Selbst Profis beißen sich die virtuellen Zähne aus

Sicherer Router wird zum Zerberus

Für Infrastrukturen von sicherheitstechnischen Anwendungen – und dazu gehören insbesondere auch die Netze zur Alarmübertragung von Gefahrenmeldungen und Notrufsystemen – ist es unabdingbar, dass Sicherheitsvorkehrungen auf alle denkbaren Szenarien vorbereitet sind , um nicht ausgespäht oder sabotiert zu werden. Dazu ist die Entwicklung wirkungsvoller Schutzmaßnahmen notwendig.

Ein im zu sichernden Objekt eingesetzter Sicherheitsrouter muss die aktuellen und absehbaren Anforderungen an Übertragungstechnik, Fernadministration und Remoteanwendungen inkl. Überwachung der Anschlüsse und nachgeschalteten Gewerke wie Brandmelde-, Einbruchmelde-, oder Sprachnotrufsystemen wie zum Beispiel den Aufzugsnotruf abdecken.

Anforderungsprofil

Um diesen Anforderungen bestmöglich Rechnung zu tragen, hat die TAS Sicherheits- und Kommunikationstechnik die folgenden Punkte bei der Entwicklung des Sicherheitsrouters SIRO-Port berücksichtigt.

- Bewusster Verzicht auf den Einsatz von Standard-Betriebssystemen wie z.B. Linux, deren Grundsatzproblematik in Bezug auf Sicherheitsaspekte ausrechend diskutiert ist.
- Einsatz eines gehärteten Betriebssystems nach den strengen Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik. Alle NSL- sowie Remote TCP-IP Verbindungen sind mittels AES oder (im BSI-Anwendungsbereich) Chiasmus verschlüsselt.
- Die gesicherte Authentifizierung aller externen Verbindungen inkl. der Fernservicetunnel erfolgt durch Preshared Keys oder vorinstallierte Zertifikate.
- Das Risiko von Verbindungsunterbrechungen durch Denial-of-Service Attacken wurde durch mehrfach redundante Verbindungen über IP/ DSL und Funknetze minimiert. Als Übertragungswege können TCP-IP, GSM/GPRS/UMTS und LTE-Funknetzte kombiniert werden. Bei einer Attacke auf einem einzelnen Übertragungsweg wird unmittelbar der konfigurierte Ersatzweg über eine unabhängige Trasse genutzt.
- Der Anschluss des SIRO-Port kann durch das integrierte DSL-Modem direkt am von Netzstrom unabhängigen DSL-Anschluss erfolgen.
- Der Router ist vollständig notstromversorgt, sodass bei Ausfall der Stromversorgung im Objekt, die Konnektivität der Übertragungswege nicht gefährdet ist. Sowohl Funknetze als auch das integrierte DSL-Modem müssen vollständig gemäß hohen Anforderungen der nationalen und europäischen Richtlinien für Einbruch- Brand- und Aufzugsnotrufrichtlinien notstromversorgt sein.
- Die bis zu 4 LAN-Buchsen und diverse herkömmliche Systemschnittstellen ermöglichen einen flexiblen Einsatz Im Sicherheitsumfeld. Die LAN-Ports sind vollständig voneinander getrennt und erlauben eine Kommunikation untereinander lediglich über die Schicht 7 (Applikationsgateway) des OSI-Referenzmodells.

Test bestanden

Für die Bestätigung des gewünschten Sicherheitsniveaus wurde die Tübinger SySS GmbH, das in Deutschland auf dem Gebiet von Penetrationstests führende Unternehmen, beauftragt.

Mehrere Tage prüften die Experten den SIRO-Port auf gängige sowie exotische Schwächen und Sicherheitslücken: Die grundsätzliche Systemarchitektur, die IP-Schnittstellen, die Funknetzzugänge und die DSL-Schnittstelle wurden auf logikbasierte Angriffe, bekannte Linux- und Windows-Angriffe, Man-in-the-Middle-Angriffe, GSM- Rouge Network Tests und Breitband-Rauschunterdrückungsangriffe getestet.

Im Rahmen der Tests konnte die Verfügbarkeit des SIRO-Port nicht unterbrochen werden. Das System ist nicht gegen bekannte Standardangriffe auf Linux und Windows verwundbar. Nach umfangreichen Prüfungen konnte dem SIRO-Port ein sehr gutes Sicherheitsniveau bescheinigt werden.

WWW.TAS.DE