



صنعت میگوی کشور در یک دهه اخیر، علاوه بر بهبود معیشت روستاییان و اشتغال‌زایی، موفق به ارزآوری بیش از ۱.۲ میلیارد دلار شده است که نشان‌دهنده جایگاه مهم آن در اقتصاد ملی است. به گزارش اقتصادسراسرآمد، در تحلیلی که توسط علی اکبر خدایی – دبیر کل اتحادیه تولید و تجارت آبزیان منتشر شده، آمده است: تولید میگو از ۱۷,۷۹۵ تن در سال ۱۳۹۴ به اوج خود یعنی ۶۰,۶۳۱ تن در سال ۱۴۰۱ رسید. تولید در سال‌های ۱۴۰۲ و ۱۴۰۳ به دلیل شیوع بیماری AHPND در استان‌های بوشهر و هرمزگان، با افت شدید مواجه شد. اما پیش‌بینی می‌شود تولید سال جاری به بیش از ۶۱ هزار تن برسد که بالاترین رکورد تاریخ صنعت است و جهش آن عمدتاً در رشد تولید در استان بوشهر نسبت داده می‌شود.

در زمینه صادرات، گشایش موانع اداری و قرنطینه‌ای با روسیه و چین موتور اصلی رشد بوده است. روسیه به مهم‌ترین بازار صادراتی تبدیل شده و سهم آن به ۵۸.۵٪ در سال ۱۴۰۳ افزایش یافته است. این در حالی است که صادرات به چین به دلیل بیماری AHPND کاهش یافته است. امارات متحده عربی نیز جایگاه دوم را حفظ کرده است.

بالترین درآمدا ارزی در سال ۱۴۰۰ با ۱۸۲.۷ میلیون دلار ثبت شد. درآمد سال ۱۴۰۳ به حدود ۹۱.۶ میلیون دلار کاهش یافت. این کاهش بیش از آنکه ناشی از افت جهانی قیمت باشد، به سیاست‌های سختگیرانه دولت در نحوه بازگشت ارز صادراتی نسبت داده شده است. در نهایت، صنعت میگو نیازمند مدیریت دقیق عواقب زیست‌محیطی روش‌های تولید فوق‌متراکم و رفع موانع بازگشت ارز برای حفظ روند رشد درآمدی در آینده است.

استان مرکزی باز یگر کلیدی آبی‌پروری در کشور



مدیر شیلات سازمان جهاد کشاورزی استان مرکزی گفت: این استان با ایجاد زیرساخت‌های استراتژیک در بخش آبی‌پروری، به یکی از بازیگران کلیدی در حفظ زنجیره ارزش آبی‌پروری کشور تبدیل شده است.

به گزارش اقتصادسراسرآمد، حسن اکبری به ایرنا افزود: با توجه به اینکه تراز تجاری بخش کشاورزی و غذا در سال‌های اخیر به منفی ۱۳ میلیارد دلار رسیده و سرانه مصرف مواد غذایی تحت تأثیر تورم با کاهش مواجه شده است، تکمیل حلقه‌های نهایی زنجیره تولید از ضرورت‌های اجتناب‌ناپذیر توسعه بخش کشاورزی در استان مرکزی به شمار می‌رود که این موضوع در بخش آبی‌پروری مورد توجه قرار گرفت.

وی اظهار کرد: اجرای این پروژه مهم در راستای راهبردهای وزارت جهاد کشاورزی و با هدف تضمین امنیت غذایی به‌عنوان یکی از ارکان اصلی امنیت ملی آغاز و دستاوردهای قابل توجهی برای استان به همراه دارد.

