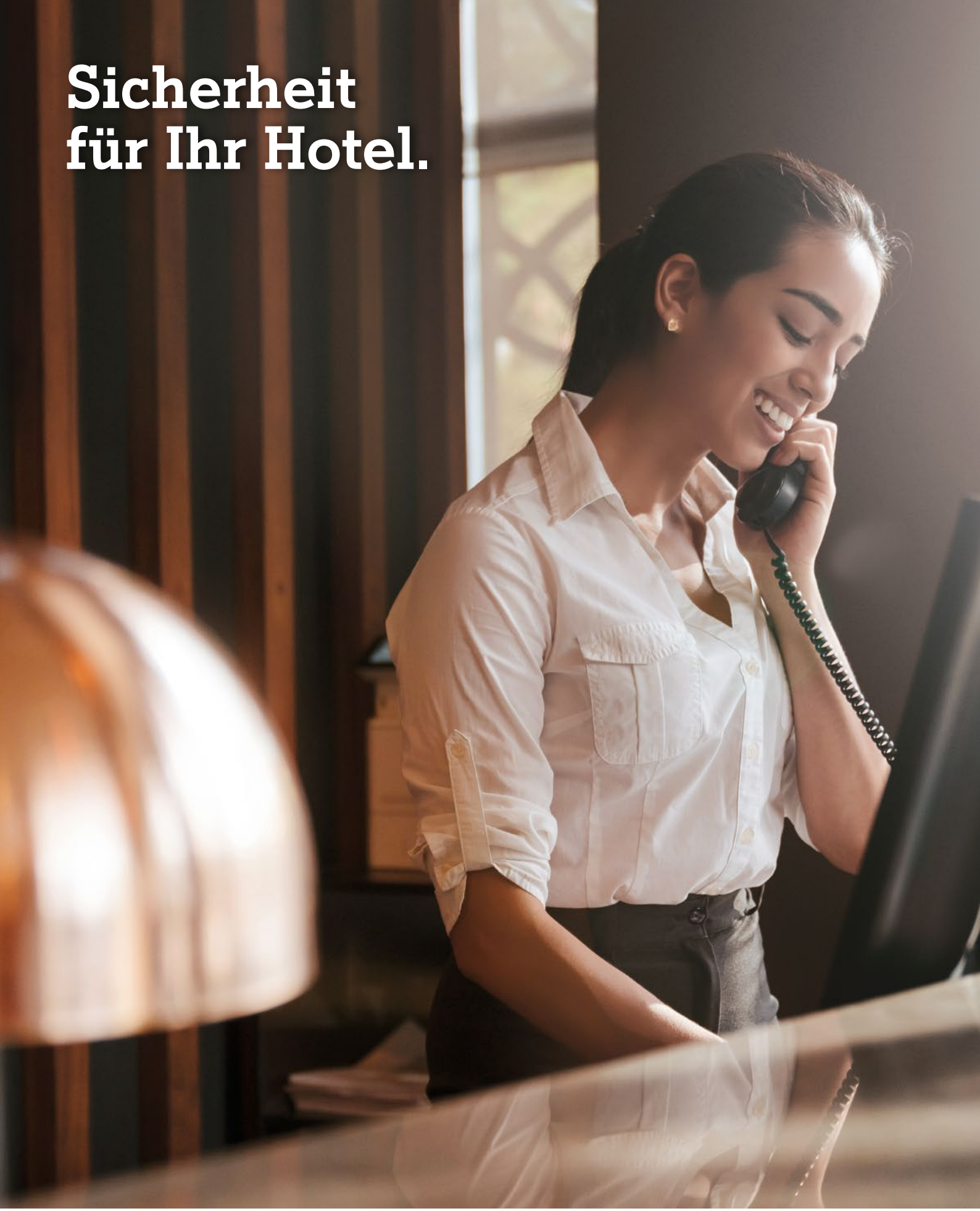
Sicherheit für Ihr Hotel.



