Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Soziale Medien & Soziale Netzwerke

1 Einsatz im Unternehmenskontext

Das Internet bietet heutzutage unter dem Schlagwort „soziale Medien“ zahlreiche Plattformen, in denen sich Menschen austauschen können: Sie veröffentlichen die Fotos ihres letzten Urlaubs, pflegen und erweitern ihre beruflichen Kontakte oder laden ihre Freunde ein, virtuelle Nachbarn in Anwendungen und Spielen zu sein.

Auch für einen Großteil der Unternehmen ist die Präsenz in mindestens einem sozialen Medium heutzutage fester Bestandteil von Marketingkonzepten und Werbekampagnen. Insbesondere Unternehmensbereiche, wie Marketing, Vertrieb, Presse- und Öffentlichkeitsarbeit, Customer Relationship Management (CRM) oder Kundensupport, können kaum noch auf ein Engagement in sozialen Medien verzichten.

Die Gefahren werden dabei aber häufig unterschätzt. Privatsphäre und Datenschutz sind längst nicht mehr die einzigen Themen, die im Zusammenhang mit sozialen Medien kontrovers diskutiert werden. Auch (Cyber-) Kriminelle haben die Beliebtheit dieser Plattformen als Chance erkannt. In der Berichterstattung der Medien werden die damit verbundenen Gefahren i. d. R. jedoch aus Sicht der Privatanwender betrachtet. Allerdings können soziale Medien gerade für Unternehmen eine Herausforderung bezüglich der IT-Sicherheit darstellen.

Ziel dieses Dokuments ist es daher, Empfehlungen für den Einsatz sozialer Medien im Unternehmensumfeld zu geben, um so den Abfluss von geschäftskritischen Informationen zu verhindern. Primäre Zielgruppe sind kommerzielle Nutzer, wobei auch Aspekte der privaten Nutzung behandelt werden, die in Konflikt mit den Interessen des jeweiligen Unternehmens stehen könnten. Darüber hinaus adressiert diese Empfehlung auch solche Unternehmen, die soziale Medien zur eigenen Darstellung nicht nutzen, sondern lediglich Risiken und Probleme durch private Aktivitäten der Mitarbeiter in sozialen Medien vermeiden möchten.

2 Sicherheitsrisiken

Bei der rein privaten Nutzung von sozialen Medien sind maßgeblich die folgenden Sicherheitsrisiken als kritisch zu bewerten:

- Identitätsdiebstahl,
- Offenlegung privater Informationen / Schutz der Privatsphäre,
- Datenschutzverletzung,
- Phishing,
- Mobbing und Cyberstalking.

Der Einsatz sozialer Medien im Unternehmenskontext bringt eine Reihe weiterer Sicherheitsrisiken mit sich. Auch müssen einige der für private Nutzer relevanten Risiken anders bewertet werden, da bei einem Sicherheitsvorfall im Kontext eines sozialen Mediums in der öffentlichen Wahrnehmung evtl. das Unternehmen als Verursacher gesehen wird, über dessen Präsenz beispielsweise Schadsoftware verbreitet wurde.

- Identitätsdiebstahl: Kriminelle versuchen zunehmend, bestehende Accounts zu hacken, um diese Identitäten für ihre Zwecke zu missbrauchen. So ist es denkbar, dass ein Angreifer das Profil eines Unternehmens bzw. das eines Mitarbeiters übernimmt und z. B. zur Verbreitung von Malware oder Spam verwendet. Neben dem Diebstahl von existierenden Identitäten bzw. Profilen ist es natürlich auch möglich, dass Angreifer selbst ein Profil erstellen, in welchem sie vorgeben, dass es sich um ein Unternehmen bzw. um einen Mitarbeiter davon handelt.
- Social Engineering: Das häufig unreflektierte Kommunikationsverhalten von Mitarbeitern in sozialen Medien kann Angreifern das Social Engineering mitunter sehr leicht machen. So können die dort veröffentlichten Informationen verwendet werden, um Passwortfragen zu erraten oder um Dinge zu erfahren, die bei personalisierten Angriffen (Spear Phishing) dienlich sind. Werden Identitäten externer Partner gestohlen, zu denen bereits eine Verbindung in sozialen Medien besteht, so erleichtert dies Angriffe im Bereich Social Engineering. Denkbar wäre auch ein Abfluss vertraulicher Informationen und Dokumente, falls ein Angreifer unter einer gestohlenen Identität Nachrichten versendet, wie z. B. „Meine E-Mail ist ausgefallen, schicken Sie mir bitte doch das Dokument xy an ...“. Durch evtl. unbeabsichtigt veröffentlichte bzw. freigeschaltete Informationen können Angreifer evtl. auch einen Ansatzpunkt für Erpressungsversuche in Erfahrung bringen. Dies ist gerade dann der Fall, wenn das Kommunikationsverhalten insbesondere im privaten Bereich zu sehr von Offenheit geprägt ist.
- Vorsätzlicher oder fahrlässiger Verrat von Betriebs- und Geschäftsgeheimnissen: Sind die Kontakte eines Mitarbeiters offen für jeden lesbar, so können Angreifer hierdurch sukzessive die Unternehmensstrukturen sowie die Beziehungen zu Kunden und Partnerunternehmen in Erfahrung bringen. Darüber hinaus können auch Dokumente und andere firmenvertrauliche Informationen sowohl fahrlässig als auch vorsätzlich veröffentlicht werden. Häufig bedarf es nicht einmal eines gezielten Angriffs, damit vertrauliche Informationen eines Unternehmens nach außen dringen. Selbst wenn ein Mitarbeiter z. B. in seinem privaten Profil lediglich Bilder veröffentlicht, so können diese unter Auswertung von darin ggf. eingebetteten Geodaten und Korrelation mit Postings des Mitarbeiters durchaus Aufschluss darüber geben, wann sich die Person wo befunden hat und mit welchem Firmenkunden sie z. B. in Kontakt stand.
- Soziale Medien als Einfallstor für Schadsoftware: Soziale Medien verwenden i. d. R. aktive Inhalte wie Java Script. Dies ermöglicht potenziell die Ausnutzung aktueller Schwachstellen in den Browsern der Nutzer. In versendeten Nachrichten oder veröffentlichten Postings kann sich, wie in herkömmlichen E-Mails auch, Schadsoftware bzw. ein Link darauf befinden. Kennt der Empfänger den (vermutlichen) Absender, ist die Wahrscheinlichkeit einer Infektion hoch. Die weitere Verbreitung einer solchen Malware kann dann z. B. über die Kontakte des infizierten Nutzers erfolgen. Mögliche Angriffsvarianten in diesem Kontext sind Cross-Site-Scripting (XSS), Clickjacking und (Spear-) Phishing.
  In einigen sozialen Medien gibt es die Möglichkeit, Apps (insbes. Spiele) innerhalb des Mediums im Browser zu verwenden. Problematisch ist, dass diese Anwendungen von Drittanbietern stammen, deren Sicherheitsstandard oder Geschäftsmodell nicht zwangsläufig denen der sozialen Medien selbst entsprechen muss. Auf diese Weise können – ob beabsichtigt oder nicht – Schadprogramme verbreitet und Nutzer ausspioniert werden.

