Mit Manipulation in der Datenübertragung Tür und Tor geöffnet?

Angriffe auf Zutrittskontrollanlagen können vielfältiger Natur sein. Zum einen besteht die Möglich des Angriffs auf die Daten des Zutrittskontroll-Datenbankservers wo u.a. Personenstammdaten, Zutrittsprofile und Ereignisse gespeichert und verarbeitet werden, zum anderen kommt das Gespräch sehr schnell auf die Sicherheit der Luftschnittstelle zwischen Ausweis und Ausweisleser.

Die nachfolgende Betrachtung behandelt ausschließlich Angriffsmöglichkeiten auf Datenübertragungswege innerhalb einer Zutrittskontrollanlage und nicht Angriffe auf den Datenbankserver oder sonstige Manipulationsmöglichkeiten!

Grundsätzlich sind alle Objekte, in denen ein Transpondertyp verwendet wird und dessen Sicherheitsmechanismen überwunden wurden wie z.B. Legic Prime und Mifare Classic, potenziell gefährdet. Darüber hinaus gibt es weitere Sicherheitslücken in Zutrittskontrollsystemen, die es ermöglichen - entsprechende Kenntnisse und Aufwand vorausgesetzt - Daten zu manipulieren und damit den unberechtigten Zutritt zu Sicherheitsbereichen zu erlangen. Dies trifft besonders dann zu, wenn das Zutrittskontrollsystem und die zugehörigen organisatorischen Maßnahmen nicht kompetent geplant und konsequent umgesetzt wurden.

Manipulation von Daten versus Schwächen im Sicherheitsmanagement

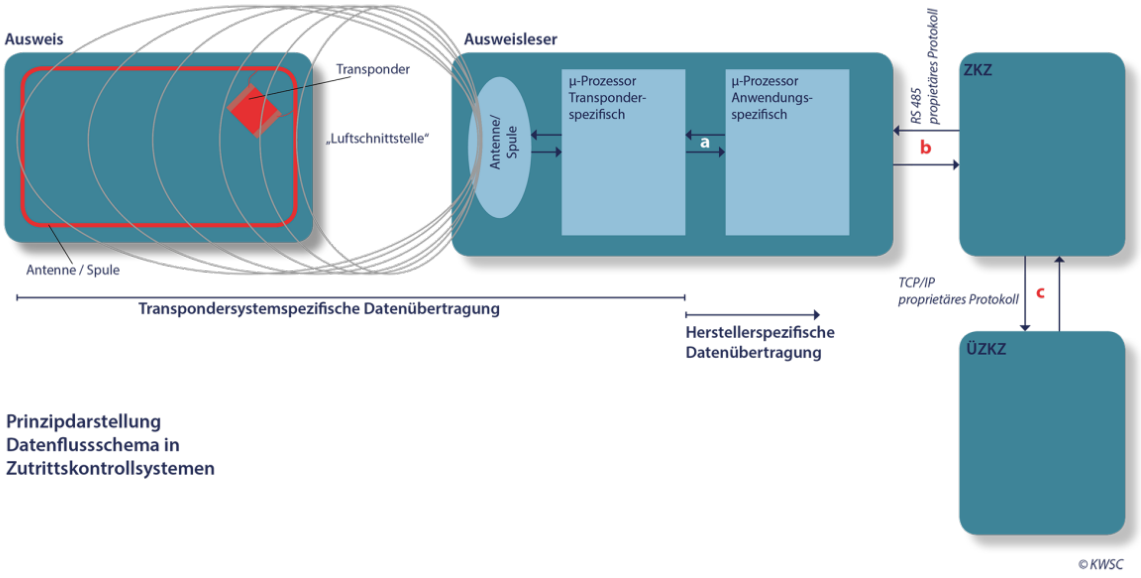
Das sei vorweg gesagt: Die einfachste Methode unberechtigt Zutritt zu erlangen erfordert keinerlei technische Kenntnisse, sondern nur ein freundliches „Guten Morgen“ und ein Lächeln auf den Lippen. In der Regel wird ein Zutrittsberechtigter, der die Tür freigeschaltet hat, einer unberechtigten Person diese höflich aufhalten und damit den Zutritt ermöglichen. An dieser Stelle muss ganz pragmatisch das Sicherheitsmanagement ansetzen. Dazu gehört u.a. Schulung und Sensibilisierungen der Mitarbeiter, Konzeption von Sicherungszonen und Sicherungslinien sowie abgestuften Sicherheitsmaßnahmen an den Zutrittsstellen der Sicherungslinien. Das ist jedoch nur am Rande das Thema dieses Beitrags. Das vorstehend genannte Beispiel zeigt aber, dass die Betrachtung von Risiken durch eine Datenmanipulation wenig Sinn macht, wenn die schutzzielorientierten Grundsätze und Gebote zu Errichtung eines Zutrittskontrollsystems bei der Konzeption und Planung nicht umgesetzt wurden.

