







Checkliste IT-Sicherheit

aufgrund eines Beschlusses
des Deutschen Bundestages


IT-Sicherheit in sozialen Netzwerken

Gefahr/ Risiko	Erhebung des Ist-Zustands	Maßnahme
Zugriff durch Unbefugte	Verfügen die für Social Media genutzten Geräte (PC, Smartphone, Tablet) über einen ausreichenden Basisschutz inklusive Viren-Schutz, Personal Firewall und weiterer Sicherheitsanwendungen, die den Update-Status überwachen?	<p style="text-align: right;">Umgesetzt? </p> <p>Stellen Sie den Schutz mit Hilfe der „Checkliste Basisschutz“ her.</p>
	Haben Sie in den AGBs und Datenschutzbestimmungen geprüft, welche Rechte der Betreiber des Netzwerkes an den eigenen Bildern, Texten und Informationen bekommt?	<p style="text-align: right;">Umgesetzt? </p> <p>Klären Sie die Rechte des Betreibers, bevor Sie Daten im Netzwerk hochladen. Seien Sie sich über die mögliche Verwertung Ihrer Bilder und Texte bewusst.</p>
	Sind die Accounts aller Unternehmensprofile mit starken Passwörtern versehen?	<p style="text-align: right;">Umgesetzt? </p> <p>Vergeben Sie ausschließlich sehr starke Passwörter (vgl. Checkliste Basisschutz).</p>
	Wurde ein Verantwortlicher für den Bereich Social Media im Unternehmen festgelegt?	<p style="text-align: right;">Umgesetzt? </p> <p>Legen Sie einen bestimmten Personenkreis als Verantwortliche fest; dieser sollte die alleinige Kontrolle über die Verwaltung und Redaktion der Social-Media-Kanäle haben.</p>
Unangemessene/ Veraltete Inhalte	Werden die Social-Media-Kanäle täglich kontrolliert/betreut?	<p style="text-align: right;">Umgesetzt? </p> <p>Reduzieren Sie die Anzahl der Social-Media-Kanäle so, dass alle Kanäle täglich kontrolliert werden können.</p>
	Werden Drittanbieteranwendungen innerhalb sozialer Netzwerke genutzt?	<p style="text-align: right;">Umgesetzt? </p> <p>Verzichten Sie aus datenschutzrechtlichen Gründen auf die Nutzung von Drittanbieteranwendungen.</p>

Weitergabe an
Informationen an
Unbefugte

Sind die Privatsphäre-Einstellungen der genutzten Kanäle entsprechend eng gewählt, sodass möglichst wenige Informationen an unbefugte Dritte gelangen können?


Nein

Umgesetzt? 

Nutzen Sie die Möglichkeiten der Privatsphäreinstellungen; schränken Sie die Sichtbarkeit der Beiträge so ein, dass nur der gewünschte Personenkreis Zugriff auf diese hat. Aktivieren Sie das „Aktivitätenprotokoll“ zur Überprüfung von Markierungen (bei Facebook).

Gibt es eine Kommunikationsstrategie für die einzelnen sozialen Netzwerke?


Nein

Umgesetzt? 

Geben Sie niemals vertrauliche Daten wie Betriebsinterna preis. Sensibilisieren Sie auch Ihre Mitarbeiter dahingehend, so wenige Informationen wie möglich über die Organisation und Infrastruktur des Unternehmens (z.B. durch Fotos) öffentlich zu machen. Erstellen Sie hierzu eine Richtlinie (Social Media Guideline), die den Umgang mit sozialen Netzwerken beschreibt und Bestandteil des Arbeitsvertrages ist.

Werden Kontaktanfragen vor der Bestätigung kritisch geprüft?


Nein

Umgesetzt? 

Vergewissern Sie sich im Zweifel über einen anderen Kommunikationsweg (z.B. Telefon) über die Echtheit eines Profils.

Kennt das verantwortliche Social Media Team die Gefahren der sozialen Netze wie Clickjacking, Phishing und Social Engineering?

Ja

Umgesetzt? 

