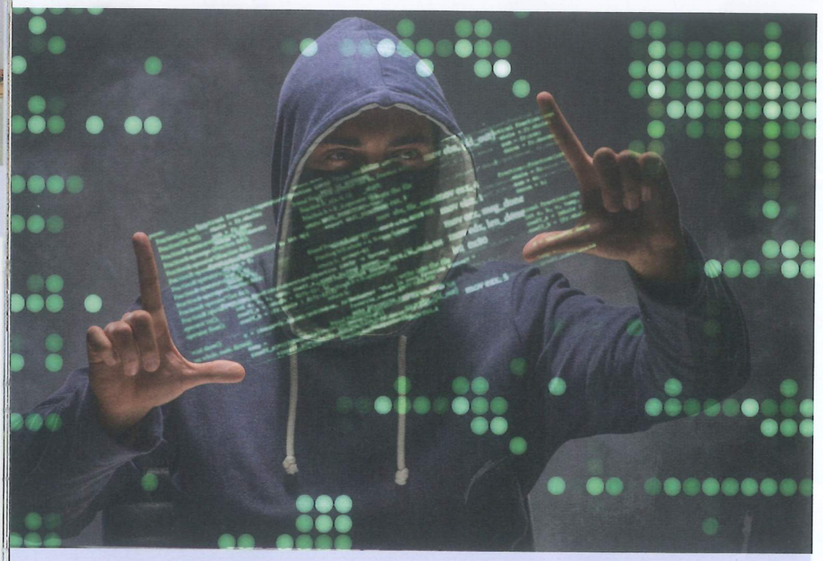
Sicher? Nicht.

Ein Team von Berliner Sicherheitsforschern hat das Buchungssystem Amadeus gehackt. Einfach so. Und so einfach, wie die Experten sagen. FaktuM wollte wissen, ob Buchungs- und persönliche Daten hier tatsächlich auf dem digitalen Serviertablett liegen.

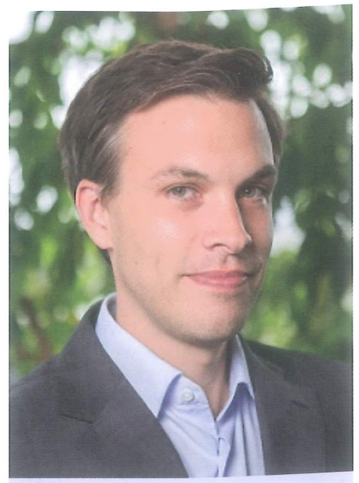


Cyber-Kriminalität: Viele Unternehmen haben die Gefahr noch nicht erkannt

Die Aktion hat Riesenwellen geschlagen: Das Berliner Unternehmen Security Research Labs (kurz: SR Labs) hat das Buchungssystem Amadeus – das über eine Datenbank mit Millionen von Kundendaten verfügt – gehackt. Nicht, um sich zu bereichern. Oder jemandem zu schaden. Sondern um aufzuzeigen, wie einfach das geht.
Genau genommen hat das Team um SR Labs-Chef Karsten Nohl die Website CheckMyTrip (über die Kunden ihre Buchungsdetails einsehen können) mit Brute-Force-Angriffen attackiert. Dabei werden mit roher Rechengewalt alle möglichen Kombinationen ausprobiert. In diesem Fall mit großem Erfolg: Einmal drin, konnten die Hacker Flüge einfach umbuchen. Oder persönliche Daten abrufen. Wie die private Telefonnummer eines deutschen Bundestagsabgeordneten. Ein Skandal. Gegenüber dem ARD sagte Nohl, das System von Amadeus sei aus den 80ern.
Das solchermaßen kompromittierte Unternehmen wehrte sich. Man prüfe zwar jetzt zusätzliche Sicherheitsmaßnahmen wie die Einführung eines Passworts (!). Aber: Die Seite sei gegen automatisierte Roboterangriffe geschützt und keineswegs so einfach zu hacken, wie behauptet wurde, teilte Amadeus mit. Der Angriff habe nur aufgrund eines temporären Wartungsfensters funktioniert. SR Labs hingegen sagt, man habe über eine Zeitspanne von mehreren Wochen hinweg immer wieder Attacken gestartet – ohne blockiert worden zu sein.
Wie einfach ist es für jemanden, der Ahnung hat, tatsächlich, sich Zugang zu verschaffen? FaktuM fragte bei **Daniel Miedler** (Business Unit Head Netzwerk, Infrastruktur und Security des heimischen Service- und Lösungsanbieters für Informationstechnologie Dimension Data Austria) nach.