Schwachstellen im Datenfluss einer Zutrittskontrollanlage (ZKA)

Die Angriffsmethoden erfordern erhebliche technische Kenntnisse und teilweise hohen zeitlichen Aufwand. Es ist daher naheliegend, dass potentielle Angreifer auch Kosten/Nutzen-Betrachtungen anstellen. Die Kardinalfrage lautet: Was gibt es zu gewinnen und geht

es nicht einfacher (siehe vorstehenden Abschnitt). Ein großer Aufwand für einen technischen Angriff wird sicher nur dann in Kauf genommen, wenn es keine anderen Möglichkeiten gibt, der Erfolg das rechtfertigt und keine sichtbaren „Spuren“ des Angriffs hinterlassen werden.

Schnittstellen, die Angriffen ausgesetzt sein könnten



Prinzipdarstellung
Datenflussschema in
Zutrittskontrollsystemen

1. Die Luftschnittstelle (Schnittstelle zwischen Ausweis und Ausweisleser)

An erster Stelle steht die Luftschnittstelle. Die Kommunikation zwischen Ausweis und Ausweisleser findet hier statt, die µ-Prozessoren auf beiden Seiten und das dort laufende Programm und Protokoll sind spezifisch für den eingesetzten Transpondertyp, und werden beide im Regelfall durch den Hersteller des Transponders (Mifare, Legic, HID, usw.) hergestellt.

2. Die Schnittstelle a (Interne Schnittstelle im Ausweisleser)

Der Ausweisleser wird durch einen µ-Prozessor des Herstellers der ZKA gesteuert. Dieser gibt über Schnittstelle a dem transponderspezifischen µ-Prozessor u.a. vor, welches Segment des Ausweises gelesen werden soll, und erfährt über diese Schnittstelle, ob ein gültiger Ausweis erkannt wurde, sowie dessen Ausweisnummer.

3. Die Schnittstelle b (Schnittstelle zwischen Ausweisleser und Zutrittskontrollzentrale)

Der Ausweisleser kommuniziert über Schnittstelle b mit der Zutrittskontrollzentrale (ZKZ) und übermittelt die gelesene Ausweisnummer an die ZKZ. In der ZKZ sind alle für diesen

Zutrittspunkt berechtigten Ausweisnummern mit ihren Zutrittsprofilen (Raum- und Zeitzonen) gespeichert. Dort wird nach Prüfung der erforderlichen Zutrittsrechte der erkannten Ausweisnummer entschieden, ob die Tür freizugeben ist.

4. **Die Schnittstelle c (Schnittstelle zwischen Zutrittskontrollzentrale und übergeordneter Zutrittskontrollzentrale / ZK-Datenbankserver)**

Die ZKZ wiederum ist über Schnittstelle c mit dem Server der Zutrittskontrollanlage (ÜZKZ Übergeordnete Zutrittskontrollzentrale) verbunden. In der ÜZKZ werden alle Nutzer der Zutrittskontrollanlage mit ihren Ausweisnummern und Zutrittsprofilen verwaltet. Ausweisnummern und zugehörige Zutrittsprofile werden in regelmäßigen Zeitabständen und / oder nach Datenänderungen an die ZKZ übertragen.

