WWW.NETWORK-KARRIERE.COM

09.2018 4,75 €

NETWORK-KARRIERE

EUROPAS GRÖSSTE WIRTSCHAFTSZEITUNG FÜR DEN DIREKTVERTRIEB

Guido Bierther, 18 Jahre Airnergy: belächelt, beschimpft – bestaunt, belohnt.

Aaron Palmer, Rain International: Seed Nutrition: Neue Chancen erkennen und die Welt verändern.

Sophie Zillmann, Zija International: Zija Natural Health Revolution bietet außergewöhnliche Karriere- und Geschäftsmöglichkeiten.

Andreas Friesch, LR Health & Beauty: Führungswechsel bei LR Health & Beauty: Andreas Friesch zum neuen CEO bestellt.

4 196668 504755 09

www.seitz-mediengruppe.de

NETWORK-KARRIERE VERBINDET

RUFMORD: VIRTUELLE ATTACKEN MIT REALEN KONSEQUENZEN

Fotolia/© FotolEdhar

Facebook, Twitter, XING: Längst profitieren große Unternehmen von den interaktiven Anwendungen des Social Web. Auch im Mittelstand wächst langsam ein Bewusstsein für das enorme Potenzial des viel zitierten Web 2.0, die Nähe der Firma zur Zielgruppe zu steigern. Dabei bildet das gute Ansehen eines Betriebs einen der zentralen Erfolgsfaktoren für funktionierende Kundenbindung. Was jedoch speziell kleine und mittelständische Unternehmen unterschätzen: Besonders im Internet ist ihre Reputation leicht angreifbar. Denn der virtuelle Raum bietet ohne regulative Mechanismen den perfekten Nährboden für mediale Angriffe und die Verbreitung von diffamierenden Behauptungen. Hier ist Aufklärung in Form von professioneller Beratung gefragt und im Anschluss eine erste Umsetzung zumindest kleiner Schritte.

Fotolia/© pressmaster

Genauso divers wie die digitalen Möglichkeiten, so unterschiedlich präsentieren sich die Bedrohungsszenarien, mit denen sich Firmen im digitalen Zeitalter konfrontiert sehen. Längst interessieren sich Erpresser, unlautere Konkurrenten und frustrierte Geschäftspartner nicht mehr nur für das Know-how eines Betriebs. Immer häufiger attackieren sie gezielt den guten Ruf eines Unternehmens. Dabei reicht die Bandbreite dieser Angriffe von banalen Racheakten ehemaliger Mitarbeiter bis hin zu politisch motivierten Kampagnen von Aktivisten wie Anonymous. Dementsprechend kann auch jede Branche solchen Attacken zum Opfer fallen. Freiberufler wie Ärzte oder Anwälte sind genauso beliebte Ziele wie mittelständische Automobilzulieferer, größere Maschinenbauer oder Handwerksbetriebe mit lokaler Verankerung. Fest steht: Im sogenannten Darknet kann nahezu jeder das nötige Rüstzeug erwerben, um das Ansehen eines Unternehmens wirkungsvoll zu schädigen. Dafür benötigen potenzielle Aggressoren nicht einmal spezielle Computerkenntnisse. Ein paar gezielte Mausklicks und schon verbreiten Fake News sowie negative Kommentare sich auf stark frequentierten Bewertungsportalen oder werden über Facebook oder Twitter geteilt. Selbst größer angelegte Online-Offensiven sind mit wenig mehr Aufwand verbunden: Dabei bilden DDoS-Attacken, die den Unternehmensserver lahmlegen, und gesteuerte Astroturf-Kampagnen in sozialen Netzwerken, die schlechte Bewertungen durch eine vermeintliche Graswurzelbewegung vortäuschen, keine Seltenheit. Doch ganz egal, wie der Angriff erfolgt, eines haben diese Methoden alle gemein: Sie beschädigen das Image des Unternehmens nachhaltig. Denn obwohl die Öffentlichkeit im Netz zunächst rein virtuell scheint, ist sie erschreckend real. Besonders die wirtschaftlichen Folgen durch geplatzte Deals oder verärgerte Kunden bleiben über Jahre hinweg spürbar und können somit offline zum existenzgefährdenden Risiko heranwachsen.

