MPC-2610

Sicherheitsmaßnahmen

In dieser Hilfe werden die Sicherheitsmaßnahmen für die Dateiübertragung und das Streaming mit dem Gerät beschrieben.

MPC-2610
Sicherheitsmaßnahmen

Sicherheitsmaßnahmen

Unter diesem Thema werden Vorsichtsmaßnahmen für die Verbindung des Geräts mit einem Netzwerk beschrieben.

- Der Kommunikationsinhalt kann von unautorisierten Dritten in der Nähe des Signals abgefangen werden, ohne dass Sie es merken. Wenn Sie die WLAN-Kommunikation nutzen, implementieren Sie geeignete Sicherheitsmaßnahmen, um den Kommunikationsinhalt zu schützen.
- Falls Sie die WLAN-Einstellung [Security] auf [None] gesetzt haben und eine Verbindung zu einem Zugangspunkt herstellen, wird die drahtlose Kommunikation zwischen Kamera und Zugangspunkt nicht verschlüsselt und kann von Dritten innerhalb der Signalreichweite abgehört werden. Verwenden Sie zur Erhöhung der Sicherheit die Verschlüsselungsprotokolle WPA2 oder WPA3.
- SONY KANN KEINE HAFTUNG FÜR SCHÄDEN JEDER ART DURCH UNTERLASSENE GEEIGNETE SICHERHEITSMASSNAHMEN AN ÜBERTRAGUNGSGERÄTEN, DURCH UNVERMEIDBARE DATENPREISGABE AUFGRUND DER ÜBERTRAGUNGSSPEZIFIKATIONEN ODER DURCH SICHERHEITSPROBLEME JEGLICHER ART ÜBERNEHMEN.
- Je nach Betriebsumgebung können unbefugte Dritte im Netzwerk unter Umständen auf dieses Gerät zugreifen. Achten Sie beim Verbinden des Geräts mit dem Netzwerk darauf, dass das Netzwerk gut abgesichert ist.
- Schließen Sie dieses Produkt beim Verbinden mit einem Netzwerk über ein System an, das eine Schutzfunktion bietet, wie etwa ein Router oder eine Firewall. Andernfalls können Sicherheitsprobleme auftreten.

TP1002221137

MPC-2610
Sicherheitsmaßnahmen

Vorsichtsmaßnahmen für die Internet-Verbindung

Unter diesem Thema werden Vorsichtsmaßnahmen für die Verbindung des Geräts mit dem Internet beschrieben.

- Das Gerät kann sich nicht per WLAN mit Zugangspunkten verbinden, die lediglich die mit Schwachstellen behafteten Verschlüsselungsmethoden WEP oder WPA verwenden.
- Das Gerät ist kein Netzwerkgerät (z. B. Router oder Switch/Hub). Es wird dringend empfohlen, dass Sie das Gerät mit einem Netzwerk verbinden, bei dem Sie die Netzwerkeinstellungen geeignet konfigurieren und verwalten können, um sich vor netzwerkbasierten Angriffen wie DoS-Angriffen (Denial of Service) zu schützen.
- Verbinden Sie das Gerät mit dem Netzwerk über einen Router, der geeignet konfiguriert ist und verwaltet wird, oder verbinden Sie das Gerät mit einem LAN-Anschluss, der über die gleichen Eigenschaften verfügt. Wenn Verbindungen ohne derartigen Schutz hergestellt werden (z. B. bei der Verwendung von kostenfreiem WLAN), können Sicherheitsprobleme auftreten. Bei ordnungsgemäßer Konfiguration bieten Router ausreichenden Schutz vor DoS-Angriffen oder Funktionsverlust bei Geräten im Netzwerk. Falls Sie ungewöhnliche Aktivitäten bemerken, trennen Sie die Kamera umgehend vom Netzwerk.

TP1002221138

MPC-2610
Sicherheitsmaßnahmen

Vorsichtsmaßnahmen bezüglich der Netzwerkfunktion

Unter diesem Thema werden Vorsichtsmaßnahmen bezüglich der Netzwerkfunktion des Geräts beschrieben.