Angriff auf die Luftschnittstelle

Die Sicherheit der Datenübertragung der Luftschnittstelle hängt direkt von der Integrität der Sicherheitsmechanismen des Transpondertyps ab. Sind diese überwunden, können Ausweise geklont und / oder verfälscht werden. Dies ist jedem möglich, dem die Sicherheitsmechanismen des gehackten Transpondertyps bekannt sind, und Zugriff auf den gehackten Transpondertyp hat. Außer geklonten / verfälschten Ausweisen können programmgesteuerte Geräte verwendet werden, die dem Ausweisleser das Vorhandensein eines gültigen Ausweises vortäuschen. Diese Thematik ist bereits ausführlich in zahlreichen Veröffentlichungen behandelt, so dass in diesem Beitrag nicht weiter darauf eingegangen werden muss.

In jedem Fall ist nach Überwindung der Sicherheitsmechanismen des in der eigenen Anlage genutzten Transpondertyps die Einleitung von Maßnahmen erforderlich. Art und Umfang dieser Maßnahmen ergeben sich aus den Sicherheitsanforderungen des Objekts. Da der sofortige und vollständige Tausch aller Ausweise und Ausweisleser nur in Ausnahmefällen in Frage kommt, sollte unter Abwägung aller bestehenden Risiken eine Migrationsstrategie zu einer sicheren Ausweistechnologie entwickelt und umgesetzt werden.

Der Relay Angriff

Weniger bekannt ist die Möglichkeit eines Relay-Angriffes. Ausweisleser nach ISO 14443 haben eine Reichweite von 10 – 15 cm. Durch Zwischenschaltung eines bidirektionalen Sender-Empfängers mit höheren Feldstärken kann die Reichweite auf einige Meter vergrößert werden. So ist es denkbar, dass bei Nutzung eines solchen Geräts ein mit Abstand vorbeigehender Zutrittsberechtigter mit seinem Ausweis in der Tasche eine Tür freischaltet, wobei der Ausweis „glaubt“, er kommuniziert mit einem systemzugehörigen Ausweisleser, und umgekehrt. Gegen einen solchen Angriff helfen nur technische Maßnahmen innerhalb des Ausweislesers, wie z.B. die Überwachung der Antwortzeiten, die jedoch nicht zu den Standardleistungsmerkmalen aller Fabrikate und Typen von Ausweislesern gehören.

Der Denial of Service Angriff

Bei Verwendung eines aktiven Störsenders wird das elektromagnetische Feld zwischen Ausweisleser und Ausweis so beeinflusst, dass die Kommunikation unterbunden wird. Dadurch wird zwar der Zutritt nicht erlangt, aber hier zeigt sich das Erfordernis einer systematischen Sicherheitsorganisation, in der das Vorgehen bei „unerklärlichen“ Störungen vorgegeben ist. Die denkbar schlechteste Lösung ist es, bei Störung eines Ausweislesers mit unbekannter Ursache die zugehörige Tür auf „Dauerfrei“ zu schalten, in vielen Unternehmen ist das gängige Praxis. Damit hätte der Täter sein Ziel unberechtigt Zutritt zu erlangen, erreicht.

Angriff auf die Schnittstelle a

Obwohl die Datenübertragung an dieser Stelle meist unverschlüsselt erfolgt, ist dies weniger kritisch. In einer aktiv genutzten, installierten ZKA ist diese Schnittstelle kaum zerstörungsfrei zugänglich und nutzbar. Häufig sind die Funktionen der beiden µ-Prozessoren des Ausweislesers auch in einem Chip vereint, und damit ebenfalls nicht zugänglich. Zur Erlangung unberechtigten Zutritts ist diese Schnittstelle unter Praxisbedingungen nicht geeignet.