ÖSTERREICHISCHE HOTELIERVEREINIGUNG

Deloitte.

A1

Inhalt

Einleitung

Die Digitalisierung ist voll in der Hotellerie angekommen. Viele Vorgänge im Hotel konnten durch sie vereinfacht und optimiert werden. Gleichzeitig bringt die Digitalisierung aber auch Risiken mit sich. Neben bis dato klassischen Zielen wie Handkassen oder Tresors rückt vermehrt die digitale Infrastruktur ins Zentrum krimineller Aktivitäten. Cybercrime-Fälle haben massiv zugenommen, gerade bei KMUs. In den letzten zehn Jahren haben sich die Anzeigen von Cybercrime versechsfacht. Das macht das Thema Sicherheit auch in der Hotellerie zur Chefsache.

Beim Schutz Ihrer Daten und IT-Infrastruktur können Sie auf die Zusammenarbeit dreier Experten bauen: Die Österreichische Hoteliervereinigung (ÖHV) kennt Ihre Branche wie kein anderer. Durch zahlreiche Cyber-Security-Checks kann Deloitte umfassendes Know-how im Bereich Cyber-Sicherheit für Hotels beisteuern. A1 bietet weitreichende Expertise auf dem Gebiet der IT- und Gebäudesicherheit, die jederzeit maßgeschneidert an die jeweiligen Bedürfnisse und Rahmenbedingungen Ihres Hotels angepasst werden kann.

Eine im Herbst 2018 von der ÖHV und A1 durchgeführte Umfrage zeigt, dass die Hälfte aller Hoteliers bereits Probleme im Bereich IT-Sicherheit hatte, rund 75 % der Befragten wünschten sich, zu diesem Thema mehr Informationen zu haben. Auch das diesjährige Studien-Update der 2016 erstellten Digitalisierungsstudie „Hotellerie 4.0“ von der ÖHV, dem deutschen Hotelverband IHA und Roland Berger bestätigte die anwachsende Wichtigkeit des Themas. Waren es im Jahr 2016 noch 39 % der Hotels die Datensicherheit als potenzielle Gefahr der Digitalisierung sahen, stieg dieser Wert 2019 auf 61 % an.

Basierend auf diesen Ergebnissen und Erfahrungsberichten des ÖHV-Partners A1 und dem Beratungsunternehmen Deloitte wurde in Zusammenarbeit dieser Leitfaden zum Thema Sicherheit im Hotel erstellt. Anhand von Praxisbeispielen aus dem Alltag wird dargestellt, wie schnell Ihr Betrieb zum Angriffsziel werden kann, welche Rolle der Faktor Mensch dabei spielt und was Sie vorab tun können. Nutzen Sie diesen Leitfaden, um mögliche Sicherheitsmängel und passende Lösungen mit Ihrem IT-Betreuer und den Sicherheitsexperten von A1 und Deloitte zu besprechen.

Vor der Ankunft

Szenario 1:

Ein Gast möchte seinen Aufenthalt über die Website Ihres Hotels buchen.

Welche Gefahr besteht?
Die Verbindung zu Ihrer Website ist möglicherweise nicht gesichert. In diesem Fall geschieht der Datenaustausch zwischen Ihrem Hotel und potentiellen Gästen unverschlüsselt. Kriminelle haben so ungehindert Zugang zu allen übermittelten Daten wie Zahlungsdetails. Möglicherweise erscheint deshalb im Internetbrowser des Besuchers Ihrer Website eine Sicherheitswarnung, die ihn verunsichert und von einer Buchung abhält.

Was können Sie tun?
Stellen Sie Ihre Website auf HTTPS bzw. TSL/SSL um, damit übertragene Daten verschlüsselt und die Authentizität der Anfragen sichergestellt wird. Hierfür benötigen Sie ein gültiges SSL- bzw. TSL-Zertifikat.
A1 bietet Ihnen die Möglichkeit, einer SEO-optimierten, für Mobile Devices angepassten Website mit gültigen SSL Zertifikat – selbst oder durch Profis erstellt. Mehr unter A1.net/marketplace-a1-webpresence-service.