- Abwerben von qualifizierten Mitarbeitern: Insbesondere wenn Mitarbeiter Informationen wie Firmenzugehörigkeit, Organisationseinheit, Projekte oder Qualifikationen frei zugänglich machen, kann dies durch Headhunter gezielt genutzt werden, um qualifizierte Mitarbeiter abzuwerben. Dies führt unweigerlich auch zum Abfluss von fachlichem Know-how und internem Wissen.
- Verminderung der Produktivität: Zuletzt sei angemerkt, dass insbesondere die Nutzung sozialer Medien während der Arbeitszeit die Produktivität der Mitarbeiter massiv vermindern kann.

3 Social Media Strategie

Wichtig bei der Unternehmensdarstellung in sozialen Medien ist, dass von Beginn an eine fundierte Strategie zur Umsetzung definiert wird. Nur so lassen sich auch geeignete Vorgaben – nicht zuletzt mit Blick auf Sicherheit – festschreiben. Eine solche Strategie sollte u. a. die folgenden Inhalte umfassen:

- Kriterien für die Auswahl der Plattform(en)
- Etablierung von Strukturen und Prozessen
- Klassifizierung der Daten / Informationen
- Bewertung rechtlicher Fragestellungen
- Monitoring der Social Media Nutzung
- Festschreibung von Nutzervorgaben

Die Strategie muss in jedem Fall derart gestaltet werden, dass insbesondere die sicherheitsspezifischen Aspekte und Festlegungen mit der Sicherheitsleitlinie des Unternehmens vereinbar sind. Zudem sollte eine regelmäßige Re-Evaluierung der Strategie vorgenommen werden.

4 Kriterien für die Auswahl der Plattform(en)

4.1 Wahl eines etablierten Plattform-Anbieters

Die Zielgruppen eines Unternehmens lassen sich ein konkretes soziales Medium i. d. R. nicht vorgeben, sodass ein Engagement eines Unternehmens meist parallele Präsenzen auf den wichtigsten Plattformen erfordert. Ist jedoch eine Auswahl der Plattform u. a. unter dem Aspekt der Sicherheit möglich bzw. gewünscht, so können die folgenden Kriterien herangezogen werden.

- Infrastruktur und Sicherheitsmanagement: Server-Systeme, Policies, interne Prozesse, IT-Grundschutz
- Schnittstellen: Input-/Outputvalidierung, Datentransfer, Massenabfragen
- Identity Management & Schutz der Identitäten: Authentisierung, Schutz gegen Identitätsmissbrauch
- Datenschutz und rechtliche Aspekte: Pflichtangaben, AGBs, Nutzerrechte
- Nutzerfreundlichkeit & Unterstützung der Nutzer: Sicherheitsspezifische Konfigurationsmöglichkeiten, Dokumentation / Hilfe, Kontaktmöglichkeiten

In der Praxis erweist sich eine ganzheitliche Bewertung solcher Faktoren jedoch als sehr schwierig, da die hierzu erforderlichen Informationen seitens der Plattform-Anbieter mitunter nicht hinreichend transparent gemacht werden.

Bei der Auswahl einer Plattform sollte sich ein Unternehmen auch immer bewusst sein, dass es eine enge Bindung mit dem jeweiligen Plattform-Anbieter eingeht. Sobald ein Unternehmen ein bestimmtes soziales Medium für die Unternehmenspräsenz gewählt und erste Aktivitäten dort gestartet hat, befindet es sich bereits in einer starken Abhängigkeit zum jeweiligen Platt-

form-Anbieter. Migrationspfade zu anderen sozialen Medien sind i. d. R. nicht vorhanden. Ein Wechsel zwischen den Plattform-Anbietern ohne größere Reibungsverluste ist dann i. d. R. kaum noch möglich (Vendor Lock-In).

4.2 Aufbau einer eigenen Plattform

Vor allem in großen Unternehmen bieten soziale Medien die Möglichkeit, Synergien zu fördern und ungewollt redundante Tätigkeiten zu vermeiden. Insbesondere wenn kritische Informationen dabei ausgetauscht werden, sollten hierzu keinesfalls öffentliche soziale Medien eingesetzt werden. Vielmehr können für einen solchen Zweck soziale Medien innerhalb eines Unternehmens selbst betrieben werden. Entsprechende Softwareprodukte für Enterprise Social Media sind sowohl im kommerziellen Umfeld als auch unter freier Lizenz verfügbar.

