



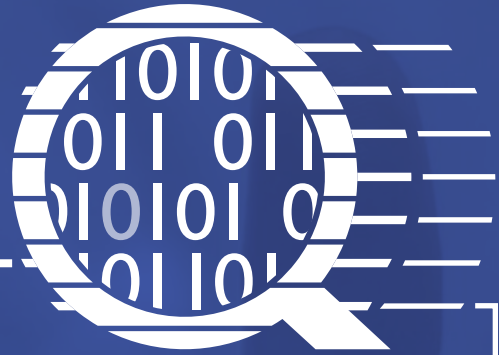
آشنایی با مراکز عملیات امنیت



شناخت
هوش تهدید سایبری

فرصت‌ها و
تهدیدهای نئوبانک‌ها

امنیت باید به
کسب و کار بانکی گره بخورد



چشم انداز

معتمدترین مرجع و عامل پیشران
در ارتقای امنیت، پایداری و تاب‌آوری در
زیست بوم تولید و تبادل اطلاعات بانکی

کاشف

مدیریت امن الکترونیکی
(سهامی خاص)

مأموریت

رگولاتوری امنیت، رسیدگی به رخدادها، تعاملات هدفمند و به
اشتراک‌گذاری دانش در زیست‌بوم تولید و تبادل اطلاعات بانکی
به‌منظور مقابله هوشمند با تهدیدات و مخاطرات سایبری و مالی

راهبردهای اصلی



تقویت همکاری‌های عملیاتی، تعاملاتی،
اشتراک‌گذاری و تحلیل اطلاعات



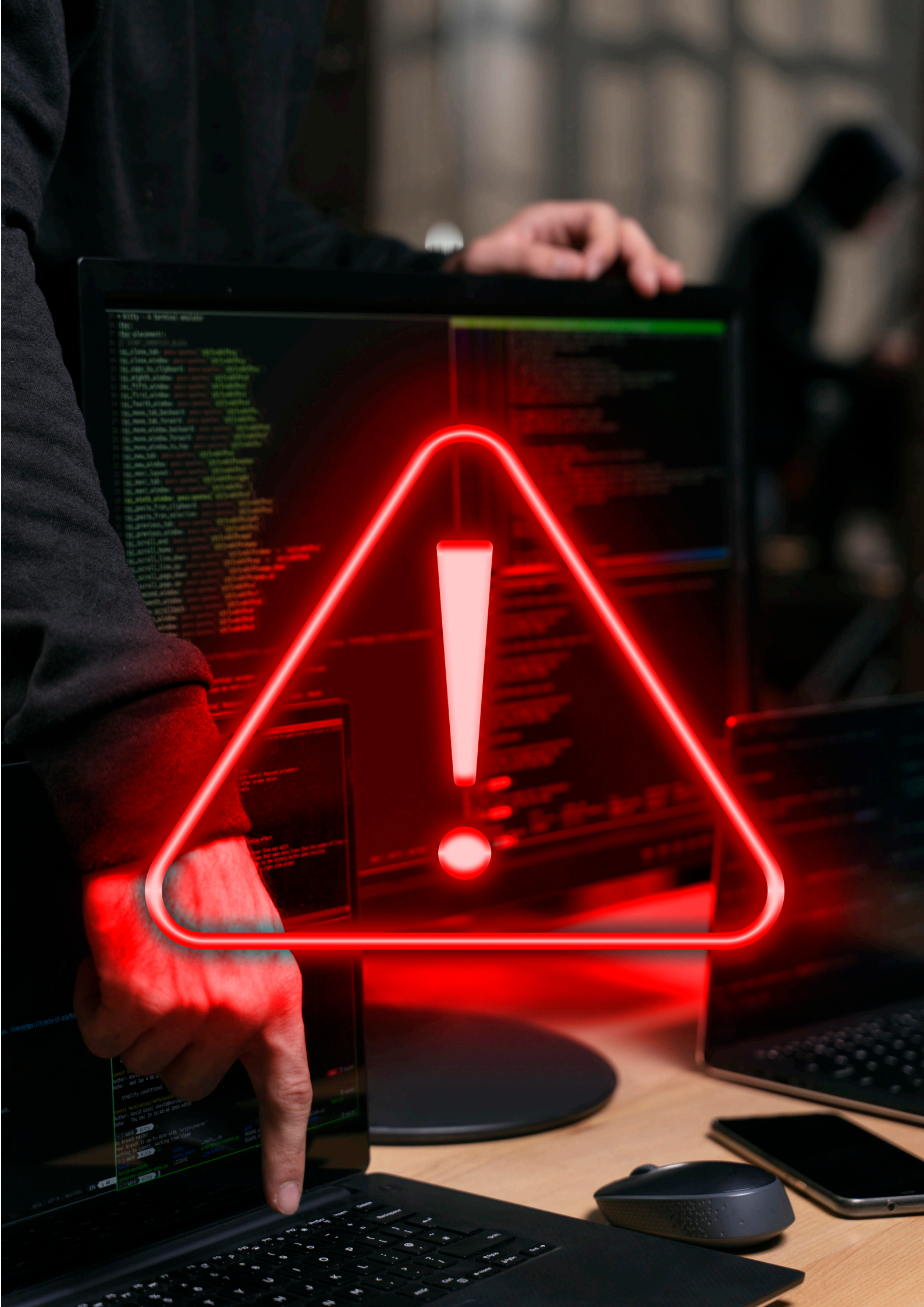
ارتقاء حکمرانی امنیت اطلاعات،
مدیریت مخاطرات و تطابق‌پذیری

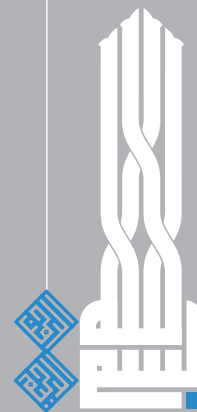


تقویت اعتماد حاکمیت، ذینفعان و
بازیگران حوزه بانکی



ارتقاء توانمندی شناسایی و
پاسخگویی به تهدیدها و رخدادها





فهرست

سرمقاله

۵ کاشف، بازیگر مهم نسل چهارم بانکداری

گفت و گو

۷ باید میان سرعت فناوری و امنیت توازن برقرار کنیم

۱۰ هوش مصنوعی ظرفیت انجام جرائم سایبری را به شدت افزایش می‌دهد

۱۳ امنیت باید به کسب و کار بانکی گره بخورد

۱۷ آشنایی با سامانه سرآمد

زیرساخت

۱۹ نظام، جایگاه معماری و انواع مراکز عملیات امنیت

۲۵ آشنایی با هوش تهدید سایبری

مورد کاوی

۳۵ سیر تکامل امنیت سایبری در بانکداری

۳۹ احراز هویت صوتی، گامی برای افزایش امنیت

۴۱ زمین بازی تغییر خواهد کرد

۴۳ آشنایی با سامانه رادار

۴۴ فرصت‌ها و تهدیدهای نئوبانک‌ها

راهکار

۴۹ در نقش مشاور کنار بانک‌ها ایستاده‌ایم

۵۲ مدیریت عملکرد با متد OKR و اهمیت آن در افزایش بهره‌وری نیروی انسانی

۵۴ هدف ما رسیدگی مستمر به رخدادهای بانکی است

۵۷ آشنایی با سامانه رسا

۵۸ سامانه‌هایی که از درون نیازها سر برمی‌آورند

۶۱ بزرگ‌ترین چالش امنیت کمبود نیروی انسانی است

۶۴ آشنایی با سامانه پاسبانک

۶۵ اهداف کلان کاشف

۶۶ شناخت مدل‌های مرجع CERT / CSIRT



کتاب سال امنیت فا و
سال دوازدهم-دوره جدید
۱۴۰۲

صاحب امتیاز:

موسسه فرهنگی هنری دیده بان ایما تدبیر

مدیر مسئول و سردبیر

علیرضا صالحی درجزینی

با تشکر از همکاری

مهران محرمیان، امین مهاجر،
حسین قرایی، میثم نجار، فریا
یاراحمدی، سارا دلیریان

ویراستاری و آماده سازی:

دیده بان

لیتوگرافی و چاپ: سینا

نشانی

سهروردی شمالی، حاج حسنی
پلاک ۵۵ طبقه اول

تلفن: ۸۸۷۴۹۴۱۰

www.didehban.com

info@didehban.com

مدیرعامل

کاشف، بازیگر مهم نسل چهارم بانکداری

شرکت کاشف در دهمین سال فعالیت خود، با تمرکز بر توسعه هرچه بیشتر سامانه‌ها و خدماتی که ارائه می‌کرده است، طی یک سال گذشته؛ با تلاش و همکاری مدیران و همکاران، برنامه‌های جدیدی را در راستای تحقق اهداف و انتظارات بانک مرکزی تدوین نموده است. این برنامه‌ها شامل ارتقاء حکمرانی امنیت اطلاعات، مدیریت مخاطرات و تطابق پذیری، ارتقاء توانمندی شناسایی و پاسخگویی به تهدیدها و رخدادها، تقویت همکاری‌های عملیاتی و تحلیل اطلاعات و در نهایت تقویت اعتماد حاکمیت، ذینفعان و بازیگران حوزه بانکی است.