Szenario 2:

Ein Gast gibt am Telefon Informationen durch, die handschriftlich notiert werden.

Welche Gefahr besteht?
In Ihrem Unternehmen gibt es unter Umständen keine Clean-Desk-Policy. Dabei handelt es sich um Maßnahmen, die alle Arbeitsplätze und Drucker frei von sensiblen Informationen (Passwörter, Zugangsdaten, persönliche Daten, finanzielle Informationen, etc.) halten sollen. Solche frei zugänglichen Informationen können missbräuchlich verwendet oder gestohlen werden.

Was können Sie tun?
Formulieren Sie eine Clean-Desk-Policy und klar definierte Regeln zur Verwendung der Arbeitsplätze. Zusätzlich sollten sich Computer automatisch nach einigen Minuten selbst sperren, damit nur berechtigte Mitarbeiter den Computer bedienen kann.

Bei der Ankunft

Szenario 3:

Das hoteleigene IT-System stürzt während des Geschäftstages plötzlich ab.

Welche Gefahr besteht?
In Ihrem Unternehmen gibt es möglicherweise keine ausformulierte, konkrete und getestete Vorgehensweise beim Ausfall von IT-Systemen, Sicherheitsvorfällen oder Datenverlust. Das gefährdet nicht nur den reibungslosen Geschäftsablauf, sondern auch die Daten Ihrer Gäste. Bei besonders kritischen Abläufen können sensible Daten verändert, zerstört oder öffentlich zugänglich gemacht werden.

Was können Sie tun?
Erstellen Sie für Notfälle einen Plan, der zumindest Kontaktdaten für die zuständigen IT-Experten und eine Checkliste für die ersten Schritte enthält. Sämtliche Mitarbeiter müssen wissen, wo dieser Plan zu finden ist und ihn zumindest strukturell kennen.

Damit es gar nicht so weit kommt, lagern Sie sensible Dienste einfach aus. A1 bietet Ihnen DSGVO-konforme Lösungen, mit denen Sie Ihre IT-Infrastruktur auf ausfallsicheren Cloud-Servern in österreichischen Rechenzentren betreiben können. Mehr unter A1.net/marketplace-paygo und A1.net/marketplace-vps.

Szenario 4:

Durch einen Systemabsturz kommt es zum Verlust wichtiger Daten.

Welche Gefahr besteht?
Ihre Server und Systeme werden unter Umständen nicht ausreichend gesichert, zudem gibt es kein Konzept für die Datenwiederherstellung. Das erhöht das Risiko unwiderbringlich verlorener Daten.

Was können Sie tun?
Legen Sie fest, wann und wie oft von den Systemen Backups erstellt werden sollen. Dies betrifft vor allem die Dauer bis zur Wiederverfügbarkeit von Daten, Häufigkeit und Umfang von Backups (Kosten-Nutzen-Rechnung). Zusätzlichen Schutz bei Feuer, Diebstahl und Trojaner, die Ihre Backups verschlüsseln, erreichen Sie mit Offsite-Backups. A1 bietet Cloud-Lösungen für Ihre Backups. Mehr unter A1.net/A1-cloud-storage.

Während des Aufenthalts

Szenario 5:

Ein Mitarbeiter steckt einen an der Rezeption abgegebenen USB-Stick an den Computer an oder öffnet einen schadhaften Anhang einer E-Mail.