Einfacher als Enigma

FaktuM: Das Team von Security Research Labs hat mit seinem Hack-Angriff auf das Amadeus-System eine Lawine losgetreten. Sie konnten Buchungen nicht nur einsehen, sondern auch manipulieren. Und zwar, wie die Profis sagten, mir sehr einfachen Mitteln. Wie genau ging das vonstatten?
Miedler: Amadeus ist ein großes Buchungsportal, das viele unterschiedliche Anbieter zusammenbringt. Flugreisen, Hotels uvm. sind hier angebunden. Mit CheckMyTrip bietet Amadeus die Möglichkeit, über seinen Nachnamen und einen sechsstelligen Buchungscode seine Buchung einzusehen, Dinge zu verändern oder auch persönliche Daten auszulesen. Das Problem an der Sache ist: Man hat dafür den Buchungscode als Passwort gewählt. Der ist aber nur sechs Stellen lang und besteht nur aus Großbuchstaben sowie aus Ziffern von 0 bis 9. Das heißt, man hat schon ein sehr schwaches Passwort an diese Stelle gesetzt.
FaktuM: Es ist also wirklich einfach, das System zu knacken?
Miedler: Ein guter geschichtlicher Vergleich ist vielleicht das System „Enigma" aus dem Zweiten Weltkrieg. Das konnte dechiffriert werden, weil man zum Beispiel den Anfangssatz einer verschlüsselten Nachricht wusste und daraus ein Muster ableiten konnte, um auf den Schlüssel zu kommen. Heutzutage hat man für die sogenannten Brute-Force-Attacken – also das brutale Ausprobieren aller möglichen Kombinationen – viel mehr Rechenleistung. Zusätzlich gibt es noch sehr viele gängige Nachnamen wie Müller oder Huber. Dass einer mit diesem Namen eine Buchung getätigt hat, ist ziemlich wahrscheinlich. Dazu kommt das limitierte Passwort aus nur sechs Stellen. Und: Ich weiß auch, dass das immer in einer Sequenz vergeben wird. Mit Datum und Uhrzeit kann ich relativ gut sagen, wie sich das zusammensetzen wird. Der Brute-Force-Angriff lässt sich damit auf ein paar wenige tausend Kombinationen einschränken.
FaktuM: Konkretes Vorwissen ist also nicht nötig?
Miedler: Wenn ich natürlich einen Namen weiß, der definitiv zu einem gewissen Zeitpunkt gebucht hat, ist es noch einfacher. Aber auch ohne dieses Wissen kann ich eine Brute-Force-Attacke starten. Das Problem neben dem schwachen Passwort war, dass es eben vor diesen Attacken keinen Schutz gab. Manche Portale blockieren zum Beispiel einen Usernamen nach drei Fehlversuchen temporär. Das verzögert einen Angriff. So etwas hat hier nicht existiert. Ebenso wenig wie eine sogenannte Bot Detection – die Kontrolle, ob der Zugriff durch einen Menschen erfolgt. In diesem Fall wurde ein Script eingesetzt, das über Cloudcomputer bei Amazon lief. Gerade hier wäre die Überprüfung, ob ein Mensch oder eine Maschine zugreift, intelligent gewesen. Dafür gibt es unterschiedliche Methoden. All diese fehlenden Schutzmechanismen haben dazu geführt, dass das System so ausgenutzt werden konnte.
FaktuM: Amadeus hat sich gerechtfertigt, dass man gegen automatisierte Roboterangriffe sehr wohl geschützt sei und dass das nur aufgrund eines „temporären Wartungsfensters" passieren konnte. Was Sie da sagen, klingt aber nicht so.
Miedler: Grundsätzlich wäre es natürlich möglich, dass eine Wartung zwischengeschaltet und ein direkter Zugriff erlaubt ist. Aber ganz ehrlich: Wenn ich so ein System warte, habe ich entweder ein Redundanzsystem (*Anm.: ein parallel laufendes System, das beim Ausfall des anderen den Dienst gewährleistet*) oder ich blockiere für diesen Zeitraum den Zugriff auf die Seite. Ob das mit dem Wartungsfenster stimmt, kann ich nicht beurteilen. Allerdings wurden die Angriffe, wie in der Studie beschrieben, ja nicht nur zu einem bestimmten Zeitpunkt gemacht.