In Abhängigkeit der konkreten Anforderungen an eine Social Media Plattform, die sich aus der Strategie ergeben, ist mitunter auch der Einsatz solcher Enterprise-Lösungen für den externen Kontakt mit Kunden und Partnern sinnvoll. Von Vorteil ist dabei, dass die Plattform vollständig unter eigener Kontrolle gehalten werden kann. Somit ergibt sich eine bessere Vereinbarkeit mit der Sicherheitsleitlinie des Unternehmens. Dabei geht allerdings der Vorteil verloren, dass der Unternehmensauftritt Teil des sozialen Mediums ist, in dem die Zielgruppe ohnehin bereits registriert und täglich aktiv ist.

Für den Eigenbetrieb von Enterprise Social Media sind insbesondere die entsprechenden Vorgaben aus dem BSI-Standard zur Internet-Sicherheit (ISi-Reihe)[1], dem IT-Grundschutz[2] sowie der Empfehlungen zur Cyber-Sicherheit[3] zu beachten, um ein hinreichendes Sicherheitsniveau zu erzielen.

5 Etablierung von Strukturen und Prozessen

Zur Umsetzung der Social Media Strategie ist es erforderlich, geeignete Strukturen und Prozesse zu etablieren. Hierzu gehören u. a.

- Antragsverfahren zur Nutzung
- Freigabeprozedere für Beiträge
- Unterstützung der Mitarbeiter (in Großunternehmen z. B. in Form eines Competence Center)
- Security-Team zur Unterstützung der Mitarbeiter und zur Gewährleistung der Einhaltung der Sicherheitsvorgaben

Dabei sind insbesondere die Rollen und Verantwortlichkeiten klar zu regeln und zu dokumentieren.

Für das Antragsverfahren sind beispielsweise folgende Festlegungen zu treffen:

- Wie wird der Antrag gestellt?
- Wer entscheidet über den Antrag?
- Verifikation der Verträglichkeit mit der definierten Social Media Strategie
- Freigabe zur eigenständigen Einrichtung des Accounts bzw. Veranlassung der zentralen Einrichtung
- Registrierung des Mitarbeiters bzw. Accounts für Monitoring-Prozesse
- Dokumentation und Kommunikation der Freigabe bzw. Berechtigungen für das eigenständige Agieren im sozialen Medium
- ggf. Freigabe für die Verwendung von Logos und Produktbezeichnungen

1 BSI-Standard zur Internet-Sicherheit (ISi-Reihe), https://www.bsi.bund.de/ISi-Reihe/
2 BSI IT-Grundschutz, https://www.bsi.bund.de/grundschutz/
3 BSI Empfehlungen zur Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de/ACS/Informationspool

6 Klassifizierung der Daten / Informationen

Die Strategie zur Nutzung von sozialen Medien sollte eindeutig regeln, welche Informationen veröffentlicht werden sollen bzw. dürfen und welche nicht. Geschäftszahlen, Personalien oder strategische Informationen sollten explizit ausgeschlossen werden. Gleiches gilt für Kundenbeziehungen und Produktinformationen, die nicht auch auf dem offiziellen Internetauftritt des Unternehmens frei zugänglich sind und/oder für die keine Zustimmung der betroffenen Kunden bzw. Verantwortlichen vorliegt.

Prinzipiell besteht hier die Möglichkeit, ein Freigabeprozedere für sämtliche Veröffentlichungen in sozialen Medien zu etablieren, welches zentral dafür sorgt, dass nur die Daten publiziert werden, die auch veröffentlicht werden sollen. Dies entspricht der herkömmlichen zentralen Steuerung der Unternehmenskommunikation durch PR- oder Marketingabteilungen.

Alternativ kann eine genaue Festlegung der Berechtigungen bzw. Befähigungen (Clearance) erfolgen, welche den mit dem öffentlichen Auftritt betrauten Mitarbeitern genaue Vorgaben hierzu macht, sodass nur in besonderen Fällen das Durchlaufen eines Freigabeprozederes erforderlich ist. Dieser Ansatz wird in der Praxis häufig gewählt, wenn ausgewählte Mitarbeiter eine Art Leuchtturmposition einnehmen und als Botschafter für das Image des Unternehmens agieren. Auch für Mitarbeiter einer bestimmten Abteilung bzw. in einer bestimmten Rolle können mit definierten Standardfreigaben ausgestattet werden.

7 Bewertung rechtlicher Fragestellungen

Bei der Erarbeitung einer Strategie für die Nutzung von sozialen Medien sind auch rechtliche Fragestellungen relevant, die sowohl das Unternehmen selbst als auch die privaten Nutzer betreffen kann. Diese werden aktuell mitunter intensiv diskutiert, sodass an dieser Stelle keine abschließende Bewertung oder Empfehlung erfolgen kann. Im Rahmen der Strategie zur Nutzung sozialer Medien ist eine Beurteilung dieser Fragestellungen sowie eine Ableitung entsprechender Maßnahmen und Vorgaben erforderlich.

7.1 Datenschutz

Durch die kritische Berichterstattung in den Medien werden viele private Nutzer zunehmend für das Thema „Datenschutz in sozialen Medien“ sensibilisiert. Sie möchten nicht zwangsläufig das Risiko einer Profilbildung durch Plattform-Anbieter oder Dritte tolerieren müssen, nur um sich über Produkte zu informieren oder um an Gewinnspielen oder sonstigen Angeboten teilzuhaben. Daher empfiehlt es sich, zumindest die wichtigen Teile der öffentlichen Internetpräsenz nicht exklusiv in sozialen Medien geschehen zu lassen. Alternativ sollte auch immer ein Zugriff auf die entsprechenden Angebote über die konventionelle Webpräsenz möglich sein. Hierdurch wird vermieden, dass Nutzer zu Aktivitäten in sozialen Medien bewegt werden können, über die später beispielsweise eine Profilbildung zur Erleichterung von Angriffen erfolgen kann.