Angriff auf die Schnittstelle b

Diese Schnittstelle ist außerhalb des Sicherheitsbereichs an den Anschlussklemmen des Ausweislesers zugänglich. Für Innentäter, ggf. auch durch Social Engineering „motivierbar“, ist sie entlang der gesamten Leitungsführung bis in die ZKZ, auch innerhalb des Sicherheitsbereichs, zugänglich.

Insbesondere in älteren Anlagen wurde diese Schnittstelle als unverschlüsselte „Wiegand“- oder Clock-Data-Schnittstelle ausgeführt, die trotz ihrer Defizite nach wie vor angeboten werden. Unverschlüsselte Datenübertragung bedeutet, die übertragenen Daten können nicht nur ausgelesen, sondern auch „verstanden“ und damit nachgebildet oder verfälscht werden.

In modernen Systemen erfolgt die Kommunikation dieser Schnittstelle im Regelfall über einen RS 485 BUS unter Verwendung eines proprietären Protokolls des Herstellers der ZKA, eine verschlüsselte Datenübertragung ist prinzipiell möglich. Nicht alle am Markt angebotene Systeme nutzen die Möglichkeit der verschlüsselten Datenübertragung.

Spoofing und Replay Angriff

Bei unverschlüsselter Datenübertragung ist es möglich, z.B. auf einem Notebook, ohne Beteiligung des Ausweislesers, ein Datenpaket mit einer zutrittsberechtigten Ausweisnummer zu generieren und über die Anschlussleitung des Ausweislesers einzuspielen. Bei einem Replay-Angriff wird eine zuvor abgehörte und aufgezeichnete Datenübertragung zu einem

späteren Zeitpunkt wieder eingespielt. Wird dabei eine Ausweisnummer mit Zutrittsberechtigung verwendet, erkennt die ZKZ keine Unregelmäßigkeit und wird die Tür freigeben. Hiervor schützt auch nicht jede Art von Verschlüsselung. Keinen Schutz gegen Replay Angriffe bietet eine statische Verschlüsselung, bei der für alle Übertragungen derselbe Schlüssel verwendet wird. Das Datenpaket selbst ist zwar unverständlich, aber konstant für jeden einzelnen Ausweis. Es ist zwar nicht verfälschbar, jedoch erfolgreich wiederholbar. Schutz vor Replay Angriffen bietet nur eine starke Verschlüsselung, für die vor jeder Datenübertragungssitzung zwischen Ausweisleser und ZKZ der zu verwendende Schlüssel neu ausgehandelt wird. Wiederholungen einer aufgezeichneten Übertragung werden dadurch von der ZKZ erkannt und nicht akzeptiert.

Denial of Service – Angriff

Bei den meisten Systemen sind mehrere Ausweisleser „in Reihe“ auf den RS 485 BUS geschaltet. Dies trifft auch für die meisten Systeme zu, bei denen für jeden Ausweisleser eigene Anschlussklemmen in der ZKZ vorgesehen sind, die BUS – Topologie wird hier innerhalb der ZKZ gebildet. Bei einem Denial of Service – Angriff wird ein ständiger, beliebiger Datenstrom an beliebiger Stelle in den BUS eingespielt, wodurch für alle BUS-Teilnehmer, d.h. alle auf diesem BUS angeschlossenen Ausweisleser, keine Kommunikation mehr möglich ist. Aus „unerklärlichen“ Gründen funktioniert die Zutrittskontrolle nicht, und wie bereits oben gesagt, ist die Dauerfreischaltung der betroffenen Türen als Reaktion auf die Störung eine schlechte Lösung.

Abhilfe

Sicherheit gegen äußere Angriffe schafft die Verwendung von geteilten Ausweislesern, bei denen nur die Antenne außerhalb, die Elektronik und die Anschlussklemmen des Lesers innerhalb des Sicherheitsbereichs angeordnet sind. Eine vollständige Sabotageüberwachung der Ausweisleser, Verteiler in der Leitungsführung und der ZKZ durch Deckel- und Abreißkontakte kann nur dann Erfolg zeigen, wenn die entsprechenden Meldungen bemerkt, angezeigt und unmittelbar, z.B. durch Intervention, bearbeitet werden. Auch hier sei auf die Erfordernis einer funktionierenden Sicherheitsorganisation verwiesen, durch die Angriffe auf sicherheitstechnische Einrichtungen rechtzeitig bemerkt und abgewiesen werden können.

