

**endian|OS**

Tecnologia medica: il potenziamento per una digitalizzazione sicura

Uno dei maggiori produttori mondiali di scanner diagnostici a ultrasuoni e a risonanza magnetica si affida da anni alla manutenzione remota. Per assicurarsi che l'accesso digitale non diventi un bersaglio per gli attacchi informatici, l'azienda protegge la sua tecnologia medica sensibile con il software Endian 4i Edge. Questo ha permesso di aggiornare i gateway esistenti con una protezione a radiofrequenza a una potente appliance di sicurezza.

“Per molto tempo la tecnologia medica è stata progettata per essere utilizzata in sistemi chiusi. A causa della digitalizzazione e della relativa connessione a Internet, questi dispositivi sono diventati un potenziale obiettivo per gli attacchi informatici”, spiega Raphael Vallazza, CEO di Endian. “La PIATTAFORMA DIGITALE SECURA di ENDIAN offre l'opportunità di collegare in rete e proteggere i dispositivi medici attraverso un retrofit semplice e veloce, senza la necessità di procedure di approvazione successive.”

Tecnologia medica: un caso speciale di digitalizzazione

L'installazione di un gateway di sicurezza IoT davanti a un dispositivo medico è generalmente una buona soluzione per il riadattamento della tecnologia medica esistente con tutti i componenti di connettività e sicurezza necessari per una digitalizzazione sicura. Tuttavia, l'implementazione di gateway di sicurezza IoT per scanner MRI e dispositivi a ultrasuoni è complessa in quanto questi dispositivi generano radiazioni ad alta frequenza durante l'uso, che possono interferire con il funzionamento dei gateway di sicurezza IoT. Per stabilire la connettività nel tipico ambiente IT eterogeneo di un ospedale, il produttore di dispositivi medici ha utilizzato gli speciali gateway di SECO, protetti dalle radiofrequenze e conformi a tutte le normative mediche.

“Per molto tempo la tecnologia medica è stata progettata per essere utilizzata in sistemi chiusi. A causa della digitalizzazione e della relativa connessione a Internet, questi dispositivi sono diventati un potenziale obiettivo per gli attacchi informatici”

Raphael Vallazza,
Endian CEO

Software per gateway di sicurezza IoT per una sicurezza IT completa

Per continuare a utilizzare questi gateway, il produttore ha optato per una soluzione unica di Endian; che offre una piattaforma integrata di cybersecurity che collega il mondo digitale (IT) e quello fisico (OT). Il gateway Endian 4i Edge X viene utilizzato per collegare i dispositivi fisici ed esiste anche una versione software, l'Endian 4i Software.

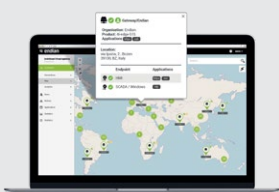
Il software Endian 4i Edge trasforma qualsiasi PC industriale e gateway IoT (tecnologia x86 o ARM) in una potente soluzione di connettività e cybersecurity per proteggere i dispositivi medici. Diverse funzioni di sicurezza finemente sintonizzate assicurano poi una protezione completa. La Deep Packet Inspection (DPI) analizza i pacchetti di dati inviati in rete. A differenza delle normali metodologie di analisi, che si limitano ai soli metadati, la DPI si spinge fino al livello dell'utente ed è in grado di rilevare oltre 300 protocolli IT e OT, nonché 2.000 applicazioni. Una rete privata virtuale (VPN) garantisce un accesso remoto sicuro, crittografando i dati durante la trasmissione in modo che non possano essere letti o manipolati. Se un aggressore supera il firewall, il sistema di rilevamento delle intrusioni (IDS) riconosce l'attacco e il sistema di prevenzione delle intrusioni (IPS) può impedirne il proseguimento o la diffusione nella rete.

Gestione granulare degli accessi per una maggiore sicurezza

La gestione granulare dei diritti di accesso fornisce un ulteriore livello di sicurezza. La Switchboard di Endian è uno strumento di gestione centrale della PIATTAFORMA DIGITALE SICURA ENDIAN, offre la possibilità di assegnare diversi diritti agli utenti o ai gruppi di utenti. Ad esempio, è possibile definire chi può accedere a quali dispositivi, quali azioni possono essere eseguite e quali dati possono essere visualizzati. Ogni accesso è documentato, in modo che sia sempre visibile chi è stato su quale dispositivo, quando e quali azioni sono state eseguite.

Protezione sempre aggiornata nonostante un sistema operativo obsoleto

Endian Switchboard consente inoltre di installare gli ultimi aggiornamenti di sicurezza su tutti i gateway IoT. Questo è stato particolarmente importante per il produttore di dispositivi medici, perché gli ecografi e gli scanner MRI che necessitavano di accesso remoto erano basati sul sistema operativo Windows XP. Poiché Microsoft ha smesso di fornire aggiornamenti per questo sistema operativo nel 2014, il suo utilizzo è ora troppo rischioso dal punto di vista della sicurezza informatica. “Nell'industria e anche nella tecnologia medica, le macchine sono spesso in funzione per dieci anni o più”, spiega Raphael Vallazza. “Non è quindi raro che i dispositivi medici siano ancora in uso con sistemi operativi vecchi. Aggiornando i gateway attraverso la switchboard, tutti i dispositivi sono protetti. Questo è un aspetto fondamentale in vista della direttiva NIS2, che sarà recepita nel diritto nazionale entro la fine del 2024”.



Endian Switchboard è il cuore di Endian Secure Digital Platform e da esso è possibile gestire in maniera centralizzata un'ampia gamma di operazioni. Abilitare l'accesso remoto sicuro ai macchinari in campo, la raccolta e visualizzazione dei dati, edge computing e l'amministrazione granulare degli accessi e permessi degli utenti.



Endian 4i Edge Software: trasformare qualsiasi gateway IoT (x86) o PC industriale in un'appliance di cybersecurity industriale Endian 4i. La piattaforma Endian 4i (operata da EndianOS) è stata concepita su misura per rispondere alle esigenze del mercato, per proteggere e connettere asset industriali come PLC, HMI, RTU e altri sistemi SCADA.

Nessun pericolo legato ai dispositivi di archiviazione mobili

Gli ecografi e gli scanner per la risonanza magnetica sono stati esposti a un altro rischio per la sicurezza informatica: i medici e il personale ospedaliero utilizzano regolarmente chiavette USB per archiviare le immagini degli esami. Tuttavia, il malware può entrare nelle macchine anche attraverso questi supporti di memorizzazione esterni e persino diffondersi attraverso la rete se i dispositivi sono collegati al sistema IT.

Per contrastare questo problema, è necessario che le chiavette USB non vengano più collegate direttamente all'ecografo o alla risonanza magnetica, ma al gateway IoT, che dispone anche della porta USB necessaria. Sul gateway IoT è stato installato un software antivirus per proteggere i dispositivi dal malware. Ogni volta che viene utilizzata una chiavetta USB, viene prima scansionata alla ricerca di eventuali virus o trojan e i programmi dannosi vengono bloccati.

Il fatto che tutti i sistemi esistenti potessero essere adattati in modo così rapido e sicuro senza dover acquistare nuovo hardware ha convinto la società. In futuro, tutti i dispositivi di nuova generazione saranno forniti con la piattaforma digitale sicura ENDIAN.



Endian SRL

Hypatiastraße 2
I-39100 Bozen (BZ) Italy

Tel: +39 0471 631 763
E-mail: info@endian.com