



Do 14.01.10 22:00

Datenklau per Funk – Sicherheitsrisiko an deutschen Flughäfen

Die Diskussion über die Sicherheit an deutschen Flughäfen geht weiter – Stichwort „Nacktschanner“. Doch nun gibt es ein ganz neues Problem: Hacker sind in der Lage, die Ausweise des Personals heimlich per Funk zu kopieren. Mit solchem Datenklau könnten sich Terroristen Zugang zu sicherheitsrelevanten Bereichen verschaffen.

Da regt sich ganz Deutschland über Sinn oder Unsinn sogenannter Nacktschanner an deutschen Flughäfen auf – und niemand bemerkt, dass an anderer Stelle eine wesentlich größere Sicherheitslücke klappt! KONTRASTE hat aufgedeckt, dass sich potentielle Terroristen mit einem Datendiebstahl per Funk mühelos Zugang auf das Flughafengelände verschaffen können. Eine beängstigende Vorstellung. Matthias Deiß mit den Einzelheiten.

Flughafen Hamburg, vor einer Woche. Erhöhte Sicherheitsstufe nach dem Anschlagversuch von Detroit, jeder Passagier wird penibel kontrolliert.

Keine Personalkontrollen dagegen an vielen Eingängen für das Flughafenpersonal, dabei ist hier die Sicherheit besonders gefährdet, wie KONTRASTE nachweist.

Im Zentrum des Sicherheitslecks stehen die Chipkarten der Flughafenmitarbeiter. Sie lassen sich per Funk heimlich auslesen. Terroristen, die diesen Abhörvorgang beherrschen, kommen am Hamburger Flughafen mit den geklauten Daten ohne persönliche Kontrolle direkt zum Rollfeld und können eine Bombe an Bord eines Flugzeugs schmuggeln, erzählt uns ein Mitarbeiter.

Mitarbeiter (Stimme nachgesprochen)

„Ich habe mit der Karte Zugang zum sicherheitssensiblen Bereich. Das heißt, ich komme über Zufahrtstore, Straßen, über Terminals und Gates direkt aufs Vorfeld und natürlich auch in ein Flugzeug. An der Tür direkt vor dem Rollfeld wird in der Regel nicht persönlich, sondern nur mit der Karte kontrolliert.“

Der Datenklau per Funk findet KONTRASTE heraus, ist nur deshalb möglich, weil das am Flughafen Hamburg verwendete Zugangssystem Legic Prime ungenügend gesichert ist. Und so funktioniert der Datenklau.

Das Lesegerät am Personaleingang sendet elektromagnetische Wellen aus. Wird eine Mitarbeiterkarte vorbeigeführt, aktivieren die Wellen den Funkchip auf der Karte, der nun seine Informationen preis gibt. Das Lesegerät prüft diese Informationen und öffnet die Tür.

Das ist eine Kopie des offiziellen Lesegeräts. Nachgebaut von den Hackern des Chaos Computer Clubs in Berlin.

Kommt ihr falsches Lesegerät in die Nähe einer Mitarbeiterkarte, liest es die Chipdaten ebenfalls aus und speichert sie.

Am Flughafen reicht dafür ein gezielter Remppler im vollen Terminal oder auf der Rolltreppe, denn viele Mitarbeiter tragen ihre Ausweise offen am Körper.

Mit den so geklauten Daten wird das falsche Lesegerät zu einem falschen Mitarbeiterausweis. Das Lesegerät am Flughafen checkt dessen Daten, erkennt einen Mitarbeiter und öffnet die Tür. Das System ist geknackt.

Karsten Nohl, Chaos Computer Club

„Das System auszuhebeln ist einfach, was uns sehr überrascht hat, weil es als Sicherheitssystem vermarktet wird und sehr verbreitet ist. Wir waren schlicht schockiert, überhaupt keine Hürden zu finden, die wir hätten überwinden müssen.“

Die beiden Computerspezialisten Henryk Plötz und Karsten Nohl geben ihre brisante Entdeckung Ende Dezember an die Sicherheitsbranche weiter. Seitdem müsste der Flughafen also Bescheid wissen. Bis heute aber wird an den Personalzugängen unzureichend kontrolliert. Dabei könnte sich längst auch anderswo herumgesprochen haben, dass das Zugangssystem nicht mehr sicher ist.