از جمله دستاوردهای قابل اشاره، دریافت مجوز راه‌اندازی اپراتور امنیت و مرکز MSSP، اخذ مجوز دانش بنیان و دریافت مجوز آزمایشگاه ارزیابی امنیتی از افتای ریاست جمهوری است. این اقدامات در جهت ارتقای جایگاه کاشف در زیست‌بوم امنیت اطلاعات کشور صورت گرفته است. در واقع چشم‌انداز ما در کاشف تبدیل شدن به معتمدترین مرجع و عامل پیشران در ارتقای امنیت، پایداری و تاب‌آوری در زیست‌بوم تولید و تبادل اطلاعات بانکی است.

راه‌اندازی و عملیاتی نمودن آزمایشگاه کاشف و انجام بیش از هفتاد آزمون و ارزیابی در حوزه‌های وب، شبکه، برنامه‌های موبایل، برنامه‌های نماد و گواهی امضاء دیجیتال از جمله طرح‌هایی است که با تلاش مستمر همکاران به بار نشسته و توانسته یکی از نیازهای حیاتی این حوزه را رفع کند.

ارائه خدمات امنیت فناوری اطلاعات به شبکه بانکی و صرافی‌ها که ذیل موضوع اپراتور امنیت در کاشف شروع شده، می‌تواند سرآغاز جدیدی برای ارائه چنین خدماتی در کشور باشد. با توجه به آنکه در حال حاضر خدمات MSSP گسترش نیافته و فرهنگ استفاده از آن ایجاد نشده است، شروع چنین فعالیتی ریسک‌ها و مخاطرات خاص خود را دارد. کاشف با علم به این نکات، خدمت‌رسانی به‌عنوان اپراتور امنیت را شروع کرده است.

شبکه‌های بانکی به‌عنوان یکی از حساس‌ترین و مهم‌ترین سامانه‌های اطلاعاتی کشور، به‌طور خاص یکی از اهداف اصلی بسیاری از حملات امنیتی است. جا دارد که اینجا به برخی از سرویس‌های مهم MSSP اشاره کنیم.

پایش و تشخیص تهدیدات را می‌توان یکی از نقاط کلیدی این خدمت دانست. کاشف با کمک ابزارها و سامانه‌های پیشرفته مانیتورینگ، ترافیک شبکه، رویدادها و فعالیت‌های غیرمعمول را به‌دقت نظارت می‌کند و به شناسایی سریع حملات و تهدیدات امنیتی کمک می‌نماید. پس از آن پاسخگویی سریع به حملات اهمیت دارد تا استمرار فعالیت بانکی تضمین شود.

مدیریت ریسک برای بانک‌ها و صرافی‌ها، مدیریت ریسک امنیتی از اهمیت بسیاری برخوردار است که کاشف به‌عنوان سرویس‌دهنده MSSP با راهکارهایی برای شناسایی، ارزیابی و مدیریت ریسک‌های امنیتی کمک می‌کند تا بانک‌ها بهبود پایداری و امنیت خود را حفظ کنند.

پایایی و قابلیت اطمینان، استمرار کسب‌وکار و حفظ و بهبود مستمر سامانه‌ها به لحاظ حفظ امنیت، اهمیت این خدمت را نشان می‌دهد.

نکته دیگری که کاشف بر اجرای آن سعی وافر دارد، فرهنگ‌سازی و توسعه دانش و آگاهی در حوزه امنیت اطلاعات است. انجام این امر نیز با راه‌اندازی آکادمی امنیت بانکی در کاشف شروع شده است. در آکادمی امنیت علاوه بر ارتقای دانش و آگاهی در حوزه امنیت، تلاش خواهد شد تا تمام توانمندی‌های عملی و کاربردی در این حوزه در اختیار متخصصان و فراگیران قرار گیرد.

کاشف، همه آنچه گفته شد را در کنار انجام فعالیت‌های مستمر در زمینه شناخت ناهنجاری‌های مالی، کشف تقلب، کشف درگاه‌های قمار، مسدودسازی کارت‌ها و درگاه‌های غیرمجاز و همکاری با مرکز مدیریت راهبردی افتا، قوه قضاییه و پدافند غیرعامل به‌طور دائمی به‌عنوان می‌رساند تا همچنان به‌عنوان بازوی فعال بانک مرکزی نقش خود را ایفا نماید.

■ ویژه‌نامه امنیت بانکداری ■ زمستان ۱۴۰۲ ■

گفت‌وگو





باید میان سرعت فناوری و امنیت توازن برقرار کنیم

رفع مشکلات امنیتی با تکیه بر توانمندی‌ها ممکن است و توانمندی از برآیند نیروی انسانی، فناوری و فرایند حاصل می‌شود. لذا پیشرفت فناوری، به نوبه خود باعث بهبود توانمندی در پاسخ به نیازهای امنیتی محسوب می‌شود. مهران محرمیان، معاون فناوری‌های نوین بانک مرکزی، از فرصت‌ها و تهدیدهای فناوری برای امنیت بانکی می‌گوید.

امروزه پایه و اساس بسیاری از فعالیت‌های اقتصادی و اجتماعی کشور بر فضای سایبری بنا شده است. با ظهور این جوامع اطلاعاتی به هم پیوسته و همگرا خسارت‌های ناشی از حملات سایبری رو به افزایش بوده و پیش‌بینی می‌شود که تهدیدات ناشی از این فضا بسیار خطرناک‌تر و مخرب‌تر نیز بشود.

با ایجاد هر سرویس جدید در حوزه بانکی و پرداخت دو مسئله به صورت هم‌زمان مطرح می‌شود؛ از یک سو، سرعت ارائه برای استفاده کاربران و از سوی دیگر، مخاطرات و ریسک‌های مختلف از جمله ریسک‌های امنیتی؛ بنابراین باید بین سرعت در ارائه خدمت و ارزش‌آفرینی در عین حفظ امنیت و مدیریت ریسک‌ها توازن و تناسب برقرار کرد. اگر این توازن به درستی برقرار نشود ممکن است به یک شکست تجاری و تأخیر در ارزش‌آفرینی منجر شود. چون ایجاد امنیت نباید بیش از اندازه وقت بگیرد. از سوی دیگر اگر بدون در نظر گرفتن امنیت، صرفاً به ارائه سریع‌تر سرویس اقدام شود، قطعاً به معنای دامن زدن به ریسک‌های امنیتی خواهد بود؛ بنابراین مهم‌ترین موضوع در توسعه و کاربری فناوری‌های نوین بانکی، یافتن همین توازن میان امنیت و سرعت است.

فناوری در خدمت امنیت

یکی از موضوعات مهمی که باید به آن توجه کرد، نقش و تأثیر فناوری در ارتقای امنیت است. همان‌طور که پیشرفت‌های فناورانه به ارائه سرویس‌ها و محصولات جدید منجر می‌شود، سطح امنیت را هم ارتقا می‌دهد. نمونه این کاربرد را می‌توان در روش‌های تشخیص و احراز هویت مبتنی بر هوش مصنوعی، استفاده از فناوری در اعتبارسنجی و... مشاهده کرد. بانک‌ها و سایر فعالان این حوزه باید متناسب با سرمایه‌گذاری و تلاش برای ارائه خدمات و محصولات جدید، استفاده از فناوری برای ارتقای امنیت را هم دنبال کنند.