- Falls unbefugter Zugriff erkannt wird, ist die Kamera ggf. nicht mehr zu Kommunikation in der Lage. Stellen Sie in diesem Fall die Verbindung von Anfang an wieder her.
- Die Authentifizierungsdaten zum Verbinden mit dem Gerät werden angezeigt, wenn Sie [Network] – [Network Setup] – [Show Authentication] verwenden. Achten Sie darauf, dass der Bildschirm bzw. das QR-Codebild von niemandem betrachtet oder kopiert werden kann.
- Ein Benutzername und Kennwort müssen zum Zeitpunkt des Kaufs eingestellt werden. Achten Sie beim Festlegen Ihres Benutzernamens und des Passworts darauf, dass die Einstellungen nicht für andere Personen sichtbar sind. Legen Sie den Benutzernamen und das Kennwort wie folgt fest.

[User Name]	– Legen Sie einen Benutzernamen fest, der aus 1 bis 16 Zeichen besteht. – Werkseitig ist hierfür „admin“ eingestellt. – Die folgenden Zeichen sind gültig. Buchstaben (groß und klein), Ziffern, Sonderzeichen (! % + , - . = _)
[Password]	– Legen Sie ein Kennwort fest, das aus 8 bis 16 Zeichen besteht, darunter mindestens einen Buchstaben und mindestens eine Ziffer. – Die folgenden Zeichen sind gültig. Buchstaben (groß und klein), Ziffern, Sonderzeichen (! % + , - . = _)

TP1002221139

MPC-2610
Sicherheitsmaßnahmen

Vorsichtsmaßnahmen bezüglich WLAN

Unter diesem Thema werden Vorsichtsmaßnahmen für die Verbindung des Geräts per WLAN beschrieben.

- In der Hilfe zu diesem Gerät werden WLAN-Zugangspunkte und WLAN-Router, die LAN-Verbindungen weiterleiten, als „Zugangspunkte“ bezeichnet.
- [Security] (Verschlüsselungsmethode) kann auf [None], [WPA2] oder [WPA3] eingestellt werden. Vom Aspekt der Sicherheit her wird [WPA2] oder [WPA3] empfohlen. Wenn [None] ausgewählt ist, wird vor dem Herstellen der Verbindung eine Meldung angezeigt. Um die WLAN-Verbindung abzusichern, wird dringend empfohlen, nur Verbindungen zu Zugangspunkten mit WPA2- oder WPA3-Verschlüsselung herzustellen.
- Standardmäßig ist beim Registrieren eines WLAN-Zugangspunkts unter Verwendung von [Manual Register] die WPA2-Verschlüsselungsmethode ausgewählt.
- Wenn Sie eine Verbindung zu einem Zugangspunkt ohne jegliche Sicherheitseinstellungen herstellen, können Sie Hackerangriffen, böswilligen Zugriffen Dritter oder Angriffen aufgrund von Schwachstellen ausgesetzt sein. Sofern nicht unvermeidlich, wird eine Verbindung ohne jegliche Sicherheitseinstellung nicht empfohlen.
- Es ist sehr wichtig, die Sicherheit eines WLAN zu konfigurieren. Sony übernimmt keine Haftung für Schäden, die aus Unterlassung von Sicherheitsmaßnahmen resultieren oder falls ein Sicherheitsproblem durch unvermeidliche Umstände bei der Verwendung eines WLAN auftritt.

TP1002221140

MPC-2610
Sicherheitsmaßnahmen

Vorsichtsmaßnahmen bezüglich USB-Tethering

Unter diesem Thema werden Vorsichtsmaßnahmen für die Verbindung des Geräts per USB-Tethering beschrieben.

- Verwenden Sie nur vertrauenswürdige Smartphone-Geräte zum Tethering. Aus Sicherheitsgründen wird vom Anschließen von Geräten unbekannter Herkunft abgeraten.

TP1002221141

Hinweise zur FTPES (FTPS)-Funktion

Die FTPS-Funktion unterstützt verschiedene Verschlüsselungsalgorithmen, um sichere Dateiübertragung zu gewährleisten. Für die Kompatibilität mit einer breiten Palette von Servern werden mehrere Verschlüsselungsalgorithmen unterstützt, von denen einige nicht mit dem aktuellen Stand der Sicherheit übereinstimmen.

