سرقت کرده‌اند و آن‌ها را برای فروش گذاشته‌اند.

امسال عربستان با شرکت امنیتی دراگوس برای حفاظت از دارایی‌های صنعتی و زیرساخت‌های حیاتی خود در شرکت آرامکو یادداشت تفاهم همکاری امضا کرده است. براساس این تفاهم‌نامه این دوشرکت در حوزه مونتاژ سخت‌افزاری و آموزش فناوری عملیاتی به پرسنل آرامکو و شرکت‌های وابسته به آن همکاری خواهد کرد. از سویی امکان استقرار سریع فناوری‌های خدمات سایبری برای حفاظت از زنجیره‌های تامین حیاتی همچون سوخت‌رسانی فراهم می‌آید. این تفاهم‌نامه همچنین از ارکان اصلی چشم‌انداز ۲۰۳۰ عربستان خواهد بود.

معنی حمله سایبری به پمپ‌بنزین‌ها

در همه‌جای دنیا پمپ‌بنزین‌ها به دلیل آسیب‌پذیری‌های ناشناخته، تبدیل به طعمه‌های آسانی برای هکرها شده‌اند و این هکرها از راه دور می‌توانند بر این سیستم‌ها نفوذ کنند. گزارش‌ها از حملات به این سیستم‌ها نشان می‌دهد به دلیل نوع سازوکاری که پمپ‌بنزین‌ها دارند حمله به چنین زیرساخت‌هایی به مهارت خاصی نیاز ندارد.

بنابرگزارش شرکت ای‌ام‌اس (Environmental Monitoring Solutions)، یک هکر سایبری می‌تواند از آسیب‌پذیری‌های موجود در جایگاه سوخت سوءاستفاده کرده و موفق شود تا: تمام سیستم‌های سوخت‌رسانی را خاموش کند، قیمت سوخت را تغییر دهد و حتی باعث نشت سوخت شود. یا امکان سرقت پول از پایانه‌های پرداخت را فراهم آورد زیرا کنترل‌کننده مستقیماً به پایانه پرداخت متصل می‌شود، بنابراین ممکن است تراکنش‌های پرداخت سرقت شوند. پلاک خودرو و هویت راننده را هم می‌توان از فیلم دوربین مداربسته پمپ‌بنزین‌ها پاک کرد.

کار هکرها مختص به این موارد نیست. حمله به سیستم‌های نظارت بر سوخت، مخازن سوخت، سیستم‌های امنیتی یا دستگاه‌های اینترنت اشیا که داده‌های نظارتی را برای چنین سیستم‌هایی فراهم می‌کنند می‌تواند عواقب مخربی داشته باشد.

گفته می‌شود که گیج‌های خودکار مخازن (ATG) در تقریباً ۳ درصد از ۱۵۰ هزار پمپ‌بنزین ایالات‌متحده فاقد رمز عبور اولیه برای جلوگیری از نفوذ هکرها هستند. بر این اساس روی کاغذ پورت‌های کنترلی در این ATGها در برابر حملات آسیب‌پذیر هستند و باعث می‌شود پمپ بنزین به دلیل خوانش اشتباه مخزن متوقف شود.

در سال ۲۰۲۰ چنین حمله سایبری به شرکت آی‌ان‌ای، بزرگ‌ترین شرکت نفت کرواسی باعث شد زنجیره پمپ‌بنزین‌های این شرکت فلج شود. این حمله از طریق باج‌افزار کلاپ انجام شده بود که سرورهای پشتیبان این شرکت را آلوده و بعد رمزگذاری کرد. هرچند با این حمله توان سوخت‌رسانی شرکت مختل نشد اما با این حمله سایبری، پمپ‌بنزین‌های زیرمجموعه این شرکت توان صدور فاکتور و پرداخت قبض‌های آب و برق و گاز را نداشت (آی‌ان‌ای یکی از عرضه‌کنندگان گاز در کرواسی هم هست).