Welche Gefahr besteht?
Ihre Mitarbeiter sind möglicherweise nicht ausreichend im Bereich der Informationssicherheit geschult. Das erhöht das Risiko von Malware, Trojanern oder Phishing durch achtlos geöffnete Anhänge in E-Mails oder das Öffnen von Dateien eines nicht vertrauenswürdigen USB-Sticks oder DVD. Ohne Bewusstsein für grundlegende Angriffsmuster können Sicherheitsvorfälle nicht rechtzeitig erkannt werden, oder es erfolgt eine falsche oder zu späte Reaktion. Gefahr droht auch durch Social Engineering, bei dem das Opfer durch den Inhalt einer E-Mail dazu bewegt wird, einen Anhang oder eine Website zu öffnen, wodurch entweder ein gefährlicher Code ausgeführt wird oder das Opfer auf einer gefälschten Seite vertrauliche Daten preisgibt. Besonders Phishing-Angriffe werden immer ausgefeilter, da die gefälschten E-Mails genau auf das Opfer zugeschnitten werden („Spear-Phishing").

Was können Sie tun?
Vermitteln Sie Ihren Mitarbeitern, dass sie ein wesentlicher Faktor für die erfolgreiche Umsetzung von Informationssicherheits-Maßnahmen darstellen. Technische Sicherheitsmaßnahmen alleine können Angriffe nämlich nie vollständig abwehren. Daher sollte jeder im Unternehmen zum sicheren Umgang mit bestimmten Anwendungen und über aktuelle Beispiele für Angriffs- und Betrugsmuster informiert werden.
Wichtig sind zudem auch die Sensibilisierung zu den Gefahren und Methoden von Phishing, Schulungen zu sicheren Passwörtern und zum Umgang mit persönlichen Daten, um eine Verletzung der DSGVO zu verhindern. A1 bietet Ihrem IT-Verantwortlichen oder IT-Partner mit der Cyber Range umfassende Trainingsmöglichkeiten zu verschiedensten Angriffsszenarien – so sind Sie optimal abgesichert, egal wie Sie betreut werden. Mehr unter A1.net/A1-cyber-range.

Während des Aufenthalts

Szenario 6:

Ein Gast wählt sich mit einem infizierten Notebook, Tablet oder Mobiltelefon ins ungeschützte Hotel-WLAN ein.

Welche Gefahr besteht?
Ihr Hotel ist unter Umständen durch eine nicht vorhandene oder ungenügend konfigurierte Firewall nicht ausreichend vor Malware, Viren und Trojanern geschützt. Das interne Netzwerk ist der Transportweg für alle Daten zwischen den einzelnen Devices, auch vom und zum Internet.
Die meisten Hotels stellen ihren Gästen gratis WLAN zur Verfügung. Wichtig ist, dass das interne und das Gäste-WLAN voneinander getrennt sind. Dadurch wird gewährleistet, dass niemand unberechtigt Zugriff auf Laufwerke oder Systeme erlangt, auf denen sensible Daten lagern oder der Anschluss eines infizierten Geräts das gesamte hotelinterne System lahmlegt.

Was können Sie tun?
Setzen Sie eine Firewall der „Next Generation", eine intelligente Firewall, ein. Diese schützt sowohl vor Angriffen von außen als auch davor, dass Ihre Mitarbeiter auf Websites mit gefährlichem Inhalt zugreifen können. Zudem teilt sie verschiedene Netzwerkbereiche in Einzelsegmente auf. Dateien, die nicht eindeutig gut- oder bösartig sind, kann die Firewall gefahrenlos in einer sogenannten Sandbox testen. A1 bietet an Ihre Anforderungen angepasste, von Profis konfigurierte und gemanagte Next-Generation-Firewalls an. Mehr unter A1.net/A1-firewall-vpn-service.

Legen Sie zudem eine „Schutzzwiebel" um Ihre Daten, indem Sie

- Ihre E-Mails vorfiltern, bevor Sie an die Rechner weitergeleitet werden. A1 bietet Cloud-Lösungen, bei denen Malware und Spam vorgefiltert und entfernt werden. Mehr unter A1.net/marketplace-ikarus-mailsecurity.
- Ihre E-Mails verlässlich vor Viren schützen. Antivirenschutz-Sicherheitslösungen für PCs und Notebooks unter A1.net/marketplace-ikarus-anti-virus-service.
- Ihr Netzwerk regelmäßig auf Sicherheitslücken überprüfen. Vollautomatisierte Lösungen finden Sie unter A1.net/marketplace-offensity.
- Ihre bestehenden Firewalls regelmäßiger Konfigurations-Reviews unterziehen und Policy-Formulierungen vornehmen.

