Anna Cardillo und Manuel Atug

Bußgeldbescheid des ICO gegen Marriott: PCI DSS und trotzdem nicht sicher?

Mit Bescheid vom 30.10.2020 verhängte die britische Datenschutzbehörde ICO gegen Marriott International Inc. ein Bußgeld in Höhe von 18,4 Mio. britische Pfund wegen Verletzung der Pflichten aus Art. 5 Abs. 1 lit. f, 32 DSGVO. Marriott habe personenbezogene Daten nicht in einer Weise verarbeitet, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Trotz Brexit lohnt sich ein Blick in den 91-seitigen Bescheid der Nachbarn, denn die dort beschriebenen Versäumnisse sind auch in deutschen Unternehmen sowie Behörden häufig anzutreffen. Der Schwerpunkt des Beitrags liegt dabei auf den technischen und organisatorischen Aspekten.

Was war passiert?

Im Jahr 2014 wurden die IT-Systeme der Hotelkette Starwood durch unbekannte Angreifer kompromittiert. Die Angreifer verschafften sich Zugang zum Cardholder Data Enviroment (CDE) und Zugriff auf dort gespeicherte personenbezogene Daten der Hotelgäste, einschließlich überwiegend unverschlüsselter Passdaten und verschlüsselter Kreditkarteninformationen. Im Jahr 2016 erwarb Marriott die Hotelkette Starwood mit IT-Systemen inkl. der „eingenisteten Angreifer". Die Angreifer weilten unbemerkt über Jahre bis in den Herbst 2018 hinein in den IT-Systemen und hatten sich inzwischen Zugang zu personenbezogenen Daten von rund 339 Mio. Hotelgästen (weltweit) innerhalb des Starwood-Netzwerks verschafft. Dieser Zugang ermöglichte es den Angreifern, mehrfach personenbezogene Daten von Starwood-Gästen zu exportieren. Dazu erstellten die Angreifer zunächst Tabellen mit bestimmten Datenkategorien. Als die Angreifer eine Tabelle mit Kreditkarteninhaberdaten erstellten, wurde am 7. September 2018 ein Alarm ausgelöst und die Angreifer wurden entdeckt. Andere von den Angreifern zuvor erstellte Tabellen mit Gästedaten enthielten keine Zahlungsinformationen, dafür aber Reservierungsdaten sowie Passnummern und lösten keinen Alarm aus. Marriott hatte offensichtlich Sicherheitsmaßnahmen entsprechend dem Anforderungskatalog PCI DSS (Payment Card Industry Data Security Standard) umgesetzt, von diesen Maßnahmen wurden allerdings nicht alle Daten der Gäste abgedeckt.

Unzureichende Multi-Faktor-Authentifikation

Der ICO stellte fest, dass in tatsächlicher Hinsicht ganz offensichtlich nicht alle Benutzerkonten und Systeme mit Zugriffsmöglichkeit auf das CDE mittels Multi-Faktor-Authentifizierung (MFA) gesichert waren. Dies führe indes nicht zu einem Verstoß Marriotts gegen Art. 5 Abs. 1 lit. f, 32 DSGVO. Marriott habe sich von Starwood vertraglich zusichern lassen, dass der Zugriff auf das CDE nur mittels MFA möglich sei. Des Weiteren habe Marriott auf zwei Reports of Compliance von unabhängigen PCI DSS-Auditoren am 29.04.2016 (vor Übernahme) und am 23.05.2017 (nach Übernahme) vertrauen dürfen. Die Auditoren bescheinigten, dass jeder Zugriff auf das CDE nur mittels MFA möglich sei.

Unzureichende Überwachung von Konten

Vorwerfbar sei Marriott jedoch, dass keine geeigneten Maßnahmen ergriffen worden seien, um unbefugte Aktivitäten von (legitimierten) Benutzern zu erkennen und zu verhindern. Marriott habe versäumt, eine angemessene laufende Überwachung der Benutzeraktivitäten, insbesondere der Aktivitäten privilegierter Konten, einzurichten.

