Net2–Empfehlungen zur Netzwerksicherheit

Damit Ihr Paxton Net2 System vor Ort so sicher wie möglich ist, empfiehlt Paxton dem Errichter (oder der IT-Abteilung), in jeder der 7 Schichten des **OSI** - Modells (Network *Open Systems Interconnection*) bewährte Praktiken der IT-Sicherheitsmechanismen zu implementieren.

Starke Sicherheit auf physikalischer Ebene einrichten

- Implementieren Sie starke physische Sicherheit für Geschäftsräume beispielsweise durch Verwendung biometrischer Identifikatoren, Transponder-basierter Authentifizierung usw., damit ein Außenstehender gestoppt werden kann, bevor sie/er ein Gebäude mit einem Unternehmensnetzwerk betreten kann.

Implementierung von Kontrollstandards für Netzwerkzugriffe wie der IEEE 802.1X Authentifizierung zur Sicherung von LAN und WLAN

- Dieser Standard erzwingt die Sicherheitsrichtlinie, indem nur konformen Geräten Zugriff auf Netzwerkressourcen gewährt wird, wenn diese Geräte an einen physikalischen LAN-Port angeschlossen sind oder mit einer WLAN-SSID verbunden sind. Dieser Standard behandelt nicht nur die Authentifizierungs- und Autorisierungsfunktionen, sondern kontrolliert auch die Daten, auf die bestimmte Benutzer zugreifen dürfen, indem Sie Benutzer, Ihre Geräte und ihre Netzwerkfunktionen erkennt. IEEE 802.1 x wird nativ von allen Windows-, Mac-und Linux-Rechnern unterstützt.

Verwendung von Firewalls der nächsten Generation zur Verhinderung von externen und internen Angriffen

- Implementieren Sie eine Firewall der nächsten Generation, die neben der herkömmlichen paketbasierten ‚Stateful Inspection', auch Application Layer Inspection, Intrusion Prevention und Erkennung, die Sicherung von Web-Traffic, etc. ausführt.
- Dehnen Sie außerdem alle potenziell unsicheren internen Layer 2 VLANs an die Firewall aus und schützen Sie den Zugriff von diesen VLANs zu anderen vertrauenswürdigen/sicheren VLANs, indem Sie konfigurierbare Sicherheitsrichtlinien verwenden.

Richten Sie VLANs (Virtual Local Area Networks) ein, für Netzwerksicherheit und Trennung

- VLANs gestatten es uns, Datenpakete von mehreren Netzwerken (wie Abteilungsnetzwerken, kritischen Servernetzen usw.) getrennt zu halten. Die Netzwerk-Segmentierung mittels VLAN schafft eine Ansammlung isolierter Netzwerke innerhalb des Unternehmensnetzwerks und verringert die Angriffsfläche, denn selbst wenn sich ein Außenseiter Zugriff auf ein kleines logisches Netzwerk verschafft, kann er Geräte in anderen VLANs nicht einsehen oder direkt angreifen.

Implementieren Sie starke Passwörter für die Authentifizierung von Net2 Server-Anwendungen und zugehörigen Datenbanken