Hardware und Software Sicherheitsmerkmale

IP-Video-, Digital Signage- und Guest Experience-Lösungen

Bei Exterity bemühen wir uns sicherzustellen, dass unsere End-to-End-IPTV-Lösungen sicher, robust und zuverlässig sind. Dieser kurze Leitfaden beschreibt die Sicherheitsmerkmale für unsere Hardware und Software und erläutert ihre Bedeutung. Um mehr über Inhaltssicherheit zu erfahren, lesen Sie unseren Leitfaden zur Inhaltssicherheit.

Unser Angebot	Warum es wichtig ist
Wir sind ISO 9001 zertifiziert	Unsere Workflows für den technischen Entwurf und die Fertigung sind geprüft und garantieren Qualitätssicherung auf höchstem Niveau. Wir fertigen unsere End-to-End-Lösungen in Großbritannien an und haben so die vollständige Kontrolle über unseren Produktionsprozess.
Sichere Prozessoren auf allen Embedded-Plattformen *(AvediaPlayer Media Player, AvediaStream Encoder und Gateways)*	Gewährleistet physische Sicherheit und Robustheit und bedeutet, dass diese Plattformen ausschließlich Exterity-Software abspielen, was wiederum die Installation bösartiger Codes verhindert. Es bedeutet außerdem, dass wir die Inhaltsschutzanforderungen unserer Broadcaster erfüllen und sicher Premium-Kanäle über ein IP-Netzwerk übertragen können. Zusätzlich werden im Clear Web verteilte Daten nicht über offene Standardschnittstellen übermittelt, was den leichten Zugriff und Änderungen von Dritten verhindert.
Ausschließlich von Exterity unterzeichnete Upgrades können auf unseren Produkten installiert werden *(AvediaPlayer Media Player, AvediaStream Encoder und Gateways)*	Garantiert, dass ausschließlich verifizierte und vertrauenswürdige Firmware verwendet werden kann, um Ihre Exterity-Produkte zu aktualisieren und bedeutet, dass keine bösartigen Codes auf Ihrer Exterity-Hardware installiert werden können.

AvediaServer

AvediaPlayer
Media Player

AvediaStream
Gateway

What we offer	Why it's important
Wir verwenden Sicherheitsschrauben an unseren AvediaPlayer Media Playern	Da sich Media Player oft in öffentlichen Orten befinden, benutzen wir besondere Sicherheitsschrauben beim Anbau. Dies bedeutet, dass spezielle Werkzeuge benötigt werden, um unsere Produkte zu befestigen oder zu entfernen. Normale Werkzeuge funktionieren nicht. Somit sind die Geräte gegen unbefugten Zugriff geschützt.
HTTPS-basierte Benutzeroberfläche	Unsere Webadmin-Oberflächen sind mit HTTPS abgesichert, damit Kommunikation zwischen dem Administratorrechner und dem Exterity-Gerät verschlüsselt ist und Man-in-the-Middle-Angriffe verhindert werden können.
HTTP-Proxy-Unterstützung	Bedeutet, dass nur bestimmte Geräte auf das Internet zugreifen können und gewährleistet die Sicherheit des internen Netzwerks.
802.1x Protokoll *(AvediaPlayer Media Player der Serie 93)*	Schützt Netzwerke vor unbefugten Zugriffen, weil nur zertifizierte Geräte über das IP-Netzwerk funktionieren.
SSH-Protokoll	Bietet sichere Authentifizierung und schützt Kommunikation mit starken Verschlüsselungsprotokollen. Zugriff über ungesicherte Kommandozeilen wird nicht unterstützt.
Netzwerk-Firewall	Wird verwendet, um Administratorenzugriff und/oder Zugriffskontrolle auf die Ports der Exterity-Geräte zu verwalten.
Unterstützung für Single Sign On und Active Directory *(AvediaServer, AvediaStream Origin Server, Transcoder und e5640 Encoder)*	Erleichtert Ihren Benutzern den Zugriff auf das System und gibt Ihnen gleichzeitig die Gewissheit, dass Ihre Sicherheitsrichtlinien mit Hilfe von Active Directory Integration eingehalten werden. Single Sign On ermöglicht die Einhaltung dieser Richtlinien und gewährleistet Zugriff auf den AvediaServer mit verringertem Risiko, dass Passwörter verloren gehen, vergessen werden oder zu schwach sind.
Nutzer-basierte API-Zugangskontrolle *(AvediaServer, AvediaStream Origin Server, Transcoder und e5640 Encoder)*	Ermöglicht Ihnen zu entscheiden und zu kontrollieren welche Nutzer oder Gruppen von Nutzern auf spezifische Fähigkeiten auf dem Server zugreifen können, wie zum Beispiel Zugriff auf Systemeinstellungen, Erstellen und Verwalten von Inhalten, u.v.m..
Passwortschutz	Alle unsere Geräte sind durch ein Passwort geschützt.
Penetrationsprüfung	Nach jeder Neuveröffentlichung von Software simulieren wir einen Cyber-Angriff, um Schwachstellen zu finden bevor es die Angreifer tun.

Exterity Europe
t: +33 (0)3 52 84 01 23 w : www.exterity.com e : sales@exterity.com