فناوری همراه

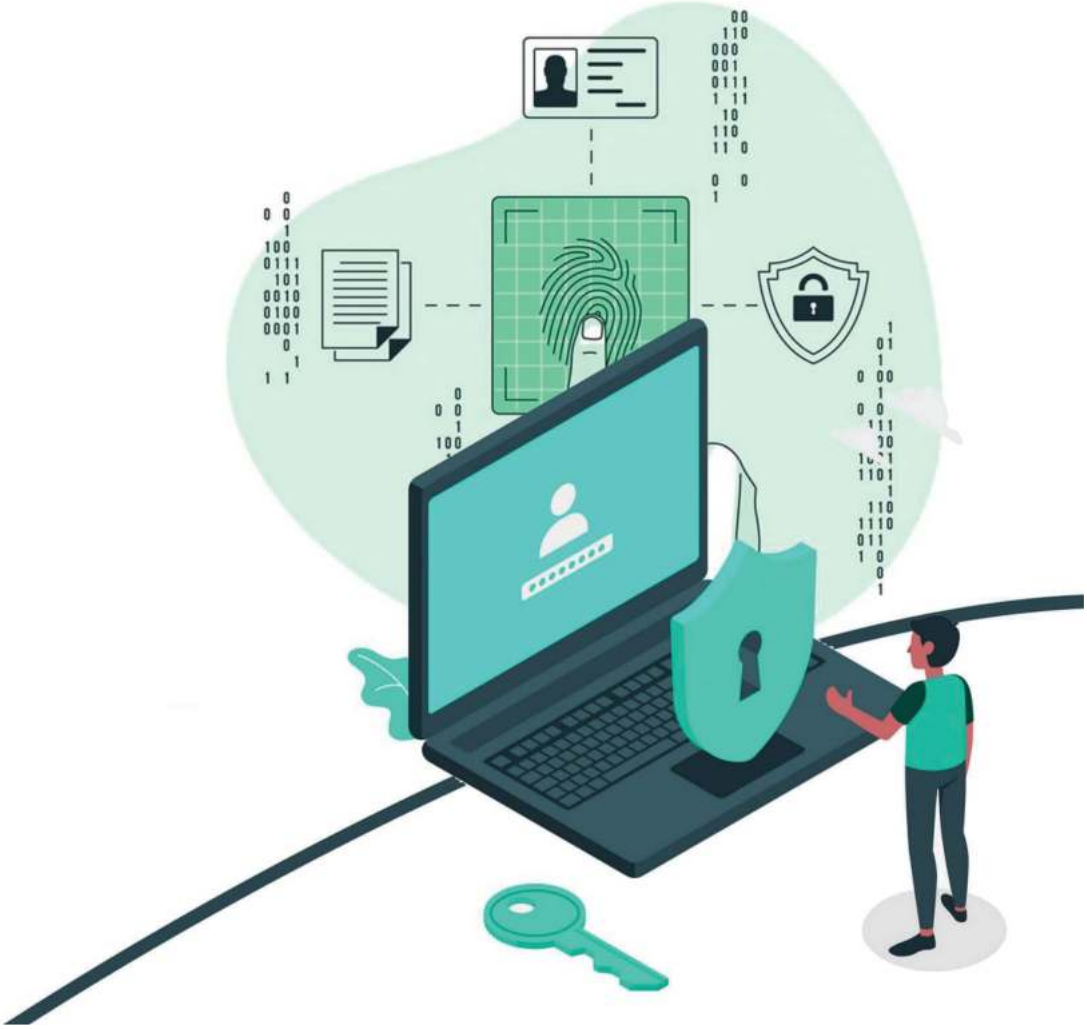
NO.۴

Fanavari hamrah

■ فصلنامه‌ی خبری تحلیلی

■ زمستان ۱۴۰۰ ■ شماره‌ی چهارم

فصلنامه‌ی «فناوری همراه» یکی از خروجی‌های رصد فناوری با هدف به اشتراک گذاری محتوای مرز دانش حوزه‌ی صنعت تلکام است



نوآوری، کلید آینده امن

هیچ کس حمله سایبری و تهدیدهای این حوزه را دوست ندارد، ولی وجود آنها یک چیز را برای ما به ارمغان می آورد: یک روحیه نوآور حقیقی! در واقع هر شرکت، مجموعه و نهادی برای آنکه بتواند از خودش در برابر تهدیدهای سایبری دفاع کند، باید پا به پای فناوری‌های نو و توسعه های آتی آنها دست به نوآوری در حوزه امنیت بزند.

هیچ کس حمله سایبری و تهدیدهای این حوزه را دوست ندارد، ولی وجود آنها یک چیز را برای ما به ارمغان می آورد: یک روحیه نـــوآور حقیقی! در واقع هر شرکت، مجموعه و نهادی برای آنکه بتواند از خودش در برابر تهدیدهای سایبری دفاع کند، باید پا به پای فناوری‌های نو و توسعه‌های آتی آنها دست به نوآوری در حوزه امنیت بزند.
طی دهه اخیر، نوآوری‌های حوزه امنیت ســـایبری یک زیرســـاخت جدید در دفاع در برابر تهدیدها پیش روی دولت‌ها و شبکه‌های کسب‌وکار قرار داده است. به ویژه با همه‌گیری ویروس کرونا و فراگیر شدن دورکاری، اهمیت یک نظام به‌روز و نوآور در حوزه امنیت سایبری بیش از هر زمان دیگری آشکار شده است. همچنین، سرعت تحول دیجیتال در کنار ظهور مداوم فناوری‌های نو، شمار حملات سایبری را طی سال‌های اخیر به طرز قابل توجهی افزایش داده و دلیل دیگری بر لزوم نوآوری در حوزه امنیت سایبری است.

این مهم در حیطه فعالیت اپراتورهای تلفن همراه که امروزه فراهم آورنده زیرساخت ارتباطی پرســـرعت و خدمات نوین دیجیتال هستند، بیش از هر زمان دیگری احساس می‌شود. به این ترتیب یکی از حیاتی‌ترین ویژگی‌های متخصصین امنیت در تمام حوزه‌ها از جمله اپراتورهای تلفن همراه آن است که در عمل نوآور باشند و به شکل آینده‌نگرانه و پیش‌دستانه در این حوزه فعالیت کنند.

نوآوری و امنیت سایبری

اگر بخواهیم به ارتباط نوآوری و امنیت سایبری بپردازیم، می‌توان گفت هر دو در خدمت هم هستند و خدمات متقابلی به یکدیگر می‌رســـانند. به بیان دیگر، آنچه از نوآوری در فضای فناوری‌ها و راهبردها رخ می‌دهد می‌تواند در کنـــار هم منجر به جهانی امن تر برای شـــبکه‌ها، کامپیوترها، داده، سیســـتم‌های مالی و غیره

شود. در واقع امنیت سایبری امروزه به یک ماموریت حیاتی برای دولت‌ها و سازمان‌ها در سرتاسر جهان تبدیل شده است. آنطور که پیمایش سال ۲۰۲۰ شرکت PWC نشان می‌دهد: «تقریبا تمام (۹۶درصد) سازمان‌های مورد مطالعه اعلام کرده‌اند که راهبرد جدیدی برای امنیت سایبری خود بعد از ظهور کووید-۱۹ تنظیم کرده‌اند. از این میان حدود نیمی از آنها امنیت سایبری را در تمام تصمیم‌های سازمان خود لحاظ کرده‌اند-که این رقم حدود ۲۵درصد بیشتر از رقم به دست آمده در پیمایش سال گذشته (۲۰۱۹) است.» بیایید کمی به این عدد بیاندیشیم. تقریبا نیمی از کسب‌وکارها موضوع امنیت سایبری را در تک تک تصمیمات خود لحاظ می کنند.

از سوی دیگر، این امنیت سایبری است که سازمان‌ها و کسب‌وکارها را توانمند می کند تا در جهان دیجیتال ایفای نقش کنند و دست به نوآوری های مختلف بزنند. در واقع اگر سازمانی نتواند در برابر تهدیدهای سایبری دفاع مناسبی داشته باشد، عملا امکان فعالیت خود را از دست می‌دهد. توانایی دولت‌ها و سازمان‌ها در این حوزه در نحوه عملکرد و کارآمدی آنها کاملا موثر است. آنطور که جیمز نان پرایس، مدیر خدمات ریسک سایبری دیلویت می گوید: «ما همه در یک قایق هستیم. دیجیتال و سایبر تقریبا در همه چیز رسوخ کرده؛ جهان، جهان دیجیتال است؛ جهان روی سرپنجه امنیت سایبری می چرخد.»

نظام نوآوری کشورها در امنیت سایبری

همان‌طور که پیش از این گفته شد امنیت سایبریِ موثر، نیازمند سطحی از نوآوری است که شیوه‌ها و فرآیندهای جاری را متحول کند. اما نوآوری اتفاقی نیست؛ نوآوری اغلب نتیجه سیستماتیک یک اکوسیستم فعال و پویاست. اکوسیستمی که هر سه جریان اصلی تحقیق و توسعه را که در شکل ۱ به تصویر کشیده شده است، حمایت کرده و بر اساس یک راهبرد کلان، آنها را در فرآیند تجاری‌سازی تبدیل به محصولات و خدماتی کند که در نتیجه آنها امنیت سایبری کشور ارتقا یابد.

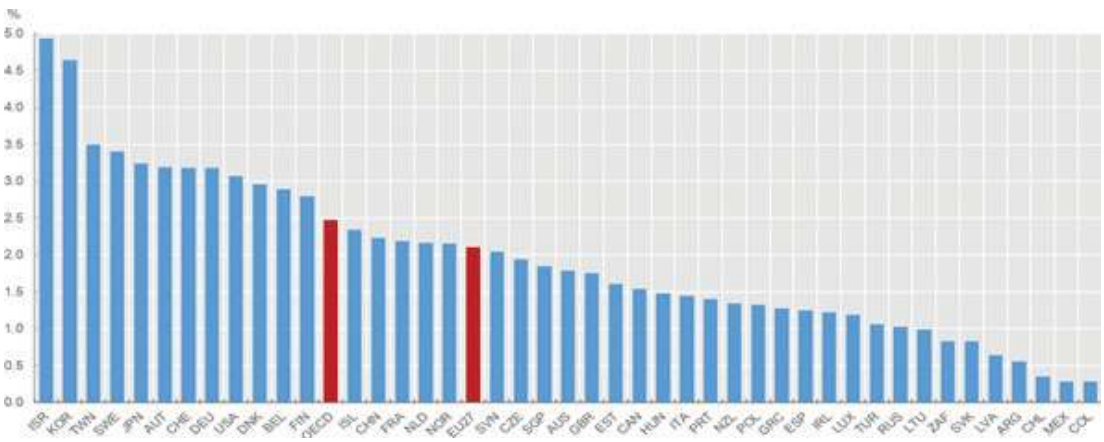
شکل۱- سه جریان اصلی R&D در کشورها

در حالی که بخش کسب‌وکار، اکثریت قریب به اتفاق تحقیقات کاربردی و توسعه تجربی در فناوری اطلاعات و ارتباطات را انجام می‌دهد، دانشگاه‌ها عمدتاً در تحقیقات پایه شرکت می کنند و نوآوری، تا حد زیادی به همکاری بین همه این کنشگران وابسته است: دولت، کسب‌وکارها و دانشگاه.

در اواخر دهه ۱۹۸۰ مفهوم نظام ملی نوآوری (NIS) در علم اقتصاد و مدیریت، منبعث از همین همکاری بین کنشگران مختلف در یک حوزه دانشی و فناورانه شکل گرفت. این مفهوم به ما اجازه می‌دهد تا کل محدوده فعالیت کنشگران و تعاملات بین آنها را در سطح ملی در کشورهای مختلف تحلیل کنیم.

در این بخش به راهبردهای نوآورانه و نظام نوآوری امنیت سایبری رژیم اشغالگر قدس و بریتانیا که در بین ۱۰ کشور برتر نوآوری در حوزه امنیت سایبری هستند (به ترتیب پنجم و هشتم) می‌پردازیم.

یکی از معیارهای رایج برای سنجش توان نوآوری کشورها، اندازه‌گیری بودجه تحقیق و توسعه به عنوان درصدی از تولید ناخالص داخلی (GDP) است. با این معیار، در شکل ۲، مقایسه‌ای بین اصطلاحا شدت تحقیق و توسعه در کشورهای سازمان همکاری و توسعه اقتصادی (OECD)، کشورهای عضو اتحادیه اروپا و سایر اقتصادهای جهان به تصویر کشیده شده است که



شکل۲- مقایسه شدت R&D در کشورهای عضو OECD و سایر اقتصادها در سال ۲۰۱۹- [۱]

تفاوت معناداری را در این معیار برای رژیم اشغالگر قدس نسبت به سایرین نشان می‌دهد. در حالی که به طور متوسط در سال ۲۰۱۹، کشورها حدود ۲ درصد از GDP خود را هزینه تحقیق و توسعه می‌کردند، این میزان برای رژیم صهیونیستی نزدیک به ۵ ثبت شده است. در کشور ما بر اساس اسناد بالادستی و نقشه جامع علمی کشور تا پایان سال ۱۴۰۴، باید چهار درصد تولید ناخالص داخلی را اعتبارات پژوهشی تشکیل دهد و سهم بخش خصوصی در تامین هزینه‌های تحقیقات هم، دو درصد تولید ناخالص داخلی درنظر گرفته شده است؛ هر چند در عمل و در بودجه پیشنهادی دولت‌ها در ادوار مختلف این میزان محقق نشده است.

در رژیم صهیونیستی، بخش قابل توجهی از این بودجه تحقیقاتی صرف موضوع امنیت سایبری می‌شود. یکی از مهم‌ترین دلایل این میزان بالای سرمایه‌گذاری در حوزه امنیت سایبری توسط رژیم اشغالگر قدس، حجم زیاد تهدیدات و حملات به آن است. گزارش شرکت مشاوره امنیت سایبری F۵ مدعی است در سال ۲۰۲۰، رژیم اشغالگر قدس بیش از هر منطقه‌ای در جهان، تحت حملات سایبری بوده است. فقط در سال ۲۰۱۵ بیش از ۱۰۰ استارتاپ امنیت سایبری در اسرائیل شکل گرفت که ۷۸ مورد از آنها حدود ۴۰۰ میلیون دلار جذب سرمایه کردند و به گفته رییس دفتر امنیت سایبری این رژیم (INCB) یک رکورد در این سال به لحاظ تعداد استارتاپ و جذب سرمایه ثبت شد. در همین سال هشت شرکت در حوزه امنیت سایبری توسط سرمایه گذاران خارجی در مجموع به مبلغ ۷۰۰ میلیون دلار خریداری شد.

به‌علاوه، صادرات شرکت‌های رژیم صهیونیستی از حدود ۲۰۰ میلیون دلار در دهه گذشته به حدود ۱۰ میلیارد دلار در سال ۲۰۲۰ بالغ شده است، یعنی پنج برابر و در رتبه دوم جهان پس از ایالات متحده. رکورد دیگر این رژیم مربوط به تعداد استارتاپ‌هاست. با حدود ۶۰۰۰ استارتاپ فعال در حوزه فناوری، تل‌آویو بهترین شهر خارج از ایالات متحده برای شرکت‌های نوپا نام گرفته است.

در سال ۲۰۱۰، نیروی ملی اقدام سایبری، سوالی را مبنی بر چگونگی افزایش انگیزه‌ها برای توسعه فناوری سایبری و تبدیل این رژیم به یکی از پنج اقتصاد برتر این حوزه مطرح کرد. پاسخی که ۸۰ متخصص شاغل در ۸ کمیته بعد از ۶ ماه بررسی موضوع به این سوال دادند، افزایش همکاری در اکوسیستم این رژیم شامل دولت، ارتش، دانشگاه و صنعت بود. این پیشنهاد مورد پذیرش قرار گرفت و راهبردهایی در این زمینه تدوین شد. همچنین با تاکید بر R&D در سایبر پیشرفته، اداره سایبر ملی (INBC) با دو ماموریت شکل گرفت: ارتقای تحقیق و توسعه در موضوع فضای سایبری و رشد صنعت سایبری بر پایه صادرات. به‌علاوه، از ابتدای سال ۲۰۱۷، پنج دانشگاه این رژیم با حمایت INBC مرکز تحقیقات سایبری تاسیس کردند. هرچند INBC تقریبا نیمی از بودجه این مراکز را تامین می‌کند اما تخصیص بودجه درون نهادی هر مرکز به صورت مستقل از دخالت دولتی و با معیارهای آکادمیک و تحقیقات عالی صورت می‌پذیرد تا به این ترتیب از دستوری شدن فرآیند نوآوری جلوگیری شود. این در حالی‌ست که این مراکز دانشگاهی به جز تحقیق در علوم و مهندسی، به تحقیقات در حوزه سیاستگذاری و تلاش برای ارتقای سطح دانش عمومی هم ورود کرده‌اند.

راهبردهای اصلی نظام نوآوری رژیم صهیونیستی در حوزه امنیت سایبری موارد ذیل را شامل می‌شود:

تسهیلگری دولت در حوزه امنیت سایبری

شاید بتوان گفت مهم‌ترین نقش را در نظام نوآوری امنیت سایبری این رژیم، دولت بر عهده دارد. پارک فناوری‌های پیشرفته شهر بیر-شوا به عنوان محل گردهم آوردن علایق، نیازها و توانمندی‌های بخش‌های دولتی و خصوصی در حوزه امنیت سایبری شناخته می‌شود. به‌علاوه، این رژیم با هدف جذب نیروهای متخصص و افراد مستعد در حوزه امنیت سایبری، موفق شده است شرکت‌های بین‌المللی مانند اوراکل، IBM و دویچه‌تلکام را متقاعد به ساخت مراکز تحقیقاتی خود در این پارک کند. همچنین آزمایشگاه‌های پیشرفته، مانند موسسه ملی تحقیقات سایبری، ادارات دولتی پاسخگوی فوری در این حوزه و بنگاه‌های سرمایه‌گذاری خطرپذیر (VCها) هم در این پارک مستقر هستند. یکی دیگر از تسهیل گری‌های دولتی در این حوزه، اعطای ۲۰ درصد از دستمزد نیروی متخصص امنیت سایبری در شرکت‌های خصوصی مستقر در پارک از سوی دولت است.

آموزش امنیت سایبری در مدارس و دانشگاه‌ها

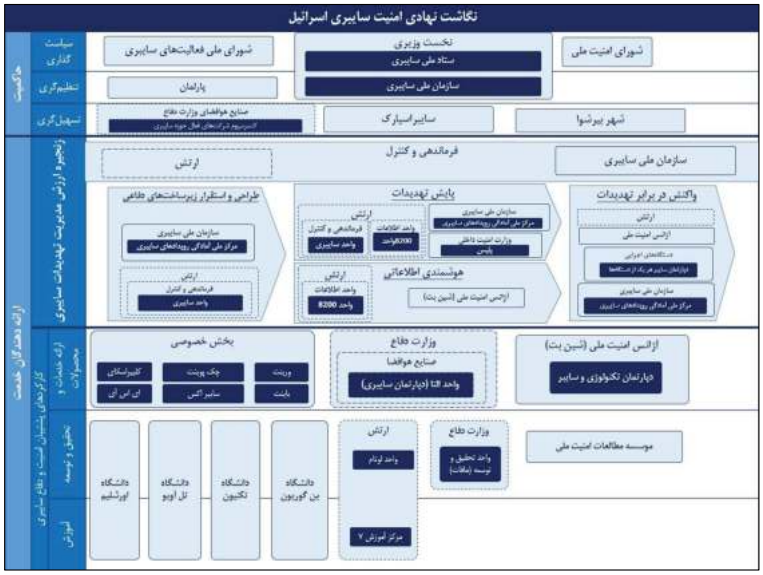
یکی از پایه‌ای‌ترین مبانی هر سیستم دفاع سایبری، موضوع آموزش و توانمند کردن جمعیت از نقطه نظر فناوری و تهدیدات این حوزه است. این آموزش‌ها در رژیم اشغالگر قدس از دوران راهنمایی آغاز می‌شود و در آزمون ورودی دوره دبیرستان هم مورد ارزیابی قرار می‌گیرد. به‌علاوه، تعداد زیادی رشته دانشگاهی در مقطع لیسانس در حوزه امنیت اینترنت هم ایجاد شده است.

آینده نگری

دولت رژیم صهیونیستی به کمک اتاق فکرهای متعدد خود، مصمم به تبدیل شدن به یک ابرقدرت حوزه امنیت سایبری است. آژانس فضایی این رژیم در کنار نیروی ملی اقدام سایبری و شورای ملی تحقیق و توسعه، اکوسیستمی را شکل داده‌اند تا در زمان افزایش تهدیدهای اینترنتی، مقامات را مطلع کرده و اطلاعات لازم را به آنها برساند. پیشدستی و آینده‌نگری یکی از موارد حیاتی در موفقیت امنیت سایبری کشورهاست.

تبدیل ارتش رژیم صهیونیستی به یک مرکز رشد استارتاپی

این رژیم، ماموریت‌هایی از جنس نقش‌آفرینی در اکوسیستم



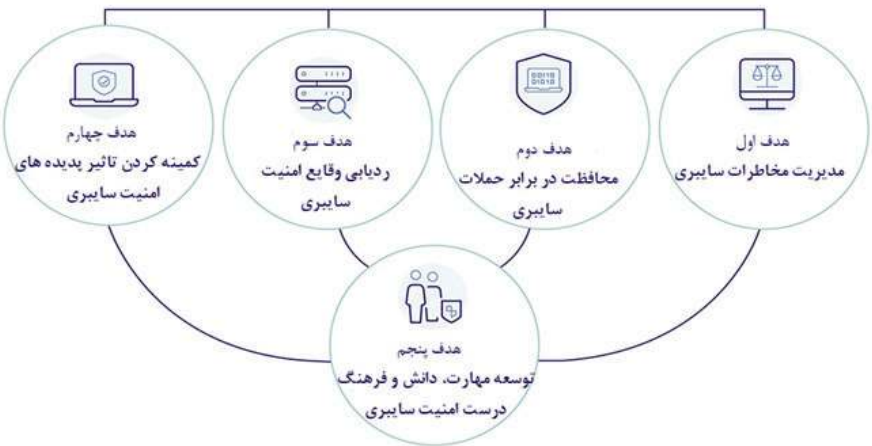
شکل ۳- نگاشت نهادی امنیت سایبری رژیم صهیونیستی -[۸]

نوآوری امنیت سایبری را به ارتش خود سپرده است تا به این ترتیب بخشی از بودجه این نهاد نظامی صرف نوآوری شود و از سوی دیگر بخشی از اهداف امنیتی در حوزه سایبر محقق شود. این راهبردها و ارتباط و تعاملات نهادها و کنشگران در نگاشت نهادی امنیت سایبری این رژیم در شکل ۳ به نمایش درآمده است.

گفتنی است یکی از شرکت‌های جهانی این رژیم با نام آلوت (Allot) راهکارهای هوشمندی شبکه و SECaaS را به تعدادی از اپراتورها و شرکت‌های مخابراتی در سراسر جهان می‌فروشد. نام اپراتورهای مشتری این شرکت به دلایل امنیتی فاش نمی‌شود اما راهکارهای ارائه شده از سوی این شرکت منجر به ارائه خدمات امنیت سایبری و کنترل والدین به مشترکین این اپراتورها شده است. اپراتورها و شرکت آلوت در درآمد ماهیانه ناشی از فروش این خدمات با هم شریک هستند.

در انگلستان، نخستین بار چند ماه بعد از رژیم صهیونیستی و در سال ۲۰۱۱، راهبرد ملی امنیت سایبری برای یک بازه پنج ساله تدوین شد. در این راهبرد مقرر شد در زیرساخت‌های ملی و حیاتی، دولت با متولیان و اپراتورهای این زیرساخت‌ها به صورت مشترک برنامه مدیریت مخاطرات سایبری را پیش برَد. به‌علاوه، مقرر شد کسب‌وکارها در هر حوزه و با هر اندازه‌ای بتوانند در قالب طرح‌های مختلف از جمله طرح الزامات سایبری (Cyber Essentials Scheme) به تناسب از راهنمایی متخصصین با حمایت دولت بهره‌مند شوند.

راهبرد دوم امنیت سایبری ملی (NCSS) که در سال ۲۰۱۶ تدوین شد و تا پایان ۲۰۲۱ ادامه داشت، توانست حدود ۲ میلیارد دلار در اقدامات تحولی جذب سرمایه کند. این حجم از سرمایه‌گذاری عجیب و بی‌دلیل نیست اگر بدانید فقط در بازه سپتامبر ۲۰۲۰ تا آگوست ۲۰۲۱، تعداد ۷۷۷ حمله سایبری در این کشور انجام شد که ۴۰ درصد حملات به بخش‌های دولتی بوده است. به دلیل همین تهدیدهای فزاینده، دولت انگلستان برنامه‌هایی را برای راهبرد پنج ساله این کشور در سال ۲۰۲۱



شکل ۴- اهداف راهبرد امنیت سایبری ۲۰۲۱ انگلستان -[۴]

تدوین کرد تا کشور را به لحاظ امنیت سایبری، منطبق بر قوانین و پاسخگو کند.

بر اساس راهبرد ۲۰۲۱ امنیت سایبری انگلستان، مقرر شد تمام دستگاه‌های دولتی در برابر آسیب‌ها و حملات تا پیش از سال ۲۰۳۰ تاب‌آور باشند. پنج هدف این راهبرد کلان که سال گذشته مصوب شد در شکل ۴ به تصویر کشیده شده است.

به‌علاوه، این راهبرد شامل پنج اقدام اولویت‌دار بر اساس پنج هدف اصلی برای حصول به دستاوردهای مد نظر دولت تا سال ۲۰۲۵ به شرح زیر است:

رکن ۱- تقویت اکوسیستم سایبری کشور

این رکن از راهبرد با در پی گرفتن یک رویکرد کل‌نگر به جامعه، متمرکز بر بهره‌مندی بخش‌های مختلف کشور از توسعه بخش امنیت سایبری است. منطبق با هدف شماره ۵، افزایش مهارت‌ها و توسعه استعدادهای جامعه و حصول اطمینان از تقویت و تنوع نیروی کار سایبری از دیگر اقداماتی است که در این رکن راهبرد قابل تعقیب است. تشکیل هیات مشورتی سایبر ملی متشکل از رهبران ارشد فعال در بخش خصوصی، برای به چالش کشیدن، حمایت و آگاه‌سازی رویکرد دولتی به این حوزه، از اقدامات صورت گرفته در این بخش است.

رکن ۲- ایجاد یک کشور دیجیتال تاب‌آور و موفق

غایت این رکن، کاهش مخاطرات سایبری است تا کسب‌وکارها بتوانند از مزایای اقتصادی فناوری دیجیتال را حداکثر بهره را ببرند و شهروندان هم امن‌تر و مطمئن‌تر، تبادل داده کنند.

این رکن راهبردی سه جنبه کلیدی را برای مفهوم تاب‌آوری سایبری تعیین می‌کند: (۱) مخاطره سایبری باید فهم شود. (۲) اقداماتی برای ایمن‌سازی سامانه‌ها و پیشگیری و مقاومت در برابر حملات سایبری انجام شود. و (۳) دولت و سازمان‌ها برای به حداقل رساندن تأثیر حملاتی که اتفاق می‌افتد، آماده و تاب‌آور باشند. این رکن متمرکز بر تغییرات رفتاری با هدف ارتقای امنیت سایبری است که ممکن است این امر شامل قانون‌گذاری هدفمند برای بخش‌هایی باشد که پتانسیل حمله سایبری به آنها بیشتر است.

بر اساس این رکن، دولت اذعان دارد که باید رهبری امنیت سایبری کشور را بر عهده گرفته و امنیت سایبری بخش دولتی را به عنوان بهترین نمونه عملی (Best Practice) در کشور تقویت کند. همچنین دولت باید بر فرآیندهای مدیریت ریسک موثرتر، پاسخگویی بیشتر، سیستم‌ها، شبکه‌ها و خدمات نظارتی جامع‌تر، واکنش سریع‌تر و مقیاس‌پذیر به حوادث و سرمایه‌گذاری بیشتر در تقویت مهارت‌ها، دانش و فرهنگ، متمرکز شود. برای این مهم، قدم آغازین می‌تواند مشاوره در مورد اصلاحات در قوانین شبکه و سیستم های اطلاعاتی، اجرای چارچوب امنیتی جدید برای شرکت‌های مخابراتی و اپراتورهای تلفن همراه انگلستان و توسعه یک چارچوب قانونی متناسب برای اطمینان از اینکه سامانه انرژی هوشمند آینده انگلستان در برابر تهدیدات سایبری ایمن و مقاوم است، باشد.

رکن ۳- حرکت به سمت فناوری‌های پیشرو و حیاتی برای ایجاد یک قدرت سایبری

این رکن تصدیق می‌کند که برای انگلستان، دنبال کردن مزیت استراتژیک در علم، فناوری و نوآوری، پیش‌شرطی برای دستیابی به اهداف گسترده‌تر به عنوان یک قدرت سایبری خواهد بود.

برای ایجاد و حفظ مزیت رقابتی در فناوری‌های مرتبط با امنیت سایبری، گسترش قابلیت‌های تحقیقات و نوآوری انگلستان (از جمله مرکز ملی امنیت سایبری (NCSC)) با تمرکز بر فناوری‌های نوظهور مورد نظر است تا رویکردهایی ترویج شود که امنیت را در فناوری‌های جدید به صورت «ایمن در طراحی» (Secure-by-Design) فراهم می‌کند. همچنین بر این اساس، دو لایحه زیرساخت‌های امنیت محصول و زیرساخت ارتباطات برای اعمال حداقل استانداردهای امنیتی در همه محصولات جدید قابل اتصال که در انگلستان فروخته می‌شوند، اجرا خواهد شد.

رکن ۴- رهبری جهانی

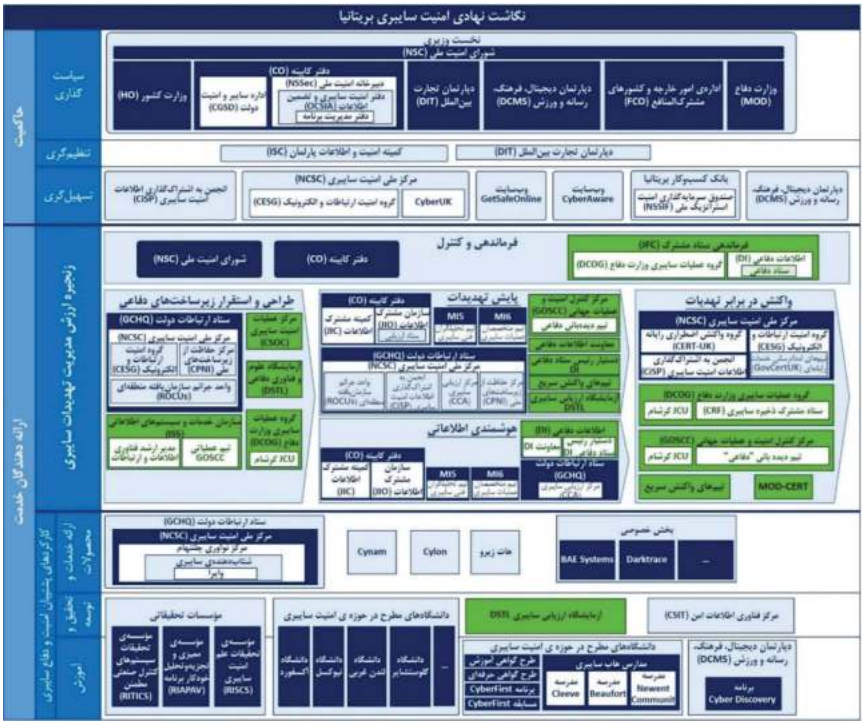
مطابق این رکن، فعالیت انگلستان در فضای سایبری یکی از ملاحظات کلیدی در سیاست خارجی دولت خواهد بود. راهبرد کلان امنیت سایبری انگلستان با نگاهی واحد و یکپارچه به اجزای دولت، متعهد به سرمایه‌گذاری و بهره‌مندی بیشتر از صنعت و دانشگاه است. تمرکز بر حفاظت از زنجیره‌های تامین بین‌المللی و زیرساخت‌های حیاتی، پیشبرد استفاده امن از فناوری‌های دیجیتال و همکاری با شرکای صنعتی از دیگر اقدامات کلیدی مرتبط با این رکن است. در همین چارچوب، همکاری انگلستان با سازمان‌ها و شراکت‌های چندجانبه از جمله سازمان ملل، فایو آیز (اتحادیه امنیتی و اطلاعاتی شامل پنج کشور از جمله انگلستان)، ناتو و G۷ ادامه خواهد یافت.

به علاوه، ایجاد یک کمپین بین‌المللی بهداشت سایبری برای حفاظت از منافع و شهروندان انگلستان در خارج از کشور از دیگر برنامه‌های این راهبرد است تا با تعریف ماموریتی بین‌المللی، هزینه فعالیت‌های مخرب مانند هک، سرقت داده و باج افزار را افزایش دهد.

رکن ۵- ارتقای امنیت کشور در فضای سایبری و از طریق امنیت سایبری

این رکن شامل نگرانی‌هایی در مورد تهدیدات در فضای سایبری (به عنوان مثال برای فعالیت‌های آنلاین)، تهدیداتی برای انگلستان و شرکا از طریق فضای سایبری (به عنوان مثال برای شبکه زیرساخت‌های حیاتی ملی)، و تهدیداتی برای عملکرد زیرساخت‌های سایبری بین‌المللی است.

بر این اساس، دولت از طریق برنامه آفند و پدافند سایبری ملی، روی قابلیت‌های سایبری آفندی هم سرمایه‌گذاری کرده و با ایجاد قابلیت‌های تشخیص و ارزیابی تهدید در سطح جهانی، به دنبال مختل کردن و افزایش هزینه میزبانی فعالیت‌های سایبری مجرمانه و خصمانه برای سایر کشورها است. مرکز ملی امنیت



شکل ۵- نگاشت نهادی امنیت سایبری انگلستان- [۷]

سایبری (NCSC) همچنین در حال بررسی راه‌هایی برای ردیابی تهدیدات در حال ظهور است. این مرکز در این زمینه با موسسه آلن تورینگ (Alan Turing Institute) برای استفاده از یادگیری ماشینی برای شناسایی انواع خاصی از حملات سایبری همکاری می‌کند.

ارکان راهبردی و اقدامات کلیدی اشاره شده و نقش نهادهای مختلف انگلستان در پیشبرد اهداف راهبردی این کشور را در نگاشت نهادی امنیت سایبری در شکل ۵ می‌توان مشاهده کرد.

نقش اپراتورهای شبکه تلفن همراه در امنیت سایبری

امروزه صنعت تلکام به عمق فعالیت‌های روزمره افراد، کسب‌وکارها و دولت‌ها نفوذ کرده است. مخابرات، تقریباً در همه شئونات زندگی امروز حضور دارد و پایه‌ای را شکل داده که همه ارکان حیاتی دیگر جامعه روی آن زیرساخت عمل می‌کنند. همین امر موجب جذابیت این صنعت برای حمله‌کنندگان سایبری است.

به‌علاوه، همه‌گیری کرونا نشان داد که چگونه بحران‌ها می‌توانند مردم را به استفاده هرچه بیشتر از راه‌حل‌های اینترنتی و موبایل کنند. این وضعیت برای اپراتورهای شبکه همراه، محرکی برای کسب‌وکار بهتر بود. با این حال، اتکای فزاینده به تلفن همراه می‌تواند شمشیر دولبه‌ای برای اپراتورها و مشتریان سازمانی آنها باشد. افزایش نقاط پایانی سلولی (از جمله دستگاه‌های متصل به اینترنت اشیا) و استفاده روزافزون از آنها، با انفجاری در حملات سایبری، و حمله به شبکه‌های مخابراتی و اینترنتی عمومی و خصوصی، همراه شده است.

سال ۲۰۲۱، GSMA سومین گزارش سالیانه تهدیدات اپراتورهای شبکه را منتشر کرد. بر اساس این گزارش، از سال ۲۰۲۰ و با شروع همه‌گیری کرونا و افزایش استفاده از فضای مجازی، تهدیدها و حملات به شبکه‌های موبایل بالا گرفت و در سال بعد هم ادامه یافت. این مخاطرات، در حالی شدت گرفته است که حوزه‌های مخاطرات سنتی همچنان روی اپراتورها فشار وارد می‌کند.

شبکه‌های تلفن همراه ثابت کرده‌اند که در میزان ترافیک و خدماتی که بر عهده دارند و موجب افزایش عملیات‌هایشان شده، بسیار تاب‌آور هستند. طی دو سال گذشته، شبکه های تلفن همراه از سلامت اقتصادی و اجتماعی جامعه که با کووید-۱۹ به چالش کشیده شد، حمایت کردند؛ وظیفه‌ای سنگین که انگیزه‌های صنعت را برای شناسایی و کاهش تهدیدات امنیتی، قوت بخشید. بسیاری از تهدیدات امنیتی شبکه قابل پیش‌بینی هستند و با پیشگیری مناسب، اقدامات ادامه‌دار و هوشیاری، می‌توان میزان خطر آنها را کاهش داد. ترندهای فعلی که به سمت شبکه‌های بازتر و مجازی‌تر است، روی رویکردهای امنیتی هم اثرگذار بوده است. رویکردهای جدید امنیت را از طریق مردم، فرآیندها و فناوری و از طریق چرخه کامل عمر از تعریف خدمات، استقرار، عملیات و در نهایت انحلال، مدیریت می‌کند.

صنعت شبکه های مخابراتی سیار می‌داند که با هیچ تهدید امنیتی نمی‌توان به صورت مجزا مقابله کرد و تهدیدکنندگان به به سوءاستفاده از آسیب‌پذیری‌ها در فناوری‌ها و فرآیندهای مستقر

شکل ۶- مهم‌ترین موضوعات امنیتی صنعت تلکام در سال ۲۰۲۱ -[۶]

شـــده ادامه خواهند داد تا به هدف خود برسند. در مواجهه با این تهدید مداوم، توسعه یک برنامه گسترده بسیار حیاتی است.

آژانس اتحادیه اروپا برای امنیت ســـایبری (ENISA) با هدف درک تهدیدهای در حال تحول پیش روی صنعت، گزارش‌های جامعی در مورد تهدید ســـایبری و بخصوص 5G منتشر کرده است. بر این اساس، امنیت شبکه‌های مخابرات سیار باید پیوسته در حال تکامل بوده و به شـــکلی پویا و نوآورانه با تغییرات ایجاد شده در تهدیدها خود را وفق دهد. به علاوه، مهم‌ترین موضوعات امنیتی صنعت برای ســـال ۲۰۲۱، موارد ذکر شـــده در شکل ۶ اعلام شد.

جمع‌بندی و پیشنهاد

دیدیم که نوآوری در موضوع امنیت سایبری به اندازه خود امنیت سایبری مهم و حیاتی است. این امر به دلیل سرعت تغییرات فناورانه در هر دو سوی امنیت سایبری -هم از سمت سازمان‌ها و کسب‌وکارهایی که به دنبال امن شدن داده و شبکه خود هستند و هم از سمت تهدیدکنندگان و تخریبگران- است. اما نکته اینجاست که تهدیدکنندگان اغلب از روش‌ها و فناوری‌های پیشرفته‌تری استفاده می‌کنند و فناوری امنیت سایبری و کنشگران این حوزه را مجبور به تغییر می‌کنند. تغییری که جز با نوآوری قابل حصول نخواهد بود.

همچنین دیدیم که کشورها از طریق رویکرد نوآوری باز و با ایجاد سازوکارهای همکاری در اکوسیستم برای تقویت امنیت سایبری ملی خود تلاش می‌کنند. با بررسی دو مورد از موفق‌ترین نظام‌های ملی نوآوری در حوزه امنیت سایبری (رژیم صهیونیستی و انگلستان) و بررسی راهبردهای کلان آنها در این حوزه، در مجموع می‌توان توسعه سازوکار همکاری بخش‌های دولتی و خصوصی، توسعه سازوکار همکاری بخش نظامی و صنعت، تدوین برنامه پابرجای تحقیق و توسعه و توسعه بازارها را به عنوان اصلی‌ترین اقدامات راهبردی با هدف نوآوری در امنیت سایبری با رویکرد سیستمی و باز در نظر گرفت.

همه اینها در حالی است که شبکه های تلفن همراه نسل بعدی، باید سرعت های بالاتر و تاخیر کمتری را ارائه دهند و به این ترتیب نحوه استفاده جامعه از فناوری را به طرز چشمگیری تغییر خواهند داد. از آنجا که این سطح از اتصال، چالش‌ها و خطرات جدیدی را به همراه دارد، رهبران امنیت سایبری اپراتورها در خط مقدم برای نوآوری و فرصت‌های جذاب توسعه برای افزایش ایمنی و امنیت برای تمام ارکان جامعه و مشتریان سازمانی خود خواهند بود. امری که بر لزوم ارتباط نظام‌مند بخش امنیت شبکه‌های تلفن همراه با اکوسیستم نوآوری و شرکت‌های دانش‌بنیان و نوآفرین تاکید دارد.

منابع:

[1]OECD Main Science and Technology Indicators 2021- www.oecd.org/sti

[2] Security through innovation. Cybersecurity sector as a driving force in the national

[3] economic development- The Kosciuszko Institute 2017

[4] Policy paper-Government Cyber Security Strategy: 2022 to 2030-Updated 17 February 2022

[5] Guide to Developing a National Cybersecurity Strategy Strategic Engagement in Cybersecurity 2nd Edition 2021

[6] Mobile Telecommunications Security Landscape- GSMA 2021

[۷] کتاب نظام مدیریت امنیت سایبری انگلیس- صاافتا- ۱۳۹۷

[۸] کتاب نظام مدیریت امنیت سایبری رژیم صهیونیستی- صاافتا- ۱۳۹۷

مصاحبه با مدیرعامل شرکت نامدار، هولدینگ امنیت فاوا زیرمجموعه همراه اول

امنیت فاوا، امیدها و انتظارها

در این شماره پای صحبت‌های مهندس رضا نوری عضو هیات مدیره و مدیرعامل شرکت توسعه امن فناوری نامدار -بزرگترین هولدینگ امنیت فاوا کشور- نشسته‌ایم. مهندس نوری که خود دانش آموخته فناوری اطلاعات و ارتباطات است و سابقه طولانی در بخش امنیت فناوری اطلاعات و ارتباطات کشور دارد، ضمن معرفی هولدینگ نامدار، به تبیین چالش‌ها و امیدها و انتظارها در این بخش پرداخته است.

لطفا شـــرکت نامدار را برای مخاطبین نشریه به اختصار معرفی کنید.

شـرکت توسـعه امن فناوری نامـدار با رویکـرد مدیریت تحقیقات حـوزه امنیت فـاوا و ارائـه راهکارهـا، برنامه‌ها و سیاسـت‌های توسـعه فناوری‌های امنیتی و همچنین جهت‌دهی و انتخاب روش‌های مناسـب برای دسـتیابی به فنـاوری، به عنـوان یکـی از شـرکت‌های زیرمجموعه شـرکت ارتباطات سـیار ایـران (همـراه اول) ثبت شـده است.

این شـرکت در سـال ۱۳۹۲ با هـدف ایجاد یـک محیط تخصصـی و پویـا بـرای فعالیـت در زمینه‌هـای مختلف امنیـت فنـاوری اطلاعـات و ارتباطـات و اکوسیسـتم دیجیتال کشـور، توسـط همـراه اول ایجاد شـد. متعاقبا در سـال ۱۳۹۶ و در راسـتای هم‌افزایی و افزایش سـطح فنـاوری، هولدینـگ نامـدار ثبـت شـد و بـا نـام تجاری نامدار کـه شـامل شـرکت‌های دانش بنیـان؛ امـن افزار گستر شریف، پژوهشـکده پارسا شریف، پیشـتازان امن کاوی عمـاد، فنـاوران هویـت الکترونیکی امـن (هویتا)، زیسـت بـوم مجـازی درسـا و یافتـار پژوهـان پیشـتاز رایانش اسـت، شـروع بـه فعالیـت کرد.

شـرکت‌های زیرمجموعـه هولدینـگ تخصصـی نامدار، همسـو بـا اهـداف کلان ایـن مجموعـه، بـه سـه گـروه مشـتری شـامل همـراه اول، شـرکت‌های زیرمجموعـه همـراه اول و همچنیـن پـروژه هـای ملـی، محصـول و خدمـات ارائـه می کننـد.

شرکت های که اشاره کردید هر کدام چه ماموریت هایی دارند و در چه حوزه‌هایی فعالیت می کنند؟

در حـال حاضـر شـرکت هـای تابعـه نامـدار بـا ایـن ماموریت‌هـا سـازماندهی شـده‌اند:

- شـرکت یافتـار پژوهـان پیشـتاز رایانـش: ارائـه محصـولات و خدمـات اعمـال خـط مشـی شـبکه‌های بـزرگ و اپراتورهـای ارتباطـی همـراه و ثابـت؛
- شـرکت امن افزار گسـتر شـریف: تولیـد محصولات امن‌سـازی شـبکه، ارائه راهکارهای جامع امنیت فضای مجازی سـازمان ها؛
- شـرکت پیشـتازان امن کاوی عماد: ارزیابی امنیتی و امن سـازی؛
- شـرکت فنـاوران هویـت الکترونیکـی امـن: تولیـد محصـولات و ارایـه خدمـات احـراز هویـت و امضـای دیجیتـال و
- شـرکت زیسـت بـوم فضـای مجـازی درسـا: تولید محتـوا

رویکرد شرکت نامدار در خصوص بومی سازی فناوری‌های پرکاربرد در صنعت کشور چیست؟

تمرکـز هولدینگ نامدار بـر حوزه تحقیـق و توسـعه و نـوآوری است. از سوی دیگر، بومی‌سـازی تجهیـزات و سـامانه‌های اسـتراتژیک امنیتـی در حوزه ICT بـا کاربـری در سـطح ملـی از اصلی‌ترین وظایـف ایـن شـرکت است.

