# Durchgecheckt

Bruno Cirone, DOAG Themenverantwortlicher Security

Es ist schon erstaunlich, was man als Oracle-Datenbank-Berater im Lauf seines Berufslebens so alles erlebt. Gerade im Security-Bereich gibt es immer wieder Aha-Erlebnisse, die einem die Sprache verschlagen. Zwei exemplarische Beispiele.

Beim ersten Beispiel wurde ich vom Deutschland-CIO eines amerikanischen, multinationalen Chemiekonzerns beauftragt, einen Security-Check bei einem seiner Tochterunternehmen vorzunehmen. Es sollte nur ein Tag dauern und einfach nur eine Geschmacksrichtung der Security wiedergeben. Also es war klar, er wollte von mir ein pauschales Okay erhalten – und dies natürlich, ohne größere Investitionen zu tätigen.

Aber was sollte ich überhaupt prüfen? Die Antwort war einfach und klar: „Natürlich alles." Selbstverständlich ist dies von einer Person gar nicht zu bewältigen. Insbesondere an nur einem Tag ist das absolut unmöglich und eher absurd. Daher hatte ich den Auftrag zunächst abgelehnt. Der CIO bat mich trotz meiner Bedenken, den Auftrag anzunehmen, was ich dann wegen meiner Neugier tat.

Das Tochterunternehmen war ein Forschungslabor und forschte unter anderem nach Additiven, um die Stoffe länger haltbar, kälteresistenter und geschmeidiger zu machen. Es war klar, dass diese Forschungsergebnisse (Patente) einen erheblichen Wert für das Unternehmen darstellten.

Nach der Beauftragung musste ich ein polizeiliches Führungszeugnis vorlegen und meine finanzielle Situation erklären. In dieser Zeit bekam ich verschiedene Anrufe von Auskunfteien, die alle mehr oder weniger das Gleiche wissen wollten: „Seit wann existiert Ihre Firma?", „Haben Sie Referenzkunden?" etc.

Etwa zwei Wochen vor dem Termin erhielt ich eine DVD mit einem Belehrungsfilm, der die Sicherheitsmaßnahmen erklärt und ebenso, an wen man sich wenden muss, falls man das Gefühl hat, dass etwas nicht in Ordnung ist. Ich musste diesen Film ansehen und danach online einen Prüfungsfragebogen fehlerfrei ausfüllen. Erst danach wurde der Termin final bestätigt.

Am Beratungstag musste ich meinen Pass beim Empfang hinterlegen und be-

kam einen Besucherausweis, danach wurde ich von einem Mitarbeiter abgeholt. Beim Laborkomplex angekommen, wurde mein Besucherausweis durch einen spezielleren Ausweis ausgetauscht.

Endlich ging es an dem eigenen Rechenzentrum vorbei in einen Besprechungsraum. Auf mich warteten etwa fünfzehn Wissenschaftler und Laborleiter. Ich fragte meinen Begleiter, ob die Server von der zentralen Administration betreut werden. Er meinte: „Natürlich nicht, wir sind hier in einem Hochsicherheitsbereich, da haben auch die internen Administratoren keinen Zugriff drauf." Ich war von den bisherigen Sicherheitsmaßnahmen beeindruckt. So einfach konnte keiner hier reinkommen.

Die Besprechung lief wie erwartet. Keiner der Teilnehmer hatte meinen Besuch gefordert oder gar gewünscht. Da galt es zunächst, die Angst vor dem Security-Thema zu nehmen. Die Besprechung wurde im Lauf des Tages immer angenehmer, aber auch anstrengender.

Nach rund zwölf sehr intensiven Stunden war die Besprechung kurz vor dem Ende. Ich hatte mein Notebook runtergefahren, die Unterlagen zusammengestellt und meinen Aktenkoffer schon fast geschlossen. Da hatte einer der Wissenschaftler doch noch eine Frage: „Können wird die Datenbank weiterhin über eine ODBC-Anbindung komplett auf das Notebook kopieren und dann mit Microsoft Access weiterarbeiten?" Ich sackte in meinem Stuhl zusammen und konnte nur noch ein „Wie bitte?" von mir geben. Der Wissenschaftler meinte: „Ich muss ja weiterarbeiten können, wenn ich im Zug unterwegs bin oder auf dem Flughafen auf meinen Flug warte." Ich dachte noch an einen letzten Strohhalm: „Haben Sie auf dem Notebook eine Verschlüsselungssoftware und wann wird der Bildschirm gesperrt?" Die Antwort war für mich nicht überraschend. „Die Verschlüsselungssoftware haben wir mal bestellt, aber irgendwie war die wohl zu teuer und zu aufwendig, daher nutzen wir sie nicht. Ich schalte meine Bildschirmsperre ab; es nervt, wenn ich dann alle paar Minuten mein Passwort eingeben muss." Ich konnte eine gewisse Frustration nicht verbergen.

