mci

Cyber Attacks & Data Security in der Eventbranche

WIE VERANSTALTUNGEN VOR CYBER-ANGRIFFEN
EFFEKTIV GESCHÜTZT WERDEN KÖNNEN

Inhaltsverzeichnis

1. Einleitung

Die Welt befindet sich in einem rapiden technologischen Wandel, der sich auf alle Bereiche unseres Zusammenlebens erstreckt. Der Mensch des 21. Jahrhunderts ist umfassend digital vernetzt und verwaltet einen Großteil seiner privaten und beruflichen Daten online. Dies hat selbstverständlich Auswirkungen auf die Kommunikation zwischen Unternehmen und Kunden.

In der Eventbranche wird durch moderne Technik ein Besuchererlebnis ermöglicht, das einen schnellen und gezielten Informationsaustausch fördern soll. So lassen sich Kontaktdaten schnell erfassen und mit einem Klick speichern, nachdem online verfügbare Unternehmenspräsentationen oder Spiele Lust auf die jeweiligen Dienstleistungen oder Produkte gemacht haben. Informationen wie Kreditkartennummern, persönliche Daten und/oder Social-Media-Profildaten müssen jedoch vertraulich behandelt und ausreichend geschützt werden.

Das vorliegende Whitepaper beschäftigt sich mit dem Thema „Cyber-Security in der Eventbranche“ und behandelt im Kern die Gefahren eines Cyber-Angriffs auf Eventdaten. Veranstaltern und Organisatoren sollen Möglichkeiten und Maßnahmen gezeigt werden, um Kundendaten effektiv gegen derartige Angriffe zu schützen und das Event zum Erfolg zu führen.

2.Cyber-Security: Grundsätzliches

Wie können Veranstalter sensible Registrierungsdaten, die einfach in Felder eingetragen oder abgehakt werden, vor unbefugtem Zugriff schützen? Der geeignete Schutz solcher Daten ist seit geraumer Zeit ein heißes Thema in der Event-Branche.

2.1. Warum wird Cyber-Security benötigt?

Der Sicherheitszustand des Webs wurde im vergangenen Jahrzehnt besonders von staatlich organisierten Gruppen infrage gestellt, die sich unter dem Vorsatz der „Vorbeugung“, aber leider auch der destruktiven „Unruhestiftung“ unerlaubten Zugang zu ausländischen Datenbanken verschafft haben.

Hacktivismus ist ein weiterer Fokus, der nicht übersehen werden darf, denn auch positive Absichten eines „Anonymous“-Hackers könnten die Sicherheit der Registrierungsdaten und damit die Reputation des Veranstalters gefährden. Die zunehmende Vernetzung zwischen Event-Teilnehmern untereinander sowie zwischen Teilnehmern und Veranstaltern, macht eine effektive Sicherung der digitalen Schnittstellen unentbehrlich.

Damit ein „High-Profile-Event“ nicht Opfer einer Cyber-Attacke wird, müssen spezielle Maßnahmen etabliert sein, die einem externen Datenzugriff vorbeugen. Hierzu zählen vor allem eine von Experten im Vorhinein zu erstellende Risikoanalyse aller Event-Prozesse sowie die Früherkennung von Systemfehlern und -lücken, die durch Hacker ausgenutzt werden könnten.

7. Die steigende Verantwortung für Event-Manager

Der rapide Fortschritt in der Soft- und Hardware-Entwicklung und die zunehmende Automatisierung versprechen auf den ersten Blick, zukünftig weniger Zeit in die Pflege von Daten investieren zu müssen. Doch in den herkömmlichen Event-Softwares sind zahlreiche Schritte noch immer von Anwendern auszuführen und zu überprüfen. Hinzu kommt eine wachsende Bedrohung durch Hacker und Cyber-Terroristen, die es auf sensible Informationen abgesehen haben.

Mit der Einführung der neuen DSGVO „müssen Organisatoren [...] wesentlich höhere Standards im Hinblick auf den Umgang mit personenbezogenen Daten schaffen als bislang“[1]. Außerdem müssen sie dafür bürgen können, dass alle Drittanbieter (z. B. Hotels, Reiseveranstalter etc.) DSGVO-konform arbeiten.

Ein Veranstalter muss wissen, wie viele Informationen für die Registrierung notwendig sind, um nicht zu viel speichern zu müssen. Dennoch dürfen keine wichtigen Fragen bei der Anmeldung vergessen werden, um einen reibungslosen Ablauf zu ermöglichen.

In enger Absprache mit Experten und mit Blick auf die Risikoanalyse muss der Veranstalter darüber entscheiden, wie viel Cyber-Security für das Event angemessen ist. Wenn sich durch eine entsprechende Risikoanalyse die besondere Gefährdung eines Events herausstellt, so muss das Management der Cyber-Security entsprechend gut organisiert sein, um dem hohen Risiko standzuhalten.

1 https://www.events-magazin.de/eventbranche/diese-auswirkungen-hat-die-europaeische-datenschutzgrundverordnung-auf-events/?utm_source=eventsmagazine_daily_nl&utm_campaign=Diese_Auswirkungen_hat_die_Europ%C3%A4ische_Datenschutzgrundverordnung_auf_Events_150218&utm_medium=email

Ihr Kontakt zu MCI

Max Burger (MCI Berlin)
Director Business Development
MCI | Germany

MCI Deutschland GmbH
Markgrafenstraße 56
10117 Berlin | Germany

Telefon: +49 30 20459426
E-Mail: max.burger@mci-group.com

Christoph Wittfeld (MCI Düsseldorf)
Director Business Development
MCI | Germany - Rhein-Ruhr

MCI Deutschland GmbH
Adlerstraße 74
40211 Düsseldorf | Germany

Telefon: +49 211 67935188
E-Mail: christoph.wittfeld@mci-group.com

Bildernachweise

Cover ..... © monsitj / fotolia
Inhalsverzeichnis ..... © kras99
Seite 3 ..... © sdecoret
Seite 4 ..... © Sashkin
Seite 5 ..... © HQUALITY
Seite 6 ..... © Gorodenkoff
Seite 7 ..... © THANANIT
Seite 8 ..... © monsitj
Seite 10 ..... © Gennady Danilkin
Seite 11 ..... © Nikolay N. Antonov
Seite 14 ..... © MCI
Seite 16 ..... © nd3000
Seite 17 ..... © Rawpixel.com