Auch für die Umsetzung von konventionellen Webangeboten haben soziale Medien Auswirkungen hinsichtlich Datenschutz. Häufig werden auf einzelnen Seiten Verlinkungen zu sozialen Medien vorgenommen, um anderen zu zeigen, dass man als Nutzer die jeweilige Seite empfiehlt bzw. um zu sehen, wie viele Personen bzw. welche der eigenen Kontakte eine solche Empfehlung ausgesprochen haben. Hierzu gehören beispielsweise der „Like-Button“ (Facebook), der „+1“-Button (Google+) oder der „Tweet Button“ (Twitter).

Das Problem an solchen Buttons ist, dass bereits beim Aufruf der jeweiligen Website eine Verbindung mit den dort verlinkten sozialen Medien erfolgt. Ist der Nutzer zur gleichen Zeit dort

angemeldet, ermöglicht dies eine umfangreiche Profilbildung hinsichtlich des Nutzerverhaltens. Auch wenn Besucher einer Website nicht in einem sozialen Netz registriert oder angemeldet sind, ist eine – ggf. eingeschränkte – Profilbildung möglich.

Es bestehen verschiedene Lösungsmöglichkeiten hierzu (sog. „Zwei-Klick-Lösungen“)[4], bei denen der Besucher einer Website die Funktionalität dieser Buttons zunächst explizit aktivieren muss. Allerdings werden auch diese von Datenschützern als kritisch betrachtet. Zudem verstoßen diese Lösungsmöglichkeiten teilweise gegen die Nutzungsbedingungen der sozialen Medien.

7.2 Urheber- und Nutzungsrechte

Besondere Vorsicht beim Unternehmensauftritt in sozialen Medien ist hinsichtlich des Urheberrechts geboten. Während die Inhalte bei klassischen Internetauftritten i. d. R. ausschließlich vom Unternehmen selbst bereitgestellt wurden, können bei sozialen Medien andere Nutzer Inhalte hinzufügen. Dies gilt sowohl für Texte (z. B. Auszüge aus Zeitungsartikeln) als auch Multimedia-Dateien (z. B. Bilder und Videos). Für entsprechende Urheberrechtsverletzungen kann neben dem Nutzer, der die Inhalte eingefügt hat, ggf. auch das Unternehmen belangt werden, das die jeweilige Seite im sozialen Medium verantwortet (Störerhaftung). Dies ist insbesondere daher problematisch, da nicht ohne Weiteres erkennbar ist, ob der jeweilige Nutzer im Besitz der erforderlichen Rechte an den Inhalten ist. Selbst ein zeitnahes Monitoring der Präsenz in sozialen Medien ist hierbei nicht hilfreich, da andere Nutzer die entsprechenden Inhalte übernehmen können und spätestens damit das Entfernen der Inhalte praktisch unmöglich ist. Eine abschließende juristische Bewertung dieser Thematik ist derzeit nicht möglich.Ein weiteres Problem können die Nutzungsrechte an den im sozialen Medium veröffentlichten Informationen und Dateien sein. In einigen sozialen Medien räumt der Nutzer mit der Zustimmung zu den Nutzungsbedingungen umfangreiche Rechte an allen veröffentlichten Daten und Dateien ein. Dabei kann es sich z. B. um eine „nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz“[5] handeln, die zumindest für einige Unternehmen mit Blick auf Marken- und Schutzrechte problematisch sein kann. Dieser Aspekt ist im Rahmen der Social Media Strategie hinsichtlich der zu veröffentlichenden Daten zu beachten.

Von besonderer Bedeutung für die Strategie des Unternehmens sind auch die Nutzungsbedingungen, die für die Zielgruppe im sozialen Medium gelten. Die Nutzungsbedingungen des jeweiligen Plattform-Anbieters geben hierfür natürlich den Rahmen vor. Ergänzend sollten möglichst Festlegungen getroffen werden, wie z. B. mit kritischen Äußerungen Dritter in der Präsenz des Unternehmens umgegangen wird. Hierzu sollten die Nutzer explizite Hinweise bekommen, dass z. B.

- sowohl positive als auch negative Äußerungen zugelassen sind und konstruktiv diskutiert werden sollen,
- eine redaktionelle Prüfung und Überarbeitung erfolgt, durch die beispielsweise anstößige oder beleidigende Beiträge gelöscht werden können.

7.3 Gesetzliche Verpflichtungen

Auftritte in sozialen Medien unterliegen dem Telemediengesetz, dessen Einhaltung sichergestellt werden muss. Dazu gehört beispielsweise ein Impressum. Zusätzlich gilt – soweit das Telemediengesetz keine spezifischen Regelungen enthält – das Bundesdatenschutzgesetz.

4 socialshareprivacy, http://www.heise.de/extras/socialshareprivacy/
5 Facebook Nutzungsbedingungen, https://www.facebook.com/legal/terms/update?ref

8 Monitoring der Social Media Nutzung

Für Unternehmen gibt es eine Reihe von Gründen, sich nicht nur selbst in sozialen Medien zu engagieren, sondern auch die Aktivitäten Dritter dort zu beobachten. Dabei geht es nicht darum, die eigenen Mitarbeiter zu überwachen, sondern vielmehr um die Betrachtung aller im direkten Unternehmenskontext getroffenen Äußerungen innerhalb der sozialen Medien. Daher sollte auch nicht der Datenverkehr aus dem eigenen Unternehmen heraus in die sozialen Medien analysiert werden. Stattdessen sollte ein neutraler Zugriff auf die sozialen Medien erfolgen. Hierzu gehören neben unternehmenskritischen Kampagnen Dritter (z. B. Protestbewegungen, Hacktivismus, etc.) auch nicht-autorisierte Aktivitäten der eigenen Mitarbeiter sowie von Auftragnehmern im Rahmen der Nutzung für das Unternehmen hinsichtlich der Veröffentlichung kritischer Daten und Informationen.