هوش مصنوعی نیز کمک‌های بسیاری به امنیت کرده و سرویس‌های خوبی با اتکا به آن طراحی و عملیاتی شده است، اما نکته مهم این است که چون هوش مصنوعی بر بستر کلان داده است، محافظت از این داده‌ها از جنبه‌های مختلف حائز اهمیت خواهد بود. جلوگیری از سوءاستفاده از کلان داده‌ها، تعریف

مشارکت فعال در آنها، تعیین حداقل‌های الزامی امنیت در خدمات و محصولات بانکی و با نهادسازی و ایجاد یک مرجع تخصصی برای امنیت نظام بانکی کشور که «شرکت کاشف» نمود واقعی این موضوع است، می‌تواند به بانک‌ها در زمینه حفظ امنیت و افزایش تاب‌آوری و پایداری کمک کند.

هرکدام از بانک‌ها در باره تاب‌آوری و افزایش امنیت خود، تجربیات متفاوتی دارند که در صورت اشتراک‌گذاری این تجربیات، بسیاری از هزینه‌ها و فرصت‌ها صرفه‌جویی می‌شود؛ بنابراین کمترین دخالتی که بانک مرکزی می‌تواند در خصوص افزایش تاب‌آوری و ارتقای امنیت بانک‌ها انجام دهد، ایجاد فضا و سازوکار مناسبی برای اشتراک‌گذاری تجارب بانک‌هاست. علاوه بر این از بطن این تجارب، توصیه‌هایی در حوزه امنیت و ... استخراج می‌شود که در قالب‌های مختلف اعم از الزام یا پیشنهاد از سمت بانک مرکزی به نظام بانکی ارائه می‌شود. از سوی دیگر بانک مرکزی تلاش می‌کند مسیر ارتباطی سایر نهادهای نظارتی و مسئول در حوزه امنیت و پایداری شبکه با بانک‌ها باشد و بر همین اساس هم برخلاف گذشته دخالت بیشتری در موضوع امنیت و پایداری شبکه بانکی دارد.



نقش کلیدی در تأمین امنیت بانک‌ها

از دیدگاه قانونی و حاکمیتی، بانک مرکزی متولی ایجاد هماهنگی عملیاتی و راهبردی در سطح نظام بانکی و تحقق هماهنگی نظامات سایبری در سطح این زیرساخت است. مهم‌ترین وظایف حاکمیتی عبارت‌اند از ارزش‌گذاری، جهت‌دهی و پایش.

به این ترتیب بانک مرکزی باید مشخص کند که چه چیزهایی در حوزه امنیت اطلاعات مهم هستند، بانک‌ها و مؤسسات اعتباری غیربانکی در مقاطع زمانی مختلف باید به چه اهداف و مقاصد تعریف‌شده‌ای برسند و در آخر فرایندی مدون و آزموده شده برای پایش این موضوع در جریان باشد. در واقع این، مأموریتی است که به بانک مرکزی سپرده شده است و در این راستا با مجموعه‌ای از سیاست‌گذاری‌ها، نهادسازی، هماهنگ‌سازی، ایجاد زیرساخت‌های فنی و ... وظایف خود را انجام داده و بانک‌ها و مؤسسات اعتباری هم باید تمامی تلاش خود را با لحاظ کردن رهنمودهای بانک مرکزی به کار ببندند.

در راستای تحقق نظامات امنیت و تاب‌آوری سایبری همانند نظام جامع پیشگیری و مقابله با حوادث سایبری، ارائه شده توسط مرکز ملی فضای مجازی کشور، جایگاه حاکمیتی و قانونی بانک مرکزی به عنوان فرصتی هم‌افزا در سطح زیرساخت حیاتی بانکی و پرداخت است. در واقع با اجرای تلاش‌های کلیدی بازوهای اجرایی در ارائه خدمات

دسترسی‌ها و ... از جمله مسائلی است که در کنار استفاده از هوش مصنوعی باید به آن‌ها توجه شود.

حفظ امنیت و افزایش تاب‌آوری

مقوله امنیت در شبکه بانکی، موضوعی یکپارچه است چراکه به لحاظ درهم تنیدگی اجزای شبکه، ریسک یا مخاطره امنیتی یک بانک به سرعت و به راحتی قابل تسری به سایر بخش‌های شبکه خواهد بود؛ بنابراین بانک مرکزی باید از جایگاه حاکمیتی خود، نسبت به حفظ استانداردهای امنیتی تک‌تک اجزای شبکه حساس باشد. معاونت فناوری بانک مرکزی با هماهنگ‌سازی نهادهای بالادستی، ایجاد ادبیات مشترک و همسوسازی اعضای نظام بانکی در تفهیم امنیت و تاب‌آوری در کل نظام بانکی، ترویج فرهنگ امنیت اطلاعات با ایجاد دغدغه برای تصمیم‌گیران و مدیران ارشد نظام بانکی، ایجاد آگاهی وضعیتی از امنیت اطلاعات نظام بانکی، ایجاد زیرساخت‌های فنی و فرهنگی به اشتراک‌گذاری اطلاعات، تعریف خدمات امنیتی حاکمیتی و الزام بانک‌ها و مؤسسات اعتباری به

سرمایه‌گذاری بر روی تحقیقات امنیت سایبری خاص و توسعه اقدامات در این زمینه‌ها و تنظیم اولویت‌های سالیانه تحقیق و توسعه برای شکل‌دهی انجمن‌ها و نشست‌های علمی و نوآورانه می‌شود.

جایگاه معاونت فناوری در استانداردسازی کارهای فناورانه

در حال حاضر استانداردسازی از چند طریق انجام می‌شود. برای آن دسته از محصولات و خدماتی که نیاز به اتصال به زیرساخت‌های حاکمیتی دارند، باید استانداردهای فنی ابلاغ‌شده را رعایت کرده باشند تا این اتصال رخ دهد. در واقع این نوع استانداردسازی در ابتدای امر باید وجود داشته باشد تا امکان خدمت‌رسانی فراهم شود.

برای آن دسته از محصولات و خدمات بانکی که به صورت مستقل و توسط بانک‌ها و مؤسسات اعتباری، شرکت‌های وابسته به آن‌ها یا پیمانکاران ایشان توسعه یافته‌اند، مجموعه‌ای از الزامات ابلاغ‌شده و فرایندهای ممیزی برای حصول اطمینان از رعایت این الزامات، به صورت دوره‌ای انجام می‌شود.

استانداردها، در واقع حداقل‌های پذیرفته‌شده از سوی اعضای یک صنعت محسوب می‌شوند و نباید سقف مطالبات یک نظام، تلقی شوند. با این توصیف، بانک‌ها و مؤسسات اعتباری برای بقا و افزایش سهم بازار خود باید همواره سطح کیفیت محصولات و خدمات خود را ارتقا بخشند. خوشبختانه به دلیل حساسیتی که مشتریان بانکی در انتخاب محصولات و خدمات بانکی دارند، رقابتی قابل‌توجه میان اعضای نظام بانکی به وجود آمده است و امنیت نیز به‌عنوان یک مؤلفه مهم برای مشتریان این حوزه بسیار مورد توجه است و همین موضوع، پیش‌رانی قدرتمند برای امنیت اطلاعات در به‌کارگیری استانداردهای روز دنیا از سوی بانک‌ها و مؤسسات اعتباری شده است.

کارهایی که باید انجام بدهیم

معاونت فناوری بانک مرکزی برای توسعه امنیت در آینده قصد تقویت شرکت کاشف را به‌عنوان بازوی اجرایی بانک مرکزی در حوزه امنیت اطلاعات دارد. همچنین معرفی امنیت به‌عنوان یک رکن اساسی و مزیت رقابتی در خدمات و محصولات بانکی یکی از کارهایی است که روی آن تمرکز داریم.

حمایت از برنامه‌های مرتبط با توانمندسازی نیروی کار امنیت اطلاعات و حمایت از نوآوری‌ها در حوزه امنیت اطلاعات از جمله کارهایی است که باید در مورد آن اهتمام بورزیم. همچنین نظارت مستمر و مبتنی بر فناوری‌های نوین و آینده‌نگری در حوزه امنیت نیز همواره در برنامه کار این معاونت قرار دارد.