Was sind privilegierte Konten?

Privilegierte Konten haben besondere oder erweiterte Rechte, so dass mit ihnen wesentliche Systemeinstellungen und -konfigurationen geändert werden können. Beispielsweise können damit weitere Dienste gestartet oder angepasst und umkonfiguriert werden, Software nachinstalliert oder auch Nutzer hinzugefügt oder bestehenden Nutzerrechte erweitert und angepasst werden. Unter Linux allgemein bekannt ist z. B. das privilegierte Konto root und unter Windows das Konto Administrator.

Wie überwacht man diese nach best practice?

Idealer Weise ist sichergestellt, dass alle Administratoren mit ihrem Nutzerkonto arbeiten und nur die administrativ relevanten Befehle und Tätigkeiten mit den privilegierten Rechten als Administrator ausführen. Dies kann z. B. unter Linux mit sudo und unter Windows mittels run as (oder Ausführen als) sichergestellt werden. Ein „shared admin account" entspricht darüber hinaus auch nicht mehr dem Stand der Technik.

Es muss eine eindeutige Zuordnung erfolgen können, unter welchem Nutzerkonto welche Befehle ausgeführt wurden. So kann wesentlich besser nachvollzogen werden, an welcher Stelle und vor allem was genau passiert ist, wenn es einen Vorfall gab. Unter den verschiedenen Betriebssystemen gibt es unterschiedliche Methoden, wie ein „Audit Trail" erzeugt wird, mit dem nachvollzogen werden kann, welche Befehle der jeweilige privilegierte Nutzer zu welchem Zeitpunkt ausgeführt hat. Dabei sind aber auch die

Datenbanken zu berücksichtigen und dort ist ebenfalls ein Audit Trail zu aktivieren. Ebenso in den Middleware Systemen und am Frontend, also in der Anwendung selbst.

Hierzu gibt es gängige Anhaltspunkte und Merkmale, die dabei aufgezeichnet werden sollten, beispielweise:
- Alle Aktionen, die als Nutzer mit erweiterten Rechten vorgenommen wurden;
- Alle ungültigen Zugriffsversuche;
- Änderungen an den Identifizierungs- und Authentifizierungsmechanismen;
- Rechteanpassungen bei Nutzerkonten;
- Veränderungen an Prüfprotokollen und Logdateien und Zugriffsversuche auf die Audit Trails selbst.

Die Audit Trail Logeinträge sollten dabei die gängigen Parameter für die Nachvollziehbarkeit beinhalten wie Benutzeridentifizierung, Ereignistyp, Datum und Uhrzeit, Angabe von Erfolgen oder Fehlschlägen, Ereignisursprung und Identität oder Name der betroffenen Komponente (Daten, Systemkomponenten oder Ressourcen). Diese Audit Trails werden dann vor unbefugten Zugriffen oder Veränderungen geschützt und idealer Weise auf einem zentralen Protokollserver oder einem SIEM (Security Incident Event Manager) abgelegt.

Eine Auswertung dieser Audit Trails und Protokolldaten kann dann – durchaus auch automatisiert – mit geeigneter Softwareunterstützung vorgenommen werden, indem man sog. „Use Cases" definiert und diese dann täglich nach Anomalien und Auffälligkeiten auswertet und immer wieder auf die gelebten Businessprozesse des Unternehmens justiert. Auch hier handelt es sich wie so oft um einen fortlaufenden Prozess und keine einmalige Konfiguration.

Die hier beschriebenen Maßnahmen werden im PCI DSS Standard für den administrativen und den Fernzugriff auf die CDE bereits seit vielen Jahren verbindlich vorgeschrieben.

