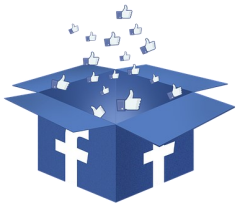
IT-Sicherheitstipp Nr.2 – April 2019

Umgang mit Social Media



Was bedeutet Social Media?

Mit der Entwicklung des Internets stiegen das Interesse und die Bereitschaft der Nutzenden, selbst Inhalte im Netz bereitzustellen. Dies muss nicht immer auf einer eigenen Website sein. Oft ist es einfacher, Fotos, Erlebnisse oder Kommentare auf Internetseiten zu veröffentlichen, die technisch von Dritten dafür gepflegt und angeboten werden.

Dabei besteht häufig die Möglichkeit, die von anderen veröffentlichten Daten zu kommentieren oder sogar weiterzuentwickeln. Daher der Name „Social Media“.

Bekannte Social Media–Dienste:
(aktive Nutzeranzahl in Deutschland)

- WhatsApp (46 Mio.)
- Facebook (32 Mio.)
- XING (15 Mio.)
- LinkedIn (13 Mio.)
- Instagram (10 Mio.)
- Skype (9 Mio.)
- Facebook Messenger (9 Mio.)
- Snapchat (6 Mio.)
- YouTube (6 Mio.)
- iMessage (5 Mio.)
- Twitter (2,5 Mio.)
- Google+ (wird abgeschaltet)

Typische Social Media-Dienste

Eine Vielzahl sogenannte Messenger-Dienste wie z.B. WhatsApp oder Snapchat dienen dem spontanen Austausch von kurzen Nachrichten und Fotos, meist per Smartphone.

Die meisten Social Media-Dienste sind kostenfrei und die Anmeldung ist schnell erledigt (die Abmeldung jedoch oft nicht!).
Der Reiz des Internets besteht heute nicht nur darin Informationen abzurufen, sondern auch darüber zu kommunizieren.

Geschäftsmodell bei Social Media

Das Betreiben der technischen Plattformen für Social Media-Dienste kostet Geld. Da diese aber meist kostenfrei angeboten werden, finanzieren sich die Betreibenden über Spenden (z.B. Wikipedia) oder über Werbung (z.B. Facebook).

Die Werbenden sind aber nur an der Finanzierung der Plattformen interessiert, wenn sie einen wirtschaftlichen Vorteil erhalten. Dieser besteht, neben der Möglichkeit Werbung zu platzieren, meist darin, Nutzerdaten der Besucherinnen und Besucher zur Auswertung zu erhalten, um noch gezielter zu werben.

Gefahren:

- Phishing
- Accountmissbrauch
- Datenschutzaspekte
- Urheberrecht
- Meinungsblasen „Social Bots“
- Bedenken Sie immer: „Das Internet vergisst nie!“
- Cyber-Stalking
- Gefälschte Online-Identitäten

Probleme bei Social Media

Bei der Nutzung von Social Media-Diensten fällt eine Vielzahl von nutzerbezogenen Daten an, die für die Werbung interessant sind.

Beim Besuch von Social Media-Angeboten Dritter wird häufig auf Ihrem Computer oder Smartphone ein "Cookie" (eine kleine Textdatei) hinterlassen, der vom Betreibenden der Seite, aber auch von Dritten, wieder ausgelesen werden kann. Über Cookies, die manchmal jahrelang gespeichert werden, ist es leicht möglich, das Surfverhalten der Besucherinnen und Besucher nachzuvollziehen.

Bei geschickter Nutzung der Cookies und anderer Daten, die Sie im Internet veröffentlichen oder unbewusst hinterlassen, besteht so die Gefahr, dass Dritte erkennen, wo Sie wie lange gesurft haben, was Sie kaufen möchten, wo Sie wohnen oder welche Hobbys Sie haben. Dies kann wiederum auch dafür genutzt werden, Sie als Angriffsziel für das sogenannte Social Engineering auszuwählen.

Wer viel über Sie weiß, dem werden Sie auch schneller vertrauen!

Social Media sicher nutzen

Die Möglichkeiten, Social Media so zu nutzen, dass möglichst wenig personenbezogene Daten übertragen werden, sind derzeit eingeschränkt. Viele der Dienste leben davon, dass die Nutzerinnen und Nutzer persönliche Daten offenbaren.

