Tre consigli per la sicurezza cibernetica

Tra i costruttori, la sicurezza cibernetica sta diventando un motivo di crescente apprensione, dato che ogni settimana si assiste alla creazione di nuove tipologie di ransomware e di altri virus di sistema.

Qualsiasi società può diventare bersaglio di un attacco cibernetico. Il modo migliore per prevenire questa eventualità è pianificare in anticipo e prepararsi ad eventi inattesi.

1 Dispositivi connessi

I dispositivi mobili offrono vantaggi in termini di monitoraggio delle condizioni, manutenzione preventiva e strumenti analitici. Se i produttori che si avvalgono di dispositivi connessi desiderano individuare e risolvere le avarie del sistema, devono assegnare la priorità ai regolari aggiornamenti di sicurezza e alle verifiche software.

2 Sistemi di generazione precedente

In generale, i sistemi informatici industriali non vengono aggiornati o sostituiti con la stessa frequenza delle tecnologie di consumo. Di conseguenza i produttori rimangono esposti ad attacchi più datati come Heartbleed o Shellshock.

In alcuni dei sistemi più vecchi può essere ancora installato un software originale OpenSSL. Le vulnerabilità di questo software possono esporre il sistema agli aggressori che hanno quindi la possibilità di ascoltare di nascosto o rubare i dati.

Molte aziende di software hanno rilasciato aggiornamenti critici gratuiti per contrastare le vulnerabilità. Tutti i produttori devono semplicemente aggiornare il loro software.

3 Sistemi di produzione automatizzati

Le reti e i sistemi aziendali non sono gli unici elementi a rischio. Anche i sistemi di controllo industriali possono diventare bersaglio di attacchi di tipo ramsoware. Se l'attacco blocca i computer della produzione, possono verificarsi onerosi tempi di inattività I produttori devono salvaguardare i sistemi di produzione automatizzati attraverso le celle di protezione, un'efficace forma di difesa contro gli attacchi di tipo man-in-the-middle.

Nell'epoca di Industry 4.0, i dispositivi connessi e i sistemi automatizzati possono essere soggetti a ulteriori minacce. Il modo migliore per prevenire un attacco è pianificare in anticipo e prepararsi ad eventi inattesi.