به‌علاوه، پروژه‌های فناورانه این هولدینگ بـا راهبـری و اجـرای تیـم‌های علمـی و اجرایـی شـرکت‌های دانش‌بنیان تابعه آن و مبتنی بر ظرفیـت شـرکت‌های خـلاق و نـوآور کـه همگـی در ناحیـه نوآوری شـریف اسـتقرار دارنـد انجـام می‌شـود.

بنابرایـن می‌تـوان گفـت عمـده فعالیـت این شـرکت چـه در زمینه پژوهـش و جـذب فنـاوری هـای نوظهور و اجـرای پـروژه هـا و تسـت و ارزیابـی فناوری‌هـا و چـه در زمینـه طراحـی و توسـعه امنیـت تجهیـزات، سـامانه‌ها و پلتفرم‌هـای ICT و بومی‌سـازی محصولات اسـتراتژیک، همگی بـا اولویت‌بندی نیازهـای گروه‌های مشـتریان و با حمایت از تولیدکننـدگان توانمند داخلی و شـرکت‌های نوپـای صاحـب فناوری‌های نویـن انجام می شـود.

تا کنون چه اقدامات کلیدی و پروژه‌هایی در شرکت نامدار انجام شده و چه دستاوردهایی حاصل شده است؟

در موضـوع توسـعه بومی سـازی محصـول و راهکارهای احـراز هویـت، قـرارداد موبایـل کانکـت، قـرارداد ایجاد مرکـز میانـی بانـک مرکـزی (همـکاری بـا خدمـات انفورماتیـک) و قـرارداد ایجـاد مرکـز میانـی بانک‌هـای عامل را در دسـت داریـم. در حوزه ارائه خدمـات نوآورانه امنیـت ابـری، قـرارداد خدمـات امنیـت مدیریت شـده (MSSP) و توسـعه و تولیـد پلتفـرم SECaaS از دسـتاوردهای شـرکت اسـت. همچنیـن بـا هـدف توسـعه همکاری با شـرکت‌های گـروه همـراه اول، طرح هفت‌گانـه امنیـت در شـرکت‌های مبین‌نـت، افرانـت، نـاک، بهسـا، سـتاره اول، بهارتل، رفـاه اول، کسـب‌وکار هوشـمند و جیرینـگ انجـام شـده اسـت.

بـه عـلاوه بـا هـدف تامیـن نیازمندی‌هـای پروژه‌هـای زیرسـاختی شـبکه ملی اطلاعات، دو موضوع موتور جستجو ملی ذره بین و اینترنت خانـواده (Parent of Control) در شـرکت نامـدار پیگیری می‌شـود.

در کنـار اینهـا، بـازوی اجرایـی مرکـز کاشـف در انجـام آزمون‌های ارزیابـی امنیت بانـک های کشـور و ممیزی آن بـا هـدف توسـعه بـازار بانک‌های کشـور، مشـارکت بـا معاونـت نـوآوری ریاسـت جمهوری بـرای صـادرات

محصولات با هدف توسعه صادرات محصولات بومی و آسیب شناسی هک و نفوذ به وزارتخانه‌ها و سازمان‌های دولتی از دیگر اقدامات و دستاوردهای این شرکت بوده است.

آیا موضوع نوآوری و رصد فناوری‌های آینده در شرکت نامدار پیگیری می‌شود؟

بله. در هولدینگ نامدار، رویکرد نوآوری‌های درون و برون سازمانی (نظام نوآوری باز) و حمایت از استارت‌آپ ها و شرکت‌های دانش‌بنیان مد نظر قرار گرفته است. همچنین در این مجموعه، رصد فناوری به عنوان یکی از وظایف و مأموریت‌های اصلی تعریف شده است. شناسایی فناوری‌های نوظهور و اطلاع از آخرین وضعیت فناوری‌های موجود، توسعه محصولات و خدمات فعلی و ارائه محصولات و خدمات نوین و سازماندهی حوزه پژوهش و فناوری از جمله اقدامات این مجموعه است تا بتواند به کمک فرآیند مدیریت سبد فناوری، شناسایی و اولویت‌بندی در فناوری زیست بوم ICT را محقق کند.

وضعیت کشور را در پیشبرد پروژه‌های امنیت فاوا چگونه ارزیابی می کنید؟

هرچند کارهای بسیار خوب و ارزشمندی در این حوزه در کشور انجام شده است، اما ما در کشور از دو موضوع رنج می‌بریم، یکی نبود نگاه همه‌جانبه و سیستماتیک به موضوع امنیت فاوا و دوم، کمبود سرمایه‌گذاری در این حوزه. در واقع تعریف امنیت فاوا هنوز خوب شکل نگرفته است. یعنی مثلا در یک سازمان و مجموعه بزرگ، نباید فقط یک اداره و معاونت دغدغه امنیت فاوا را داشته باشد و این دغدغه باید در تمام ارکان سازمان و پروژه‌ها تسری پیدا کند. مشکل دیگری که وجود دارد کندی بوروکراتیکی است که گریبانگیر سازمان‌های کشور است و به هیچ عنوان با فوریت موضوعات امنیتی همخوانی ندارد.

از طرف دیگر ما از نبود سرمایه‌گذاری مناسب در بخش امنیت رنج می‌بریم. حوزه امنیت در کشور تا حد زیادی مغفول مانده است. وقتی طرح‌های بزرگ با تعداد بسیار بالای کلاینت تعریف می‌شود، این انتظار وجود دارد که یک زیرساخت امنیتی مناسب در همین حد برای این موضوع دیده شود.

به عنوان نمونه می توان به پلتفرم‌های نوظهور در فناوری‌های صنعتی کشور از جمله IIoT اشاره کرد. اگر این پلتفرم وارد صنایعی مانند خودروسازی کشور شود، چند ده میلیون کاربر خواهد داشت و لازم است سرمایه‌گذاری کلانی در بخش امنیت صورت پذیرد. در واقع بخش امنیت هر کار بزرگی باید متناسب با بزرگی آن طرح باشد.

اگر سرمایه‌گذاری مناسب در پروژه‌های امنیت انجام شود، آیا توانمندی لازم به ویژه به لحاظ نیروی انسانی در کشور وجود دارد تا بومی‌سازی در این حوزه صورت گیرد؟

ما ابلاغ حاکمیتی برای استفاده از محصولات بومی در حوزه امنیت داریم. پس وظیفه داریم شرایط را برای تحقق این امر مهیا کنیم. البته موضوع کمبود نیروی انسانی در حوزه امنیت فاوا و شبکه، یک موضوع جهانی است و در جهان با عنوان The Cybersecurity Talent Deficit شناخته می‌شود. با این حال، ما ظرفیت بسیار خوبی در بخش شرکت‌های دانش‌بنیان در این حوزه داریم که هولدینگ نامدار هم با زبده‌ترین شرکت های دانش‌بنیان در این بخش که همگی در ناحیه نوآوری شریف مستقر هستند، همکاری دارد. در واقع کلیه شرکت‌های ما دانش‌بنیان هستند.

اما یک کمبود جدی در حوزه آموزش در این بخش هم در کشور وجود دارد که باید به همت آموزش عالی رفع شود. در همراه اول هم ما با همکاری آکادمی همراه، بمنظور جذب کارآموز در حوزه امنیت همکاری داریم تا منابع انسانی مناسب را در اختیار ما و شرکت‌های دانش‌بنیان تابعه قرار دهند. ما حتی این امکان را داریم که دانشجویان مستعد را بورسیه نماییم تا در حین تحصیل کار را فراگیرند.

در بومی سازی خدمات و محصولات امنیتی با چه کمبودهای دیگری روبرو هستیم؟

یکی از بزرگترین چالش‌ها این است که تقریبا هر چه در کشور انجام شده، پروژه‌های امنیت IT است و پروژه امنیت CT خیلی کم تعریف شده است. این یکی از ضعف‌ها است که باید هرچه زودتر به سمت رفع آن گام برداریم.

خوشبختانه در حال حاضر محصولات توسعه داده شده بومی در کشور، قابل رقابت با Top۱۰ دنیا هستند و به لحاظ دانش فنی حقیقتا در جای خوبی ایستاده‌ایم اما لازم است برای ترافیک‌های بالا و محصولاتی در مقیاس ترافیک میلیونی سرمایه‌گذاری‌های کلانی در کشور انجام شود تا به نقطه مطمئنی در این حوزه برسیم.

چه ظرفیت‌هایی برای تعامل متقابل بین شرکت نامدار و

مرکز تحقیق و توسعه همراه اول وجود دارد؟

علاوه بر ظرفیت‌های فنی شرکت نامدار و انجام پروژه‌هایی مثل موبایل کانکت که هم‌اکنون با شرکت هویتا ، پروژه AI با شرکت یافتار، پروژه CGNAT با شرکت امن افزار و... در دست داریم، هولدینگ نامدار ظرفیت‌های ستادی برای مدیریت پروژه‌های کلان را هم دارد. در واقع در خصوص پروژه‌های حوزه امنیت ما می‌توانیم به عنوان یک شرکت صددرصدیِ همراه اول، اصطلاحا بازوی مدیریتی برای ورود به این پروژه‌ها باشیم و در پیشبرد آنها به مرکز تحقیق و توسعه همراه اول کمک کنیم و واسط پیگیری و انجام توافق‌نامه با دانشگاه‌ها و هاب‌ها در حوزه امنیت باشیم.

مشتاقیم سخن پایانی و جمعبندی شما را بشنویم.

در مجموع معتقدم موضوع امنیت فاوا، جای کار بسیاری در کشور دارد ولی به قدر نیاز به آن پرداخته نشده و مغفول مانده است. خوشبختانه کارهای بسیار بزرگی مانند 5G، IoT و AI در همراه اول برای نخستین بار در کشور در حال انجام است که بسیار تحسین‌برانگیز هستند و پیش‌بینی می‌شود برای این اقدامات بزرگ و ارزشمند، پشتوانه امنیتی خوبی تدبیر شده و سرمایه‌گذاری‌های متناسب با خود پروژه در حوزه امنیت آنها انجام شود. ما هم به عنوان یک شرکت همراه اولی با توان و ظرفیت شرکت‌های دانش‌بنیان تابعه خود، آماده‌ایم تا به عنوان بزرگترین هولدینگ حوزه‌امنیت‌فاوا گام‌های خوبی در این مسیر برداریم.

مصاحبه با دکتر حسن قدس دبیر کمیسیون برنامه ریزی و ارتباطات کانون هماهنگی دانش، صنعت و بازار افتا:

بومی‌سازی، پاسخی در خور به چالش‌های امنیتی فناورانه

فناوری که به تعبیر هایدگر هویت تمدن غربی است، وقتی وارد کشورهایی می‌شود که فقط استفاده‌کننده هستند، موجب استیلای فرهنگ غربی و در نتیجه جهانی سازی می‌شود. به‌علاوه، این وضعیت به وجود آورنده چالش‌های فرهنگی، اقتصادی و امنیتی کلان برای کشورها است. غلبه بر این مشکل در گرو بومی‌سازی فناوری و کاربردهای آن و همسوسازی محصولات فناورانه با نیازهای اجتماعی، فنی و ارزش های بومی هر کشور است.
در این شماره پای صحبت‌های دکتر حسن قدس دبیر کمیسیون برنامه ریزی و ارتباطات و عضو هیات موسس کانون هماهنگی دانش، صنعت و بازار امنیت فضای تولید و تبادل اطلاعات -افتا- و معاون سابق پژوهشی شرکت صاایران نشسته‌ایم تا به بررسی لزوم و اهمیت بومی‌سازی در رفع چالش‌های امنیت در حوزه ICT و سایبری بپردازیم.

با کانون هماهنگی صنعت، دانش و بازار افتا شروع کنیم. لطفا این کانون را برای مخاطبین فناوری همراه معرفی کنید.

کانون‌های هماهنگی صنعت، دانش و بازار با مصوبه شورای عالی انقلاب فرهنگی در سال ۹۵ شکل گرفتند. معاونت علمی ریاست جمهوری متولی ارائه مجوز به این کانون‌ها به عنوان نهادهای NGOای است که فعالیت آنها هماهنگی سه حوزه‌ی دانش یعنی دانشگاه‌ها، صنعت (شرکت‌ها) و بازار یعنی فضای کسب‌وکار است. مقدمات اجرایی کانون افتا رسماً در سال ۹۸ شکل گرفت و مصوباتش در معاونت علمی ریاست جمهوری انجام شد. کانون افتا محورش را بر روی صنعت سایبری گذاشته که صنعت رو به رشدی است و یکی از زیرمجموعه‌های صنعت فاوا محسوب می‌شود. ابعاد این صنعت در حال حاضر کوچک و در حد چندهزار میلیارد می‌باشد ولی پیش‌بینی می‌شود که با توجه به ملاحظات امنیتی که باید در زیرساخت‌های کشور به خصوص زیرساخت‌های حیاتی و حساس رعایت کنیم این صنعت می‌تواند حداقل تا چند ده برابر بزرگ‌تر شود. بازار مورد نیاز افتا حدود هفت تا دوازده هزار میلیارد برآورد شده است که فعلاً با آن خیلی فاصله داریم. بنابراین یکی از محورهای اصلی کانون افتا در راستای هماهنگی صنعت، دانش و بازار همین توسعه بازار افتا است که امیدوارم با برنامه‌هایی که انجام می‌دهد بتواند آن را به نتیجه برساند.

اهمیت بومی‌سازی در چیست؟ با فرض این که کشور از لحاظ تعاملات سیاسی و بین‌المللی در سطح مناسبی قرار گیرد، آیا هنوز هم باید برای بومی‌سازی تلاش کرد؟

به چند دلیل موضوع بومی‌سازی در صنعت سایبری و صنعت افتا یکی از دغدغه‌ها و ضرورت‌های کشور است. مهم‌ترین دلیل این موضوع، تخاصم کشورهای قدرتمند جهانی با کشور ایران است و این تخاصم شکل کم‌هزینه‌اش را به سمت تهدیدات سایبری برده که با یک ویروس چند هزار یا حداکثر چند ده هزار دلاری بتوانند تجهیزات چند میلیارد دلاری را متوقف نگه دارند یا دچار آسیب کنند. یکی از راه‌های مقابله با تعارضات و جنگ‌های سایبری، اتکای صنعت بهره‌بردار در حوزه‌های مهم و حساس کشور از قبیل نفت، انرژی و حمل‌ونقل و غیره به ظرفیت‌های داخلی است به نحوی که آسیب‌پذیری آنها برای ما حداقل قابل کشف و اشاره باشد.
بسیاری از محصولات خارجی مدعی هستند که تست‌های ارزیابی و تست‌های امنیتی را انجام داده‌اند اما فرآیند ورود محصولات به کشور ما یک فرایند مستقیم و قابل اتکا نیست. در گزارشی که در یکی از آزمایشگاه‌های معتبر کشور تهیه و بالغ بر ۷۰۰ تست مختلف انجام شده است بیش از ۹۵ درصد محصولات وارداتی دارای آسیب‌پذیری‌های اساسی

بودند و عمدتاً تقلبی و غیراصل یا دارای نرم‌افزارها و سرورهای قدیمی بودند.

موضوع استراتژی بومی‌سازی در حوزه افتا و حوزه سایبری، جزء استراتژی‌هایی است که به واسطه شکل‌گیری آسیب‌پذیری‌ها و تهدیدات سایبری در سطح جهانی و در اکثر کشورها به صورت یک استراتژی غالب درآمده است. آمریکا در بسیاری از موضوعات، ممنوعیت استفاده از تجهیزات چینی در زیرساخت‌هایش را به عنوان یک اصل اعلام کرده و با جدیت اجرا می‌کند. اروپایی‌ها هم جهت کاهش وابستگی شدیدشان به حوزه‌های فناوری‌های آمریکایی برنامه‌های جدی را پیاده کرده‌اند. در هند ظرفیت‌های خیلی خوبی شکل گرفته و ترکیه هم برنامه‌هایی را در این زمینه اجرا کرده است. در بسیاری از کشورهایی که قبلاً توجه کمتری به موضوع بومی‌سازی در صنعت سایبری به خصوص حوزه مخابرات و IT و امنیت می‌شد، طی یک دهه اخیر تغییر استراتژی دیده می‌شود. باید توجه داشت که این سه حوزه به شدت وابستگی ایجاد می‌کند. چون تمام دارایی‌های داده ما از مسیر مخابرات و IT عبور می‌کند و صنعت امنیت می‌تواند امنیت این تبادلات رو حفظ کند. در کشور ما هم با توجه به شرایط نامناسب تعاملات بین‌المللی در چهار دهه اخیر و تخاصم‌های موجود، نیاز به برنامه راهبردی بلند مدت و پایدار برای بومی‌سازی به شدت احساس می‌شود و حتی در صورت رسیدن به توافق در تعاملات سیاسی و برجام نیز باید ادامه داشته باشد.

اکوسیستم بومی‌سازی در حوزه محصولات سایبری و مخابراتی را در کشور چگونه ارزیابی می‌کنید؟ آیا اصلا اکوسیستمی به معنای واقعی در این حوزه داریم؟

یک اتفاق خوبی که صورت گرفته و باید آن را به عنوان یک فرصت عالی معرفی کنیم، قابلیتی است که از سال ۹۲ پیرو مصوبه سال ۸۹ مجلس در خصوص قانون دانش‌بنیان در معاونت علمی رییس جمهور و صندوق شکوفایی عملیاتی شد. طیف گسترده‌ای از شرکت‌های دانش‌بنیان یعنی بالغ بر ۴۰ درصد این شرکت‌ها در حوزه الکترونیک و فناوری اطلاعات شکل گرفته است و از تعداد ۶۵۰۰ شرکت بیش از ۳۰۰۰ شرکت در این حوزه فعالیت می‌کنند. بعضی از شرکت‌ها قدیمی و خیلی از آن‌ها جدید هستند و معمولاً بر اساس نیروی انسانی خیلی خوب و دانشگاهی شکل گرفته‌اند. پس ما یک اکوسیستمی را در حوزه نظام ملی نوآوری داریم که قابل توسعه و گسترش بوده، صندوق‌های حمایت و توسعه فناوری داشته، ساختارهای حقوقی و قانونی برای آن تعریف شده و تقریباً در بخش‌های مختلف رسوخ یافته است. این یک ظرفیت بسیار ارزشمندی است. اما وقتی به صنعت الکترونیک، صنعت مخابرات و صنعت افتا نگاه کنیم یک سری نابه‌سامانی‌هایی را در این صنایع می‌بینیم. یعنی ما نظام ملی نوآوری‌مان کمتر از یک دهه است شکل گرفته و قاعده‌مند شده، با وضعیت مطلوب فاصله دارد ولی حرکتش رو به رشد بوده است. بنابراین، با وجود موفقیت‌هایی که در برخی بخش‌ها داریم اما اکوسیستم ما ناقص بوده و خوب طراحی نشده است و نیاز به یک بازمهندسی جدی برای مقابله با چالش‌های این حوزه دارد. نیاز به یک هماهنگی بین وزارت صمت، وزارت ارتباطات و معاونت علمی وجود دارد، البته اینجا نقش شورای عالی فضای مجازی نقشی ویژه است ولی من قابلیت یا ظرفیتی را که به صورت جدی به موضوع بومی‌سازی توجه بکند، نمی‌بینم. هرچند ما یک کمیسیون به نام بومی‌سازی در مرکز ملی فضای مجازی داریم ولی یک کمیسیون رسمی و مصوب نیست و به عنوان یک کمیسیون فرعی در معاونت فنی طراحی شده و در حال حاضر بیش از ۹ ماه است که جلسه‌ای نداشته و به نظر می‌رسد که فرآیندش خیلی کند شده و لازم است در یک بازمهندسی جدی همه این نهادها با هم تنظیم قواعد شوند.

تجربه‌های موفقی از بومی‌سازی محصولات چه در حوزه مخابرات و چه در حوزه سایبر تا کنون داشتیم؟

نمونه‌های موفق به تعداد محصولات و شرکت‌های موفق وجود دارد، یعنی آنهایی که علی‌رغم پیچیدگی‌ها و مسائل بازار توانستند داخل یک بازار نسبتاً گسترده را مبتنی بر دانش و تولید شکل دهند، موفق بوده اند. اما از نمونه‌هایی که می‌توانم اشاره کنم محصول پادویش از شرکت امن‌پرداز است که بیش از هفده سال مستمر کار R&D و توسعه بازار انجام داده، هم بر روی کار کیفی و هم کار بازرگانی و هماهنگی با بازار کار کرده است. آقای مهندس حسینی تجارب بسیار زیادی را در حوزه فناوری و نوآوری دارد. موضوع کار شرکت آنها بسیار های‌تک و پیچیده است، ضمن اینکه هم‌زمان روی کسب سهم از بازار کار کردند و رقبای خارجی قوی را از بازار داخلی خارج کردند که کار سخت و مثبتی بود که این شرکت با سرعت خوبی انجام داد. این یک تجربه موفق است که باید بیشتر به تجربیات، مشکلات و نحوه موفقیت آن در این بازار پرداخت. نمونه موفق دیگر مجموعه آقای دکتر پاکروان در شرکت پرمان است که بر روی بحث توسعه سوئیچ‌های SDH کارهای خوب و موفقی انجام داده است. این شرکت با دانش فنی و نیروهای متخصص، رعایت کیفیت در کار و محصول و رعایت مدل‌های اقتصادی مناسب توانسته با وجود مشکلات مختلف، سهمی از بازار را در حوزه پیچیده مخابرات کشور که معمولاً رانت‌های عجیبی به شرکت‌های خارجی می‌دهند، بدست آورد. مورد دیگر مجموعه پیام‌پرداز است که بعد از گذشت ۲۵ سال با شیوه کار مبتنی بر دانش در برخی محصولات خود هم توانسته ظرفیتش را گسترش دهد و هم نیروی انسانی و سهم بازارش را تقویت کند. ما تقریباً ۵۰ تا ۶۰ شرکت خوب در این حوزه داریم که با دانش فنی خود و بدون استفاده از رانت توانسته‌اند محصولات موفقی داشته باشند.

چالش‌های بومی‌سازی چیست؟ آیا این صنعت نیاز به محرک‌های حاکمیتی برای رشد و بلوغ دارد، یا نیازمندی بازار در سمت تقاضا به‌اندازه‌ای جذاب هست تا اکوسیستم به شکل ارگانیک رشد پیدا کند؟

در شرایط فعلی حداقل حوزه‌ای که من می‌بینم هنوز به رشد و بلوغ کافی نرسیده و نیاز به مداخله حاکمیت دارد. البته حاکمیت در مورد نوع مداخله‌اش هم خوب عمل نمی‌کند. دلیل اینکه مداخله حاکمیتی نیاز است این است که بازار واقعی افتا طبق محاسبات ما در کشورهایی با شرایط ما که در معرض تحریم و تهدید هستند بین ۳ تا ۷ درصد از صنعت ICT آن کشور است. صنعت ICT ما فکر کنم بازاری حدود ۲۵۰ هزار میلیارد دارد که ۳ تا ۷ درصد آن چیزی حدود ۷ تا ۲۰ هزار میلیارد تومان می‌شود ولی چیزی که ما الان در بازار واقعی فعلی سنجش کردیم بین عدد تقریبی ۱ تا ۲ هزار میلیارد تومان است و بخش داخلی یعنی آن چیزی که توسط صنعت بومی تامین می‌شود در حدود ۳۰۰ تا ۵۰۰ میلیارد تومان است. این فاصله زیاد بین مقدار مطلوب و میزان واقعی حجم بازار، بیانگر مشکل شکست بازار است. اینکه نمی‌توانیم بازارمان را خوب بفهمیم و این مشکل هم کاملا مربوط به یک طرف نیست و اینجا نیاز به مداخله دولت وجود دارد و باید این مداخله از نوعی باشد که هم تولید داخل کیفیت پیدا کند و هم جهت‌گیری‌ها به سمت ظرفیت‌ها و توانمندی‌های داخلی برود. ما الان داریم برعکس این قضیه را می‌بینیم، مثلاً می‌بینیم که محصولات به راحتی از مسیر گمرک می‌آیند، بدون هیچ‌گونه ارزیابی وارد زیرساخت‌ها می‌شوند و چند سال بعد خبر آن پس از خرید، نصب و بکارگیری به نهاد حاکمیت می‌رسد که حالا که ما خریدیم، نمی‌توانیم دور بیندازیم. از آن طرف محصول داخلی که تولید می‌شود هنوز تمام نشده می‌گویند بفرستید آزمایشگاه و پس از طی یک فرآیند یک‌ساله و صرف هزینه تاییدیه می‌دهند. پس از گرفتن تاییدیه نیز بدون هیچ حمایتی می‌گوید حالا خودت برو بازار پیدا کن. بازار هم از محصول تازه چندان استقبال نمی‌کند. شیوه ورود حاکمیت هم حتماً باید هماهنگ باشد یعنی اگر سازمانی مثل افتا یا سازمان پدافند وارد شوند ولی ناهماهنگ باشند، بهتر است که اصلاً وارد نشوند.

به نظر شما دلیل اعتماد ضعیف بهره‌برداران به توسعه‌دهندگان داخلی چیست؟ چرا محصول خارجی‌ای که امکان تامین و دریافت پشتیبانی مستقیم از مبادی اصلی و معتبر آن وجود ندارد به محصول بومی با امکان پشتیبانی داخلی آن ترجیح داده می‌شود؟

شما دوتا فرض را درنظر گرفتید که به نظرم باید روی آن‌ها تامل کنیم. فرض اول این است که آیا واقعاً محصول داخلی در نگاه بهره‌بردار کیفیت بالاتری دارد؟ اگر چنین باشد، در واقع به فرهنگ‌سازی نیاز است. یعنی به دلیل برخی صنایع بزرگ مثل خودروسازی، ما هنوز مفهوم کیفیت را در محصولات داخلی به صورت عمده نارسا می‌بینیم و این تاثیرش را در همه‌ی صنایع دیگر گذاشته است. ما در برخی

محصولات لوازم خانگی کیفیتی بالاتر از محصول مشابه خارجی داریم ولی تعدد برندهای بی‌کیفیت در این حوزه باعث شده که کیفیت محصولات خوب هم به چشم نیاید. بنابراین، باور مجموعه‌های بهره‌بردار نسبت به کیفیت همچنان پایین است که این مشکل را باید از طریق فرهنگ‌سازی و تبلیغ حل کنیم و البته از طریق خود برندها. یعنی برند باید خود را به کیفیت مناسب برساند. مساله بعدی در مورد بحث خدمات است. خدمات پس از فروش هم بخشی از کیفیت است. به این معنا که یک بخشی از کیفیت در مشخصات فنی محصول است و بخشی از آن در قابلیت شرکت برای پشتیبانی از محصول و خدمات است که این هم به واسطه برخی برندهای ناموفق در کشور باعث تردید و تعمیم به کل شده است. به نظرم ما باید یک برندسازی انجام دهیم که کاملاً بی‌رحمانه شرکت‌ها مورد ارزیابی قرار گرفته و به آن‌ها گرید و رتبه بدهیم. اگر این کار بی‌رحمانه انجام نگیرد و گریدهای سبز و زرد و قرمز یا یک و دو و سه و چهار از هم تفکیک نشوند به همه ظلم می‌شود. چون به هر حال یک عده‌ای باید تلاش کنند خود را به گرید بالاتر ارتقاء دهند و یک عده‌ای هم همچنان در همان گریدهای پایین بمانند. این آرم و برند باید در خودش یک ارزش و اعتبار بالایی داشته باشد به‌گونه‌ای که هر کس این برند را دید متوجه شود که محصول دارای کیفیت است. اگر این کار را نکنیم همه محصولات زیرسوال کیفیت و خدمات خواهند رفت. به نظرم بهترین نهادی که می‌تواند این کار را انجام دهد کانون افتا است به این جهت که یک نهاد بی‌طرف و میانجی بوده (نه بخش حاکمیتی و نه بخش صنفی است) و برای هماهنگی طراحی شده است.

ظرفیت‌های داخلی در توسعه محصولات بومی مخابراتی را چگونه ارزیابی می کنید؟

الان در شرکت‌های دانش‌بنیان و فن‌آور کشور نزدیک به ۲۵۰ تا ۳۰۰ هزار نفر نیروی انسانی متخصص وجود دارد و این ظرفیت می‌تواند هر ساله حداقل بین ۲۰ تا ۳۰ درصد افزایش پیدا کند ولی در حال حاضر این اتفاق نمی‌افتد یعنی ما در شرکت‌ها با این حجم از

نیـرو آن سـرعت توسـعه لازم را نداریم و توسـعه‌مان در حد کمتر از ده درصد است که به مسـائل شـرکت‌داری، مدیریتـی و بـازار برمی‌گردد.

نزدیک به سـه هزار شـرکت دانش‌بنیان در حـوزه ICT و فنـاوری اطلاعات از بین هفت هزار شـرکت ثبت شـده داریـم. بسـیاری از آن‌هـا توانمندی‌هـای بسـیار بـالا و محصولات بـه روزی دارنـد (در حد ۳۰ درصـد) و برخی از آن‌ها نیز جدید هسـتند که بـا گذر زمان بایـد امتحان خـود را پـس دهند.

در حـوزه فناوری‌هـای "های‌تـک"، هـوش مصنوعـی و بحـث مخابـرات بـه خصـوص کارکـرد مشـترک هوش مصنوعـی و مخابـرات شـرکت‌های بسـیار خوبـی داریم کـه یعضـی از آنهـا در سـطوح بین‌المللـی نیـز فعالیـت می‌کننـد و در نبـود بـازار داخلـی، کارهای گسـترده‌ای را بـرای کشـورهای دیگـر انجـام می‌دهنـد. این نشـان می‌دهـد کـه ظرفیت‌هـای بالقـوه مـا زیـاد اسـت امـا اینکه چـرا ایـن ظرفیـت زیـاد نیـروی انسـانی منجر به زیرسـاخت‌های صنعتـی بـرای ارائه شـرکت‌های بزرگ نمی‌شـود ناشـی از چند پارامتر اسـت: یک پارامتر اینکه ما هنوز بلوغ شـرکت‌داری، تولید شرکت و زیرساخت آن در توسـعه صنعتی‌مـان را شـکل نداده‌ایم. توسـعه نظام ملی نوآوری‌مـان تا حدی شـکل پیدا کرده اسـت، یعنی موضـوع اسـتارت‌آپ و شـرکت‌های نوپـا الان بـه قدری شـکل گرفته که ظرفیت‌هـا بتواننـد از محیط دانشـگاه وارد محیط کسـب‌وکار پایه شوند. ولی شـرکت‌داری در سـطح بلوغ بالاتر نیاز به قواعـد پیچیده‌تـری دارد که ما در ایـن بخش‌ها دانـش فنـی و دانش مدیریتـی ضعیفی را داریـم.

به نظر شـــما همـــراه اول به‌عنوان بزرگتریـــن اپراتور خاورمیانه، چه نقشـــی در اکوسیســـتم بومی‌سازی محصولات مخابراتی و شبکه‌ای می‌تواند داشته باشد؟ آیا با فعالیت‌های مرکز تحقیق و توسعه همراه اول آشنا هستید؟ به نظر شـــما رویکرد این مرکز به بومی‌سازی مثمرثمر خواهد بود؟

الحمـدالله هـم اقـای دکتـر اخـوان و هـم آقـای دکتـر بهـروزی نسـبت بـه ایـن فرآینـد دیـدگاه مثبـت و نگاه رو بـه آینـده دارنـد. اینطـور برنامه‌ریـزی کرده‌انـد کـه موارد خیلـی فورس مـاژور بـرای کوتاه مـدت خریداری شـود، چون بـه هرحـال اپراتـور همیـن الان می‌خواهد توسـعه پیـدا کنـد. ولـی هم‌زمـان بـا خریـد، آینـده را هـم در نظـر داشـتند تا بـه این شـکل نباشـد که پشـت سـر هـم خریـداری صـورت گیـرد. برنامه‌ریـزی صورت گرفته تا مثـلاً برای شـش ماه ایـن سـوئیچ‌ها خریداری شـود ولی برای دو سـال آینـده هم کـه باز سـوییچ لازم اسـت، هم‌زمان بـا خریـد کوتاه مـدت محصـول، هزینه تحقیق و توسـعه بـرای بومی‌سـازی نیـز درنظـر گرفته شـود. البته بـرای اپراتـوری که بیسـت سـال زندگی‌اش را بـا خریـد تجهیـزات گذرانـده، اینکـه بخواهـد ذهن و رویکردش را به سـمت داخـل و اسـتفاده از ظرفیت‌های بومی عوض کند، بسـیار کار سـختی اسـت. خوشبختانه مرکز تحقیق و توسـعه بـا این هـدف و سـاختار طراحی شـد و به عنوان یـک مرکز پیشـرو در حوزه بومی‌سـازی در حـال کار اسـت و تـا جایـی که اطـلاع داشـتم حدود هـزار میلیارد تومـان قـرارداد تحقیق و توسـعه‌ای منجر به محصول بـا شـرکت‌های دانش‌بنیـان داخلـی منعقد شـده اسـت. البته خوبی ایـن مرکز این اسـت کـه مجوز خرید تمـام نیازهـای همـراه اول از زیرنظر ایـن مرکز رد می‌شـود یعنی تا این مرکـز تایید نکنـد که مـا در برنامه تولیـد آینده‌مـان چـه برنامه‌ای بـرای تولیـد محصولات خریـداری شـده داریـم اجـازه خریـد محصـولات کوتاه مـدت را نمی‌دهنـد. ایـن قاعده‌گـذاری بسـیار خـوب و ارزشـمندی است.

ایـن کار یک بـار در یـک جای دیگـر هم اتفـاق افتـاده بود که بحث تجمیـع خریدهـای وزارت نفـت در دو دهه پیش بود که همـان موقع یک نهاد مشـابه را بـرای بحث تجمیع خرید تجهیـزات موردنیـاز نفت ایجـاد و باعث شـد همین فرآینـد تامیـن مشـترک منجـر بـه بومی‌سـازی برخـی قطعات و نیازمندی‌ها شـود. ایـن کار در حـوزه وزارت نیرو هـم انجام شـد و دلیـل اینکـه طـی دو دهـه موفق شـدند بخش زیادی از نیازهای کشـور را در حوزه زیرسـاخت‌های نیرو تکمیـل کنند همیـن فرآینـد تجمیع نیـاز بود.

باز هـم تاکیـد می‌کنـم یـک جایـی بایـد تجمیع‌کننده باشـد، فیلتـر کنـد و بـرای خریـد نزدیـک و خریـد دور قواعـدی بگـذارد و بعد یـک جایـی آنهـا را بـه نهادهای دانش‌بنیـان داخلـی جهـت بومی‌سـازی وصـل کنـد. یعنـی چندتـا قاعده‌گذاری اسـت کـه اگر درسـت انجام شـده و افراد مناسـبی در این سیسـتم قرار داده شـوند، این فرآیند می‌توانـد مثمرثمر و اثربخش باشـد. بنابراین من فکر می‌کنم در همـراه اول، پایه‌گـذاری خوبی انجام گرفتـه و قواعدگذاری مناسـبی روی آن گذاشـته شـده اسـت. نیـروی شـروع‌کننده و اسـتارتر آن هـم افـرادی بودنـد کـه انگیـزه و قـدرت و جسـارت کار را داشـتند و امیدواریـم کـه بـا تغییـر و تحـول و احتمـالاً اصلاحاتی و همچنیـن تشـویق و حمایـت مدیرانـی کـه در ایـن مسـیر پرریسـک گام برمی‌دارند به الگوی بسـیار خوبی بـرای توسـعه در سـایر دسـتگاه‌ها و سـازمان‌ها برسـیم ان‌شـاءالله. ■

رصد فناوری

Technology Scouting

امنیت شبکه 5G

پیشـــرفت فناوری‌های ارتباطی و افزایش چشمگیر کاربرد فناوری‌های نوظهور، بســـترهای ارتباطی را به یکی از حوزه‌های استراتژیک حاکمیت کشورها از منظر رویکردهای توسعه‌محور و امنیت‌محور تبدیل کرده‌است. توسعه و کاربرد فناوری نسل پنجم شبکه‌های مخابراتی با شتاب زیادی در دنیا در حال گسترش است. این شبکه‌ها، برخلاف نسل‌های قبلی خود، گستره وسیعی از خدمات ارتباطی و پردازشـــی را کـــه روی فناوری‌های متعدد دیگری بنا شده‌اند عرضه می‌نمایند. از این رو توجه به نکات امنیتی در طراحی، تولید و بهره‌برداری شبکه‌های مخابراتی نسل پنجم جنبه‌های متنوع و جدیدی پیدا می‌کند.

در ابتدا، شبکه‌های 5G مبتنی بر هسته شبکه 4G خواهند بود، بنابراین آسیب‌پذیری‌های شبکه 4G را به ارث می‌برند. به‌عنوان مثال، امکان انجام حملات متقابل پروتکل[1] یکی از تهدیدات ممکن است. در این نوع حمله، مهاجمین از آسیب‌پذیری در چندین پروتکل به‌طور هم‌زمان استفاده می‌کنند. حمله می‌تواند با سوءاستفاده از آسیب‌پذیری شبکه 4G یا حتی 3G آغاز شود و در نهایت منجر به سوءاستفاده از اطلاعات مورد استفاده در شبکه‌های 5G گردد. این امکان وجود دارد که مهاجم IMSI مشترک را با سوءاستفاده از آسیب‌پذیری در شبکه‌های 3G (منتشر شده

1- Cross-protocol attack

در سال ۲۰۱۸) یاد بگیرد. چنین آسیب‌پذیری‌هایی در ۷۴ درصد شبکه‌های آزمایش‌شده در مطالعات یافت شده است. این بدان معنی است که برای اینکه حفاظت کافی از شبکه 5G ایجاد شود، اپراتورها باید با امن‌سازی شبکه‌های نسل قبلی شروع کنند. سیاست‌های به‌روز و رویکرد جامع و سیستمی می‌تواند امنیت شبکه‌های 5G را از این طریق امکان‌پذیر نماید. در این مطلب دغدغه‌های امنیتی مرتبط با فناوری نسل پنجم را مرور کرده و فهرستی از استانداردها و سایر مستندات مرتبط با امنیت فناوری نسل پنجم و فناوری‌های توانمندساز نسل پنجم ارائه می‌شود.

شایان تاکید است که در فناوری نسل پنجم نیز نظیر همه‌ی کاربردهای فناوری، امنیت یک فرایند است، نه یک رویداد تک‌کاره. علیرغم فعالیت‌های گسترده در خصوص امنیت 5G در سطوح استاندارد، هنوز بسیاری از موارد امنیتی لازم ناشناخته باقی مانده است. اپراتورها باید به طور منظم توصیه‌های 3GPP و GSMA را برای محافظت از شبکه 5G خود مطالعه و اجرا کنند. پرواضح است که توصیه‌های نهادهای بین‌المللی باید به صورت متفکرانه اجرا شوند. این توصیه‌ها معمولاً عمومی هستند؛ اما هر شبکه منحصر به فرد است. تغییرات در سیاست‌های امنیتی -براساس توصیه‌ها ممیزی‌ها، یا نظارت- باید بخشی از یک فرایند کلی باشد. تأیید باید قبل و بعد از پیاده‌سازی شبکه انجام شود. به عبارت دیگر، امنیت 5G فقط داشتن معماری مناسب یا تجهیزات امنیتی آن نیست؛ بلکه ارتقاء سطح امنیت و تاب‌آوری شبکه‌های مبتنی بر 5G نیاز به ایجاد گردش کار، رویه‌ها و همکاری بین تیمی دارد.

نسل پنجم شبکه‌های سلولی مخابراتی بی‌سیم (فناوری 5G)

به طور میانگین هر ده سال یک بار، نسل جدیدی از شبکه‌های سلولی مخابراتی بی‌سیم به بازار عرضه می‌شود. فناوری 5G، نسل پنجم شبکه سلولی مخابراتی بی‌سیم است که از ویژگی‌های اصلی آن در مقایسه با نسل قبلی می‌توان از افزایش سرعت انتقال داده‌ها، کاهش تأخیر و زمان پاسخ شبکه و همچنین افزایش قابلیت اعتماد و پایداری شبکه نام برد.

در فناوری 5G، جنبه‌های مختلف یک زندگی دیجیتال در بستری امن با استفاده از فناوری‌های متنوع پیاده‌سازی می‌شود تا نیاز کاربران را از طریق مدیریت شبکه‌های انعطاف‌پذیر برطرف سازد. از جمله این فناوری‌ها می‌توان به برش‌بندی شبکه [۲]، مجازی‌سازی عملکرد شبکه [۳]، شبکه نرم‌افزار محور [۴] و محاسبات لبه با دسترسی چندگانه [۵] اشاره کرد.

برش‌بندی شبکه به عنوان ستون فقرات توسعه فناوری 5G، چندین شبکه منطقی را بر روی یک زیرساخت فیزیکی مشترک پیاده‌سازی می‌کند به صورتی که یک سیستم انعطاف‌پذیر از شبکه‌های منطقی بر روی یک محیط شبکه‌ای قابل برنامه‌ریزی ایجاد شود.

مجازی‌سازی عملکرد شبکه با پیاده‌سازی دستگاه‌های سخت‌افزاری به صورت مجازی و نرم‌افزاری، این امکان را به شبکه می‌دهد که سرویس‌های مختلف را بدون نیاز به سخت‌افزار مجزا ارائه دهد که باعث گسترش عملیات شبکه به صورت پویا می‌شود.

هم‌چنین، شبکه نرم‌افزار محور امکان تخصیص دسترسی کاربران با نیازمندی‌های خاص را به منابع شبکه (مانند پهنای باند) فراهم می‌کند. با استفاده از فناوری محاسبات لبه با دسترسی چندگانه، با پردازش اطلاعات در لبه‌ی شبکه به جای انتقال به هسته، ترافیک غیرضروری کاهش داده می‌شود که باعث افزایش سرعت عملکرد و افزایش ظرفیت منابع در دسترس می‌گردد. کاربردهای اصلی فناوری 5G به سه دسته اصلی تقسیم می‌شوند که نمونه‌هایی از هر کدام در جدول ۱ نشان داده شده است.

دغدغه‌های امنیتی در فناوری 5G

درهم تنیدگی روزافزون خدمات عمومی، صنایع اقتصادی و نظامی با دنیای دیجیتال و ورود هر چه بیشتر دارایی‌های ارزشمند به حوزه دیجیتال، منجر به تنوع، پیچیدگی و تعدد تهدیدات امنیتی به میزان قابل توجه شده است. شبکه‌های مخابراتی به دلیل در اختیار داشتن اطلاعات حساس از جمله داده‌های موقعیت مکانی، مکالمات صوتی و پیغام‌های متنی به یک هدف جذاب برای مهاجمان امنیتی با انگیزه‌های مختلف مانند انگیزه‌های مالی و یا سیاسی تبدیل شده‌اند.

معماری شبکه 5G سرویس‌گرا با NFV ، SDN و برش شبکه به اپراتورها امکان انعطاف‌پذیری مورد نیاز برای انطباق سریع شبکه‌های خود با الزامات بازار را می‌دهد. اما نکته منفی آن مشکل مدیریت همه چیز است. این امر اهمیت ممیزی‌های امنیتی را برای تشخیص آسیب‌پذیری‌ها افزایش می‌دهد که باید بررسی شود آیا سیاست‌های امنیتی به درستی پیکربندی و اعمال شده است یا خیر. حسابرسی امنیتی باید به صورت دوره‌ای باشد، هم در هنگام استقرار کار اولیه 5G و هم در حین کار معمولی. این کار امکان نظارت بر تغییرات در امنیت شبکه و اتخاذ اقدامات به موقع در مقابله با حمله را می‌دهد.

به طور کلی، یک شبکه مخابراتی از چهار قسمت اصلی تشکیل

2- Network Slicing (NS)
3- Network Function Virtualization (NFV)
4- Software-Defined Networking (SDN)
5- Multi-Access Edge Computing (MEC)

می‌شود: دسترسی رادیویی شبکه، هسته شبکه، انتقال شبکه و اتصال شبکه. هر کدام از این قسمت‌ها در اصطلاح از سه صفحه تشکیل شـــده‌اند که هر صفحه نوع متفاوتی از ترافیک را انتقال می‌دهد.

صفحه کنترل[6]، ترافیک سیگنالینگ را حمل می‌کند.

صفحه کاربر[7]، ترافیک صفحه کاربر کـــه داده‌های واقعی را که به کاربر منتقل می‌شود حمل می‌کند.

صفحه مدیریت، پیام‌هایی را که برای کنترل جلسات کاربر استفاده می‌شود حمل می‌نماید.

هر سه نوع ترافیک یک شـــبکه مخابراتی (ترافیک سیگنالینگ، ترافیک صفحه کاربر و ترافیک مدیریتی) چه به صورت منحصر به فرد و چه به صورت همزمان می‌توانند مورد توجه مهاجمان قرار گیرند. به عنوان مثال، به منظور تغییر مسیر تماس‌ها و جلوگیری از ارسال پیامک به منظور شنود یا منع سرویس[8] باید مهاجمان ترافیک سیگنالینگ را ویرایش کنند. همچنین، بدون اقدامات امنیتی مناســـب برای ترافیک صفحه کاربر، حریم خصوصی و محرمانه بودن اطلاعـــات کاربر در معرض خطر قـــرار می‌گیرد. ترافیک مدیریتی یک هدف جذاب برای دسترسی مهاجمان به منابع شبکه اســـت، جایی که آن‌ها می‌توانند ترافیک و داده‌های شبکه را دستکاری کرده و مزاحمت ایجاد نمایند. کاهش خطرات و تهدیدهای مربوط به مدیریت شبکه نیاز به سیاست‌های امنیتی و کنترل دسترسی و نظارت بر امنیت در مکان‌های مناسب دارد.