Angriff auf die Schnittstelle c

In modernen Systemen erfolgt die Vernetzung der ZKZ mit der ÜZKZ über Ethernet unter Verwendung des Netzwerkprotokolls TCP/IP. Steueranweisungen, Meldungen und Inhalte (Nutzdaten) werden mittels herstellerspezifischer, proprietärer Protokolle übertragen. Es würde zu weit führen, im Rahmen dieses Beitrags auf grundsätzliche Fragen der Sicherheit von IP Netzen einzugehen. Sicherheitsrelevante Anwendungen, so auch die Zutrittskon-

trolle, sollten immer über abgeschottete Netzwerksegmente kommunizieren, die als physikalisch getrenntes Netz oder „logisch“ getrennt als Subnetz ausgeführt werden. Prinzipiell können hier alle modernen Verschlüsselungsverfahren eingesetzt werden.

Die Vernetzung älterer Systeme erfolgt über RS 485 BUS, ähnlich wie unter Schnittstelle b beschrieben, jedoch ist das zu übertragende Datenvolumen deutlich größer als auf Schnittstelle b. Da Ver- und Entschlüsselung sowohl Rechenkapazität wie Zeit erfordern und das zu übertragende Datenvolumen erhöht, erfolgt hier nur selten eine verschlüsselte Übertragung.

Unabhängig von der BUS-/Netztopologie sollte der physische Zugang zu den Knoten beschränkt und überwacht sein, um Denial of Service Angriffe (siehe oben) auszuschließen oder zumindest rechtzeitig zu erkennen. Erfolgt die Übertragung der Nutzdaten unverschlüsselt, ist dies umso wichtiger. Jeder, der Zugang zu dem Netz erlangt und das unverschlüsselte proprietäre Protokoll ausspäht, kann Daten auf der ZKZ verändern, z.B. sich selbst Zutrittsrechte zuweisen, die vom Sicherheitsverantwortlichen nicht vorgesehen sind. Einer Veränderung der Daten der ÜZKZ über das Netz stehen zusätzlich noch die Sicherheitsmechanismen der verwendeten Datenbank entgegen, sofern diese entsprechend eingerichtet sind.

Fazit

Die beschriebenen Angriffsmethoden auf die Datenintegrität einer Zutrittskontrollanlage erfordern erheblichen Aufwand für die Vorbereitung, technische Kenntnisse und Zugangsmöglichkeit zu den einzelnen Funktionseinheiten. Ob zu erwarten ist, dass potenzielle Täter diesen Aufwand tatsächlich auf sich nehmen, sollte – unter besonderer Bewertung der Sicherungsmaßnahmen an den Zugangsstellen und der begleitenden organisatorischen Maßnahmen - in einer Risikobetrachtung bewertet werden.

Ob und welche Sicherheitsmaßnahmen gegen Datenmanipulation bzw. missbräuchliche Datenzugriffe in einem Zutrittskontrollsystem implementiert sind, geht aus den Herstellerangaben hervor. Entscheidend ist die gesamtheitliche Betrachtung der Risiken, bei der Angriffe auf die Datenwege zum Zweck der Datenmanipulation nur eine Teilmenge darstellen.

Abschließend noch eine Anmerkung zur Sicherheit der Luftschnittstelle. Auch wenn die aktuellen Transpondersysteme der führenden Hersteller zurzeit sicher sind, ist es nur eine Frage der Zeit, bis auch diese überwunden werden. Auch hier kann vorausschauende Konzeption und Planung eine eventuell später erforderliche weiche Migration auf einen neuen Transpondertyp erheblich kostengünstiger gestalten.