Die Etablierung entsprechender Monitoring-Prozesse ist zu empfehlen, um sowohl mögliche Probleme frühzeitig zu bemerken als auch entsprechend reagieren und Schaden vom Unternehmen abwenden zu können. Es existiert eine Reihe von Softwareprodukten und Dienstleistungen, um ein Monitoring von sozialen Netzen hinsichtlich des eigenen Unternehmens zu gewährleisten.

9 Festschreibung von Nutzervorgaben

Soziale Medien gehören zum Alltag von Mitarbeitern und Kunden. Ein Unternehmen kann sich daher nicht einfach auf die Position zurückziehen, den Zugriff auf die entsprechenden Plattformen während der Arbeitszeit durch Firewallregeln zu unterbinden. Vielmehr bedarf es geeigneter Empfehlungen und Vorgaben (Policies), um sowohl das Unternehmen als auch die Mitarbeiter zu schützen. Bei der konkreten Ausgestaltung einer solchen Policy ist allerdings zu beachten, dass diese für unzulässig erklärt werden kann, wenn sie die Arbeitnehmer unangemessen benachteiligt. Daher sollte für die einzelnen Formulierungen die (rechtliche) Verbindlichkeit genau geprüft und eindeutig dokumentiert werden. Es empfiehlt sich also explizit zwischen (ggf. sanktionierbaren) verbindlichen Vorgaben und (unverbindlichen) Empfehlungen zu differenzieren. Je nach Berufszweig oder Branche sind diese Policies natürlich entsprechend anzupassen, da hier ggf. besondere rechtliche Vorgaben bzgl. der Außenkommunikation zu beachten sind (z. B. Finanzsektor, Mediziner, Juristen). In jedem Fall ist bei der Erarbeitung von Nutzervorgaben und Empfehlungen das Mitbestimmungsrecht des Personal- bzw. Betriebsrats zu beachten (Dienst- bzw. Betriebsvereinbarung). Diese Vorgaben sind – je nach Anwendungsfall – neben der eigenen Belegschaft auch auf Dritte (Partner, Auftragnehmer, etc.) zu übertragen.

Alternativ zur Verpflichtung der Mitarbeiter gemäß einer solchen Policy kann diese natürlich auch als Orientierungshilfe dazu dienen, um im Rahmen einer Sensibilisierungsmaßnahme geeignete Empfehlungen zu erstellen. Hierzu sind darüber hinaus die weiteren Publikationen des BSI[6] [7] in diesem Themenbereich zu beachten.

9.1 Social Media Policy für die private Nutzung

Mitarbeiter benutzen soziale Medien natürlich auch privat. Dabei ist ein Bezug zum Arbeitgeber häufig ersichtlich oder gar explizit genannt. Äußerungen der Mitarbeiter werden daher vielfach direkt mit dem Unternehmen in Verbindung gebracht oder gar als offizielle Aussage bzw. Position des Unternehmens interpretiert. Zur Vorbeugung sollten entsprechende Policies definiert werden, welche die private Nutzung von sozialen Medien zur Aufgabe im Unternehmen abgrenzen und die Mitarbeiter auf ihre Rechte und Pflichten hinweisen.

6 BSI für Bürger, https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/SozialeNetze/sozialeNetze_node.html

7 IT-Grundschutz, 15. Ergänzungslieferung: M 5.157: https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf
IT-Grundschutz Baustein Personal: https://www.bsi.bund.de/dok/10095918
IT-Grundschutz Baustein Sensibilisierung und Schulung: https://www.bsi.bund.de/dok/10095888

In Unternehmen und Behörden sollte prinzipiell die private Nutzung des Internets während der Arbeitszeit geregelt werden. Selbst wenn diese untersagt wird, so empfiehlt sich aufgrund der Charakteristika sozialer Medien dennoch, Empfehlungen für die private Nutzung mit Bezug zu beruflichen Aktivitäten zu machen. Zudem ist zu beachten, dass das Dulden bzw. Zulassen einer uneingeschränkten privaten Nutzung während der Arbeitszeit dazu führen kann, dass dem Unternehmen die Kontrolle der Nutzung über Verbindungs- und Nutzungsdaten untersagt ist. Daher sollte die private Nutzung die Einwilligung zur Erfassung bestimmter Nutzungsdaten (z. B. genutzte soziale Medien, Datenvolumen, etc.) der Mitarbeiter einfordern. Besonders wichtig ist, die private Nutzung während der Arbeitszeit unter einen Widerrufsvorbehalt zu stellen.

Entsprechende Vorgaben können z. B. in Form einer Dienstvereinbarung oder als Teil bzw. Ergänzung des Arbeitsvertrags definiert werden. Ein entsprechendes Muster findet sich im Anhang „Template: Social Media Policy für die private Nutzung“. Darin sind die auf jeden Fall anzupassenden Passagen hervorgehoben.

9.2 Social Media Policy für die berufliche Nutzung

Ist die berufliche Nutzung sozialer Medien zulässig, so sind hierzu dringend wichtige Regelungen zu treffen. Eine entsprechende Policy sollte in Einklang mit der unternehmensweiten Social Media Strategie erstellt werden und zudem die externe Sicht (Image) sowie das Eigenverständnis hinsichtlich unternehmerischer Werte berücksichtigen. Diese grundlegenden Richtlinien und Verhaltensregeln können bei Bedarf durch Empfehlungen zur Konfiguration und Kommunikation ergänzt werden. Ein entsprechendes Muster findet sich im Anhang „Template: Social Media Policy für die berufliche Nutzung“. Darin sind anzupassende Passagen hervorgehoben. Für sämtliche Mitarbeiter, die für das Unternehmen in sozialen Medien auftreten, sollte ein an die Policy angepasstes Schulungs- und Sensibilisierungsprogramm obligatorisch sein.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

10 Template: Social Media Policy für die private Nutzung

Hinweis: Das Template dient lediglich als allgemeiner Leitfaden. Aufgrund der rechtlichen und tatsächlichen Besonderheiten jedes Einzelfalles sowie der dynamischen Rechtslage muss der Verwender vor Einsatz des Templates stets prüfen, ob Anpassungen oder Korrekturen notwendig sind.