مدیر شیلات سازمان جهاد کشاورزی استان مرکزی تصریح کرد: نخستین محور، کاهش ضایعات و افزایش بهره‌وری در بخش آبی‌پروری استان است، چرا که با توسعه صنایع فراوری و بسته‌بندی مدرن، از خروج محصولات خام و فسادپذیر از چرخه مصرف جلوگیری می‌شود و ارزش افزوده حاصل از تبدیل ضایعات به محصولات باکیفیت، محقق می‌شود. وی افزود: دومین دستاورد مهم این طرح، ایجاد اشتغال پایدار و رونق تولید است. در شرایطی که سرمایه‌گذاری در بخش کشاورزی طی سال‌های گذشته با کاهش روبه‌رو بوده، بخش آبی‌پروری با جذب سرمایه‌گذاران و ایجاد فرصت‌های شغلی پایدار، الگویی موفق از پیوند توسعه روستایی با اقتصاد ملی ارایه می‌دهد.

مدیر شیلات سازمان جهاد کشاورزی استان مرکزی همچنین تأمین بازارهای ملی و صادراتی را از دیگر مزیت‌های این اقدام برشمرد و گفت: امروز این استان نه‌تنها توان تأمین و عرضه محصولات تولیدی آبی‌ری را دارد، بلکه با تبدیل شدن به یکی از قطب‌های فراوری آبزیان کشور، نقشی موثر در تنظیم بازار داخلی و کاهش وابستگی به واردات ایفا می‌کند.



کرد. راهکار اما در تعویض یکباره تمام تجهیزات یا بازنشستگی سریع ناوگان قدیمی خلاصه نمی‌شود، بلکه باید در پیاده‌سازی لایه‌های دفاعی هوشمندانه و متناسب با محدودیت‌های این شناورها جستجو شود. جداسازی شبکه‌های عملیاتی حیاتی از ارتباطات عمومی و اینترنت پرسرعت، به‌کارگیری سامانه‌های پایش مستمر برای شناسایی رفتارهای غیرعادی و مهم‌تر از همه، تدوین پروتکل‌های واکنش سریع در مواجهه با حملات، از جمله اقداماتی است که می‌تواند بدون نیاز به بازسازی اساسی، سطح ایمنی این کشتی‌ها را به طرز چشم‌گیری افزایش دهد. در این میان، نقش سازمان‌های رده‌بندی و نهادهای نظارتی بین‌المللی در الزامی کردن استانداردهای حداقلی امنیت سایبری برای کشتی‌های با هر سن و سالی، نقشی تعیین‌کننده و حیاتی خواهد بود.

اینترنت پرسرعت در کشتی‌ها، نعمت یا نعمت‌امنیتی؟

انقلاب ارتباطات دریاهایا ورود اینترنت ماهواره‌ای پرسرعت، به ویژه استارلینک، فصل تازه‌ای را در تاریخ دریانوردی مدرن گشوده که تأثیرات آن فراتر از تصور فعالان باسابقه این صنعت بوده است. تا پیش از این، ملوانان در دل اقیانوس‌ها با محدودیت شدیدی پهنای باند و هزینه‌های سرسام‌آور ارتباطات ماهواره‌ای دست و پنجه نرم می‌کردند و تماس با خشکی به مکالمات ضروری یا پیام‌های متنی مختصر خلاصه می‌شد. اما امروز، نسل جدید ارتباطات، کشتی‌ها را به شناورهایی کاملاً متصل تبدیل

کرده که خدمه آن می‌توانند از پهنای باندی به مراتب بیشتر از بسیاری از نقاط شهری برخوردار باشند. این تحول، افزون بر افزایش رفاه و بهبود روحیه خدمه که خود مزیتی ارزشمند است، امکان نظارت لحظه‌ای بر عملکرد موتورها، دریافت به‌روزرسانی‌های فوری نرم‌افزاری، برگزاری جلسات ویدیویی با دفتر مرکزی و دسترسی بی‌وقفه به اطلاعات هواشناسی و نقشه‌های ناوبری را فراهم کرده است. شرکت‌های کشتیرانی پیشرو امروز می‌توانند ناوگان خود را از راه دور مدیریت کرده و با تحلیل داده‌های ارسالی از شناورها، مصرف سوخت را بهینه‌سازی کرده و از بروز خرابی‌های پرهزینه پیشگیری کنند.

