SICUREZZA RIELLO CONNECT

Tecnologie utilizzate dalla soluzione Riello Connect per mantenere al sicuro i vostri dati

RIELLO ELETTRONICA

riello ups

INDICE

Sicurezza e facilità d'uso costituiscono i pilastri della soluzione **Riello Connect**.
Questo documento illustra le misure di sicurezza implementate nell'ambito della soluzione Riello Connect per mantenere i vostri dati al sicuro.

Che cos'è Riello Connect?

Riello Connect è una soluzione di gestione a distanza basata sul cloud che permette ai centri di assistenza e agli utenti finali di monitorare e controllare da remoto i sistemi Riello UPS.

Come funziona Riello Connect:

Un gateway di comunicazione Riello Connect si collega alle apparecchiature presenti sul campo per mezzo di una connessione seriale, Ethernet o I/O. Il gateway invia le informazioni attraverso Internet o la rete cellulare (GSM/GPRS/3G) al centro dati basato sul cloud di Riello Connect.

Accedendo al sito di Riello Connect su *www.riello-ups.com*, gli utenti possono prendere visione di tutti i parametri del loro sistema UPS tramite computer, tablet o smartphone.

Grazie a Riello Connect è anche possibile impostare un tunnel di sicurezza per il debugging o la programmazione da remoto con il normale software di configurazione dell'utente. Questa funzione è denominata "Accesso remoto (Remote Access)".

Come il server Riello Connect riesce a mantenere sicuri i vostri dati

La sicurezza dei dati su Riello Connect è garantita da infrastrutture di server all'avanguardia dotate di potenza di backup, protezione antincendio e personale operativo 24 ore su 24, 7 giorni su 7. Riello Connect è un sistema ridondante distribuito in diversi server e in diverse sedi: ciò aumenta la disponibilità sul campo sia per gli utenti, sia per i gateway RCT di Riello Connect, riducendo al minimo il rischio di perdita dei dati.

Sicurezza nella trasmissione dati da/a Riello Connect

Sicurezza significa molto di più della semplice protezione dei dati nel server Riello Connect. Per mantenere sicuri i dati trasmessi a e da Riello Connect, la soluzione sfrutta quattro metodi diversi:

- **Crittografia tra browser web utente e cloud server Riello Connect**
- **Crittografia tra gateway RCT Riello Connect e cloud server Riello Connect**
- **Autenticazione utente all'accesso a Riello Connect (inclusa verifica in due passaggi)**
- **Permessi utente personalizzati**

2

Crittografia tra browser web utente e cloud server (certificato sito web)

Per rendere sicura la comunicazione tra il browser web dell'utente e Riello Connect viene utilizzata una connessione crittografata SSL/TLS 2048 bit RSA/256 bit AES.
L'identità del sito web Riello UPS (https://www.riello-ups.com) viene verificata in modo indipendente ed è in possesso di un certificato SSL Extended Validation.

Quando si visitano i siti web con certificati SSL Extended Validation, la barra degli indirizzi del browser web visualizza le informazioni concernenti l'identità legale del titolare in un caratteristico campo verde.
Le comunicazioni con il cloud server Riello Connect saranno sempre protette da una chiave di sessione con crittografia fino a 256 bit (minimo 128 bit).

3

Crittografia tra gateway remoto e cloud server Riello Connect

La comunicazione tra il gateway remoto RCT di Riello Connect collegato al dispositivo e il cloud server Riello Connect è crittografata attraverso una chiave a 128 bit TLS (Transport Layer Security): ciò rende sicura la comunicazione tra il dispositivo e il punto di monitoraggio.

Autenticazione tra Riello Connect e gateway RCT

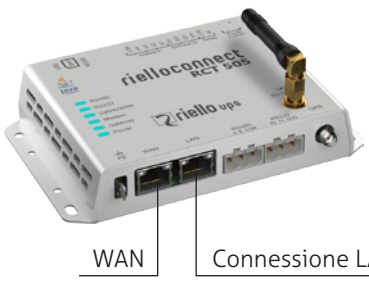
Quando il gateway RCT di Riello Connect si collega a Riello Connect, è necessario convalidare un certificato, a garanzia del fatto che il gateway si stia realmente connettendo a Riello Connect (e non ad altri server). Dal lato di Riello Connect, il gateway RCT viene identificato come gateway valido grazie a credenziali univoche.