Hinterfragen Sie die geteilten Inhalte Ihrer Kontakte stets kritisch und überprüfen Sie diese auf Anzeichen für Betrugsversuche wie Clickjacking.

Nutzen Mitarbeiter soziale Netze für private Zwecke?


Ja

Umgesetzt? 

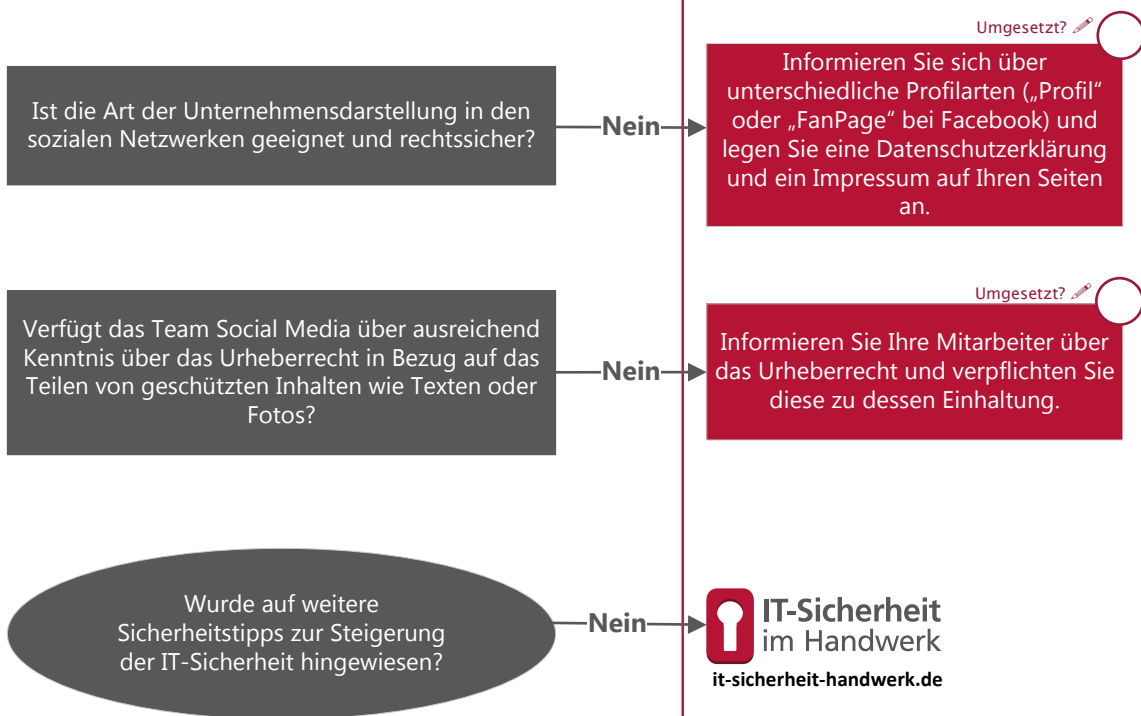
Weisen Sie Ihre Mitarbeiter auf die Gefahren des Social Engineering hin (vgl. „Checkliste Basisschutz“).

Nutzen Mitarbeiter soziale Netze für berufliche Zwecke und kommunizieren unter eigenem Namen auf den unternehmenseigenen Social-Media-Plattformen?

Ja

Umgesetzt? 

Legen Sie Richtlinien für eine professionelle Kommunikation auf den Unternehmensplattformen wie der Facebook-„FanPage“ fest bzw. fordern Sie die verantwortliche Person dazu auf, diese zu erstellen.



Task Force „IT-Sicherheit in der Wirtschaft“

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Die Task-Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task-Force und ihren Angeboten sind unter:

www.it-sicherheit-in-der-wirtschaft.de abrufbar

www.it-sicherheit-handwerk.de



itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.



Heinz-Piast-Institut für Handwerkstechnik an der Leibniz Universität Hannover



Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur



if(is)- Institut für Internet-Sicherheit der Westfälischen Hochschule