روز آمد، مستمر و قابل‌اطمینان، بانک مرکزی نقش کلیدی در تحقق امنیت ملی در حوزه سایبری ایفا می‌کند.

چشم‌انداز بانک مرکزی برای ایجاد اثرگذاری و مسئولیت‌پذیری در زمینه پاسخ‌دهی و آگاهی‌تهدید شامل بهبود تشخیص، تحلیل، پاسخ‌دهی به تهدیدات پیچیده و کاهش آنها می‌شود که بر روی بانک‌ها متمرکز است. این راهبرد شامل ابتکار عمل و پیش‌قدمی برای نظارت تهدیدات از طریق استقرار آزمایشگاه‌های مرجع ارزیابی و ممیزی و انطباق سنجی کنترل‌های امنیتی، استقرار مراکز عملیات امنیت سایبری (SOC-ISAC)، راه‌اندازی تیم پاسخ‌گویی به رخداد (CSIRT-CERT)، اشتراک‌گذاری اطلاعات به‌منظور تسهیل و تسریع فرایند ایجاد آگاهی وضعیت سایبری و تصمیم‌سازی کم‌مخاطره، توسعه برنامه و طرح مدیریت بحران امنیت سایبری و پیاده‌سازی برنامه‌های تمرینی و مانورهای امنیت سایبری است.

در زمینه آموزش مشتریان و کاربران، پیاده‌سازی مدل‌های آموزشی و افزایش آگاهی مشتریان و کاربران برای حفاظت آنلاین از خود دارای اولویت است و شامل آگاهی‌رسانی روش‌های امنیت اطلاعات بانکی مشتریان به صورت گسترده و از طریق رسانه‌های عمومی و تأثیرگذار فناوری اطلاعات، انتشار ابزارهای عملیاتی ضد اسپم و روال‌های آن‌ها و تحلیل جایگزین‌های شکل‌دهی و آموزش مشتریان در رابطه با مخاطرات امنیت سایبری مرتبط با اطلاعات و تبادلات بانکی می‌شود.

همکاری در سطح ملی به‌منظور ارتقا و بهبود امنیت و تاب‌آوری در زیرساخت‌ها، شبکه‌ها، محصولات و خدمات کار دیگری است که می‌توان با تقویت و استحکام همکاری‌های امن با بانک‌ها به‌منظور پشتیبانی از اشتراک‌گذاری اطلاعات سایبری، تقویت قراردادهای همکاری‌ها با سایر زیرساخت‌ها به‌منظور افزایش آگاهی در زمینه مخاطرات سایبری، تهدیدات و آسیب‌پذیری‌ها، ارتقا و بهبود تعاملات پیوسته تجاری برای امنیت و حفاظت از بانک‌ها و تدوین و ارائه طرح‌ها و برنامه‌های همکاری ملی در راستای محافظت از زیرساخت‌های حیاتی به انجام آن اهتمام ورزید.

پی‌ریزی چارچوب قانونی و اجرای مؤثر آن برای پیگیری‌های جرائم سایبری نیازمند بهبود همکاری یکپارچه میان امنیت سایبری و اجرای قانون، به‌روزرسانی چارچوب‌های قوانین داخلی و مجرمانه با ارزیابی تغییرات فناوری و موارد مجرمانه و بهره‌مندی از چارچوب‌های قانونی به‌منظور اشتراک‌گذاری اطلاعات و بهبود تعاملات اجرایی قوانین کشور است.

همچنین بهبود و ارتقای مهارت‌های امنیت سایبری با حرکت به سمت تحقیقات و توسعه راه‌حل‌های نوآورانه شامل به‌کارگیری روش‌های حفظ و به‌کارگیری جدید،

چشم‌انداز بانک مرکزی برای ایجاد اثرگذاری و مسئولیت‌پذیری در زمینه پاسخ‌دهی و آگاهی‌تهدید شامل بهبود تشخیص، تحلیل، کاهش و پاسخ‌دهی به تهدیدات سایبری پیچیده می‌شود که بر روی بانک‌ها متمرکز است

مهندس امین مهاجر

هوش مصنوعی ظرفیت انجام جرائم سایبری را به شدت افزایش می‌دهد

از این رو، طراحی اصولی سازوکارهای ارائه خدمات الکترونیکی به‌ویژه در زیست‌بوم بانکی و پرداخت کشور که با معیشت و افکار عمومی جامعه ارتباط مستقیم دارد، امری نه فقط لازم، بلکه حیاتی است. توسعه خدمات و کسب‌وکارهای پولی و بانکی متعدد بر پایه تحلیل و طراحی ضعیف، هرچند مزایای رقابتی و منافع کوتاه‌مدتی را نصیب برخی بنگاه‌های اقتصادی و شرکت‌های تابعه آن‌ها می‌کند، اما در بلندمدت به قابلیت اعتماد خدمات لطمه وارد کرده و همه موجودیت‌های نظام بانکی و پرداخت را متضرر می‌کند. این امر را در حوزه پرداخت‌بازی‌ها و Open-API، کیف پول‌های دیجیتال و اپلیکیشن‌های موبایلی آسیب‌پذیر تجربه کرده‌ایم و بهای آن را نیز پرداخته‌ایم. در نتیجه، تحلیل و طراحی اصولی در کنار بهره‌گیری از فناوری‌های اثبات‌شده روز دنیا به همراه توجه به هماهنگی‌های بین دستگاهی، اهتمام به چهارچوب‌های امنیتی نهادهای نظارتی و تنظیم‌گر و فرهنگ‌سازی عمومی در حوزه استفاده صحیح از ابزارهای تکنولوژیک، می‌تواند راهگشا باشد.

بهبود امنیت و افزایش تاب‌آوری و پایداری

شرکت‌های زیرمجموعه گروه ملی انفورماتیک، به‌ویژه شرکت کاشف نقش تعیین‌کننده‌ای در تدوین الزامات امنیتی در حوزه‌های مرتبط با تاب‌آوری امنیتی و نظارت مستمر بر وجود انطباق و حسن اجرای آن‌ها در موجودیت‌های نظام بانکی و پرداخت دارند.

باید با نگاهی تخصصی و دقیق در حوزه امنیت اطلاعات و افزایش تاب‌آوری و پایداری (Contingency and Resilience) سخن گفت. ابتدا در زمینه اصول و استانداردهای تاب‌آوری و پایداری، می‌توان به طرح‌ها و برنامه‌های گوناگونی اشاره کرد که هر یک از آن‌ها یکی از ارکان و ملزومات تاب‌آوری و پایداری در حوزه خدمت‌دهی و امنیت اطلاعات را شامل می‌شوند؛ از جمله این مفاهیم و طرح‌های بنیادی در حوزه تاب‌آوری امنیت اطلاعات می‌توان به مواردی همچون طرح‌های تداوم کسب‌وکار و بازیابی از فاجعه (BCP/DRP)، طرح‌های تداوم عملیات (Continuity of Operations Plan - COOP)، طرح‌های تداوم سرویس‌دهی سامانه‌های اطلاعاتی (Information System Contingency Plan - ISCP) و فرایندهای مدیریت رخداد (Incident Handling) و تعاملات ویژه در مدیریت بحران (Crisis Communication Plan) اشاره کرد.

علاوه بر اهتمام به الزامات و پیاده‌سازی این طرح‌ها در زمینه تداوم عملیات و کسب‌وکار، تاب‌آوری و پایداری همچنین باید هماهنگی در واکنش به رخداد و تبیین فرایندهای مدیریت شرایط بحران امنیت اطلاعات در شبکه بانکی و پرداخت وجود داشته باشد. در همین رابطه شرکت کاشف، علاوه بر توسعه فرایندها و دستورالعمل‌های اعلام شرایط هشدار امنیت اطلاعات در نظام بانکی، پروژه‌ای تحت عنوان امداد سایبری و عملیات فارتیک رخدادهای

توسعه خدمات و کسب‌وکارهای متعدد بر روی پلتفرم‌های گوناگون از جمله وب، موبایل و PWA، که معمولاً اطلاعات محرمانه مالی، هویتی و حریم خصوصی افراد را در خود نگهداری کرده و انتقال می‌دهند، به صورت بالقوه در معرض انواع تهدیدات سایبری و روش‌های کلاهبرداری و تقلب قرار دارند. این در حالی است که سازوکاری مانند پیامک رمز پویا، به دلیل توسعه قابل توجه روش‌های نوین فیشینگ و اپ‌های جعلی و مخرب که اقدام به سرقت رمز پویا از کاربر می‌کنند، اثربخشی خود را از دست داده و یا در آینده نزدیک از دست خواهد داد.