با وجود آن که فناوری 5G مزایای بسیار زیادی به همراه خواهد داشت اما در عین حال ممکن است با ظهور این فناوری، مخاطرات امنیتی جدیدی نیز پدیدار شوند. پیش‌بینی‌های مختلف حاکی از آن است که تعداد مشترکان فناوری 5G در سال‌های آتی رشد قابل توجهی خواهند داشت. برای مثال اریکسون پیش‌بینی کرده که تا انتهای سال ۲۰۲۶ تعداد مشترکان 5G به ۳.۵ میلیارد نفر خواهد رسید. از این رو از آنجا که تعداد بسیار زیادی از کاربران و ابزارها به این فناوری متصل می‌شوند، احتمال وقوع حمله ناشی از آلوده شدن آن به ویروس بیشتر می‌شود. به عنوان مثال ممکن است تعدادی از دستگاه‌ها و تجهیزات اینترنت اشیاء به ویروس‌های مهاجمان آلوده شـــوند که می‌توانند با به‌دســـت گرفتن کنترل تجهیزات اینترنت اشـــیاء خطرات امنیتی جدی برای کل شبکه ایجاد کنند. علاوه براین، فناوری 5G، از الگوهای جدید طراحی شبکه مخابراتی مانند MEC، SDN، NS و NFV استفاده خواهد کرد تا مشکلات مربوط به نحوه اتصال، انعطاف‌پذیری و هزینه‌ها را برطرف کند، اما به‌نظر می‌رسد یکپارچه‌سازی این فناوری با این الگوها مجموعه جدیدی از دغدغه‌های امنیتی را به همراه دارد. دیگر عواملی که خطرات امنیتی را در فناوری 5G افزایش می‌دهند عبارتند از: تعریف ســـناریوهای جدید کاربـــردی، چالش‌های بکارگیری سیستم ابری، بهره‌برداری از پیکربندی خودکار شبکه، استفاده از زیرساخت مشترک، پیچیده و مقیاس‌پذیر بودن این فناوری که افزایش نیازمندی تنظیمات شـــبکه را به صورت پویا در بر دارد.

6- Control Plane
7- User Plane
8- Denial of Service (DoS)

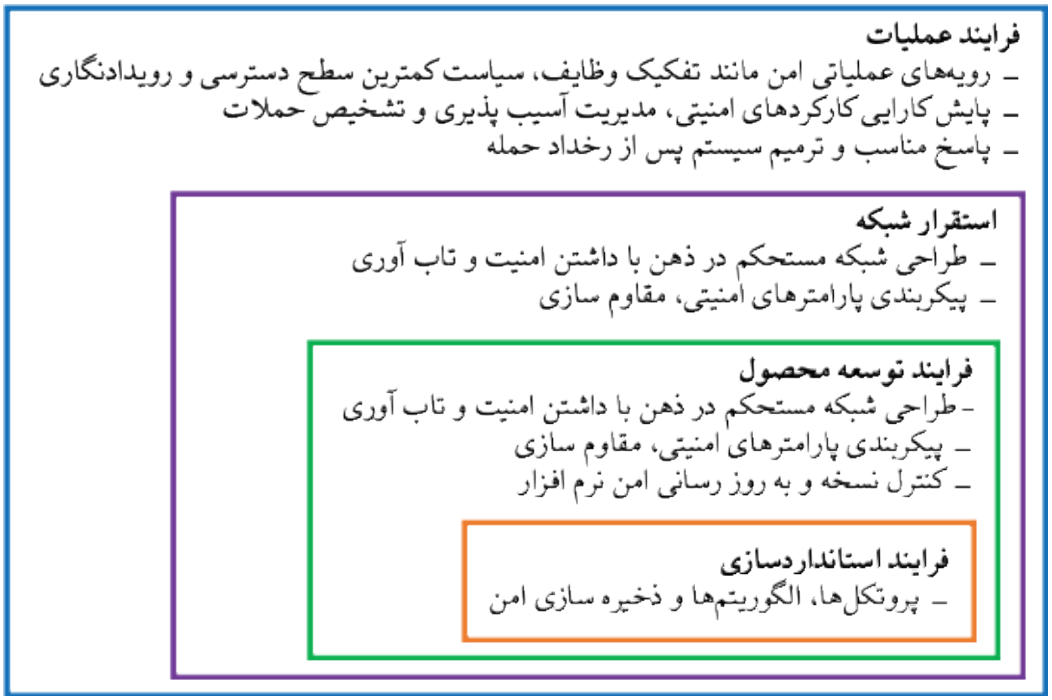
توجه به امنیت در فرآیندهای مختلف توســـعه و بهره‌برداری

برای دستیابی به امنیت در شـــبکه‌های مخابراتی لازم است در تمام طول فرآیندهای استانداردســـازی، تولیـــد و بهره‌برداری به مســـائل امنیتی توجه کامل شـــود. طبق تقسیم‌بندی شکل ۱، فرآیند استانداردســـازی[9] اولین مرحله است که به موجب آن معیارهای چگونگی همکاری شـــبکه‌های مختلـــف تعیین و در مورد چگونگی محافظت از شبکه‌ها و کاربران در برابر تهدیدات

9- Standardization Process

پهن‌باند بهبود یافته تلفن‌همراه (سرعت و کیفیت بالا)	پخش سریع ویدیو	واقعیت مجازی/افزوده	ابزارهای بدون سیم کارت
اینترنت اشیاء انبوه (مخابره کارا و کم‌هزینه)	کشاورزی هوشمند	شهر هوشمند	اندازه گیری هوشمند
سیستم‌های بحرانی (تأخیر کم با قابلیت اطمینان بالا)	کنترل ترافیک	جراحی از راه دور	رانندگی خودکار خودرو

جدول ۱: نمونه‌هایی از کاربردهای اصلی 5G



شکل ۱: فرآیندهای مختلف توسعه و بهره‌برداری شبکه [۲]

امنیتی توافق می‌شود. مرحله دوم، فرآیند توسعه محصول است که عرضه‌کنندگان[10]، استانداردهای مورد توافق برای عناصر و اجزاء کارکردی شبکه را طراحی، توسعه و اجرا می‌کنند که نقشی اساسی در امن‌سازی محصول نهایی شبکه دارند. در مرحله سوم که استقرار شبکه[11] نامیده می‌شود، طراحی و پیکربندی شبکه برای رسیدن به سطح امنیتی هدف‌گذاری‌شده و همچنین تنظیم پارامترهای امنیتی انجام می‌شوند. در نهایت، فرایندهای عملیاتی که خدمات سیستم را طبق چارچوب امنیتی هدف‌مند در اختیار کاربران نهایی قرار می‌دهند وابستگی زیادی به استقرار و عملیات شبکه دارند. همان‌گونه که در شکل ۱ تأکید شده است، در تمام این فرآیندها توجه همه‌جانبه به مسائل امنیتی ضروری است.

ویژگی‌های پایه‌ای امنیتی در مرحله استانداردسازی مشخص می‌شود، اما عرضه‌کنندگان در طول فرآیند توسعه و همچنین اپراتورها در طول مراحل استقرار و عملیات، فضای مانور زیادی برای اجرای مسائل امنیتی به منظور بهره‌برداری شبکه دارند. عرضه‌کنندگان مختلف فناوری‌های متداول را به گونه‌های متفاوتی پیاده‌سازی می‌کنند. به این ترتیب، کیفیت و امنیت پیاده‌سازی عرضه‌کنندگان متفاوت است و رقابت بین آن‌ها عامل مهمی در تعیین سطح امنیت محصول نهایی است.

تهدیدات فناوری 5G به شش دسته اصلی تقسیم می‌شوند

10- Vendor
11- Deployment

که نمونه‌هایی از هر دســـته در جدول ۲ نشـــان داده شده است.

تهدیدات هسته شبکه	تهدیدات مربوط به NS، NFV و SDN؛ شنود و ویرایش ترافیک شبکه؛ استفاده‌های فرصت‌طلبانه از منابع مشترک؛ دستکاری تنظیم‌کننده منابع شبکه؛ دستکاری داده‌های پیکربندی شبکه؛ بهره‌برداری از معماری ضعیف طراحی در شبکه؛ بهره‌برداری از رابط کاربردی برنامه‌نویسی؛ بهره‌برداری از شبکه با تنظیمات یا پیکربندی نامناسب؛ دستکاری ترافیک هسته شبکه؛ شناسایی شبکه و جمع‌آوری اطلاعات؛ سناریوهای کلاهبرداری مربوط به اتصالات رومینگ
تهدیدات دسترسی شبکه	سوء استفاده از منابع طیف؛ مسمومسازی پروتکل تفکیک آدرس[12]؛ گره دسترسی شبکه جعلی[13]؛ حملات دریافت IMSI؛ مسدودکردن فرکانس رادیویی؛ گمراه کردن MAC؛ دستکاری داده‌های پیکربندی شبکه دسترسی؛ تداخل رادیویی؛ دستکاری ترافیک رادیویی
تهدیدات مجازی‌سازی شبکه	سوء استفاده از منابع محاسباتی ابر؛ سوء استفاده از پروتکل ارتباطی مراکز داده؛ دور زدن مجازی‌سازی شبکه
تهدیدات زیرساخت فیزیکی	دستکاری تجهیزات سخت‌افزاری؛ بهره‌برداری از UICC و تجهیزات کاربر؛ تهدید دسترسی به امکانات MNO
تهدیدات محاسبات چندگانه در لبه	دروازه MEC تقلبی[14]؛ اضافه بار گره لبه؛ سوءاستفاده از رابط‌های برنامه‌نویسی لبه باز
تهدیدات عمومی شبکه	حمله منع سرویس؛ شنود؛ سرقت یا جعل هویت؛ سوءاستفاده از احراز اصالت؛ نرم‌افزار مخرب[15]؛ بهره‌برداری از معایب امنیتی، مدیریتی و فرایندهای عملیاتی؛ بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری؛ تخریب، سرقت و دستکاری اطلاعات

جدول ۲: تهدیدهای فناوری 5G

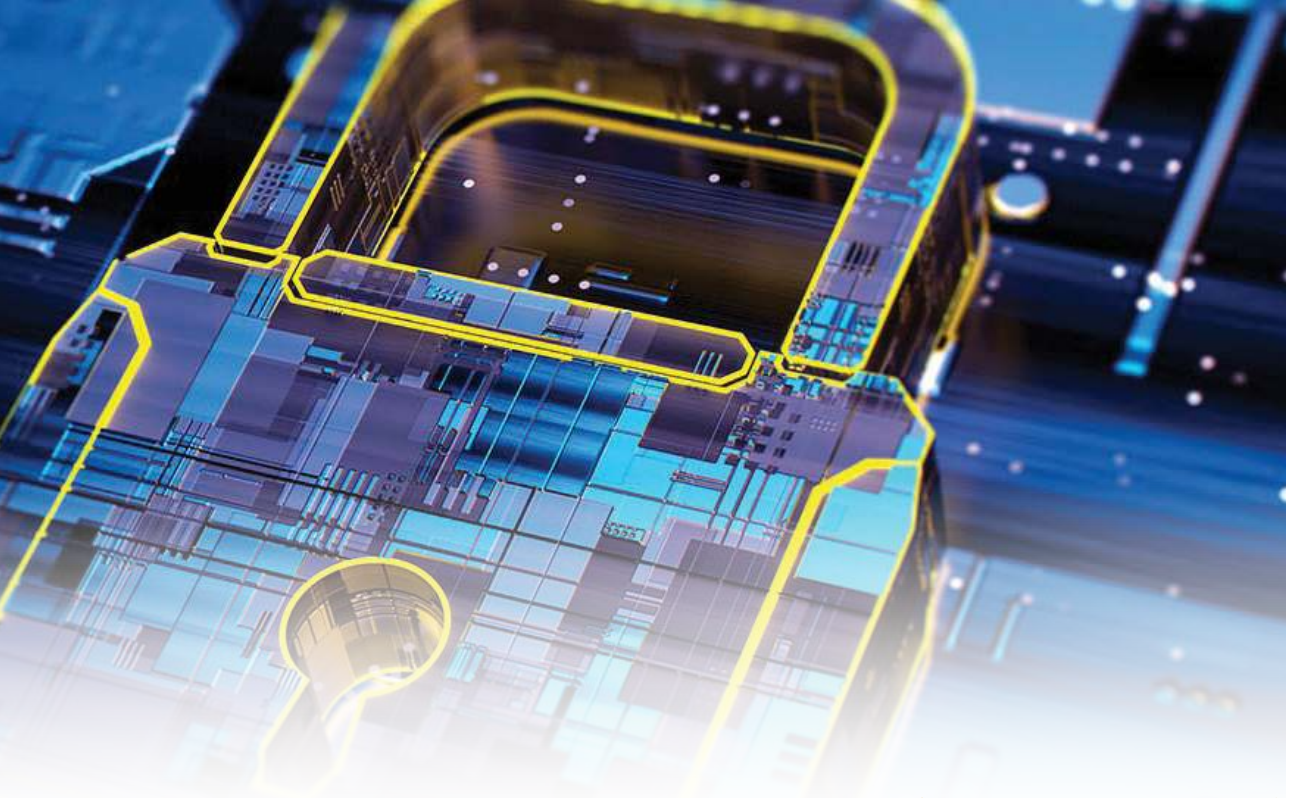
استانداردهای امنیتی در فناوری 5G

سازمان 3rd Generation Partnership Project (3GPP) که استانداردهای مربوط به گیرنده‌ها و فرستنده‌های شبکه سلولی مخابراتی بی‌سیم را تدوین می‌کند، استاندارد TS 33.501 را در مورد معماری و فرایندهای امنیتی برای سیستم 5G ارائه کرده است. این سازمان ملزومات امنیتی فهرست شده در جدول ۳ را که توسط ITU مشخص شده‌اند، در این استاندارد به کار برده است.

احراز اصالت	تایید هویت کاربران و هستار مخابراتی در شبکه
عدم انکار	عدم انکار هر فعالیت انجام شده در شبکه توسط کاربران یا هستار مجاز
امنیت پیام	حفاظت پیام از شنود یک هستار غیر مجاز
یکپارچگی پیام	حفاظت پیام از ویرایش توسط یک هستار غیر مجاز
قابلیت دسترسی	حفاظت از رد دسترسی به منابع شبکه توسط یک هستار غیر مجاز
حریم خصوصی	حفاظت اطلاعات کاربران و هستارهای شبکه
کنترل دسترسی	حفاظت منابع شبکه از استفاده غیر مجاز

جدول ۳: ملزومات امنیتی فناوری 5G

12- Address Resolution Protocol (ARP) poisoning
13- Fake access network node
14- False or rouge MEC gateway
15- Malicious Software



امنیت سایبری مش

پیش‌بینی می‌شود که تا سال ۲۰۲۴ سازمان‌های مختلف با پذیرش یک معماری مش امنیت سایبری و با یکپارچه‌سازی ابزارهای امنیتی به منظور تحقق یک اکوسیستم همکاری متقابل تاثیر زیان مالی ناشی از رخدادهای امنیتی شخصی را تا ۹۰% کاهش خواهند داد. تجهیزات، داده‌ها، نرم‌افزارهای کاربردی سازمان همگی فضای داخلی سازمان را ترک کرده و در نقاط مختلفی خارج از محدوده فیزیکی سازمان مستقر می‌شوند. لذا دیگر فضای به نام فضای داخلی یک سازمان که بتوانیم آن را امن فرض کرده و آن را جدا از فضای خارجی سازمان در نظر بگیریم وجود ندارد. مدیران امنیت سازمان‌ها می‌بایست ابزارهای امنیتی را در یک اکوسیستم با همکاری متقابل و با یک رویه معماری مش امنیت سایبری که مقیاس‌پذیر، قابل ارتقاء و قابل انطباق باشد، یکپارچه نمایند. معماری مش امنیت سایبری یک لایه پشتیبانی بنیادی فراهم می‌کند که به خدمات امنیتی کمک می‌کند تا بتوانند با همکاری یکدیگر یک فضای امنیت دینامیک ایجاد نمایند.

کلمات کلیدی: امنیت سایبری مش، امنیت، معماری امنیت سایبری مش، هویت توزیع شده

امروزه در بخش‌ها و سازمان‌های خصوصی و دولتی، رهایی از هر گونه تهدید به یک فعالیت مهم تبدیل شـــده است. مدیریت ریســـک امنیت ســـایبری یعنی پیدا کـــردن اینکه چه چیزی‌هایی ممکن است اشتباه رخ دهد و سپس تصمیم گیری در مورد بهترین راه‌ها برای جلوگیری یا به حداقل رساندن این مشکلات بالقوه. مراکز داده برای ایمن سازی به شدت به بخش سخت افزاری امنیت سایبری از قبیل دیواره آتش، استفاده از نرم افزارهایی برای نظارت بر فعالیت شبکه و آنتی ویروس نظارت بر سرورها، دسکتاپ و لپ تاپ‌ها در برابر حملات ویروس‌ها وابســـته هســـتند. زمانی که لپ‌تاپ، دستگاه‌های تلفن همراه و اینترنت اشیا (IoT) در یک سازمان استفاده می‌شوند، تغییر قابل توجهی در خط‌مشی‌ها و نحوه بررسی یا نظارت امنیت سایبری در سازمان ایجاد می‌شود زیرا کاربر برای انجام کار به ســـازمان بر می گردد. با شیوع همه گیری کرونا و اجازه سازمان‌ها به دور کاری از منزل، چالش‌ها و مشکلات جدیدی را به وجود آمد. برای ایجاد امنیت باید تمام قوانین امنیتی بازنگری شوند و سیاست امنیتی باید به دارایی‌های خارج از سازمان گسترش یابد. سیاست سازمان در خصوص اســـتفاده کارمندان از لپ تاپ‌های شخصی برای دسترسی به سیستم و سرورها باید بررسی شود. موارد مذکور تنها گوشه ای از چالش‌ها می‌باشد و همه این موارد منجر به پیدایش مفهومی با عنوان امنیت سایبری مش گردید.

امنیت سایبری مش

مش امنیت سایبری رویکردی اســـت که می کوشد به سازمان‌ها کمک کند تا بتوانند با نیازمندی‌های عصر دیجیتال انطباق یابند. با توسعه دورکاری در ایام کرونا و گسترش استفاده از تجهیزات خودی (BYOD) خارج از سازمان، داده‌های سازمان‌ها به خارج از سایت‌های بسته داخل سازمان انتقال یافته و حفاظت از آن‌ها دشوار شده است. مش امنیت‌ســـایبری رویکرد معماری توزیع‌شده را با کنترل‌های امنیتی مقیاس‌پذیر و انعطاف‌پذیر ترکیب می‌کند تا بتواند داده‌های توزیع‌شده سازمانی را حفاظت نماید [۱].

ترند امنیت سایبری مش، یکپارچه‌سازی کنترل‌های امنیتی با هم و

توسعه آن‌ها به منظور گسترش عملکرد حتی در مورد دارایی‌های توزیع شده می‌باشد. این سیستم سه واقعیت مختلف را که بر امنیت کسب‌وکارها موثر هستند مد نظر قرار می‌دهد:

- مهاجمان در محیط‌های سربسته فکر و عمل نمی‌کنند، اما سازمان‌ها اغلب کنترل‌های امنیتی را در محیط‌های محاصره شده پیاده می‌کنند.
- محیط پیرامونی سازمان‌ها بسیار گسسته‌تر و وسیع‌تر شده است.
- بسیاری از سازمان‌ها به دنبال تحقق استراتژی‌های چندابری هستند و نیاز به رویه‌های امنیتی تلفیقی دارند.

مش امنیت سایبری چندین لایه بنیادی فراهم می‌آورد که می‌توانند به عنوان نیروهایی تقویت‌کننده در صورت یکپارچگی با محصولات امنیتی مختلف عمل کنند. این موضوع در شکل ۱ نشان داده شده است.

باج‌افزارها و دیگر حملات امنیت سایبری که همه روزه در رسانه‌های خبری شاهد بروز و ظهور آن‌ها هستیم، منجر به زیان‌های بزرگ در منابع سازمان‌ها می‌شوند. جرائم حوزه امنیت سایبری، خصوصا باج‌افزارها منجر به بروز اختلالات گسترده در دنیای فیزیکی می‌شوند، خصوصا وقتی که یک زیرساخت حیاتی را مورد حمله قرار داده باشند، مانند حمله‌ای که به خط انتقال نفت در ماه مه ۲۰۲۱ در آمریکا اتفاق افتاد.

تحلیل گر گارتنر فلکیس گاتگن [1] معتقد است که مش امنیتی در حال حاضر بیشتر به عنوان یک استراتژی مطرح است تا یک معماری استاندارد و مشخص، هر چند همین مفهوم می‌تواند سازمان‌ها را برای مقابله با تهدیدات مقاوم نماید [۲].

برخلاف تکنولوژی‌هایی مانند SIEM [2] و SOAR [3] که هدف‌شان یکپارچه‌سازی ابزارهای امنیتی است، مش امنیتی تجزیه و تحلیل امنیتی یکپارچه را جهت شناسایی و پاسخ به تهدیدات

1- Felix Gaehtgens
2- Security Incident and Event Management
3- Security Orchestration, Automation and Response

مورد استفاده قرار می‌دهد. این ساختار مش هم‌چنین شامل لایه‌های هویت، خط مشی، وضعیت و داشبورد است.

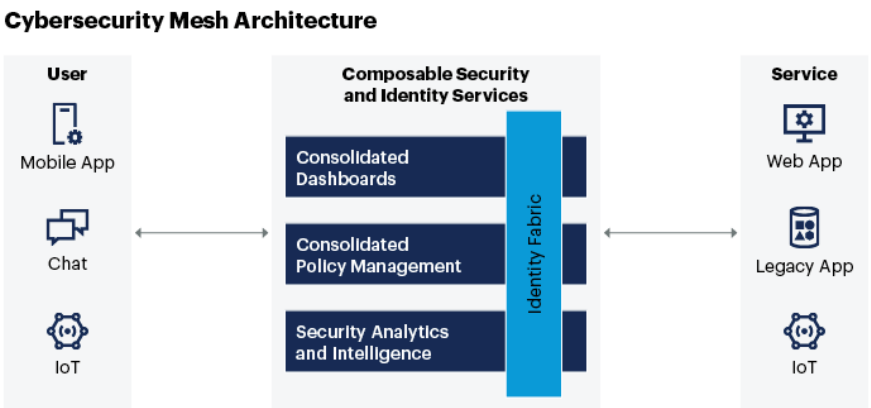
گسستگی محیط پیرامونی سازمان‌ها

در گذشته همه داده‌های یک سازمان در داخل آن و در یک محیط فیزیکی بسته بود. با گسترش کرونا و افزایش میزان دورکاری و اعتماد به محیط‌های چندابری و استقرار داده‌ها بر روی بسترهای ابری، بسیاری از داده‌های سازمان‌ها دیگر در دیتاسنترهای اختصاصی سازمان‌ها قرار ندارند و کاربران سازمان نیز به نرم‌افزارهای مستقر بر روی ابر از هر کجای دنیا می‌توانند دسترسی پیدا نمایند. در یک محیط توزیع شده، هویت کاربران و محتوای مورد استفاده آن‌ها تنها راه کنترل دسترسی به سیستم است. سازمان‌های زیادی از یک استراتژی چندابری پیروی می‌کنند. بر اساس چندین مطالعه مختلف، سازمان‌ها تمایل دارند که از خدمات چندین ارائه کننده خدمات ابری استفاده نماید. با توجه به آنکه هر کدام از ارائه کنندگان خدمات ابری معمولا از رویه‌های مختلفی پیروی می‌نمایند، ارائه یک ساختار امنیتی واحد بین تمامی ارائه کنندگان خدمات ابری دشوار و چالش برانگیز خواهد بود. بنابراین توسعه استانداردها و ارائه محصولات جدید در حال پر کردن این شکاف است.

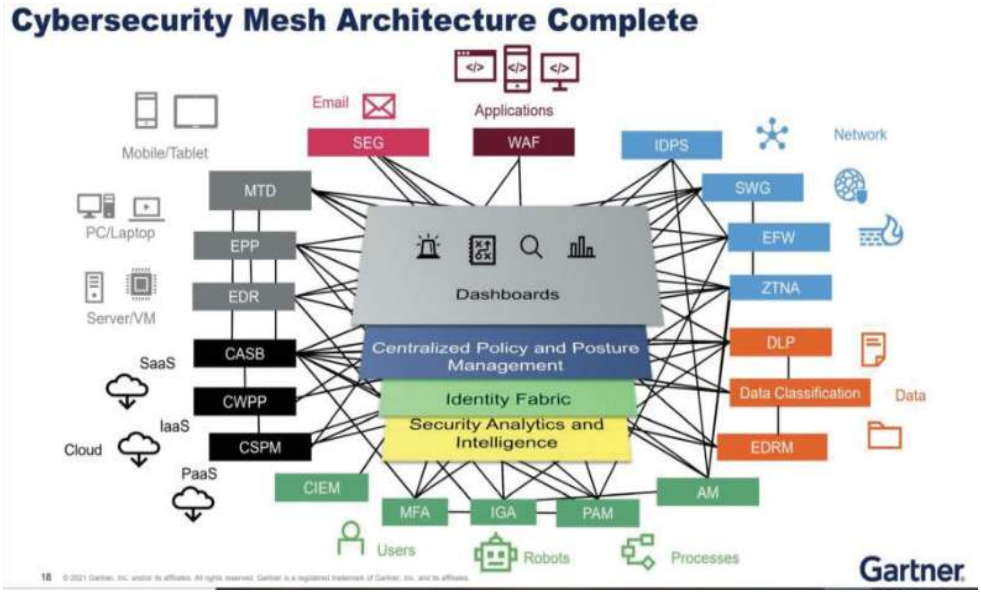
معماری امنیت سایبری مش

معماری مش امنیت سایبری یک رویه قابل انطباق و مقیاس‌پذیر به منظور توسعه کنترل‌های امنیتی به کلیه داده‌های توزیع شده یک سازمان است. انعطاف‌پذیری آن به شکل خاص برای رویکردهای رو به افزایش ماژولار که با معماری چندابری هیبرید سازگار هستند مناسب است. CSMA [4] یک اکوسیستم امنیتی مقاوم، انعطاف‌پذیر و قابل انطباق ارائه می‌نماید. در این معماری به جای آنکه هر ابزار امنیتی در یک محیط مستقل عمل نماید، یک مش امنیت سایبری ایجاد می‌شود که برای ابزارهای مختلف

4- Cybersecurity mesh architecture



شکل ۱-معماری امنیت سایبری مش



شکل ۲-معماری کامل و لایه‌های مش امنیت سایبری [۳]

قابلیت همکاری متقابل را از طریق چندین لایه پشـــتیبان فراهم می‌نماید. لایه‌هایی مانند مدیریـــت رویه تلفیقی، هوش امنیتی و ساختار توزیع شده مدیریت هویت کاربران (Identity Fabric) جزو لایه‌های پشتیبیان این معماری برای تحقق اهداف مد نظر هستند.

CSMA کمک می کند تا ابزارهای امنیتی با فراهم کردن یک سری از خدمات مانند مدیریت توزیع شـــده هویت کاربران، تحلیل‌های امنیتی، هوشمندی، خودکارسازی و پاسخ، هماهنگی و مدیریت رویه‌های متمرکز با هم یکپارچه شـــوند. CSMA مشخصا با تکیه بر قابلیت ارتقاء و انطباق، مقیاس پذیری و قابلیت همکاری کنترل امنیتی بیشتری را محقق می‌سازد. این تکنولوژی، ۴ لایه اختصاصی بنیادی برای ایجاد همکاری متقابل بین کنترل‌های خاص امنیتی ارائه می‌نماید و پیکربندی و مدیریت آن‌ها را تسهیل می کند. این ۴ لایه عبارتند از:

تجزیه و تحلیل امنیتی: با یادگیری درس‌ها و گردآوری و تحلیل داده‌های تمامی ابزارهای امنیتی، نسبت به انواع تهدیدات امنیتی شناختی گسترده‌تر ایجاد می‌شـــود که منجر به ایجاد قابلیت ارائه پاسخ‌های دقیق‌تر و شفاف‌تر خواهد شد.

ساختار توزیع شده مدیریت هویت: در این ساختار قابلیت‌هایی مانند خدمات دایرکتوری، دسترسی وفق‌پذیر، مدیریت توزیع شده هویت، اثبات هویت و مدیریت مجوزهای دسترسی به منابع کاربران ارائه خواهند شد.

مدیریت وضعیت و رویه تلفیقی[5]: می‌توان یک سیاست مصوب مرکزی را به ســـاختارهای پیکربندی بومی برای ابزارهای امنیت اختصاصی ترجمه کرد و یا به عنوان یک گزینه پیشرفته‌تر می‌توان خدمات صدور مجوز زمان اجرای دینامیک ارائه نمود.

داشبوردهای تلفیقی: با ارائه یک دید ترکیبی نسبت به اکوسیستم امنیتی، تیم‌های امنیتی قادر خواهند بود که بسیار سریع‌تر و موثرتر نسبت به رخدادهای امنیتی پیش رو پاسخ‌گو باشند.

تجهیزات، داده‌ها، نرم‌افزارهای کاربردی ســـازمان همگی فضای داخلی ســـازمان را ترک کرده و در نقاط مختلفی خارج از محدوده فیزیکی سازمان مستقر می‌شوند. لذا دیگر فضایی به نام فضای داخلی یک سازمان که بتوانیم آن را امن فرض کرده و جدا از فضای خارجی سازمان در نظر بگیریم وجود ندارد. در چنین شرایطی در یک فضای توزیع شده که افراد ممکن است از هر نقطه‌ای به هر چیزی دسترسی پیدا کنند، هویـــت و محتوا تنها صفحات کنترلی در دســـترس ما خواهند بود.

مش امنیت سایبری فراتر از XDR[6]

XDR به عنوان یک راهکار جدید توسط شرکت‌های امنیت فناوری اطلاعات برای اتصال محصولات امنیتی با هم در یک پلتفرم واحد ارائه شده است. XDR می‌تواند یک پایه و اساس بالقوه برای تجزیه و تحلیل‌های امنیتی باشد که CSMA به آن نیاز دارد، همین‌طور SOAR و SIEM می‌توانند برای این منظور اســـتفاده شـــوند که می‌توانند ارزشـــی را به لایه تجزیه و تحلیل امنیتی در مش امنیت بیفزایند.

در این بین، تکنولوژی لبه سرویس دسترسی امن (SASE) می‌تواند یک رویکرد مش برای ارائه توابع مشخصی در یک ساختار یکپارچه باشد اما مش امنیتی چشم‌انداز وسیع‌تری را شامل می‌شود.

هویت توزیع شده

هویت توزیع شده کلید دست‌یابی به مش امنیتی است. ذیل یک ساختار هویت توزیع شده چنانکه در شکل ۳ نیز نشان داده شده است، هویت‌ها به المان‌های سیستم لینک خواهند شد و تکیه کمتری بر هویت مرکزی خواهند داشت.

5- Consolidated policy and posture management

6- Extended Detection and Response

سیستم‌های سنتی مدیریت هویت و کنترل دسترسی (IAM[7]) از دید مقیاس‌پذیری، قابلیت اطمینان، حریم خصوصی و امنیت مشکلاتی داشتند. به جهت مشکلات ذاتی سیستم IAM در طول حیات آن خود به نقطه شکستی برای سرقت اطلاعات هویت و دسترسی افراد تبدیل شده است.

با تمام این تفاسیر تکنولوژی هویت توزیع شده هنوز به عنوان یک تکنولوژی اثبات نشده مطرح است که با پشتیبانی تکنولوژی‌هایی مانند زنجیره بلوکی توسعه یافته است و ریسک‌های احتمالی آن در توسعه سرویس‌ها با زنجیره بلوکی همچنان نامشخص است.

پیشنهادات و توصیه‌ها

مدیران فناوری اطلاعات سازمان‌ها که بر روی مدیریت هویت و کنترل دسترسی کاربران تمرکز دارند می‌بایست موارد زیر را در نظر بگیرند:

به منظور مقابله با پیچیدگی‌های روزافزون امنیت سایبری مدیران امنیت باید زیرساخت‌های امنیتی خود را هر چه بیشتر یکپارچه سازند و برای تحقق آن بر مدیریت مرکزی و اعمال رویه‌های توزیع‌شده[8] تمرکز نمایند.

به منظور تضمین امنیت سازمان در آینده، تکنولوژی‌های امنیت سایبری‌ای باید انتخاب شوند که یکپارچه‌سازی المان‌ها با بکارگیری واسط‌های برنامه‌نویسی نرم‌افزار را میسر سازند. این تکنولوژی‌ها باید قابلیت افزودن افزونه‌ها و شخصی‌سازی آنها، پشتیبانی از استانداردها و تحلیل‌های توسعه‌یافته را داشته باشند.

همچنین لازم است فواصل مفهومی بین وندورهای محصولات مختلف مورد استفاده در زیرساخت سازمان را با بکارگیری استانداردهای امنیتی کنونی و آتی برای همکاری متقابل بین آن‌ها تکمیل نمود.

به منظور تدوین استراتژی تحقق CSMA در بلندمدت، باید لایه‌های پشتیبان پیاده شود. این کار با انتخاب یک رویه مبتنی بر وندور اولیه و پر کردن شکاف‌های دانشی موجود و یا با انتخاب بهترین روشهای شناخته شده از ابتدا صورت می‌گیرد. بیشترین لایه‌های پشتیبانی CSMA ممکن باید محقق شود: تحلیل‌های امنیتی، مدیریت رویه‌ها و داشبوردهای یکپارچه و ...

نتیجه‌گیری و جمع‌بندی

در این مقاله با چالش‌های نوین در تحقق امنیت سایبری آشنا شدیم و دیدیم که یکی از راهکارهای پیشنهادی جهت مقابله با این چالش‌ها پیاده‌سازی معماری مش امنیتی است. در این معماری همکاری متقابل بین المان‌های امنیتی و نظارتی و تحلیل یکپارچه داده‌های انبوه به شناسایی هر چه سریعتر و مقابله با تهدیدات و حملات احتمالی به سیستم‌ها کمک خواهد کرد. هر چند که مش امنیتی در حال حاضر بیشتر به عنوان یک نظریه مطرح است ولی در آینده نزدیک تمامی سازمان‌ها ناچار به انطباق با آن خواهند شد. مش امنیتی موضوعی فراتر از پیاده‌سازی یک سیستم شناسایی و پاسخ در نقاط انتهایی (XDR) است و به نوعی ترکیبی از قابلیت‌های SASE، SOAR، XDR و تحلیل‌های یکپارچه می‌باشد. در این راستا ابزارهایی مانند کنترل و مدیریت یکپارچه دسترسی کاربران از مهم‌ترین ابزارهای تحقق امنیت در این معماری هستند و احراز هویت توزیع شده در این ساختار می‌تواند به کمک زنجیره بلوکی نیز محقق گردد ■

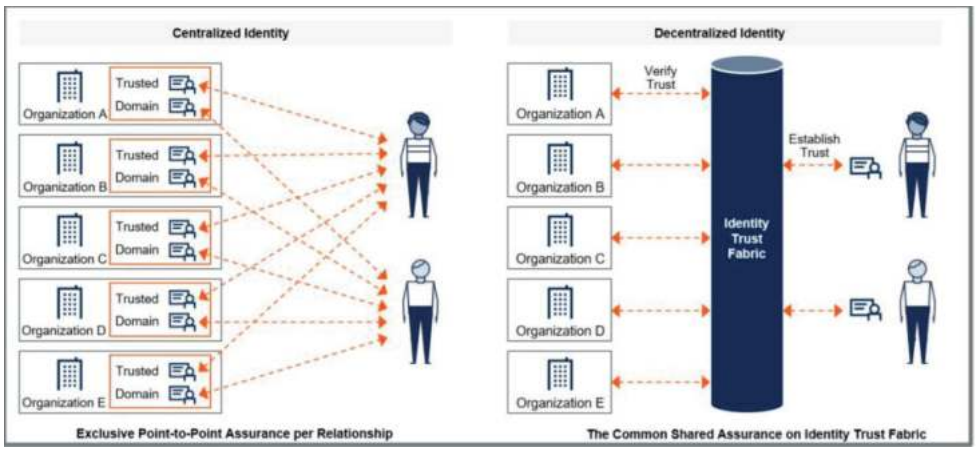
منابع

[1] M. E. b. Osman, "Cybersecurity Mesh," University Malaysia Sarawak, Sarawak Malaysia , 2021.

[2] J. H. a. 5. m. Felix Gaehtgens, "Top Strategic Technology Trends for 2022 --12 Trends Shaping the Future of Digital Business," Gartner , Stamford, 2021.

[3] P. Shread, "Cybersecurity Mesh, Decentralized Identity Lead Emerging Security Technology: Gartner," Oct 2021. [Online]. Available: https://www.esecurityplanet.com/networks/cybersecurity-mesh-decentralized-identity-emerging-security-technology/.

7- identity and access management
8- decentralized policy enforcement



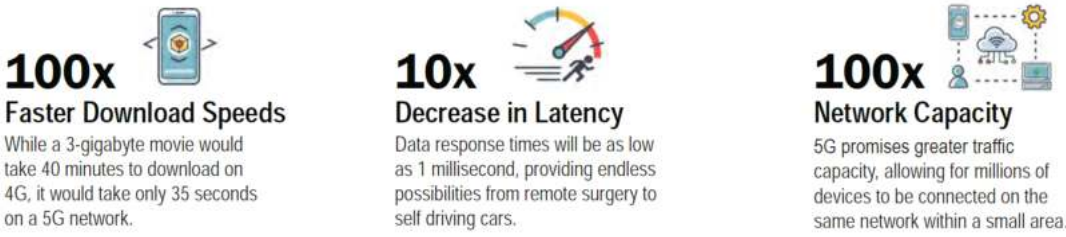
شکل ۳- هویت توزیع شده در مقایسه با هویت مرکزی (منبع- گارتنر)

فناوری همراه
fanavari hamrah
فصلنامه‌ی خبری تحلیلی
زمستان ۱۴۰۰ شماره‌ی چهارم

اپراتورهای مخابراتی و امنیت نسل پنج

5G محل استقرار و ارائه محصولات و خدمات نوین و توان پردازشی را تغییر خواهد داد. پس از استقرار کامل و گسترده اکوسیستم 5G تمامی سازمان‌ها با آن درگیر و برای تحقق منابع جدید درآمدی بدان نیازمند خواهند شد. 5G با استفاده از محاسبات لبه‌ای به منظور افزایش سرعت پردازش، حافظه‌های قوی در نزدیکی کاربر را افزایش داده و کارآیی بی‌درنگ به همراه پهنای باند وسیع و تاخیر کم به همراه خواهد داشت. در حالیکه 5G در میانه ۲۰۲۰ تنها توسط ۹۳ اپراتور و در حدود ۴۰ کشور در دست استقرار بوده است، IDC پیش‌بینی کرده که تعداد کاربران 5G از ۱۳,۶ میلیون در سال ۲۰۱۹ به بیش از ۱,۸ میلیارد در سال ۲۰۲۴ خواهد رسید. با این حال استقرار 5G خصوصا در شرایط حضور هم‌زمان 5G و نسل‌های قبلی شبکه چالش‌های امنیتی بسیاری در پیش خواهد داشت و نیازمند رویکردهایی مانند اعتمادصفر، امنیت داده‌ها، امنیت محاسبات لبه‌شبکه، امنیت در نقاط انتهایی اتصال به شبکه خواهد بود. پیش‌بینی شده که ۵۷% از اپراتورها به کمک ارائه‌دهندگان خدمات امنیت MSSP در تضمین امنیت 5G خواهند کوشید. در این مقاله به بررسی چالش‌های امنیتی پیش‌روی تحقق 5G و راهکارهای پیشنهادی برای مقابله با آن خواهیم پرداخت.

کلمات کلیدی: امنیت، 5G، محاسبات لبه موبایل، اعتمادصفر، امنیت زیرساخت‌های مجازی.



شکل ۱- اختلاف در سرعت، ظرفیت و تاخیر قابل دست‌یابی در 5G نسبت به 4G

5G نسل جدید شبکه‌های تلفن همراه است که با هدف ارائه سه نوع سرویس در کشـــورهای مختلف در دست استقرار می‌باشد:

- دسترسی پهن‌باند توسعه یافته به دیتای موبایل (eMBB[1])
- مخابرات داده با تاخیر بسیار کم و قابلیت اطمینان بسیار بالا (URLLC[2])
- مخابرات داده بین ماشین‌ها در حجم وسیع (mMTC[3])

تاخیر انتهابه‌انتهای بسیار کمتر (تا ۱ میلی‌ثانیه در مقایسه با تاخیر ۵۰ میلی‌ثانیه نسل‌های قبلی) در تبادل داده‌های حیاتی مورد نیاز برای کنترل مجموعه‌های صنعتی از الزامات نسل جدید است. این تاخیر کم مستلزم شبکه‌ای امن می‌باشد. از طرف دیگر مخابرات داده بین ماشین‌ها در این نسل انقلابی بزرگ به حساب می‌آید. افزایش چند صد برابری تجهیزات IoT متصل به شـــبکه، سطح حمله[4] بسیار وسیع‌تری را ایجاد خواهد کرد. ضمن آنکه ماهیت کاربردهای این شبکه مانند اســـتفاده از آن برای کنترل عملکرد کارخانه‌های صنعتی و نیروگاه‌های مولد برق (مانند نیروگاه‌های اتمی) و... نیاز به امنیت در آن ر ضروری‌تر می‌نماید [۱].

مجازی‌سازی و شبکه‌های مبتنی بر نرم‌افزار قابلیت‌های اساسی

1- enhanced Mobile BroadBand (eMBB)
2- Ultra-reliable and low-latency communications
3- massive machine type communications
4- Attack Surface

موردنیاز جهت تحقق 5G هســـتند که خود چالش‌های امنیتی بزرگی ایجاد می‌نمایند.

افزایش تعداد نودهای متصل به شبکه چالشی عظیم در مدیریت هویت کاربران متصل به شبکه ایجاد می کند، خصوصا که کاربران جدید می توانند ماشین‌ها و تجهیزات IoT باشند که ممکن است در تعداد بسیار زیاد بتوانند به شبکه متصل شوند. تضمین امنیت در چنین شبکه‌ای مستلزم همکاری متقابل اپراتورها و کاربران وسازمان‌ها و رعایت الزامات امنیتی از سوی هردو خواهد بود.

با توجه به گســـترش زیرســـاخت‌های ابری در نســـل پنجم و پیاده‌سازی بخش‌های مهمی از شـــبکه بر روی بستر ابری، مدل امنیت اشتراکی و مجازی می‌بایست توسعه یابد.

5G قابلیت‌های جدیدی از قبیل قطعه‌بندی شـــبکه[5] را فراهم می کند که سبب می‌شـــود هر یک از کاربران بتوانند باتوجه به کیفیت سرویس موردنیاز بخش مشـــخصی از منابع‌شبکه را به خوداختصاص دهند. اگرچه به صورت پیش‌فرض 5G امنیت ذاتی بیشتری نسبت به نســـل‌های قبلی خواهد داشت و قابلیت‌هایی مانند رمزنگاری برروی هوا و رمزنـــگاری IMSI های کاربران ارائه می‌نماید که احتمال حملات eavesdropping را کاهش می‌دهد، با این حال 5G برای امنیت کامل نیاز به اقدامات بیشتری خواهد داشت.

اپراتورهای تلکام و چالش‌های امنیتی پیش روی

5- Network Slicing

استقرار 5G

در یک ارزیابی که توســـط AT&T صورت پذیرفت، مطابق نتایج حاصل، اپراتورها چالش‌های امنیت پیش‌روی 5G را مطابق شکل ۱ ارزیابی کرده‌اند.

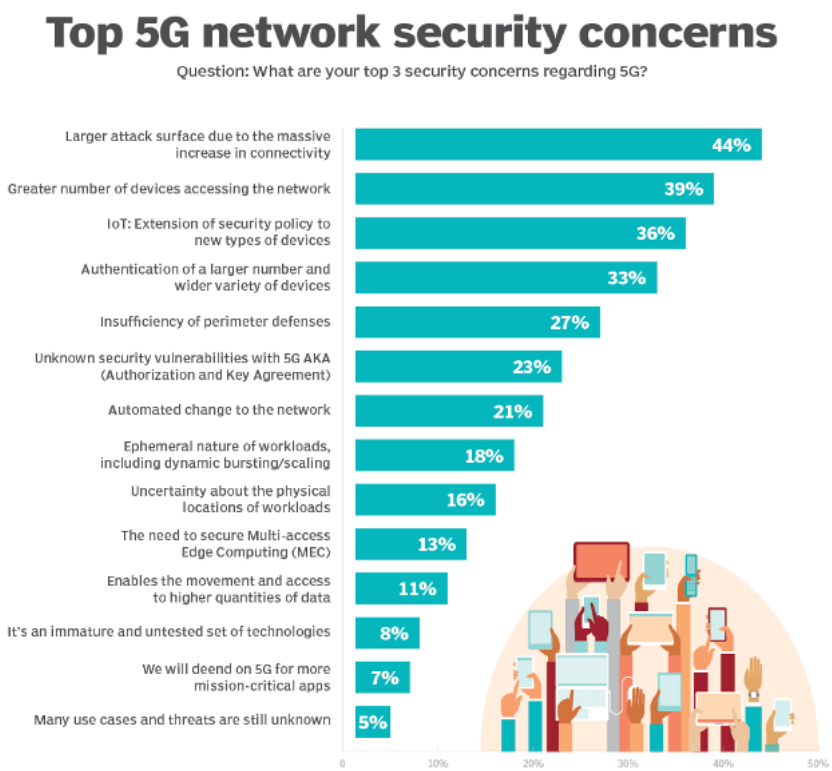
مجازی‌سازی امنیت[6]

افزایش تعـــداد تجهیزات متصل به 5G احتمـــال وقوع حملات بیشـــتری را فراهم می‌آورد. ســـازمان‌های امنیتی می‌بایست به منظور پاسخ به ســـرعت بالای تبادل داده در 5G به‌جای اعمال دســـتی[7]، تغییرات امنیتی خود را به صورت دینامیک و خودکار اعمال نمایند. مجازی‌سازی امنیت به‌عنوان مهم‌ترین پیشرفت حوزه امنیت در 5G، با انعطاف بیشتر در اعمال یکپارچه و سریع تغییرات و وصله‌های جدید امنیتی به ســـازمان‌ها کمک خواهد کرد تا از وجود جزیره‌های مجزا از هم که برخی رویه‌های قدیمی و نادرســـت دارند، دوری کنند. با افزایش پیچیدگی در مدیریت امنیت، اســـتفاده از خدمات یک فراهم‌کننده ســـرویس امنیت مدیریت‌شده می‌تواند یکی از گزینه‌های مهم تحقق امنیت باشد.

