IT-Sicherheitsmanagement für Ihr Unternehmen

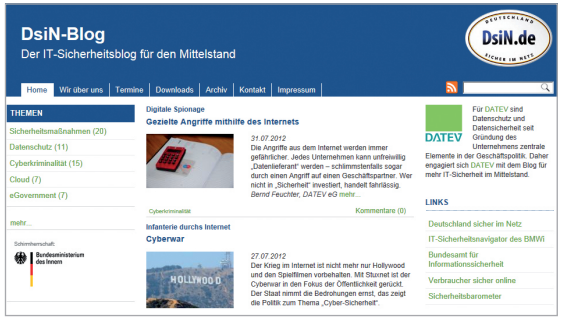
DsiN-Sicherheitscheck

Mit dem DsiN-Sicherheitscheck erhalten Sie einen Überblick über die Informationssicherheit in Ihrem Unternehmen. Der Fokus liegt auf der elektronischen Kommunikation, der Verfügbarkeit von IT-Systemen und mobilen Arbeitsweisen. Die Auswertung gibt Hinweise auf Ihren individuellen Handlungsbedarf. Mit den technischen und organisatorischen Empfehlungen von DsiN können Sie Ihre IT-Sicherheitslage verbessern.

www.sicher-im-netz.de/sicherheitscheck

IT-Sicherheitsblog für den Mittelstand

Im Blog von Deutschland sicher im Netz können Sie sich mit unseren IT-Sicherheits-Experten zu aktuellen IT-Fragen wie Cloud Computing und eGovernment austauschen. Zudem erhalten Sie Tipps zu wichtigen Sicherheitsmaßnahmen und Datenschutzfragen.



www.dsin-blog.de

Über Deutschland sicher im Netz e.V.

Produktneutral und herstellerübergreifend ist Deutschland sicher im Netz e.V. (DsiN) zentraler Ansprechpartner für Verbraucher und mittelständische Unternehmen zu Fragen der IT-Sicherheit.
DsiN unterstützt Unternehmen bei der Umsetzung eines bedarfsgerechten Sicherheitsmanagements, zum Beispiel mit leicht verständlichen Informationen zum Thema IT-Sicherheit, praxisrelevanten Checklisten, Leitfäden und konkreten Handlungsempfehlungen. Denn IT-Sicherheit ist eine wesentliche Grundlage für reibungslose Geschäftsabläufe.

Kontakt:

Deutschland sicher im Netz e.V.
Albrechtstraße 10 a
10117 Berlin
Tel. +49 (0) 30 27576-310
Fax +49 (0) 30 27576-51310
info@sicher-im-netz.de

www.sicher-im-netz.de
www.dsin-blog.de

Social Media – mit Sicherheit

IT-Sicherheit für Unternehmen

Schirmherrschaft

Bundesministerium des Innern

DEUTSCHLAND DsiN.de SICHER IM NETZ

Social Media für Unternehmen

Netzwerke, Blogs, Videoplattformen oder Kurznachrichtendienste nehmen für die Kommunikation mit Kunden, insbesondere mit jungen Zielgruppen, mittlerweile eine bedeutende Rolle ein. Die Hälfte aller Unternehmen nutzt bereits Soziale Medien.* Auch kleine und mittlere Unternehmen sollten überlegen, in welcher Weise der Einsatz von Social Media zur Steigerung der Markenbekanntheit und für den Erhalt der Wettbewerbsfähigkeit sinnvoll ist.

Anwendungsgebiete

Neben der schnellen und effizienten Kommunikation mit bestehenden Kunden, z. B. zu Servicefragen, lassen sich neue Zielgruppen und die nächste Kundengeneration erschließen. Dazu tragen die vielfältigen Empfehlungs- und Weiterleitungsfunktionen von Social Media bei. Einfache Umfragefunktionen bieten gute Möglichkeiten, um kostengünstig Marktforschung zu betreiben. Auch für die Ansprache potenzieller Mitarbeiter eignen sich Soziale Medien.