Unzureichende Überwachung von Datenbanken

Neben der unzureichenden Überwachung der Benutzerkonten und der mit diesen verbundenen Benutzeraktivitäten unterließ es Marriott laut ICO auch, die Datenbanken innerhalb des CDE angemessen zu überwachen. Die Aufsichtsbehörde wirft dem Unternehmen vor: (a) Unzulänglichkeiten bei der Einrichtung von Sicherheitswarnungen für Datenbanken innerhalb des CDE, (b) das Versäumnis, die Protokolle zu aggregieren und (c) das Versäumnis, die im System des CDE stattfindenden Aktivitäten zu protokollieren, wie z. B. die Erstellung von Dateien und den Export ganzer Datenbanktabellen.

Marriott hatte hierbei zwar Produkte wie IBM Guardium eingesetzt, um die Aktivitäten in der Datenbank innerhalb des CDE mit folgenden Funktionen zu überwachen: Erstens protokollierte es alltägliche Aktivitäten wie das Erstellen Lesen, Aktualisieren oder Löschen von Daten innerhalb einer Datenbank. Zweitens gab es unter bestimmten Umständen Warnmeldungen aus. Ungewöhnliche, eben nicht alltägliche, Aktivitäten legitimer Benutzerkonten, wie z. B. Durchführung eines kompletten „Dump" der Datenbank (vollständige Kopie oder umfangreicher Auszug der Inhalte) wurden indes nicht überwacht oder protokolliert.

Im Geschäftsbetrieb sollte solch eine Aktivität eher selten vorkommen und damit auch auffallen. Warnmeldungen waren zudem nur für Auffälligkeiten bei Tabellen, die Zahlungskarteninformationen beinhalteten, aktiviert. Aber ohne Protokollierung – mittels geeigneter Use Cases – können diese wesentlichen Auffälligkeiten wie ein Datenbank-Dump eben nur schwerlich bemerkt werden. Marriott verfügte über die Möglichkeiten, denn die geeignete Anwendung war vorhanden und die entsprechende Konfigurationsanpassung war recht einfach realisierbar.

Marriott verteidigte sich in dem Zusammenhang damit, dass IBM Proventia und McAfee IntruShield, zwei Systeme, die Protokolle erzeugen und aggregieren, eingesetzt worden seien. Dieser Einwand überzeugte den ICO zu Recht nicht. Es gibt verschiedene Ziele, die man mit unterschiedlichen Anwendungen, die Protokolle erzeugen, erreichen kann und will. Proventia und IntruShield sind netzwerkbasierte Intrusion Detection Systeme, welche Angreifer im Netzwerk erkennen sollen. Sie sind daher von ihrer Grundfunktion her nicht dafür vorgesehen, die Protokollierung in der Datenbank vornehmen zu können oder diese auszuwerten und dafür Alarm zu schlagen.

Mangelnde Serverhärtung

Der ICO wirft Marriott zudem das Fehlen einer Serverhärtung als Präventivmaßnahme vor. Diese hätte Angreifer daran hindern können, Zugang zu Administratorkonten zu erhalten. Darüber hinaus hätten etwaige Angreifer entdeckt werden können, bevor sie ein Netzwerk durchqueren. Insbesondere die Implementierung von „Whitelisting" sei eine Möglichkeit, mit der Marriott eine Serverhärtung hätte durchführen können. Unter Serverhärtung versteht man unter anderem:
- die Deinstallation von unnötigen Diensten oder Softwareteilen, Treibern, Features und Subsystemen;
- das Löschen aller unnötigen Standardkonten und die Änderung sämtlicher Standardeinstellungen auf sichere Parameter;
- Aktivierung nur von den Diensten, Protokollen, Daemons etc., welche unbedingt erforderliche sind;
- Implementieren von zusätzlichen Sicherheitsfunktionen für die benötigten und ggf. unsicheren Dienste, Proto-

kolle, Daemons etc. (wie z. B. einen SSL Tunnel für die Nutzung von Telnet);
- Konfiguration der Sicherheitsparameter, um Missbrauch zu vermeiden.