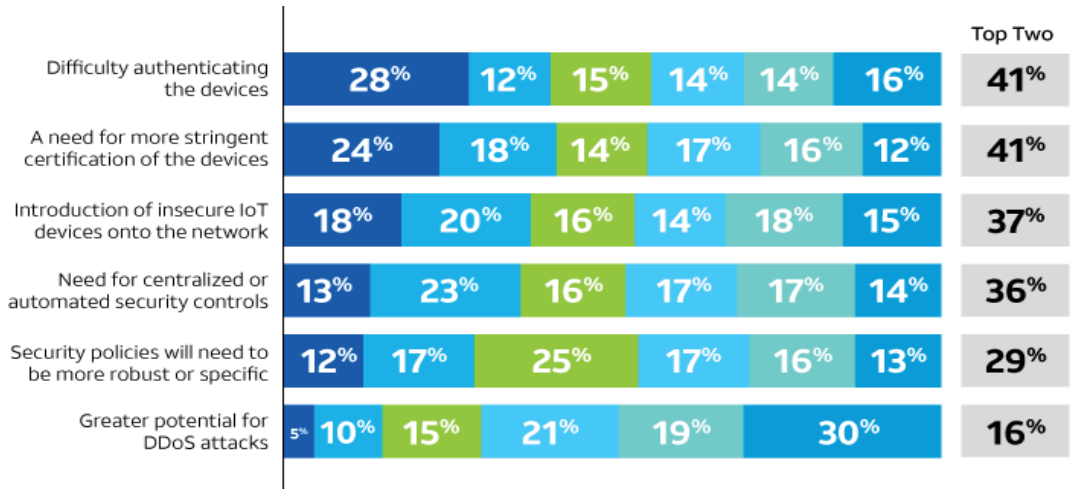
امنیت در نقطه انتهایی شبکه

امنیت در نقطه انتهایی شـــبکه (Endpoint Security) از دیگر

6- Security Virtualization
7- manual



شکل ۱- چالش‌های اصلی پیش‌روی امنیت در نسل پنجم مخابراتی



شکل ۲- چالش‌های امنیتی 5G از دید متخصصان امنیت

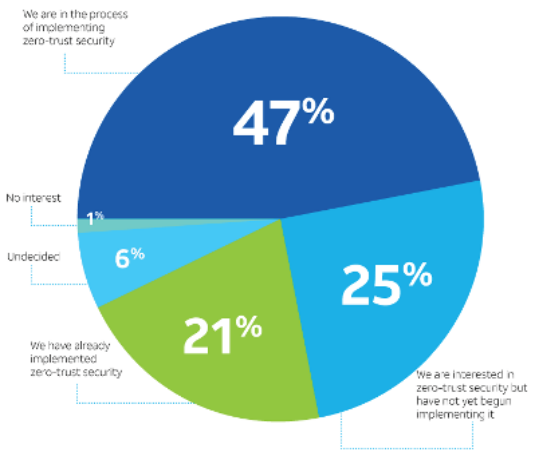
چالش های مهم در 5G خواهد بود. قابلیت مکالمه مستقیم بین ماشین‌ها در 5G در عین کاهش تاخیر تبادل داده سبب می‌شود تجهیزات، خود نیز مجبور باشند مستقل از شبکه مراقب داده‌های مبادله شده باشند و از حملات به سرویس تجهیزات نزدیک به‌هم[۸]، جلوگیری نمایند. در تصویر ۱ چالش‌های اصلی مربوط به امنیت 5G مرتبط با تجهیزات انتهایی نشان داده شده است.

در شکل ۲ رده‌بندی چالش‌های امنیتی تحقق 5G از دید متخصصان امنیت بیان شده است. در این تصویر از چپ به راست درصد افرادی که چالش مدنظر را مهم‌ترین چالش امنیتی پیش‌روی 5G می‌دانند، مشخص شده است.

هویت تجهیزات و میزان دسترسی آن‌ها

افزایش تعداد نودهای ناشناس متصل به شبکه نگرانی نسبت به اینکه چه کسی و در چه‌مکان وزمانی با چه سطحی از دسترسی به شبکه دسترسی دارد را به وجود آورده است. در این بین یک مدل امنیتی از نوع اعتماد-صفر[۹] می‌تواند تا حدی پاسخ‌گوی این نگرانی‌ها باشد. به موازات این مدل، پیاده‌سازی ابزارهای مدیریت و نظارت بر هویت و دسترسی‌های کاربران (IAM[۱۰]) از جمله الزامات اولیه در برقراری امنیت در 5G است. استفاده از MFA[۱۱] می‌تواند به افزایش امنیت در شبکه کمک نماید که تاکنون تحقق آن متوقف مانده است. سازندگان تجهیزات IoT به‌منظور کاهش هزینه‌ها ممکن است بسیاری اصول امنیتی را نادیده بگیرند. در چنین شبکه پیچیده‌ای می‌بایست اصول و رویه‌های کنترل وحفاظت امنیتی به سرعت بروزرسانی شوند و مراکزی برای نظارت بر رویه‌های جاری در بخش‌های مختلف شبکه وجود داشته باشد.

8- Proximity Service (ProSe) intrusions
9- zero-trust
10- Identity and Access Management
11- Multi Factor Authentication



شکل ۳- میزان علاقمندی سازمان‌های بزرگ به تحقق مدل امنیت با اعتماد صفر (Zero-Trust Security Model)

شناسایی تهدیدات و پاسخ به آن‌ها و مدل امنیت اشتراکی[۱۲]

استفاده از ابزارهای تحلیل حملات و تهدیدات شبکه (Threat Analytics) به منظور افزایش هوش و بینش نسبت به تهدیدات احتمالی (Threat Intelligence) از جمله ضروریات تحقق 5G است.

با توجه به سرویس‌های نوین حوزه 5G خصوصا سرویس‌های باتاخیر بسیارکم، کنترل صنایع حیاتی نیازمند کنترل از راه دور بوده و حملات مبتنی بر منطق بیزنسی[۱۳] می‌تواند افزایش چشم‌گیری داشته باشد. افزایش حجم ترافیک داده مبادله شده سبب می‌شود که نیاز به یادگیری ماشین و تحلیل حجم عظیم

12- Shared Security Model
13- Business logic Attack

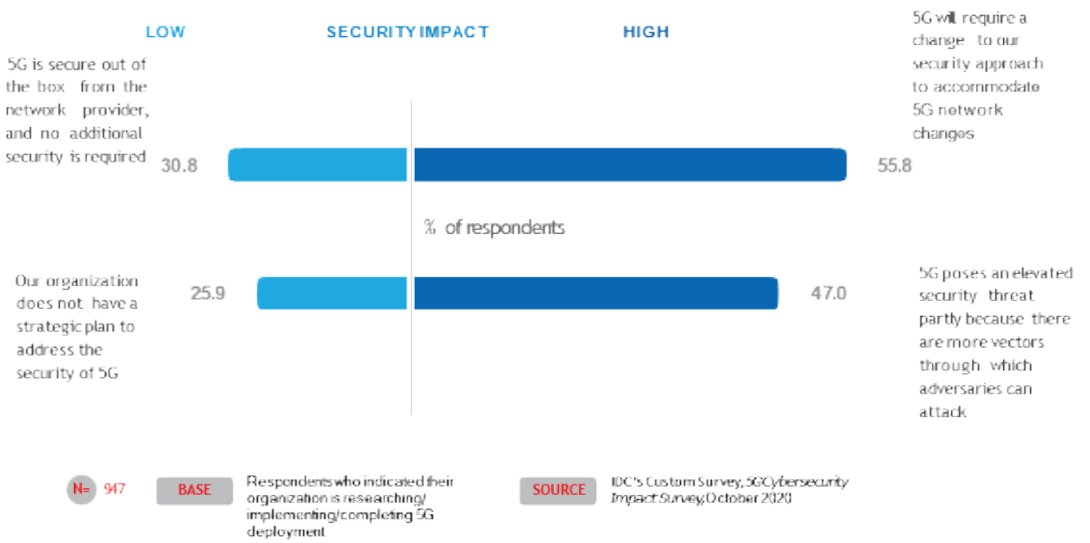
شکل ۴- راه کارهای تضمین امنیت 5G نوکیا

داده‌ها در لبه‌های شـــبکه اهمیت ویژه‌ای یابد. هوش مصنوعی می‌بایست مرتب با انواع حملاتی که برای بیزنس‌های مشابه در نقاط مختلف دنیا اتفاق افتاده، آموزش ببیند و یک مدل اشتراکی برای تحقق امنیت در این نســـل مورد نیاز خواهد بود که در عین افزایش لایه‌های امنیتی، حریم خصوصی را نیز مدنظر قرار دهد. مدل اشتراکی سبب می‌شود سیستم بتواند حملات جدید واقع شده در شبکه را به صورت هوشـــمند شناسایی و نسبت به آن‌ها به‌صورت خودکار پاسخ مناسبی[۱۴] ارائه نماید [۱].

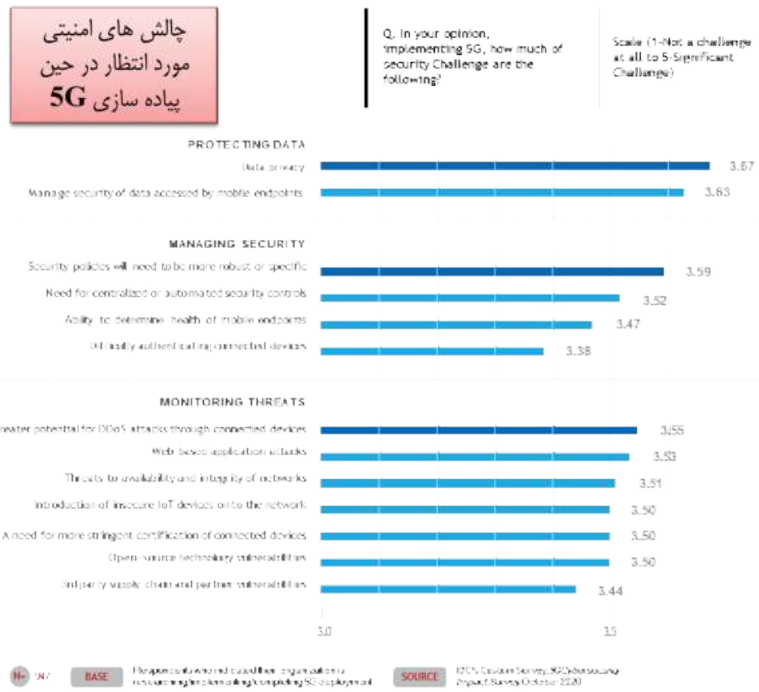
در گام اول، تحقق 5G در کنار 4G قرار داشته (NSA[۱۵]) و بخش اصلی هسته شبکه هم‌چنان مبتنی بر 4G خواهد بود و لذا مزایای شبکه جدید و نقاط ضعف شناخته شده در شبکه قدیمی می‌توانند حمله به سیســـتم را تســـهیل نمایند. اگرچه اساسا 5G امنیت بیشتری نسبت به 4G دارد، لیکن مهاجرت به نسل پنجم مستلزم سپری شدن دوره گذار است. لذا اولین گام هر اپراتور، شناسایی نقاط ضعف زیرســـاخت کنونی و تلاش در جهت ایمن‌سازی آن است.

در یک تحقیق انجام شده توسط AT&T (شـــکل ۵) ۵۵,۸% از کســـانی که در حال بررسی یا استقرار 5G هســـتند گفته‌اند که تضمین امنیت در 5G نیازمند تغییر در رویکرد امنیتی سازمان است و ۲۵,۹% هم گفته‌اند که برنامه مشخص استراتژیک برای مقابله با مشکلات امنیتی 5G ندارند.

14- automated response and remediation
15- Non Stand-Alone Deployment

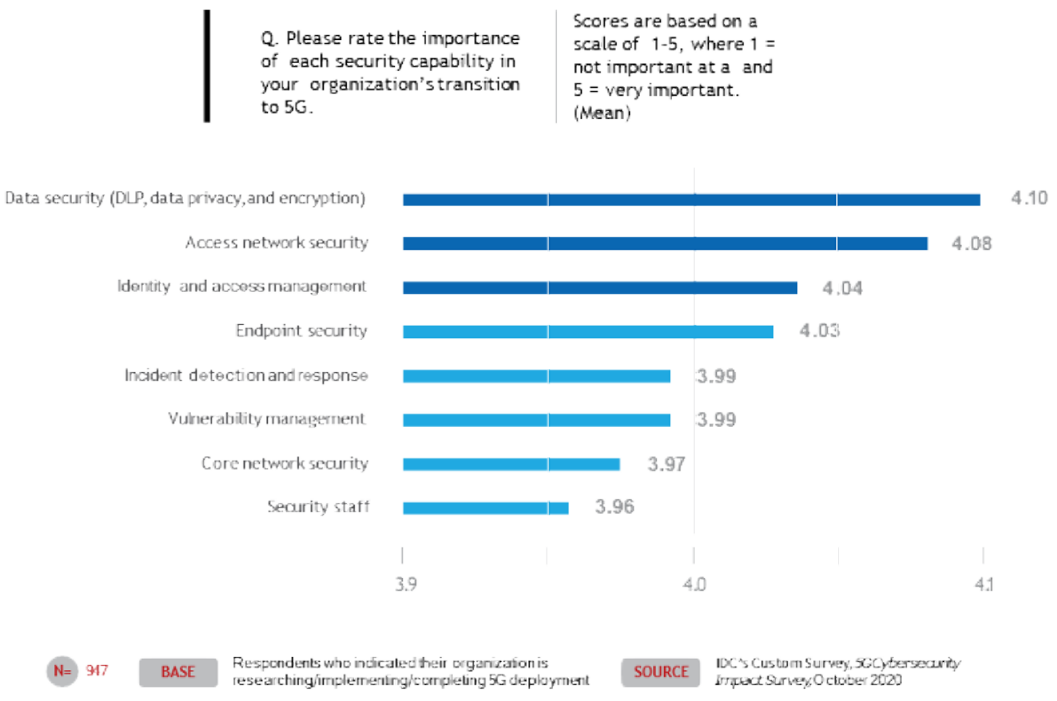


شکل ۵- امنیت در 5G و برنامه سازمان‌ها در قبال آن [۱]



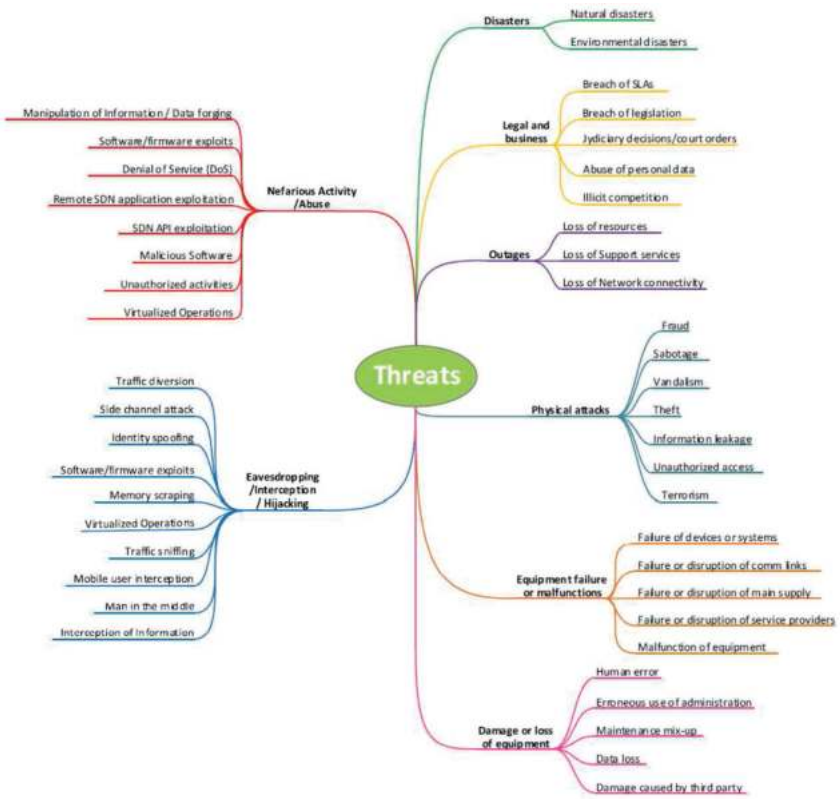
شکل ۶- چالش‌های امنیتی قابل تصور در طول استقرار 5G

در یک تحقیق صورت گرفته (شکل ۶) توسط AT&T بیش از ۶۵% پاسخ‌دهندگان حفظ حریم خصوصی داده‌ها را مهم‌ترین چالش در 5G دانسته‌اند. در مطالعه‌ای جداگانه مدیران IT سازمان‌هایی که در حال بررسی یا استقرار 5G هستند تضمین حریم‌خصوصی داده‌ها را بـــه عنوان مهم‌ترین قابلیت امنیتـــی موردنیاز در طول مهاجرت سازمان به 5G ارزیابی کرده‌اند.



شکل ۷- چالش‌های امنیتی قابل تصور در طول استقرار 5G

در یک دسته‌بندی می‌توان انواع حملات و تهدیدات امنیتی در 5G را به شکل زیر خلاصه نمود:



شکل ۸- انواع تهدیدات امنیتی در یک شبکه 5G/SDN [۳]

به صورت کلی خط مشی برقراری امنیت در 5G می‌بایست موارد ذیل را در نظر بگیرد:

حملات جدید ممکن است از سرعت بالای 5G استفاده نمایند.

تحقق امنیت می‌بایست از مزایای مجازی‌سازی و خودکارسازی/ هوشمندسازی مقابله با حملات مختلف خصوصا در نقاط اصلی محتمل استفاده نماید.

ساختار توزیع شـــده 5G و تنوع تجهیزات متصل به آن خصوصا ربات‌هایی که به صورت مستقل عمل می کنند سبب می‌شود که در مقابل تامین کنندگان مختلف، معماری اعتماد صفر در پیش گرفته شـــود. لذا تمرکز بر تشـــخیص هویت و کنترل دسترسی تجهیزات اهمیت ویژه‌ای خواهد شد تا بتوان سیل عظیم تجهیزات ناشناس متصل به شبکه را کنترل نمود.

افزایش تجهیزات خودکار و رباتیک متصل ممکن است منجر به افزایش حملات توزیع شده ممانعت از سرویس (DDOS) در 5G گردد.

با توجه به سطح گسترده‌تر حملات در شبکه 5G، هوش مصنوعی می‌تواند در مقابله با حملات موثر باشد.

پیچیدگی امنیت در 5G سبب می‌شود اساسا امنیت در این نسل نیازمند همکاری متقابل بین اپراتورهـــای ارائه کننده خدمات و مشتریان دریافت کننده سرویس باشد. به همین جهت یک مدل امنیت اشتراکی می‌بایست با همکاری ذینفعان اصلی توسعه یابد.

با توجه به گستره 5G و پیچیدگی امنیت در آن، شرکت‌های ارائه کننده سرویس امنیت مدیریت شـــده (MSSP[16]) می‌توانند به اپراتورها در کاهش هزینه‌های برقراری امنیت کمک نمایند [1].

نتیجه‌گیری و جمع‌بندی

نسل پنجم شبکه‌های مخابرات سلولی در حال توسعه و استقرار جهانی می‌باشد و اپراتورهای مخابرات سلولی به تدریج در حال پیاده‌سازی آن هســـتند. 5G به عنوان زیرساختی برای سه نوع سرویس مهم دسترســـی پهن باند، مخابرات داده بین ماشین‌ها به صورت انبوه (mMTC)، مخابرات با تاخیر بسیار کم (ULLC) ارائه شده است. تحقق این سرویس‌ها به صورت خودکار مستلزم توسعه زیرساخت‌های ابری در لبه شبکه و افزایش چشم گیر در تعداد نودهای متصل به شبکه خواهد شد. هم‌چنین از طرف دیگر نرم‌افزاری و مجازی شدن زیرساخت‌های شبکه و توسعه پردازش ابری توزیع شده از دیگر الزامات تحقق این سرویس‌ها هستند که همگی آن‌ها به‌خودی خود چالش‌های امنیتی بسیاری در پیش خواهند داشـــت. به منظور مقابله با انواع چالش‌های مطرح شده استفاده از رویکردهای اعتماد صفر و توسعه سیستم‌های مدیریت و کنترل دسترسی توزیع شده الزامی خواهد بود. در عین حال به جهت گستره وسیع سطح حملات در 5G توسعه یک مدل امنیت اشتراکی بین ذینفعان اصلی به کاهش ریسک‌های امنیتی کمک خواهد کرد. پیچیدگی و گستره سطح حمله موجود در شبکه 5G به اندازه‌ای وسیع اســـت که متخصصان حوزه امنیت اپراتورهای موبایل را به استفاده از فراهم کنندگان سرویس امنیت مدیریت شده توصیه می‌کنند. ■

16- Managed Security Service Provider

منابع

[1] P. F. a. E. al, "5G AND THE JOURNEY TO THE EDGE," AT&T, Dallas USA, 2021.

[2] B. M. &. A. C. Team, "Security at the Speed of 5G, Preparing your business for 5G acceleration," AT&T Cybersecurity Insights™ Report, NY, 2019.

[3] L. M. E. Marco Lourenço, "ENISA THREAT LANDSCAPE FOR 5G NETWORKS: Threat assessment for the fifth generation of mobile telecommunications networks (5G)," European Union Agency for Cybersecurity (ENISA), Brussels, 2019.

مجازی سازی
توابع شبکه و امنیت

NFV به مجازی سازی توابع شبکه گفته می‌شود. در یک سیستم NFV تجهیزات سخت‌افزاری در واقع سرورها، ذخیره‌سازها و حافظه‌های با دسترسی تصادفی رم‌ها هستند که توان پردازشی، حافظه ذخیره‌سازی و ارتباطات شبکه‌ای برای NFV ها را از طریق یک لایه مجازی‌سازی فراهم می‌آورند. معماری NFV از چهار لایه مجزا تشکیل شده است. از ریسک‌های امنیتی مرتبط با NFV می‌توان ریسک شکست در تفکیک، شکست در پیاده سازی صحیح توپولوژی شبکه، حملات رد سرویس و ... را نام برد. از نمونه‌های بهترین شیوه‌های تضمین امنیت در NFV نیز می‌توان استفاده از ماژول پلتفرم قابل اعتماد و امنیت کرنل لینوکس، نام برد.

کلمات کلیدی: مجازی سازی توابع، امنیت، SDN، NFV.

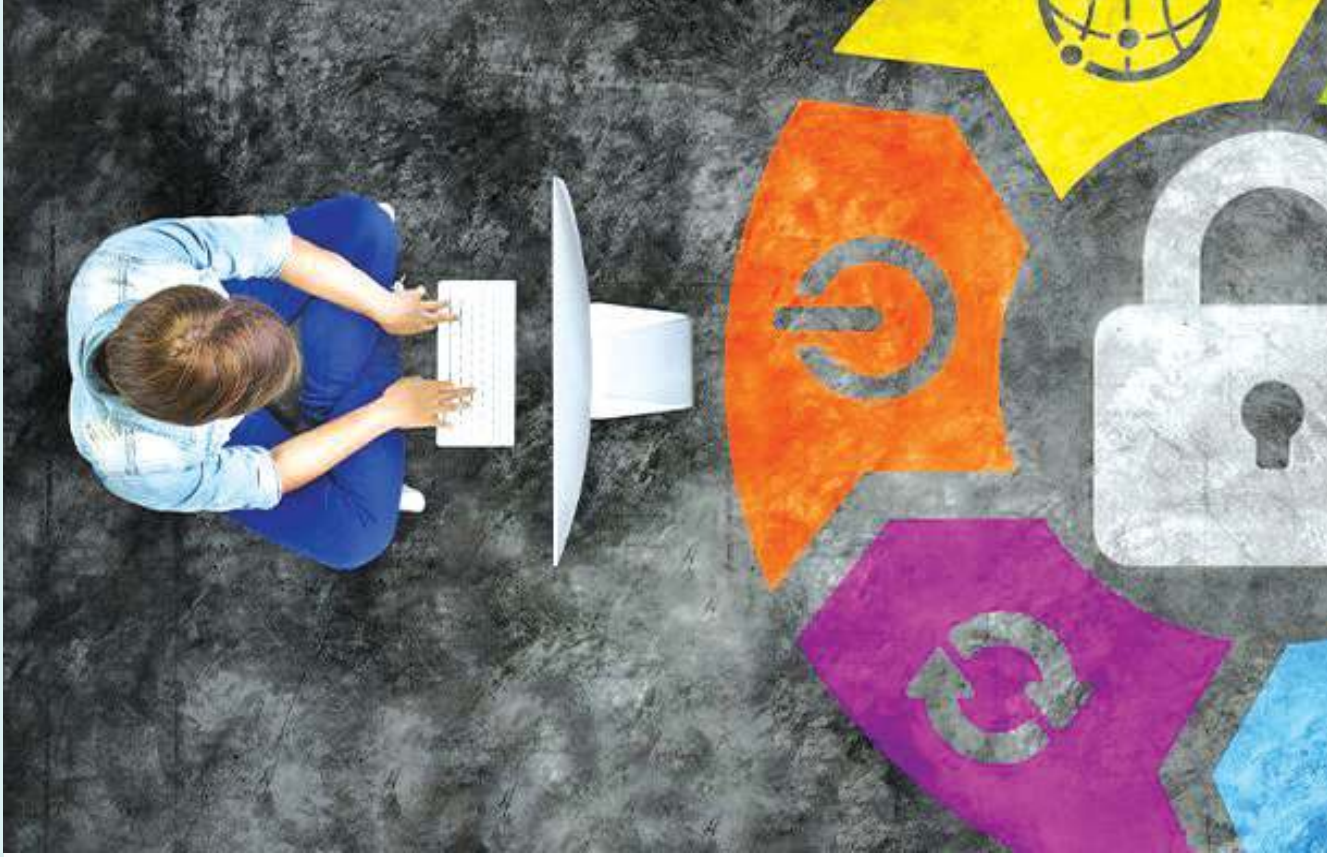
NFV به مجازی سازی توابع شبکه گفته می‌شود و به عبارت دیگر یعنی ارائه سرویس‌های مختلف شبکه بدون نیاز به سخت افزار و این به معنی عدم وابستگی به سخت افزار خاص است. NFV به عنوان یکی از زیرساخت‌های پایه‌ای نوین در 5G برای تحقق بسیاری از سرویس‌های جدید در 5G ضروری است. NFV ابزاری فراهم می‌کند تا بتوان عملکردهای شبکه را بدون نیاز به تجهیزات سخت‌افزاری جدید پیاده‌سازی کرد. این قابلیت به صورت خاص امکان شبکه‌سازی چابک[1] و پیاده‌سازی مقرون به صرفه توابع شبکه را میسر می‌سازد. در یک سیستم NFV تجهیزات سخت‌افزاری در واقع سرورها، ذخیره‌سازها و رم‌ها هستند که توان پردازشی، حافظه ذخیره‌سازی و ارتباطات شبکه‌ای برای NFV ها را از طریق یک لایه مجازی‌سازی[2] فراهم می‌آورند. NFV زمان عرضه به بازار توابع شبکه را کاهش داده و قابلیت برقراری سرویس‌های نرم‌افزاری بر اساس نیاز مشتری در کوتاه‌ترین زمان ممکن را میسر می‌سازد. با این وجود امنیت در NFV نگرانی‌های مهمی درباره قابلیت انطباق آن با زیرساخت‌های مخابراتی به همراه دارد.

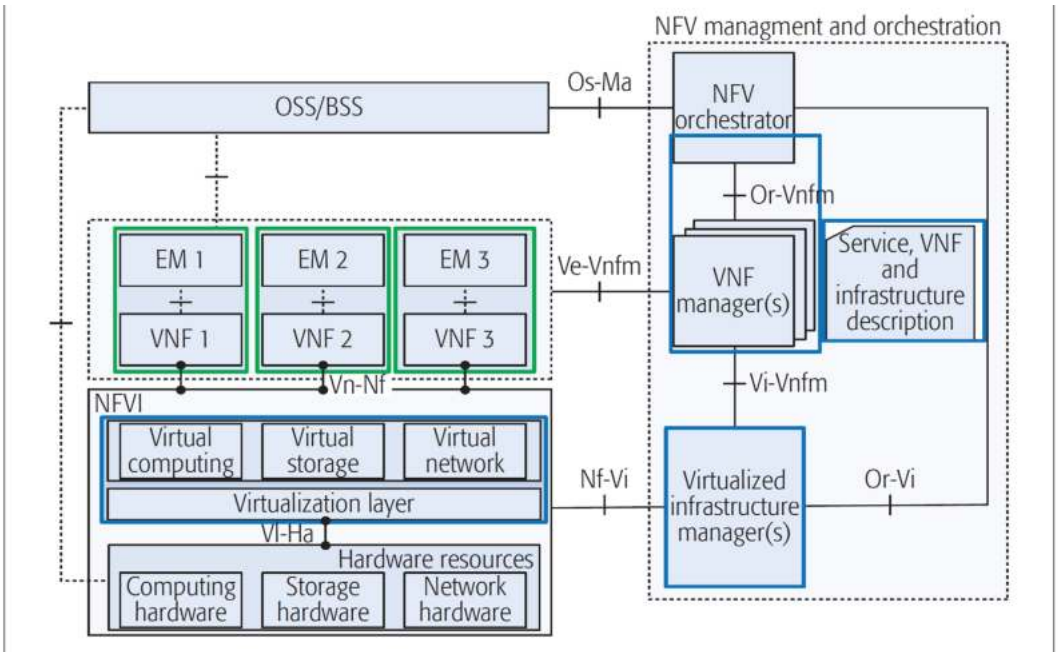
معماری NFV

معماری NFV از چهار لایه مجزا تشکیل شده است:

1- Agile Networking

2- Virtualization Layer





شکل ۱-معماری NFV

لایه مجازی سازی توابع شبکه:[۳] این لایه شامل دو زیربخش VNF[۴] و EMS[۵] اســت. بخش VNF از جمله بلاک‌های ابتدایی معماری NFV است که توابع شــبکه را مجازی سازی می کند و این VNF ها بر روی ماشــین‌های مجازی اجرا می‌شــوند. بخش EMS وظیفه مدیریت VNF را بر عهده دارد. توابع مدیریت شامل مدیریت خطا، پیکربندی، حسابداری، عملکرد و امنیت است.

لایه NFVi[۶]: این لایه زیرســاخت مورد نیاز برای اجرای اجزای سخت افزاری و نرم افزاری را فراهم می کند. به عبارت دیگر محیطی را برای استقرار، مدیریت و اجرای VNF ها ایجاد می کند.

لایه BSS[۸]/**OSS**[۷]: بخش OSS با مدیریت شــبکه، مدیریت خطا، مدیریت پیکربندی و مدیریت خدمات سروکار دارد و BSS مسئول مدیریت مشتری، مدیریت محصول و مدیریت سفارشات است.

لایه MANO[۹]: لایه MANO با هر دو لایه NFVI و VNF تعامل دارد. لایه MANO تمام منابع موجود در لایه زیرساخت را مدیریت می کند، همچنین توانایی حذف و ایجاد منابع را دارد و و مدیریت تخصیص VNF ها نیز از وظایف آن است.

3- VNF
4- Virtual Network Function
5- Element Management System
6- NFV infrastructure
7- Operation Support Subsystem
8- Business Support System
9- Management and Orchestration

ریسک‌های امنیتی NFV

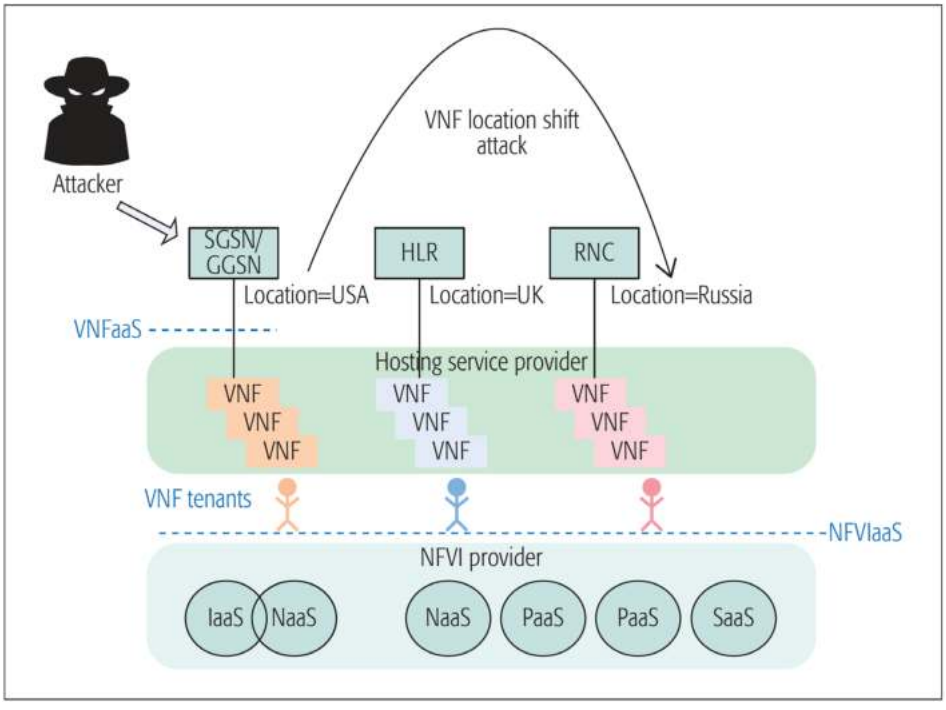
ریسک شکست در تفکیک: سناریویی را در نظر بگیرید که در آن مهاجم با حمله به یک NFV که بر روی یک Hypervisor اجرا می‌شود می‌کوشد تا به آن نفوذ کند. با در دست گرفتن کنترل سیستم عامل یک NFV و به کارگیری ارتباط با شبکه مدیریت ابری و استفاده از ابزارهای کمکی، مهاجم به API مدیریت Hypervisor دست خواهد یافت و از این طریق کنترل Hypervisor را به‌دست خواهد گرفت که این می‌تواند نتایج مخربی به دنبال داشته باشد. این حملات به جهت تفکیک نامناسب بین NFVها و Hypervisor می‌توانند اتفاق بیفتند. این حمله ، VM Scape نامیده می‌شود.

شکست در پیاده‌سازی صحیح توپولوژی شبکه: با به کارگیری NFV، المان‌های شبکه مجازی مانند روترها مجازی می‌توانند به سرعت پیاده‌سازی و به کار گرفته شوند. افزایش سرعت توسعه و پیاده سازی شبکه ممکن است سبب شود که ما نظارت کافی را از دست داده و در برخی نقاط پروتکل‌های امنیتی را در نظر نگیریم، برای نمونه فایروال مورد نیاز را نصب نکنیم. این امر یک نقطه ضعف امنیتی بوده و ممکن است به سرعت موجب نفوذ مهاجمان به شبکه گردد. در مقایسه با پیاده‌سازی تجهیزات شبکه فیزیکی پویایی تجهیزات شبکه مجازی و ارتباطات آن می‌تواند منجر به تفکیک نامناسب بین شبکه و زیرشبکه‌های آن گردد. مهاجم در صورت نبود تجهیزات حفاظت امنیتی کافی مانند دیوار آتش قوی، IPS/IDS و DPI قادر خواهد بود اطلاعات کافی در مورد زیرساخت شبکه چندسایتی را به‌دست بیاورد.

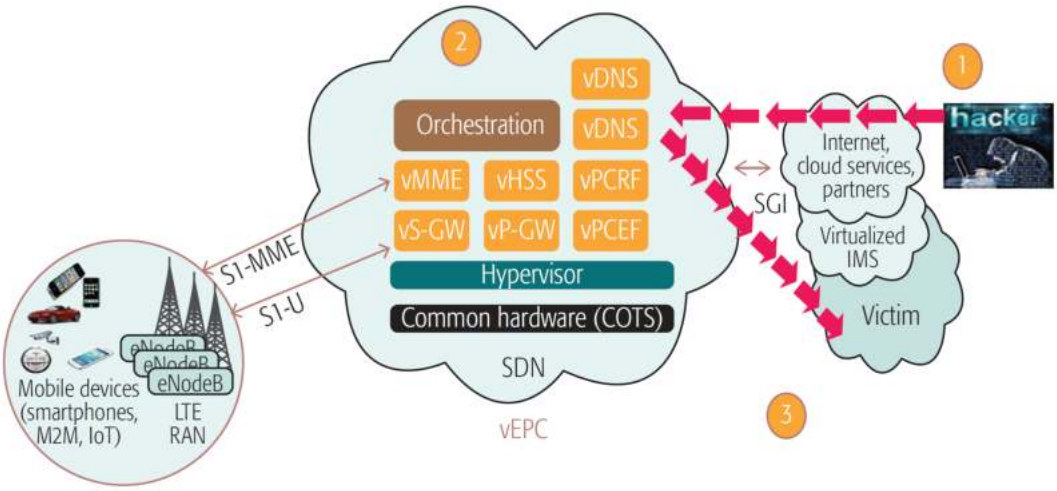
شکست در انطباق با قوانین رگولاتوری: در گذشته با توجه به حضور المان‌های فیزیکی توابع شبکه مانند سوئیچ‌ها و روترها امکان تغییر موقعیت فیزیکی آن‌ها وجود نداشت اما با توسعه SDN و ایجاد NFVها امکان حملات تغییر موقعیت قرارگیری یک NFV از یک نقطه به نقطه دیگر وجود خواهد داشت. چنانچه در شکل ۲ نیز نشان داده شده است تغییر موقعیت به نحوی که با قوانین رگولاتوری انطباق نداشته باشد ممکن است منجر به توقف کامل سرویس گردد که احتمال دارد هدف اصلی مهاجم برای آسیب به اپراتور باشد.

حملات رد سرویس: حملات رد سرویس به شبکه مجازی یا واسط‌های عمومی NFV ها انجام می‌شود تا بتوانند منابع شبکه را به طور کامل مصرف و معطل نمایند و دسترسی به سرویس را متوقف کنند. یک حجم زیاد از ترافیک می‌تواند از یک NFV آسیب دیده تولید شده و به دیگر NFV ها ارسال شود. برای نمونه یک حالت از این حملات که به DNS Amplification نیز معروف است در شکل ۳ ارائه شده است. در این تصویر فرد مهاجم پس از حمله و به‌دست گرفتن کنترل چندین قربانی، مرتب اقدام به تولید تعداد زیادی درخواست ARP می‌نماید. این درخواست‌ها به سمت سرور DNS هدایت می‌شوند. Orchestrator مخصوص این سیستم قادر خواهد بود در صورت افزایش حجم درخواست‌ها یک نسخه جدید از این سرور vDNS را بارگذاری نماید و این فرآیند تکراری تا زمانی که ظرفیت سیستم برای توسعه بیشتر به پایان برسد ادامه خواهد یافت و پس از آن تبعا سیستم قادر به پاسخ‌گویی به درخواست‌های بیشتر نخواهد بود.

مهاجمان مزاحم داخلی: گاهی اوقات ممکن است که حملات از



شکل ۲- حمله تغییر موقعیت قرارگیری NFV



شکل ۳- یک نمونه از حمله DNS Amplification با هدف ایجاد شرایط رد سرویس

داخل شبکه و توسط مهاجمان بدخواه داخلی باشد. در این سناریو یک کاربر مدیر سیستم[10] ممکن است که کپی از حافظه سیستم دریافت کرده و با استخراج شناسه کاربری کاربران و کلمات کلیدی SSH امنیت سیستم را به خطر بیندازد. در چنین سناریویی وجود یک سیستم مدیریت شناسه کاربران و کنترل دسترسی یا همان IAM می تواند مفید باشد.

علیرغم خطرات امنیتی معرفی شـــده توســـط NFV و اقدامات امنیتی ذکر شده که باید در نظر گرفته شوند، این واقعیت را باید در نظر گرفت که NFV فرصت‌های امنیتی جدیدی فراهم می کند درحالی که از راهکارهای تحقـــق امنیت از زمان طراحی و امنیت بعنوان یک‌سرویس پشتیبانی می کند. مزیتی که NFV به ارمغان می‌آورد این‌است که نمونه‌ســـازی خودکار و مدیریت چرخه عمر منابع و خدمات مجازی را از طریق چارچوب NFV MANO ترویج می کند. در نهایت، شایان ذکر است که پیاده سازی طراحی خوب کنترل‌های امنیتی، نظارت مستمر، پیشگیری، شناسایی و کاهش حملات در معماری NFV را تضمین می کند که برای یک محیط امن NFV ضروری است [۱].

نمونه‌های از بهترین شیوه‌های تضمین امنیت در NFV

استفاده از ماژول پلتفرم قابل اعتماد(TPM):[11] با استفاده از یک TPM به عنوان یک سخت‌افزار قابل اعتماد، اجزای حساس سیستم از قبیل سخت‌افزار پلتفرم، BIOS، OS Kernel و دیگر اجزای حساس سیســـتم به صورتی امن ذخیره‌سازی و نگهداری می‌شوند. اطلاعات داخل پلتفرم صرفا زمانی که سیستم مجددا راه‌اندازی می‌شود بازخوانی می‌شـــوند و هیچ راهی برای نوشتن اطلاعات جدید بر روی TPM در حالتی که سیستم روشن و در حال اجرا باشد وجود ندارد. تایید صحت و اعتبار اطلاعات داخل آن نیز صرفا توسط رویه کنترل راه‌اندازی (LCP[12]) TPM و یا توسط سرور راه دور Attestation قابل انجام خواهد بود.

امنیت کرنل لینوکس: در پلتفرم‌های مجازی کرنل سیستم‌های میزبان یک جزء بسیاری حیاتی اســـت که تجزیه بین کاربرها را فراهم می کند. SELinux ماژولی‌اســـت که توسط آژانس امنیت ملی آمریکا توسعه یافته اســـت و این ماژول در داخل کرنل ایجاد شده و تفکیک قوی بین کاربران موقت بخش‌های مختلف ماشین مجازی ایجاد می‌نماید. مجازی‌سازی امن (sVirt[13]) یک فرم جدید از SELinux است که به منظور یکپارچه‌سازی اجباری بین امنیت کنترل دسترسی با Hypervisorهای مبتنی بر لینوکس توسعه یافته اســـت. فرای این ابزارها، ابزارهای ایمن‌سازی کرنل دیگری نیز وجود دارند که Hidepd یکی از آن‌ها است. این نرم‌افزار به این منظور ایجاد شده است که کاربران غیرمجاز یک سیستم نتوانند به اطلاعات فرآیندهای کاربران دیگر دسترسی یابند.

بررســـی و نظارت بر Hypervisor: با بررســـی و نظارت بر Hypervisor می تواند با دقت بالا نرم‌افزارهای نصب شده داخل ماشین‌های مجازی را بررســـی کند تا بتواند رفتارهای غیرعادی را شناسایی و گزارش نماید. این ســـامانه ناظر بر Hypervisor به عنوان یـــک IDS داخلی عمل می کند که بـــه اطلاعات وضعیت کلیه VM های سیستم دسترسی دارد به گونه‌ای که Root Kit و Boot Kit داخل ماشین‌های مجازی به سادگی قابل پنهان کردن نخواهند بود.

رمزنگاری حافظه NFVها: دیسک‌های حافظه که مرتبط با NFV ها هستند ممکن است که شامل داده‌های حساس باشند. لذا یکی از راه های حفاظت از آن‌ها رمزنگاری آن‌ها و ذخیره‌سازی کلیدهای رمزنگاری در نقاطی ایمن مانند ماژول TPM اســـت. علاوه بر این

10- System Administrator
11- trusted platform module (TPM)
12- launch control policy
13- Secure Virtualization

	Security risk	Target	Best practices
1	Compromised hypervisor	Platform	Separation of VM and management traffic, regular hypervisor patching
2	Isolation failure	Platform/VNFs	Hypervisor introspection, security zoning
3	Platform integrity	Platform	TPM boot integrity, remote attestation
4	DDoS attack	VNFs	Flexible VNF strategic deployment to defend against DDoS
5	Malicious insider	VNFs	Volume/swap encryption, VNF image signing, strict operational practices
6	Regularity compliance failure	VNFs	Geo-tagging using remote attestation

شکل ۴ - خلاصه‌ای از ریسک‌های امنیتی و اهداف آن‌ها و راهکارهایی کاهش احتمال وقوع آن‌ها

Hypervisor باید به گونه‌ای برنامه‌ریزی نماید که بتواند به صورت امن دیسک‌های مجازی را در صورت Crash کردن NFV ها کاملا پاک نموده و اطلاعات روی آن را از بین ببرد. VM Swapping یک تکنیک مدیریت حافظه است که به کمک آن می توان بخش‌های حافظه را از حافظه اصلی به دیسک‌هایی انتقال داد که به عنوان حافظه ثانویه به کار می‌روند تا بتوان بازدهی عملکرد سیستم را افزایش داد.