Sicherheit nicht vernachlässigen

Damit keine vertraulichen Informationen wie Kunden- oder Mitarbeiterdaten an die Öffentlichkeit geraten, sollten Sicherheitsaspekte bei der Kommunikation in Sozialen Netzwerken nicht vernachlässigt werden. Meist sind diese weniger technischer sondern vielmehr organisatorischer Natur. Für IT-Sicherheit trägt jeder Verantwortung, daher sollten Mitarbeiter kontinuierlich für die Gefahren sensibilisiert werden, die bei der öffentlichen Kommunikation in Sozialen Netzwerken entstehen können.

*Die BITKOM-Studie „Social Media in deutschen Unternehmen" ist auf www.bitkom.org verfügbar.

10 Regeln für die sichere Nutzung von Social Media

1. Eine **Social Media Guideline** – also eine Richtlinie, die den Umgang mit Sozialen Netzwerken beschreibt– ist idealerweise Bestandteil des Arbeitsvertrags. Um zu vermeiden, dass Geschäftsgeheimnisse an die Öffentlichkeit gelangen, sollten ein paar Regeln den Mitarbeitern deutlich machen, was vom Arbeitgeber gewünscht ist und was nicht. So ist es z.B. sinnvoll Themen zu benennen, die verstärkt bzw. keinesfalls in Social Media aufgegriffen werden.

2. Vor der Erstellung eines Auftritts in einem Sozialen Netzwerk ist in den **Allgemeinen Geschäftsbedingungen und Datenschutzbestimmungen** sorgfältig nachzulesen, welche Rechte die Betreiber an eigenen Bildern, Texten und Informationen bekommen.

3. Um **private und berufliche Äußerungen** klar zu trennen, sollten Mitarbeiter über separate Darstellungen in Sozialen Netzwerken auftreten. Beispiel privat: Lieschen Müller, Beispiel beruflich: Lieschen Müller, Firma XY.

4. Alle Zugänge sollten durch **sichere Passwörter** geschützt werden, die mindestens 8 Zeichen lang sind sowie Klein- und Großschreibung, Ziffern und Sonderzeichen beinhalten.

5. Konkurrenten können soziale Netzwerke für **Social Engineering**, also das Ausspähen von Wettbewerbern, nutzen. Kontaktanfragen sollten daher vor der Bestätigung kritisch geprüft werden. In den Einstellungen sollte festgelegt sein, dass fremde Personen nicht die eigenen Kontakte einsehen können.

6. Berührungsängste mit Sozialen Netzwerken können z. B. durch einen Workshop abgebaut werden, bei dem sich Mitarbeiter über ihre **Erfahrungen austauschen**. Bevor ein Mitarbeiter selbst als Autor aktiv wird, sollte er als „Follower" bzw. Leser Erfahrungen sammeln.

7. Vor der Verwendung von Fotos sollte sichergestellt werden, dass die Bildrechte auch für Online-Medien erworben wurden. Zudem ist ein Impressum bei allen Internetangeboten Pflicht. So können teure **Abmahnungen** vermieden werden.

8. Kriminelle nutzen Soziale Netzwerke für **Phishing**, also den Diebstahl von Zugangs- und Zahlungsdaten. Daher sollten Mitarbeiter nicht unvorsichtig auf Links klicken und keinesfalls auf dahinterliegenden, gefälschten Seiten Benutzernamen und Kennwörter eingeben.

9. **Diskussionskultur:** In manchen Foren und Diskussionsgruppen kommentieren Nutzer Unternehmenseinträge extrem kritisch oder beleidigend. Um Image-Schäden zu vermeiden, sollten die Mitarbeiter die Vorwürfe in Ruhe mit dem Vorgesetzten besprechen. Es empfiehlt sich, die Vorwürfe sachlich zu beantworten, die Diskussion dabei aber nicht endlos zu führen.

10. Äußern sich Mitarbeiter in Sozialen Netzwerken in unerwünschter Form, so gilt die Reihenfolge Ermahnung, Abmahnung, Kündigung. Bei schwierigen Fällen in den Bereichen Personal, Recht und Business Development ist es ggf. sinnvoll, sich extern **beraten zu lassen**.