تهدیداتی همچون استفاده غیرمجاز از ابزارهای پرداخت در حوزه قمار و شرط‌بندی، درگاه‌های پرداخت غیرمجاز، سوءاستفاده از ظرفیت‌های بانکداری باز به‌ویژه در ارتباط با شرکت‌های پرداخت‌یار و پرداخت‌ساز و توسعه اپلیکیشن‌های جعلی یا دستکاری شده، از جمله تهدیدات امنیتی حال حاضر صنعت بانکداری و پرداخت کشور محسوب می‌شوند. تهدیداتی که باید نرخ رشد آن‌ها را موازی با ظرفیت‌های هوش مصنوعی دانست که در دسترس مهاجمان قرار دارند.

با این اوصاف، امضای دیجیتال و سازوکار احراز هویت کاربران به موضوع مهمی تبدیل شده است و انجام آن، مشارکت و هماهنگی بین دستگاه‌ها و نهادهای مختلف را می‌طلبد که نقش محوری بانک مرکزی و شرکت ملی انفورماتیک به‌عنوان بازوی اجرایی حوزه خدمات و امنیت اطلاعات بانک مرکزی را پررنگ‌تر می‌کند.

پیشرفت فناوری و مشکلات امنیتی

روند رو به رشد فناوری و وابستگی روزافزون کسب‌وکارها به زیرساخت‌های فناورانه، مخاطرات امنیتی بیشتری را متوجه دارایی‌های اطلاعاتی ارائه‌دهندگان خدمات و حریم خصوصی افراد می‌کند. باید توجه داشت که پیشرفت تکنولوژی اساساً ابزاری است که هم در اختیار ارائه‌دهندگان سرویس است، هم بازیگران تهدید و هم نهادهای نظارتی. در واقع این یک مسابقه ماراتن بین استفاده‌کنندگان از تکنولوژی و سوءاستفاده‌کنندگان از آن است.

سطح خدمات (SLA) به‌عنوان نمونه موفق دیگری از جایگاه حاکمیتی شرکت ملی انفورماتیک قابل ذکر است. با لحاظ کردن اصول و ملاحظات حاکمیت داده در صنعت بانکی، می‌توان نقش حاکمیتی شرکت ملی انفورماتیک را به‌عنوان بازوی اجرایی بانک مرکزی، اثربخش و فرصت‌ساز ارزیابی کرد.

برنامه‌های آینده برای توسعه امنیت

شرکت مدیریت امن الکترونیکی کاشف، ذیل شرکت ملی انفورماتیک، مسئولیت اصلی تنظیم‌گری، نظارت و عملیات امنیت اطلاعات در شبکه بانکی را بر عهده دارد. در همین رابطه شرکت کاشف، برنامه‌های توسعه‌ای، نظارتی و عملیاتی مختلفی را در حوزه امنیت انجام داده و در دستور کار دارد.

نظارت، ممیزی و انطباق‌سنجی امنیتی، رگولاتور امنیت حوزه بانکی، تدوین چهارچوب کنترلی نظام امنیت اطلاعات بانکی، آزمایشگاه ارزیابی امنیتی بانکی، هماهنگی در رسیدگی به رخدادهای امنیت اطلاعات نظام بانکی، امداد سایبری و عملیات فارتزیک در محل، ایجاد آکادمی امنیت و راه‌اندازی اپراتور امنیت و مرکز ارائه خدمات امنیت مدیریت‌شده (MSSP) از جمله اقدامات این مجموعه برای ارتقای امنیت نظام بانکی است.

بانکی را در دستور کار دارد که با هماهنگی مراجع امنیتی به بانک‌ها و مؤسسات اعتباری در واکنش مؤثر و سریع به رخدادهای و تهدیدات به وقوع پیوسته کمک می‌کند. تدوین و اطمینان از اجرای صحیح الزامات امنیتی متناسب در کنار مشارکت و مساعدت در حوزه عملیات امنیت با موجودیت‌های زیرمجموعه، نقشی است که شرکت ملی انفورماتیک در ارتقای تاب‌آوری و پایداری امنیت کسب‌وکار در حوزه پولی و بانکی کشور ایفا می‌کند.

جایگاه حاکمیتی شرکت ملی انفورماتیک


بازگشت به راهبردهای شش‌گانه عالی فضای مجازی و به‌تبع آن، برنامه‌های مرکز مدیریت راهبردی افتای ریاست جمهوری و ایجاد و توسعه ظرفیت‌های تنظیم‌گری و اپراتور امنیت در بخش‌های مختلف صنایع و زیرساخت‌های حیاتی کشور به‌منظور ارتقای سطح آمادگی در مواجهه با تهدیدات امنیت اطلاعات در قالب ساختاری سلسله‌مراتبی امری ضروری است. این جایگاه مستلزم ایجاد تعاملات مستمر و مؤثر میان تنظیم‌گر و اپراتور امنیت یک صنعت با مراجع امنیتی و نظارتی کشور است. بانک مرکزی و به‌تبع آن، شرکت ملی انفورماتیک به‌عنوان بازوی اجرایی آن بانک، پوشش‌دهنده این جایگاه حاکمیتی میان موجودیت‌های صنعت بانکی و پرداخت کشور با مراکز امنیتی و نظارتی کشور است.

از سویی دیگر، زیرساخت تکنولوژیک بانکی و پرداخت کشور که به‌عنوان یکی از ساختارهای فناوری اطلاعات به‌روز و قابل‌اعتماد کشور و منطقه به‌شمار می‌آید و پایداری خدمات آن در طول زمان برای عموم جامعه و فعالان این حوزه نیز اثبات‌شده است، نیازمند ساختاری میانی به‌منظور ایجاد و توسعه زیرساخت‌های مشترک، هماهنگی‌های فناورانه و تسهیل و تسریع فرایندهای جریان کارهای سیستمی با سایر دستگاه‌های اجرایی کشور است. ارائه یک خدمت بانکی تعاملات متعدد و متنوعی را با سایر نهادهای مجریه و مقننه کشور می‌طلبد. به‌عنوان مثال خدماتی همچون تخصیص ارز یا ایجاد کانال‌های اعتباری تجاری که در سیستم بانکی اتفاق می‌افتد، مجموعه‌ای از تعاملات با قانون‌گذار، وزارت اقتصاد، وزارت صمت، سازمان امور مالیاتی و بسیاری دستگاه‌های دیگر را در پس خود داشته است که همگی توسط بانک مرکزی و ظرفیت‌های اجرایی شرکت ملی انفورماتیک صورت می‌پذیرد.

نمونه ساده دیگری که مردم همه‌روزه با آن سروکار دارند سرویس‌های بین‌بانکی مانند چکاوک و شتاب و رمز پویا است که با جایگاه حاکمیتی و اجرایی شرکت ملی انفورماتیک و بانک مرکزی ایجاد شده‌اند. نقش سامانه سرآمد و ارتباط با دستگاه قضایی کشور در ثبت و رسیدگی به دستورات قضایی در قالب توافقات



