Empfehlungen für die Cyber Security beim Alarmbildempfang

Eine Einführung in das Thema finden Sie hier: www.ebues.de/AlarmempfangFTP.pdf

Für die **Cyber-Sicherheit des FTP-Servers** sind u.a. folgende Maßnahmen möglich:

- FTP-Server **mandantenfähig** konfigurieren: Jedem Kunden wird auf dem FTP-Server ein eigener Account mit individuellem starken Passwort zugewiesen, mit dem er Daten nur in sein eigenes Unterverzeichnis auf dem FTP-Server schreiben kann. So werden die Daten aller Kunden klar voneinander getrennt (Mandantenfähigkeit).
- Als einfache Sicherheitsmaßnahme kann die **Firewall** so eingerichtet werden, dass FTP-Verbindungen nur von bestimmten IP-Adressen angenommen werden; alle Verbindungsanforderungen von anderen IP-Adressen werden von der Firewall sofort abgewiesen. Dies setzt voraus, dass alle Alarmsender eine feste IP-Adresse haben.
- Verbindungen zwischen den Kunden und der Leitstelle können mittels **VPN** getunnelt werden, damit kein öffentlicher Zugriff auf die übertragenen Daten möglich ist.
- Der FTP-Server kann in einer **DMZ** (Demilitarisierten Zone) mit zweistufiger Firewall betrieben werden: https://de.wikipedia.org/wiki/Demilitarized_Zone.
- Der Transport der Dateien von der DMZ ins durch die **2. Firewall** geschützte LAN erfolgt durch einen eigenen Hintergrund-Dienst, der auf einem Server im LAN läuft, nur zugelassene Dateiarten (jpg, txt) ggf. nach weiterer Prüfung des Dateiinhalts über einen eigens dafür freigegebenen Port transportiert und alles andere löscht. Dazu können Sie beispielsweise www.ebues.de/FileMover.pdf nutzen.
- Alle Dateien werden sofort nach ihrer Übertragung von der DMZ ins LAN auf dem FTP-Server **automatisch gelöscht**. Somit sind diese Dateien auch bei einem erfolgreichen Angriff auf die DMZ vor unberechtigten Zugriffen geschützt.
- Auf dem FTP-Server **Virenscanner mit Echtzeitschutz** betreiben, der verhindert, dass schädliche Dateien überhaupt auf die Festplatte geschrieben werden können.
- Betriebssysteme, Virenscanner und FTP-Server-Software (z.B. FileZilla) durch regelmäßige **Updates** immer auf dem neuesten Sicherheitsstand halten.
- Sichern Sie regelmäßig die Einstellungen des FileZilla-Servers, indem Sie ein **Backup** des Ordners `C:\ProgramData\filezilla-server` erstellen.
- Alle Softwarekomponenten laufen in **virtuellen Maschinen** und können somit nach eventuellen Angriffen oder anderen Störungen aus einem geprüften VM-Image heraus schnell wiederhergestellt und auf einen wohldefinierten sicheren Stand gebracht werden.
- Die gesamte EBÜS-Anlage kann in einem **separaten Netz** betrieben werden, um Rückwirkungen auf andere Netze und geschäftskritische Prozesse auszuschließen. Die Netzwerktrennung kann entweder physikalisch oder durch Konfiguration eines VLANs erfolgen: https://de.wikipedia.org/wiki/Virtual_Local_Area_Network
- Der von uns verwendete FTP-Server FileZilla unterstützt auch **SSL/TLS** (FTPS): → https://secorio.com/knowledge-base/installation-des-ssl-zertifikats-in-filezilla/
- Damit dies für eine sichere Alarmübertragung genutzt werden kann, muss es auch auf Seiten der Bildquelle unterstützt werden. FileZilla setzt zudem eine „TLS session resumption“ voraus, was ebenfalls von der Bildquelle unterstützt werden muss, da sonst bei TLS die Kommunikation abgebrochen wird.

Lassen Sie uns bitte gern gemeinsam beraten, welche Kombination von Maßnahmen für Ihre gegebene Konstellation am besten passt. Dies hängt u.a. von den Sicherheits-Policies ab, die in Ihrem Hause und mit Ihren Kunden vereinbart wurden.

FTP-Server wie FileZilla (→ https://filezilla-project.org/) werden seit vielen Jahren auch von großen Unternehmen für vielfältige Zwecke betrieben und haben sich zur herstellerneutralen standardisierten Übergabe von Daten aller Art sehr gut bewährt.