Remote Attestation: تکنیک تایید از راه دور می‌تواند به منظور ارزیابی قابلیت اعتماد یک پلتفرم NFV به کار رود. این مفهوم مبتنی بر boot integrity measurement leveraging TPM است. تایید از راه دور می‌تواند به عنوان یک سرویس ارائه شود و می‌تواند توسط مالک یک پلتفرم و یا مصرف کننده آن به منظور اثبات آنکه آیا پلتفرم به شکلی قابل اعتماد Boot شده است مورد استفاده قرار بگیرد. نمونه‌هایی از پیاده‌سازی عملیاتی و موجود کنونی برای سرویس تایید از راه دور شامل ابزار یکپارچگی ابر باز (OpenCIT[۱۴]) است که یک نرم‌افزار Open Source بوده و در Github میزبانی می شود.

در جدول زیر خلاصه‌ای از ریسک‌های امنیتی که معرفی گردید و در مورد آن‌ها صحبت شد، اهداف مهاجمان ایجاد کننده این ریسک‌ها و راهکارهایی به منظور کاهش احتمال وقوع این ریسک‌ها به صورت خلاصه ارائه شده است [۲].

نتیجه‌گیری

در این مقاله به صورت مختصر به معرفی ساختارهای جدید شبکه مبتنی بر نرم‌افزار و بررسی چالش‌های امنیتی پیش‌روی استقرار ساختارهای SDN/NFV پرداختیم. دیدیم که نرم‌افزاری شدن ساختار با وجود مزایای شگرف و انعطاف زیادی که با خود به همراه دارد چالش‌های امنیتی جدیدی به وجود می‌آورد که تحقق آن‌ها را مستلزم در نظر گرفتن ملاحظات امنیتی خواهد کرد. در واقع نرم‌افزاری شدن شبکه در عین چالش‌های امنیتی فرصت‌ها، محافظت امنیتی جدیدی نیز فراهم می کند. انواع مختلفی از حملات از جمله حملات ردسرویس، عدم انطباق با قوانین رگولاتوری و تغییرات ناخواسته معماری شبکه تنها برخی از چالش‌های پیش‌روی تحقق این معماری بودند که معرفی شدند. دیدیم که با نمونه‌سازی خودکار و مدیریت چرخه عمر منابع و خدمات مجازی از طریق چارچوب NFV MANO تحقق امنیت در این ساختار تسهیل خواهد شد. در نهایت نیز چند راهکار نوین برای حفاظت امنیتی در سیستم شامل استفاده و امن‌سازی کرنل لینوکس، رمزنگاری NVFها و نظارت بر hypervisorها معرفی گردید. به طو خلاصه تضمین امنیت ساختار جدید شبکه نرم‌افزاری نیازمند دقت کافی در طرح‌ریزی و استقرار امن آن خواهد بود.

14- open cloud integrity tool

منابع

[1] T. AssemAlameddine1MakanPourzandi-AmineBoukhtouta, “NFV security survey in 5G networks: A three-dimensional threat taxonomy,” Computer Networks, vol. 197, pp. 1-29, Oct 2021.

[2] S. Lal, T. Taleb and A. Dutta, “NFV: Security Threats and Best Practices,” IEEE Communications Magazine, vol. 55, no. 8, pp. 211 - 217, 2017.

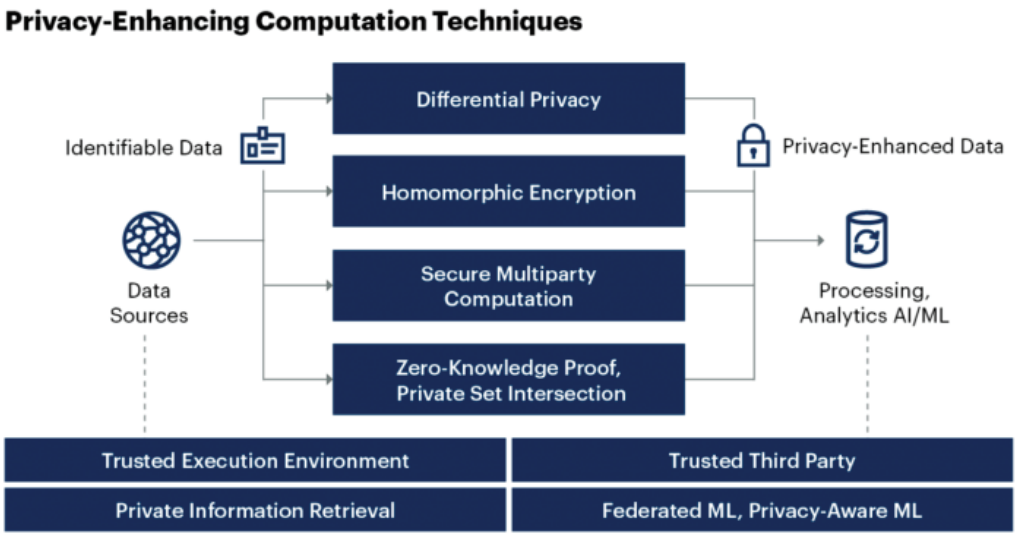
محاسبات با حفظ حریم خصوصی

محاسبات با حفظ حریم خصوصی، گروهی از سیستم‌ها، فرآیندها و تکنیک‌هایی هستند که پردازش را قادر می‌سازد تا از داده‌ها ارزش به‌دست آورد در حالی که حریم خصوصی و امنیت برای افراد حفظ می‌گردد. انواع روش‌های نرم افزاری و سخت افزاری برای محافظت از داده‌ها وجود دارد. برخی از نمونه‌ها عبارتند از: محاسبات چند جانبه ایمن، رمزگذاری هومومورفیک، اثبات دانش صفر و محیط اجرایی قابل اعتماد (TEE). هر تکنیک مزایا و معایب خود را داشته و با چالش نحوه محافظت ایمن از داده‌های در حال استفاده دست و پنجه نرم می‌کند. PETها به طرق مختلف به حفظ حریم خصوصی و داده‌ها کمک می‌کنند. دسته اول PETها ابزارهایی هستند که داده‌ها را تغییر می‌دهند. گروه دیگری از PETها به جای تغییر دادن داده‌ها، بر پنهان کردن یا محافظت از داده‌ها تمرکز می‌کنند. و در نهایت، دسته سوم سیستم‌ها و معماری داده‌های جدید را برای پردازش، مدیریت و ذخیره داده‌ها نشان می‌دهد.

کلمات کلیدی: محاسبات با حفظ حریم خصوصی، تکنولوژی حفظ حریم خصوصی، تغییر داده، حفاظت داده

"تا سال ۲۰۲۵، حدود ۶۰ درصد از سازمان‌های بزرگ از یک یا چند تکنیک محاسبات با حفظ حریم خصوصی در تجزیه و تحلیل، هوش تجاری یا رایانش ابری استفاده خواهند کرد." گارتنر محاسبات با حریم خصوصی را به عنوان یک روند کلیدی فناوری سازمانی برای سال ۲۰۲۲ معرفی کرده است.

ارزش واقعی داده‌ها صرفاً در داشتن آن‌ها نیست، بلکه در نحوه استفاده از آن برای مدل‌های هوش مصنوعی و تجزیه و تحلیل است.



شکل ۱ مدل بررسی شده در گارتنر

روش‌های محاسبات با حفظ حریم خصوصی (PEC) اجازه می‌دهد که داده‌ها در بین اکوسیستم‌ها به اشتراک گذاشته ضمن ایجاد ارزش، حریم خصوصی نیز حفظ شود.

تکنیک‌های حفظ حریم خصوصی

PETها به طرق مختلف به حفظ حریم خصوصی و داده‌ها کمک می‌کنند. دسته اول PETها ابزارهایی هستند که داده‌ها را تغییر می‌دهند. این دسته معمولاً به دنبال برهم زدن یا قطع رابطه بین داده‌ها و فردی که با آن‌ها در ارتباط است هستند. گروه دیگری از PETها به جای تغییر دادن داده‌ها، بر پنهان کردن یا محافظت از داده‌ها تمرکز می‌کنند. رمزنگاری نمونه‌ای از این نوع است زیرا فرمت داده‌ها را تغییر می‌دهد، اما به‌جای تغییر دائمی، آن‌ها را موقتاً پنهان می‌کند. در نهایت، دسته وسیعی از PETها وجود دارد که سیستم‌ها و معماری داده‌های جدید را برای پردازش، مدیریت و ذخیره داده‌ها نشان می‌دهد. برخی از این سیستم‌ها، داده‌ها را برای محاسبات یا ذخیره‌سازی تجزیه می‌کنند در حالی که برخی دیگر لایه‌های مدیریتی را برای ردیابی و ممیزی فراهم می‌نمایند که اطلاعات کجا و برای چه هدفی جریان دارد.

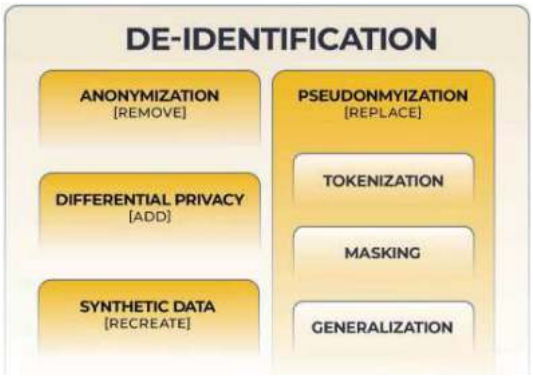
تغییر داده‌ها[1]

هویت زدایی داده‌ها[2] یک اصطلاح فراگیر شامل انواع روش‌ها و ابزارهایی برای شناسایی خصوصیات مجموعه داده‌ها می‌باشد. بسیاری از فعالیت‌های داده نیازی به شناسایی مستقیم افراد یا پیوند دادن آن‌ها به داده‌های مرتبط ندارند. برای مثال، واحدها ممکن است فقط نیاز به درک آمار توصیفی، مانند میانگین‌ها، یا نحوه تعامل مشتریان با محصولات به عنوان یک گروه داشته باشند. برای این گونه موارد می‌توان داده‌ها را به‌طور دائم تغییر

1- Altering data
2- Data de-identification

شکل ۲ روش‌های افزایش حریم خصوصی

داد تا پتانسیل ربط دادن آن‌ها به یک فرد کاهش یابد. در ادامه روش‌هایی از هویت زدایی مورد بررسی قرار می‌گیرد.



شکل ۳ هویت زدایی

ناشناس سازی[3]

اصطلاح ناشناس سازی به طور گسترده در بحث‌های مربوط به حفظ حریم خصوصی استفاده می‌شود و به طور کلی می‌تواند به معنای هویت زدایی باشد. ناشناس‌سازی یکی از تکنیک‌های اصلی افزایش حریم خصوصی است که در صنایع و سازمان‌ها استفاده می‌شود، هرچند که ثابت شده است اگر چندین منبع داده ترکیب شوند، نسبتاً ناامن است. حذف شناسه‌ها از داده‌ها می‌تواند یک فرآیند دستی یا خودکار باشد. برای فرآیندهای خودکار، تأیید اینکه اطلاعات صحیح، در حال حذف شدن است مهم است.

مشکل اصلی ناشناس سازی این است که اطلاعات حذف شده از مجموعه داده‌ها را می‌توان با ترکیب اطلاعات از منابع مختلف بازسازی کرد. در دهه ۱۹۹۰، دکتر لاتانیا سوینی دریافت که داده‌هایی که شناسه‌های مستقیم (نام، آدرس، شماره تلفن و غیره) را حذف می‌کنند، هنوز هم می‌توانند برای شناسایی افراد هنگام ترکیب با پایگاه‌های داده دیگر، از جمله آن‌هایی که در دسترس عموم هستند، استفاده شوند. وی دریافت که ٪۸۷ از جمعیت ایالات متحده را می‌توان تنها با استفاده از تاریخ تولد، جنسیت و کد پستی آن‌ها شناسایی کرد.

قوانین جدید، مانند GDPR، این ضعف را تصدیق می‌کند و حذف اطلاعات را به اندازه کافی قوی برای هویت زدایی نمی‌داند.

مستعارسازی[4]

مستعار سازی فرآیندی است که طی آن بخش‌های از اطلاعات که سری تلقی می‌شوند توسط مقادیری تصادفی جایگزین می‌شوند. این روش در کنار راه‌های دیگری همچون رمزنگاری داده‌ها، به منظور حفاظت از اطلاعات شخصی افراد، حریم خصوصی آن‌ها و به طور کلی افزایش سطح امنیت استفاده می‌شود.

3- Anonymization
4- Pseudonymization

توکن‌سازی[5]، پوشاندن[6] و عمومی‌سازی[7] روش‌های مختلف مستعار سازی هستند. در حالی که این روش‌ها متفاوت هستند، اما یک ویژگی مشترک دارند و آن اینکه به جای اطلاعات حساس و قابل شناسایی از اطلاعات ساختگی استفاده می‌شود در عین حال قابل استفاده هم هستند و به همین دلیل امکان پردازش و تجزیه و تحلیل مداوم داده‌ها پس از مستعار سازی نیز فراهم است.

توکن‌سازی داده حساس را با یک توکن جایگزین می‌کند. توکن‌ها معمولاً رشته‌های تصادفی از اعداد و حروف هستند و در بسیاری از موارد قابل برگشت می‌باشند. یک موجودیت کلیدی خواهد داشت که توکن‌ها را با اطلاعات واقعی آن‌ها مطابقت می‌دهد.

استفاده رایج از توکن‌سازی در سیستم‌های پرداخت است. هنگامی که یک مصرف کننده کارت اعتباری را می‌کشد، آن عدد با یک توکن جایگزین شده و تنها توکن ذخیره می‌شود.

شبکه‌های کارت دارای کلیدی هستند که بدانند کدام توکن با شماره کارت واقعی یک فرد مرتبط است.

پوشاندن مانند توکن‌سازی است، قطعات داده را با رشته‌های تصادفی از اعداد و/یا حروف جایگزین می‌کند. یک تفاوت کلیدی بین توکن‌سازی و پوشاندن این است که پوشاندن معمولاً برای داده‌های در حال پردازش اعمال می‌شود و دائمی می‌باشد. پردازش ممکن است شامل ایجاد، ویرایش، حذف، مشاهده یا چاپ داده باشد.

عمومی‌سازی یک تکنیک متفاوت است که یک عبارت عمومی را به جای یک عبارت خاص وارد می‌کند. معمولاً در شناسه‌های غیر مستقیم استفاده می‌شود. به عنوان مثال، به جای افشای سن واقعی یک فرد، یک پایگاه داده عمومی شده ممکن است هر فرد را به یک محدوده سنی، مانند «۱۸-۳۰» یا «۳۱-۴۵» اختصاص دهد.

K-Anonymization یک تکنیک مرتبط است که تعداد خطوطی را که باید عمومی شوند تا اینکه هیچ فردی نتواند از یک گروه بزرگ متمایز شود تعیین می‌کند.

مستعار سازی بسیار بالغ است و چندین استاندارد برای این تکنیک‌ها وجود دارد. برای مثال، شورای استانداردهای امنیتی صنعت پرداخت (PCI SSC)، توکن‌سازی را روشی تایید شده برای محافظت از داده‌های کارت می‌داند.

متأسفانه، مانند ناشناس‌سازی که در بالا توضیح داده شد، این روش‌ها به‌طور خودکار حریم خصوصی ایجاد نمی‌کنند، حتی اگر اطلاعات حساس و قابل شناسایی مانند شماره کارت اعتباری مبهم شوند.

محققان MIT دریافتند که می‌توانند افراد را بر اساس فراداده یا جزئیات توصیفی مرتبط با تراکنش‌های کارتشان علی‌رغم استفاده از توکن‌ها، شناسایی کنند.

5- tokenization
6- masking
7- generalization

حریم خصوصی تفاضلی[8]

حریم خصوصی تفاضلی به جای حذف یـا تغییر عناصر داده به شناسـه‌های مبهم، داده‌های تصادفی، اضافی یا «نویز» را اضافه می‌کند. هدف از حریم خصوصی تفاضلی اضافه کردن داده‌های تصادفی و اضافی به اندازه کافی است تا اطلاعات واقعی در میان نویز پنهان شـود. حفظ حریم خصوصی تفاضلی امکان تجزیه و تحلیل دقیق روی داده‌ها را به صورت کلـی فراهم می‌کند، زیرا علیرغم نویز اضافه شده، داده‌های ترکیبی می‌توانند سیگنال‌های دقیقی ارائه دهند.

یکی از مزایای حریم خصوصی تفاضلی این اسـت که شناسایی مجدد با ترکیب مجموعه داده‌ها دشوار است زیرا مهاجم نمی‌داند کدام اطلاعات درست است.

داده‌های مصنوعی[9]

شکل دیگری از تغییر داده‌ها برای محافظت از حریم خصوصی، ایجاد داده‌های کاملاً جدید و مصنوعی اسـت. این گامی فراتر از مستعار سازی است، که داده‌های واقعی را با داده‌های تغییر یافته جایگزین می‌کند، یا حریم خصوصی تفاضلی، که اطلاعات اضافی و جعلی را در مجموعه داده‌های واقعـی وارد می‌کند. داده‌های مصنوعی معمولاً از طریق یادگیری ماشـین ایجاد می‌شـوند و ویژگی‌های داده‌های دنیای واقعی را تقلید می‌کنند.

داده‌ها با تغذیه داده‌های واقعی در الگوریتم‌های یادگیری ماشین ایجاد می‌شوند، که ویژگی‌ها و روندها را شناسایی می‌کنند و آن‌ها را در اطلاعات مصنوعی تکرار می‌کنند.

مزیت اصلی استفاده از داده‌های مصنوعی این است که می‌توان آن را برای موارد استفاده مختلف سفارشی کرد و در عین حال نیاز به جمع آوری و ذخیره اطلاعات واقعی در مورد افراد را محدود نمود. داده‌های مصنوعی را می‌توان برای آموزش مدل‌های دیگر یا برای آزمایش سیستم‌های جدید استفاده کرد.

یکی از اشکالات اصلی داده‌های مصنوعی، وابستگی آن به کیفیت داده‌های اصلی اسـت که برای آموزش سیسـتم‌های یادگیری ماشین استفاده شده است. ممکن است در داده اصلی سوگیری وجود داشته باشد یا ممکن است نماینده داده‌های مورد نظر نباشد و داده‌های مصنوعی آن مسائل را تکرار کند.

محافظت از داده[10]

فناوری‌های حفـظ حریم خصوصـی که از داده‌هـا محافظت می‌کنند، اطلاعات اصلی را تغییر نمی‌دهند. در عوض، آن داده‌ها را در زمان‌های خاصی نامفهوم یا غیرقابل استفاده می‌کنند تا از دسترس اشخاص غیرمجاز به آن جلوگیری گردد.

برای PETهایی که از داده‌ها محافظت می‌کنند، مهم اسـت که سـه حالت مختلف محافظت از داده‌ها متمایز گردند: در حالت استراحت[11]، در حال اسـتفاده[12] یا در حال انتقال[13]. روش‌های مختلفی برای محافظت از داده‌ها وجود دارد.

در ادامه به اختصار به برخی از این تکنولوژی‌ها خواهیم پرداخت:

رمزنگاری

قابل تشـخیص‌ترین و رایج‌ترین شـکل محافظـت از داده‌ها،

8- Differential Privacy
9- Synthetic Data
10- shielding data
11- at-rest
12- in-use
13- in-transit

رمزگذاری اســـت. رمزگذاری یک فرآیند برگشت‌پذیر است که داده‌ها را به شـــکل نامفهومی به نام متن رمـــز تبدیل می‌کند. رمزگشایی متن رمز، داده‌ها را به شکل اصلی خود (که به آن متن ساده می‌گویند) تبدیل می‌کند.

هدف از رمزگذاری و رمزگشایی این است که فقط کاربران مجاز برای دسترسی به متن ساده با استفاده از یک کلید برای تبدیل، دسترسی داشته باشـــند. حتی اگر کاربران غیرمجاز به داده‌های رمزگذاری شـــده یا متن رمز شده دسترســـی پیدا کنند، بدون دسترسی به کلید قادر به خواندن آن نخواهند بود.

رمزنگاری هومومورفیک

در حالی که رمزگذاری سنتی می‌تواند داده‌ها را در حالت استراحت و در حین انتقال ایمن کند، رمزگذاری هومومورفیک می‌تواند از داده‌های در حال استفاده محافظت کند. محافظت از داده‌های در حال استفاده دشوارتر از دو حالت دیگر است زیرا هنوز باید داده‌ها برای پردازش قابل درک باشند. رمزنگاری هومومورفیک قابلیت استفاده از داده‌ها را در زمانی که محافظت می‌شود حفظ می‌کند. در این تکنیک همچنان یک کلید معمولا نامتقارن وجود دارد که برای رمزگشایی اطلاعات استفاده می‌شود، اما داده‌ها می‌توانند در طول پردازش محافظت شوند.

این تکنیک هنوز در مراحل اولیه بلوغ خود است اما این پتانسیل را دارد که به طور گســـترده در برنامه‌هـــای کاربردی مختلف از قراردادهای هوشـــمند گرفته تا پردازش پرداخت مورد استفاده قرار گیرد. برخی از شرکت‌های مبتنی بر فناوری شروع به استفاده مستقیم از این تکنیک در محصولات خود کرده‌اند. به عنوان مثال، رمزگذاری هومومورفیک برای نظارت بـــر اینکه آیا گذرواژه‌های ذخیره‌شده در مرورگرها در معرض نقض داده‌ها قرار گرفته‌اند یا خیر، استفاده می‌شود. با این حال، رمز عبور در طول این تجزیه و تحلیل رمزگذاری شـــده باقی می‌ماند. شـــکل‌های مختلفی از رمزگذاری هومومورفیک وجـــود دارد که بر اســـاس پیچیدگی محاســـباتی که روی داده‌ها انجام می‌شـــود متفاوت هســـتند. دسته‌بندی HE شامل سه دسته زیر می‌باشد:

- partially homomorphic encryption,
- somewhat homomorphic encryption,
- fully homomorphic encryption

افزایش حریم خصوصی سخت‌افزاری[14]

تولید کنندگان رایانه به طور فزاینده‌ای ویژگی‌های غیرقابل عرضه و افزایش دهنده حریم خصوصـــی را در خطوط تولید خود برای رسیدگی به موارد اســـتفاده تجاری و شخصی معرفی می‌کنند. صرف‌نظر از کاربرد اصلی، این نوع ســـخت‌افزار برای محافظت از داده‌هایی که در دستگاه‌ها جریان می‌یابند، مستقر می‌شوند.

نمونه‌هایی از ســـخت افزارهای افزایش دهنده حریم خصوصی عبارتند از:

- صفحه‌نمایش‌های حریم خصوصی که محتوای صفحه نمایش را از همه به جز کاربر مخفی می‌کند.
- احراز هویت بیومتریک، از جمله اثر انگشـــت و/یا تشخیص چهره.
- مکانیسم‌های Anti-interdiction که دستکاری سخت‌افزار و نرم‌افزار را تشخیص می‌دهند این دستکاری ممکن است در حین چرخه انتقال دستگاه از سازنده به کاربر نهایی رخ دهد.

14- Privacy Enhanced Hardware

سیستم‌ها و معماری[15]

دسته نهایی PET ها سیستم‌ها و فرآیندهای جدید بـــرای فعالیت‌هـــای داده‌ای اســـت. سیســـتم‌ها و معماری‌ها به جای تغییر دادن داده‌ها یا محافظت از آن، راه‌های امن‌تر و حفظ حریم خصوصی‌تری را بـــرای مدیریت اطلاعات ایجاد می‌کنند. برخی از این سیستم‌ها همچنین شفافیت و نظارت بیشـــتری را بر روی فعالیت‌های داده از جمله جمع آوری، پردازش، انتقال، استفاده و ذخیره سازی امکان پذیر می‌کنند.

محاسبات چند جانبه[16]

محاســـبات چند جانبه تکنیکی است که موجودیت‌های مختلف را قادر می‌ســـازد تا بدون افشای اطلاعات کامل با داده‌ها تعامل داشته باشند. این تکنیک داده‌ها را در چندین «اشتراک» تعیین می‌کند که توسط نهادهای مختلف توزیع و تحلیل می‌شوند. تقسیم اطلاعات به این معنی است که اگر هر نهادی در معرض خطر قرار گیرد، مجموعه کامل داده‌ها در معرض خطر قرار نمی‌گیرد.

محاســـبات چند طرفه را نیـــز می‌توان بـــا تکنیک‌هایی مانند رمزگذاری هوموفیک که توضیح داده شد ترکیب کرد، بنابراین حتی "اشتراک‌ها" در طول تجزیه و تحلیل داده‌ها آشکار نمی‌شوند.

استفاده از محاسبات چند جانبه در میان داده‌های توزیع‌شـــده از قبل، این مزیت را دارد که هرگز آن‌ها را در یک مخزن مرکزی ترکیب نمی‌کند، در نتیجه ریسک را خیلی بیشتر کاهش می‌دهد.

محاســـبات چند جانبه یک تکنولوژی بالغ است و امروزه بسیاری از ســـازمان‌های تحقیقاتی از آن استفاده می‌کنند.

پراکندگی داده‌ها[17]

پراکندگی داده به فرآیندی اطلاق می‌شـــود کـــه در آن داده‌ها به قطعات کوچک‌تر تقســـیم می‌شـــوند و در یک زیرســـاخت ذخیره‌سازی توزیع‌شـــده نگهداری می‌شوند که معمولاً چندین مکان جغرافیایی را در بر می‌گیرد.

در این فرآیند، از نرم افزار برای شکستن فیلدهای داده به صورت تصادفی اســـتفاده می‌شـــود. پراکندگی داده‌ها می‌تواند امنیت داده‌ها و حفظ حریم خصوصی را افزایش دهد، زیرا اگر یک مکان ذخیره‌سازی مورد تعرض قرار گیرد یا به فایل‌های آن دسترسی پیدا شود، اطلاعات بدون قطعات باقی مانده، کامل یا قابل درک نخواهد بود.

15- systems and architectures
16- Multi-Party Computation
17- Data dispersion

رابط‌های مدیریتی[18]

از آنجایی که شرکت‌ها داده‌ها را جمع آوری می‌کنند، برای قابل دسترس کردن و عملیاتی کردن اطلاعات به سیستم‌های تجاری نیاز است. نهادها ممکن است بخواهند داده‌ها را متمرکز کنند یا سیستم‌ها را پیوند دهند تا داده‌ها را در واحدهای تجاری قابل استفاده کنند و در عین حال محرمانه بودن اطلاعات را نیز حفظ کنند. رابط‌های مدیریتی، سیستم‌های نرم‌افزاری هستند که بین مجموعه داده‌ها یا پایگاه‌های داده و کارمندان یا نهادهایی که به آن مجموعه داده‌ها یا پایگاه‌های داده دسترسی دارند قرار می‌گیرند.

یکی از عناصر مهم این نوع سیستم‌ها، توانایی آن‌ها در شناسایی انواع داده، برچسب‌گذاری اطلاعات یا افزودن ابرداده است که ویژگی‌های خاصی از داده‌ها را توصیف می‌کند، مانند حساسیت. برای مثال، اگر اطلاعات به عنوان حساس شناسایی شود، سیستم‌ها می‌توانند سایر تکنیک‌های افزایش حریم خصوصی را به‌طور خودکار و بدون دخالت انسان انجام دهند، مانند تغییر داده‌ها.

نتیجه‌گیری

فناوری‌های تقویت‌کننده حریم خصوصی مجموعه‌ای از ابزارهای جذاب و هیجان‌انگیز هستند که می‌توانند به جذب ارزش داده‌ها و حفظ امنیت، محرمانگی و خصوصی بودن آن‌ها کمک کنند. علیرغم این پتانسیل، PETها راه‌حل‌های مستقلی برای نگرانی‌های حفظ حریم خصوصی و امنیتی نیستند و باید همراه با سیاست‌های قوی و سیستم‌های حاکمیتی مورد استفاده قرار گیرند. از آنجایی که رگولاتورها، سیاست‌گذاران و کسب‌وکارها این فضا را بررسی می‌کنند، درک تنوع تکنیک‌ها و سیستم‌هایی که PETها را تشکیل می‌دهند و همچنین نقاط قوت و اهداف مختلف آن‌ها مهم است. ■

منابع:

[1] Burke, Brian, P. H. (2020). Top Strategic Technology Trends for 2021- Gartner. Gartner, 1–12. https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe%0Ahttps://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe%0Ahttps://ec.europa.eu/digital-single-market/en/news/communicatio

[2] Kaitln Asrow, F. P. A., & Spiro Samonas, S. R. S. (n.d.). Privacy Enhancing Technologies: Categories, Use Cases, and Considerations. Federal Reserve Bank of San Francisco,. https://www.frbsf.org/banking/publications/fintech-edge/2021/june/privacy-enhancing-technologies/Privacy-Enhancing-Technologies_FINAL_V2_TOC-Update.pdf

18- Management Interfaces

دیتا فابریک

گارتنر از معماری‌های دیتا فابریک به عنوان یکی از ۱۰ روند برتر در سال ۲۰۲۲ نام برده، زیرا دسترسی یکپارچه و اشتراک‌گذاری داده‌ها را در یک محیط داده توزیع‌شده امکان‌پذیر می‌سازد. دیتا فابریک برای پیوند دادن منابع توزیع شده صرف نظر از مکانی که در آن قرار دارند (ابر یا محلی یا راه دور) یا APIهایی که برای تبادل داده در معرض نمایش هستند استفاده می‌شود. دیتا فابریک ترکیبی از چندین لایه مختلف است و برای بهره بردن از ارزشی که دیتا فابریک ایجاد می‌کند، رهبران تجزیه و تحلیل داده بایداز فناوری اطمینان حاصل کنند، قابلیت‌های اصلی مورد نیاز را شناسایی کنند و ابزارهای مدیریت داده موجود را ارزیابی کنند.

کلمات کلیدی: دیتا فابریک، فراداده، تجزیه و تحلیل، انبارداده، دریای داده

در عملیات‌های سازمانی، ده‌ها مورد استفاده بلادرنگ وجود دارد که به معماری داده‌ای در مقیاس عظیم و با سرعت فوق‌العاده نیاز دارد که بتواند هزاران یا حتی میلیون‌ها تراکنش را به طور همزمان پشتیبانی کند. مثال‌ها فراوان است:
ارائه یک نمای ۳۶۰ درجه به مشتری، تلفن گویای سلف سرویس، سامانه ارتباط با مشتری، پورتال مشتری سلف سرویس (وب یا موبایل)، سرویس چت و ربات‌ها، توکن کردن تراکنش‌های کارت اعتباری، کشف کلاهبرداری آنلاین و . . .
این موارد به یک پلتفرم کلان داده نیاز دارند که بتواند زمان پاسخ دهی در ثانیه را برای انجام پرس و جوهای پیچیده پشتیبانی کند.

چابکی مدیریت داده به یک اولویت ماموریتی حیاتی برای سازمان‌ها در محیطی متنوع، پراکنده و پیچیده تبدیل شده است. برای کاهش خطاهای انسانی و هزینه‌های کلی، رهبران داده و تجزیه و تحلیل (D&A) باید فراتر از شیوه‌های سنتی مدیریت داده نگاه کنند و به سمت راه‌حل‌های مدرن مانند یکپارچه سازی داده‌های مبتنی بر هوش مصنوعی حرکت کنند.
معماری دیتا فابریک به طور خاص برای رسیدگی به چالش‌های پیش روی چشم انداز داده‌های ترکیبی پیچیده طراحی شده است.

دیتا فابریک

برای تعریف دیتا فابریک یا الیاف داده اجازه دهید با برخی از تعاریف اولیه شروع کنیم.

طبق واژه‌نامه گارتنر، دریاچه داده[1] به مجموعه‌ای از ذخیره‌سازی داده‌های مختلف اشاره دارد. این داده‌ها در یک کپی از فرمت منبع - ساختاریافته یا بدون ساختار - ذخیره شده و علاوه بر داده اصلی نگهداری می‌شوند.
انبار داده[2]، فرآیند جمع‌آوری و مدیریت داده‌ها از منابع مختلف، برای ایجاد نوعی دیدگاه تجاری است. انبار داده‌ها برای اتصال، گزارش‌دهی، بررسی و تحلیل داده‌های تجاری از منابع مختلف مورد استفاده قرار می‌گیرد و هسته اصلی سیستم هوش تجاری به شمار می‌رود.
سیستم مدیریت پایگاه داده[3] برای ذخیره و سازمان‌دهی داده‌ها استفاده می‌شود که معمولاً دارای فرمت‌ها و ساختارهای تعریف شده است. سیستم مدیریت پایگاه داده‌ها بر اساس ساختار اصلی و استفاده یا استقرار آن‌ها طبقه‌بندی می‌شوند.
پایگاه داده رابطه‌ای معمولاً با زبان پرس و جو SQL کار می‌کند و بر اساس روابط بین موجودیت‌های داده سازمان‌دهی شده است. پایگاه داده غیر رابطه‌ای (NoSQL) اغلب در داده‌های بزرگ و برنامه‌های کاربردی وب بلادرنگ استفاده می‌شود و برای استفاده در مقیاس وسیع بهینه شده است.
دیتا فابریک یک لایه یکپارچه از داده‌های متصل از منابع داده یک شرکت بدون توجه به فناوری، فرمت، یا محل نگهداری منابع است. دیتا فابریک می‌تواند داده‌های پردازش‌شده را در ذخیره‌گاه داده‌های خود حفظ کرده و ایمن کند و آن‌ها را به برنامه‌های کاربردی، موتورهای تصمیم‌گیری بلادرنگ ML/AI و

1- Data Lake
2- Warehousing Data
3- DBMS

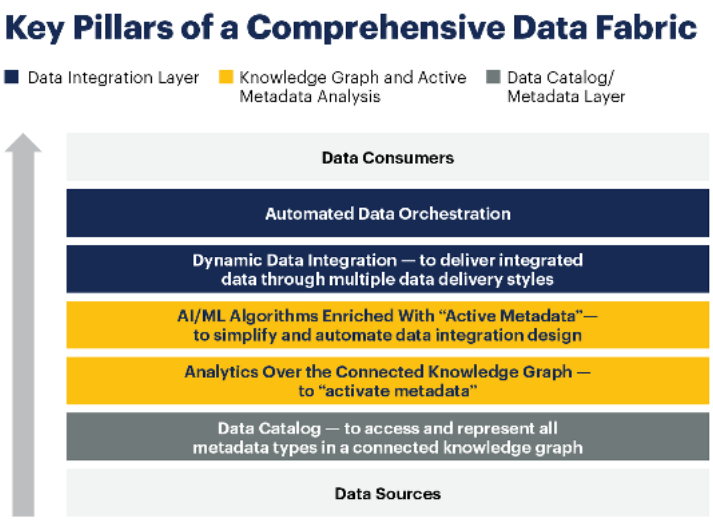
فروشگاه‌های بزرگ داده تحویل دهد. یک دیتا فابریک عملیاتی می‌تواند داده‌های سازمانی را در زمان واقعی یکپارچه، پردازش و ارائه دهد. دیتا فابریک برای پیوند دادن منابع توزیع شده صرف نظر از مکانی که در آن قـــرار دارند (ابری ، محلی یـــا راه دور) یا APIهایی که برای تبادل داده در معرض نمایش هستند استفاده می‌شود.

سازمان‌ها امروزه دارای داده‌هایی هستند که به‌صورت محلی و یا در چندین محیط ابری مستقر شده اند. انواع داده‌ها (خارج از حجم عظیم داده ها) شامل داده‌ها در پایگاه‌های داده رابطه‌ای، فایل های مسطح، دریاچه‌های داده و ... است. مدیریت داده‌ها، فناوری‌هایی چون ETL دسته‌ای تا پردازش جریانی را در بر می گیرد. تعداد زیاد برنامه‌ها، پلتفرم‌ها و انواع داده‌ها، مدیریت پردازش، دسترســـی، امنیت و ادغام در چندین پلتفرم را دشـــوار (و گاهی غیرممکن) می کند. دیتا فابریک مدیریت داده را در یک محیط ادغام می کند و به طور خودکار منابـــع داده و فناوری‌های متفاوت را در محیط داخلی و ابری مدیریت می کند.

اجزای کلیدی Data Fabric

دیتا فابریک ترکیبی از چندین لایه مختلف است. در اینجا برخی از اجزای کلیدی لازم برای اجرای صحیح دیتا فابریک بیان می‌شود: مجموعه ای از فراداده[4]ها که به خوبی به هم متصل شده اند، اساس طراحی دیتافابریک است. این شـــامل خدماتی است که به دیتا فابریک اجازه می‌دهد تا هر نوع فراداده ای را شناسایی و تجزیه و تحلیل کند.

4- Meta data



کاتالوگ داده[5]، دسترسی به همه انواع فراداده را از طریق نمودار دانش[6] فراهم می‌کند. همچنین به صورت گرافیکی فراداده حاضر را به شیوه‌ای آسان برای درک به تصویر می‌کشد و روابط منحصر به فرد بین آن‌ها ایجاد می‌کند.

تجزیه و تحلیل، زمانی که با نمودارهای دانش مرتبط می‌شود، به فعال سازی ابرداده کمک می‌کند. به‌این ترتیب نمودارها قادر می‌شوند تا داده‌های خود را با معانی غنی کنند و این باعث می‌شود تا کار برای تحلیلگران داده و دانشمندان آسان تر شود.

مجموعه‌ای از ابزارهای استاندارد یکپارچه‌سازی داده‌ها، تحویل داده‌های یکپارچه را از طریق چندین روش تحویل داده تضمین کرده و کمک می‌کند تا نمودارهای دانشی که تجزیه‌وتحلیل‌شده‌اند تنظیم گردند.

دیتا فابریک ایجاد شده باید دارای بک بون تطبیق داده[7] قوی باشد. دیتا فابریک باید با سبک‌های مختلف تحویل داده سازگار باشد و محدود به هیچ کدام نباشد. پشتیبانی از انواع داده‌های مختلف، در دسترس بودن آن را برای همه نوع کاربر را تضمین می‌کند.

سه حالت معماری دیتا فابریک

به طور کلی، به نظر می‌رسد حداقل سه مفهوم غالب از معماری دیتا فابریک وجود دارد.

اولین برداشت دیتا فابریک را به عنوان یک معماری کاملاً غیرمتمرکز می‌بینند، یعنی وسیله‌ای برای دستیابی به داده‌هایی که بدون ادغام آن‌ها در یک جای متمرکز توزیع می‌شوند همانند دریای داده یا انبار داده.این مفهوم بر نقش دسترسی متمرکز در معماری داده تأکیدی ندارد و در رادیکال‌ترین حالت، نیاز به دسترسی متمرکز را کاملاً رد می‌کند.

در مقابل، برداشت دوم و فراگیرتر در مورد دیتافابریک، مخازن متمرکز را به عنوان شرکت‌کنندگان غیرمجاز در معماری داده‌های توزیع‌شده می‌بینند: داده‌های موجود در دریای داده یا انبار داده مانند سایر منابع برای دسترسی در معرض دید قرار می‌گیرند. این برداشت از معماری دیتا فابریک شامل منابع داده متمرکز است، اما با این وجود به دسترسی غیرمتمرکز امتیاز می‌دهد.

سومین برداشت از دیتا فابریک، آن را زیربنای معماری داده ترکیبی می‌داند. این طرح در واقع نقش کلیدی را برای دریای داده و یا انبار داده تعیین می‌کند. این وضعیت به نفع دسترسی متمرکز و در مقابل دسترسی غیرمتمرکز است: دیتا فابریک راهی را به معماران داده می‌دهد تا هم منابع داده‌ای پراکنده را با هم پیوند دهند و هم نیازهای دسترسی غیرقابل پیش‌بینی مصرف‌کنندگان متخصص، مانند دانشمندان داده، مهندسان ML و AI را برآورده کنند.

دیتا فابریک و امنیت

دیتا فابریک همچنین می‌تواند برنامه‌های امنیتی را با گره زدن داده‌ها و برنامه‌های کاربردی از سراسر سیستم‌های فیزیکی و

5- Data Catalouge
6- knowledge graph
7- data compatibility backbone

فناوری اطلاعات بهبود بخشد.

به عنوان مثال، یک تیم امنیت می‌تواند با پیوند دادن اطلاعات از کارتخوان‌های درب که برای باز کردن درها اســـتفاده می‌شود، با داده رویدادهای سیستم‌های رایانه‌ای که از داخل مرکز به آن‌ها دسترسی پیدا می‌کند امنیت آن‌ها را بهبود بخشد. این امکان انجام تجزیه و تحلیل پیچیده تری از رفتار معمولی و غیرعادی را برای ایجاد هشدارهای امنیتی بلادرنگ در صورت لزوم فراهم می‌کند.

چگونه رهبران تجزیه و تحلیل داده می‌توانند از معماری دیتا فابریک اطمینان حاصل کنند که ارزش تجاری ارائه می‌دهد؟

برای بهره بردن از ارزشی که دیتا فابریک ایجاد می‌کند، رهبران تجزیه و تحلیل داده بایـــد از فناوری اطمینـــان حاصل کنند، قابلیت‌های اصلی مورد نیاز را شناسایی کنند و ابزارهای مدیریت داده موجود را ارزیابی نمایند.

- دیتا فابریک باید همه اشکال فراداده را جمع آوری و تجزیه و تحلیل کند

اطلاعات مفهومی، پایه و اســـاس طراحی دیتا فابریک اســـت. اطلاعات متنی، پایه و اساس طراحی یکپارچه داده پویا است. باید مکانیزمی وجود داشته باشد (مانند مجموعه ای از فراداده‌ها که به خوبی به هم متصل شده اند) که دیتا فابریک را قادر می‌سازد تا انواع فراداده‌ها مانند فنی، تجاری، عملیاتی و اجتماعی را شناســـایی، متصل و تجزیه و تحلیل کند.

- دیتا فابریک باید فراداده‌های غیرفعال را به فراداده‌های فعال تبدیل نماید.

برای به اشتراک گذاری داده‌ها، برای شرکت‌ها مهم است که فراداده‌ها را فعال کنند. برای اینکه این اتفاق بیفتد، دیتا فابریک باید به طور مداوم فراداده‌های موجـــود را با معیارها و آمارهای کلیدی تجزیه و تحلیل کند و سپس مدل نمودار بسازد. بر اساس روابط منحصر به فرد و مرتبط با کسب و کار، فراداده‌ها را به شیوه ای آسان برای درک به تصویر بکشـــید. از معیارهای کلیدی فرا داده برای فعال کردن الگوریتم‌های AI/ML استفاده گردد که در طول زمان یاد می‌گیرند و پیش‌بینی‌های پیشرفته‌ای را در مورد مدیریت داده و یکپارچه‌سازی ارائه می‌دهند.

- دیتا فابریک باید نمودارهای دانش را ایجاد و مدیریت کند.

این جایی است که سحر و جادو اتفاق می‌افتد. نمودار دانش روابط بین موجوداتی را که در مدل‌های مختلف داده کشف می‌کند، شناسایی و برقرار می‌کند. در یک سطح رسمی، نمودار دانش تلاش می‌کند تا اکتشافات خود را در یک هستی‌شناسی در حال تکامل قرار دهد. به این ترتیب، طرحواره‌ای از موجودیت‌های مرتبط، انتزاعی ("مشتری") و عینی ("جین") ایجاد می‌کند، آن‌ها را در دامنه‌ها گروه‌بندی می‌کند و در صورت امکان، روابط بین دامنه‌ها برقرار می‌کند.

- دیتافابریک باید دارای ســـتون فقرات یکپارچه سازی داده قوی باشد.

دیتا فابریک باید با ســـبک‌های مختلف تحویل داده (شامل، اما نه محدود به ETL، استریم، پیام رسانی، و مجازی سازی داده یا ریزسرویس‌های داده) سازگار باشد. باید از همه انواع کاربران داده پشتیبانی کند - از جمله کاربران فناوری اطلاعات (برای الزامات یکپارچه ســـازی پیچیده) و کاربران تجاری (برای آماده سازی داده‌های سلف سرویس).

نتیجه‌گیری

مقایسه دیتا فابریک در مقابل دریاچه داده و پایگاه داده، دیتا فابریک معماری انتخابی برای موارد استفاده عملیاتی در مقیاس عظیم، حجم بالا و زمان واقعی است. اما آن‌ها با هم بهتر عمل می‌کنند. از یک طرف، دیتا فابریک می‌تواند داده‌های قابل اعتماد را برای دریا و انبار داده‌ها آماده کند و از سوی دیگر، دریاچه‌ها و انبارها می‌توانند بینش‌هایی را به دیتا فابریک برای استفاده در زمان واقعی ارائه دهند.