Für die private Nutzung von sozialen Medien gelten die folgenden Vorgaben und Empfehlungen.

1. Geltungsbereich und Begriffsbestimmung
    1. Die vorliegende Policy regelt die Nutzung von sozialen Medien (Social Media) im privaten Umfeld, soweit sie die Arbeit betrifft.
    2. Social Media subsumiert sämtliche Plattformen und (Web-) Anwendungen, in denen Nutzer mit anderen kommunizieren und Informationen sowie mediale Inhalte austauschen. Blogs und Foren fallen ebenfalls unter diesen Begriff.
    3. Als private Nutzung werden sämtliche Aktivitäten in Social Media verstanden, die nicht explizit seitens des Unternehmens autorisiert bzw. veranlasst werden. Andernfalls liegt eine berufliche Nutzung vor.
    4. Formulierungen mit dem Präfix (V) stellen verbindliche Vorgaben dar, während es sich bei dem Präfix (E) lediglich um Empfehlungen handelt.
2. Nutzung während der Arbeitszeit
    1. (V) Die private Nutzung sozialer Medien während der Arbeitszeit ist ***[zulässig | nicht zulässig | in geringem Umfang zulässig | während der Pausenzeiten zulässig] [für die folgenden Plattformen:]. [Voraussetzung für die private Nutzung ist die schriftliche Einwilligung hinsichtlich der zentralen Erfassung der verwendeten sozialen Medien, des verursachten Datenvolumens sowie der Verweildauer.] [Die Gewährung der privaten Nutzung kann jederzeit durch die Unternehmensleitung widerrufen werden.]***
3. Nutzerprofil
    1. ***(V/E)*** Die Nennung des Arbeitgebers ***[ist nicht erwünscht | ist erwünscht | darf erfolgen]***.
    2. ***(V/E)*** Die Nennung der Aufgabenbereiche ***[ist nicht erwünscht | ist erwünscht | darf erfolgen | darf nicht erfolgen]***.
    3. (E) Prinzipiell gilt – insbesondere mit Blick auf berufliche Interessenskonflikte oder Erleichterung von Social Engineering – das Gebot der Datensparsamkeit hinsichtlich berufsbezogener Angaben im Nutzerprofil.
    4. (V) Die Verwendung beruflicher E-Mail-Adressen oder sonstiger Kontaktinformationen für die private Nutzung ist untersagt.
    5. (E) Die im Nutzerprofil veröffentlichten Daten sind möglichst in ihrer Sichtbarkeit für andere zu beschränken. Persönliche Daten und veröffentlichte Informationen sollten nur vertrauenswürdigen Personen zugänglich sein.
4. Kontakte und Kommunikation
    1. (V) Externe rein berufliche Kontakte dürfen ***[nicht | nicht öffentlich einsehbar | nicht von Dritten einsehbar]*** zum jeweiligen Profil hinzugefügt werden.

2. (V) Berufliche Kontakte zu Kolleginnen und Kollegen dürfen ***[nicht | nicht öffentlich einsehbar | nicht von Dritten einsehbar]*** zum jeweiligen Profil hinzugefügt werden.
3. (E) Seien Sie prinzipiell zurückhaltend mit Kontakten bzw. Kontaktanfragen, die im beruflichen Kontext stehen (könnten).
4. (E) Wenn Sie „zweifelhafte" Anfragen von Bekannten erhalten, erkundigen Sie sich außerhalb der sozialen Medien nach der Vertrauenswürdigkeit dieser Nachricht.
5. (E) Die Mitgliedschaft in Gruppen, Fanpages, etc. sollte nicht zu Interessenskonflikten führen.

5. Veröffentlichen von Informationen
   1. (E) Es dürfen keine Informationen über berufliche Aktivitäten publiziert werden. Wahren Sie das Dienstgeheimnis (vgl. Arbeitsvertrag). Hierzu gehören neben fachlichen Daten auch Unternehmensdaten, Personalien und sonstige Interna. Berücksichtigen Sie zudem bestehende Vertraulichkeitsvereinbarungen (Non-disclosure Agreements).
   2. (E) Bedenken Sie, dass das Löschen einmal veröffentlichter Informationen nahezu unmöglich ist.
   3. (E) Vermeiden Sie Äußerungen, bei denen Interessenskonflikte mit beruflichen Aufgaben entstehen könnten.
   4. (V) Es ist untersagt, Aussagen zu Produkten oder Dienstleistungen zu treffen, für die ein Bezug zum Arbeitgeber, einem Kunden, einem Wettbewerber oder zu beruflichen Aktivitäten besteht.
   5. (V) Es dürfen keine Informationen zu beruflichen Reisen veröffentlicht werden, da dies ggf. weitere Rückschlüsse erlaubt. Neben textuellen Nennungen betrifft dies auch die Veröffentlichung von Fotos und Videos – insbesondere da diese häufig automatisch mit Geodaten versehen werden.

6. Allgemeine Regelungen
   1. (E) Bedenken Sie stets, dass die Grenzen zwischen beruflicher und privater Nutzung von Social Media sehr leicht diffundieren können – insbesondere in der Wahrnehmung durch Dritte. Verhalten Sie sich daher prinzipiell zurückhaltend. Bedenken Sie nicht nur, welche Informationen sie veröffentlichen, sondern auch wie diese z. B. durch kulturelle Unterschiede von Dritten wahrgenommen werden könnten.
   2. (E) Erkundigen Sie sich über die Allgemeinen Geschäftsbedingungen und die Bestimmungen zum Datenschutz des genutzten sozialen Mediums. Prüfen Sie kritisch, welche Rechte Sie den Betreibern sozialer Medien an den von Ihnen eingestellten Bildern, Texten und Informationen einräumen.
   3. (E) Unterscheiden Sie immer explizit zwischen Meinungen und Fakten.
   4. (E) Gehen Sie davon aus, dass sämtliche in Social Media veröffentlichten Daten und Informationen frei verfügbar sein können, auch wenn Sie beispielsweise Dinge nur für direkte Bekannte veröffentlichen. Meist ist dann auch die Auffindbarkeit über Suchmaschinen gegeben. Einmal veröffentlichte Informationen können i. d. R. praktisch nicht gelöscht werden.
   5. (E) Machen Sie explizit und unmissverständlich klar, dass Sie sich im sozialen Medium als Individuum äußern. Ein Hinweis an zentraler Stelle, wie beispielsweise der Folgende, ist ratsam: „Die Meinungen auf dieser Seite sind meine eigenen und entsprechen mitunter nicht denen meines Arbeitgebers."