Es werden also zur Serverhärtung Konfigurationsstandards für alle Systemkomponenten entwickelt. Diese orientieren sich an den Herstellerempfehlungen oder auch an anerkannten Standards zur Härtung von Systemen wie z. B. den CIS Benchmarks, der ISO Normenreihe, dem SANS Institut oder dem NIST, aber auch an den Bausteinen des BSI IT-Grundschutz.

Whitelisting wiederum ist eine Schutzmethodik, die alles verbietet, was nicht explizit erlaubt wurde. So kann z. B. der Zugriff auf die administrative Umgebung nur auf explizit zugelassene IP-Adressen von Systemen gewährt werden. Damit wird ein Zugriff von allen anderen Systemen standardmäßig unterbunden. Ein Angreifer muss also nicht nur die Zugangsdaten des Administrators abgreifen, sondern auch von einem per Whitelisting legitimierten System aus den Anmeldevorgang vornehmen, was die Ausnutzung dadurch deutlich erschwert.

Mangelnde Verschlüsselung

Zahlungskartendaten (wohl auch nur die sog. primären Kontonummern = PAN) und teilweise auch Passnummern wurden von Marriott verschlüsselt. Oracle-Datenbanken – die Starwood-Reservierungsdatenbank enthielt Tabellen, die in einer Oracle-Datenbank gespeichert waren – boten die Funktion, Tabelleneinträge ebenfalls zu verschlüsseln. Diese Möglichkeit nutzte Marriott jedoch nicht. So blieben vor allem die meisten Passnummern der Hotelgäste unverschlüsselt. Marriott verteidigte sich damit, dem in der Informationssicherheit vorgesehenen risikobasierten Ansatz gefolgt zu sein. Entsprechend dem PCI CSS Standard seien Zahlungskarteninformationen als besonders schutzbedürftig eingestuft worden.

Nicht verschlüsselt und dem Zugriff des Angreifers ausgesetzt waren: Kundennummer, Name, Geschlecht, Geburtsdatum des Gastes, VIP-Status, Mitgliedschaft im Bonusprogramm, Anschrift, Ländercode des Reisepasses, Telefonnummer, Faxnummer, E-Mail-Adresse und Ablaufdatum der Kreditkarte, Passnummern von 5,25 Mio. Gästen, Reservierungsbestätigungen, Ankunftszeit, Abreisedatum, Flugnummer und Airlinecode, Zimmertyp sowie die Gesamtzahl der Gäste im Zimmer.

Der risikobasierte Ansatz konnte Marriott nicht zum Vorteil gereichen. Zum einen blieb Marriott die Vorlage einer dokumentierten Risikoanalyse schuldig. Zum anderen mag es zwar zutreffend sein, dass im Rahmen des PCI DSS Standards Zahlungskarteninformationen als besonders schutzbedürftig zu betrachten sind. Dies befreit die Verantwortlichen jedoch nicht davor, auch die übrigen personenbezogenen Daten zu betrachten und angemessen zu schützen. Besonders Passnummern dürften schutzbedürftig sein. Die Einlassung, man habe einen risikobasierten Ansatz gewählt, war darüber hinaus wenig glaubhaft, da es ja durchaus Passnummern gab, die verschlüsselt waren. Es blieb unklar, weshalb nur ein Teil, ein anderer wiederum nicht verschlüsselt wurde.

Im Übrigen erläutert PCI DSS in der Einleitung zur Anwendbarkeit: „Wenn der Name des Inhabers, der Servicecode und/oder das Ablaufdatum zusammen mit der PAN gespeichert, verarbeitet oder weitergegeben werden oder anderweitig innerhalb der Karteninhaberdaten-Umgebung (CDE) vorhanden sind, müssen diese Daten gemäß den PCI-DSS-Anforderungen geschützt werden."