Von der FTPS-Funktion unterstützte Verschlüsselungsalgorithmen

Die folgenden Verschlüsselungsalgorithmen werden unterstützt.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Empfohlene Verschlüsselungsalgorithmen

Basierend auf den NIST-Empfehlungen (NIST SP 800-57 Teil 1 Revision 5) und verwandten Sicherheitsstandards werden die folgenden Verschlüsselungsalgorithmen empfohlen.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Hinweise zu veralteten Algorithmen

Die FTPS-Funktion unterstützt aus Kompatibilitätsgründen auch die folgenden Algorithmen, diese sind jedoch gemäß den NIST-Empfehlungen (NIST SP 800-57 Teil 1 Revision 5) und verwandten Sicherheitsstandards veraltet und werden ggf. in einer zukünftigen Version entfernt.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Hinweise zur Verbindungskompatibilität

Die FTPS-Funktion ist mit einem ausgewogenen Verhältnis zwischen Sicherheit und Kompatibilität konzipiert. Gegenwärtig werden aus den nachfolgend aufgeführten Gründen veraltete Algorithmen unterstützt; diese werden jedoch ggf. in einer zukünftigen Version entfernt, um die Sicherheit zu verbessern.

- Selbstständige Fotografen und Videofilmer müssen Verbindungen zu Servern bei verschiedenen Kunden herstellen.
- Die Kompatibilität mit älteren Systemen und veralteten Servern muss aufrechterhalten werden.
- Nicht alle Nutzer sind darauf vorbereitet, zu einer sichereren Umgebung zu wechseln, da sich die Änderung der Einstellungen für den Verschlüsselungsalgorithmus auf der Serverseite kompliziert gestalten kann.
- Die FTPS-Einstellungen werden häufig mit anderen sicheren Diensten geteilt. Jegliche Änderungen müssen wohlüberlegt erfolgen, da sie sich möglicherweise auf andere Dienste auf dem Server auswirken.
- Um die Interoperabilität in verschiedenen Umgebungen sicherzustellen, muss eine breite Palette von Verschlüsselungsalgorithmen unterstützt werden.

Der während einer FTPS-Verbindung verwendete Verschlüsselungsalgorithmus wird durch automatische Aushandlung mit dem Zielserver bestimmt und hängt daher von den Servereinstellungen ab. Im Bewusstsein der Sicherheitsrisiken erhält derzeit die Kompatibilität Vorrang, um auf die verschiedenen Anforderungen der Nutzer einzugehen.

Sicherheitsrisiken

Die Verwendung veralteter Algorithmen wie CBC/DHE/RSA/SHA-1 erhöht das Risiko, dass verschlüsselte Daten von einem Angreifer entschlüsselt oder manipuliert werden und somit Daten bei einer Übertragung offengelegt werden können.

Empfehlungen für eine sichere Verbindung

Bevor Sie die FTPS-Funktion verwenden, prüfen Sie, ob der Zielserver der Verbindung den empfohlenen Verschlüsselungsalgorithmus unterstützt. Aktivieren Sie nur die empfohlenen Verschlüsselungsalgorithmen auf der Serverseite und deaktivieren Sie die veralteten.

Hochladen mithilfe einer sicheren FTP-Übertragung

Sie können Dateien verschlüsselt mithilfe von FTPS im Explicit-Modus (FTPES) für die Verbindung mit dem Ziel-Dateiserver hochladen.
Um eine sichere FTP-Übertragung zu erzielen, setzen Sie [Using Secure Protocol] in den Einstellungen für den Zielserver der Dateiübertragung auf [On] und importieren Sie ein Zertifikat.

Referenzen

- Recommendation for Key Management, Special Publication 800-57 Part 1 Revision 5, NIST, 2020.
- Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication 800-131A Revision 2, NIST, 2019.
- Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, NIST, 2005 (einschließlich Aktualisierungen vom 06.10.2016).

Zertifikat

Speichern Sie das von der FTPES (FTPS)-Funktion verwendete Zertifikat im Stammverzeichnis einer Speicherkarte. Legen Sie den Dateinamen wie folgt fest.
certification.pem (PEM-Format)
Die maximale Größe des Zertifikats, die geladen werden kann, beträgt 1 MB pro Zertifikat.

TP1002221142