German
Business Protection

Risk Consultancy
Business Enablement
Compliance & Security

Sicherheitslagebild Deutschland

März 2017

Berlin, den 10. März 2017

Hotline	+49 30 63967027-0
Fax	+49 30 63967027-99
E-Mail	info@gbp-security.com
Internet	gbp-security.com

Wie sich Sicherheitslücken negativ auf den Wert Ihrer Marke auswirken können

Häufig wird über den „Wert“ einer Marke gesprochen – aber worin besteht dieser eigentlich? Der Wert einer Marke besteht nicht nur aus den finanztechnischen Kennzahlen und Bewertungen. Er spiegelt sich nicht zuletzt auch darin wieder, wie viele Menschen Produkte einer Marke gegenüber den jeweiligen Konkurrenzprodukten präferieren. Die Menschen sind häufig sogar bereit, einen höheren Preis für ein begehrtes, also „wertvolles“ Produkt, wie bspw. Apples Iphone zu bezahlen, auch wenn die alternativen Produkte am Markt eine quasi identische Leistung aufweisen. Starke Marken können häufig einen höheren Verkaufspreis für ihr Produkt verlangen, was zu höheren Gewinnen führt.

Um eine starke Marke aufzubauen braucht es mitunter Jahre oder Jahrzehnte. Hingegen kann der Wert einer Marke sehr schnell verschwinden, wenn die positive Wahrnehmung des Produkts oder der Dienstleistung in Frage gestellt wird. In der Vergangenheit verloren Marken ihren Wert häufig aufgrund einer Vielzahl von Ereignissen, wie z.B. Produktrückrufen, Produktausfällen oder mangelnder Zuverlässigkeit eines Produkts, wie man zuletzt eindrucksvoll am Unternehmen Volkswagen sehen konnte, dessen Marktwert nach Bekanntwerden des Abgasskandals zwischenzeitlich um mehr als 50% eingebrochen war und die Marke VW im weltweiten Ansehen hat sinken lassen.

Das Internetzeitalter hat neben den beschriebenen Gefahren zudem eine weitere Dimension, nämlich die Problematik eines adäquaten Schutzes von Markenwerten, eröffnet. Heutzutage sind Webseiten und Webanwendungen der sichtbarste und zunehmend anfälligste Teil der Infrastruktur eines Unternehmens. Es ist keine Überraschung, dass Cyberkriminelle täglich Tausende von Webseiten auf der Suche nach Schwachstellen scannen.

Wenn eine Sicherheitslücke von Hackern entdeckt wird, sind es nicht nur Verbraucherdaten die kompromittiert werden. Wenn öffentlich bekannt wird, dass eine Sicherheitslücke identifiziert und ausgenutzt wird, fallen dadurch das Verbrauchervertrauen in das Produkt sowie das Vertrauen in die Marke selbst, was häufig zu sinkenden Verkäufen sowie zu einem sofortigen Umsatzrückgang führen kann. Dies kann wiederum in langfristigen Umsatzverlusten münden, welche in Reaktion massive Investitionen seitens des Unternehmens nach sich ziehen, in dem Versuch, das Vertrauen der Verbraucher zurückzugewinnen. Derartige Sicherheitslücken sorgen für Schlagzeilen in den Medien, insbesondere wenn große Unternehmen und ihre Marken betroffen sind. Als Beispiel sei hier die vor einigen Tagen entdeckte Sicherheitslücke bei Samsung Smart-TV’s zu nennen, deren Auswirkung sich womöglich erneut negativ auf die Verkaufszahlen sowie auf das ohnehin angeschlagene Image der Marke Samsung auswirken könnte.

Gerade kleine und mittlere Unternehmen (KMU) machen den Fehler zu denken, dass ihre geringere Größe sie automatisch immun gegen derartige Bedrohungen macht, dabei wirken sich derartig negative Schlagzeilen gerade für kleinere Marken oftmals direkt existenzbedrohend aus. Deshalb sollten speziell auch KMUs davon ausgehen, dass gerade sie von Cyberkriminellen mindestens gleichermaßen bedroht sind. Angesichts der Tatsache, dass solche Firmen häufig nicht über die finanziellen Mittel verfügen wie große Unternehmen, ist die Existenzbedrohung für KMUs tatsächlich häufig sogar größer.

Daher ist es gerade auch für KMUs sehr wichtig, derartige Probleme ernst zu nehmen und proaktiv zu handeln, um Cyberkriminelle abzuschrecken. Dies bedeutet insbesondere, dass die Unternehmen ihre Webseiten und Webanwendungen entsprechend schützen und ihre Mitarbeiter auf die Einhaltung klarer Regeln beim Umgang mit sensiblen Kundendaten schulen müssen. Die Umsetzung des BSI-Grundschutzkonzeptes und/oder die unternehmensweite Implementierung der ISO 27001 ist dabei häufig ein sinnvoller erster Schritt; jedoch müssen diese Strukturen auch von allen Mitarbeitern im Unternehmen gelebt werden. Technologie hilft, aber es darf nicht vergessen werden, dass es meistens der Angestellte oder Geschäftspartner ist, der das schwächste Glied bei der Verteidigung von Unternehmensdaten ist weshalb es diese besonders für diese Gefahren zu sensibilisieren gilt.

Disclaimer: Beurteilungen von Sicherheitslagen beruhen auf den zum angegebenen Zeitpunkt verfügbaren und als vertrauenswürdig eingeschätzten Informationen der German Business Protection (GBP). Obwohl bei der Zusammenstellung der Informationen größte Sorgfalt angewandt wurde, kann GBP für die Aktualität, Richtigkeit oder Vollständigkeit keine Gewähr übernehmen. In keinem Fall kann GBP für etwaige Schäden irgendwelcher Art verantwortlich gemacht werden, die durch die Verwendung der hier bereitgestellten Informationen entstehen, seien es direkte oder indirekte Schäden bzw. Folgeschäden einschließlich entgangenen Gewinns. Gefahrenlagen sind oft unübersichtlich und können sich rasch ändern.