Während des Aufenthalts

Szenario 7:

Ein Mitarbeiter verliert das Hotel-Mobiltelefon.

Welche Gefahr besteht?

Möglicherweise verfügen die in Ihrem Hotel verwendeten Mobilgeräte und Notebooks über unverschlüsselte Datenträger. Nutzen Mitarbeiter ihr Smartphone auch für private Zwecke, können Daten versehentlich mit Dritten geteilt werden – etwa über soziale Medien. Durch die DSGVO ist es notwendig geworden, als Hotellier einen Überblick über die Speicherung und Absicherungen von Gästedaten zu haben.
Sollten Gästedaten in unbefugte Hände gelangen, ist eine Meldung bei der Datenschutzbehörde notwendig, andernfalls machen Sie sich strafbar.

Was können Sie tun?

Verwenden Sie eingebaute Verschlüsselungsmethoden und Passwörter beim System- oder Gerätestart. Auch für USB-Sticks sollte die Verschlüsselung aktiviert werden. Alle Sicherheitsmaßnahmen können nur dann wirken, wenn die Daten auf den Geräten aller Mitarbeiter geschützt werden. Der Verlust verschlüsselter Geräte muss nicht der Datenschutzbehörde gemeldet werden.

Schützen Sie PCs oder Notebooks vor Schadsoftware, die auch persönliche Daten auslesen kann. Mehr unter A1.net/marketplace-ikarus-anti-virus-service.

Mit einer Mobile Device Management-Lösung (MDM) von A1 behalten Sie die Übersicht über alle Geräte im Unternehmen. Hier kann auch die Nutzung gesteuert und das Installieren von fragwürdigen Apps unterbunden werden, damit die Geräte und somit Ihre Daten geschützt bleiben. Mehr unter A1.net/marketplace-ikarus-mobile-management.

Während des Aufenthalts

Szenario 8:

Zur Sicherheit werden Teile des Hotelbereichs durch Videokameras überwacht.

Welche Gefahr besteht?
Unter Umständen ist Ihre Videoüberwachungsanlage unsicher oder falsch konfiguriert. Während Videoüberwachung generell das Sicherheitsgefühl erhöht und im Zweifelsfall die Dokumentation von Vorfällen erleichtert, birgt sie auch viele Risiken. Bei IP-basierten Netzwerkkameras können Unbefugte möglicherweise über das Internet auf sensible Informationen wie Live-Bilder oder Aufzeichnungen zugreifen. Ist die Kamera-Software veraltet, können Hacker über das Gerät in Ihr internes Netz eindringen.
Die Überwachung muss auch immer im Sinne der DSGVO erfolgen, mit Verstößen machen Sie sich strafbar. So dürfen laut DSGVO Videoaufzeichungen nur 72 Stunden lang gespeichert werden.

Was können Sie tun?
Stellen Sie sicher, dass die eingesetzten Geräte dem neusten Stand der Technik entsprechen und sorgen Sie für Anbindung an eine Notrufzentrale, um im Ernstfall schnell reagieren zu können. A1 berät Sie gerne im Sinne eines durchgängigen Gesamtkonzepts. So machen auch zusätzlich Alarmsysteme oder Alarmierungsknöpfe Sinn. Mehr unter A1.net/A1-object-security-alarm-video-service.

