 47 Prozent der Fälle das Internet im Verlauf eines Bewerbungsverfahrens zur Recherche verwenden. Besonders oft kommt das in der IT-, Kommunikations- und der Finanzbranche vor. Zusätzlich gaben 81 Prozent der befragten Personalverantwortlichen an, dass die Online-Präsenz von Bewerberinnen und Bewerbern in Zukunft noch an Bedeutung gewinnen wird. In diesem Sinne ist es wichtig, auf den eigenen Online-Auftritt zu achten und das Internet gezielt als Jobmotor zu nutzen.

Business-Netzwerke:
Dienen der beruflichen Vernetzung und der Präsentation der eigenen Person als Fachkraft; funktionieren wie soziale Netzwerke.

www.xing.at
www.linkedin.com

Eine aktuelle und gepflegte Webpräsenz – ob eine eigene Webseite oder „nur“ ein Profil in ***BUSINESS-NETZWERKEN*** – kann gezielt als Unterstützung für die Bewerbung und die Repräsentation nach außen gesehen werden. Jedoch sollten die Daten regelmäßig aktualisiert werden, da ein vernachlässigter Webauftritt keinen professionellen Eindruck hinterlässt. Profile in Business-Netzwerken bieten die Möglichkeit, sich geschäftlich zu vernetzen, nach interessanten Stellen Ausschau zu halten oder selbst als potenzielle Arbeitskraft gefunden zu werden.

Alert-Dienst:
Der wohl bekannteste Alert-Dienst ist der Google-Alert. Ein Alert-Dienst ist ein Informationsdienst, der per E-Mail-Benachrichtigung oder RSS informiert, wenn neue Ergebnisse zu einem vorher festgelegten Schlagwort, Namen oder sonstigen Abfragekriterien auftauchen.

Es empfiehlt sich außerdem, regelmäßig eine Suche nach sich selbst im Internet durchzuführen. Somit können rechtzeitig Schritte eingeleitet werden, falls etwas Nachteiliges im Internet zu finden ist, beispielsweise (unvorteilhafte) Fotos der eigenen Person, die ohne Zustimmung veröffentlicht wurden. Eine weitere Möglichkeit ist, einen ***ALERT-DIENST*** für den eigenen Namen einzurichten. Er informiert, wenn der eigene Name im Internet auftaucht. Somit können böse Überraschungen – beispielsweise beim Bewerbungsgespräch – vermieden werden.

Bei einem Bewerbungsgespräch sollte heutzutage damit gerechnet werden, dass sich die Personalverantwortlichen unter Umständen im Internet schlau gemacht haben und Fragen zum Online-Auftritt stellen, vor allem, wenn die Profile in Online-Netzwerken öffentlich sind oder der eigene Klarname statt eines Pseudonyms oder Nicknames verwendet wird. Die Personalverantwortlichen wollen sich oftmals nur einen allgemeinen Eindruck von den Bewerberinnen und Bewerbern, ihrer Persönlichkeit, ihrem Internetverhalten oder auch der Internetkompetenz verschaffen.

Das berühmte „Partyfoto“ kann potenzielle Arbeitgeber abschrecken und Postings über den ehemaligen „dummen Chef“ zeigen nicht nur unprofessionelles Verhalten, sondern auch fehlendes Bewusstsein für den eigenen Online-Auftritt – und beide können im Internet weite Kreise ziehen. Die geringste Konsequenz ist die eines negativen Ersteindruckes. Umso wichtiger ist es, über das eigene Auftreten im Internet informiert zu sein und es aktiv zu gestalten!

Tipps für einen professionellen Internetauftritt:

- → ***Suche nach sich selbst:*** *Mittels Suchmaschinen regelmäßig nach sich selbst zu suchen hilft, den Überblick über den eigenen Online-Auftritt zu behalten, und gibt die Möglichkeit, sofort entsprechende Maßnahmen zu setzen, wenn „überraschende“ Einträge auftauchen.*
- → ***Alert-Dienst:*** *Online-Dienst, der Benachrichtigungen schickt, wenn der zuvor eingestellte Suchbegriff (z. B. der eigene Name) im Internet auftaucht.*
- → ***Pseudonyme:*** *Bei sozialen Netzwerken, die überwiegend privat genutzt werden, empfiehlt es sich nicht, den eigenen Klarnamen zu verwenden, sondern ein Pseudonym oder einen Nickname.*
- → ***Privatsphäre-Einstellungen:*** *Möchten Bewerberinnen und Bewerber verhindern, dass ihre privaten Fotos oder Postings von potenziellen Chefs gefunden werden, sollten sie unbedingt ihre Profile und Fotos auf „privat“ schalten.*
- → ***Business-Netzwerke:*** *Ein Profil in einem Business-Netzwerk ist die wichtigste Plattform zur Präsentation der eigenen Person als qualifizierter Fachkraft, zusätzlich gibt es Möglichkeiten, Networking zu betreiben und sich mit anderen auf professioneller Ebene zu vernetzen.*

Achtung:

Es gibt vereinzelte Erfahrungsberichte von Bewerberinnen und Bewerbern, die beim Bewerbungsgespräch gezielt nach ihrem Auftritt in sozialen Netzwerken befragt wurden, teilweise sollten sie sogar den Nutzernamen preisgeben, unter dem sie beispielsweise auf Facebook zu finden sind. Derartige Praktiken sind fragwürdig. In einem extremen Fall wurden sogar die Zugangsdaten zu den Social-Media-Konten verlangt, damit diese während des Bewerbungsgesprächs live „überprüft“ werden konnten. Solche Fragen sind unzulässig, da die Informationen dem privaten Bereich der Bewerberinnen und Bewerber angehören und zudem nicht mit der Arbeitsstelle in direktem Zusammenhang stehen.