اما این اتصال همیشگی و پرسرعت، روی دیگری نیز دارد که کمتر مورد توجه قرار گرفته و آن افزایش تصاعدی سطح دسترسی برای مهاجمان سایبری است. هر کشتی متصل به استارلینک، درست مانند یک رایانه همیشه آنلاین در خشکی، دارای اینترنتی منحصربه‌فردی است که آن را در معرض پوشش‌های خودکار و حملات گسترده قرار می‌دهد. خطری که اینجا وجود دارد نه در فناوری خود استارلینک، بلکه در تأمادگی زیرساخت‌های امنیتی ناوگان دریایی جهانی اگر چه از منظر ظرفیت حمل و تنوع شناورها همواره رو به توسعه بوده، اما واقعیتهای انکارناپذیر در دل این صنعت خودنمایی می‌کند: میانگین سنی بالای کشتی‌ها. بسیاری از شناورهایی که امروز اقیانوس‌ها را در می‌نورند، در دوره‌ای طراحی و ساخته شده‌اند که خبری از تهدیدات سایبری امروزی نبود و به همین دلیل، زیرساخت فناوری آن‌ها در برابر حملات مدرن، آسیب‌پذیری‌های بنیادینی دارد. این شکاف عمیق میان نسل فناوری‌های به‌کاررفته در این کشتی‌ها و پیچیدگی روزافزون حملات سایبری، وضعیتی خطرناک خلق کرده که می‌توان آن را به استحکامات ظاهرآمقاوم اما بی‌کن شده‌ای تشبیه کرد که از درون آماده فروپاشی است. سیستم‌های قدیمی ناوبری، تجهیزات کنترلی فاقد پروتکل‌های امنیتی مدرن و نبود زیرساخت مناسب برای دریافت به‌روزرسانی‌های منظم، همگی دست به دست هم داده‌اند تا ناوگان فرسوده به اهدافی آسان و جذاب برای گروه‌های باج‌افزاری و حتی خرابکاران دولتی تبدیل شوند. غافلگیری تلخ ماجرا اینجاست که هزینه‌نوسازی یاایمن‌سازی این کشتی‌ها در برابر تهدیدات سایبری، در مقایسه با خسارات هنگفت ناشی از توقف عملیات، غرق شدن محموله یا حتی به کل نشستن یک شناور، رقمی ناچیز محسوب می‌شود. پرسش اساسی که اینجا مطرح می‌شود آن است که آیا باید امنیت سایبری ناوگان فرسوده را به عنوان یک چالش غیرقابل حل و پرهزینه نادیده گرفت، یا آن را به مثابه یک اولویت راهبردی برای تضمین تداوم کسب‌وکار و ایمنی دریانوردی تعریف کرد؟ تجربه نشان داده که نگاه ساده‌انگارانه به این موضوع، نه فقط مالکان کشتی، که تمام زنجیره تأمین را با مخاطرات جدی مواجه خواهد

خبر

در راستای توسعه همکاری‌های دانشگاه و صنعت صورت گرفت؛

امضای تفاهم‌نامه دانشگاه امیر کبیر وهلدینگ تایدواتر برای تربیت نیروی انسانی متخصص

دانشگاه صنعتی امیرکبیر و یک هلدینگ با امضای تفاهم‌نامه‌ای آموزشی – پژوهشی، همکاری مشترک خود را در زمینه مدیریت بنادر، لجستیک و توسعه اقتصاد پایدار دریامحور با هدف تربیت نیروی انسانی متخصص و تقویت پیوند دانشگاه و صنعت گسترش می‌دهند.

