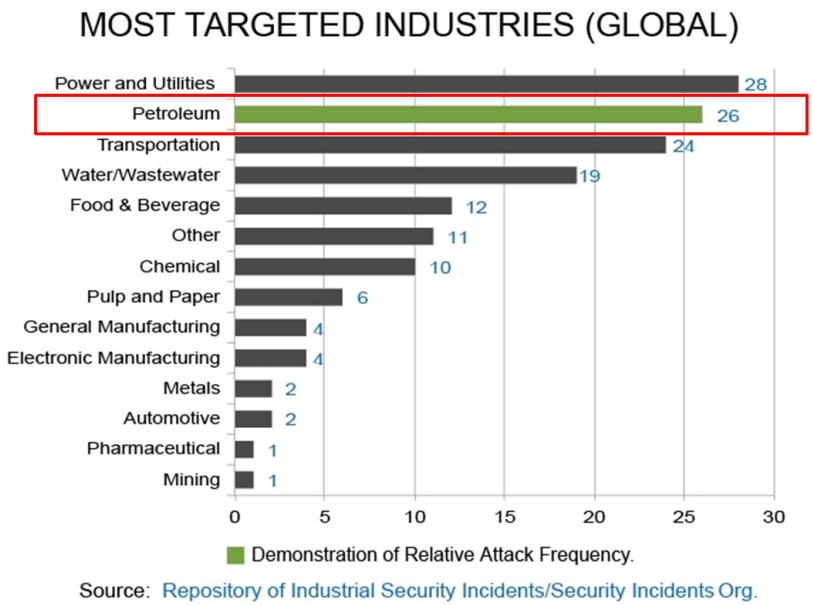
یکپارچه سازی معماری های چندلایه برای کاهش آسیب پذیری های سایبری در بخش های نفت و گاز

زمینه

امروزه، تولیدات تاسیساتی مانند میدان نفتی، پالایشگاه نفت و حفاری گاز در دریا، بیش از پیش دیجیتالی و متصل شده اند. دستگاه‌هایی مانند PLC ، HMI، SCADA، حسگرها و سیستم‌های محاسباتی تعبیه‌شده به منظور بهینه‌سازی اتوماسیون و تولید، فناوری‌های عملیاتی متصل به هم هستند. اگرچه دیجیتالی شدن و اتصال دستگاه های OT بهره وری و خروجی را برای صنعت نفت و گاز افزایش داده است، درها به روی حملات سایبری در همان زمان باز است. در واقع، تعداد حملات سایبری به صنایع تولید برق به طور مداوم در حال افزایش است. بر اساس تحقیقات انجام شده، بیش از 60 درصد شرکت های برق در سال های گذشته با حداقل یک حمله مواجه شده اند و صنعت نفت به عنوان یکی از هدفمندترین صنایع برای حملات سایبری معرفی شده است.



از آنجایی که نفت و گاز دو ابزار اصلی برای زندگی روزمره هستند، دارایی‌های حیاتی مانند پالایشگاه‌ها، کارخانه‌های تولید و سایت‌های نصب، هدف‌های مهمی برای هکرها هستند. اگر این محیط‌های OT مورد حمله قرار گیرند، پیامدهای جدی شامل تعطیلی کارخانه، شکست تولید، و ایجاد داده‌های محرمانه می‌شود که در نهایت باعث خرابکاری اقتصاد ملی و ایجاد وحشت در عموم می‌شود. بنابراین، هنگامی که دستگاه‌های OT متصل هستند، باید از ارتباطات ایمن در کل ترافیک و پروتکل‌های شبکه ICS اطمینان حاصل کنیم.