FaktuM: SRL-Chef Karsten Nohl sprach davon, dass das System aus den 1980ern sei. Und es sei nicht das einzige, das so altmodisch ist. Ist da Ihrer Erfahrung nach was dran?
Miedler: Es ist definitiv etwas dran, dass es sehr viele Systeme gibt, die auf einem veralteten Status sind. Die 80er sind vielleicht ein bisschen extrem. Was man diesem System nicht vorwerfen kann, ist, dass es nicht einfach funktioniert. Das heißt, man hat vielleicht ursprünglich Funktionalität über Sicherheit gestellt. Heute sind aber solche Schwachstellen ein großes Business. Das sind nicht irgendwelche Teenager, die in einer Garage ausprobieren, was möglich ist. Da steckt eine ganze Industrie dahinter. Es sind moderne Verbrecher. Dagegen gibt es noch keinen adäquaten polizeilichen Schutz. Viele Unternehmen haben hier noch nicht die richtigen Investments getätigt, um die Sicherheit zu erhöhen, ohne die Nutzbarkeit einzuschränken. Oder sie haben auch einfach die Gefahr noch nicht erkannt.
FaktuM: Was ist der häufigere Grund?
Miedler: Oftmals ist es auch dem Umstand geschuldet, dass man Systeme nur schwer warten kann. Viele Unternehmen scheuen davor zurück, weil sie die Produktionssysteme nicht gefährden wollen. Aber das ist ein sehr gefährliches Spiel. Es muss ein Patch Management (*Anm.: schließt Sicherheitslücken, behebt Fehler oder fügt bislang nicht vorhandene Funktionen hinzu*) implementiert werden, um in regelmäßigen Abständen zu evaluieren, ob ein System noch der Zeit entspricht oder ob Anpassungen nötig sind. Viele Unternehmen haben das Risiko einfach noch nicht erkannt, das sie eingehen, wenn sie das nicht tun.
FaktuM: Es wurde auch die Frage aufgeworfen, ob eine Website wie CheckMyTrip überhaupt Sinn macht. Ist das ein wichtiges Service – oder einfach nur ein Sicherheitsrisiko?
Miedler: Das ist wieder so eine Gratwanderung zwischen Funktionalität und Security. Ist es unbedingt notwendig? Nein, wahrscheinlich nicht, weil man die Buchungsdaten ohnehin per Mail erhält. Andererseits wird man heute von E-Mails überschwemmt, nicht immer sind sie auf allen Geräten länger als eine Woche synchronisiert oder sie sind nicht immer zugänglich. Aus meiner Sicht spricht nichts gegen so ein Portal. Aber wenn ich diese sensiblen, personenbezogenen Daten der Öffentlichkeit zugänglich mache, dann muss ich auch jeden möglichen Schutz bieten. Wenigstens die Möglichkeit, ein stärkeres Passwort zu wählen. Schließlich geht es hier um persönliche Daten. Wenn ich Ihre Adresse weiß und dass Sie eine Woche nicht zu Hause sind – dann kann eine virtuelle Gefahr ganz schnell in der realen Welt landen. Weil dann ein Einbruch ziemlich simpel wird.
FaktuM: Das heißt, hier kann ziemlicher Schaden verursacht werden.
Miedler: Ja, aber der Schaden ist natürlich auch gegeben, wenn Ihr Flugticket auf einmal nicht mehr da ist.
FaktuM: Amadeus meinte, man prüfe jetzt „zusätzliche Sicherheitsmaßnahmen wie die Einführung eines Passworts". Sollte eine Passwortabfrage bei einem solchen Daten-Sammler nicht ohnehin vorhanden sein?
Miedler: Wenn ich die Daten so online stelle, muss es geschützte Schnittstellen – auch zu meinen Business-Partnern – geben. Also ja, gerade in der heutigen Zeit sollte das eigentlich gegeben sein.
FaktuM: Wie legt man ein Passwort so an, dass es wirklich gut schützt?
Miedler: Zum einen müsste man eine Passworterkennung hinterlegen, die ein Passwort, das nicht aus Groß- und Kleinbuchstaben, mindestens einem Sonderzeichen oder das aus Wörterbuch-Wörtern besteht, gar nicht zu-