6. (E) Erteilen Sie keine juristischen Ratschläge.
7. (E) Beachten Sie bei Ihren Äußerungen bestehende Schutzrechte und Schutzmarken. Dies gilt auch für Firmen- und Produktlogos.
8. (E) Versenden Sie niemals unerwünschte Werbung (Spam).
9. (E) Nehmen Sie Abstand von politischen Äußerungen, unsachlichen oder emotionalen Diskussionen, Beleidigungen, Rufschädigung, Bedrohungen und pornografischen Inhalten.
10. (V) Veröffentlichen Sie keine Informationen oder sonstige Äußerungen zum Unternehmen, zu Kolleginnen/Kollegen, Kunden, Partnern, Auftragnehmern, etc. Bedenken Sie, dass solche Äußerungen im Rahmen des Monitoring von Social Media durch das Unternehmen bemerkt werden können.
11. (E) Anfragen zu beruflichen Themen sollten in die entsprechenden Kanäle geleitet werden, damit u. a. die Nachvollziehbarkeit der Unternehmenskommunikation gewährleistet ist.

7. IT-Sicherheit
    1. (E) Nutzen Sie soziale Medien nur mit ausreichend abgesicherten PCs. Die Nutzung mobiler Geräte (Tablet, PDA, etc.) in Verbindung mit entsprechenden Apps ist nicht zu empfehlen.
    2. (E) Nutzen Sie soziale Medien nur aus sicheren und vertrauenswürdigen Netzwerken heraus. Nutzen Sie insbesondere keine unverschlüsselten WLANs.
    3. (E) Bedenken sie stets, dass auch über soziale Medien Schadsoftware verbreitet werden kann. Beachten Sie die Sicherheitshinweise des BSI[8] allgemein sowie zu sozialen Medien im Speziellen.
    4. (E) Verwenden Sie für jede Internetanwendung, insbesondere auch wenn Sie in verschiedenen sozialen Medien angemeldet sind, ein unterschiedliches und sicheres Passwort.
    5. (E) Klicken Sie nicht wahllos auf Links – soziale Medien werden verstärkt dazu genutzt, um Phishing zu betreiben.
8. Ansprechpartner im Unternehmen
    1. (E) Innerhalb des Unternehmens sind ***die folgenden Ansprechpartner*** definiert, die bei Fragen kontaktiert oder bei Verfehlungen im Rahmen der privaten Nutzung umgehend informiert werden sollten:

8 BSI für Bürger, https://www.bsi-fuer-buerger.de

11 Template: Social Media Policy für die berufliche Nutzung

Hinweis: Das Template dient lediglich als allgemeiner Leitfaden. Aufgrund der rechtlichen und tatsächlichen Besonderheiten jedes Einzelfalles sowie der dynamischen Rechtslage muss der Verwender vor Einsatz des Templates stets prüfen, ob Anpassungen oder Korrekturen notwendig sind.

Für die berufliche Nutzung von Social Media gelten die folgenden verbindlichen Vorgaben und Bestimmungen.

1. Geltungsbereich und Begriffsbestimmung
   1. Die vorliegende Policy regelt die Nutzung von sozialen Medien (Social Media) im beruflichen Umfeld.
   2. Social Media subsumiert sämtliche Plattformen und (Web-) Anwendungen, in denen Nutzer mit anderen kommunizieren und Informationen sowie mediale Inhalte austauschen. Blogs und Foren fallen ebenfalls unter diesen Begriff.
   3. Als berufliche Nutzung werden sämtliche Aktivitäten in Social Media verstanden, die explizit seitens des Unternehmens autorisiert bzw. veranlasst werden. Andernfalls liegt eine private Nutzung vor.
2. Antragsverfahren zur beruflichen Nutzung
   1. Bevor Sie in Social Media aktiv werden oder einen Nutzeraccount (Profil) erstellen, ist ***das folgende Antragsverfahren*** zu durchlaufen. ***[Erst nach dessen Abschluss darf ein Account erstellt werden. | Im Rahmen dieses Verfahrens wird ein Account zentral erstellt.]***
3. Nutzerprofil
   1. Trennen Sie berufliche und private Aktivitäten in sozialen Netzen mittels separater Accounts.
   2. Verwenden Sie Passwörter mit einer hinreichenden Komplexität (mindestens 10 Zeichen, bestehend aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen). Wechseln Sie regelmäßig Ihr Passwort.
   3. Das Nutzerprofil wird im Rahmen des Antragsverfahrens zentral erstellt und darf nicht verändert werden.
      Alternativ (4.-6.)
   4. Sorgen Sie für eine maximale Transparenz für berufliche Accounts. Verwenden Sie Ihren echten Namen und geben Sie die Firmenzugehörigkeit und Rolle Ihre im Unternehmen erkennbar an.
   5. Die Verwendung privater E-Mail-Adressen oder sonstiger Kontaktinformationen für die berufliche Nutzung ist untersagt.
   6. Deaktivieren Sie die Möglichkeit von Beiträgen Dritter auf der Pinnwand Ihres Accounts.
4. Kontakte und Kommunikation
   1. Die Kommunikation innerhalb des Unternehmens ***[darf | darf nicht]*** über soziale Medien erfolgen. ***[Hierfür sind ausschließlich die Kommunikationsmittel des Unternehmens zu verwenden.]***
   2. Die Kommunikation mit Externen (Kunden, Geschäftspartnern, etc.) ***[darf | darf nicht]*** über soziale Medien erfolgen. ***[Hierfür sind ausschließlich die Kommunikationsmittel des Unternehmens zu verwenden.]***
   3. Externe berufliche Kontakte dürfen ***[nicht | nicht öffentlich einsehbar | nicht von Dritten einsehbar]*** zum jeweiligen Profil hinzugefügt werden.