10.10.10.10



HACKED

```
MEM: 1024M/4096M
CPU: 89.41%

netcon1 = new CANTailor(Vars.HW_MOTOR_L_PWM);
netcon2 = new CANTailor(Vars.FIRE_MOTOR_2_PORTS);
beaterBarRoller = new Tailor(Vars.BEATER_BAR_ROLLER_PORTS);
stick = new CANTailor(Vars.WIICK_PORTS);
steeringMotor = new CANTailor(Vars.TELESCOPE_PORTS);

/Sensors
stickJoy = new Logitech(Vars.JOYSTICK_L_PORT);
stickJoy2 = new Logitech(Vars.JOYSTICK_R_PORT);

control = new Controller(Vars.CONTROL_JOYSTICK_PORTS);


firePiston = new DoubleSolenoid(Vars.LIFT_PISTON_FORWARD_PORT,
Vars.LIFT_PISTON_REVERSE_PORTS);
firePiston2 = new DoubleSolenoid(Vars.FIRE_PISTON_FORWARD_PORT,
Vars.FIRE_PISTON_REVERSE_PORTS);
lockSolenoid = new DoubleSolenoid(Vars.LOCK_SOLENOID_FORWARD,
Vars.LOCK_SOLENOID_REVERSE_PORTS);

grabSense = new DigitalInput(Vars.GRAB_SENSE_PORT);
loadSense = new DigitalInput(Vars.LOAD_SENSE_PORT);
armDeploySense = new DigitalInput(Vars.ARM_DEPLOY_SENSE);
shooterUpperLimit = new DigitalInput(Vars.SHOOTER_UPPER_LIMIT);
shooterLowerLimit = new DigitalInput(Vars.SHOOTER_LOWER_LIMIT);

aimShooter = new LimitedSpeedController(shooterUpperLimit,
shooterLowerLimit,
new CANTailor(Vars.SHOOTER_ARM_PORTS);
beaterBarPot = new Tailor(Vars.BEATER_BAR_POT_PORTS);

fireEncoder = new Encoder(Vars.LIFT_ENCODER_PORT_A,
Vars.LIFT_ENCODER_PORT_B);
telescopeEncoder = new Encoder(Vars.TELESCOPE_ENCODER_PORT_A,
Vars.TELESCOPE_ENCODER_PORT_B);

shooterPot = new AnalogPotentiometer(Vars.SHOOTER_POTENTIOMETER);
beaterBarPot = new AnalogPotentiometer(Vars.BEATER_BAR_POT);
```



Demographic Analyzer SW1.4

P.I.D.	USER	PRI	NI	VIRT	RES	SHR	CPU%
5107	netcon0	55	08	459	2180	2344	12.41%
5108	netcon1	87	12	555	3465	2188	11.85%
5109	netcon2	17	00	4E			19.17%
5110	netcon3	18	54	10	root@kali:~/htb/bores/hackard/gebeater		
5111	netcon4	28	28	21	gebeater V1.9		
5112	netcon5	77	24	17	=====		

```
Terminal 01
group_name: task_group - 1
priority: group_name:task_group
status: group_name:task_group
log: netcon0
log 1:
=====
hostname = (q)hostname - 888093_93_2
// Make sure we always allocate at 16
```

SYSTEM

```
chooser = new SendableChooser();
chooser.addObject("Default Auto", SmartDashboard.getDefaultAuto());
chooser.addObject("My Auto", customAuto);
SmartDashboard.putData("Auto chooser", chooser);

airCompressor = new Compressor(DriveTrain.Solenoid, new CANTailor(Vars.DRIVE_TRAIN_SOLENOID));
```




امنیت باید به کسب و کار بانکی گره بخورد

حسین قرایی گرکانی، مدیرعامل کاشف، مهم‌ترین مأموریت این شرکت را حفظ و توسعه امنیت فناوری اطلاعات در حوزه بانکی برمی‌شمارد. در ادامه پای صحبت‌های او نشستیم که یک سال می‌شود سکان هدایت کاشف را در دست گرفته است.

مهم‌ترین مأموریت کاشف، امنیت و امن‌سازی در حوزه بانکداری و بانک مرکزی است، چه در حوزه امنیت اطلاعات و چه در حوزه امنیت شبکه.

به سطح بالاتر بباییم مقداری جای کار دارد و باید در زمینه امنیت اطلاعات و امنیت شبکه، رگولاتوری اتفاق بیفتد که نقش کاشف در این مورد برای بانک مرکزی نقش بسیار مهمی است. باید الزاماتی از سمت رگولاتور به بانک‌ها ارجاع شود که سطح امنیت خود را ارتقا بدهند. به نظر می‌رسد کسب و کار بانکی به امنیت اطلاعات گره نخورده و ما باید کاری کنیم که کسب و کارها ارزش اعتماد را در حوزه امنیت درک کنند. یعنی بدانند وقتی امنیت را برقرار می‌کنند در واقع دارند برای مشتریان خود اعتماد ایجاد می‌کنند و در حقیقت، امنیت را جزء مسائل متفرقه کسب و کارشان نبینند، بلکه امنیت اطلاعات را ابزاری ببینند که به جذب مشتری کمک می‌کند؛ اما متأسفانه امنیت در بسیاری از جاها مغفول مانده است.

امنیت، اولویت اولی که آخر دیده می‌شود

امنیت جدا از اینکه فناوری و دانش جدیدی است، در ایران هم یک رشته جوان و جدید محسوب می‌شود. در کسب و کارها، امنیت نسبت به سایر موضوعات کسب و کاری اولویت ندارد. بانک‌ها هم کل تمرکزشان بر روی کسب و کار در حوزه مالی است. در حقیقت می‌توان گفت در حوزه مالی تقریباً سودی که از مشتری می‌گیریم و سودی که به مشتری می‌دهیم خیلی اختلاف فاحشی دارند و لذا می‌توانند مشکلات مرتبط با امنیت اطلاعات را هم پوشش بدهند و خیلی از آسیب‌پذیری‌ها و حفره‌ها و مخاطرات و حوادثی که در حوزه بانکداری اتفاق می‌افتد به سبب این موضوع پوشش داده می‌شود. اگر بخواهیم در حوزه بانکداری از سطوح مختلف امنیت شبکه و امنیت اطلاعات

بخش دولتی و نیمه‌دولتی به بخش خصوصی با حقوق‌های بسیار بالا که امکان پرداخت آن‌ها در بخش‌های دولتی و نیمه‌دولتی فراهم نیست و دیگری مهاجرت از ایران به خارج از کشور و یا به سمت آزاد و فریلنس کار کردن. در همه حوزه‌های آی‌تی این مشکل وجود دارد ولی در حوزه امنیت اطلاعات این موضوع خیلی پررنگ‌تر است و باید به آن پرداخته شود. حاکمیت باید در مورد این موضوع تدبیری بیندیشد. چون با ادامه این روند حوزه امنیت و آی‌تی کشور در آینده دچار مخاطره بسیار زیادی می‌شود. باید میزان حقوق متخصصان آی‌تی را مانند حقوق کارشناسان صنعت نفت جدا ببینیم. زیرساخت کشور بر اساس آی‌تی و سی‌تی است؛ در حالی که حقوق افراد این حوزه شاید حقوق متوسط رو به پایینی باشد. لذا نیروها ترجیح می‌دهند به کشورهای اطراف یا اروپا مهاجرت کنند یا به صورت آزاد کار کنند.

دانشگاه از صنعت فاصله دارد

یکی از موضوعات مهم دیگری که به آن برخورد کردیم سطح تخصص افراد در حوزه امنیت است. آموزش‌های بین‌المللی در ایران بسیار کم‌رنگ است و اگر امروز برای آن چاره‌ای نیابیم شاید در آینده جزو بی‌سوادهای دنیا در حوزه آی‌تی قلمداد شویم.

ما باید واحدهای درسی دانشگاهی را تغییر بدهیم؛ مخصوصاً در حوزه آی‌تی و امنیت اطلاعات. موضوعاتی که در دانشگاه تدریس می‌شود قدیمی و در مواردی حتی خیلی قدیمی هستند. میان دانشگاه و صنعت ما فاصله افتاده است و این دغدغه اصلی کسانی است که هم در صنعت حضور دارند و هم در دانشگاه. صنعت ما مسیر خودش را می‌رود و دانشگاه ما هم مسیر مقاله‌محور خودش را می‌رود. پیش‌گرفته و فراموش کرده است که احتیاجات و نیازهای صنعت را مورد توجه و تحقیق قرار دهد. در کشورهای پیشرفته دنیا کوآپ راه‌اندازی کرده‌اند. اشخاص یک‌ترم به دانشگاه می‌روند و یک‌ترم، کار کردن در آن حوزه را تجربه می‌کنند و به این ترتیب دانش از پایین به بالاتر رقیق می‌شود. متأسفانه در حال حاضر و در بسیاری از موارد، کارشناسان در صورت داشتن توانمندی، فقط به خرید تجهیزات بسنده می‌کنند و وارد سطوح دیگر دانش فنی نمی‌شوند.