منابع:

[1] Gupta, A. (2021). Data Fabric Architecture is Key to Modernizing Data Management and Integration. https://www.gartner.com/smarterwithgartner/data-fabric-architecture-is-key-to-modernizing-data-management-and-integration

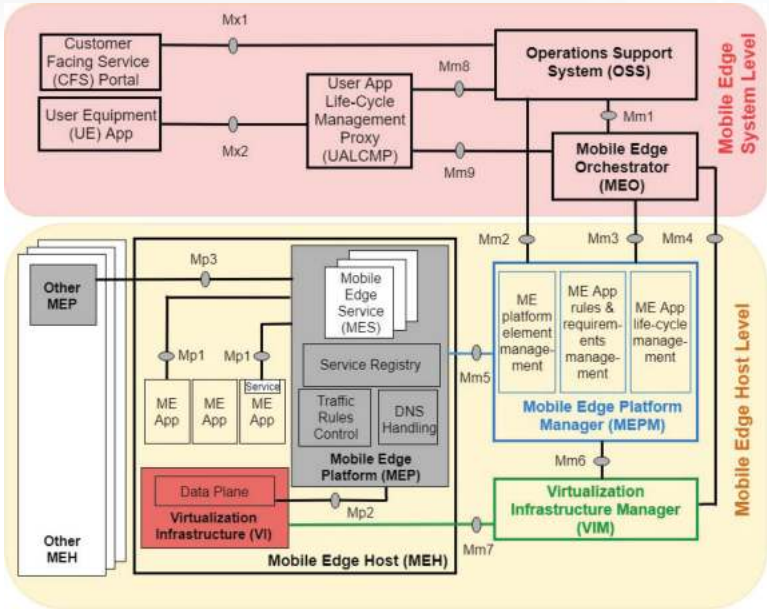
[2] Stephen Swoyer. (2021). Data Fabric Architecture: Advantages and Disadvantages. https://www.itprotoday.com/analytics-and-reporting/data-fabric-architecture-advantages-and-disadvantages

امنیت محاسبات لبه موبایل

محاسبات لبه شبکه دسترسی (Multi-Access Edge Computing-MEC) در واقع توسعه‌ای بر محاسبات ابری است که می‌کوشد توان محاسباتی، حافظه‌ذخیره‌سازی و شبکه ارتباطی را در لبه شبکه و نزدیک‌ترین نقطه به کاربر نهایی مستقر سازد. توسعه MEC در پاســـخ به نیاز به مخابرات با تاخیر بسیار کم در شـــبکه‌های 5G صورت گرفته است. معماری MEC با پشتیبانی از کاربردها و خدمات، پلی بین محاسبات ابری و کاربر نهایی برقرار می‌کند و شامل تجهیزات و سیستم‌های متصل به‌هم و لایه‌ای است. با پیشرفت تکنولوژی، MEC نیز با تهدیدات بسیاری روبرو می‌باشد. MEC درواقع توسعه‌ای بر نسل جدید محاسبات ابری موبایل است که با یک ساختار توزیع شده می‌کوشد ساختار ابری را درنزدیک‌ترین نقطه به کاربر نهایی مستقر سازد. با اینکه استقرار معماری محاسبات لبه‌شبکه نرم‌افزاری، مشکلاتی مانند Jitter و تاخیر را حل می‌کند، نقاط ضعف بیشتری ایجاد کرده و سطح حمله گسترده‌تری به وجود می‌آورند. در این مقاله پس از بررسی کاربردها، مفاهیم پایه‌ای و معماری MEC ابتدا چالش‌های امنیتی و در ادامه راهکارهایی برای مقابله با آن‌ها ارائه خواهدشد. بردارهای تهدید و حمله به MEC مورد ارزیابی قرار گرفته و پیشنهاد می‌شود که جهت تحقق امنیت در MEC چندین لایه امنیتی مستقر گردد.

کلمات کلیدی: محاسبات لبه شبکه دسترسی (Multi-Access Edge Computing-MEC)، امنیت، حریم خصوصی، 5G.

توســـعه موازی 5G و IOT سبب شـــده که در پاسخ به نیازهای سیستم‌های IOT مانند تاخیر و Jitter کم، پهنای باند بیشتر و فضای ذخیره‌سازی حافظه بسیار زیاد، تغییراتی نیز در معماری 5G ایجاد شده و محاســـبات ابری به لبه‌شبکه دسترسی منتقل گردد. با وجـــود ارتقـــای حاصل از به‌کارگیـــری MEC، چالش‌های امنیتـــی نیز ایجاد شـــده که ناشـــی از ناهمگونی در سرویس‌های IOT است که یکپارچه‌سازی تکنولوژی‌های مختلف در محاسبات ابری را پیچیده می‌کند و نگهداری سطح عملکرد مورد انتظار خدمت در شـــبکه‌های 5G را دشوار می‌ســـازد. در ادامه به بررســـی تهدیدات احتمالی در پیاده‌ســـازی MEC در انطباق با استانداردهای ETSI پرداخته و راه‌حل‌های احتمالی برای مقابله با آن‌ها ارائه خواهیم کرد [۲].



شکل ۱- معماری مرجع MEC

افزایش تعداد تجهیزات هوشمند متصل به شبکه تا صدها میلیارد، نیازمند ظرفیت اضافی و پهنای باند بیشتر در ایستگاه‌های پایه موبایل خواهد بود. عملکرد تضمین شده شبکه 5G به منظور تضمین تاخیر کمتر از ۱میلی‌ثانیه، قابلیت دسترسی ۹۹,۹۹۹۹۹% و نرخ داده 10Gbps، از چالش‌های پیش‌روی 5G خواهندبود. معماری کنونی پردازش ابری به جهت فاصله جغرافیایی گسترده آن قادر به تضمین این سطح عملکرد نخواهد بود. به‌همین جهت به‌منظور پاسخ به این نیازمندی‌ها انستیتو استاندارد مخابراتی اروپا (ETSI۱) مفهوم پردازش لبه‌ای با دسترسی چندگانه را معرفی نمود.

شبکه‌های MEC می‌توانند به صورت زیرساخت‌های ابری کوچک‌شخصی پیاده شوند که ریسک نشت اطلاعات را افزایش داده. استفاده از رویکرد طراحی مبتنی‌برامنیت می‌تواند در افزایش امنیت موثر باشد، خصوصا که معماری توزیع‌شده این سیستم منجر به توزیع داده‌های کاربران خواهد شد [۱].

1- European Telecommunications Standards Institute

معماری MEC

معماری مرجعی ارائه شده در [۳] که در شکل ۱ نشان داده شده، MEC را به دو سطح سیستمی و میزبان تقسیم کرده است.

هماهنگ‌ساز لبه موبایل hypervisor (MEO[۲]) اصلی در پیاده‌سازی MEC است. سیستم پشتیبانی عملیات (OSS[۳]) مسئول ارائه دسترسی به درخواست‌های ثبت‌نام کاربران، که از تجهیزات کاربران و از طریق پروکسی مدیریت چرخه حیات کاربردی کاربر (UALCMP[۴]) ارسال شده، می‌باشد. پرتال سرویس روبروی مشتری (CFSP[۵]) وظیفه مدیریت دسترسی به سرویس‌های شخص ثالث را برعهده دارد. MEO، OSS، UALCMP و CFSP المان‌هایی هستند که در سطح سیستمی MEC قرار داده شده‌اند. یک درخواست سرویس تایید شده MEC وارده از یک نرم‌افزار کاربردی بر روی تجهیزات کاربران (UE App) یک سرویس لبه‌ای موبایل (MES[۶]) را ذیل یک کاربرد لبه‌ای موبایل (ME App) صدا می‌زند که در یک زیرساخت مجازی (VI[۷]) بر روی یک میزبان لبه موبایل (MEH[۸]) اجرا می‌شود. کلیه کاربردهای واقع بر روی میزبان لبه شبکه موبایل بر روی ماشین‌های مجازی نصب می‌شوند. هر دوی MEPM[۹] و VIM[۱۰] به صورت پیوسته MEO را از میزان استفاده خود از منابع مجازی موجود آگاه می‌کنند.

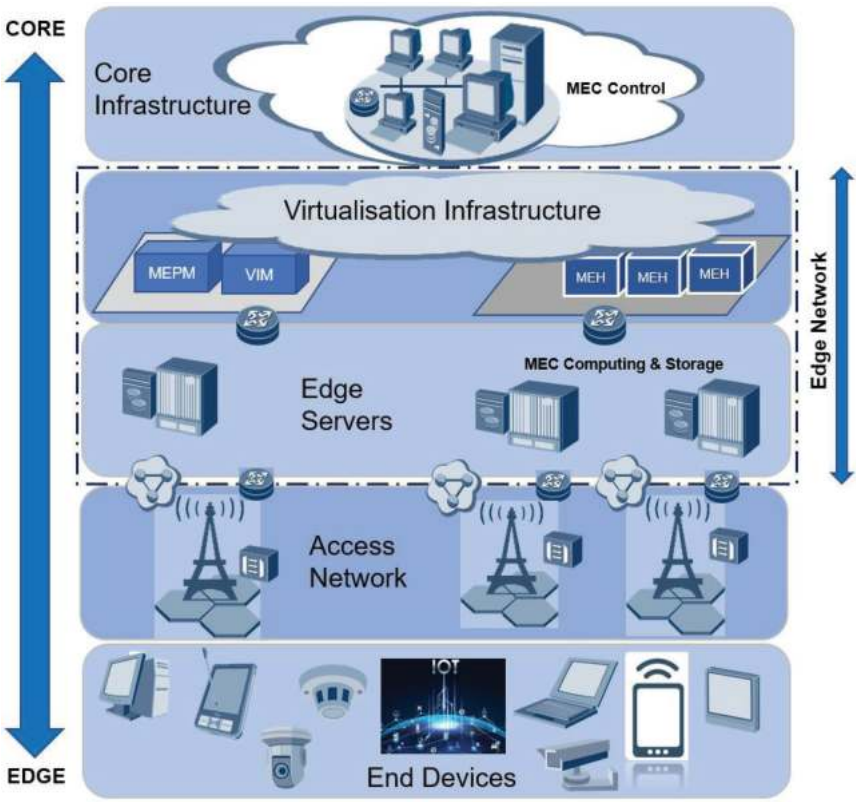
ساختار عملکردی MEC شامل ۴ لایه است، تجهیزات انتهایی، شبکه دسترسی، زیرساخت هسته و شبکه‌لبه که در شکل ۲ نشان داده شده است. تجهیزات انتهایی IIOT از طریق شبکه دسترسی به لایه‌های عملکری و اینترنت متصل می‌شوند. شبکه‌لبه مفاهیم MEC و NFV را ترکیب می‌کند. زیرساخت هسته نیز توابع کنترل و مدیریت مرکزی MEC برای تجهیزات انتهایی موبایل را برعهده دارد [۱].

MEC می‌تواند در پیاده‌سازی کاربردهایی مانند واقعیت افزوده، خدمات مکان‌محور، ذخیره‌سازی توزیع‌شده محتوا، تحلیل‌های ویدئویی، خودروهای بدون‌راننده خودکار و ... به‌کار گرفته شود.

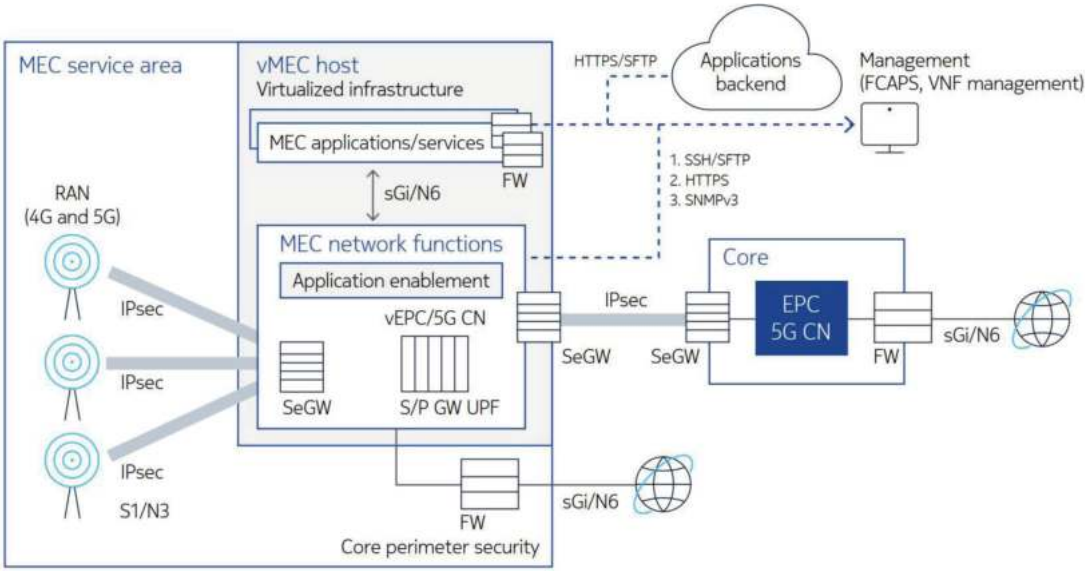
معماری شبکه امنیت MEC

نیازمندی‌های امنیتی MEC به‌شکلی خلاصه عبارتند از: احراز هویت المان‌ها، تایید هویت، امنیت شبکه باتفکیک ترافیک، تضمین یکپارچگی نرم‌افزارها، شناسایی بدافزارها در لایه MEC، رمزنگاری داده‌ها، استفاده از تجهیزات MEC مقاوم در برابر دستکاری. برخی از این ویژگی‌ها ذاتا در معماری MEC وجود دارند. لیکن با توسعه و استقرار 5G و MEC مهاجمان به

2- Mobile Edge Orchestrator
3- Operation Support System
4- User Application Life-Cycle Management Proxy
5- Customer Facing Service Portal
6- Mobile Edge Service
7- Virtualization Infrastructure
8- Mobile Edge Host
9- Mobile Edge Platform Manager
10- Virtual Infrastructure Manager



شکل ۲- ساختار عملکردی MEC



شکل ۳-معماری شبکه امنیت MEC

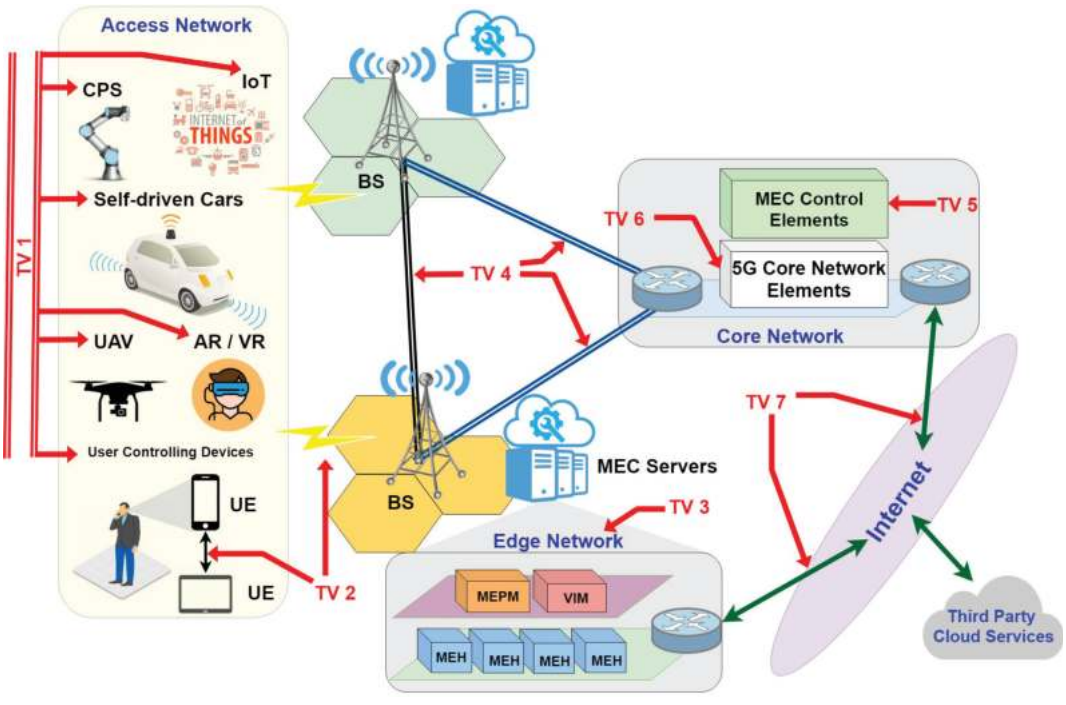
صورت گسترده آن‌ها را مورد حمله قرار خواهند داد. فضای MEC ریسک‌های امنیتی پردازش ابری و شبکه‌هاو ماشین‌های مجازی را به ارث خواهد برد. MEC ریسک‌های امنیتی در پیاده‌سازی به همراه خواهد داشت و می‌تواند در سطح شبکه با اصولی مشابه هسته شبکه موبایل پیاده شود. دروازه امنیتی (SeGW) می‌تواند برای خاتمه تونل‌های IPSec ورودی از المان‌های شبکه‌رادیویی چنانکه در شکل ۳ نشان داده شده، به کار رود.

برای کاهش ریسک‌های امنیتی MEC یک معماری متمرکز امنیتی موردنیاز است که بتواند چهارچوب امنیتی MEC سلسله‌مراتبی که قادر به پوشش لایه تجهیزات فیزیکی، لایه اجزای مجازی، زنجیره حیات نرم‌افزارهای کاربردی، پلتفرم MEC، تابع صفحه کاربر و امنیت سیستم مدیریت را پشتیبانی نماید.

بردارهای تهدید MEC

هفت بردار تهدید احتمالی MEC در تصویر ۴ نشان داده شده‌اند.

بردار تهدید یک: آسیب‌پذیری‌های تجهیزات کاربران (UE) اولین محل تهدید MEC است. هر تجهیز متصل به یک BTS حتی سنسوری کوچک یک UE است. داده‌های ذخیره‌شده در



شکل ۴- بردارهای تهدید MEC

تجهیزات کاربران حریم خصوصی آن‌ها بوده و حفظ آن مهم است. رایج‌ترین نوع حملات به تجهیزات کاربران دستکاری فیزیکی آن است که مهاجمان را قادر می‌سازد کنترل تجهیز ومنابع آن را به‌دست بگیرند. تروجان‌های نرم‌افزاری نیز عملکرد مشابهی دارند. با بازیابی اطلاعات تجهیزات قدیمی کاربران حملات کانال جانبی[11] مختلفی ممکن است اتفاق بیفتد. با وجود محدودیت منابع تجهیزات کاربران مهاجمان از همان منابع محدود برای حمله به MES می‌توانند استفاده کنند. همین‌طور MES ممکن است بگونه‌ای هدایت شود که منابع بیشتری در MEH به تجهیزات کاربران، اختصاص دهد. چنین حملاتی می‌توانند خودروها، سیستم‌های سایبرفیزیکی صنعتی خودکار (CPS[12])، شبکه‌های هوشمند برق، خودروهای بدون سرنشین هوایی (UAVs[13]) را هدف قرار دهند. استفاده از سامانه شناسایی حملات (IDS[14]) هوشمند یکی از راهکارهای مقابله با چنین حملاتی است.

بردار تهدید دو- حملات به کانال‌های مخابراتی بین یک UE و ایستگاه پایه و یا شبکه‌های اقتضایی بین تجهیزات کاربران، دسته دوم از حملات احتمالی در MEC هستند. واسط هوایی[15] ارتباطی در یک شبکه موبایل به‌شدت در معرض آسیب است. ماهیت باز و در دسترس واسط ارتباطی هوایی امکان حملات مختلفی از جمله Man-In-The-Middle، eavesdropping, Sybil, spoofing, Smurf و Denial of Service (DoS), relay را فراهم می‌آورد.

به منظور کاهش سربار استفاده از راهکارهای تضمین امنیت در لایه‌های بالایی شبکه، روش‌های امنیت در لایه فیزیکی (PLS[16]) به صورت گسترده به منظور امن‌سازی مخابرات موبایل و کانال‌های offloading پیشنهاد می‌گردند. استراتژی‌هایی ازقبیل پروتکل‌های امنیت سبک، رمزنگاری خمیده بیضوی (ECC[17])، رمزنگاری مبتنی بر هویت (IBE[18]) و پروتکل‌های امنیتی برای مخابرات نوع ماشین مستقیم، می‌توانند برای این منظور استفاده شوند.

بردار تهدید ۳: شبکه لبه موبایل (MEN) یا لایه میزبان یک سیستم MEC یک زیرساخت عملکردی برجسته برای MES می‌باشد. این بخش شامل VIM، MEPM و MEHها است که سرویس‌های provisioning و حافظه ذخیره‌سازی را برای مشترکین MEC در اختیار می‌گذارند. MEH ها در یک فضای بسته با ارتباط محدود با سطح سیستم MEC، اینترنت و مشترکین کار می‌کنند. به همین جهت وقوع حملات Interposing در آن‌ها در مقایسه با شبکه دسترسی محدود است. لیکن حملاتی که تکنولوژی‌های مجازی‌سازی را هدف قرار می‌دهند مانند حمله‌های دستکاری در ماشین مجازی[19]، VM escape، تغییر مکان قرارگیری توابع شبکه مجازی (VNF Location Shift)، تقویت سیستم نام دامنه[20] احتمال دارد که در این زیرساخت محقق شوند. این نوع از حملات عملکرد المان‌های Orchestration در سطح میزبان را تحت تاثیر قرار می‌دهند. مهاجرت VM و Offloading شبکه موبایل مواردی هستند که در حین آن‌ها محتوای مخرب می‌تواند به MEH نفوذ کند. علاوه بر آن تمایل به پیاده‌سازی سرویس‌های MEC به صورت سرورهای MEC کوچک که قادر به پوشش یک یا چند مایکروسل هستند نیز رو به افزایش است و این امر مشکلاتی را برای اپراتورهای موبایل در زمینه تامین امنیت فیزیکی ایجاد می‌نماید.

برای مقابله با چنین حملاتی می‌توان از یک ابزار مدیریت پلتفرم قابل اعتماد (TPM) و یا VM Introspection استفاده نمود. رمزنگاری درایوهای توابع شبکه مجازی، پیوستگی آن‌ها در برابر حملات فیزیکی را تضمین خواهد کرد.

بردار تهدید ۴: حملات محدودی هم وجود دارند که ممکن است بر روی لینک ارتباطی بین هسته و لبه در سیستم MEC اتفاق بیفتند. نوعا در شبکه‌های موبایل، این ارتباطات با به کارگیری لینک‌های رادیویی، مایکروویو، فیبرنوری یا تکنولوژی ماهواره برقرار می‌شوند. بنابراین حملات Inerposing به صورت خاص برای چنین تکنولوژی‌های انتقال داده، حملات اصلی محتمل هستند. بردارهای حمله از قبیل Sybil، پالس‌های الکترومغناطیسی، DDOS، DOS، دستکاری فیبر نوری، پالس مخفی و jamming محتمل‌ترین حملات برای چنین تکنولوژی‌هایی هستند. اگر چه انتقال داده در مسیرهای طولانی با رمزنگاری یا استفاده از VPN ایمن می‌گردد، با توجه به اینکه این لینک‌ها نوعا داده‌های کنترل و اطلاعات لاگ سرویس را انتقال می‌دهند، یکپارچگی اطلاعات انتقال یافته اهمیت ویژه‌ای خواهد

11- Side Channel Attack
12- Cyber-Physical Systems
13- Unmanned Aerial Vehicles
14- Intrusion Detection System (IDS)
15- air-interface
16- Physical Layer Security
17- Elliptic Curve Cryptography
18- Identity Based Encryption

19- VM manipulation
20- Domain Name System (DNS) amplification

داشت.

بردار تهدید ۵: UALCMP، OSS، MEO و CFSP المان‌های کنترلی در MEC هستند که می‌توانند مورد حمله واقع شوند. المان‌های مدیریت درخواست اشتراک در یک MEC یعنی UALCMP و CFSP در معرض حملات DoS و DDoS هستند و حملات وارد شده را از سطح لبه به سایر سطوح بازارسال خواهند کرد.

OSS در معرض حملات masquerading و spoofing قرار دارد که در طی آن مهاجمان می‌کوشند با ابراز خود به شکل یک کاربر قانونی در سیستم نفوذ کنند. عملیات بدون وقفه در MEO وابسته به اطلاعاتی است که این المان از MEPM و VIM در مورد سرویس‌های میزبان، به لحاظ استفاده آن‌ها از منابع سیستم، دریافت می‌کند.

به منظور ایمن‌سازی ساختارهای داخلی MEO روش‌های بازبینی داخلی دقیق Hypervisor[۲۱] می‌توانند مورد استفاده قرار بگیرند. برای پیاده‌سازی زیرساخت مجازی در لینوکس، ابزار لینوکس توسعه یافته امنیت[۲۲] می‌تواند به عنوان یک ابزار مقاوم‌سازی کرنل[۲۳] عمل کند. TPMها نیز ابزارهایی اساسی برای تصدیق اعتماد به المان‌های درگیر در سطح سیستم می‌باشند.

بردار تهدید ۶: MEC یک تکنولوژی یکپارچه‌سازی در 5G می‌باشد. بنابراین عملکرد درست هسته 5G برای شبکه‌های موبایل و MEC بسیار مهم است. سیگنالینگ یک عملکرد اصلی در میان المان‌های شبکه Core می‌باشد. المان‌های Core شبکه 5G به شکل توابع شبکه مجازی (VNFs) توسعه داده خواهند شد. لذا آن‌ها نسبت به حملاتی مانند DoS و DDoS، VNF manipulation، تغییر موقعیت قرارگیری توابع مجازی شبکه[۲۴] و ... آسیب‌پذیرند. مکانیزم امنیتی پیکربندی خودکار در [۴] برای ایمن‌سازی فرآیند احراز هویت و ارتباطات بین توابع شبکه مجازی ارائه شده است.

بردار تهدید ۷: ارتباطات برقرار بین سطح سیستمی MEC و سطح لبه با اینترنت به منظور دست‌یابی به سرویس‌های ابری سایر سرویس‌دهندگان، در این دسته از بردارهای تهدید هستند. در یک سناریوی حمله می‌توان یک کاربر ثالث را در نظر گرفت که از طریق سطح لبه MEC می‌کوشد تا داده‌های آن‌ها را قبل از انتقال به سرویس ابری متناظر آن، شنود کند. این ارتباطات نسبت به حملات MITM، رله، packet sniffing و spoofing آسیب‌پذیرند.

21- hypervisor introspection methods
22- Security Enhanced Linux (SELinux)
23- kernel hardening tool
24- VNF location shift

نتیجه‌گیری

در این مقاله دیدیم که پردازش لبه‌ای با دسترسی چندگانه از ابزارهای اصلی در تحقق اهداف ترسیم شده برای 5G است. دیدیم که توسعه چشم‌گیر تعداد کاربران در لبه شبکه و نیاز به تاخیر کم و توان پردازشی و ذخیره‌سازی بالا در نزدیکی کاربر نهایی ایده اصلی توسعه MEC بوده است. با این وجود این تکنولوژی نوین چالش‌های امنیتی زیادی نیز با خود دارد. دیدیم که احراز و تایید هویت انبوه کاربران، یکپارچگی داده‌ها، جلوگیری از نصب و مقابله با بدافزارها در لایه MEC و حفظ محرمانگی همگی از چالش‌های این تکنولوژی هستند و بردارهای هفت‌گانه تهدید این تکنولوژی به صورت مجزا تحلیل و راهکارهایی برای مقابله با آن‌ها ارائه گردید. برای مقابله با تهدیدات مختلف احتمالی روش‌های مختلفی از جمله استفاده از ابزارهای کنترل هویت و دسترسی، ابزارهای شناسایی حملات، تونل‌های VPN و رمزنگاری داده‌ها و نیز استفاده از تجهیزات MEC مقاوم در برابر دستکاری می‌توانند استفاده شوند. ■

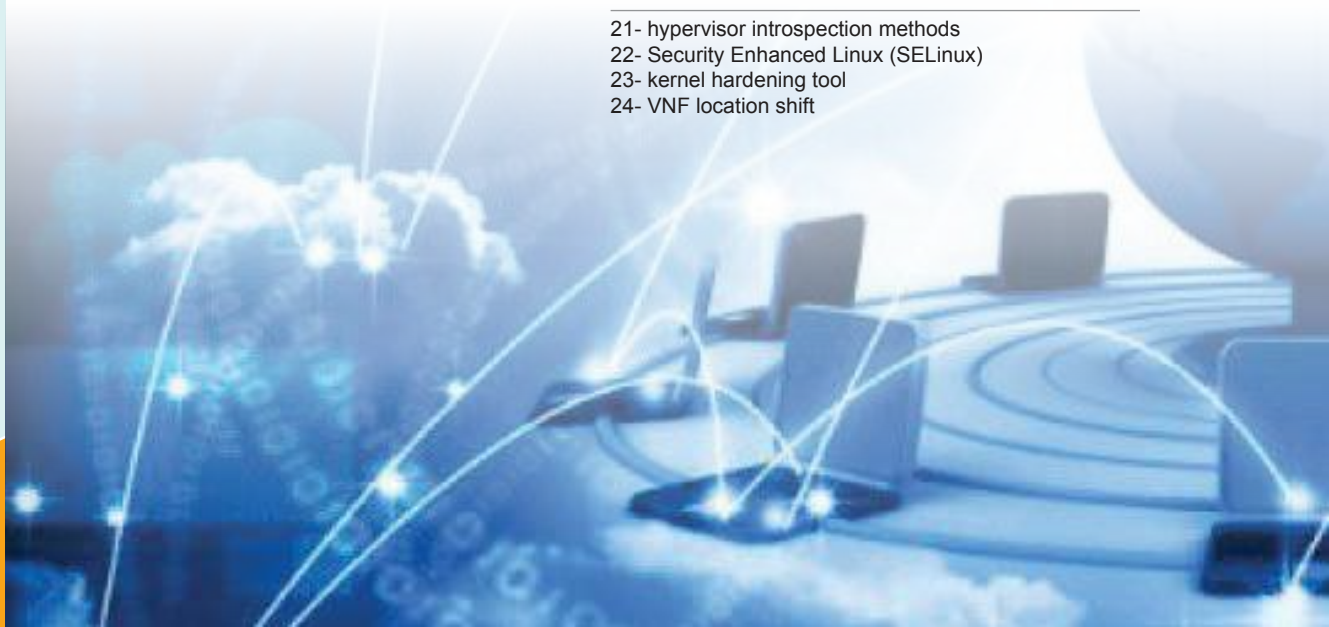
منابع:

[1] M. A. G. A. S. L. BELAL ALI, "Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review," IEEE Access Journal , دلج 9, pp. 18706-18721, 2021.

[2] A. D. J. M. L. Pasika S Ranaweera, "Realizing Multi-Access Edge Computing Feasibility: Security Perspective," رد IEEE Conference on Standards for Communications and Networking (CSCN 2019), Granada, Spain, 2019.

[3] "ETSI, "Mobile Edge Computing (MEC) Framework and Reference Architecture," ETSI White Paper #3,," European Telecommunications Standards Institute, 2016.

[4] P. P. a. J. R. H. Kim, "Auto-configurable Security Mechanism for NFV," KSII Transactions on Internet & Information Systems, مرامش 12, دلج 2, 2018.



ابزار فناوری
Technology tools

بلک هت

ck hat®

بلک‌هت (Black Hat) یک سری از رخدادهای بین‌المللی در حوزه امنیت سایبری است که فنی‌ترین و مرتبط‌ترین اطلاعات در مورد تحقیقات انجام شده در حوزه امنیت سایبری را ارائه می‌کند. این کنفرانس از یک کنفرانس سالانه ساده در گذر زمان به ارزشمندترین سری رخدادهای امنیت اطلاعات تبدیل شده است. این رخداد چند روزه جامعه امنیت سایبری را با آخرین تحقیقات لبه تکنولوژی، ترندها و توسعه‌های انجام شده در این حوزه آشنا می‌کند.
این کنفرانس در سال ۲۰۲۲ از ۶ تا ۱۱ آگوست در شـــهر لاس‌وگاس آمریکا برگزار خواهد شد و به دو شکل حضوری و مجازی قابل دسترس خواهد بود.

در جلسات توجیهی و دوره‌های آموزشی بلک‌هت که در نتیجه بازخوردها و طبق نیازمندی‌های مطرح شده در جامعه امنیت جهانی طراحی و ارائه شده، تلاش می‌شود تا مغزهای متفکر فعال در این صنعت را کنار هم آورده و موضوعاتی ارزشمند را در اختیار آن‌ها قرار دهد. بلک‌هت می‌کوشد تا با انگیزش متخصصان در تمامی سطوح شغلی، زمینه رشد و همکاری بین افراد حاضر در آکادمی و محققان کلاس جهانی این حوزه، با رهبران امنیت سایبری در بخش‌های دولتی و خصوصی را فراهم آورد. جلسات توجیهی و آموزشی بلک‌هت که همه ساله در آمریکا، اروپا و آسیا برگزار می‌شود، مکانی را برای محققان برگزیده امنیت اطلاعات و اساتید این حوزه فراهم می‌کند تا بتوانند مخاطبین مطالب خود را یافته و موضوعات مد نظر را به آن‌ها ارائه دهند.

بلک‌هت چه می‌کند؟

کنفرانس بلک‌هت شامل سه بخش اصلی می‌باشد که عبارتند از:
جلسات توجیهی بلک‌هت (Briefings)
آموزش بلک‌هت
ابزارهای بلک‌هت (Arsenal)

جلسات توجیهی

از زمان ایجاد این مجموعه از ۲۴ سال قبل، طی این جلسات تلاش شده متخصصان حوزه امنیت سایبری در مکانی برای یادگیری و آگاهی از آخرین ریسک‌ها، تحقیقات و ترندهای حوزه امنیت اطلاعات گرد هم آورده شوند. محققان پیشرو در امنیت اطلاعات از اقصی نقاط جهان با حضور در این گردهمایی کارهای تحقیقاتی و دستاوردهای علمی خود را با سایرین به اشتراک می‌گذارند. حاضرین در این کنفرانس قادر خواهند بود که از آخرین و نفس‌گیرترین تحقیقات انجام شده در موضوعات مختلف امنیت اطلاعات از شناسایی آسیب‌پذیری‌ها در تجهیزات مصرف‌کنندگان عادی، تا تهدیدات زیرساخت‌های بین‌المللی حیاتی و سایر موضوعات مرتبط آگاه شوند.
بخش جلسات توجیهی خود شامل بخش‌های مختلفی است که عناوین متفاوت مهندسی معکوس، حریم خصوصی و هویت کاربران و هک کردن را در بر می‌گیرد. این قسمت همچنین شامل سخنرانی‌هایی از سخنرانان کلیدی و رهبران عرصه امنیت اطلاعات است. برخی از این سخنرانان کلیدی این دوره عبارتند از:

متخصصان فناوری اطلاعات، تحلیل گیران امنیت اطلاعات، مدیران ریسک، مهندسان و معماران امنیتی، متخصصان تست نفوذ، توسعه‌دهندگان نرم‌افزارهای امنیتی، رمزنگاری، برنامه‌نویسان و نیروها و متخصصان فناوری اطلاعات دولتی از جمله گروه‌های مخاطب این نمایشگاه هستند.

- رابرت لنتز، افسر ارشد امنیتی، دپارتمان دفاع ایالات متحده آمریکا.
- مایکل لین
- آمیت یوران مدیر اسبق بخش امنیت سایبری ملی دپارتمان امنیت میهن[1] ایالات متحده آمریکا.
- ژنرال کیت بی آلکساندر، مدیر اسبق آژانس امنیت ملی ایالات متحده آمریکا.

آموزش

دوره‌های آموزشی بلک‌هت شامل دروس فنی انحصاری است که عناوین مختلفی را از تست نفوذ، سوءاستفاده از اپلیکیشن‌های مبتنی بر وب، تا ساخت و حفاظت از سیستم‌های صنعتی سوپروایزری اسکادا شامل می‌شود. این دوره‌ها اغلب به صورت اختصاصی برای بلک‌هت طراحی شده و ارائه می‌شود. این درس‌های عملی حمله و دفاع متقابل توسط متخصصان فعال صنعت امنیت اطلاعات از سرتاسر دنیا آموزش داده خواهند شد. هدف از برگزاری این دوره‌ها آمادگی برای شناسایی و حفاظت از چشم‌انداز امنیت اطلاعات در آینده است.

ابزارهای بلک‌هت

ابزارها بخشی از کنفرانس است که به صورت اختصاصی به محققان و گروه‌های منبع باز مکانی برای نمایش آخرین ابزارهای امنیت اطلاعات منبع باز ارائه می‌کند.

این بخش با هدف ارائه زنده ابزارها در یک ساختار تعاملی به شکلی است که حاضران بتوانند سوالات خود در مورد هر ابزار پرسیده و حتی از آن به صورت زنده استفاده کنند. بخش ابزار از سال ۲۰۱۰ به بخش‌های این کنفرانس افزوده شد. ToolsWatch شامل آرشیوی از تمامی بخش‌های ابزار گذشته می‌باشد.

بورد بازبینی و انتخاب محتوا برای کنفرانس

بورد بازبینی شامل بیش از ۱۰۰ متخصص امنیت شناخته شده و معتبر از دانشگاه و صنعت در سرتاسر جهان است که هر کدام در یکی از زمینه‌های امنیت اطلاعات دارای تخصص هستند. بورد بازبینی، بلک‌هت را در زمینه جهت‌گیری‌های استراتژیک آن هدایت کرده و محتوای پیشنهادی جهت ارائه در کنفرانس را بازبینی و برنامه‌ریزی می‌کند. این بخش همچنین بینشی کم‌نظیر برای جامعه تحقیقاتی فراهم می‌کند.

تمامی مقالات ارسال شده توسط تیم بازبینی ارزیابی می‌شوند. هر مقاله ارسالی به صورت مجزا به منظور اثبات یکتایی و عدم تکرار محتوای ارائه شده در آن و میزان تخصصی و دقیق بودن محتوا، مورد ارزیابی قرار می‌گیرد. در طول فرآیند ارزیابی دینامیک، بورد ارزیابی کنفرانس بلک‌هت با پرسش سوالاتی به صورت پیوسته به ارزیابی، دقت، صحت و یکتایی مطالب ارائه شده در هر مقاله می‌پردازند. بهترین مقالات ارائه شده، مقالات آکادمیک سطح بالا، کدهای اثبات مفهومی (POC Codes) و یا نمایش‌های ویدئویی هستند. بلک‌هت از رویکرد پرداخت به منظور پذیرش ارائه محتوا پیروی نمی‌کند. جلسات ارائه محتوای بلک‌هت همگی به صورت مستقل و بر مبنای محتوای مطالب تخصصی انتخاب می‌شوند و صرفا به جهت حمایت مالی کسی نمی‌تواند بخشی به خود اختصاص دهد.

جذب نخبه‌ها و تحقیقات ارزشمند حوزه امنیت اطلاعات

بلک‌هت در هر یک از بخش‌های خود تحقیقات و آسیب‌پذیری‌های جدید و عمیقی را ارائه کرده است. این مجموعه قویا از ارائه‌های جدید و دقیق که توسط

1- Homeland

متخصصان داده می‌شود پشتیبانی و آن را تشویق می‌کند. بلک‌هت یک همکاری مشترک و قوی با بنیاد مرزی الکترونیک (EFF[2]) دارد که مشاوره‌های حقوقی و ارزشمندی را برای ارزیابی، حفاظت و کنترل ابعاد حقوقی کلیه مقالاتی که در هر بخش از این کنفرانس ارائه می‌شود، فراهم می‌کند.

چه کسانی باید در این کنفرانس شرکت کنند؟

متخصصان امنیت

متخصصان فناوری اطلاعات، تحلیل‌گران امنیت اطلاعات، مدیران ریسک، مهندسان و معماران امنیتی، متخصصان تست نفوذ، توسعه‌دهندگان نرم‌افزارهای امنیتی، رمزنگاری، برنامه‌نویسان و نیروها و متخصصان فناوری اطلاعات دولتی از جمله گروه‌های مخاطب این نمایشگاه هستند.

کلیه حاضران در نمایشگاه قادرند مهارت‌های خود را با آخرین ابزارها و تکنیک‌های موجود و نوین در صنایع مختلف از طریق شرکت در جلسات ارائه مقالات و آموزش‌های اختصاصی کنفرانس به روز کنند. حاضران در نمایشگاه قادر خواهند بود با چالش‌ها و موفقیت‌هایی که دیگران در زمینه‌های مرتبط با امنیت اطلاعات و ارتباطات تجربه می‌کنند، آشنا شوند. به‌علاوه، در مورد کاربردها، مدل‌های توسعه و بهترین تجربه‌های مرتبط با پلتفرم‌های نوظهور، می‌توانند مشارکت داشته باشند.

دسته دیگر از مخاطبان این کنفرانس شامل مدیران امنیتی، توسعه دهندگان کسب‌وکار و سرمایه‌گذاران حوزه امنیت اطلاعات، CISOها[3]، مدیران ارشد اجرایی، مدیران عامل سازمان‌ها، معاونین فناوری اطلاعات و مشاوران سازمان‌ها هستند.

این گروه از مخاطبان با حضور در این نمایشگاه قادر به هم‌فکری و شبکه‌سازی با دیگر مدیران امنیت اطلاعات، متخصصان و سرمایه‌گذاران احتمالی در حوزه امنیت اطلاعات و ارتباطات خواهند بود. صحبت رو در رو و نزدیک با سایرین فرصت آگاهی از فرصت‌های پیش‌رو در صنایع امنیت اطلاعات را به افراد خواهد داد.

دسته دیگر از مخاطبان و حاضران در این نمایشگاه کمپانی‌های وندور و حامیان مالی این نمایشگاه هستند. کلیه وندورها و اشخاص فعال در توسعه خدمات،

2- Electronic Frontier Foundation

3- Chief Information Security Officer

میان‌افزارها، سخت‌افزارها و نرم‌افزارهای حوزه امنیت اطلاعات می‌توانند از مخاطبان و حاضران در این نمایشگاه باشند.

بلک‌هت همه ساله بیش از ۲۰،۰۰۰ متخصص امنیت و مدیران اجرایی را از سرتاسر جهان گرد هم می‌آورد که پویاترین و متمرکزترین گردهمایی جامعه امنیت اطلاعات در دنیا به حساب می‌آید. بدین ترتیب افراد قادر خواهند بود که نوآوری‌ها، خدمات و محصولات و تخصص‌های پیشرفته خود را در یک بازه دو روزه به سایر مخاطبان ارائه کنند.

تالار کسب و کار

تالار کسب و کار مکانی است که همه ساله بیش از ۳۵۰ شرکت‌کننده، راهکارهای امنیت اطلاعات و استارت آپ، آخرین ابزارها، تکنولوژی‌ها و خدمات خود در پشتبانی از جامعه امنیت را ارائه می‌کنند.

افراد جویای کار و سازمان‌ها و شرکت‌ها نیازمند نیروی کار افراد جویای کار فصلی، دانشجویان، دانشکده‌ها و کمپانی‌ها به دنبال استخدام نیروی کار همگی از مخاطبان دیگر این گردهمایی بزرگ هستند. بلک‌هت فرصتی برای شبکه‌سازی با بهترین متخصصان فصلی در صنعت امنیت اطلاعات است. ملاقات رو در رو با زبده‌ترین متخصصان حوزه امنیت اطلاعات از مزایای اصلی حضور در این کنفرانس می‌باشد. به شکلی متقابل افراد جویای کار نیز در این گردهمایی قادر به مذاکره با موثرترین و قوی‌ترن کمپانی‌های حاضر در حوزه امنیت فناوری اطلاعات از اقصی نقاط دنیا خواهند بود.

متخصصان آکادمیک

بلک‌هت فرصتی برای دانشجویان فراهم می‌کند تا بتوانند با متخصصان برتر صنعت امنیت فناوری اطلاعات تعامل داشته و در بخش‌های کنفرانس و فعالیت‌های تعاملی اختصاصی تعریف شده ارتباط برقرار کرده و توانمندی‌های خود را عرضه کنند. اساتید و دانشجویان فعال در حوزه آکادمیک می‌توانند از تخفیف ویژه در نظر گرفته شده برای متخصصان آکادمیک برای شرکت در این کنفرانس بهره‌مند شوند. ■

منابع

https://www.blackhat.com/
https://en.wikipedia.org/wiki/Black_Hat_Briefings

کنفرانس RSA

کنفرانس RSA به صورت عمومی به عنوان بزرگترین رخداد امنیتی در جهان شناخته می‌شود. کنفرانس امنیت RSA رخدادی است که فعالان حوزه امنیت سایبری از آن غافل نمی‌شوند. ده‌ها هزار نفر از اقصی نقاط زمین برای حضور در این کنفرانس به آنجا پرواز می‌کنند و در ایام پیش از کرونا بالغ بر ۴۲،۰۰۰ نفر در سانفرانسیسکو از آن بازدید کرده بودند. RSA یک رخداد کامل و ارزشمند برای تمامی متخصصان حوزه امنیت در سطح جهان است که می‌تواند به توسعه و گسترش شبکه‌های امنیت اطلاعات ایشان کمک کند.

دنیای فناوری اطلاعات و ارتباطات به سرعت در حال تغییر بوده و امنیت سایبری یکی از مهم‌ترین اولویت‌ها در آن است. آگاهی از آخرین رویکردها و ترندهای تکنولوژی امنیت سایبری یکی از موضوعاتی است که می‌بایست مورد توجه مدیران امنیت و فناوری اطلاعات سازمان‌های مختلف قرار بگیرد. در این کنفرانس این امکان برای متخصصان و تصمیم‌گیران این حوزه فراهم خواهد شد که با رویکردها و ترندهای جدید حوزه امنیت فناوری اطلاعات و ارتباطات آشنا شوند.

در سال ۲۰۲۲ این کنفرانس از ۶ تا ۹ ماه ژوئن در شهر سانفرانسیسکو برگزار خواهد شد و با توجه به شرایط همه‌گیری جهانی افراد قادر خواهند بود به صورت حضوری و یا مجازی در آن شرکت کنند.