به گزارش اقتصادسراسرآمد، تفاهم‌نامه همکاری آموزشی میان این دانشگاه وهلدینگ تایدواتر خاورمیانه با هدف توسعه آموزش‌های تخصصی و گسترش همکاری‌های علمی –صنعتی در حوزه مدیریت بنادر و اقتصاد پایدار دریامحور به امضا رسید.در آیین امضای این تفاهم‌نامه، مرتضی کلاه‌دوزان، معاون آموزشی و تحصیلات تکمیلی دانشگاه صنعتی امیرکبیر، با خیرمقدم به مدیرعامل، اعضای هئیت‌مدیره و همراهان هلدینگ تایدواتر خاورمیانه و همچنین نمایندگان شرکت آموزش فناوری ساحل و فراساحل، اظهار کرد: امضای این تفاهم‌نامه گامی مثبت در جهت مشارکت جدی‌تر

«سرآمد» بررسی می‌کند؛

تهدیدات سایبری در صنعت دریایی

کشتی‌های فرسوده در تیررس حملات سایبری

ارتباطات بی‌سیم محافظت‌نشده میان تجهیزات و ضعف در به‌روزرسانی منظم سیستم‌های قدیمی مدیریت ترمینال، همگی نقاط کوری هستند که می‌توانند فاجعه‌ای عظیم رقم بزنند. مقاوم‌سازی بنادر در برابر این طوفان سایبری، نیازمند سرمایه‌گذاری کلان در مراکز عملیات امنیتی اختصاصی، طراحی دقیق شبکه‌های جداگانه برای بخش‌های مختلف عملیاتی و مهم‌تر از همه، ایجاد پروتکل‌های روشن برای شرایط اضطراری و قطع یکدک استست تا در صورت وقوع حمله، امکان ادامه حداقلی عملیات و بازگشت سریع به شرایط عادی وجود داشته باشد.

آموزش سایبری خدمه؛ خط‌مقدمدفاع در دریا

پیچیده‌ترین دیوارهای آتش و پیشرفته‌ترین سامانه‌های شناسایی نفوذ نیز در نهایت در برابر یک کلیک ساده و ناآگاهانه بر روی یک لینک آلوده، بی‌دفاع و تسلیم خواهند بود. این حقیقت تلخ اما انکارناپذیر، جایگاه بی‌بدیل انسان را در معادله پیچیده امنیت سایبری دریایی آشکار می‌سازد، آن‌هم در شرایطی که آمارها حکایت از آن دارد که نزدیک به نیمی از حوادث سایبری در این صنعت، ریشه در حملات فیشینگ و مهندسی اجتماعی دارد. ملوانانی که ماه‌های متمادی دور از خانواده و در انزوا و خشکی دریانوردی می‌کنند، هنگام چک کردن ایمیل‌های شخصی یا اداری خود در آب‌های بین‌المللی، ممکن است هرگز تصور نکنند که پشت یک پیام به ظاهر ساده از سوی یک شرکت تأمین‌کننده یا حتی یکی از دوستان، گرومی از مجرمان سایبری کمین کرده‌اند. استفاده بی‌رویه از حافظه‌های جانبی شخصی برای انتقال فایل میان رایانه‌ها نیز یکی دیگر از عادات خطرناکی است که هر ساله بادفزارهای متعددی را وارد شبکه داخلی کشتی‌ها می‌کند و تمامی تدابیر امنیتی گرانقیمت را نقش بر آب می‌سازد.

