19. Sicherheitslücke durch neues "elektronisches Sperrwerkzeug" bei E-Schließsystemen

Sicherheit elektronischer Schließsysteme durch neue Geräte infrage gestellt!

Bereits seit Anfang des Jahres in Form von Entwicklungsstufen und Prototypen wurde die Existenz spezieller Übertragungsgeräte von Daten bekannt und in einigen Veröffentlichungen darüber berichtet.

Anlässlich der Security wird nun von der Firma MIB-Elektronik auf dem Stand der Firma Wendt dieses Gerät offiziell dem Markt vorgestellt (Halle 7.0, Stand 7.-210). Durch die Existenz eines solchen Hilfsmittels entsteht eine so große Sicherheitslücke bei Schließsystemen, die ausschließlich auf elektronischer Basis aufbauen, dass nicht mehr von der erforderlichen Sicherheit gesprochen werden kann.

Anfang des Jahres wurden Hinweise bekannt, dass sich Elektronikspezialisten damit befassen, Schließsysteme, d. h. in erster Linie Schließzylinder, jedoch auch Sicherungssysteme in reiner berührungsloser Übertragung von Daten (Zeiterfassung, Zugangskontrolle, Alarmanlagen) durch eine Datenübertragung von einem anderen Ort zum Empfangsgerät bemühen. Die Inaugenscheinnahme der ersten Prototypen ließen bereits das Ziel der Entwicklung erkennen, die im Wesentlichen darauf basierte, dass nicht der Versuch unternommen wurde, die Datenspeicher zu entschlüsseln, sondern dass das Datenpaket, in welcher Form es auch immer entstanden ist, „huckepack“ auf ein extrem schnelles Übertragungsnetz, also in Echtzeit gepackt und zum Empfänger übertragen wird.

Dazu ein Beispiel: Ein Hausbesitzer verfügt über eine elektronische Alarmanlage, die über einen Datenchip deaktiviert wird.

Er befindet sich zum Essen in einem Restaurant, hängt seine Jacke über den Stuhl. In der Jackentasche befindet sich u. a. der Datenträger (Transponder) für die Alarmanlage.

In räumlich kurzer Distanz wird das Empfangsgerät zu der Jacke gebracht, etwa durch eine weitere Jacke, die auf der benachbarten Stuhllehne abgelegt ist. Der Datentransfer zu dem Partnergerät, mit dem auch ein zweiter Mann vor dem Objekt stehend ausgestattet ist, kann beginnen. Aufgrund des extrem schnellen Übertragungsweges kann eine räumliche Distanz von mehreren Kilometern, der Prototyp wies Erfolge bis ca. 10 km auf, vorgenommen werden.

Wie die Demonstration gezeigt hat, wird auf diesem Wege die Alarmanlage ausgeschaltet. Beim Auslesen des Speichers der Alarmanlage erscheint der Datenträger des Eigentümers. Bei der bisherigen Demonstration war es unabhängig, ob es sich um einen Festcodetransponder, einen Wechselcodetransponder oder um ein cryptologisch verschlüsseltes Transpondersystem handelte.

Das Datensignal selbst wird nicht aufgelöst, sondern so wie es von dem Datenträger abgegeben wird, auch die Response beim Cryptosystem bleibt unverändert und unaufgelöst, wird es auf dem schnellen Übertragungsweg zum Empfänger, in diesem Fall der Alarmanlage, transportiert. Aufgrund dieses schnellen Übertragungsweges wird es sogar möglich sein, die Informationen in ein Zeitfenster hinein zu übertragen. Es entstand somit kein Unterschied, ob nun der Datenträger direkt an dem Schließzylinder oder dem Bedienteil der Alarmanlage gewesen ist oder 10 km davon entfernt aufbewahrt wurde. Zurzeit sind die Geräte, wie die kürzlich eingeholten Informationen, bezogen auf die Präsentation der Security ergeben hat, für alle Schließzylinder und Sicherungssysteme im 125 kHz

Bereich der elektronischen Schlüssel, Bedienteile von Zeiterfassungs-/Zugangskontrollen- sowie Alarmanlagensystemen tauglich.

Geräte im 13.56 MHz-Bereich und für Kfz sollen folgen.

Eine weitere große Anwendungsmöglichkeit besteht bei der Datenübertragung von Fahrzeugbediensystemen wie beispielsweise dem Keyless-Go bei Mercedes und den in Planung befindlichen Systemen von BMW, Audi usw., bei dem lediglich das Tragen der Karte am Körper durch Annäherung an das Fahrzeug eine Öffnung und beim Sitzen im Fahrzeug das Starten möglich gemacht wird.

Die Existenz derartiger Geräte stellt die Sicherheit von rein elektronischen Schließ- und Sicherungssystemen infrage.

Im Falle eines Schadenereignisses (Einbruchsdiebstahl, Entwendung eines Fahrzeuges usw.) muss der Versicherungsnehmer dem Versicherer gegenüber den Einbruchsdiebstahl nachweisen. Das Auslesen der Speicher würden lediglich die Daten des Chips oder Transponders von dem Versicherungsnehmer aufzeigen.

Eine Nachweismöglichkeit, dass dieses Gerät eingesetzt wurde und somit ein Fremdtäter in Betracht kommt oder der Eigentümer einen Einbruchsdiebstahl vortäuschen will, ist ausgeschlossen. So wie bisher bei mechanischen Sicherungssystemen die Möglichkeit bestanden hat, etwa durch Nachweis, dass Sperrwerkzeuge zur Betätigung eines Schließsystems eingesetzt wurden und damit die Existenz eines Fremdtäters anhand der Spuren belegt werden konnte, ist bei dem Einsatz dieses Gerätes nicht mehr möglich.