در RSAC ۲۰۲۰ رهبران صنایع مختلف و متفکران انقلابی از اقصی نقاط جهان گرد هم خواهند آمد. این کنفرانس دستیابی به راهکارهای متحول کننده را تسهیل می‌کند به علاوه، محصولات و راهکارهایی که ممکن است برای بازدیدکنندگان جذاب باشند در این کنفرانس ارائه می‌شود. افراد می‌توانند با جستجوی در سایت نمایشگاه و با استفاده از از راهنماهای موجود و یا بازارچه آنلاین RSAC Marketplac، اطلاعات بیشتری به دست آورند. در هر حالت کاربران می‌توانند با صدها وندور فعال در صنایع مختلف آشنا شده، با متخصصان آن‌ها دیدار کرده و چالش‌های خود را با آن‌ها در میان بگذارند و دمویی از آخرین راهکارهای آن‌ها را مشاهده کنند. RSAC Marketplace هم در دسترس افراد بوده و بازدیدکنندگان می‌توانند اقلام مورد نیاز خود را در این سایت به صورت آنلاین جستجو کرده و لیستی از وندورهایی که تمایل به ملاقات حضوری و مکالمه با آن‌ها در طول نمایشگاه RSAC ۲۰۲۲ دارند تهیه کنند.

از لحظه ورود به کنفرانس تا CyBEER Ops، کاربران قادر خواهند بود که متخصصان امنیت سایبری دیگر را رودررو ملاقات کرده و با ایشان صحبت کنند، همچنین افراد می‌توانند چالش‌های خود را در حوزه امنیت سایبری با متخصصین در میان گذاشته و نظرات متخصصان دیگر را از زوایای مختلف ارزیابی کنند تا بتوانند راهکار احتمالی مورد نیاز خود را بشناسند.

همچنین حاضران در نمایشگاه و کنفرانس قادر خواهند بود با حضور در دوره‌های کوتاه مدت آموزشی و استفاده از دستورالعمل‌های جدید و سرفصل‌های فناوری نوین ارائه شده توسط شرکت‌های مختلف آشنا شوند. انجمن‌هایی مانند SANS، FAIR، ISC دوره‌های آموزشی مختلف و متنوعی در طول این کنفرانس فراهم آورده‌اند که در آنها آموزش‌های عملی برای عناوین امنیت سایبری متنوعی ارائه می‌شود. این دوره‌ها برای حاضران در نمایشگاه بسیار جذاب و کاربردی بوده و مجموعه مهارت‌های گسترده‌تری را که برای بسیاری از بازدیدکنندگان می‌توانند

RSA® Conference

ارزشمند و مفید باشند در اختیار ایشان قرار خواهند داد.
در کنار این نمایشگاه ۱۷امین رقابت سالانه جعبه شنی نوآوری RSAC۱ نیز برگزار می گردد. در این رقابت بازدیدکنندگان قادر خواهند بود که رقابت بین استارت‌آپ‌های مختلف شاهد باشند. بازدیدکنندگان قادرند که کمپانی‌های نوپا و جدید حوزه امنیت را در سایت نمایشگاه به مشاهده کرده و محل حضور ایشان را در نمایشگاه بیابند.
در کنفرانس RSA مجموعه برگزار کننده به دنبال یافتن راه‌هایی برای توسعه گفتگوهای امنیت سایبری به روشی خلاقانه هستند. به همین جهت علاوه کنفرانس RSA اصلی کنفرانس‌های RSA دیگری تحت عنوان RSAC Unplugged در سرتاسر دنیا برگزار می‌شوند که در آن رهبران صنایع محلی و فعالان این حوزه در طول یک روز با یکدیگر در کنفرانس شرکت می کنند. محل‌های برگزاری این کنفرانس‌ها در سال‌های مختلف متفاوت بوده‌اند و سال ۲۰۱۹ در سیدنی و بانگکوک برگزار شده‌اند.

RSAC 365

کنفرانس RSA به عنوان بزرگترین نمایشگاه و گردهمایی امنیت سایبری در جهان برنامه جدیدی را که فرصت‌های یادگیری در تمام طول سال برای جامعه امنیت سایبری فراهم می کند تحت عنوان RSAC 365 نیز معرفی کرده است. برنامه جدید محتوای آموزشی مرتبط و بایاس نشده‌ای که شامل Webcastها، پادکست‌ها، بلاگ‌ها، ویدئوها و غیره می‌باشد را به صورت رایگان در اختیار بازدیدکنندگان از RSAC قرار خواهد داد.
کنفرانس RSA همزمان با راه‌اندازی زیرساخت‌های RSAC365، طی اعلامیه‌ای از کلیه افراد و سازمان‌های فعال در حوزه امنیت سایبری دعوت به ارائه ایده‌های خود برای فرصت‌های یادگیری آنلاین کرده است. رویکرد جدید یک فرآیند ارسال محتوای همیشه در دسترس برای تمام طول سال است که جامعه امنیت سایبری را تشویق به اشتراک گذاری تجربیات و دانش خود با سایرین می کند تا بتوانند مهارت‌های جدیدی آموخته و در مورد چالشی‌ترین موضوعات روز حوزه امنیت سایبری با هم به تبادل نظر کنند.

شبکه‌سازی و تعامل

حاضران در نمایشگاه قادر خواهند بود در برنامه‌های متنوعی که

1-17th annual RSAC Innovation Sandbox Contest

برای شبکه‌سازی و ارتباط با سایرین تدارک دیده شده شرکت کنند. به صورت کلی موارد زیر می‌توانند به عنوان فرصت‌های شبکه‌سازی و تعامل موجود در این کنفرانس در نظر گرفته شوند:

ایستگاه ورودی استقبال در نمایشگاه: در استقبال از بازدیدکنندگان ضمن پذیرایی، با حضور در کنار سازمان‌های پیشرو امنیت اطلاعات با راهکارهای آن‌ها آشنا شوند.

Expo Pub Crawl: حامیان اصلی نمایشگاه در این بخش در دسترس بوده و علاقمندان می‌توانند با حضور در آن ضمن پذیرایی با آخرین محصولات ارائه شده توسط آن‌ها آشنا شده و پیشنهاداتی را دریافت کنند.

Women's Networking Reception: در این قسمت بانوان توانمند و خلاق حوزه امنیت سایبری می‌توانند با هم دیدار کرده و ایده‌های خود را به اشتراک بگذارند.

CyBEER Ops: همه ساله در این کنفرانس یک گردهمایی جانبی تفریحی نیز برگزار می‌شود که بازدیدکنندگان با شرکت در آن علاوه بر تفریح می‌توانند با سایر فعالان در این حوزه ارتباط برقرار کرده و آشنا شوند.

Birds of a Feather: در این همایش بازدیدکنندگان دارای بلیت کامل نمایشگاه قادر خواهند بود که با سایر اعضای تاثیرگذار حوزه امنیت سایبری ملاقات داشته و در مورد موضوعات موردعلاقه طرفین گفتگو کنند.

Learning Labs: در این آزمایشگاه‌ها افراد با همکاری متقابل و تعامل دوطرفه موضوعات جدیدی را می‌آموزند. کارگاه‌های عملی این آزمایشگاه‌ها، مهارت‌های امنیت سایبری را با یک سری از شبیه‌سازی‌های دنیای واقعی و فعالیت‌هایی فراگیر تقویت می‌کند.

Tutorials & Trainings: در این بخش بازدیدکنندگان قادر خواهند بود که در گردهمایی‌های آموزشی که توسط موسسات مهم و مطرح در این حوزه برگزار می‌شوند شرکت کرده و با موضوعات نوین حوزه امنیت سایبری آشنا شوند.

Capture the Flag & Hands-on Activities: جلساتی که در آن یک متخصص این حوزه به صورت زنده به پرسش‌های بازدیدکنندگان در مورد یک موضوع خاص پاسخ می‌دهد.

برنامه‌ها و رخدادهای جانبی

کنفرانس RSA برنامه‌ها و رخدادهای جانبی هم دارد که می‌تواند برای هر کسی از دانشجویان امنیت تا مدیران ارشد امنیت اطلاعات مفید باشد. در ادامه به معرفی مختصر آن‌ها خواهیم پرداخت:

Cryptography Track: در این بخش افراد مختلف قادر خواهند بود که مقالات تحریر یافته خود در حوزه‌های مختلف مرتبط با رمزنگاری ارسال کرده و پس از تایید و انتخاب در جلساتی آن را ارائه کنند و افراد حاضر در نمایشگاه از آن‌ها پرسش خواهند کرد.

CE Credits: در این کنفرانس شرکت‌کنندگان قادرند که از اعتبارات آموزشی که در همکاری با موسسات کلیدی در این حوزه تدارک دیده شده است، استفاده کنند.

LoyaltyPlus: در این برنامه افرادی که ۵ سال یا بیشتر با بلیت حضور کامل در نمایشگاه حاضر شده باشند، می‌توانند به عنوان مهمان ویژه از امتیازات ویژه‌ای که برای آن‌ها در نظر

RSA® Conference

گرفته شده است، استفاده کنند.

Innovation Sandbox Contest: این بخش همان‌طور که قبلا اشاره شد، بخشی است که نوآوران حوزه امنیت سایبری به رقابت پرداخته و ده منتخب برتر بین آن‌ها سه دقیقه فرصت خواهند داشت که در پانل قضاوت حاضران خود را عرضه کنند.

Sandbox: جعبه شنی به عنوان یک زیرساخت نوآوری، موضوعات مختلف امنیت سایری را به شکلی نو مورد بررسی قرار می‌دهد. در RSAC2022 هفت جعبه شنی مختلف با تجربیاتی ارزشمند ارائه خواهد شد.

Early Stage Expo: این فضای نمایشگاهی شرکت‌های نوظهور و جدید را که می‌توانند رهبران آینده حوزه امنیت باشند معرفی خواهد کرد و ۳۰ استارت‌آپ در آن حاضر خواهند شد.

Broadcast Alley: در این بخش که اتاق خبر غیررسمی RSAC2022 است، رسانه های برتر حضور داشته و با مهمانان اختصاصی بسیار مهم مصاحبه‌هایی خواهند داشت.

College Day: در این قسمت افراد جویای کار می‌توانند با شرکت‌های بزرگی که به دنبال نیروهای جوان و توانمند هستند و فرصت‌های موجود آشنا شوند.

Sponsored Experiences: در این قسمت پیشنهادات حمایتی هیجان‌انگیزی برای بازدیدکنندگان ارائه خواهد شد و افراد می‌توانند ضمن نوشیدن قهوه در بازی‌ها هم شرکت کنند.

Security Scholar: در این گردهمایی که صرفا با دعوت از قبل قابل حضور است، دانشجویان مشخصی با متخصصان حوزه امنیت سایبری مرتبط می‌شوند تا با روش‌های مختلف رقابت در حوزه امنیت سایبری آشنا شوند.

eFraud Global Forum: این همایش که یک همایش یک‌روزه است افراد برگزیده‌ای که با دعوت قبلی در آن حاضر می‌شوند، به تبادل نظر در زمینه اکوسیستم ضدفریب ۲ جهانی می‌پردازند.

Executive Security Action Forum: در این انجمن هم گروهی از بزرگان و مدیران ارشد امنیت سایبری از ۱۰۰۰ کمپانی بزرگ جهانی با هم دیدار داشته و در حوزه امنیت سایبری با هم به تبادل افکار می‌پردازند.

International Cybersecurity Forum: در این همایش تصمیم‌سازان ارشد بین‌المللی حوزه امنیت سایبری به صورت محرمانه گرد هم می‌آیند و به راه‌هایی برای شکل‌دهی آینده امنیت سایبری می‌اندیشند.

RSAC Security Operations Center: بازدیدکنندگان در این قسمت قادر خواهند بود از یک مرکز عملیات امنیتی از نزدیک بازدید کرده و با آن آشنا شوند.

First-Time Attendees Roundtable Discussions & Networking: افرادی که برای اولین بار در این کنفرانس حاضر می‌شوند می‌توانند با شرکت در این نشست با ابعاد کنفرانس آشنا شده و سوالات خود را در موضوعات مختلف از کنفرانس و نمایشگاه بپرسند.

هزینه‌های شرکت در کنفرانس RSA

افرادی که به دنبال حضور در این کنفرانس باشند در چهار حالت مختلف می‌توانند در آن حاضر شوند که هر حالت دسترسی‌های متفاوتی دارد:

Full: در این حالت بازدیدکنندگان قادر به استفاده از تمام امکانات و جلسات تدارک دیده شده در RSAC خواهند بود و هزینه آن ۲۱۹۵ دلار است.

Expo Plus: این نسخه محدودترین بلیت حضور فیزیکی در نمایشگاه است که در آن افراد قادر به حضور در تعداد محدودی سخنرانی کلیدی و جلسات خواهند بود و در عین حال می توانند از نمایشگاه نیز دیدن کنند. هزینه این بلیت ۳۲۵ دلار است.

Expo: بلیتی که با آن بازدیدکننده صرفا مجاز به بازدید از نمایشگاه جانبی خواهد بود با هزینه ۵۰ دلار.

بلیت دیجیتال: که در آن کاربر به صورت برخط قادر به دسترسی به تمامی محتوای دیجیتال ارائه شده در این نمایشگاه با پرداخت ۴۹۵ دلار خواهد بود.

منابع:

https://www.rsaconference.com/usa/

2- anti-fraud ecosystem

Security

اخبار فناوری
technology news

همراه فناوری
fanavari hamrah
فصلنامه‌ی خبری تحلیلی
زمستان ۱۴۰۰ شماره‌ی چهارم

افزایش میزان پذیرش اعتماد صفر

از گسترش و توسعه خدمات ابری تا افزایش چشم‌گیر استفاده از تجهیزات موبایل توسط کاربران در سطح جهان، از ظهور و بروز تهدیدات امنیت سایبری جدید و پیشرفته در سطح جهان تا تغییر ناگهانی فضای کاری و حرکت سازمان‌ها به سمت افزایش میزان دورکاری کارکنان همگی نشان‌گر آن هستند که دهه گذشته، دهه‌ای بسیار پرچالش و آکنده از تغییر جهت‌هایی بوده است که سبب شده سازمان‌ها فرآیند تحول و ارتقای زیرساخت‌های امنیتی خود را شتاب دهند و با مدل‌های امنیتی جدید انطباق یابند. از طرفی هر چه بیشتر پیش می‌رویم میزان تغییرات بیشتر می‌شود و این امر نشان‌دهنده آن است که سرعت تغییرات کمتر نخواهد شد و ما باید خودمان را برای آن آماده کنیم.

برای مقابله با این نرخ سریع تغییرات و افزایش میزان تهدیدات، مدل اعتمادصفر به عنوان یک استراتژی امنیت سایبری برای سازمان‌ها در سطح جهان معرفی شده است. در مدل اعتمادصفر با فرض وجود یک شکاف امنیتی در سیستم وضعیت هویت کاربران و تجهیزات متصل، نقاط انتهایی، اجزای شبکه و دیگر منابع موجود بر اساس داده‌ها و سیگنال‌های موجود کنترل می‌شود. این مدل با اتکای بر اجرای خط‌مشی‌های امنیتی بی‌درنگ محتوایی در راستای کاهش میزان دسترسی‌های ممتاز و کاهش میزان ریسک قدم برمی‌دارد. در این مدل از مجموعه داده‌های عظیم در دسترس، تحلیل رفتار کاربران، فرآیند خودکارسازی و یادگیری ماشین به منظور شناسایی سریع، مقابله و بازیابی از حملات احتمالی استفاده می‌شود.

سازمان‌هایی که زودتر با این مدل انطباق یافته‌اند مزایای آن را مشاهده کرده‌اند و به صورت کلی سازمان‌هایی که با یک تفکر اعتماد صفر در فضای کاری خود عمل می‌کنند، مقاوم‌تر، پاسخ‌گوتر و حفاظت شده‌تر از سازمان‌های متکی بر مدل‌های قدیمی و سنتی حفاظت و امنیت پیرامونی هستند.
پذیرش و انطباق با مدل اعتماد صفر در حال شتاب‌گیری است.
برای تهیه گزارش میزان انطباق با مدل اعتماد صفر سال ۲۰۲۱

شکل۱- منافع به کارگیری مدل اعتمادصفر به ترتیب اهمیت

با بیش از ۱۲۰۰ فرد تصمیم‌گیر حوزه امنیت سایبری در سازمان‌های مختلف در یک بازه زمانی ۱۲ ماهه درباره روش انطباق با مدل اعتماد صفر مصاحبه شده است. نکات برجسته تحقیقات انجام شده به شرح زیر هستند:

تحقق مدل اعتماد صفر در حال حاضر بالاترین اولویت امنیتی سازمان‌ها است. ۹۶ درصد از افراد تصمیم‌گیر در حوزه امنیت سایبری معتقدند تحقق مدل امنیت صفر موضوعی حیاتی برای موفقیت سازمان آن‌ها است. امروز اثبات شده که آینده امنیت سازمان‌ها به شدت نیازمند تاکید بر تحقق مدل اعتماد صفر است. در پاسخ به اینکه دلایل اصلی سازمان برای انطباق و تحقق مدل امنیت صفر چیست، سازمان‌ها افزایش میزان امنیت و افزایش چابکی در انطباق با قوانین رگولاتوری، افزایش سرعت شناسایی تهدیدات و بازیابی از آنها، افزایش سهولت و دسترسی به تحلیل‌های امنیتی را به عنوان مهم‌ترین دلایل ذکر کرده‌اند.

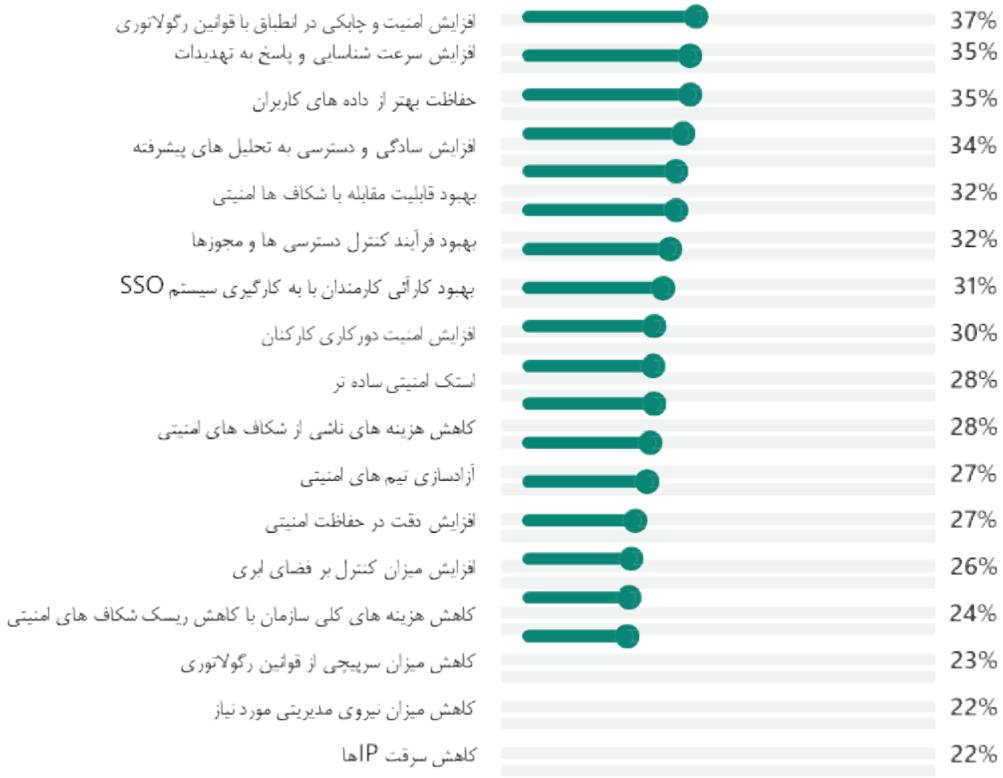
آشنایی، پذیرش و انطباق با این مدل به سرعت در حال افزایش است. ۹۰% از تصمیم‌گیران حوزه امنیت سایبری با این مفهوم آشنا بوده و ۷۶% از آن‌ها در حال پیاده‌سازی آن در سازمان خود بوده‌اند که این اعداد نسبت به گزارش قبلی منتشر شده از اعداد ۲۰% و ۶% به این مقادیر افزایش یافته که رشد چشم‌گیری است و نشان از توسعه پذیرش این مفهوم در سطح سازمان‌های دارد.

کار ترکیبی (دورکاری+حضور در سازمان) یکی از عوامل اصلی حرکت به سمت پذیرش و انطباق این مدل بوده است. حرکت به سمت توسعه کار ترکیبی که با گسترش کرونا شتاب یافته، پذیرش و انطباق با مدل اعتماد صفر را رشد بخشیده است به نحوی که ۸۱ درصد از سازمان‌ها اعلام کرده‌اند که در حال حاضر مدل کاری ترکیبی را آغاز کرده و بخشی از نیروی کاری خود را به صورت ترکیبی به کار گرفته‌اند. اعتماد صفر برای حفظ امنیت داده‌های سازمانی در چنین سازمان‌هایی به منظور حفاظت از منافع سازمان امری ضروری خواهد بود.

بیش از نیمی از مصاحبه شوندگان معتقدند که از سایر سازمان‌ها در انطباق و حرکت به سمت تحقق این مدل پیش‌تر هستند. ۵۲% گفته‌اند که نسبت به زمان‌بندی پیش‌بینی شده در زمینه انطباق و تحقق مدل اعتماد صفر جلوتر هستند و ۵۷% معتقدند که از سایر سازمان‌ها جلوتر هستند. واضح است تحولاتی که طی دو سال گذشته اتفاق افتاده و گسترش کرونا و اجبار به دورکاری تاثیری شگرف در پذیرش این مفهوم در سازمان‌ها داشته است و در عین حال پذیرش آن نیز سبب شده که سازمان‌ها با اطمینان بیشتر و موثرتر بتوانند فعالیت‌های خود را پیگیری کنند.

اعتمادصفر همچنان به عنوان یک اولویت اصلی سازمان‌ها مطرح خواهد بود و نیازمند تزریق بودجه برای تحقق آن است. بیش از نیمی از پاسخ‌دهندگان انتظار داشتند که اهمیت تحقق استراتژی اعتمادصفر تا سال ۲۰۲۳ بیشتر نمایان شود و ۷۳% انتظار داشتند که بودجه موردنیاز جهت تحقق این استراتژی افزایش یابد. با درک بیشتر مزایای و منافع تحقق مدل اعتمادصفر، رهبران سازمان‌ها بیشتر به سمت آن حرکت کرده و انتظار می‌رود که این اعداد در گذر زمان افزایش داشته باشند.

نتایج ارزیابی انجام شده میزان اهمیت منافع حاصل از به کارگیری یک مدل امنیت اعتمادصفر در شکل ۱ به تصویر کشیده شده است.



شکل ۱- منافع به کارگیری استراتژی اعتماد صفر

در تصویر زیر نیز موانع اصلی در استقرار و تحقق استراتژی اعتماد صفر نشان داده شده است.

شکل ۲- موانع اصلی در استقرار و تحقق استراتژی اعتماد صفر

این گزارش میزان پیشـــرفت در پذیرش مدل اعتماد صفر برای سازمان‌هایی از صنایع و بازارهای مختلف را نشان می‌دهد. امید است که نتایج این تحقق بتواند به شما برای شتابدهی در استراتژی‌های پذیرش مدل اعتماد صفر در سازمان کمک نماید، میزان پیشرفت جمعی و اولویت‌بندی رقبای شما را آشکار ساخته و دیدی نسبت به وضعیت فضای در حال تحول سریع آتی در اختیار بگذارد.

اشکال جدی ارتقای سطح دسترسی لینوکس که به مدت ۱۲ سال پنهان مانده بود!

آسیب‌پذیری PwnKit به کاربران غیرمجاز اجازه دسترسی Route می‌دهد.
محققان امنیتی یک اشکال افزایش سطح دسترسی محلی را در برخی نسخه‌های لینوکس پیدا کرده‌اند که به کاربر غیرمجاز اجازه می‌دهد تا کدی را با دسترسی روت یک آبَر کاربر با دسترسی بالا اجرا کند و به آن‌ها امکان دسترسی به کل سیستم را می‌دهد.

شرکت امنیتی کوالیس (Qualys) باگ را PwnKit نامیده و گفته polkit یا PolicyKit در ماه می ۲۰۰۹، یعنی ۱۲ سال پیش معرفی شده است.

کوالیس گفته که این آسیب‌پذیری که در دستور pkexec polkit نهفته دارای باگ در کد بوده و به مهاجمان اجازه می‌دهد برای معرفی متغیرهای محیطی ناامن، نوشتن‌های خارج از محدوده (out-of-bounds writes) انجام دهند. با وجود اینکه محققان کد اثبات مفهوم را برای PwnKit منتشر نکرده‌اند، ولی اظهار داشته‌اند که «با توجه به اینکه استفاده از این آسیب‌پذیری آسان است، پیش‌بینی می‌شود که سوءاستفاده‌های عمومی از آن ظرف چند روز در دسترس قرار گیرند».
در این بین iTnews اشاره کرده است که کدهای اثبات مفهومی این آسیب‌پذیری بر روی صفحات وب پست شده و در دسترس عموم قرار دارند.
نسخه‌های Ubuntu، Debian، Fedora و CentOS Linux توسط محققان امنیتی کوالیس به عنوان نسخه‌های آسیب‌پذیر لینوکس در برابر این آسیب‌پذیری تأیید شده‌اند. هرچند این احتمال وجود دارد که سایر نسخه‌های لینوکس نیز آسیب‌پذیر باشند.
در ۱۸ نوامبر سال گذشته کوالیس این آسیب‌پذیری را به شرکت رد هت (Red Hat) گزارش کرده است و اکنون وصله‌ها در دسترس هستند. به‌عنوان رفع عیب موقت، امکان حذف بیت SUID از برنامه pkexec با chmod ۰۷۵۵ نیز وجود دارد.
در حالی که polkit از سیستم‌عامل‌های مشابه یونیکس مانند Solaris و توزیع‌های مختلف BSD و همچنین لینوکس پشتیبانی می‌کند اما متخصصان کوالیس اظهار داشته‌اند که بررسی دقیقی نسبت به اینکه آیا این آسیب‌پذیری در آن‌ها نیز وجود دارد، انجام نداده‌اند.

سیستم عامل OpenBSD که یک سیستم عامل مبتنی بر امنیت و صحت کد است به سادگی قابل سوء استفاده نیست، زیرا syscall execve() که در کرنل آن وجود دارد از اجرای برنامه‌های با تعداد argc صفر ۱ جلوگیری می‌کند.
در مورد Polkit در ماه‌های اخیر باگ‌های ارتقای دسترسی ممتاز دیگری نیز گزارش شده است که امکان اجرای کد در قسمت Root را به کاربران می‌دهد.
در ماه ژوئن سال گذشته، محقق امنیتی آقای کوین بک‌هاوس در یک پست منتشر شده در وبلاگ خود در مورد یک باگ با عمر ۷ ساله در Polkit نوشته است که در این باگ به سادگی در همکاری با دیگر ابزارهای کمکی سیستم قابل سوء استفاده خواهد بود.
محققان کوالیس، تنها افرادی نیستند که با PwnKit مواجه شده‌اند؛ چراکه محقق دیگری به نام رایان مالون در سال ۲۰۱۳ نیز همین باگ را شناسایی کرده و به‌طور عمومی گزارش کرده بود. وی حتی وصله‌ای امنیتی برای رفع آن نوشته و منتشر کرده بود؛ هرچند در نهایت موفق نشد روشی برای جلوگیری از سوءاستفاده از این آسیب‌پذیری ارائه کند. در ماه ژوئن گذشته نیز، کوین بک‌هاوس، محقق امنیتی گیت‌هاب، یک آسیب‌پذیری دیگر برای افزایش سطح دسترسی در لینوکس گزارش کرد. نام ردیابی این باگ CVE-۲۰۲۱-۳۵۶۰ است.
پس از شناسایی کامل و اعلان عمومی وجود این باگ امنیتی، توزیع‌کنندگان اصلی لینوکس وصله‌هایی برای این آسیب‌پذیری منتشر و متخصصان امنیتی نیز به‌طور جدی از مدیران درخواست کرده‌اند که نصب این وصله را در اولویت قرار دهند.

منبع

https://www.itnews.com.au/news/serious-linux-privilege-escalation-bug-lay-hidden-for-12-years-575115

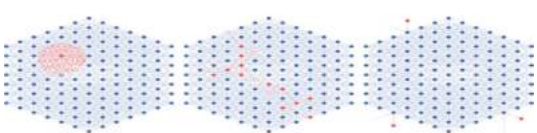
1- Zero argc count

امن سازی سیستم های هوش مصنوعی با استحکام متخاصم

(adversarial robustness)

سیستم‌های مبتنی بر هوش مصنوعی می توانند نسبت به حملات خصمانه (adversarial attacks) آسیب پذیر باشند. IBM می کوشد تا این سیستم‌ها را در برابر هک‌شدن مقاوم کرده، ریشه مشکلات را شناسایی و با پیش‌بینی استراتژی‌های نوین و طراحی مدل‌های مستحکم آن‌ها نسبت به حملات مقاوم نماید.

در سال های اخیر مدل ها و مجموعه‌داده‌های هوش‌مصنوعی به صورت انفجاری رشد داشته‌اند. پیشنهاد موسیقی‌های جدید یا گزینه‌های خریدآنلاین، کمک به حفظ جان انسان‌ها با شناسایی تومورها و غیره برخی کاربردهای مطرح این حوزه هستند.



در طول استقرار مدل‌های هوش‌مصنوعی، به منظور تحقق بهترین کارآیی شرایط بادقت کنترل می‌شوند ولی در دنیای‌واقعی شرایط اغلب به شکل دلخواه نیستند. لذا مدل‌ها باید به گونه‌ای طراحی شوند که نسبت به آسیب‌های احتمالی در دنیای واقعی مقاوم باشند.

زمینه تحقیقاتی یادگیری ماشین متخاصم می کوشد تا بین مدل‌های هوش‌مصنوعی در زمان توسعه و استقرار پلی برقرار کرده و آن‌ها را در برابر ناملایمات احتمالی در دنیای‌واقعی مقاوم سازد. در دنیای واقعی مدل‌های هوش‌مصنوعی ممکن است هم به‌صورت ناخواسته (مانند دریافت داده تخریب‌شده)، وهم عامدانه مانند تلاش یک هکر برای نفوذ وآسیب به عملکرد سیستم در معرض ناملایمات قرار گیرد که هر دو می‌تواند منجر به تولید نتایج نادرست شود. در کارهای تحقیقاتی انجام‌شده، IBM می کوشد نقاط ضعف احتمالی در مدل‌های هوش مصنوعی را شناسایی کرده و آن‌ها را در برابر حملات مقاوم سازد.

شناسایی نقاط ضعف

باید توجه داشت آگاهی از نقاط قوت و ضعف به یک اندازه مهم هستند و باید با شناخت نقاط ضعف در راستای رفع آن‌ها گام برداریم.

داده‌های سمی

یکی از مهم‌ترین حملات احتمالی به سیستم‌های هوش‌مصنوعی ورود داده‌های سمی به آنهاست. در صورت دسترسی، فردمهاجم قادر خواهد بود با تزریق داده‌های آموزشی غلط باعث شود مدل هوش‌مصنوعی به شکلی غیرمطلوب عمل نماید.

انطباق دامنه بدون نظارت (UDA[1]) یک رویکرد تعمیم است که در آن دانش از یک دامنه مبدا برچسب‌گذاری‌شده به یک دامنه هدف برچسب‌گذاری‌نشده با یک توزیع داده متفاوت انتقال می‌یابد. UDA زمانی که به‌دست‌آوردن مجموعه داده‌های مقیاس‌بزرگ منظم، زمان‌بر و پرهزینه باشد، مناسب است. بسیاری از الگوریتم‌های UDA با تنظیم یک حدبالای خطای دامنه‌ی‌مبدا و کمینه‌کردن واگرایی بین توزیع داده دو دامنه عمل می‌کنند. به جهت نبود حد پایین روی خطای مبدا بسیاری از این الگوریتم‌ها با وجود موفقیت روی داده‌های نمونه در سناریوهای معین دچار شکست می‌شوند و این امر حکایت از آن دارد که روش‌های UDA نسبت به توصیع داده حساس بوده و درنتیجه نسبت به حملات خصمانه مانند داده‌های ورودی سمی آسیب‌پذیر هستند.

برای فهم تاثیر این ضعف، تاثیر ورود داده‌های سمی بر کارایی روش‌های UDA رایج با ارائه ترکیبی از داده‌های تمیز و داده‌های بابرچسب‌گذاری غلط ارزیابی شدند و نتایج نشان‌دهنده کاهش دقت دامنه هدف تا ۰% با سمی‌کردن ۱۰% از داده‌ها بود. این وضعیت حکایت از محدودیت‌های‌شگرف دربه‌کارگیری روش‌های UDA دارد.

اختلال وزن

تغییر در پارامترهای وزن‌دهی یک مدل یادگیری‌ماشین می‌تواند خروجی موردانتظار از مدل را متاثر کند. حساسیت نسبت به اختلال وزن تاثیر جدی در فشرده‌سازی مدل، ارزیابی گپ تعمیم و استحکام متخاصم دارد.

مقابله باحملات

بهترین دفاع حمله است: با پیش‌بینی روشی که مهاجمان ممکن‌است حمله کنند به مقابله خواهیم پرداخت.

مهندسی معکوس برای بازیابی داده‌های خصوصی

یادگیری فدرال عمودی (VFL[2]) یک چهارچوب یادگیری‌ماشین است که درآن مدلی با داده‌هایی از مالکان مختلف درباره موضوعی مشترک آموزش (train) داده می‌شود. مثلا داده‌هایی از بیمارستان‌های مختلف درباره بیماران مشابه برای آموزش استفاده می‌شود. برای حفاظت حریم‌خصوصی، تنها پارامترهای مدل و گرادیان نحوه تغییرآنها مبادله می‌شوند. اما در صورت قابلیت بازیابی داده‌ها از روی گرادیان درطول VFL نشت‌داده بزرگی ممکن خواهد شد.

ما مدل حمله‌ای به نام CAFE3 به منظور بازیابی داده‌های خصوصی با کیفیتی بالاتراز روش‌های موجود ارائه کرده‌ایم که شامل بسته‌های بزرگ داده است که نتایج شبیه‌سازی نشانگر ریسک بسیار بزرگ نشت داده در VFL است.

به عنوان یک روش کاهش CAFE، پیشنهاد می‌شود داده‌های گرادیان اشتباه بجای داده‌های واقعی درطول آموزش مبادله شوند. تا زمانی که شباهت گرادیان‌های درست و اشتباه بیش‌ازسطح مشخصی باشد، کارایی یادگیری هردو یکسان خواهد بود.

یادگیری متخاصم رویکردی است که به دنبال کمینه کردن بیشینه زیان متخاصم است. اگر یک روش Min-Max تعمیم‌یافته

1- Unsupervised domain adaptation

2- Vertical federated learning

بتواند برای توسعه حملات متخاصم موثرتر به کار گرفته شود، در فریب مدل‌های هوش‌مصنوعی در سه سناریوی مختلف شامل چرخش، ترجمه و روشن کردن بهتر عمل خواهد کرد.

در مدل پیشنهادی ما وزن‌های دامنه روی توزیع احتمال بین مجموعه‌ی دامنه‌ها در یک سناریو اختصاصی بیشینه می‌گردند. درنهایت چهارچوب Min-Max پیشنهادی ما به تنظیمات امنیتی ترجمه می‌شود و مدلی آموزش می‌بینند که زیان متخاصم را در بدترین فضا در مواجه با چندین حمله متخاصم، کمینه می‌نماید و نتایج آن عملکردی به مراتب بهتر را نشان می‌دهد.

طراحی مدل‌ها و الگوریتم‌های مستحکم

حفظ استحکام در طول یادگیری متضاد: یادگیری متضاد (CL) تکنیک یادگیری ماشین است که طی آن مدلی خصوصیات عمومی یک مجموعه داده بدون برچسب را با شناسایی نقاط داده مشابه یا متفاوت می‌آموزد. یادگیری بدون اتکا به برچسب‌ها، یادگیری خودنظارتی است که بسیار مفید است. خودنظارتی امکان پیش‌آموزش مستحکم را فراهم می‌کند، هرچند این قابلیت در تنظیم‌دقیق مدل برای یک وظیفه مشخص بسمت پایین انتقال پیدا نمی‌کند. تلاش می‌شود انتقال استحکام از پیش‌آموزش به تنظیم-دقیق را با یادگیری متخاصم (AT[3]) ارتقا داده شود.

AT معمولا برای یادگیری نظارتی با داده‌های برچسب‌گذاری‌شده به کار می‌رود، اما با حذف پیش‌نیاز داده برچسب‌گذاری‌شده، با یک چهارچوب CL متخاصم (AdvCL) جدید استحکام مدل افزایش می‌یابد. چهارچوب شامل دوجزء اصلی است. اولا با تمرکز برداده‌های پرتکرار نحوه انتخاب مدل بهبود یافته است و ثانیا یک محرک نظارتی با تولید شبه برچسب‌هایی برای داده‌ها از طریق خوشه‌بندی خصوصیات به منظور افزایش قابلیت انتقال استحکام با آن یکپارچه شده است.

3- Adversarial training

طراحی با داده‌های آلوده

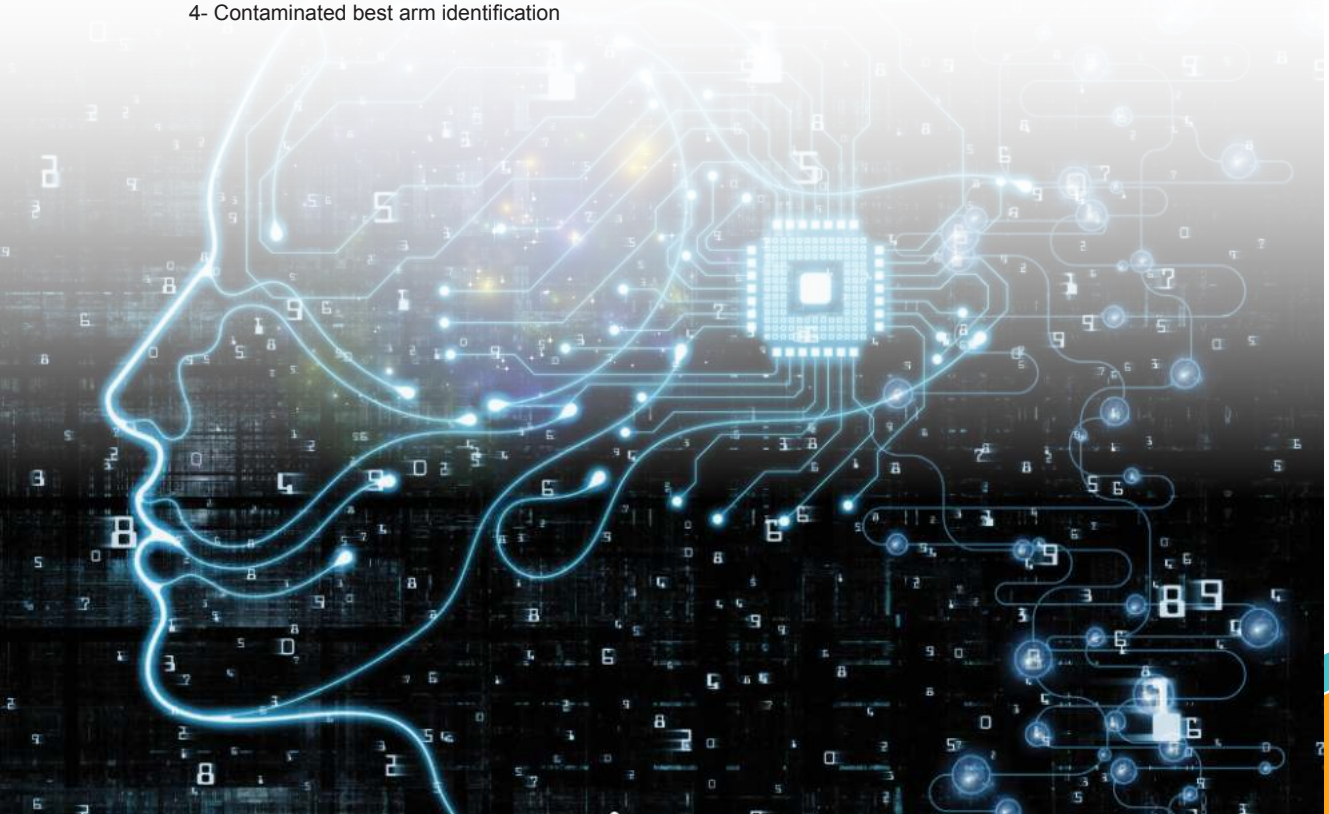
شناسایی بهترین بازوی آلوده (CBAI[4])، رویکردی برای انتخاب بهترین گزینه‌ها (بازوها) با فرض آسیب‌پذیری داده‌ها نسبت به تخریب متخصام است. برای مثال یک سیستم پیشنهاد کتاب ممکن است کتاب‌هایی پیشنهاد دهد که نامربوط یا بدخواهانه باشند و این نمونه‌های آلوده مانع از شناسایی بهترین بازو خواهدشد.

دو روش برای CBAI پیشنهاد داده می‌شود که اولی مبتنی بر کاهش هم‌پوشانی بین بازه‌های اطمینان برای بازوهای مختلف و دیگری مبتنی بر حذف متمادی بازوهای زیربهینه است. الگوریتم‌ها شامل تخمین متوسط پاداشی است که کمترین انحراف از متوسط واقعی با به‌کارگیری کمترین نمونه‌ها را دارد. با ارائه قوانین تصمیم‌گیری برای انتخاب دینامیک بازوها درگذرزمان، متوسط هر بازو را تخمین زده، فرآیند انتخاب بازو را متوقف کرده و در نهایت بهترین بازو انتخاب می‌شود. هر دو الگوریتم قادرند باوجود آلودگی برخی نمونه‌ها، بهترین بازو راشناسایی کرده و عملکردی بهتر از روش‌های CBAI برای مجموعه داده‌های مصنوعی ودنیای واقعی کنونی داشته باشند که نهایتا منجر به ارتقای استحکام مدل‌های هوش‌مصنوعی کنونی خواهند شد.

هوشمندسازی سیستم‌های هوش‌مصنوعی آینده

الگوریتم‌های هوش‌مصنوعی سال‌هاست به دنبال دستیابی به دقت کافی جهت به‌کارگیری در دنیای واقعی هستند، هرچند امنیت روش‌ها، عملکرد منصفانه، همکاری متقابل و استحکام آن‌ها چندان مدنظر نبوده است. توسعه‌دهندگان می‌بایست مدل‌های هوش‌مصنوعی را با شناسایی حرکت‌های آتی مهاجمان و حفره‌های امنیتی نسبت به آن‌ها مقاوم کنند. ■

4- Contaminated best arm identification



مدیران ارشد امنیت اطلاعات چگونه برای مقابله با تهدیدات در ۲۰۲۲ آماده می‌شوند؟

جک واسو معاون امنیت، هویت و انطباق مایکروسافت به تحلیل راهکارهای پیش‌روی مدیران ارشد امنیت سازمان‌ها (CISOs) در سال ۲۰۲۲ پرداخته است.

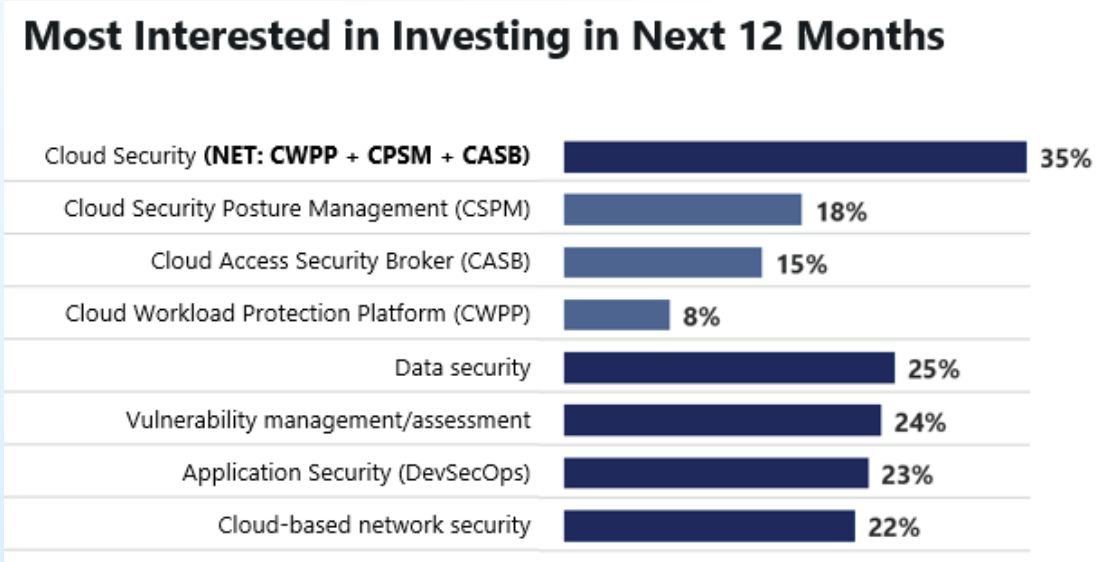
با نگاه به سال‌های گذشته، چشم‌انداز امنیت، تغییرات چشم‌گیری را به شکلی پیوسته پشت سر گذاشته است. همه روزه شاهد هزینه‌های پرداختی بزرگی هستیم که سازمان‌ها در ابعاد مختلف در مواجه با چالش‌های همه‌گیری کرونا، توسعه دارایی‌های دیجیتال و تحول در تهدیدات با آن روبرو هستند. تعهد برای حفاظت از مردم و سازمان‌ها در چنین محیطی از اهمیت بالایی برخوردار است. باتوجه به ماموریت ما برای کمک به رهبران امنیت و تضمین تامین ابزارهای موردنیاز جهت تحقق امنیت، ما به‌صورت پیوسته می کوشیم با فهم اولویت‌های این حوزه و با تحقیق از رهبران امنیتی، دانش خود را به روز کرده و برخی از داده‌هایی را که می تواند برای سایرین مفید باشد به اشتراک بگذاریم.