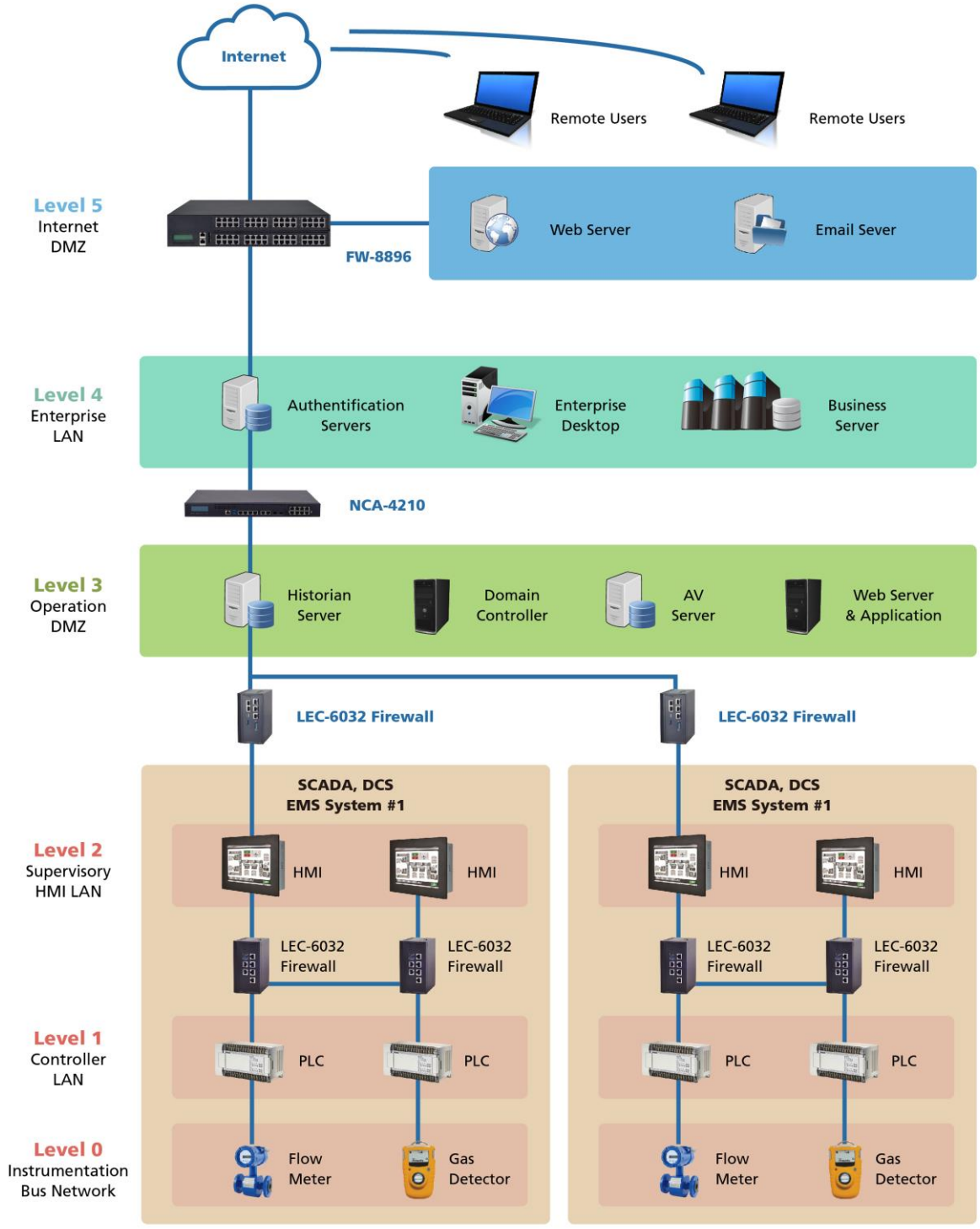
الزامات

پروتکل‌های OT سنتی ICS و SCADA در برابر تهدیدات سایبری آسیب‌پذیر هستند، زیرا این پروتکل‌ها معمولاً بدون محافظت و باز باقی می‌مانند. این آسیب پذیری هکرها را به سمت دستکاری پالایشگاه ها و کارخانه های نفت و گاز با معرفی بدافزارها از طریق نقاط دسترسی مختلف شبکه های کنترل جذب می کند.