Sicurezza per le comunicazioni di rete mobile

Quando le comunicazioni avvengono tramite la rete mobile, i dati crittografati SSL/TLS trasmessi sono anche incapsulati per mezzo della crittografia dello standard GSM/3G.

Quando il gateway di comunicazione di Riello Connect si collega alla rete mobile, riceve dal gestore di rete un indirizzo IP che non è necessariamente un indirizzo IP pubblico. Risulta quindi impossibile navigare o eseguire il ping del gateway. Inoltre utilizzare una scheda SIM senza un indirizzo IP pubblico per il gateway Riello Connect impedirà che dai motori di ricerca abbia origine un traffico dati indesiderato e che gli indirizzi IP siano scansionati da bot scanner.

All'interno dell'RCT



Sicurezza per le comunicazioni Ethernet

I gateway della serie 50x RCT di Riello Connect hanno in dotazione due porte di rete Ethernet: WAN e LAN. Questa separazione rende possibile, ad esempio, l'uso di firewall esterni sulla porta LAN a garanzia dell'applicazione di politiche di sicurezza rigorose.

Utilizzo del firewall

Per utilizzare i servizi il gateway RCT di Riello Connect deve essere in grado di comunicare con il server Riello Connect. È possibile impostare il firewall in modo da bloccare tutto il traffico in entrata e garantire la sicurezza del sito, senza interferire con la capacità di funzionamento della soluzione Riello Connect. Tuttavia, è ancora richiesto il traffico in uscita affinché il gateway Riello Connect possa stabilire una comunicazione con Riello Connect (deve essere aperta una porta in uscita: l'eventuale blocco di tutte le porte in uscita significherebbe che nessuna comunicazione sarebbe possibile).

Garantire la comunicazione in sicurezza

Il gateway RCT di Riello Connect va sempre installato dietro un firewall, dal momento che il metodo di comunicazione utilizzato dal gateway RCT di Riello Connect non prevede che il gateway sia esposto con un accesso IP pubblico.

Un'installazione di questo tipo rende impossibile aprire una connessione e stabilire una comunicazione da Internet al gateway RCT di Riello Connect — la comunicazione è possibile unicamente tramite Riello Connect.

Questo vale anche quando si utilizza una connessione cellulare e significa che il gateway RCT di Riello Connect non dovrebbe far parte di un piano di abbonamento di telefonia mobile con un indirizzo IP pubblico.

4

Autenticazione utente (inclusa verifica in due passaggi)

Ogni account utente su Riello Connect è protetto da password. A determinare i diritti di accesso per l'utente specifico sono il nome utente e la password. Riello Connect richiede una password composta da sei caratteri. Tuttavia, per garantire una maggiore sicurezza, accertarsi di:

- **servirsi di password che non siano utilizzate anche per altri siti**
- **attenersi alle comuni procedure ritenute ottimali per la generazione di password**

Verifica in due passaggi

Il controllo di verifica è simile a quello adottato dalle banche per innalzare il proprio livello di sicurezza. È necessario che il numero di telefono cellulare dell'utente sia registrato su Riello Connect. Quando un utente autorizzato chiede di accedere al sistema Riello Connect, la verifica che viene utilizzata comprende due passaggi. Una volta che l'utente ha inserito le proprie credenziali utente nella pagina di login di Riello Connect (username e password), riceverà un SMS con un codice di sicurezza da utilizzare una volta sola. Per poter accedere al sistema Riello Connect occorre inserire il codice entro 15 minuti.

Inserite la vostra password per collegarvi a Riello Connect.

Riceverete un messaggio di testo sul vostro cellulare da inserire in Riello Connect.

Accesso consentito!

Quando un utente effettua il login al sistema Riello Connect, nel sistema vengono registrate data e ora per almeno 4 settimane. Queste informazioni sono memorizzate unicamente nel sistema e non sono a disposizione degli utenti.

L'amministratore dell'account può vedere quando è avvenuto l'ultimo accesso a Riello Connect da parte di ciascun utente.

Per garantire che l'accesso all'account Riello Connect sia sicuro, la configurazione di tutti gli utenti e dell'amministratore prevede una verifica in due passaggi, il che comporta il controllo di ogni sessione con il codice di sicurezza ricevuto tramite SMS.