ÖHV-Tipp: Bitte beachten Sie, dass eine Videoüberwachung nur zulässig ist, wenn die gesetzlichen Voraussetzungen vorliegen, nämlich wenn bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt könnte das Ziel oder der Ort eines gefährlichen Angriffs werden. Dies ist dann gegeben, wenn das überwachte Objekt bereits einmal Ziel oder Ort eines gefährlichen Angriffes war, eine Wiederholung wahrscheinlich ist und sich dieser gefährliche Angriff innerhalb der vergangenen 10 Jahre ereignet hat. Außerdem ist die spezielle Sorgfaltspflicht zum Schutz des überwachten Objektes zu beachten. Öffentlicher Raum darf zum Zweck des Objektschutzes nur soweit erfasst werden, wie es zur Erreichung dieses Zweckes unumgänglich notwendig ist (z.B. unmittelbar an das Hotel angrenzende Teile des Gehsteigs). Eine darüber hinausgehende Überwachung von öffentlichen Plätzen ist nicht erlaubt. Völlig unzulässig ist jedenfalls die Durchführung von Überwachungen an Orten, die dem höchst persönlichen Lebensbereich zuzurechnen sind (z.B. Hotelzimmer, Umkleide- oder WC-Kabinen). Verboten ist auch die gezielte Videoüberwachung zur Kontrolle von Mitarbeitern an der Arbeitsstätte.

Bei der Abreise

Szenario 9:

Um Gäste schnellstmöglich zu betreuen, haben die Rezeptions-PCs einfache bzw. keine Passwörter, oft werden Passwörter auch auf Post-its an den Bildschirmen angebracht.

Welche Gefahr besteht?
Möglicherweise können Unbefugte ganz einfach auf Ihr System und auf sensible Daten zugreifen.

Was können Sie tun?
Legen Sie fest, dass hotelinterne Passwörter zumindest 8 Zeichen lang sind und Groß-/Kleinschreibung sowie Sonderzeichen enthalten müssen. Ebenso sollten diese Passwörter nie an anderer Stelle wiederverwendet werden. Besteht der Verdacht, dass ein Passwort gehackt oder auf eine andere Art kompromittiert wurde, sollte es sofort geändert werden. Diese Regeln sollen für alle Mitarbeiter gelten.

Kundenbindungs-Maßnahmen

Szenario 10:

Sie möchten Gästen Ihren Hotel-Newsletter zuschicken.

Welche Gefahr besteht?

Unter Umständen verstößt der Versand des Newsletters gegen die EU-Datenschutzgrundverordnung (DSGVO). Diese vereinheitlicht europaweit die Verwendung personenbezogener Daten, Geldstrafen können empfindlich hoch sein.

Was können Sie tun?

Die Nutzung der E-Mail-Adresse für einen Newsletterservice bedarf grundsätzlich der schriftlichen Einverständniserklärung des Gastes und dem Hinweis auf sein Recht auf Widerruf. Der Empfänger muss jederzeit die Möglichkeit haben, den Newsletter wieder abzubestellen. Diese Möglichkeit ist auf jedem Newsletter zu integrieren. Die Bestellung und Abbestellung des Newsletters inkl. der Einwilligungserklärung ist zu dokumentieren. Weitere nützliche Informationen finden Sie im ÖHV-Leitfaden „Datenschutz in der Hotellerie“ unter www.oehv.at/Publikationen/OHV-Studien-Leitfaden/DSGVO.

Die Umsetzung der DSGVO erfordert eine detaillierte Planung, eine Analyse des Ist-Zustands Ihres Unternehmens und einen Maßnahmenplan zum Erreichen des Soll-Zustands. Das Beratungsunternehmen Deloitte bietet Ihnen hier umfassende Workshops, um Ihr Unternehmen für die DSGVO zu rüsten. Mehr unter www.deloitte.at/dsgvo.

Cyber-Security-Check

Viele Hotels sind beim Thema Cyber Security gefährdet und unzureichend vorbereitet. Häufig herrscht Aufholbedarf in den Bereichen IT-Sicherheit und Datenschutz. Deshalb bietet Deloitte den Ready-Set-Go Security Check an. Dieser wurde speziell auf die österreichische Hotellerie und Gastronomie abgestimmt und wird in der Regel innerhalb eines Tages von den Deloitte Experten durchgeführt. Dabei erhalten Sie Auskunft über den aktuellen Status der Cyber Security Ihres Hotels und einen individuellen Maßnahmenplan zur Optimierung. Für nähere Auskünfte wenden Sie sich bitte an readysetgo@deloitte.at.