به منظور محافظت از دستگاه های متصل به هم و پروتکل های شبکه، صاحبان دارایی های حیاتی باید پلتفرم های امنیتی شبکه چند لایه را برای شبکه های OT/IT خود برای اجرای لیست سفید، نظارت بر الگوی ترافیک، پروتکل ها و بازرسی بسته ها و سیاست های امنیتی پیاده سازی کنند. پلتفرم‌ها باید دارای طراحی قوی، عملکرد بهینه و اتصال ورودی/خروجی با پیکربندی مناسب برای برآوردن درخواست‌های امنیتی در محیط‌های چالش‌برانگیز باشند.

راه حل سخت افزاری چند لایه

برای رسیدگی به مسائل امنیت سایبری در صنعت نفت و گاز، LEC-6032 و NCA-4210 شرکت لنر مجموعه های بهینه برای استقرار OT و DMZ هستند. برای استقرار جانبی OT، LEC-6032 یک سیستم تعبیه شده بدون فن با درجه حرارت صنعتی است که در سایت های ICS و SCADA به عنوان فایروال لیست سفید و بازرسی بسته ها مستقر می شود. برای طرف DMZ، NCA-4210 یک دستگاه 1U Rackmount با CPU میکرو معماری 14 نانومتری اینتل، پردازنده نسل ششم Intel® Core™ (با اسم رمز Skylake-S) است که به‌عنوان UTM و IPS استفاده می‌شود.


Internet
Remote Users
Remote Users
Level 5
Internet
DMZ
FW-8896
Web Server
Email Sever
Level 4
Enterprise
LAN
Authentification
Servers
Enterprise
Desktop
Business
Server
NCA-4210
Level 3
Operation
DMZ
Historian
Server
Domain
Controller
AV
Server
Web Server
& Application
LEC-6032 Firewall
LEC-6032 Firewall
SCADA, DCS
EMS System #1
SCADA, DCS
EMS System #1
Level 2
Supervisory
HMI LAN
HMI
HMI
HMI
HMI
LEC-6032
Firewall
LEC-6032
Firewall
LEC-6032
Firewall
LEC-6032
Firewall
Level 1
Controller
LAN
PLC
PLC
PLC
PLC
Level 0
Instrumentation
Bus Network
Flow
Meter
Gas
Detector
Flow
Meter
Gas
Detector

امنیت سایبری در شبکه OT

برای اجرای اقدامات امنیتی و جلوگیری از دسترسی غیرمجاز از راه دور، LEC-6032 یک فایروال صنعتی فشرده و 7/24 است که برای بخش های نفت و گاز طراحی شده است. طراحی مستحکم بدون فن LEC-6032 قطعی سیستم را کاهش می دهد و گرد و غبار داخل دستگاه را به حداقل می رساند. LEC-6032 همچنین دارای دمای عملیاتی طولانی با محدوده حداکثر -40 درجه سانتیگراد تا 70 درجه سانتیگراد است. این کارکرد گسترده ای را در محیط های سخت محیطی در سایت های مستقر ICS فراهم می کند. علاوه بر این، نوسانات الکتریکی ممکن است در زیرساخت های حیاتی رخ دهد و این ممکن است سیستم های اجرا شده را ویران کند.

برای جلوگیری از وقوع خرابی ها، LEC-6032 دارای پورت های COM ایزوله با حفاظت در KV ESD15 و حفاظت مغناطیسی برای پورت های اترنت است. با توجه به اتصال به شبکه، LEC-6032 پیکربندی‌های پورت LAN مختلف از جمله GbE LAN، پورت‌های فیبر SFP، و بای پس LAN پیشرفته Gen.3 را بسته به مجموعه‌های مدل خاص ارائه می‌کند.