Schon aus dem Standard ergibt sich also, dass die vorstehend genannten Daten ebenfalls hätten verschlüsselt bzw. der Zugriff darauf hätte überwacht werden müssen.

Fazit und Empfehlungen für die Praxis

Das Ziel Marriotts lag ganz offensichtlich darin, den Anforderungen der Kartenorganisationen zu genügen, die darauf gerichtet sind, den Schutz der Karteninhaberdaten während der Verarbeitung sicherzustellen. Den Datenschutz hatte Marriott weniger vor Augen, hatten die getroffenen Sicherheitsmaßnahmen doch nahezu ausschließlich die Zahlungskarteninformationen im Fokus.

Schutz von Zahlungskarteninformationen reicht allein nicht aus

Der PCI DSS bietet eine Hülle und Fülle an sehr konkreten Schutzmaßnahmen zur Absicherung von Karteninhaberdaten der internationalen Zahlungssysteme. Diese auf weitere relevante und schützenswerte Daten zu erweitern, ist an vielen Stellen kein erheblicher Aufwand. Insbesondere wenn – wie im Fall Marriott – die Softwarelizenzen vorhanden sind und umfangreiche Prozesse bereits eingeführt wurden. Die Umsetzung der Anforderungen des PCI DSS-Standards allein reicht ohne einen ganzheitlichen Ansatz nicht aus, um den Anforderungen aus Art. 32 DSGVO zu genügen.

Es gibt viele verschiedene Anforderungen an ein Unternehmen. Die Einhaltung von datenschutzrechtlichen Bestimmungen oder auch der sichere Umgang mit unternehmensrelevanten Daten gehören dazu. Mit einem integrierten Sicherheitsmanagementsystem, welches die Informationssicherheit wie auch den Datenschutz berücksichtigt, können alle Anforderungen optimal aufeinander abgestimmt und harmonisiert werden. Weitere Anforderungskataloge wie der PCI DSS können dann ebenfalls dort hinein integriert werden. So betreibt man ein vollständiges Informationssicherheitsmanagementsystem (ISMS), wel-

ches alle Anforderungen in sich vereint. Dabei sollten die für die einzelnen Anforderungskataloge und gesetzlichen Vorgaben Zuständigen nicht alleine, sondern Hand in Hand (integriert) agieren.

Qualifikation der Mitarbeiter

Jede Organisation muss sich zudem die Frage stellen, ob die Personalauswahl die benötigte Fachexpertise abdeckt und ob diese Expertise in Qualifikationen, aber auch in Fortbildungen, angemessen Berücksichtigung findet. Dies gilt gleichermaßen für die Administratoren, aber auch für Mitarbeiter der Dienstleister.

Nun kann in der Regel der Verantwortliche die Qualifikation seiner Beschäftigten und Dienstleister im Bereich der IT – Marriott hatte Accenture als IT-Dienstleister beauftragt – nicht einschätzen. Zertifikate helfen da bekanntlich wenig. Ob Sicherheitseinstellungen richtig vorgenommen wurden, vermag der Auftraggeber in der Regel ebenfalls nicht zu beurteilen. Schwachstellen-, Pen-Tests sowie Sicherheits- und Datenschutzaudits durch unabhängige Prüfer sollten daher regelmäßig durchgeführt werden. Auch ein Wechsel der Dienstleister oder zumindest der externen Prüfer für Pen-Tests, Security Scans und Sicherheitsaudits können helfen, neue und frische Einblicke von außen zu erhalten. Hilfreich ist auch, die Qualität und nicht nur den Preis bei der Auswahl der Dienstleister und Prüfer hervorzuheben.