با وجود این تصویرنگران‌کننده، همین ملوانان می‌توانند به نیرومندترین و مؤثرترین خط دفاعی در برابر تهدیدات سایبری تبدیل شوند، به شرط آنکه نگاه به آنها از یک «حلقه ضعف» به «سرمایه‌ای هوشمند» تغییر یابد و آموزش‌های متناسب با شرایط واقعی زندگی در دریا برای آنها طراحی و اجرا شود. آموزش‌های سنتی و تئوریک که گاه در قالب سخنرانی‌های خشک و یک‌طرفه ارائه می‌شوند، هرگز نمی‌توانند ملوانی را برای تشخیص یک ایمیل فیشینگ حرفه‌ای یا امتناع از استفاده از یک حافظه جانبی ناشناس آماده کنند. آنچه مورد نیاز است، برگزاری کارگاه‌های عملی و شبیه‌سازی حملات واقعی روی کشتی‌هاست تا خدمه با عینک تجربه، تفاوت میان یک درخواست معمولی و یک تله سایبری را درک کنند. آموزش چگونگی تشخیص نشانی‌های جعلی اینترنتی، بررسی هویت فرستندگان ایمیل‌های مشکوک و پروتکل مشخص برای مواجهه با موقعیت‌های غیرعادی، باید سه بخش جدایی‌ناپذیر از برنامه‌های آماده‌سازی خدمه پیش از سفر تبدیل شود. علاوه بر این، ایجاد فرهنگ گزارش‌دهی در میان خدمه، به‌گونه‌ای که بدون ترس از سرزنش یا توبیخ، هرگونه اتفاق مشکوک را به بلافاصله به افسران مسئول اطلاع دهند، می‌تواند نقش چشمگیری در مهار سریع تهدیدات و جلوگیری از گسترش آنها به بخش‌های حیاتی کشتی ایفا کند.

دنیاى دریانوردی امروز در پیسج تاریخی خود قرار دارد؛ جایی که امنیت فیزیکی دیگر برای محافظت از کشتی‌ها و محموله‌های گرانبها کافی نیست و نبرد در عرصه‌ای ناپیدا اما سرنوشت‌ساز جریان دارد. آنچه از خلال بررسی تهدیدات سایبری در این صنعت آشکار می‌شود، تصویری از آسیب‌پذیری‌های زنجیره‌وار و به‌هم‌پیوسته‌ای است که از کشتی‌های فرسوده با سیستم‌های قدیمی آغاز شده و تا بنادر هوشمند و مدرن امتداد می‌یابد. استارلینک اگرچه پنجره‌ای تازه به سوی ارتباطات پرسرعت گشوده، اما هم‌زمان درهای نفوذ را نیز به روی مهاجمانی گشوده که از هر نقطه ضعفی برای ایجاد اختلال استفاده می‌کنند. در این میان، آنچه به مثابه یک عامل تعیین‌کننده و حیاتی خودنمایی می‌کند، توجه به نیروی انسانی به عنوان نخستین و آخرین خط دفاعی است. ملوانانی که بسا آموزش‌های هدفمند و کاربردی، از یک تهدید بالقوه به یک دارایی هوشمند تبدیل می‌شوند. عبور از این طوفان سایبری نیازمند نگاهی جامع و چندلایه است؛ جایی که فناوری‌های مدرن، پروتکل‌های دقیق و آگاهی نیروی انسانی در هماهنگی کامل با یکدیگر، سدی مستحکم در برابر موج فزاینده حملات ایجاد کنند.

بنادر هوشمنددر برابر طوفان سایبری

بنادر به عنوان حلقه اتصال خشکی و دریا، همواره نقشی محوری در پویایی اقتصاد جهانی ایفا کرده‌اند، اما نسخه مدرن آنها با مفهوم «هوشمندی» چنان عجین شده که امروزه کمتر ترمینالی را می‌توان یافت که بدون اتکا به فناوری‌های پیشرفته دیجیتال اداره شود. این تحول دیجیتال که با استقرار هزاران سنسور اینترنت اشیا، سامانه‌های خودکار تخلیه و بارگیری، نرم‌افزارهای یکپارچه مدیریت ترمینال و ارتباط بی‌درنگ با کشتی‌ها و گمرکات همراه بوده، بهره‌وری را به سطح بی‌سابقه‌ای رسانده و زمان ماندگاری کالا در اسکله را به حداقل ممکن کاهش داده است. بنادر هوشمند امروز موجوداتی زنده و پویا هستند که هر جزء آن‌ها با دیگری در حال تبادل اطلاعات است؛ از لحظه ورود کشتی به آب‌های نزدیک بندر تا خروج کالا از دروازه‌های پایانی، همه چیز توسط الگوریتم‌های پیچیده و سیستم‌های خودکار