4. Berufliche Kontakte zu Kolleginnen und Kollegen dürfen ***[nicht | nicht öffentlich einsehbar | nicht von Dritten einsehbar]*** zum jeweiligen Profil hinzugefügt werden.
5. Bei individuell genutzten beruflichen Profilen, die nicht gleichzeitig von der Öffentlichkeitsarbeit betreut werden, sind Anfragen der Presse an diese ***[zu verweisen | weiterzuleiten]***.
6. Die Mitgliedschaft in Gruppen, Fanpages, etc. sollte sich auf berufliche Interessen beschränken und nicht zu Interessenskonflikten führen.

5. Veröffentlichung von Informationen
   1. Bedenken Sie, dass das Löschen einmal veröffentlichter Informationen nahezu unmöglich ist.
   2. Veröffentlichen Sie Informationen ausschließlich gemäß der Ihnen explizit übertragenen Berechtigungen und Freigaben. Wahren Sie darüber hinaus das Dienstgeheimnis (vgl. Arbeitsvertrag). Hierzu gehören neben fachlichen Daten auch Unternehmensdaten, Personalien und sonstige Interna. Berücksichtigen Sie zudem bestehende Vertraulichkeitsvereinbarungen (Non-disclosure Agreements). Im Zweifelsfall ist vorab ***[der Fachvorgesetzte | die Öffentlichkeitsarbeit]*** zu beteiligen.
6. Allgemeine Regelungen
   1. Bedenken Sie stets, dass die Grenzen zwischen beruflicher und privater Nutzung von Social Media sehr leicht diffundieren können – insbesondere in der Wahrnehmung durch Dritte. Verhalten Sie sich daher prinzipiell zurückhaltend. Bedenken Sie stets nicht nur, welche Informationen sie veröffentlichen, sondern auch wie diese z. B. durch kulturelle Unterschiede von Dritten wahrgenommen werden könnten.
   2. Unterscheiden Sie immer explizit zwischen Meinungen und Fakten.
   3. Gehen Sie davon aus, dass sämtliche in Social Media veröffentlichten Daten und Informationen frei verfügbar sein können, auch wenn Sie beispielsweise Dinge nur für direkte Bekannte veröffentlichen. Meist ist dann auch die Auffindbarkeit über Suchmaschinen gegeben. Einmal veröffentlichte Informationen können i. d. R. praktisch nicht gelöscht werden.
   4. Erteilen Sie keine juristischen Ratschläge.
   5. Beachten Sie bei Ihren Äußerungen bestehende Schutzrechte und Schutzmarken. Dies gilt auch für Firmen- und Produktlogos.
   6. Versenden Sie niemals unerwünschte Werbung (Spam).
   7. Nehmen Sie Abstand von politischen Äußerungen, unsachlichen oder emotionalen Diskussionen, Beleidigungen, Rufschädigung, Bedrohungen und pornografischen Inhalten.
   8. Veröffentlichen Sie keine Informationen oder sonstige Äußerungen zum Unternehmen, zu Kolleginnen/Kollegen, Kunden, Partnern, Auftragnehmern, etc. Bedenken Sie, dass solche Äußerungen im Rahmen des Monitoring von Social Media durch das Unternehmen bemerkt werden können.
   9. Leiten Sie Anfragen zu beruflichen Themen in die entsprechenden Kanäle, damit u. a. die Nachvollziehbarkeit der Unternehmenskommunikation gewährleistet ist.

7. IT-Sicherheit

    1. Nutzen Sie soziale Medien nur mit ausreichend abgesicherten PCs. Die Nutzung mobiler Geräte (Tablet, PDA, etc.) in Verbindung mit entsprechenden Apps ist ***[erlaubt | untersagt | nicht empfohlen]***.

    2. Nutzen Sie soziale Medien nur aus sicheren und vertrauenswürdigen Netzwerken heraus. Nutzen Sie insbesondere keine unverschlüsselten WLANs.

    3. Bedenken sie stets, dass auch über soziale Medien Schadsoftware verbreitet werden kann. Beachten Sie die Sicherheitshinweise des BSI[9] allgemein sowie zu sozialen Medien im speziellen.

    4. Verwenden Sie für jede Internetanwendung, insbesondere auch wenn Sie in verschiedenen sozialen Medien angemeldet sind, ein unterschiedliches und sicheres Passwort.

    5. Klicken Sie nicht wahllos auf Links – soziale Medien werden verstärkt dazu genutzt, um Phishing zu betreiben.

8. Monitoring und Maßnahmen bei Verstößen

    1. Die Einhaltung der Dienstvereinbarung wird stichprobenartig überprüft. Bei beruflichen Accounts werden zudem regelmäßig die sicherheitsspezifischen Einstellungen geprüft.

    2. Ein Verstoß gegen die Dienstvereinbarung hat zur Folge, dass ***dem jeweiligen Mitarbeiter die berufliche Nutzung untersagt wird. Arbeitsrechtliche Konsequenzen sind ebenfalls möglich.***

9. Ansprechpartner im Unternehmen

    1. Innerhalb des Unternehmens sind ***die folgenden Ansprechpartner*** definiert, die bei Fragen kontaktiert oder bei Problemen im Rahmen der beruflichen Nutzung umgehend informiert werden sollten:

9 BSI für Bürger, https://www.bsi-fuer-buerger.de