در ماه ژوئن ۲۰۲۳ به پمپ‌بنزین‌های غول انرژی سانکور در کانادا حمله شد. این شرکت یکی از بزرگ‌ترین شرکت‌های انرژی در آمریکای شمالی است با چندین پالایشگاه و شبکه‌ای از بیش از ۱۸۰۰ خرده‌فروشی و عمده‌فروشی. پس از این حمله این شرکت اعلام کرد، احتمال دارد امکان پرداخت هزینه بنزین با کارت‌های اعتباری متوقف شود.

روش‌های حفاظت از زیرساخت‌ها

معمولاً یک حمله هکری مراحل خاصی دارد که در آن هکر اول هدف خود را مشخص می‌کند، بعد در هدف خود نقاط آسیب‌پذیر شبکه را برای سوءاستفاده پیدا می‌کند و سپس حمله را به تجهیزات دیگر در شبکه گسترش می‌دهد، زیرا هکرها به دنبال چیزی ارزشمند هستند

وقتی یک هکر در حال تحقیق درباره یک حمله است، اطلاعات عمومی مانند محدوده شبکه، آدرس‌های MAC/IP، دامنه‌ها یا نام میزبان را جمع‌آوری می‌کند و احتمالاً از نرم‌افزار اسکن IP برای یافتن اهداف خود استفاده می‌کند. بعد اطلاعات جمع‌آوری‌شده را در شبکه در کنار نقاط آسیب‌پذیر شناخته‌شده و نقض‌های امنیتی شبکه قرار می‌دهند. هکرها پس از ورود به شبکه، به دنبال تجهیزات دیگری می‌گردند که از دسترسی به سایر دستگاه‌ها یا داده‌های ارزشمند در شبکه پشتیبانی می‌کند. بسته به هدف، گزینه ارزشمندی که یک هکر به دنبال آن است احتمالاً الگوی عملیات، دسترسی به سیستم‌های دیگر، داده‌های کارت اعتباری، رمز عبور یا باج‌باشد. کشورها معمولاً برای حفاظت از پمپ‌بنزین یا سایت‌های سوخت‌رسانی خود در برابر حملات سایبری، از یک سیاست امنیتی دقیق استفاده می‌کنند که ویژگی‌های پیشرفته‌ای چون گیج خودکار مخزن را داشته باشد. در این سیستم‌ها از یک فایروال به‌عنوان اولین خط دفاعی در شبکه استفاده می‌شود.

کارشناسان تاکید دارند، سیستم‌های داده‌ای مرتبط با پمپ‌بنزین‌ها باید مجهز به این شرایط باشند: انتقال داده ایمن و قابل اعتماد با احراز هویت قوی، رمزگذاری و حفاظت از یکپارچگی؛ و حفاظت از فایروال قوی و کنترل‌های دسترسی در شبکه داخلی برای محافظت از دستگاه‌های مهم مانند PLCها.

احمد بکر، کارشناس امنیت سایبری از جده عربستان، می‌گوید: امنیت سایبری موفق باید مبتنی بر رویکردی باشد که در اصطلاح به آن «دفاعی لایه‌ای» گفته می‌شود تا از بدترین رخدادها جلوگیری کند

دفاع لایه‌ای که «دفاع در عمق» نیز نامیده می‌شود، یک مفهوم اثبات‌شده مبتنی بر انواع مختلف کنترل‌های امنیت سایبری است. ایده این است که اگر یک کنترل از کار بیفتد یا توسط مهاجم دور بزند، لایه دیگر باید بتواند از سیستم محافظت کند.

در اوایل سال ۲۰۱۷، مؤسسه تحقیقاتی پونمون ایالات‌متحده

آرامکو که بزرگ‌ترین شرکت نفتی جهان است، در سال‌های اخیر هدف حملات سایبری متعددی قرار گرفته که معروف‌ترین آنها، بدافزار شامون در سال ۲۰۱۲ بود که اطلاعات تمامی رایانه‌های این شرکت نفتی را پاک کرد. امین ناصر، رئیس و مدیر اجرایی بزرگ‌ترین شرکت نفتی جهان، در جریان نشست جهانی هوش مصنوعی ۲۰۲۲ در ریاض گفته بود، حملات سایبری یکی از بزرگ‌ترین خطراتی است که آرامکوی عربستان با آن مواجه است

به همراه شرکت زیمنس ماموریت یافت تا درباره امنیت سایبری در صنعت نفت و گاز بررسی‌هایی انجام دهد. بر اساس یافته‌های آن، ۶۸ درصد از مدیران سایبری نفت و گاز ایالات متحده گفتند، شرکت‌شان حداقل یک بار تجربه از دست دادن اطلاعات محرمانه یا اختلال در عملیات‌های خود را تجربه کرده است. همان زمان این مطالعه تاکید کرد، بسیاری از سازمان‌ها از خطر سایبری آگاهی ندارند.