IT-Experte Daniel Miedler: Heute sind solche Schwachstellen ein großes Business. Das sind keine Teenager, die in einer Garage etwas ausprobieren

fotolia/ Elnur, Dimension Data Austria

lässt. Wir alle wissen aber: Das führt dann dazu, dass sich die Leute die Passwörter aufschreiben. Die Alternative zu so einem starken Passwort, das sich keiner merkt, könnte eine zweite Sicherung sein. Zum Beispiel ein Code, der per SMS übermittelt wird und der zusätzlich eingegeben werden muss. Den meisten Leuten, die es schaffen, über eine Plattform eine Buchung abzuwickeln, kann man auch zutrauen, so einen zweiten Faktor zu verwenden. Damit hätte ich einen variablen Faktor, der nicht mehr mit einer Brute-Force-Attacke ausgerechnet werden kann.

FaktuM: Es gab zuletzt auch einen Fall aus der Hotellerie, der Aufsehen erregt hat: Das Seehotel Jägerwirt wurde bereits mehrfach Ziel von Hacker-Angriffen. Was ist hier passiert?

Miedler: Vorweg: Der Fall wurde medial auch falsch dargestellt. Da war von Personen die Rede, die in ihrem Zimmer eingesperrt waren. Oder ausgesperrt. Tatsächlich passiert ist, dass das System, das die Chipcodes für die Zimmerkarten ausstellt, durch eine Attacke lahmgelegt wurde. Es wurde so kompromittiert, dass es nicht mehr benutzbar war. Dadurch konnten keine neuen Zimmerkarten mehr vergeben werden. Die Bestandsgäste konnten ihre Zimmer aber betreten und verlassen. Alles andere wäre ja fatal und niemand würde ein System so konzipieren.

FaktuM: Wie konnte es dazu kommen?

Miedler: Ein Mitarbeiter hat eine schadhafte Datei auf einem System ausgeführt, das vollen Zugriff auf den Verwaltungsserver hatte. Das System für die Zimmerkarten wurde mit Forderung einer Erpressungszahlung lahmgelegt. Viele zahlen in so einem Fall – das war sogar eine Empfehlung des FBI – und tun dann aber nichts weiter. Solche Ransom-Attacken (*Anm.: zerstören Backup-Dateien und verschlüsseln regulär genutzte Dateien*) halten sich aber häufig weitere Zugänge offen. Denn jemand, der einmal zahlt, zahlt wahrscheinlich wieder. Wenn ich das System einfach weiter verwende, kann es auch zu weiteren Angriffen kommen.

FaktuM: Hätte man verhindern können, was da passiert ist?