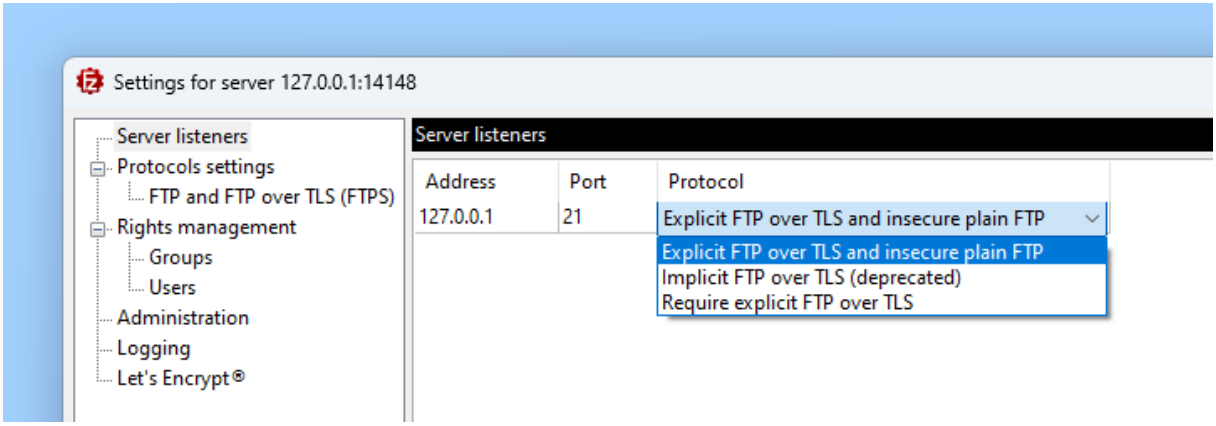
Accellence Technologies GmbH • Garbsener Landstr. 10 • D-30419 Hannover
Tel. 0511 - 277.2400 • Fax 0511 - 277.2499 • E-Mail: info@accellence.de • Website: www.accellence.de

Von Seiten EBÜS und des von uns empfohlenen FileZilla-FTP-Servers werden im Sinne der Cyber-Sicherheit auch **Verschlüsselung** und **Zertifikate** unterstützt. Falls jedoch Daten per FTP auch von solchen Geräten empfangen werden sollen, die kein TLS unterstützen, muss dies bei neueren FileZilla-Versionen explizit freigegeben werden.

Wählen Sie dazu in der Administrations-Oberfläche des FileZilla-Servers im Menü

Server → Configure… → Server listeners

mit der dort in der Spalte „Protocol“ angebotenen Combo-Box aus, ob auf dem gewählten Port (z.B. 21) auch insecure plain FTP zugelassen werden soll:



Eine detailliertere Beschreibung wie das Netzwerk konfiguriert werden sollte, finden sie in der FileZilla Dokumentation unter https://wiki.filezilla-project.org/Network_Configuration.
Es empfiehlt sich das komplette Dokument einmal durchzulesen, wenn Sie ein neues Netzwerk aufsetzen.

Neben der Datensicherheit erfordert auch die **Verfügbarkeit** des Alarmempfangs besondere Aufmerksamkeit, damit sichergestellt wird, dass Alarme jederzeit in der Leitstelle ankommen:

Die Bereitschaft der Leitstelle zum Empfang von Alarmdaten per FTP sollte regelmäßig mit unserem **TestAlarm-Generator** überwacht werden → www.ebues.de/TestAlarm.pdf

Zusätzlich sollten alle Bildquellen, die dies unterstützen, regelmäßig **Routinerufe** an die Leitstelle senden, damit auch individuelle Probleme beim Versenden der Alarmdaten rechtzeitig erkannt und abgestellt werden.
Nutzen Sie dafür die Routinerufauswertung von EBÜS → www.ebues.de/Routinerufe.pdf

Eine Anleitung für Routine-Rufe bei **Mobotix**-Kameras haben wir hier bereitgestellt:
→ www.ebues.de/KB/000007

Falls Sie ein Problem feststellen, sprechen Sie uns an, dann können wir ggf. einen Work-around dafür bereitstellen.

Stand: 30.10.2024, Dipl.-Ing. Hardo Naumann