جایگاه کاشف در امنیت شبکه بانکی

ما طرح‌هایی را در کاشف راه‌اندازی کردیم تا بتوانیم به بانک‌ها در زمینه امنیت اطلاعات کمک کنیم. یکی از موضوعاتی که چندین سال در کاشف روی آن کار شده بود مربوط به چهارچوب کنترلی در حوزه امنیت بانکداری بود. این چهارچوب طراحی شده بود اما در ابلاغ آن تأخیر

ارتقای بلوغ مرکز عملیات امنیت

متأسفانه باینکه یکی از مهم‌ترین موضوعات از زمان شروع به کار مرکز ملی فضای مجازی و شورای عالی فضای مجازی، طبق تأکیدات مقام معظم رهبری، مرکز عملیات امنیت بود ولی با گذشت بیشتر از دوازده سال، هنوز مراکز عملیات امنیت در ایران به بلوغ کافی نرسیده‌اند و اکنون که SOAR (Security orchestration, automation and response) و نسل پنجم مرکز عملیات امنیت و نیز SIEM از راه رسیده‌اند ما هنوز در کشورمان در نسل اول و دوم آن‌ها متوقف مانده‌ایم. اغلب نفوذهایی که در لایه‌های مختلف بانکی رخ می‌دهد به این خاطر است که مرکز عملیات امنیتی وجود ندارد که آن‌ها را تشخیص بدهد؛ بنابراین، یکی از مأموریت‌های مهم کاشف که از سال گذشته بر آن تمرکز بیشتری شده است، ارتقای بلوغ مرکز عملیات امنیت است. ما با سامانه‌های مختلفمان مثل رادار و FS-ISAC (Financial Services Information Sharing and Analysis Center) این الزام را ایجاد کرده‌ایم که بانک‌ها مرکز عملیات امنیت خود را ارتقا بدهند و آن را سناریو محور کنند و در پایین‌ترین سطح، بتوانند APT‌ها را تشخیص دهند. این جزء مأموریت‌های خیلی مهم کاشف است؛ جایی که شاهدیم، امنیت با کسب‌وکار گره نخورده است. مخاطرات در حوزه بانکی هم با مخاطرات آی‌تی گره نخورده است.

ساختار مشخصی برای امنیت تعریف نشده است

با توجه به این عدم بلوغ سازمانی، صنعت بانکی ما در فناوری ضعف دارد که البته قابلیت پوشش دادن این ضعف در کشور وجود دارد و می‌توانیم موضوع فناوری را در بانک‌ها، چه با تجهیزات پیشرفته دنیا و چه با تجهیزات بومی که در ایران وجود دارد، حل و فصل کنیم. ولی این همت باید در بانک‌ها باشد که بخواهند امنیت اطلاعات و امنیت شبکه خود را ارتقا بدهند. درون بانک‌ها، ساختار مشخصی برای امنیت تعریف نشده است. این مهم‌ترین مشکلی است که در ساختار بانک‌ها وجود دارد. یک بانک در بهترین حالت، واحدی را با سرپرستی یک مدیرکل زیر نظر مدیرعامل برای این کار در نظر گرفته است. شاید بتوانیم بگوییم حوزه مالی جایی است که بیشترین نیاز را به امنیت دارد؛ یعنی تهدیدات و مخاطرات مالی، تقلب‌ها، قمار و ... ایجاب می‌کند که امنیت اطلاعات این حوزه تضمین شود.

حقوق ناکافی؛ یکی از دلایل مهاجرت متخصصان

جدا از موضوع ساختار و فناوری، معضل مهاجرت نیروی انسانی و مخصوصاً مهاجرت نیروی زبده و متخصص کشور است. در ایران دو نوع مهاجرت در جریان است. یکی از

بانکی، تمرکز داریم. کاشف به عنوان مرجع اصلی ارزیابی امنیتی حوزه بانکداری، اپ‌ها، وب، شبکه و امضای دیجیتال آن‌ها را ارزیابی امنیتی می‌کند. این آزمایشگاه اکنون فعال است و امسال توانست ارزیابی‌های بسیار خوبی را در همه حوزه‌هایی که به آن‌ها اشاره شد انجام بدهد.

موضوع دیگری هم که می‌توانیم از طریق آن به افزایش امنیت بانک‌ها کمک کنیم اقدام ما برای راه‌اندازی آکادمی امنیت است تا آموزش‌های موردنیاز حوزه بانک در زمینه امنیت اطلاعات را ارائه دهیم. طراحی مفهومی آن به‌طور کامل انجام شده و بستر فیزیکی آن آماده شده و به‌زودی ارائه خدمت سراسری آن شروع می‌شود.

موضوع دیگری که در کاشف خیلی مهم است موضوع فارنزیک و تحلیل ادله است. کاشف می‌تواند با تجهیزات و سامانه‌هایی که دارد در این زمینه کمک زیادی به بانک‌ها بکند.

تعامل کاشف با نهادهای ناظر

تقریباً می‌شود گفت بر اساس نظام پیشگیری و مقابله با حوادث سایبری، مرجع هماهنگ‌کننده ما مرکز مدیریت

راهبردی افتا است که ما ارتباط خوبی با آن‌ها

داریم. یکی از کارهای کاشف، ممیزی

بانک‌ها در حوزه امنیت است که این‌ها

را همگی با تأییدیه این مرکز انجام

می‌دهیم. با پدافند غیرعامل هم

اگرچه هنوز پروژه مستقیمی نداریم

ولی در حوزه تاب‌آوری و پایداری و

قسمت پدافند بانک مرکزی همکاری

می‌کنیم و موضوعاتی مثل

اشتراک‌گذاری و تحلیل

اطلاعاتمان در آن حوزه

قرار می‌گیرد.

پیش آمده بود اما اوایل امسال به بانک‌ها ابلاغ شد. ما در این چهارچوب یک سری استانداردهای مهم را در حوزه امنیت بررسی کرده بودیم و شاخص‌های کنترلی را در آورده بودیم که شامل حداقل الزامات امنیتی جهت پیاده‌سازی بود. اگر بانک‌ها پیاده‌سازی چهارچوب کنترلی را شروع کنند، مراحل و مدل بلوغشان به سطح قابل قبولی می‌رسد چون در آن همه موضوعات از مدیریت تهدیدات، مدیریت آسیب‌پذیری‌ها، مدیریت مخاطرات و حاکمیت امنیت به‌طور کامل دیده و در جزئیات هرکدام از آن‌ها بحث‌های سیاست و حاکمیت، انطباق‌سنجی، به‌طور کامل انجام شده است. ضمن آنکه مدیریت احراز هویت و اصالت و بحث‌های مربوط به حوزه امنیت از سنسورها گرفته تا مرکز عملیات امنیت تا مرکز گوهر و مرکز اشتراک‌گذاری و تحلیل اطلاعات همه در آن دیده شده‌اند.

بانک‌ها طبق دستور بانک مرکزی و مرکز مدیریت راهبردی افتا ملزم به اجرای این چهارچوب هستند. کاشف نقش ناظر را دارد و رگولاتور اصلی بانک مرکزی است. در حال حاضر همکاری خوبی بین کاشف و بانک‌ها در این حوزه شکل گرفته و بانک‌ها در حال انجام پیاده‌سازی چهارچوب کنترلی در مجموعه خود هستند.

کمک دیگری که کاشف به بانک‌ها کرده در

همان حوزه مرکز عملیات امنیت و گوهر (گروه

واکنش هماهنگ رخدادهای رایانه‌ای) است که

از آن‌ها خواسته طراحی، ارتقا و به‌روزرسانی

مراکز عملیات امنیت و گوهر به‌طور مداوم

در برنامه کارشان باشد و در سلسله مراتب

این‌ها به مرکز اشتراک‌گذاری و تحلیل

اطلاعات بانکی در کاشف وصل می‌شوند.