Ciascun codice di sicurezza generato ha 1.000.000 di combinazioni possibili. Per sventare eventuali attacchi all'account da parte di hacker, il sistema Riello Connect blocca l'utente per 10 minuti, se sono inseriti 40 codici non validi. Per impedire che l'intruso blocchi il telefono dell'utente, possono essere richiesti non più di 20 codici di sicurezza prima che la richiesta di funzionalità dei nuovi codici di sicurezza venga bloccata per 10 minuti.

Codici di ripristino (se non potete ricevere sul vostro telefono i codici di sicurezza utilizzabili una sola volta)

Dal sistema Riello Connect è possibile stampare 10 codici di ripristino, da utilizzare quando il cellulare dell'utente viene perso, risulta danneggiato o non è disponibile per altre ragioni.
Questi codici di ripristino possono essere usati anche per il login.

5

Diritti di accesso per utenti diversi

Il cloud server Riello Connect prevede tre livelli di accesso utente: Amministratore, Project Manager e Utente.

Amministratore

Nell'account Riello Connect esiste un solo Amministratore dell'account. L'Amministratore assegna le impostazioni utente e le diverse capacità di monitoraggio per ogni rispettivo utente.

Tutte le configurazioni di monitoraggio dei dispositivi (modelli, profili, allarmi e registrazione dati) sono create dall'Amministratore.

L'Amministratore dell'account Riello Connect è in grado di autorizzare/bloccare la modifica dei dati utente, quali i dati relativi a contatti, i numeri di telefono o le pianificazioni di allarmi, da parte di Project Manager e Utenti.

L'Amministratore dell'account imposta i privilegi utente per Project Manager e Utenti, ad esempio al fine di:

- **Accedere ad uno specifico progetto Riello Connect (un progetto Riello Connect consiste in uno o più gateway Riello Connect con i relativi dispositivi collegati).**
- **Limitare i privilegi di sola lettura (sola visualizzazione) per l'accesso a dati remoti.**
- **Ricevere / riconoscere allarmi.**
- **Funzionalità Accesso remoto**
- **Capacità servizi Web**

Project Manager

Il Project Manager ha gli stessi diritti di accesso dell'Amministratore dell'account per tutti i sistemi nell'ambito del progetto specificato. Il Project Manager è anche in grado di aggiungere ai progetti nuovi gateway remoti Riello Connect.

Utente

All'Utente possono essere assegnati privilegi quali l'accesso ad uno specifico progetto Riello Connect o l'accesso di sola lettura (sola visualizzazione) a dati remoti.

6

Accesso remoto e sicurezza Riello Connect

L'accesso remoto è un servizio di Riello Connect che apre un tunnel di sicurezza verso l'UPS e consente la configurazione, la programmazione o il debugging dell'UPS da qualsiasi sede. Gli utenti si servono del loro normale software di configurazione proprio come se fossero connessi sul posto.

Per stabilire la connessione da remoto, viene installato sul PC il driver basato su PC "Quick Connect" di Riello Connect.
Si crea in tal modo un tunnel di sicurezza attraverso Riello Connect fino al gateway Riello Connect e si stabilisce una connessione virtuale all'applicazione software sul PC.

Il tunnel aperto tra il computer e la rete remota è fruibile per creare uno o più canali per le connessioni effettive a dispositivi remoti.

Dal punto di vista della sicurezza, la funzionalità Accesso remoto non è diversa dal resto della soluzione Riello Connect. I dati che vanno o che provengono da Riello Connect sono ancora coperti dal protezione SSL. L'unica differenza consiste nel fatto che l'utente si collega a Riello Connect con il software Quick Connect invece di utilizzare *www.riello-ups.com*

Altri modi per rendere sicuro l'accesso alle apparecchiature

Whitelist di inoltro dati alla porta

Un Amministratore Riello Connect può selezionare per la whitelist alcuni indirizzi IP. In tal modo fornisce agli utenti l'accesso unicamente a questi indirizzi, limitando quindi il loro accesso ad altri indirizzi IP.

Soggetto a modifiche senza preavviso. Può contenere imprecisioni

RPS S.p.A. - Membro del gruppo Riello Elettronica
Viale Europa, 7 - 37045 LEGNAGO (Verona) - Italia
T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com

Seguici sui Social Network

DATRCSXOY15IRIT