Appell an die eigene Verantwortung

SICHERHEITSRISIKO SOCIAL MEDIA

Facebook, Twitter, Xing... soziale Netzwerke erfreuen sich großer Beliebtheit, sind aber auch ein Einfallstor für kriminelle Machenschaften. Wie müssen Unternehmen damit umgehen – hilft etwa ein Nutzungsverbot für Mitarbeiter?

Soziale Netzwerke als kostengünstige Kommunikationskanäle mit großer Reichweite bieten für ihre Nutzer zahllose Möglichkeiten, sei es für den lockeren Austausch unter Gleichgesinnten, die Anbahnung beruflicher Kontakte oder die Nutzung für gezielte Marketingmaßnahmen und Imagekampagnen. Die Userzahlen kennen bisher nur den Weg nach oben. Die Gefahren, die mit der Nutzung dieser Plattformen verbunden sind, werden allerdings häufig nicht bedacht, auch zum Nachteil der Unternehmen. Denn wo sich so viele Personen tummeln, sind kriminelle Kräfte nicht weit. „Nahezu alle Angriffe auf Unternehmensdaten haben mittlerweile ihren Ursprung in den sozialen Netzwerken“, warnt Markus Geier, Geschäftsführer des Sicherheitsunternehmens Comcode. „Es besteht also für alle Unternehmen, die sich mit dieser Thematik bisher noch nicht auseinandergesetzt haben, dringender Handlungsbedarf.“

SOCIAL MEDIA ALS QUELLE VERTRAULICHER DATEN

Laut Geier recherchieren die Angreifer in den Netzwerken als erstes alle verfügbaren Informationen über das Zielunternehmen. Dazu gehören auch Daten über dort Beschäftigte. „Leider verbreiten viele Mitarbeiter recht sorglos sensible Daten im Netz, zum Beispiel detaillierte Informationen über ihren Verantwortungsbereich innerhalb der Firma. Wenn dann noch die Privatsphäre-Einstellungen nicht aktiviert sind, haben die Angreifer leichtes Spiel. Denn dann kann jeder alles lesen, inklusive Geschäftskontakte oder Freundesliste“, so der Experte. Genau diese Mitarbeiter werden in einem nächsten Schritt etwa über einen gefälschten Account kontaktiert, um an weitere Daten zu kommen. Da gibt es dann ganz harmlos wirkende Freundschaftsanfragen. Damit soll ein vertrauliches und persönliches Verhältnis zur Kontaktperson aufgebaut werden. Oder es wird versucht, in Form von Phishing-Mails Schadsoftware wie Trojaner und Viren ins Firmennetzwerk einzuschleusen. Auch Anfragen über das Telefon gehören zum Repertoire.

VERBOTE GREIFEN ZU KURZ

„Die Erfolgsquote solcher Angriffe ist enorm. Im Schnitt geben rund 80 Prozent der direkt adressierten Kontaktpersonen gutgläubig Daten weiter – auch sehr sensible“, sagt Geier, und ergänzt: „Wenn uns ein Unternehmen beauftragt, einen Scheinangriff auf das Unternehmen durchzuführen, sind wir häufig immer wieder überrascht, wie

Einen kurzen und anschaulichen Videofilm zum Thema „Cyber Security und Social Media“ gibt es auf dem Portal der News.

Markus Geier ist Experte für Cyber-Sicherheit und Geschäftsführer der ComCode GmbH (www.comcode.de) mit Sitz in Gröbenzell bei München.

viele Informationen in sozialen Netzwerken dargeboten werden und wie leicht diese für Angriffsmaßnahmen nutzbar sind.“ Er empfiehlt Unternehmen, dies unbedingt in ihren Sicherheitsüberlegungen zu berücksichtigen. Aber wie? Von einem generellen Nutzungsverbot hält Geier wenig. „Soziale Medien gehören heute einfach zu unserem Leben dazu – privat wie geschäftlich. Ein rigoroses Verbot greift deshalb zu kurz und könnte sich zudem als kontraproduktiv herausstellen. Regelungen im Umgang mit Social Media sind dagegen meiner Ansicht nach ein wirkungsvolleres Instrument.“ Dabei müsse das Rad nicht gänzlich neu erfunden werden, da vieles bereits in den Arbeitsverträgen stehen würde, beispielsweise die Verschwiegenheitsverpflichtung in Bezug auf die Weitergabe von Interna. Wichtige Regelungen könnten zudem folgende Punkte betreffen:

- Wann darf auf die sozialen Netzwerke zugriffen werden?
- Wer bekommt eingeschränkten (Anwender ohne direkte geschäftliche Nutzung), wer uneingeschränkten Zugang (zum Beispiel die Marketing-Abteilung)?
- Verbot Dateien hoch- bzw. runterzuladen (zum Beispiel Facebook-Downloads)
- Welche Informationen dürfen auf den Portalen kommuniziert werden, welche sind unternehmensintern
- Sensibilisierung für Gefahren anhand anschaulicher Beispiele
- Differenzierung zwischen privater und beruflicher Nutzung

„Mit einem Regelungswerk, das an die Vernunft und das Verantwortungsbewusstsein der Mitarbeiter appelliert, sich konstruktiv mit der Sache befasst, kommt man weiter als mit einer Liste an Verboten“, ist Geier überzeugt. „Inzwischen gibt es auch Technologien wie „Next Generation Firewalls“, die sich von den Unternehmen so einstellen lassen, dass die Dateiübertragungen eingeschränkt werden.“ Der Experte empfiehlt zudem den Gebrauch der Privatsphäre-Einstellungen, die es bei Facebook und Co. gibt. „Somit wird es für Außenstehende weitaus schwieriger, an Informationen wie Geschäftskontakte zu kommen.“ Einen Haken gebe es dennoch: „Wie in der Vergangenheit öfters geschehen, können die Betreiber dieser Portale ihre Geschäftsbedingungen jederzeit ändern und plötzlich sind vertrauliche Infos für jeden abrufbar. Das heißt, Veränderungen auf den Plattformen müssen immer im Auge behalten werden.“ ■ *-hf*

TIPPS VOM SICHERHEITSEXPERTEN

Unternehmen sollten...

- ihre Mitarbeiter zum bewussten Umgang mit Social Media motivieren
- auf die Verschwiegenheitspflicht verweisen und Beispiele für unerlaubte Informationen aufzeigen
- die Nutzung sozialer Medien mittels einer Richtlinien regulieren und dazu auch unterstützende Sicherheitstechnologien einsetzen. Diese helfen, Angriffe abzuwehren.
- von Zeit zu Zeit Analysen durchführen, welche Informationen über das Unternehmen im Netz stehen.
- ihren Mitarbeiter aktuelle Informationen zu Gefahren und Neuerungen zur Verfügung stellen.