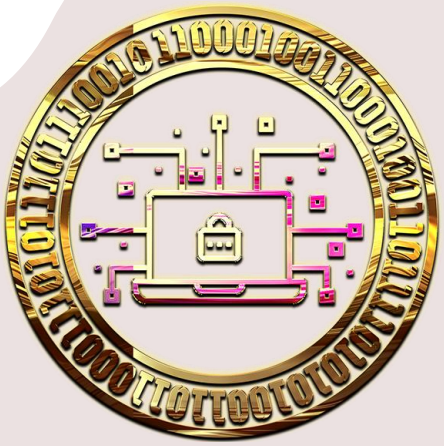
امنیت سیستم های کنترل صنعتی

بررسی معماری

در اولین قدم باید معماری IT و OT مجموعه صنعتی را کاملا بررسی و تصویرسازی شود، سیستم های نرم افزاری و مدیریتی، پروتکل های ارتباطی و دستگاه های کنترل کننده صنعتی (PLC) هم باید بررسی و پایش شوند تا از نگاه امنیت سایبری، روی آنها تست های نفوذ هدفمند پیاده سازی شده و فضاهای دارای آسیب پذیری شناسایی شوند، در این بررسی می بایست تمامی آرایش های ارتباطی و دستگاه های متصل، مشخص شده 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 شوند 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 و بصورت کارشناسی دقیق در خصوص کشف آسیب پذیری های روز صفر میباشد که در دو لایه باینری و تحت وب میتواند رخ دهد.



امنیت سیستم های کنترل صنعتی

تهدید فزاینده حملات سایبری پیشرفته به زیر ساختهای 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 علاوه بر از بین بردن تجهیزات گران قیمت، میتواند منجر به قطع عملیات حیاتی نیز شود. این حملات، به نوبه خود، می توانند منجر به هزینه های گسترده و از دست دادن اعتماد عمومی در جامعه شوند.

راه ارتباطی

تلفن:
026 368 06249

وبسایت:
unk9vvn.com

ایمیل:
info@unk9vvn.com

ارزیابی آسیب پذیری های شبکه

ارزیابی شبکه ارتباطی فضاهای صنعتی خود به تنهایی دارای لیستی از آسیب پذیری ها است که باید کامل بررسی شوند، بطور مثال در معماری شبکه های Air-Gap همواره سناریو ها و تهدیدات منحصر به فردی نهفته است که باید بصورت مجزا به آنها پرداخته شود، همچنین پروتکل های ارتباطی که همواره با سنسور ها و دستگاه های عملیاتی در تعامل هستند هم باید 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 جعبه سیاه و جعبه سفید بررسی نمایند که در اینجا تمرکز برروی کشف آسیب پذیری هاست نه ارزیابی آنها، در این خصوص پروسه تست نفوذ مراحل جامع و کامل تری از کشف آسیب پذیری ها ارائه میدهد که باعث میشود تمامی دستگاه ها و سیستم عامل ها از جمله دستگاه های IIoT مورد آزمون قرار بگیرند.

شبیه سازی تیم قرمز

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

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) هستند که در هسته اصلی عملیات روزمره در زیر ساخت های فرآوری شیمیایی، تولید نفت و گاز و سایر صنایع میباشند.

این برنامه ها شامل سوئیچ های راه آهن، مانیتورهای SCADAو 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 فناوری های مشابه استفاده می کنند.

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

فناوری IT و فناوری OT

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 کند. ما برای کل فناوری اطلاعات (IT) و فناوری عملیاتی (OT) شما، یک راه حل امنیتی جامع و غیرتهاجمی ارائه می دهیم.

تیم تهاجمی ما تجربه و دانش عمیقی از سیستم های کنترل حاصل کرده و فضای ICS و OTرا 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

شبکه Air-Gap به دلیل مجزا بودن از شبکه جهانی اینترنت طیف حملات مختص به خود را دارد که این حملات گسترده و خطرناک هستند، حملاتی بر پایه Physical Media ، Electric، Magnetic، Acoustic Electromagnetic، Optical و Thermal 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 Mediaهستند که از این روی آگاه سازی نیروهای انسانی در حوزه امنیت سایبری یک اصل خواهد بود، همچنین سخت افزار های بکارگرفته شده اگر در ساختار درستی نباشند میتوانند عوامل شکل گیری یک سناریو حمله را تشکیل دهند.