

Was unterscheidet den Fernzugriff bei einem INTEGRA-System von anderen Systemen?

Die Vernetzung von Systemen und der Zugriff von außen per Smartphone oder Rechner birgt immer das Risiko auch von unberechtigtem Zugriff. Daher sind Systeme mit Fernzugriffsmöglichkeiten über mehr oder weniger effektive Sicherheitsmechanismen geschützt. Gerade bei Alarmsystemen ist das Sicherheitsbedürfnis und die Gefahr einer manipulativen Nutzung besonders hoch. Die INTEGRA -Systeme vereinen komfortable Bedienung mit höchster Sicherheit.

- Wahlweise Direktzugriff oder verwalteter Zugriff

Grundsätzlich können Sie zwischen zwei Zugriffsarten wählen. Dem **direkten** oder **gemanagten** Zugriff. Bei dem **direkten** Zugriff wird ein wählbarer Port genutzt, über den die verschlüsselte Verbindung zustandekommt. Dieser Weg wird häufig bei Netzwerken im gewerblichen Bereich genutzt, da dies den Vorteil der einfacheren Administrierbarkeit bietet. Hierzu wird eine feste IP oder DYNDNS-Dienst am Router benötigt. Als Nachteil ist die fehlende Möglichkeit der Push-Alarmierung anzumerken. Dies ist technisch bei dieser Art der Verbindung nicht möglich.

Beim **gemanagten** Zugriff wird ein Verbindungsserver verwendet. Hier unterscheidet sich die Satel-Lösung deutlich von vielen anderen Systemen auf dem Markt. Die Satel-Server managen lediglich die Verbindungsaufnahme von Endgeräten wie Tablets oder Smartphones mit dem Alarmsystem indem sie die direkte Verbindung der Strecke ermöglichen. Die Verbindung selbst läuft nicht wie bei vielen anderen Herstellern über diese Server, es können also keine Daten abgefangen oder missbräuchlich genutzt werden. Die hierbei genutzte Technik kann man als „Security-P2P-Verbindung“ bezeichnen.

- Dreifache Codesicherung

Gleich welchen der beiden Verbindungstypen Sie wählen, es werden in jedem Fall drei Kennwörter für einen Zugriff benötigt. In der Regel richtet Ihnen der Errichter zwei davon bereits fertig ein, das letzte Kennwort ist das Benutzerkennwort. Die Nutzung ist also sehr komfortabel. Ein unberechtigter Zugriff ist aber mit diesem Kennwort alleine nicht möglich, da die beiden anderen Authentifizierungscodes fehlen.

- Protokollierung, Rechtevergabe, Attackierungsschutz

Jeder Zugriff wird protokolliert und kann an Wachdienste übermittelt werden, oder Sie können sich per App über eine Einwahl informieren lassen. Zusätzlich kann jeder Benutzer in seinen Zugriffsrechten sowohl zeitlich als auch funktionell verwaltet werden. So hat die Putzfrau beispielsweise über die App nur das Recht Freitags von 13:00 – 18:00 Uhr die Türen zu benutzen und wieder scharf zu schalten.

Bei dem Versuch Codes auszuprobieren oder bei sogenannten „Brute-Force-Attacken“ wird automatisch alarmiert und benachrichtigt, zudem wird dieser Kommunikationsweg gesperrt.

- Starke Verschlüsselung

Egal welcher Zugriffsweg von außen genutzt wird, die Daten werden nach einem aufwändigen Prinzip mehrfach verschlüsselt. Basis ist die 192-Bit AES-Verschlüsselung, welche speziell für den Sicherheitsbereich angepasst wird.

- Individuelle Freigabe selbst des Servicetechnikers

Sie als Besitzer des gesicherten Objektes alleine bestimmen darüber, wer welche Zugriffsrechte auf Ihr System hat. Bei der Übergabe wird auch dem Anlagenbauer und Servicetechniker jedes Zugriffsrecht und Bedienmöglichkeit entzogen, im Wartungsfall oder auf Ihren Wunsch hin erhält er durch Ihre Freigabe ein Zeitfenster von 1-99 Stunden, in dem er an der Anlage arbeiten kann.

Schlussfolgerung:

Die oben angeführten Punkte sind nur die wichtigsten, die das INTEGRA-System zu dem machen, was es vor Allem ist: Ein SICHERHEITS-System. Viele Smarthome- und andere Systeme verfügen oft nur über eines oder zwei dieser Merkmale, was sie häufig angreifbar macht. Zu detaillierten Fragen zu diesen Punkten steht Ihnen Ihr Errichter oder ASL-Ademco gerne zur Verfügung.

Bedenken Sie aber immer: Die Technik ist nur so gut, wie man sie lässt. Regelmäßige Wartung ist ebenso wichtig wie die Verwendung „guter“ Kennwörter und der gewissenhafte Umgang mit dem Sicherheitssystem.