در سال ۲۰۲۰، مطالعه‌ای توسط جف هنکاک، استاد دانشگاه استنفورد و شرکت امنیتی Tessian مشخص کرد ۸۸ درصد علل نقض اطلاعات مربوط به خطای کارمندان است. این بدان معنی است که یکی از بزرگ‌ترین خطرات امنیت سایبری، یعنی خطای انسانی را می‌توان از طریق آموزش به حداقل رساند.

کارشناسان امنیت سایبری تاکید دارند، در حالی که رشد غیرقابل توقف دیجیتالی‌سازی می‌تواند خطرات سایبری خاصی را افزایش دهد، اما مزایای آن برای صنعت نفت در تمام شاخه‌های آن، از تولید تا مصرف در پمپ‌بنزین‌ها، بیشتر از این خطرات است.

براساس گزارش وب‌سایت شرکت زیمنس انرژی، دیجیتالی‌سازی، که مخصوصاً برای صنعت نفت و گاز عملی است، به‌طور خودکار به‌معنای عملیات در فضای ابری نیست. این مفهوم برای زیرساخت‌های حیاتی صنعت نفت، در درجه اول به معنای استفاده از برنامه‌های دیجیتال برای نظارت بر دارایی‌های فیزیکی مانند کمپرسورها و تجهیزات، با هدف کارآمدتر و مقرون‌به‌صرفه‌تر کردن عملیات است.

از سویی به باور کارشناسان هوش مصنوعی می‌تواند در برابر جرایم سایبری همانند یک محافظ عمل کند. دیجیتالی شدن خود یکی از مؤثرترین سلاح‌ها در برابر تهدیدات سایبری است و هوش مصنوعی نیز همینطور است. هوش مصنوعی مبنایی برای نظارت بر امنیت کارخانه نوآورانه زیمنس انرژی است. یکی از سرویس‌های امنیت سایبری بر پایه هوش مصنوعی توسط خود زیمنس انرژی معرفی شده است. این پلتفرمی است که از هوش مصنوعی و روش‌های یادگیری ماشین برای جمع‌آوری و مدل‌سازی دارایی‌های انرژی در زمان واقعی استفاده می‌کند. این کار به کارشناسان امنیت سایبری اجازه می‌دهد تا حملات را قبل از اجرای آنها نظارت، شناسایی و کشف کنند.

نحوه کار هوش مصنوعی

هوش مصنوعی چگونه می‌تواند امنیت سایبری زیرساخت‌ها را تامین کند؟ در واقع عملکرد هوش‌مصنوعی در این حوزه را به‌صورت زیر می‌توان طبقه‌بندی کرد:

۱ **شناسایی پیشگیرانه تهدید:** هوش مصنوعی می‌تواند حجم وسیعی از داده‌ها را در زمان واقعی تجزیه و تحلیل و ناهنجاری‌ها و تهدیدات احتمالی را با دقت بالا شناسایی کند. این موضوع به این دلیل است که هوش مصنوعی قادر است الگوهایی را در داده‌ها بیاموزد که انسان نمی‌تواند آن‌ها را بیاموزد و می‌تواند تهدیدهایی را که ممکن است توسط ابزارهای امنیتی سنتی نادیده گرفته شود، شناسایی کند. به‌عنوان مثال، هوش مصنوعی می‌تواند برای تجزیه و تحلیل ترافیک شبکه برای شناسایی الگوهای مشکوک مانند تعداد زیادی اتصال از یک آدرس IP استفاده شود.

