تأمین زیرساخت‌های حیاتی با دستگاه امنیت سایبری سخت جان

پیش‌زمینه

با پیشرفت‌های فناوری در حوزه اینترنت اشیا (IoT) و تحلیل کلان داده‌ها، سیستم‌های فناوری اطلاعات (IT) به‌سرعت با سیستم‌های فناوری عملیاتی (OT) ادغام می‌شوند. این ادغام فرآیندهای کسب‌وکار، بینش‌ها و کنترل‌ها را در یک محیط یکپارچه ادغام می‌کند تا بهره‌وری را افزایش داده، جریان‌های کاری را بهینه کند و سودآوری را برای صنایع مختلف از جمله تولید، خدمات عمومی، حمل‌ونقل، ارتباطات، پزشکی و خرده‌فروشی افزایش دهد.

یکی از بزرگ‌ترین چالش‌ها در ادغام محیط‌های IT وOT ، نگرانی‌های امنیتی و تهدیدات جدید است. پایش شبکه می‌تواند بخشی از این تهدیدات امنیتی، به‌ویژه در عملیات صنعتی، را کاهش دهد. اما برای تضمین امنیت و کنترل شبکه، نیاز به دید گسترده‌ای از کل عملیات، شامل محیط سیستم‌های کنترل صنعتی (ICS) و زیرساخت‌های فناوری اطلاعات ادغام شده است.

نیازمندی‌ها

برای ارائه یک راه‌حل که هم حملات مبتنی بر شبکه و هم پرس‌وجوهای فعال دستگاه را پوشش دهد، لازم است عملیات صنعتی به دید کامل، امنیت و کنترل در شبکه‌های OT مجهز شوند. یک متخصص برجسته در امنیت سایبری و اسکن آسیب‌پذیری‌های OT به شرکت لنر مراجعه کرد تا دستگاه امنیت سایبری مقاومی طراحی کند که بتواند محیط صنعتی را به طور فعال ایمن کند .

دستگاه سخت‌افزاری باید به‌اندازه کافی مقاوم و قدرتمند باشد و قابلیت‌های زیر را داشته باشد :

1. گواهینامه‌های IEC-61850-3 و IEEE 1613 :

محیط‌های زیرساخت حیاتی ممکن است با نوسانات دمایی غیرمنتظره، لرزش‌ها یا عوامل خارجی دیگر مواجه شوند. بنابراین، استقرار در این محیط‌ها نیازمند این گواهینامه‌ها برای مقاومت در برابر این تأثیرات خارجی است .

2. محدوده دمای عملیاتی گسترده:

دستگاه باید در شرایط دمایی شدید موجود در محیط‌های زیرساخت حیاتی قابل‌استفاده باشد .

3. LAN Bypass پیشرفته:

برای اطمینان از تاب‌آوری شبکه عملیاتی، در صورت بروز خرابی، ترافیک LAN مقاوم به خطا در ارتباطات ICS ضروری است .

4. فناوری امنیتی:

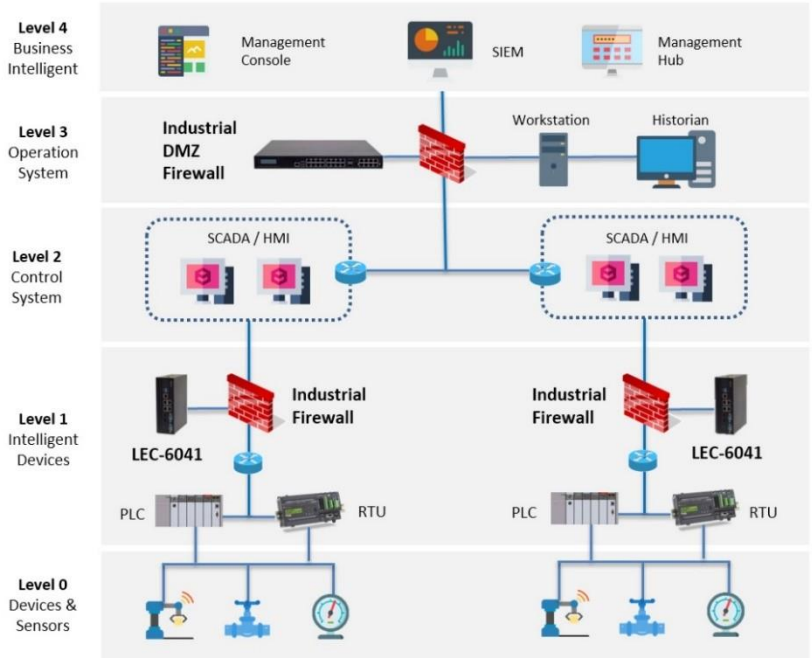
شامل یک TPM داخلی برای پردازش رمزنگاری امن و مقاومت در برابر دستکاری در سطح سخت‌افزار .

5. **مسیر قدرت دوگانه**:

در تجهیزات مستقر در بخش خدمات عمومی، تأمین توان پایدار ضروری است و مسیر قدرت دوگانه می‌تواند پایداری بیشتری را در حوزه‌های OT ارائه دهد.

IEC-61850-certified Rugged Appliance

Strengthens Critical Infrastructure OT/ICS Cybersecurity



راه‌حل‌ها

برای حفاظت از شبکه‌های صنعتی در برابر تهدیدات سایبری، نفوذگران داخلی، و/یا خطاهای انسانی، اپراتورهای صنعتی باید دید کاملی از سطح حملات داشته باشند و علاوه بر آن، قابلیت‌های تشخیص تهدید، ردیابی دارایی‌ها، مدیریت آسیب‌پذیری‌ها و کنترل پیکربندی را برای به حداکثر رساندن ایمنی و قابلیت اطمینان محیط‌های OT فراهم کنند. شرکت لنر گیتوی امنیتی مقاومی ارائه می‌دهد که می‌توانند سیستم‌های مستقر در SCADA، PLCو سیستم‌های کنترل صنعتی و خدمات عمومی را مدیریت، پایش و کنترل کنند.

LEC-6041

دستگاه LEC-6041 شرکت لنر به‌طور خاص برای حفاظت از ارتباطات بین محیط‌های IT و OT طراحی شده است. این دستگاه با استفاده از پردازنده‌های کم‌مصرف و پردازش قدرتمند Intel Atom x7-E3950 یا x5-E3930، و دارای گواهینامه‌های IEC 61850-3 و IEEE 1613، برای محیط‌های سخت طراحی شده است.

ویژگی‌های کلیدی دستگاه LEC-6041 شامل موارد زیر است:

- محدوده دمای عملیاتی گسترده: برای استفاده در محیط‌های بحرانی با شرایط دمایی شدید.
- پورت‌های I/O با حفاظت ESD تا KV15 و پورت‌های LAN با حفاظت ایزولاسیون مغناطیسی KV1.5.
- طراحی مقاوم سخت‌افزاری: اطمینان از عملکرد بدون وقفه در محیط‌های خطرناک.

دستگاه LEC-6041 دید، امنیت و مدیریت شبکه OT را فراهم می‌کند و برای زیرساخت‌های حیاتی مانند ایستگاه‌های برق، پالایشگاه‌های نفت و انرژی‌های تجدیدپذیر مناسب است.

LEC-6041

IEC 61850-3 Wide Temperature ICS Cyber Security Gateway with Intel Atom CPU

CPU	Intel Atom x7-E3950 or x5-E3930
Chipset	SoC

Read more