Miedler: Einen hundertprozentigen Schutz gibt es nicht. Meistens kommt solche Schadsoftware als Anhang an Office-Dateien, wo im Hintergrund noch ein Programm ausgeführt wird (Makro). Es gibt Schutzmaßnahmen, die solche Dateien überprüfen und das Mail erst danach freigeben. Das Problem im Tourismus ist, dass man sehr häufig mit Neukunden zu tun hat. Man kennt die nicht, will sie aber als Kunden gewinnen und öffnet, was sie geschickt haben. Wichtig ist daher, die Mitarbeiter zu sensibilisieren. Wenn zum Beispiel eine verschlüsselte Zip-Datei mitgeschickt wird. Warum sollte ein potenzieller Konferenzgast so etwas machen? Die dritte wichtige Maßnahme ist es, solche Systeme wie das zum Kartenausstellen von den normalen Büro-Computern zu segmentieren. Es ist unangenehm, wenn so ein Computer kompromittiert wird. Aber dann sollte kein Zugriff auf sensible Systeme gegeben sein. Und: Natürlich kann ein kleines oder mittleres Hotel nicht ein Schutzsystem wie ein großes Rechenzentrum auffahren. Aber es gibt z.B. sogenannte Unified Threat Management Systeme, die den Schutz schon extrem steigern.

FaktuM: Ist so etwas auch leistbar?

Miedler: Durchaus. Je nach Anforderung beginnen wir da zwischen 500 und 1.000 Euro. Man sollte hier nicht zögern, denn Cyberkriminalität entwickelt sich extrem schnell weiter. Der Schutz von heute kann morgen schon zu wenig sein.

FaktuM: Vielen Dank für das Gespräch. ■

Offenbar hat die Lufthansa inzwischen reagiert: Sie bietet neuerdings bei Flugbuchungen die Option, den Buchungscode nicht mehr in die E-Mail zu inkludieren, weil diese unverschlüsselt übertragen wird.

SPRECHEN SIE BARCODISCH?

Veränderungen verpasst: So schätzt der Wiener Sicherheitsexperte Adrian Dabrowski (SBA Research) das Amadeus-Dilemma ein.

Adrian Dabrowski

Was hier passiert ist, war kein „Hack" im technischen Sinne. Die Buchungssysteme (GDS, Global Distribution Systems) wie Amadeus und Galileo wurden für ein früheres Distributions- und Sicherheitsmodell entworfen – das heute so nicht mehr gültig ist – und seither im Kern nicht mehr angepasst.

Es hat sich aber in den letzten Jahrzehnten viel geändert: Kunden kaufen deutlich weniger über Reisevermittler ein und die Verkaufsprozesse passieren heute fast ausschließlich ohne manuelles Zutun. Früher waren GDS-Zugänge noch teurer und vertragliche Klauseln stellten sicher, dass nur berechtigte Änderungen vorgenommen werden. Dazu gehört implizit, dass der Kunde, wenn er persönlich vorstellig wurde, auch in irgendeiner Weise „identifiziert" wurde. Zum Beispiel per Ausweis, Wiedererkennung durch den Berater o.ä.

Ein Quasi-Direktverkauf bzw. ein automatisierter Direktzugriff auf den PNR (Fluggastdatensatz) durch den Kunden war in diesem Vertriebsmodell nicht vorgesehen. Und daher auch nicht im Sicherheitsmodell.

Beim Direktverkauf an den Kunden fehlte die obige Identifizierung – und mangels Alternativen wurde einfach die PNR-Kennung herangezogen, die schon für die Abwicklung der verschiedenen Aspekte des Fluges notwendig ist, statt eine neue Kennung zu erfinden. Diese ist aber quasi öffentlich: Am Ticket, am Boardingpass, am Baggage-Tag …

Dass etwas „nur" in einem Barcode kodiert ist, gilt übrigens nicht als sicher. Jeder, der „Barcodisch" spricht, kann diese Daten problemlos lesen (z.B. eine App am Handy). Der saubere Weg wäre eine Trennung der verschiedenen Funktionen der PNR-Kennung: Eine PNR für den Boardingpass, einen anderen Code für das Gepäck, wieder einen anderen Code oder ein Passwort für das Ändern der Buchung. Oder: Den direkten Kontakt mit dem Kunden suchen. ■