Lexikon

Firewall
Sicherheitssystem, das die Daten von und in das Internet filtert und nach gewissen Regeln umlenkt, um interne Systeme vor Angriffen aus dem Internet zu schützen. Die Firewall ermöglicht auch die Aufteilung des internen Computernetzes in mehrere voneinander getrennte Sicherheitszonen.

Malware
Software, die sich unerkannt auf einem Device (Computer, Tablet, Smartphone) installiert und es Angreifern ermöglicht, das Device auszuspionieren und Daten zu löschen oder zu verschlüsseln (siehe auch Ransomware).

Phishing
Durch E-Mails, die vortäuschen von einem vertrauenswürdigen Absender zu stammen, wird der Empfänger auf eine gefälschte Seite (z.B. einer Bank) geleitet, auf der versucht wird, die Zugangsdaten des Opfers zu erschleichen.

Ransomware
Sich selbständig und heimlich installierende Software, die persönliche Daten des PC-Besitzers verschlüsselt und anschließend ein Lösegeld fordert, um die Daten wieder zu entschlüsseln. Diese Erpressung ist immer mit einem Countdown verbunden: Wird nicht rechtzeitig das Lösegeld bezahlt (eigentlich immer in Form von Cryptowährung), bleiben die Daten unwiederbringlich verschlüsselt. Der PC muss dann komplett neu aufgesetzt werden, da man niemals sicher sein kann, ob nicht noch versteckte Schadsoftware vorhanden ist.

Sandbox
Eine gesicherte, abgeschottete Umgebung, in der fragwürdige Dateien gefahrlos ausgeführt werden können, um ihr Verhalten zu analysieren. Meist wird die Datei dafür zum Anbieter der Firewall oder Antivirenlösung geschickt, da die lokalen Ressourcen zu schwach sind, um solche Testläufe auszuführen.

Über uns

A1 – Internet, Telefonie, TV und IT-Lösungen aus einer Hand.
A1 ist mit mehr als 5,3 Mio. Mobilfunkkunden und mehr als 2 Mio. Festnetzanschlüssen Österreichs führender Kommunikationsanbieter. Die Kunden profitieren von einem umfassenden Gesamtangebot aus einer Hand, bestehend aus Sprachtelefonie, Internetzugang, digitalem Kabelfernsehen, Daten- und IT-Lösungen, Wholesale-Services und mobilen Business- und Payment-Lösungen. Die Marken A1, bob, Red Bull MOBILE und Yesss! stehen für höchste Qualität und smarte Services. Als verantwortungsvolles Unternehmen integriert A1 gesellschaftlich relevante und Umweltbelange in das Kerngeschäft. Mehr unter www.a1.net.

Die Österreichische Hoteliervereinigung (ÖHV) ist die freie Interessenvertretung der Hotellerie in Österreich.
Ihr gehören über 1.480 führende Hotels aller Kategorien aus Ferien-, Konzern- und Stadthotellerie an. Der Verband vertritt die Interessen der Hotellerie auf nationaler und internationaler Ebene und unterstützt seine Mitglieder mit professionellen Service- und Dienstleistungen sowie Schulungsangeboten. Mehr unter www.oehv.at.

Deloitte hat sich als führendes Beratungsunternehmen neben den Kernbereichen auch in Österreich aktiv auf Risikoanalyse für Cybersicherheit und Datenschutz spezialisiert.
Deloitte ist 2018 vom renommierten Marktforschungsinstitut Gartner zum sechsten Mal in Folge als #1 bei Security Consulting Services ausgezeichnet worden. Mit umfassender Expertise konnten die Mitarbeiter von Deloitte Österreich bereits bei zahlreichen Betrieben in der heimischen Gastronomie und Hotellerie die IT-Sicherheit und den Datenschutz optimieren. Mehr unter www.deloitte.at.