Mein Abschlussbericht hatte danach durchaus etwas Positives für die Mitarbeiter. Alle bekamen innerhalb kürzester Zeit neue Hochsicherheits-Notebooks mit eigenen Telefonkarten. Auf jedem Notebook ist eine Oracle-Datenbank installiert, die auch nur ihre eigenen Daten beinhalten durfte.

## Bei den Erlkönigen

Das zweite Beispiel stammt von einem Automobilzulieferer. Auch hier sollte ich einen schnellen Überblick über die Security-Situation liefern. Im Vorhinein wurde mir mitgeteilt, dass ich keine Kamera, Smartphone oder Telefon mit Kamera, Werkzeuge etc. mitbringen durfte. Am Werkseingang wurden mein Wagen und meine Unterlagen untersucht.

Während ich auf meine Abholung wartete, fuhren zwei LKW auf dem Werksgelände vor. Einer mit „Pampers"-Logo, der andere mit einem Logo einer Fernsehmarke. Ein Automobilzulieferer mit einem „Pampers"-LKW machte mich schon sehr neugierig, deshalb habe ich den Mitarbeiter, der mich abgeholt hat, danach gefragt. Er sagte, dass alle Erlkönige, also Fahrzeuge, die in etwa zwei bis drei Jahren auf den Markt kommen, in solchen Fahrzeugen zu ihnen gebracht werden. Es wäre ja nicht auszudenken, wenn Fotos, Videos etc. von den Erlkönigen auf ihrem Gelände gemacht werden würden. Sollte so etwas passieren, kündigen die Fahrzeughersteller den Vertrag mit den Zuliefererfirmen.

Im Werk selber gab es für diese Erlkönige einen speziellen, abgesicherten Bereich. Dort sind besondere Zutrittsausweise notwendig, die Fensterscheiben sind bleiverglast und die Techniker müssen Bleimatten über die Fahrzeuge legen, wenn sie nicht daran arbeiteten. Die LKW wurden entladen und ich konnte die Fahrzeuge sehen, die in zwei Jahren auf den Straßen fahren werden. Diese Fahrzeuge wurden mit Messtechnik vollgestopft.

Dieser Bereich hatte einen eigenen Oracle Server für etwa fünfzig Mitarbeiter. In der dazugehörigen Datenbank sind alle Daten wie Messergebnisse, Optimierungen, Anforderungen an Werkzeugen etc. festgehalten. Der Standort des Servers war allerdings nicht in diesem Hochsicherheitsbereich, sondern in einer Abstellkammer ohne besondere Sicherheitsvorkehrungen. Der Putzfrauenschlüssel diente zum Öffnen der Tür und war auch sinnvollerweise neben der Tür aufgehängt.

Nach einer kurzen Einführungsphase durfte ich meine Arbeit beginnen. Man hatte mir ein kleines Büro zur Verfügung gestellt. Die Login-Daten vom Oracle User wurden mir in einem versiegelten Umschlag übergeben. Das Passwort würde nach meinem Besuch wieder geändert. Sehr gut, bis auf die Abstellkammer war das vollkommen okay.

Im Laufe des Tages wollte ich mich als „root"-User auf dem System anmelden. Da ich das Passwort nicht wusste, habe ich einen der Techniker danach gefragt. Die Antwort war: „Das Passwort ist toor, also root rückwärts geschrieben". Was soll man dazu noch sagen? Dafür war aber der Oracle-User (auf dem Papier) bestens geschützt.

## Fazit

Diese beiden Beispiele waren etwas ungewöhnlich, aber sie zeigen die Kernprobleme sehr deutlich. Die Investition in Security-Maßnahmen wird nicht immer als sinnvoll angesehen. Security kann ja nicht mit einem Return on Invest (ROI) schöngerechnet werden. Eine fehlende Sensibilisierung und (menschliche) Nachlässigkeiten führen zu erheblichen Security-Problemen. Letztlich kann man die notwendigen Maßnahmen auf diese Formel bringen: „Security kostet Geld, Performance und Ressourcen. Keine Security kostet noch mehr Geld und gefährdet das Unternehmen".

Bruno Cirone
bruno.cirone@doag.org