Falls Sie nicht auf Social Media verzichten wollen, gibt es mehrere Möglichkeiten, für mehr Sicherheit zu sorgen:

- Verwenden Sie nicht Ihren echten Namen (dies lassen allerdings nicht alle Anbieter zu)
- Ändern Sie die Einstellungen, dass nicht alle, sondern nur Ihre Bekannten Ihre Daten einsehen können
- Stellen Sie nur Informationen ein, die Sie auch einer völlig fremden Person erzählen würden und die Sie nie mehr löschen wollen - auch nicht in 10 Jahren
- Löschen Sie regelmäßig die Cookies in Ihrem Browser
- Nehmen Sie nur Freundschaftsanfragen an, wenn Sie sicher sind, wer anfragt
- Verwenden Sie ein sicheres Passwort
- Die meisten Browser erlauben "privates Surfen", bei dem z.B. Cookies beim Schließen gelöscht werden - nutzen Sie diese Funktion!

Weitere Tipps:

Reden Sie miteinander: Eine Unterhaltung ist keine Einbahnstraße. Nur im Miteinander nutzen Sie Social Media so wie es sein sollte. Gestalten Sie aktiv mit, gehen Sie auf die Meinung anderer ein.

Dienst bleibt Dienst: Verwenden Sie keine nicht genehmigten sozialen Medien um dienstliche Inhalte mit Kolleginnen und Kollegen oder Kundinnen und Kunden zu tauschen. Veröffentlichen Sie keine Informationen, die Ihnen im beruflichen Umfeld bekannt wurden. Im Zweifelsfall schreiben Sie lieber einen Satz zu wenig als ein Wort zu viel.

Denken Sie langfristig: Spontanität ist schön, aber denken Sie daran, dass Inhalte, die Sie im Internet veröffentlichen, sich Ihrem direkten Einfluss entziehen. Veröffentlichen Sie nicht alles, was in der Situation gerade unterhaltsam erscheint. Partybilder können zum Beispiel auch von Kolleginnen und Kollegen gesehen werden. „Posten“ Sie nur das, was Sie auch nach Jahren noch sehen und lesen wollen.

Respektieren Sie Andere: Verhalten Sie sich auch in der scheinbaren Anonymität so, als ob Ihnen jemand persönlich gegenübersteht. Denken Sie an das Ziel von Social Media: den gegenseitigen Austausch.

Sprechen Sie für sich selbst: Wenn Sie privat Social Media nutzen, bleiben Sie privat, schreiben Sie in der Ich-Form. Schreiben Sie nur das, wofür Sie selbst und persönlich stehen. Eine Meinungsäußerung, in deren Zusammenhang Sie auf Ihre Tätigkeit Bezug nehmen, sollte unterbleiben. Dienstliche Bezüge haben bei der privaten Nutzung von Social Media keinen Platz.

Rechtliche Fallen: Urheberrechtsverstöße, Verleumdungen und Beleidigungen sind auch in Social Media nicht erlaubt. Auch hier gilt die Datenschutzgrundverordnung. Respektieren Sie das Recht am eigenen Bild, fragen Sie vorher, wenn Sie Fotos von anderen Personen veröffentlichen. Auch bei der Veröffentlichung von fremden Texten, Fotos oder Videos – und das fängt manchmal schon mit dem „Liken“ an – sollten Sie immer auf das Urheberrecht achten. Inhalte, die Ihnen nicht gehören, dürfen Sie nicht verbreiten ohne den Urheber zu fragen.

Bei vielen Plattformen geben Sie mit dem Upload zudem Rechte am eigenen Bild ab. Prüfen Sie das vorher, bevor Sie sich nachher vielleicht ärgern.

Achtung: Von Ihnen gemachte Bilder werden, je nach Kameramodell und Einstellung, automatisch mit EXIF-Daten (Meta-Daten) versehen, welche u.a. die Standortinformationen des gemachten Bildes beinhalten. Leider entfernen nicht alle Social Media Dienste diese Angaben vor der Veröffentlichung. Es kann also sein, dass Andere nicht nur ihre Urlaubshütte in den Bergen sehen sondern auch ganz genau wissen wo sich diese befindet.