

Link: <https://www.computerwoche.de/a/studie-attestiert-unternehmen-zu-grosse-fahrlaessigkeit-mit-web-2-0-inhalten,1897133>

Sicherheit

Studie attestiert Unternehmen zu große Fahrlässigkeit mit Web-2.0-Inhalten

Datum: 28.05.2009
Autor(en):Uli Ries

Laut einer aktuellen Studie können Mitarbeiter in nahezu jedem Unternehmen Blogs, soziale Netzwerke, Foto- und Videoportale und andere Web-2.0-Elemente am Arbeitsplatz nutzen. Allerdings schützen sich die wenigsten Unternehmen gegen die damit verbundenen spezifischen Gefahren.

Die im Auftrag von **Websense**¹ von dem britischen Marktforschungsunternehmen **Dynamic Markets**² weltweit unter 1.300 IT-Managern durchgeführte Studie **Web2.0@Work**³ zeigt eine bedenkliche Fahrlässigkeit beim Bewusstsein von und Umgang mit typischen Web-2.0-Gefahren wie der Malware-Installation oder dem Export vertraulicher Unternehmensdaten auf.

Befragt wurden IT-Manager von Unternehmen mit mindestens 250 PC-Usern aus Australien, China, Deutschland, Frankreich, Großbritannien, Hongkong, Indien, Italien, Kanada sowie den USA. Pro Land führte Dynamic Markets 100 Interviews durch, in den USA waren es 400. 68 Prozent der Interviewpartner hatten Führungsverantwortung, 32 Prozent waren CIOs oder IT-Direktoren.

Die Nutzung von Web-2.0-Diensten wie Blogs, Wikis und sozialen Netzwerken ist in 95 Prozent der befragten Unternehmen erlaubt. Man nutzt sie, um Informationen auszutauschen, **Geschäftsprozesse**⁴ zu optimieren, Partner einzubinden und Umsatz zu generieren. Darin sehen 62 Prozent der Befragten einen Vorteil fürs Geschäft. 86 Prozent der IT-Manager bestätigen eine steigende Nachfrage nach Web-2.0-Seiten und -Technologien in ihrem Unternehmen. Diese Nachfrage geht von Fachabteilungen (34 Prozent Marketing, 32 Prozent Vertrieb), aber auch von der Vorstandsebene (30 Prozent) aus. Lediglich 50 Prozent der Befragten ordnen übrigens Wikis, YouTube oder **Cloud-Computing**⁵-Seiten wie **Google Docs**⁶ überhaupt in die Kategorie Web 2.0 ein.

80 Prozent der Befragten glaubten, dass ihr Unternehmen genügend für Web-Sicherheit tut, mussten jedoch nachfolgend erhebliche Sicherheitslücken einräumen. So nehmen 68 Prozent keine Echtzeitanalyse von Web-Inhalten vor. 59 Prozent können keinen URL-Re-Direct - die Weiterleitung von einer vertrauenswürdigen auf eine gefälschte Webseite - unterbinden. 53 Prozent können nicht verhindern, dass Spionagesoftware interne Daten an Bot-Netze überträgt. 52 Prozent verfügen nicht über eine Lösung zur Entdeckung bössartigen Programmcodes auf bekannten und vertrauten Webseiten. 45 Prozent sind nicht in der Lage, den Export vertraulicher Daten an Blogs, Wikis oder andere Cloud-Webseiten zu unterbinden. Und nur 9 Prozent nutzen Sicherheitslösungen, die alle genannten Risiken abdecken.

47 Prozent der Befragten berichten, dass Anwender immer wieder versuchen, die Web-Security-Richtlinien zu umgehen. Neu einzuführende Maßnahmen müssen Anwendern daher so viele Freiheiten wie möglich einräumen, aber so viel Sicherheit wie nötig zu garantieren.

Analysen der **Websense Security Labs**⁷ belegen, dass 57 Prozent des Datenklau per Internet erfolgt. Gerade Web-2.0-Seiten, auf denen User persönliche Daten veröffentlichen, bieten ein attraktives Ziel für **Cyber-Kriminelle**⁸. Mehr als 90 Prozent aller Organisationen können die bekannten Web-2.0-Gefahren und -Risiken nicht eliminieren; es gäbe bestenfalls "einzelne Inseln der Sicherheit". Aber auch Privatanwender sollten sich genau anschauen, welcher Webseite sie persönliche Daten anvertrauen.

Die Ergebnisse der Umfrage belegen, dass Unternehmen bislang nur in Ausnahmefällen die Vorteile des Web 2.0 sicher nutzen können. Ein generelles Zugangsverbot sei kein gangbarer Weg, da gerade jüngere Mitarbeiter privat soziale Netzwerke, Blogs, Wikis & Co nutzen und dies auch für ihren Arbeitsplatz erwarten. Unternehmen müssen daher mit Sicherheitsmaßnahmen reagieren, die den Zugang zu sicheren Web-2.0-Elemente erlauben und als riskant eingestufte Inhalte nicht zugänglich machen.

Links im Artikel:

¹ <http://www.websense.com/global/de/>

² <http://www.dynamicmarkets.co.uk/>

³ <http://www.websense.com/content/web20-at-work.aspx>

⁴ https://www.computerwoche.de/knowledge_center/soa_bpm/1869128/

⁵ https://www.computerwoche.de/knowledge_center/software_infrastruktur/cloud-computing/

⁶ <http://docs.google.com/>

⁷ <http://securitylabs.websense.com/>

⁸ <https://www.computerwoche.de/schwerpunkt/c/Cyber-Kriminelle.html>

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.