امنیت سایبری در شبکه های DMZ

NCA-4210 شرکت لنر که برای دفاع از حملات سایبری پیشرفته (مانند حمله DDoS) در سرورهای تاریخ نگار و کنترل‌کننده‌های دامنه در DMZ صنعتی طراحی شده است، توسط CPU جدید 14 نانومتری ریزمعماری اینتل، پردازنده Intel® Core™ (با اسم رمز Skylake) قدرتمند شده است. با نسل بعدی طراحی سه‌بعدی، استفاده از پردازنده نسل ششم Intel® Core™ با نوید افزایش عملکرد پردازنده و در عین حال کاهش TDP همراه است. یک نوع سوکت جدید، LGA 1151، نیز برای معماری die-shrinking عرضه شده است. از نظر کارایی حافظه، NCA-4210 از DDR4 دو کاناله با فرکانس تا 2133 مگاهرتز و ظرفیت تا 32 گیگابایت در 2 x 16 گیگابایت DIMM پشتیبانی می کند. ECC نیز پشتیبانی می شود (فقط برای چیپست C236 موجود است).

یکی دیگر از ویژگی های جالب NCA-4210 استفاده از چیپست Intel® H110 و C236 است. PCH جدید ارتقای بزرگی را برای PCI Express به ارمغان می آورد. با سوکت جدید LGA 1151، NCA-4210 تا 20 خط PCIe Gen3.0 و سوکت M.2 را پشتیبانی می‌کند و بازده ورودی/خروجی را تا 40 درصد افزایش می‌دهد.

امنیت سایبری در شبکه های سازمانی

دلیل اصلی آسیب‌پذیری سایبری در شبکه‌های اتوماسیون تفکیک‌شده به دلیل وجود کدهای مخرب از بیرون است. شبکه‌های سازمانی متصل به اینترنت یا دستگاه‌های خارجی ناامن مانند لپ‌تاپ، تبلت و لوازم جانبی USB نیز باعث ایجاد حفره‌هایی برای بدافزارها و ویروس‌ها در شبکه‌های اداری و صنعتی می‌شوند.

شرکت لنر که برای محافظت از شبکه های سازمانی ساخته شده است، FW-8896، فایروال های شبکه سازمانی با کارایی بالا را با قابلیت دسترسی و قابلیت اطمینان بالا ارائه می دهد. این لوازم شبکه 2U rackmount x86 مجهز به دو پردازنده Intel® Xeon® E5-2600 v3/v4 / چیپست C612 (با نام رمز «Grantley») و حافظه DIMM ثبت شده DDR4 تا فرکانس 2133 مگاهرتز برای ارائه قدرت محاسباتی بی نظیر برای پیاده سازی است. معیارهای. FW-8896 همچنین دارای 8 اسلات ماژول NIC با حداکثر. 64 پورت اترنت، بای پس پیشرفته LAN و پشتیبانی از شتاب رمزنگاری، این دستگاه را برای برنامه های امنیتی درخواستی مانند IDS (سیستم های تشخیص نفوذ)، IPS (سیستم های جلوگیری از نفوذ)، DPI (بازرسی بسته های عمیق) در شبکه های سازمانی ایده آل می کند.

LEC-6032E

Industrial Grade PoE Network Appliance with Intel® Atom™ E3845 Processor

CPU	Intel Atom E3845
Chipset	None

Read more

FW-8896

High-performance x86 Network Security Appliance based on Dual Intel Xeon E5-2600 v3 CPUs

CPU	Dual Intel® Xeon® E5-2600 v3/v4 series CPU (Haswell/Broadwell-EP)
Chipset	Intel® C612 series Chipset

Read more

NCA-4210

1U x86 Rackmount Network Appliance Powered by Intel's 7th Gen Core Processors

CPU	Intel® Core™ i7/i5/i3 or Pentium® or Celeron® (Skylake/Kaby Lake)
Chipset	Intel® H110 or C236

Read more