Auf Prävention setzen

Entsprechend wichtig ist es, bereits im Vorfeld Krisenpotenziale ausfindig zu machen, ein Bedrohungsbild zu entwerfen und einen entsprechenden Maßnahmenkatalog zu konzipieren. In der Regel benötigen Unternehmen hierfür keinen riesigen Sicherheitsapparat, sondern individuell ausgearbeitete Konzepte, die sinnvolle Technik mit entsprechendem Personal und organisatorischen Maßnahmen verbinden. Dazu gehören neben den klassischen Schutzvorkehrungen wie Antiviren-Programme und Firewalls auch spezielle Sicherheitssoftware-Programme und Verschlüsselungstechniken. Besonders bei DDoS-Attacken, Trojanern und Viren, die ganze Systeme lahmlegen, gibt es jedoch immer wieder neue Muster und Bandbreiten. Diese ändern sich zum Teil sogar täglich, weshalb in allererster Linie auch der Faktor Mensch nicht außer Acht gelassen werden darf. In der Praxis zeigt sich immer wieder, dass gerade Mitarbeiter, ob durch leichtsinniges Verhalten oder Unwissenheit, ein großer Schwachpunkt in der Unternehmenssicherheit bleiben. Hier gilt es das Personal in speziellen Awareness-Trainings zu sensibilisieren und bestimmte Verhaltensregeln, beispielsweise für den Umgang mit Passwörtern, aufzustellen. Nur wer über Gefahren durch elektronische Kommunikationsmöglichkeiten und soziale Netzwerke informiert ist, kann aktiv mit seinem Verhalten zum Unternehmensschutz beitragen.

Schaden eindämmen

Tritt der Ernstfall trotz Präventionsmaßnahmen ein, greift ein entsprechend ausgearbeiteter Notfallplan, um den Schaden zu begrenzen. Dieser verschafft Klarheit über Handlungsweisen und führt auch in Ausnahmesituationen zu besser aufeinander abgestimmten Entscheidungen und effizientem Handeln. Grundsätzlich sollte aber für existenzbedrohende Ereignisse ein Krisenmanagement auf strategischer Ebene bestehen. Um trotz Totalausfall der firmeneigenen Webseite oder der Sabotage von Fertigungsanlagen die Fortführung der Geschäfte zu gewährleisten, sind bestimmte Organisationsmerkmale von Bedeutung. Dazu zählen neben der Festlegung der Kommunikationskanäle und der Einrichtung eines Krisenstabes auch Vorkehrungen, die den möglichen Imageverlust so gering wie möglich halten. Hier setzt das Reputationsmanagement an. Das bedeutet nicht nur die externe Kommunikation beispielsweise durch entsprechende Sprachregelungen zu steuern. Besonders im Zusammenhang mit IT-Vorfällen geht es auch darum, Ursachen schnell zu erkennen, um Angriffe zeitnah aufzuklären. Wer hier über keine eigenen Spezialisten im Bereich Unternehmenssicherheit und IT-Forensik verfügt, findet Hilfe bei externen Beratern der Sicherheitsbranche. Diese Experten geben nicht nur Maßnahmenempfehlungen, sondern untersuchen auch verdächtige Vorfälle durch genaue Erfassung, Analyse sowie Auswertung und Sicherung digitaler Spuren. Denn nur durch die umfassende Kenntnis der Sachlage ist es möglich, den Tätern auf die Schliche zu kommen. Und trotzdem: Um größere Schäden effektiv einzudämmen, bleiben besonders präventive Schutzmaßnahmen unumgänglich.

VITA

Markus Weidenauer

Markus Weidenauer ist geschäftsführender Gesellschafter der SecCon Group GmbH. Als Experte ist er bundesweit auf das Erstellen von individuellen Sicherheitskonzepten und deren Umsetzung spezialisiert. Neben Personenschutz für exponierte Familien und Einzelpersonen bietet er auch Gefahrenabwehr sowie Notfall- und Krisenmanagement für Unternehmen.

http://seccon-group.de