۵ چالش اصلی حاصل از مطالعات در شکل ۱ نشان داده‌شده‌اند. همانطور که در شکل دیده می‌شود، رهبران امنیتی بزرگترین چالش خود را مدیریت ریسک ناشی از باج‌افزارها و اخاذی سایبری (۲۹%) عنوان کرده‌اند. چالش‌های مهم بعدی به ترتیب تضمین پیکربندی منابع ابری، اپلیکیشن‌ها و بارکاری (۲۸%)، پرکردن حفره‌های حفاظتی در فضای چند-پلتفرمی، چند-ابری وهیبرید (۲۷%)، بازنشستگی و خروج متخصصان امنیتی (۲۶%) و توانمندسازی کاربرانتهایی بدون کاهش سطح امنیت دردسترس(۲۵%) عنوان شده است.

بر این اساس مقابله با باج‌افزار، اولویت اول رهبران امنیت گزارش شده است. طبق مطالعه انجام شده در پایان سال ۲۰۲۱ توسط تیم شناسایی و پاسخ مایکروسافت (DART[1])، در بازه جولای ۲۰۲۰ تا ژوئن ۲۰۲۱ حملات باج‌افزار بالغ بر ۱۰۷۰ درصد افزایش داشته است. مطالعات نشانگر پیشرفته‌تر و بالغ‌تر شدن مهاجمان و مجرمان سایبری بوده و نشان می‌دهد آن‌ها برای حملات خود حتی دیگر نیازمند توسعه فردی ابزار نیستند. امروزه افراد مهاجم قادرند که به سادگی کیت‌ها و خدمات جرائم امنیتی پیشرفته و خودکار که بسیار مقیاس‌پذیر و قابل استفاده در سطحی وسیع هستند، را خریداری کرده و به کمپین‌های خود اضافه کنند و این امر هزینه توسعه ابزارهای حمله به صورت فردی را به‌شدت کاهش داده و درآمد حاصل از این حملات، موتور حرکتی به سمت انجام حملات بیشتر شده است.

امنیت ابری چالش مهم دوم از نظر محققان بوده است، زیرا با

1- Detection and Response Team



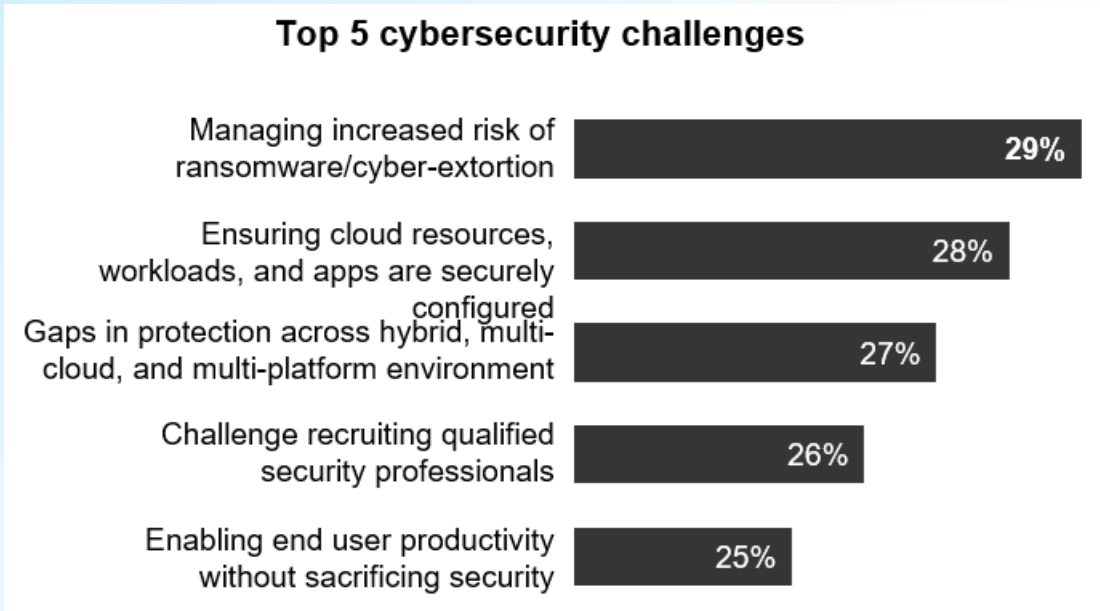
شکل ۲- حوزه‌های جذاب سرمایه گذاری امنیتی برای ۱۲ ماه آتی

وقوع همه‌گیری کرونا و تغییر مدل‌های کسب‌وکار و انتقال بخش عظیمی از داده‌های سازمان‌ها به فضای خارج از سازمان و روی ابرهای عمومی و خصوصی، تضمین امنیت داده‌های سازمانی اهمیت بیشتری یافته و محصولات و ابزارهای تحقق امنیت ابری نیز رشد و ارتقای چشم‌گیری داشته‌اند.

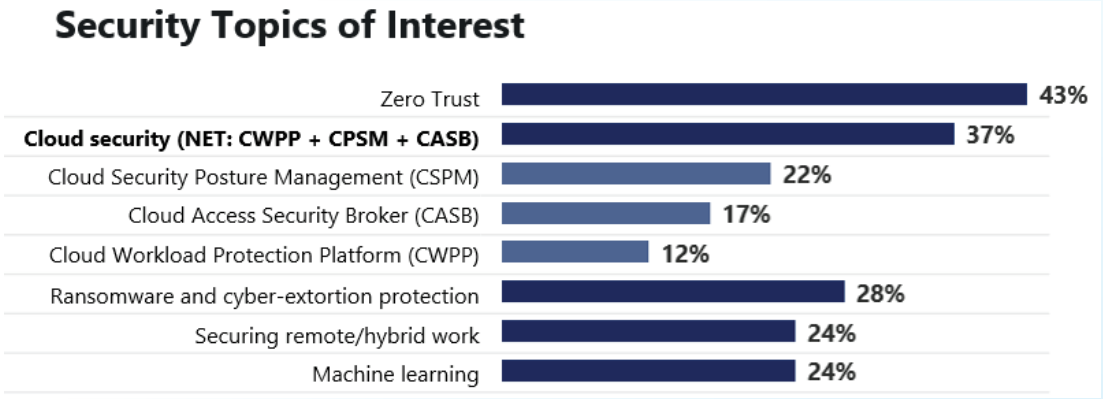
اولویت‌های سرمایه‌گذاری در ۲۰۲۲

همراستا با مهم‌ترین چالش‌های امنیت سایبری، امنیت ابری به منظور حفاظت از بارکاری، پرکردن حفره‌ها و امن‌سازی دسترسی به منابع ابری، مهم‌ترین زمینه سرمایه‌گذاری در ۱۲ ماه آتی خواهد بود. با توجه به وجود راهکارهای چند-ابری در بسیاری سازمان‌ها، یکپارچگی بین المان‌ها اهمیت ویژه‌ای خواهد داشت. مایکروسافت بعنوان یک ارائه‌کننده راهکارهای امنیتی انتها-به-انتها متعهد به امن‌سازی در سرتاسر زیرساخت‌ابری مشتریان است.

باتوجه به اهمیت حفاظت از داده‌ها، این موضوع یکی از بالاترین اولویت‌های همه سازمان‌ها است. فضای کاری هیبرید و تسریع در تحول دیجیتال منجر به افزایش حجم داده شده و نیاز به حفاظت و راهکارهای جامع افزایش یافته است. همین امر موجب شده بسیاری سازمان‌ها نیازمند تغییر استراتژی برای انطباق با شرایط جدید امنیت در جهان باشند.



شکل ۱- پنج چالش امنیتی سال ۲۰۲۲



شکل ۳- موضوعات امنیتی مورد علاقه سازمان‌ها در سال آتی

مطابق شکل ۲ اولویت‌های سرمایه‌گذاری پیشنهاد شده توسط رهبران امنیت طی ۱۲ ماه آتی به شرح زیر هستند:

- ۳۵% در امنیت ابری
- ۲۵% در امنیت داده
- ۲۴% مدیریت/ارزیابی آسیب‌پذیری
- ۲۳% امنیت اپلیکیشن (DevSecOps)
- ۲۲% امنیت شبکه مبتنی برابر

علاوه بر امنیت ابر و دیتا، آمارها حکایت از افزایش علاقه به سرمایه‌گذاری در ارزیابی و مدیریت آسیب‌پذیری‌ها به منظور الویت‌بندی تلاش‌های بازدارنده، دارد. فناوری‌های جدید مانند شناسایی و پاسخ توسعه‌یافته (XDR)، امنیت IoT[2] و OT[3] و در نهایت، لبه سرویس دسترسی امن (SASE[4]) بیش از پیش موردتوجه قرار گرفته‌اند. با استفاده از XDR، سازمان‌ها در اکوسیستم پیچیده خود بهتر قادر به شناسایی و پاسخ به تهدیدات خواهند بود. SASE نیز به مشتریان در امن‌سازی دسترسی به منابع در لبه شبکه با انعطاف و کنترل بیشتر کمک خواهد کرد.

لیست مطالعه برای سال ۲۰۲۲

با توجه به تلاش رهبران امنیتی برای کاهش تهدیدات، در آینده نزدیک تمرکز بر بردارهای تهدید با بیشترین میزان رشد مانند امنیت ابری، مدیریت دسترسی، باج‌افزارها، کارترکیبی افزایش خواهد داشت. مهم‌ترین عنوان گزارش‌شده در تحقیقات ما در تحول دیجیتال، تمرکز بر تحقق استراتژی اعتماد صفر است. با توجه به اینکه اعتمادصفر برای جلوگیری از حرکت جانبی مهاجمان طراحی شده است، این استراتژی به شدت در اولویت‌بندی و آدرس‌دهی سرمایه‌گذاری‌های متمرکز بر پیشگیری موثر خواهد بود. این استراتژی شامل غیرفعال کردن روش‌های احراز هویت قدیمی، برقراری دسترسی امن به منابع به کمک احراز هویت چندعاملی (MFA)، پیاده‌سازی کنترل‌های دسترسی مبتنی بر ریسک، استفاده از ابزارهای مدیریت وضعیت برای شناسایی و اصلاح ریسک‌ها در منابع ابری است. پیاده‌سازی این استراتژی به سازمان‌ها کمک خواهد کرد که یک فضای کاری هیبرید را امن‌تر پذیرفته و افراد، تجهیزات، اپلیکیشن‌ها، تجهیزات و داده‌های خود را محافظت کنند.

با انتقال داده‌ها به زیرساخت‌های ابری، رهبران امنیتی به دنبال یادگیری نحوه انطباق و یکپارچه‌سازی ابزارهای حفاظت از بارکاری، مدیریت دسترسی و مدیریت وضعیت، با استراتژی امنیت ابری خود خواهند بود. افزایش نگرانی‌ها نسبت به باج‌افزارها و امن‌سازی فضای کاری هیبرید و دورکاری سبب شده این دو نیز دومین اولویت سرمایه‌گذاری رهبران امنیت در سال آتی باشند.

شکل ۳ عناوینی که بیشترین علاقه‌مندی به آن‌ها وجود داشته را نشان می‌دهد که عبارتند از:

- اعتماد صفر ۴۳%
- امنیت ابری ۳۷%
- باج‌افزار و حفاظت از اخاذی سایبری ۲۸%
- امن‌سازی فضای کاری هیبرید و دورکاری ۲۴%
- یادگیری ماشین ۲۴%

دیدگاه مایکروسافت

با توجه به اینکه ارائه خدمات به مشتریان، اولویت اصلی مایکروسافت است، انجام نظرسنجی‌های ناشناس برای آشنایی با نظرات مشتریان ضروری خواهد بود. در پرسش از اغلب مشتریان سازمانی متوجه شدیم که مایکروسافت از دیدگاه مشتریان، در مقایسه با بسیاری از کمپانی‌های شناخته‌شده به عنوان یکی از سه کمپانی اصلی در صنایع امنیت IT رده‌بندی شده است. راه‌کارهای انتها-به-انتهای مایکروسافت با یک پوشش چند-ابری و چند-پلتفرمی عمیق، یک رویکرد حفاظتی جذاب برای مشتریان داشته است. البته مایکروسافت همچنان تلاش بیشتری خواهد داشت، چراکه موفقیت و حفاظت از مشتریان، اولویت اصلی و بنیادی در چشم‌انداز ماموریت آن شرکت است.

2- Internet of Things
3- Operation Technoloby
4- Secure Access Service Edge

همراه فناوری
fanavari hamrah
فصلنامه‌ی خبری تحلیلی
زمستان ۱۴۰۰ شماره‌ی چهارم

LockBit

باج‌افزاری موذی که حتی به سرورهای لینوکس هم حمله می‌کند

دنی پالمر گزارشگر ارشد امنیت سایت ZDNet گزارش می‌دهد که باج‌افزار LockBit یک باج‌افزار امنیتی است که سیستم عامل‌های ویندوزی را برای جرائم سایبری هدف قرار می‌دهد. به تازگی محققان امنیت سایبری نسخه جدیدی از آن را شناسایی کرده‌اند که Linux-ESXi نام داشته و به سرورهای لینوکس هم حمله می‌کند.

یکی از قوی‌ترین انواع باج‌افزارهایی که تاکنون سیستم‌عامل‌های ویندوزی را مورد حمله قرار می‌داد یک نسخه جدید که به لینوکس و VMware حمله می‌کند و در ماه‌های اخیر سازمان‌های بسیاری را هدف قرار داده، شناسایی شده است.

بر اساس تحلیل محققان شرکت Trend Micro، نسخه قفل‌کننده LockBit Linux ESXi 1.0 که در فروم‌های زیرزمینی در Dark Web در حال تبلیغ است، شناسایی شده است. این در حالی است که باج‌افزار LockBit که فعال‌ترین نوع خانواده باج‌افزارها در سال گذشته بود، تنها بر روی سیستم‌عامل‌های ویندوزی متمرکز بود.

LockBit به یکی از فریب‌کارترین انواع باج‌افزارها مشهور است. اکنون نسخه‌های آن که VMware و Linux را نیز مورد هدف قرار می‌دهند، معرفی و شناسایی شده‌اند که می‌توانند در سطح دنیا منتشر شده و فایل‌ها و سرورهای کاربران را آلوده کرده و شبیه هر باج‌افزاری کاربران قربانی را برای پرداخت مبالغی جهت رمزگشایی داده‌های رمز شده تحت فشار قرار دهد.

تحلیل‌گر ارشد امنیتی شرکت Trend Micro خانم جاسنتری دلا کروز معتقد است: «ارائه این نسخه جدید همراه و هم‌مسیر با گروه باج‌افزارهایی است که تلاش خود را به سمت رمزنگاری و حمله به میزبان‌های مبتنی بر لینوکس مانند سرورهای ESXi سوق داده‌اند.»

وی هم‌چنین می‌افزاید: «یک سرور ESXi نوعا میزبان چندین ماشین مجازی مختلف است که اغلب داده‌ها و خدمات مهم سازمانی را می‌تواند در بر داشته باشد. در نتیجه، موفقیت این نوع حمله و رمزنگاری توسط باج‌افزار، می‌تواند روی سرورهای ESXi تاثیری شگرف گذاشته و آسیبی بزرگ به کمپانی‌های هدف وارد کند.»

با هدف قرار دادن لینوکس، LockBit در واقع در مسیری مشابه با دیگر گروه باج‌افزارهای مشابه مانند REdvil و DarkSide طی کرده است، با این تفاوت که LockBit بسیار مشهورتر و رایج‌تر است و این به این معناست که حملات ناشی از این نوع باج‌افزار می‌تواند دایره بسیار گسترده‌تری از مخاطبان و کاربران سازمانی و غیرسازمانی را هدف قرار داده و تاثیر بسیار بیشتری در پی داشته باشد.

مشابه بسیاری حملات باج‌افزاری دیگر LockBit با سرقت اطلاعات از شبکه‌های در معرض خطر و تهدید به انتشار عمومی آن‌ها در صورت عدم پرداخت باج مورد انتظار از کاربران اخاذی می‌کند. در برخی موارد مقدار باج درخواستی تا چندین میلیون دلار نیز بالغ می‌شود.

محققان پیشنهاد می‌کنند که با توجه به آنکه شناسایی و مقابله با باج‌افزارها بر روی بستر لینوکس دشوارتر است، راه‌کار بهتر و ساده‌تر برای مقابله و جلوگیری از وقوع حملات باج‌افزاری در لینوکس، تنظیم پیکربندی‌ها، به‌روزرسانی وصله‌های امنیتی و ارتقای خط‌مشی‌های امنیتی به بهترین شکل برای مقابله با نفوذ آن‌ها در لایه شبکه و دسترسی خواهد بود

مشابه نسخه‌های قبلی LocBit، نسخه لینوکسی این باج‌افزار می‌کوشد تا با نمایش یک پیام به کاربر، او را تشویق به ارائه جزئیات اکانت سازمانی خود کند تا بدین وسیله باج‌افزار را هر چه بیشتر پخش کرده و سود بیشتری به دست آورد و حتی به کاربر پیشنهاد شراکت در سود نهایی را نیز می‌دهند. البته اینکه آیا می‌توان با تشویق نیروهای داخلی یک سازمان به افشای اطلاعات محرمانه و وعده کسب درآمد، آن‌ها را مجاب به این کار کرد، چندان مشخص نیست.

محققان پیشنهاد می‌کنند که با توجه به آنکه شناسایی و مقابله با باج‌افزارها بر روی بستر لینوکس دشوارتر است، راه‌کار بهتر و ساده‌تر برای مقابله و جلوگیری از وقوع حملات باج‌افزاری در لینوکس، تنظیم پیکربندی‌ها، به‌روزرسانی وصله‌های امنیتی و ارتقای خط‌مشی‌های امنیتی به بهترین شکل برای مقابله با نفوذ آن‌ها در لایه شبکه و دسترسی خواهد بود.

این کار شامل به روزرسانی سیستم‌ها با آخرین وصله‌های امنیتی ارائه شده به منظور جلوگیری از وقوع حملات است. خصوصا که LockBit به سوءاستفاده از نقاط ضعف سیستم‌ها و سرورها به منظور نفوذ و سوءاستفاده از آن‌ها معروف است. افرادی که مسئول انتشار این باج‌افزار هستند در سوءاستفاده از شناسه‌های کاربری و رمز عبورهای سرقت شده در دنیا شناخته می‌شوند. به همین جهت چون می‌دانیم یک شکاف داده‌ای لو رفته است، لازم است به هنگام بازیابی، کلمه عبور به روزرسانی شود تا از آن نشت اطلاعات جلوگیری شود.

همچنین در صورت نشت شناسه کاربری و کلمه عبور کاربران در یک نشت اطلاعاتی، استفاده از احراز هویت چندعاملی نیز می‌تواند یکی از مهم‌ترین و موثرترین راه‌کارها برای جلوگیری از حملات باج‌افزارها باشد تا بدین وسیله بتوان یک لایه دفاعی جدید در برابر حملات احتمالی مهاجمان مختلف ایجاد کنیم. ■

https://www.zdnet.com/article/this-sneaky-ransomware-is-now-targeting-linux-servers-too/

افزایش چشمگیر حملات فیشینگ با استفاده از افزونه‌های Excel XLL مایکروسافت

محققان امنیت‌سایبری هشدار داده‌اند که اخیرا چندین نوع بدافزار خاص به صورت مخفیانه از طریق فایل‌های Excel XLL مایکروسافت برای مخاطبان ارسال می‌شوند.

دنی پالمر گزارشگر ارشد امنیت در سایت ZDnet گزارش می‌دهد که طی ماه‌های اخیر موجی از حملات سایبری با سوءاستفاده از فایل‌های افزونه مایکروسافت اکسل به منظور ارسال چندین نوع بدافزار در کمپین‌های مختلف صورت گرفته است که می‌تواند کسب‌وکارها را در معرض خطر سرقت اطلاعات محرمانه، باج‌افزارها و سایر جرائم و حملات سایبری قرار دهد.

بر اساس جزئیات اعلامی از سوی محققان امنیتی HP Wolf، کمپین‌ها از افزونه مخرب مایکروسافت اکسل برای آلوده کردن سیستم‌ها استفاده می‌کنند و حملات سایبری از این طریق در بازه زمانی سه ماهه پایانی سال ۲۰۲۱ نسبت به مدت مشابه در سال گذشته آن تا ۶ برابر (۵۸۸%) افزایش داشته است.

فایل‌های افزونه XLL بسیار عمومی هستند، زیرا آن‌ها کاربران را قادر به استقرار یک دایره متنوع از ابزارها و توابع اضافی در مایکروسافت اکسل می‌نمایند. اما مشابه ماکروها، آن‌ها ابزارهایی هستند که ممکن است توسط مهاجمان برای حمله و آسیب به کار گرفته شوند.

حملات از طریق ارسال ایمیل‌های فیشینگ بر اساس مراجع پرداخت، صورت‌حساب‌ها، پیشنهادات قیمت، مستندات حمل و نقل بار و سفارش‌های تجاری صورت گرفته و همراه با مستندات اکسل مخرب دارای فایل‌های افزونه XLL توزیع می‌شود. اجرای فایل‌های مخرب کاربر را به نصب و فعال‌سازی افزونه تشویق و اجبار می‌کند، که به صورت مخفیانه یک بدافزار را بر روی دستگاه مقصد نصب می‌کند.

خانواده‌های بدافزار که با استفاده از فایل‌های افزونه XLL جابجا شده و توزیع می‌شوند شامل Dridex, IcedID, BazaLoader, Agent Tesla, Raccoon Stealer, Formbook, و Bitrat می‌باشند. بسیاری از این انواع بدافزارها، می‌توانند راه نفوذی به سیستم‌های کامپیوتری مبتنی بر ویندز ایجاد کند که به مهاجمان امکان دسترسی از راه دور به ماشین‌ها، مانیتور کردن فعالیت‌های کاربر و سرقت داده‌ها را می‌دهد.

محققان همچنین هشدار می‌دهند که حفره‌های نفوذ حاصل از نصب یک بدافزار بر روی کامپیوتر کاربران می‌تواند راه نفوذ و نصب بدافزارهای دیگر مانند باج‌افزارها را برای مهاجمان باز کند. به عبارتی حملات XLL می‌تواند به عنوان ابزاری برای رمزنگاری شبکه‌ها و تقاضای پرداخت باج‌های بزرگ استفاده شود.

این حملات XLL می‌تواند در سوءاستفاده از منابع قربانیان به کار گرفته شوند و بعضا اطلاعات به‌دست آمده از ایشان ممکن است که در شبکه‌های زیرزمینی Dark Web به فروش برسند.

برخی از مهاجمان به واسطه XLL برای سرویس‌های خودارقامی تا ۲۰۰۰ دلار پیشنهاد می‌دهند که با وجود بالا بودن برای کاربران فروم‌های مجرمانه جذاب بنظر می‌آید.

علاوه بر کمپین‌های مبتنی بر XLL، محققان هشدار داده‌اند که QakBot که یک فرم خاص از بدافزارهای تروجان است و اغلب به عنوان یک عامل بسترسازی برای حملات باج افزاری به کار می‌رود، نیز ممکن است از اکسل برای آسیب به قربانیان استفاده کند.

مهاجمانی که رشته ایمیل‌های یک کاربر را به منظور ارسال مستندات اکسل مخرب به قربانیان خود به سرقت می‌برند، معمولا یک فایل زیپ شده حاوی یک فایل باینری مایکروسافت اکسل (XLSB) برای قربانی ارسال می‌کنند. اگر کاربر این فایل را اجرا کند یک QakBot بر روی ماشین کاربر نصب خواهد شد.

الکس هلند، تحلیل گر ارشد مجموعه امنیتی HP Wolf می‌گوید: «سوءاستفاده از خصوصیات نرم‌افزارهای رایج برای پنهان کردن بدافزارهای مخرب از تاکتیک‌های مهاجمان است، که در این روش از انواع غیررایج فایل‌ها که ممکن است در دروازه‌های ایمیل مجاز به ارسال باشند، استفاده

می‌شود. تیم‌های امنیت باید مراقب باشند که تنها به الگوریتم‌های شناسایی فایل‌ها و عوامل مخرب کنونی خود اعتماد نکرده و همواره خود را بر اساس اطلاعات آخرین تهدیدات و روش‌های دفاع و مقابله با آن‌ها به روزرسانی کنند.»
او هم چنین اضافه می کند: «مهاجمان به صورت پیوسته از روش‌های نوین و خلاقانه‌ای استفاده می کنند تا از کشف حملات خود فرار کنند، لذا بسیار حیاتی است که کسب‌وکارها سیستم‌های دفاعی خود را برای مقابله با حملات و تهدیدات جدید بر اساس چشم‌انداز حملات احتمالی و نیازهای کسب‌وکار و مشتریان خود برنامه‌ریزی و تنظیم کنند. عاملان مهاجم در زمینه تکنیک‌های حمله به کاربران از قبیل سرقت رشته ایمیل، سرمایه‌گذاری‌های چشم‌گیری داشته‌اند که مقابله با آن‌ها و شناسایی کاربران دوست و دشمن را برای کاربران دشوارتر از گذشته می کند.»

به منظور جلوگیری از گرفتار شدن در دام حملات ناشی از سوءاستفاده از فایل‌های XLL پیشنهاد می‌شود که مدیران سیستم دروازه‌های ایمیل ورودی را به گونه‌ای پیکربندی کنند که از ورود کلیه ایمیل‌هایی که شامل فایل‌هایی با پسوند .xll باشند ممانعت کرده و تنها اجازه تحویل افزونه‌هایی را بدهند که از شرکای معتبر و مطمئن ارسال شده‌اند و حتی پیشنهاد می‌شود که افزونه‌های اکسل به طور کامل غیرفعال شوند.

۵ روند امنیت سایبری سال ۲۰۲۲ که باید مراقبش باشیم

هیچکس نمی‌توانست هرج و مرج آشکاری را که صنعت امنیت سایبری در طول سال ۲۰۲۱ تجربه کرد، پیش‌بینی کند. تعداد بی‌سابقه‌ای از حملات باج‌افزاری، خرابی زنجیره تامین SolarWinds و اخیراً کشف Log4j توسط گیمرهای Minecraft. همه اینها یک سال پیش برای زندگی واقعی بیش از حد بزرگ و غیرعادی به نظر می‌رسید.

پیش‌بینی‌ها در مورد سال پیش رو با توجه به ۱۲ ماه گذشته جسورانه به نظر می‌رسند، بنابراین فهرستی از پنج روند برتر که باید در سال ۲۰۲۲ مراقب آن‌ها باشیم به این ترتیب معرفی شده است.

علاقه رو به رشدی برای نفوذ به زیرساخت‌های دولتی و امنیت سایبری وجود خواهد داشت

SolarWinds، حمله‌ای که به شرکت خط لوله ساحل شرقی ایالات متحده (Colonial Pipeline) صورت گرفت، به نگرانی‌ها در ارتباط با نرم‌افزارهای جاسوسی و لزوم حفظ حریم خصوصی دامن زده و توجه دولت‌ها را در سرتاسر جهان به خود جلب کرده است؛ به نحوی که کارشناسان بر این باورند که سال پیش رو پر از قانون‌گذاری‌های نظارتی و کنترلی و سرمایه‌گذاری‌های امنیتی جدید خواهد بود.

در ماه‌های منتهی به انتخابات ۲۰۲۰ آمریکا در پی حملات سایبری گسترده به زیرساخت‌های حیاتی، تعداد درخواست‌های فوری از سازمان امنیت ملی آمریکا برای مقابله با حملات سایبری بالا گرفت. محققان پیش‌بینی می‌کنند که این تهدیدات سایبری سریع و گسترده در طول سال ۲۰۲۲ متمرکز بر دولت‌ها و زیرساخت‌های دولتی خواهد بود.

در پاسخ به دستور صادر شده ماه مه ۲۰۲۱ توسط رئیس جمهور آمریکا بایدن، Reiber پیش‌بینی کرده است که پیشنهادات استقرار معماری اعتماد صفر و عملیاتی‌سازی این معماری در زیرساخت‌های ارزشمند سازمان‌های دولتی در نیمه اول سال ۲۰۲۲ اجرایی خواهند شد.

هرقدر که استقرار این قبیل مدل‌های امنیتی در سازمان‌های دولتی بیشتر محقق گردد، سازمان‌های خصوصی نیز در پیروی از سازمان‌های دولتی بیشتر به سمت آن حرکت کرده و آن را مستقر خواهند کرد. پیش‌بینی می‌شود در

بده‌بستانی که برای تحقق این مدل‌ها و سرمایه‌گذاری در حوزه تضمین حریم خصوصی وجود خواهد داشت، سازمان‌ها برای حفظ اعتبار و خوش‌نامی خود در بین مشتریان و حفظ مشتریان فعلی خود سرمایه‌گذاری بیشتری در حوزه استقرار استراتژی‌های اعتماد صفر انجام خواهند داد.

مهندسی اجتماعی همچنان پابرجاست

مردم همچنان در سال ۲۰۲۲ هم انسان‌هایی خواهند بود که تا حد زیادی در انجام ساده‌ترین کارهای مجازی مورد سواستفاده قرار می‌گیرند و یا بدون در نظر گرفتن تأثیر هر اقدام بر وضعیت امنیتی سازمان، به این اقدامات مبادرت می‌ورزند و این چیزی است که مجرمان سایبری همچنان روی آن حساب می‌کنند تا کلاهبرداری‌های خود را به شیوه مهندسی اجتماعی عملی کنند.

مایک ویاکک از شرکت مشاوره امنیت Stairwell درباره چالش‌های امنیتی سال ۲۰۲۲ می‌گوید: «ما معتقدیم در سال پیش‌رو مهندسی اجتماعی همچنان به کار خود ادامه خواهد داد. مهندسی اجتماعی یکی از دشوارترین مسائل امنیتی است که باید به آن پرداخته شود، زیرا هیچ‌گونه انطباق با قوانین رگولاتوری، حاکمیت داده‌ای، یا اقدام مدیریت ریسکی نمی‌تواند این واقعیت را که انسان‌ها مستعد فریب خوردن هستند برطرف کند».

امنیت سایبری مشکلی است که همه مسئول آن هستند، اما تعداد کمی درک می‌کنند که اقدامات فردی آن‌ها چقدر ممکن است باعث آسیب شود. افرادی که در شرایط عادی بسیار جدی هستند در طول فرآیند کاری خود ممکن است که کم‌توجه و حواس پرت باشند که همین امر راه را برای نفوذ و آسیب به منافع افراد و سازمان‌ها باز خواهد گذاشت.

در این بین جیسون هونیش، معاونت سرویس و هوشیاری امنیتی مجموعه Arctic Wolf پیشنهاد داده است که دوره‌های آموزشی موثری برای تسلط کارکنان به موضوعات حوزه مهندسی اجتماعی برگزار شود تا آن‌ها را در برابر حملات احتمالی این حوزه آگاه کند. به جای استفاده از رویکردهای قدیمی هشدار باید از پیام‌های کوتاه که به سادگی قابل هضم و بهره‌برداری و یادگیری باشند، استفاده شود.

زنجیره تامین، باج‌افزاری جدید است

یان مک‌شین، مدیر ارشد فناوری در Arctic Wolf می‌گوید که امسال، صنایع مختلف نگاه خود را نسبت به باج‌افزار تغییر داده و به مرور خواهند فهمید که مشکل خود باج‌افزارها نیستند، بلکه نقطه ورود آن‌ها به سیستم، مساله خواهد بود. مک‌شین افزود: ما رویه خود را تغییر داده‌ایم تا به جای تمرکز بیشتر بر روی کارهایی که باید بعد از حمله انجام دهیم، تغییر جهت داده و بر نحوه پیش‌بینی و محافظت از خط اول حمله تمرکز کنیم. برای این منظور از علوم داده برای مدل‌سازی سناریوهایی استفاده می‌کنیم که می‌تواند ضعف‌های بالقوه در زنجیره تأمین را شناسایی و برجسته کند. این موضوع تنها با شفافیت و افشای بیشتر داده‌ها امکان‌پذیر خواهد شد.

بازیگران باج‌افزارها به‌عنوان سرویس به سمت کسب‌وکارهای کوچک و متوسط می‌روند

باج‌افزار به عنوان سرویس[1] منجر به تبدیل اخاذی دیجیتال به یک تجارت پررونق شده است و احتمالاً سال ۲۰۲۲ سال دیگری برای بازیگران تهدید باج‌افزار خواهد بود.

مک‌شین می‌گوید: کاملاً مشخص شده است که مهاجمان سایبری بین اهداف خود براساس اندازه آن‌ها تبعیض قائل نمی‌شوند. کسب‌وکارهای کوچک و متوسط هم به اندازه شرکت‌های بزرگ برای مواردی مانند حملات باج‌افزار اهداف سودآوری به شمار می‌آیند.

در شرایطی که دولت و شرکت‌های بزرگ پول نقد را به امنیت سایبری سرازیر می‌کنند، شرکت‌های کوچک و متوسط با کمبود بودجه و کارکنان کم‌کار، اهداف اصلی گروه‌های باج‌افزار خواهند بود.

صنعت امنیت سایبری در سال ۲۰۲۲ به هماهنگی بهتری نیاز دارد

تجربه سال‌های گذشته، نشان می‌دهد که رفع تهدیدات و حملات امنیتی نیازمند حل مشکلات هماهنگی وانعطاف‌پذیری بیشتری در بین تیم‌های مقابله با تهدیدات امنیتی است.

به اعتقاد مک‌شین، همانطور که در بدافزار به‌عنوان سرویس و فیشینگ دیده‌ایم، عوامل تهدید حاضرند که برای موفقیت باهم متحد شوند.

او خاطرنشان کرد: «مثلا پس از اینکه Emotet توسط مجریان قانون در ژانویه حذف شد، TrickBot شروع به کاشت مجدد عفونت‌های Emotet و کمک به بازگرداندن آن‌ها کرد.»

به گفته مک‌شین، وقتی نوبت به جامعه امنیت سایبری می‌رسد، باید کارهای بیشتری برای تقویت کل اکوسیستم انجام شود. این بدان معناست که شرکت‌های بزرگ‌تر باید ابزارها و استعدادهای خود را با کسب‌وکارهای کوچک ومتوسط و بدون منابع، با هدف محافظت از کل اکوسیستم به اشتراک بگذارند.■

منبع

https://threatpost.com/5-cybersecurity-trends-2022/177273/

1- Ransomware-as-a-service (RaaS)

روند بازار امنیت سایبری- مکنزی ۲۰۲۲

۲۱ درصد
رقم پیش بینی شده در رشد سالانه قراردادهای بیمه مستقیم حملات سایبری تا سال ۲۰۲۵

۳,۵ میلیون
رقم فرصت های شغلی خالی در حوزه امنیت سایبری در سراسر جهان

۸۵ درصد
رقم افزایش هزینه های امنیت سایبری در شرکتهای کوچک و متوسط تا سال ۲۰۲۳

۱۵ درصد
رقم افزایش سالانه هزینه های مرتبط با جرایم سایبری و بالغ شدن بر ۱۰,۵ تریلیون دلار تا سال ۲۰۲۵

۱۰۱,۵ میلیارد
رقم صرف شده در حوزه ارائه دهندگان خدمات امنیت سایبری تا سال ۲۰۲۵

چشم انداز امنیت GSMA 2021

- کدنویسی امن برای API و توسعه NFV
- فناوری ابر و مجازی سازی
- توسعه و نگهداری از گزارش های مواد نرم‌افزاری (SBOM ها) و مدیریت آسیب‌پذیری های مربوطه
- مهندسی نرم افزار امن
- علوم داده برای پیاده سازی هوش مصنوعی
- دانش پیرامون شبکه قدیمی و پروتکل ها

همراه اول

زیست بوم(اکوسیستم) امنیت فناوری اطلاعات وارتباطات

شرکت نامدار

نهادهای حاکمیتی

وزارت ارتباطات و فناوری اطلاعات

مرکز افتا ریاست جمهوری

سهامدار عمده : شرکت ارتباطات سیار ایران (همراه اول)

پیمان کاران :
شرکت های فن آور امنیت اطلاعات و ارتباطات و شرکت های دانش بنیان

تامین کنندگان :
شرکت های معتبر داخلی

فرآیندهای مدیریتی
فرآیند تامین و توسعه منابع مالی - فرآیند تامین وتدارکات
فرآیند پشتیبانی زیرساخت داخلی
فرآیند مدیریت مستندات- فرآیند تامین و توسعه منابع

فرآیندهای اصلی
فرآیند توسعه کسب و کار - فرآیند مدیریت مشتریان
فرآیند تداوم خدمت - فرآیند مدیریت پروژه
فرآیند مدیریت امنیت اطلاعات - فرآیند ارائه خدمت

فرآیندهای پشتیبانی
فرآیند پایش و بهبود
فرآیند راهبری

- شرکت های تابعه همراه اول
- شرکت های تابعه نامدار
- سازمان ها و نهادهای دولتی
- موسسات مالی و بانک ها
- شرکت های خصوصی

پرتفوی محصولات و خدمات شرکت نامدار

شرکت جدید
ارائه خدمات برای امنیت Xaas(B2B)

یافتار
پردازش هوشمند محتوا و توسعه تجهیزات پهن باند

عماد
ارزیابی امنیت و آزمون نفوذ

هویتا
احراز هویت الکترونیکی

آزمایشگاه مرجع
اصالت سنجی و صدور گواهینامه

امن افزار
ارائه راهکارهای امنیت

تولید محصولات امنیت

درسا
تولید محتوا

راهنمای مطالب ارسالی به فصلنامه فناوری همراه

نشریه فناوری همراه، مطالب دریافتی را در چهار بخش رصد فناوری، ابزار فناوری، اخبار فناوری و بینش فناوری پذیرش کرده و منتشر می‌کند. انتظار می‌رود در بخش **رصد فناوری**، مقالات و گزارش‌های ترویجی پیرامون فناوری‌های نوظهور، کاربست‌ها، ورتیکال‌ها و رهیافت‌های نوین فناورانه دریافت شود.

در بخش **ابزار فناوری** به معرفی نهادها، کنفرانس‌ها، نمایشگاه‌ها، وبسایت‌های آموزشی و... پرداخته می‌شود.

در بخش **اخبار فناوری** آخرین اخبار و تحلیل‌های مربوط به صنعت ICT جهان در حوزه سرمایه‌گذاری‌ها، توسعه محصولات، لانچ‌ها و... به چاپ خواهد رسید. بخش **بینش فناوری** نیز به معرفی و تحلیل فرآیندهایی مانند جریان‌های تحقیق و توسعه فناوری، انتقال فناوری، همکاری‌های فناورانه و برنامه‌ریزی‌های راهبردی در حوزه فناوری‌های جدید تلکام می‌پردازد.

ویژگی‌های مطلب ارسالی

- به ازای هر ۵۰۰ کلمه یک سوتیتر مناسب ارائه شود (۳۰ الی ۸۰ کلمه)؛
- برای هر گزارش حداقل ۳ منبع به روز (بعد از ۲۰۱۹) استفاده شود (در صورتی که منبعی اعتبار بالایی داشته باشد با تأیید دبیر کمیته تخصصی یک منبع کافی است؛ همچنین اگر منبعی از اعتبار بالا برخوردار بوده ولی مربوط به قبل از ۲۰۱۹ باشد، قابل قبول است)؛
- بازه زمانی اخبار و تحلیل حداکثر برای ۱ ماه گذشته باشد؛

ترتیب عناوین مقالات و گزارش‌ها

مقالات به طور دقیق شامل این عناوین باشد: چکیده، کلیدواژه‌ها، مقدمه، بدنه اصلی، نتیجه‌گیری، معرفی منابع.

- چکیده فارسی شامل گزیده‌ای از مطلب بوده و به روند مقاله از ابتدا تا نتایج اشاره دارد. چکیده مقاله، نباید کمتر از ۱۵۰ کلمه و بیشتر از ۲۵۰ کلمه باشد.
- در قسمت کلیدواژه‌ها باید حداقل ۳ و حداکثر ۵ واژه بوده که با کاما (،) از هم جدا شده و در یک خط و به ترتیب اهمیت‌شان آورده شود.
- در قسمت مقدمه به صورت کوتاه به موضوع و اهمیت آن اشاره کرده و ذهن خواننده را برای ورود به بدنه اصلی گزارش آماده کنید.
- در قسمت بدنه اصلی گزارش نتیجه رصد فناوری که در حوزه تخصصی خود انجام داده‌اید را با لحنی ساده و روان ارائه دهید.
- در قسمت نتیجه‌گیری، نتیجه گزارش از زبان نویسنده بیان گردد (۱۰۰ الی ۲۰۰ کلمه).
- منابع به ترتیب حروف الفبا و بر اساس یکی از سبک‌های معتبر رفرنس‌دهی در پایان گزارش ارائه شود.

ترتیب مطلب اخبار، ابزار و تحلیل‌ها

این نوع از مطالب به طور دقیق شامل این تیترها باشد: بدنه اصلی و منابع.

- در قسمت بدنه اصلی متن را با لحنی ساده و روان ارائه دهید.
- منابع به ترتیب حروف الفبا و بر اساس یکی از سبک‌های معتبر رفرنس‌دهی در پایان ارائه شود.

فونت

متن اصلی به صورت تک‌ستونی با قلم (فونت) B Mitra و اندازهٔ pt. ۱۴ و عناوین بخش‌ها با همین قلم و به صورت بولد تایپ شود.

حجم

- حجم مقالات بین ۱۴۰۰ الی ۲۰۰۰ کلمه باشد؛ (شامل چکیده ۱۵۰ الی ۲۵۰؛ سوتیتر ۳۰ الی ۸۰؛ نتیجه‌گیری ۱۰۰ الی ۲۰۰ و بقیه بدنه اصلی گزارش)
- حجم اخبار، ابزار و تحلیل‌ها بین ۵۰۰ الی ۱۰۰۰ کلمه باشد.

تصاویر و جداول

لازم است تصاویر مرتبط با مطلب با کیفیت بالا ارائه شده و به ترتیب به صورت شکل ۱، شکل ۲ و... شماره‌گذاری شوند.

همچنین لازم است جداول به زبان فارسی بوده و از گذاشتن جداول به صورت عکس و با زبان انگلیسی خودداری شود. جداول باید به ترتیب به صورت جدول ۱، جدول ۲ و... شماره‌گذاری شده و در نخستین مکان ممکن پس از اولین اشاره در متن قرار گیرند.

ارزیابی محتواهای ارسالی از منظر ۳ پارامتر زیر انجام خواهد شد:

- کیفیت کلی محتوا (بروز بودن، رعایت رویکرد دیده‌بانی، جذابیت و ...)؛
- رعایت اصول نگارشی فصلنامه (داشتن بخش چکیده و نتیجه‌گیری، رعایت استاندارد ۱۴۰۰ الی ۲۰۰۰ کلمه، رعایت فونت‌ها، نکات ویرایشی، فونت‌نوت و ...)؛
- کیفیت ترجمه (سلیس و روان بودن با رعایت امانت در انتقال محتوا)؛
- امتیاز نهایی پس از داوری ارزیابان فنی محتواها، عددی بین ۰ تا ۱۰۰ خواهد بود که در قالب جدول زیر انجام می‌شود:

ردیف	بازه امتیازات	سطح	وضعیت
۱	۷۶ الی ۱۰۰	A	تأیید برای انتشار
۲	۵۱ الی ۷۵	B	تأیید برای انتشار
۳	۲۱ الی ۵۰	C	رد و انتشار در صورت وجود ظرفیت
۴	۰ الی ۲۰	D	رد

لازم است جداول زیر برای مقالات ارسالی بخش رصد فناوری تکمیل شود.

نام و نام خانوادگی:

رشته تحصیلی: مدرک تحصیلی:

دانشگاه: شغل:

جایگاه سازمانی:

سابقه‌ای کوتاه (رزومه علمی و تخصصی):

محل درج تصویر

جدول ۱- مشخصات نویسنده

ارتباط موضوع با فعالیت‌های فعلی همراه اول

☐ کم ☐ متوسط ☐ زیاد ☐ کاملا منطبق

قابلیت فناوری در ایجاد تحول در کسب‌وکار

☐ کم ☐ متوسط ☐ زیاد ☐ متحول کننده

فاز توسعه فناوری

☐ حضور کامل در بازار ☐ آماده‌سازی بازار

☐ محصول مفهومی و اولیه ☐ تحقیقات کاربردی و پایه

اقدام پیشنهادی برای همراه اول

☐ اصلا ورود نکند

☐ به رصد تحولات مربوطه بپردازد

☐ جهت ورود، آمادگی کسب کند

☐ نیاز به اقدام فوری است

جدول ۲- مشخصات فناوری رصد شده

مرکز تحقیق و توسعه
همراه اول

همراه اول

فـراخـوان رصـد فناوری

مـزایـای شـرکت در فـراخـوان

چاپ محتوای ارسالی در فصلنامه «فناوری همراه»
اعطای جوایز نقدی

جهت ثبت‌نام و کسب اطلاعـات بیشتر به نشـانی
https://mci.ir/web/rd/tech-scouting مراجعه نمایید.

اسکن کنید