۲ **پاسخ خودکار حادثه:** هوش مصنوعی می‌تواند مدیریت حوادث را خودکار کند، آسیب را به حداقل برساند و بازیابی سریع را امکان‌پذیر کند. این مسئله به این دلیل است که هوش مصنوعی بدون نیاز به دخالت انسان می‌تواند به سرعت تهدیدات را شناسایی کرده و به آنها پاسخ دهد. به‌عنوان مثال، هوش مصنوعی می‌تواند برای قرنطینه خودکار دستگاه‌های آلوده یا برای برگرداندن تغییراتی که توسط یک بازیگر مخرب ایجاد شده است، استفاده شود.

۳ **تجزیه و تحلیل رفتار و نظارت کاربر:** هوش مصنوعی قادر است فعالیت‌های مشکوک کاربران را شناسایی و در برابر تهدیدات داخلی محافظت کند؛ به این دلیل که هوش مصنوعی توان آن را دارد که رفتار عادی کاربر را یاد بگیرد و می‌تواند انحرافات از آن رفتار را شناسایی کند. به‌عنوان مثال، هوش مصنوعی را می‌توان برای تشخیص اینکه آیا کاربر در تلاش برای دسترسی به داده‌های حساس از یک مکان غیرمجاز است یا خیر، استفاده کرد.

۴ **هوش‌مصنوعی و پیش‌بینی تهدید:** هوش مصنوعی می‌تواند داده‌های اطلاعاتی تهدید را برای پیش‌بینی و جلوگیری از تهدیدات احتمالی آینده پردازش کند؛ به این دلیل که هوش مصنوعی قادر به آموختن درباره تهدیدات شناخته‌شده است و می‌تواند از این دانش برای شناسایی تهدیدهای بالقوه‌ای که شاید هنوز شناخته نشده‌اند، استفاده کند. برای مثال، از هوش مصنوعی می‌توان استفاده کرد تا پیش‌بینی شود کدام سیستم‌ها احتمالاً توسط یک عامل تهدید خاص هدف قرار می‌گیرند.

۵ **تشخیص نفوذ مبتنی بر ناهنجاری:** هوش مصنوعی انحرافات از رفتار عادی را تشخیص می‌دهد و حملات روز صفر را شناسایی می‌کند. به عنوان مثال، هوش مصنوعی تشخیص می‌دهد آیا یک سیستم رفتار غیرعادی دارد که نشانه‌ای از حمله روز صفر باشد یا نه.

۶ **تشخیص فیشینگ پیشرفته:** هوش مصنوعی ایمیل‌ها و URLها را تجزیه و تحلیل می‌کند تا تلاش‌های فیشینگ را از ارتباطات قانونی تشخیص دهد. چون هوش مصنوعی ویژگی‌های ایمیل‌های فیشینگ و آدرس‌های اینترنتی را می‌آموزد و می‌تواند از این دانش برای شناسایی تلاش‌های فیشینگ استفاده کند. به‌عنوان مثال، هوش مصنوعی می‌تواند تشخیص دهد آیا ایمیلی از طرف فرستنده مشکوک می‌آید یا آدرس اینترنتی به یک وب‌سایت مخرب وصل است.

چند ابزار کاربردی امنیت سایبری مبتنی بر هوش‌مصنوعی

براساس اطلاعات وب‌سایت دیتا ساینس، ابزارها و برنامه‌های کاربردی امنیت سایبری چندی مبتنی بر هوش مصنوعی وجود دارند، از جمله:

CrowdStrike Falcon: یک پلتفرم امنیت سایبری مبتنی بر هوش مصنوعی است که قابلیت‌های تشخیص، تجزیه و تحلیل و پاسخگویی تهدید را ارائه می‌دهد.

Palo Alto Networks Cortex XDR: یک پلتفرم امنیت سایبری مبتنی بر هوش مصنوعی است که دید و کنترل جامعی را بر کل محیط فناوری اطلاعات فراهم می‌کند.

IBM Security QRadar with Watson: یک پلتفرم امنیت سایبری مبتنی بر هوش مصنوعی است که اطلاعات تهدید، تجزیه و تحلیل و اتوماسیون را ارائه می‌دهد.

شکی نیست که آینده امنیت سایبری مبتنی بر هوش مصنوعی است؛ سازمان‌هایی که می‌خواهند در رقابت در فضای اینترنتی و نیز بهسازی و بهبود زیرساخت‌های خود پیشرو و پیش‌قدم باشند، باید روی راه‌حل‌های امنیت سایبری مبتنی بر هوش مصنوعی سرمایه‌گذاری کنند.