Henryk Plötz, Chaos Computer Club

„Legic Prime ist definitiv geknackt. Wir wissen jetzt alles darüber, was wir wissen können, was wir wissen müssen und können jetzt überall einbrechen, wo Legic Prime eingesetzt wird, zum Beispiel an Flughäfen.“

Wir konfrontieren den Flughafen Hamburg mit unseren Erkenntnissen. Über Versäumnisse oder gar Konsequenzen will man mit uns nicht reden, gibt die Sicherheitsprobleme mit den Mitarbeiterkarten aber per E-Mail zu. Zitat: *„Der Flughafen Hamburg ist sich der Thematik rund um das Datensystem Legic Prime bewusst. Aus Sicherheitsgründen werden wir jedoch keine weiteren Erläuterungen geben.“*

Nach Informationen von KONTRASTE kommt das unsichere Zugangssystem außer in Hamburg auch an den Flughäfen Stuttgart, Dresden, Hannover und Berlin Tegel zum Einsatz. Einige dieser Flughäfen bestätigen unsere Informationen, vor der Kamera aber von allen kein Kommentar!

Wir wenden uns an den Hersteller der Sicherheitstechnik. Die Firma Legic sitzt in der Schweiz, gilt weltweit als einer der Marktführer für drahtlose Zugangssysteme im Hochsicherheitsbereich und ist stolz auf ihre internationale Kundschaft. Der gegenüber versicherte Legic zumindest bis 2006 in einem vertraulichen Schreiben, das KONTRASTE vorliegt, eine falsche Produktsicherheit. So heißt es darin über Legic Prime, Zitat:

„Das Aufzeichnen der übertragenen Daten und späteres Wiedereinspeisen ist nahezu unmöglich. Durch die Verschlüsselung der Daten ... wird eine sehr hohe Datensicherheit erreicht.“

Wir zeigen das Dokument dem Chaos Computer Club. Der kommt zu anderen Ergebnissen.

Karsten Nohl, Chaos Computer Club

„Legic Prime hatte keine Verschlüsselung. Das ist schlicht falsch.“

Wir wollen von Legic wissen, was hinter diesem Vorwurf steckt, werden aber abgewiesen. Kein Interview. Dafür ändert Legic plötzlich die Internethomepage. Hieß es dort vor unserer Anfrage, das System Legic Prime biete „hohe Sicherheit“, steht dort auf einmal kleinlaut nur noch „Basis-Sicherheit“.

Für die Polizei, die an den Flughäfen nicht für die Kontrollen am Gate, aber die Sicherheit auf dem Rollfeld zuständig ist, ist die von Kontraste aufgedeckte Sicherheitslücke unerträglich. Ihre Gewerkschaft fordert die betroffenen Flughafenbetreiber auf, sofort zu handeln.

Reiner Wendt, Deutsche Polizeigewerkschaft

„Zunächst einmal müssen die Karten, die den Zugangsberechtigten zur Verfügung stehen und die Lesegeräte sofort ausgetauscht und auf den neuesten Stand gebracht

werden. Was aber mindestens genauso wichtig ist, ist, dass die Flughafenbetreiber ihre Sicherheitstechnik unter die Dienstaufsicht der Bundespolizei stellen, damit regelmäßig kontrolliert wird, ob da auch nicht rumgepuscht wird und damit die nicht so weiter machen können, wie bisher."

15.000 Karten und alle Lesegeräte auszutauschen, sei viel zu teuer, heißt es am Flughafen Hamburg. Genau wie alle sicherheitsrelevanten Eingänge in Zukunft mit Personal zu bewachen. Für Terroristen stehen die Türen damit weiter offen.

Beitrag von Matthias Deiß

Stand vom 14.01.2010

Dieser Beitrag gibt den Sachstand vom 14.01.2010 wieder. Neuere Entwicklungen sind in diesem Beitrag nicht berücksichtigt.

© Rundfunk Berlin-Brandenburg

http://www.rbb-online.de/kontraste/archiv/kontraste_vom_14_01/datenklau_per_funk.html