Unabhängig davon besteht für den Täter natürlich auch die Möglichkeit, das elektronische Schließsystem wieder ordnungsgemäß zu „verschließen“, sodass auch das Entdeckungsrisiko, dass hier ein Einbruchsdiebstahl überhaupt stattgefunden hat und somit auch eine Zuordnung zur Tatzeit erfolgen kann, ebenfalls ausgeschlossen ist. Es erhebt sich jetzt die Frage, zumal die elektronischen Schließsysteme gegenüber den rein mechanischen eine Vielzahl von Vorteilen beinhalten, wie dennoch das erforderliche Sicherheitsbedürfnis trotz Existenz dieser Geräte abgedeckt werden kann.

Bisher existieren Schließzylinder mit rein mechanischen und sehr hochwertigen Schließsystemen. In den letzten Jahren wurden solche verstärkt auf den Markt gebracht.

Im Wesentlichen boten die dort eingebauten Sicherungen Widerstand gegen die Vielzahl frei zu erwerbender Nachsperrwerkzeugen.

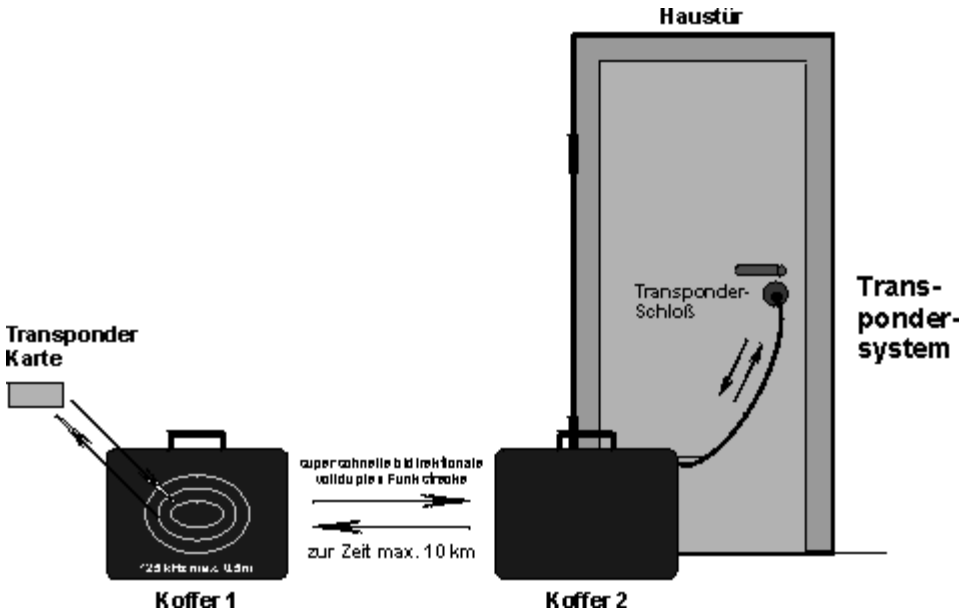
Aufgrund dieser Maßnahmen war es, wenn überhaupt, nur noch einem sehr kleinen Kreis von Spezialisten möglich, solche Zylinder und Schließsysteme zu überwinden. Es fehlten jedoch die Vorteile elektronischer Schließsysteme, z. B. durch Umstellen und Eliminieren eines in Verlust geratenen Schlüssels.

Die Industrie hat Schließsysteme einerseits mit sehr hochwertigen und aufwendig konstruierten mechanischen Sicherungseinheiten und kombiniert mit dem Einsatz der Elektronik-Komponente als handhabungsfähige Produkte auf den Markt gebracht.

Zur Überwindung eines solchen Produktes wäre somit der hochwertige Spezialist für mechanische Sicherungen und die Anwendung des o. a. elektronischen Gerätes erforderlich. Der Kreis derer, die solche Systeme überwinden können, verkleinert sich somit noch einmal.

Eine denkbare Lösung stellt eigentlich nur ein Produkt dar, das es erforderlich macht, wechselseitig kombinierte Abfragen des mechanischen Codes des Schlüssels und der elektronischen Daten vorzunehmen. Während der Handhabung muss dieser Vorgang mehrfach erforderlich werden und in einem gewissen Zeitfenster erfolgen. Werden diese Bedingungen nicht erfüllt, bleibt das Schließsystem verschlossen. Der elektronische Speicher registriert eine Fehlermeldung.

Dass solche hochwertigen Sicherungseinrichtungen ihren Preis haben, dürfte einleuchtend sein. Andererseits werden solche Schließsysteme nicht zur Absicherung einer Gartentür verwendet. Dennoch wäre hierdurch die Möglichkeit geboten, eine Absicherung hochwertigen Gutes trotz existierender mechanischer und elektronischer „Sperrwerkzeuge“ in geeigneter Weise vorzunehmen.



Manfred Göth

Kriminaltechnisches Prüflabor GÖTH, GmbH, Mayen

www.goeth.com

Mitglied der DGfK (Deutsche Gesellschaft für Kriminalistik)

und Gründungsmitglied des EVU (Europäische Vereinigung für Unfallforschung und Unfallanalyse e.V.)