



امنیت سیستم های کنترل صنعتی

Industrial Control Systems Security

امنیت سیستم های کنترل صنعتی

تهدید فزاینده حملات سایبری پیشرفته به زیرساختهای حیاتی و سیستمهای کنترل صنعتی چالشی منحصر به فرد برای سازمانها محسوب می شود. مأموران جاسوسی در دولت، تروریست ها و جرایم سازمان یافته به طور فزاینده ای سیستم های صنعتی را هدف قرار می دهند، در نتیجه باعث اختلال فیزیکی در عملیات تجاری و سرقت مالکیت معنوی می شود. اختلال در سیستم های کنترل صنعتی می تواند علاوه بر از بین بردن تجهیزات گران قیمت، بلکه منجر به قطع عملیات حیاتی نیز شود. این حملات، به نوبه خود، می تواند منجر به هزینه های گسترده و از دست دادن اعتماد عمومی در جامعه به طور کلی شود.

راه ارتباطی

تلفن:
026 368 06249

وبسایت:
unk9vvn.com

ایمیل:
info@unk9vvn.com

بررسی معماری

در اولین قدم میبایست معماری IT و OT مجموعه صنعتی را کاملا بررسی و تصویر کرد، سیستم های نرم افزاری و مدیریتی، پروتکل های ارتباطی و دستگاه های کنترلر صنعتی (PLC) همگی میبایست بررسی و پایش شوند تا در نگاه امنیت سایبری تست های نفوذ هدفمند روی آنها پیاده سازی شده و فضاهای دارای آسیب پذیری شناسایی شوند، در این بررسی می بایست تمامی آرایش های ارتباطی و دستگاه های متصل مشخص و زیر ذره بین بروند.

ارزیابی آسیب پذیری دستگاه و برنامه ها

فناوری های نرم افزاری و سخت افزاری که در فضاهای صنعتی استفاده می شود میبایست بصورت کامل ارزیابی امنیت سایبری شوند، این ارزیابی شامل سیستم عامل ها، سرویس های فعال در درگاه ها، پایگاه های داده و نرم افزار های مدیریتی و فرمان پذیر است. این ارزیابی ها بصورت کارشناسی و دقیق در خصوص کشف آسیب پذیری های روز صفر است که در دو لایه باینری و تحت وب میتواند رخ دهد.

چالش های سیستمی

سیستم های کنترل صنعتی شامل فناوری هایی مانند کنترل نظارت و اکتساب داده ها (SCADA) و سیستم های کنترل توزیع شده (DCS) است که در هسته اصلی عملیات روزمره در زیر ساخت های فرآوری شیمیایی، تولید نفت و گاز و سایر صنایع هستند.

این برنامه ها شامل سوئیچ های راه آهن، ماینیورهای SCADA و کنترل کننده های منطقی قابل برنامه ریزی (PLC) هستند. سازمان های زیرساختی که برای اقتصاد و امنیت ملی حیاتی هستند، از مراکز داده بانکی گرفته تا شبکه های برق و حمل و نقل ریلی، از بسیاری از فناوری های مشابه استفاده می کنند.

بسیاری از این سیستم ها به طور فزاینده ای به شبکه های IT متصل شده اند، و آنها را در معرض حمله سایبری قرار می دهد.

فناوری IT و فناوری OT

ترکیبی سفارشی از فناوری، اطلاعات و خدمات مشاوره ای متخصصان امنیت سایبری بوده که می تواند سازمان های صنعتی و تولیدی را قادر به شناسایی خطرات و کاهش فعالانه تهدیدات کنند. برای کل فناوری اطلاعات (IT) و فناوری عملیاتی (OT) شما یک راه حل امنیتی جامع و غیرتجاهمی ارائه می دهیم.

تیم تهاجمی ما تجربه با دانش عمیقی که از سیستم های کنترل حاصل کرده و فضای ICS و OT شناخته است، همچنین متخصصان ما که با Threat Intelligence آشنا هستند و دانش بی نظیر از رفتارهای مهاجمان درک کرده اند، آزمایش های امنیتی پیشرفته ای را انجام می دهند و به شما کمک می کنند تا تهدیدات را در شبکه های صنعتی، شناسایی و مهار کنید.

حملات شبکه Air-Gap

بطور مجزا حملات شبکه Air-Gap از طیف گسترده و خطرناکی بهره مند است، شبکه Air-Gap به دلیل مجزا بودن از شبکه جهانی اینترنت طیف حملات مختص به خود را دارد، حملاتی بر پایه Physical Media، Acoustic، Electromagnetic، Thermal، Electric، Magnetic و Optical هستند که خطرات سایبری را برای سیستم های کنترل صنعتی بشدت بالا برده است، این حملات بر پایه شبکه های صنعتی و نظامی پیاده سازی می شوند و از محرمانگی خاصی برخوردار هستند.

همچنین عوامل انسانی موتور محرک حملات Physical Media هستند که از این روی آگاه سازی نیروهای انسانی در حوزه امنیت سایبری یک اصل خواهد بود، همچنین سخت افزار های بکارگرفته شده که اگر در ساختار درستی نباشند میتوانند عوامل شکل گیری یک سناریو حمله را تشکیل دهند.

ارزیابی آسیب پذیری های شبکه

ارزیابی شبکه ارتباطی فضاهای صنعتی خود به تنهایی دارای لیستی از آسیب پذیری ها است که میبایست کامل بررسی شود، بطور مثال در معماری شبکه های Air-Gap همواره سناریو ها و تهدیدات منحصر به فردی نهفته است که میبایست بصورت مجزا به آنها پرداخته شود، همچنین پروتکل های ارتباطی که همواره با سنسور ها و دستگاه های عملیاتی در تعامل هستند هم میبایست بررسی امنیت سایبری کامل شوند.

تست نفوذ صنعتی

در تست نفوذ صنعتی همواره تیم کارشناسان می کوشند تا تمامی آسیب پذیری ها را در دو روش شناسی جعبه سیاه و جعبه سفید بررسی نمایند که در اینجا تمرکزها بر کشف آسیب پذیری ها است نه ارزیابی آنها، در این خصوص پروسه تست نفوذ مرحله بسیار جامع تر و کامل تری از کشف آسیب پذیری ها است که تمامی دستگا ها و سیستم عامل ها مورد آزمون قرار خواهند گرفت از جمله دستگاه های IIoT.

شبیه سازی تیم قرمز

اما بالاترین سطح ارزیابی امنیت سایبری مجموعه های صنعتی را میتوان شبیه سازی تیم قرمز دانست، تیم قرمز همواره می کوشد تا بصورت کاملا شبیه سازی شده روش منطق عملیاتی تمامی تیم های تهاجمی سایبری که تا به حال به مجموعه های صنعتی حمله کردند را پیاده سازی کرده و از این روی مناطق مورد اشکال و دارای شرایط مناسب برای نفوذگر نمایان کامل شود، از جمله این شبیه سازی ها میتوان به حمله سایبری صنعتی ویروس Stuxnet اشاره کرد.