

PRESSEMITTEILUNG

Berlin, den 16. Oktober 2026

Cybersecurity in der Hotellerie: HSMA Deutschland e.V. fordert mehr Transparenz bei Sicherheitsvorfällen

Der Fachverband mahnt zur Einhaltung gesetzlicher Meldepflichten und setzt auf eine offene Kommunikation, um die Cybersecurity in der Branche zu stärken.

Cyberangriffe auf Hotels haben ihren Ursprung häufig bei externen Technologieanbietern. Buchungssysteme, Property Management Systeme (PMS), Channel Manager oder Zahlungsdienstleister tauschen kontinuierlich Daten aus. Sicherheitslücken bei einem Anbieter können deshalb zahlreiche Hotelbetriebe betreffen. Die Hospitality Sales & Marketing Association Deutschland e.V. (HSMA) fordert daher mehr Transparenz bei Sicherheitsvorfällen sowie die konsequente Einhaltung gesetzlicher und vertraglicher Informationspflichten.

Vernetzte Systeme, gemeinsame Verantwortung

Mit der Digitalisierung wachsen die Abhängigkeit von externen Dienstleistern und die Zahl technischer Schnittstellen. Hotels müssen deshalb nicht nur ihre eigene IT schützen, sondern auch die Sicherheitsprozesse ihrer Technologiepartner berücksichtigen. Zu den eigenen Schutzmaßnahmen zählen Mitarbeiterschulungen, Mehr-Faktor-Authentifizierung, geregelte Zugriffsrechte und klare Notfallabläufe. Technologieanbieter bleiben zugleich verpflichtet, betroffene Vertragspartner über relevante Sicherheitsvorfälle rechtzeitig zu informieren.

Informationspflichten sind keine freiwillige Leistung

Werden Hotels verspätet über einen Cyberangriff in Kenntnis gesetzt, können sie Risiken für Gäste möglicherweise nicht rechtzeitig bewerten und gesetzliche Meldefristen versäumen. Die Datenschutz-Grundverordnung (DSGVO) verpflichtet jedoch die Auftragsverarbeiter, den datenschutzrechtlich

Verantwortlichen unverzüglich über Verletzungen des Schutzes personenbezogener Daten zu informieren. Verantwortliche müssen ihrerseits meldepflichtige Vorfälle grundsätzlich innerhalb von 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde melden. Bei voraussichtlich hohem Risiko kann zudem eine Benachrichtigung der betroffenen Personen erforderlich sein. „Nach einem Sicherheitsvorfall schulden Unternehmen Gästen, Partnern und Behörden rasche und vollständige Information. Daran hängt, ob sie ihre Verantwortung überhaupt wahrnehmen können. Jeder Tag des Schweigens vergrößert den Schaden und schwächt die rechtliche Position aller Beteiligten“, so Peter Hense, Rechtsanwalt und Partner bei Spirit Legal sowie Mitinitiator der HSMA-Initiative zur Cybersicherheit in der Hotellerie.

Verträge prüfen und Konsequenzen ziehen

Hotels sollten ihre IT-Verträge auf Informationsfristen, Zuständigkeiten und Unterstützungspflichten bei Sicherheitsvorfällen prüfen. Werden vertragliche Pflichten verletzt, können je nach Einzelfall rechtliche Ansprüche oder eine außerordentliche Kündigung infrage kommen. Die HSMA empfiehlt daher, transparente Sicherheitsprozesse bereits bei der Auswahl von Technologiepartnern zum Kriterium zu machen. Entscheidend ist auch, wie Anbieter Vorfälle erkennen, intern eskalieren und ihre Kunden informieren.

Eine offene Sicherheitskultur schützt die gesamte Branche

Ein offener Umgang mit Sicherheitsvorfällen hilft somit, Risiken einzuordnen, Schutzmaßnahmen einzuleiten und vergleichbare Schwachstellen in anderen Betrieben frühzeitig zu erkennen. Im Mittelpunkt stehen der Schutz sensibler Gästedaten und das Vertrauen in die Hospitality-Branche – nicht öffentliche Schuldzuweisungen: „Hotels können digitale Risiken nicht allein bewältigen. Wir brauchen eine Sicherheitskultur, in der Hotels und Technologieanbieter offen miteinander kommunizieren, Verantwortung übernehmen und aus Vorfällen lernen. Transparenz muss deshalb ein selbstverständlicher Bestandteil der Zusammenarbeit sein. Aber eben nicht erst dann, wenn der Schaden bereits eingetreten ist“, erklärt Anna Heuer, Wirtschaftsjuristin und Verbandsgeschäftsführerin der HSMA Deutschland e.V.

HSMA als Ansprechpartner für die Branche

Die HSMA Deutschland e.V. fördert den Austausch zwischen Hoteliers, Technologieanbietern und Branchenexperten, um Wissen über Cyberrisiken zu vermitteln und die digitale Widerstandsfähigkeit der Hotellerie zu stärken. Die Botschaft des Verbands: Eine vernetzte Hotel-Tech-Landschaft braucht gemeinsame Verantwortung, klare Prozesse sowie konsequente Transparenz. Hoteliers können sich bei Fragen zum Thema jederzeit an den Verband wenden.

Foto: XXX. Fotoquelle: Thomas Loris. Online-Nutzung unbegrenzt. Frei zum Druck. Abdruck der Presseinformation honorarfrei.

4'151 Anschläge mit Leerzeichen (Ohne Unternehmens-Footer)

Über HSMA Deutschland e.V.:

Die Hospitality Sales & Marketing Association Deutschland e.V. (HSMA) ist der führende Fachverband für die Hospitality-Branche und vereint über 1.600 Fach- und Führungskräfte aus Hotellerie und Tourismus. Als branchenübergreifendes Netzwerk und Wissensplattform fördert die HSMA aktiv den kollegialen Dialog sowie die beruflichen Interessen ihrer Mitglieder in allen relevanten Disziplinen.

Die Fachbereiche der HSMA Deutschland e.V. umfassen Online Marketing & E-Commerce, Marketing & Communication, Distribution, Revenue Management, MICE, Sales, Technology, HR & People and Culture sowie Sustainability. Ziel des Verbands ist es, Fachwissen durch strukturierten Informations- und Erfahrungsaustausch nachhaltig zu stärken. Neben Fachkongressen, Roadshows, Barcamps und weiteren Weiterbildungsformaten schätzen die Mitglieder insbesondere das hochkarätige Netzwerk und den persönlichen Austausch, der für eine erfolgreiche Zusammenarbeit innerhalb der Hospitality-Branche essenziell ist. www.hsma.de

Kontakt Unternehmen:

HSMA Deutschland e.V.
c/o Design Offices
Anna Heuer
Koppenstrasse 93
10234 Berlin
Telefon +49 176 47812663
info@hsma.de
www.hsma.de

Kontakt Medien:

Wolf.Communications
by Wolf-Thomas Karl
Schulhausstrasse 3
8306 Brüttisellen/ZH
Telefon: +41 (0)76 4985993
mail@wolftomaskarl.com
www.wolftomaskarl.com