فعالان خصوصی

افزایش عرضه گوشت

عرضه گوشت قرمز در آذر نسبت به آبان ۱۳ درصد افزایش یافت. بخش زیادی از این رشد عرضه، به گوشت‌های منجمد وارداتی مربوط می‌شود که وزارت جهاد کشاورزی با هدف تنظیم بازار آنها را وارد کرده است. منصور پوریان، رئیس شورای تامین‌کنندگان دام کشور در گفت‌وگو با ایلنا از عرضه کافی گوشت قرمز در کشور خبر داد و گفت: در حال حاضر گوشت قرمز چه از نوع گوشت گرم تولید داخل و چه گوشت منجمد وارداتی به اندازه کافی عرضه می‌شود. او در تشریح قیمت گوشت قرمز اظهار کرد: قیمت گوشت‌های منجمد از ۳۰۰ هزار تومان در هر کیلو شروع می‌شود و تا ۴۰۰ هزار تومان ادامه دارد. قیمت گوشت قرمز گرم هم از ۳۵۰ هزار تومان شروع می‌شود و تا ۴۲۰ هزار تومان پیش می‌رود. او گفت: هر قدر به روزهای پایانی سال نزدیک‌تر می‌شویم شمار دام‌هایی که کشتار می‌شود افزایش می‌یابد و عرضه را تقویت می‌کند.

صادرات بی‌برنامه

بدون برنامه و هدف برخی محصولات کشاورزی را صادر می‌کنیم. سیدرضا نورانی، رئیس اتحادیه ملی محصولات کشاورزی به ایسنا گفت: باید ابتدا آمار دقیقی از تولید و مصرف داخل داشته باشیم و سپس برای صادرات برنامه‌ریزی کنیم. او در پاسخ به اینکه آیا صادرات بی‌رویه پیاز صحت دارد یا خیر؟ گفت: وقتی صادرات پیاز و گوجه‌فرنگی آزاد است، صادرکنندگان به دنبال بازار مناسب هستند تا محصولات خود را صادر کنند. در نتیجه بدون هدف و میزان دقیق با خریداران قراردادهایی منعقد می‌کنند. بعد از آنکه در داخل با کمبود مواجه شویم و برای مصرف‌کننده گرانی پیش بیاید، به یکباره تصمیمات شبانه و خلق‌الساعه گرفته می‌شود که یا صادرات به‌طور کل ممنوع یا عوارض ۱۰۰ درصدی برای آن وضع شود. او اضافه کرد: وضع عوارض ۱۰۰ درصدی برای صادرات پیاز باعث تنظیم بازار داخل نمی‌شود، بلکه فقط منجر به کندی صادرات می‌شود.

بهبود روند تامین نهاده

روند تامین کنجاله سویا بهبود یافته و ذرت به وفور در سامانه بازارگاه وجود دارد و از این جهت مشکلی وجود ندارد. محمدرضا صدیق‌پور، دبیرانجمن جوجه یکروزه ضمن اشاره به اینکه فروش جوجه بیش از ۲۴ هزار تومان مورد تایید نیست و گرانفروشی است، درباره بهبود روند تامین کنجاله سویا توضیح داد: ذرت به وفور در سامانه بازارگاه وجود داشته و از این جهت مشکلی وجود ندارد. او در پاسخ به چرایی افزایش قیمت جوجه یکروزه در بازار به ایسنا گفت: قیمت مصوب جوجه یکروزه در ابتدای سال ۱۵ هزار و ۹۰۰ تا ۱۶ هزار و ۹۰۰ تومان تعیین شد. ولی این قیمت برای ابتدای سال بود و بعد از آن چند مرحله قیمت نهاده‌ها و ریزمغذی‌ها تغییر پیدا کرد. او ادامه داد: براساس توافق با اتحادیه سراسری مرغداران قیمت تمام‌شده جوجه یکروزه تولید داخل به طور متوسط ۲۰ هزار تومان است که ۲۰ درصد هم نوسان دارد.