1 **Railway/industrial cybersecurity/Firewall/ Metro**

فایروال صنعتی قطار امنیت سایبری قطار به زمین را تقویت می کند

اتصال پهن باند حیاتی، بنیادی برای تبدیل دیجیتالی راه آهن امروزی است

راه‌حل‌های راه‌آهن هوشمند، شبکه‌های ریلی و مترو شهری را به عصر دیجیتال سوق داده است و اتصال بی‌وقفه به ویژه برای بخش حمل‌ونقل عمومی ضروری است. ارتباطات قطار به زمین قابل اعتماد برای عملیات کارآمد در داخل هواپیما و بسیاری از کاربردهای داخل هواپیما مورد نیاز است که همچنان در حال افزایش است.

یک راه حل ارتباطی امن و با کارایی بالا از قطار به زمین، برنامه های کاربردی حیاتی ایمنی مانند کنترل قطار مبتنی بر ارتباطات (CBTC)، کنترل نظارتی و جمع آوری داده ها (SCADA)، پخش جریانی دوربین مداربسته در زمان واقعی، درب خروجی، و سیستم های اطلاعات مسافران را ارائه می دهد. (PIS). علاوه بر برنامه‌های غیرمرتبط با ایمنی مانند Wi-Fi عمومی و سیستم‌های سرگرمی سرنشین. در عین حال، راه‌های نوآورانه اپراتورهای ریلی را قادر می‌سازد تا کارآمدتر عمل کنند و ارزشی را برای مسافران در کل ناوگان به ارمغان بیاورند.

با این حال، شبکه‌های Wi-Fi سنتی ممکن است همیشه برای پشتیبانی از تحرک پرسرعت و نیازهای راه‌آهن حیاتی کافی نباشند. از آنجایی که عملکرد و کیفیت می تواند ناپایدار باشد و این فناوری در معرض خطرات امنیتی است.

آسیب پذیری های امنیت سایبری راه آهن

سیستم‌های فناوری اطلاعات حمل‌ونقل ریلی به پهنای باند بالایی از دسترسی، در دسترس بودن و امنیت نیاز دارند، به این معنی که به همان اندازه باید در برابر حملات سایبری قوی و مقاوم باشند. از آنجایی که سیستم‌های کمک راننده و کنترل سواری اکنون دارای اتصال و ارتباط هستند، این امر باعث می‌شود سیستم‌هایی که به طور سنتی بسته بودند، باز شوند، که به نوبه خود در برابر حملات مخرب آسیب‌پذیرتر خواهند بود. اگر از این ضعف‌ها استفاده شود، می‌تواند عواقب جدی داشته باشد که بر سیستم‌های اطلاعات مسافران، شبکه‌های نظارت تصویری و حتی در دست گرفتن کنترل قطار تأثیر بگذارد.

کاربردهای فناوری صنعت 4.0

استفاده از فناوری‌های انقلاب چهارم صنعتی در بخش راه‌آهن منجر به مزایای متعددی مانند دقت بهتر و ایمنی بهبود یافته در مدیریت کنترل و ترافیک راه‌آهن، علاوه بر بهبود تجربه مسافران می‌شود، اما خطرات مرتبط نیز افزایش می‌یابد. سیستم‌های حیاتی، هم‌گرایی شبکه‌های فناوری اطلاعات و OT، اتوماسیون، و گنجاندن هوش مصنوعی، با این عوامل بسیار، اپراتورهای ریلی باید مفهوم انعطاف‌پذیری سایبری را در سیستم‌های خود بگنجانند. مدیران راه‌آهن و مترو باید فوراً یک سیاست مدیریت ریسک اتخاذ کنند،

2 **Railway/industrial cybersecurity/Firewall/ Metro**

دارایی‌های حساس خود را شناسایی کنند، شبکه خود را تقسیم‌بندی کنند و راه‌حل‌های دفاع سایبری را به کار گیرند. شرکت‌های راه‌آهن و مترو باید یاد بگیرند که در برابر حملات سایبری مخرب و نحوه مقابله با آن در صورت وقوع، محافظت کنند.

توابع فناوری عملیاتی پیشرفته

یک راه حل ایمن می تواند تجربه مشتری را با اتصال پهن باند بی سیم مستمر و انعطاف پذیر برای مسافران و عملیات داخل هواپیما تضمین کند. از طریق افزودن یک لایه حفاظت از فایروال، رمزگذاری سرتاسر، و تجزیه و تحلیل پروتکل برای اطمینان از تبادل اطلاعات عملیات ایمن بین قطارها و ایستگاه اصلی. از هویت دیجیتال و احراز هویت و مدیریت دسترسی برای کنترل دسترسی به شبکه OT و زیرساخت ایمن برای نقاط پایانی در سیستم های کنترل استفاده کنید. داده های محرمانه را می توان از طریق راه حل های رمزگذاری و مکانیسم های امنیتی برای مسدود کردن بدافزارها و فساد شبکه محافظت کرد. برنامه‌های تاب‌آوری سایبری مؤثر به سازمان‌ها کمک می‌کند تا با تهدیدات امنیتی در حال تحول روبرو شوند و از بسیاری از این حملات جلوگیری کنند.

گیتوی امنیتی LEC-6041 شرکت لنر یک راه حل اتصال باند پهن با کارایی بالا و ایمن برای صنایع ریلی و حمل و نقل انبوه است. یک پلت فرم قابل اعتماد برای سیستم های اطلاعاتی در زمان واقعی و کاربردهای مدرن با فناوری انتقال درجه صنعتی. LEC-6041 برای محافظت از ارتباطات در هر دو حوزه IT و OT طراحی شده است و تمام الزامات عملکرد و قابلیت اطمینان را برآورده می کند.

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