مدیریت می‌شود. این پیوستگی و وابستگی متقابل، اگرچه کارآمدی خیره‌کننده‌ای به همراه داشته، اما در عین حال، بنادر را به هدفی وسوسه‌انگیز و فوق‌العاده آسیب‌پذیر در برابر طوفان‌های سایبری تبدیل کرده که با یک ضربه می‌تواند شریان حیاتی اقتصاد یک کشور یا حتی منطقه را مسدود کنند. حادثه تلخ باج‌افزاری بندر ناگويا در ژاپن، که عملیات پایانه صادرات خودروهای تویوتا را برای روزها فلج کرد، تنها نمونه‌ای کوچک از فاجعه‌ای است که در انتظار بنادر فاقد آمادگی لازم می‌باشد. در چنین حملاتی، مهاجمان دیگر به دنبال سرقت اطلاعات ساده نیستند، بلکه با قفل کردن سیستم‌های مدیریت محموله، از کار انداختن جرثقیل‌های خودکار یا مختل کردن سامانه‌های شناسایی کشتی‌ها، به سرعت اختلالی زنجیره‌وار در تمام فرایندهای بندر ایجاد می‌کنند. نکته هشداردهنده آنجاست که وابستگی شدید بنادر مدرن به تأمین‌کنندگان متعدد فناوری و نرم‌افزار، سطح حمله را به شدت افزایش داده و هر نقطه ضعفی در زنجیره تأمین دیجیتال، می‌تواند به منفذی برای نفوذ گسترده تبدیل شود. سنسورهای ارزان قیمت و فاقد پروتکل‌های امنیتی،



دانشگاه در ارائه خدمات آموزشی و پژوهشی در حوزه مدیریت بنادر و اقتصاد پایدار دریامحور است و می‌تواند سرآغاز همکاری‌های بلندمدت و اثربخش میان دانشگاه و صنعت برای ایجاد ارزش در سطح ملی و بین‌المللی باشد. وی با اشاره به سوابق آموزشی و پژوهشی خود در زمینه اقتصاد پایدار دریامحور افزود: در این حوزه فرصت‌های نوظهور و ارزشمندی وجود دارد که همکاری نظام‌مند میان دانشگاه و صنعت می‌تواند آن‌ها را به دستاوردهای ملموس در مسیر اشتغال‌زایی و توسعه اقتصادی تبدیل کند و منشأ خدمات مؤثر به کشور و مردم باشد. در ادامه، مهدی قائم‌مقامی، مدیرعامل و عضو هیئت‌مدیره هلدینگ تایدواتر خاورمیانه، با ابراز خرسندی از حضور در دانشگاه صنعتی امیرکبیر و انعقاد این تفاهم‌نامه گفت: هلدینگ تایدواتر خاورمیانه به‌عنوان شرکت سهامی عام پذیرفته‌شده در بورس، با بیش از نیم‌قرن سابقه در ارائه خدمات بندری و دریایی، برخورداري از بیش از چهار هزار نیروی انسانی و ۱۴ شرکت فعال، یکی از بزرگ‌ترین و توانمندترین شرکت‌های ایرانی در این حوزه به‌شمار می‌رود. وی با اشاره به جایگاه ژئوپلیتیک ایران به‌عنوان یکی از مهم‌ترین شاهراه‌های ترانزیت کالا در خاورمیانه و غرب آسیا، بر اهمیت آموزش و پژوهش در حوزه مدیریت بندر، لجستیک و اقتصاد پایدار دریامحور تأکید کرد و افزود: یکی از چالش‌های اساسی این حوزه، کمبود نیروی متخصص و باتجربه و همچنین به‌روزرسانی‌نشدن رفصل‌های آموزشی است؛ از این رو همکاری با دانشگاه صنعتی امیرکبیر به‌عنوان یکی از معتبرترین مؤسسات آموزش عالی کشور می‌تواند دستاوردهای ارزشمندی برای کشور به همراه داشته باشد.