Informationssicherheit und Datenschutz i.R.v. Due-Diligence

Der ICO ließ dahingestellt, ob es Marriott möglich war, vor der Übernahme in 2016 eine Due-Diligence-Prüfung durchzuführen oder nicht. Jedenfalls spätestens mit dem 25. Mai 2018 trafen Marriott die Pflichten aus der DSGVO, da die übernommenen IT-Systeme von Marriott weiter betrieben und personenbezogene Daten der Gäste in diesen Systemen verarbeitet wurden. In der Tat dürfte aus der DSGVO eine Pflicht zur Durchführung einer Due-Diligence-Prüfung im Rahmen von M&A-Transaktionen mit Blick auf Informationssicherheit und Datenschutz nicht herleitbar sein. Allerdings ist zu beachten, dass durchaus eine Organhaftung greifen kann, wenn eine Due-Diligence Prüfung unterbleibt (vgl. OLG Oldenburg Urt. v. 22.06.2006 – 1 U 34/03).

Darüber hinaus sollte jedes vernünftig aufgesetzte Informationssicherheits- und Datenschutzmanagement geplante Veränderungen im Kontext der Organisation (z. B. Übernahme fremder Systeme) berücksichtigen. Dies ist aus PCI DSS-Sicht sogar über den Anforderungskatalog vorgeschrieben und damit verbindlich. Der Managementprozess muss durch solche bevorstehenden Veränderungen angestoßen und in der Folge eine im Zweifel auch vorlegbare und belastbare Risikoanalyse sowie Überprüfung der vorhandenen Schutzmaßnahmen durchgeführt werden. Wenn schon nicht vorher, so kann spätestens bei Übernahme der Systeme der Verantwortliche uneingeschränkt auf diese zugreifen und entsprechend handeln. Übernahmeabsichten sollten daher sehr frühzeitig mit den Zuständigen für Informationssicherheit und Datenschutz besprochen werden (Stichwort Kommunikation).

Versäumnisse von Marriott kein Einzelfall

Leider sind die hier aufgezeigten Versäumnisse kein Einzelfall. KMU, Konzerne und auch öffentliche Stellen sind gleichermaßen von den hier beschriebenen Defiziten betroffen. Sicherheit ist in Organisationen oft – wenn überhaupt – nur in Teilen gedacht und nicht in die Prozesse und Abläufe integriert. Muss sich also ein Mitarbeiter entscheiden, ob er sein tägliches operatives Geschäft erledigt oder die Sicherheitsdokumentation nachzieht, ist klar, wie er sich immer wieder entscheiden wird. So kommen kontinuierliche und stetige Defizite zustande, die dann eine Kette von Zuständen zulässt, die einem Angreifer den erfolgreichen Einbruch in die Umgebung ermöglicht und ihn dort unbemerkt schalten und walten lässt. Mangelnde Ressourcen, fehlendes Personal, unzureichende Qualifikation, fehlende Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung, der Blick über den eigenen Tellerrand und damit einhergehend die Kommunikation und Abstimmung mit den anderen Kollegen und Bereichen lassen sich nicht durch Anschaffung von Produkten wie einem SIEM oder Ähnliches kompensieren.

Sicherheit kostet nun mal. Und wenn es „nur“ die Ausbildung und das Gehalt der wertvollen Ressource Mensch als ITSecurity-Fachkräfte ist. Aber man kann nicht ohne weiteres erkennen, ob sich diese Investition auch „gelohnt“ hat. Es bleibt halt ein erfolgreicher Angriff aus, der sonst ggf. auch ausgeblieben wäre.

Autoren: **Anna Cardillo ist Rechtsanwältin bei Spirit Legal und spezialisiert auf Datenschutz – und Informationssicherheitsrecht. Sie berät vor allem bei der Implementierung eines integrierten Informationssicherheits – und Datenschutzmanagements.**

Manuel Atug verfügt über langjährige Erfahrung im Bereich technische IT-Sicherheit und Auditierung. Er berät und begleitet Unternehmen bei der Einführung von Informationssicherheitsmanagement-Systemen und ist Mitautor von BSI IT-Grundschutz-Bausteinen sowie Projektleiter der IT-Grundschutz-Modernisierung.