کار دیگری که کاشف برای ارتقای امنیت

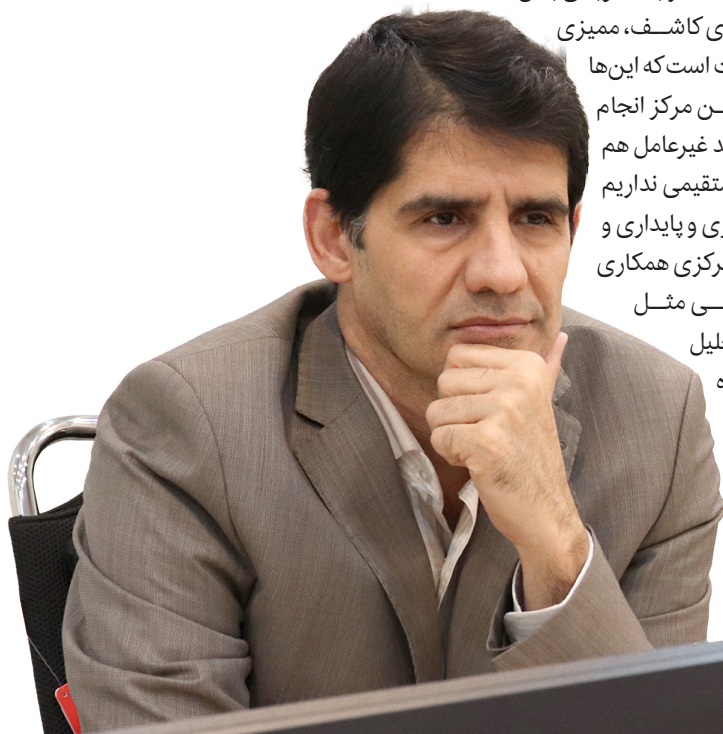
بانک‌ها انجام داده ایجاد آزمایشگاه

ارزیابی امنیتی است. گواهی‌نامه این

آزمایشگاه را نیز از مرکز مدیریت

راهبردی افتا دریافت کرده‌ایم و بر

ارزیابی امنیتی محصولات و خدمات



داشته باشیم. تقریباً کارهایی که تا الآن ذکر کردم در همین حول و حوش بوده است؛ چه چارچوب کنترلی که ممیزی و ارزیابی دارد و چه تأمین سیاست‌ها و آیین‌نامه‌ها. آنجایی که داریم الزامات می‌دهیم، جایی که آیین‌نامه می‌دهیم، جایی که ابلاغ می‌کنیم و جایی که سیاست‌گذاری می‌کنیم همه جزء کارهای اپراتور امنیت است و کارهایی که در ارزیابی امنیتی می‌کنیم همه وظایفی است که اپراتور امنیت باید انجام بدهد. چیزی که شاید مدنظر شورای عالی فضای مجازی است، این بوده که باید دستگاه هماهنگ‌کننده‌ای باشد که بتواند کل امنیت را کنترل کند یعنی طبق دستوراتی که دادند اپراتور امنیت به تعبیر من همان FS-ISAC است که کل اطلاعات را جمع و هماهنگ می‌کند و به اشتراک می‌گذارد و وضعیت سایبری را مشخص می‌کند و اگر لازم باشد سیاست‌های کلی را از مراجع بالادستی مثل شورای عالی فضای مجازی می‌گیرد و با ادبیات حوزه بانکداری ترجمه و ابلاغ می‌کند.

کارهایی که در کاشف انجام دادیم

ما امسال با تلاش همکاران مجوز دانش‌بنیانی کاشف را اخذ و توانستیم آزمایشگاه ارزیابی کاشف را راه‌اندازی کنیم و سرویس بدهیم و توانستیم با کمک معاونت فناوری نوین بانک مرکزی و مدیر ارشد امنیت بانک مرکزی، پایه و اساس مرکز ارائه خدمات امنیت مدیریت‌شده را بنا بگذاریم و توانستیم نقش اپراتور امنیت را شکل بدهیم.

چیزی که در کاشف مغفول مانده بود کمک به قوه قضاییه در دستورات قضایی بود و ما توانستیم امسال سامانه «سرآمد» راه‌اندازی کرده و سرعت آن را بالا ببریم و تقریباً شش میلیون دستور قضایی را از حوزه دادستانی به بانک‌ها انتقال دادیم و بازخورد گرفتیم و به قوه قضاییه برگرداندیم در این یک سال توانستیم نسخه اول FS-ISAC را راه بیندازیم که سامانه رادار است. سامانه رادار دو سال بود که کار می‌کرد و با همت همه همکاران کاشف توانستیم امسال همه اطلاعات را جمع‌آوری کنیم. رادار مقدمه FS-ISAC است. ما امسال توانستیم ابزار فارتیک برای کاشف تهیه کنیم و آزمایشگاه سیار فارتیک راه‌اندازی کنیم. توانستیم پروژه ISMS را هم در سطح کاشف و هم در سطح بانک مرکزی عملیاتی کنیم و مدیریت مخاطراتی را برای بانک مرکزی انجام بدهیم و مجوز اپراتور امنیت را اخذ کنیم.

در پایان تأکید می‌کنم که ما به‌عنوان اپراتور امنیت اطلاعات در شبکه بانکی، قصد داریم که سطح امنیت و سطح بلوغ این حوزه را با کمک خود بانک‌ها افزایش دهیم تا بتوانیم صنعت بانکداری را به یکی از سرآمدان حفظ امنیت اطلاعات در بین همه صنایع دیگر تبدیل کنیم.

چگونه به چهارچوب کنترلی رسیدیم

NIST و ISO و PCI-DSS و ISMS استانداردهای مهمی در این موضوع هستند و ما تقریباً چکیده این استانداردها را در چهارچوب کنترلی آوردیم که این چهارچوب حدود شصت زیررده و نزدیک به هزار و چهارصد شاخص دارد.

برای شفافیت روش پیاده‌سازی آن هم به جای اینکه آیین‌نامه خاصی بدهیم خود چهارچوب کنترلی را به صورت شاخص و بر اساس اسناد بالادستی تدوین کردیم و همچنین نرم‌افزاری در این زمینه طراحی کردیم به نام «سرابان» که این شاخص‌ها را استخراج می‌کند و به بانک‌ها می‌گوید که این شاخص‌ها مورد نیاز شما هستند و به آن‌ها زمان می‌دهد تا بروند و شاخص‌ها را پیاده‌سازی کنند و دوباره ممیزی و بازبینی بشوند. یا در حوزه نماد و مرکز ریشه، دقیقاً الزامات و آیین‌نامه‌ها را تدوین کردیم و به بانک‌ها ابلاغ کردیم. مرکز عملیات امنیت هم همین‌طور. الزامات و قابلیت‌هایی را که یک مرکز عملیات باید داشته باشد مشخص کرده و به بانک ابلاغ می‌کنیم.

الزامات امنیتی نظارت و ارزیابی امنیتی صرفی‌ها هم به کاشف به‌عنوان یک مرکز MSSP (Managed Security Service Provider) محول شده تا سرویس‌های خدمات امنیت مدیریت‌شده به آن‌ها بدهد و یک سری الزاماتی را به آن‌ها ابلاغ کردیم و گفتیم که به‌عنوان خوداظهاری وضعیت را بررسی کنند تا بعد ما به‌عنوان ممیز ورود کنیم.

کاشف همیشه حداقل الزامات امنیتی را ابلاغ می‌کند. طراحی، مشاوره و نظارت را انجام می‌دهد ولی در پیاده‌سازی وارد نمی‌شود. چون خودمان ناظر و اپراتور امنیت هستیم البته شاید در گام‌های ابتدایی این کار را تسهیل کنیم ولی سیاست کلی مان این است که این‌ها را به مرور زمان از خودمان جدا کنیم و در سلسله مراتب، ما مرجع آزمون باشیم و بانک مرکزی مرجع اعتبارسنجی. به‌عنوان مثال، ماهر بانکی کاشف اکنون تحلیل حادثه، تحلیل آرتیفکت و تریاژ می‌کند و آزمایشگاه فارتیک هم دارد ولی در آینده باید مراکز گوهر در بانک‌ها شکل بگیرد تا ماهر بتواند نقش اصلی خود را ایفا کند؛ یعنی به بانک بگوید چه کار کنند و حادثه را چگونه تریاژ کنند، نتایج را به ماهر بگویند. ما اکنون Red Team هم داریم درحالی که این تیم باید در لایه‌های مختلف سلسله مراتبی در بانک‌ها باشد.

مرکز ارائه خدمات امنیتی مدیریت‌شده

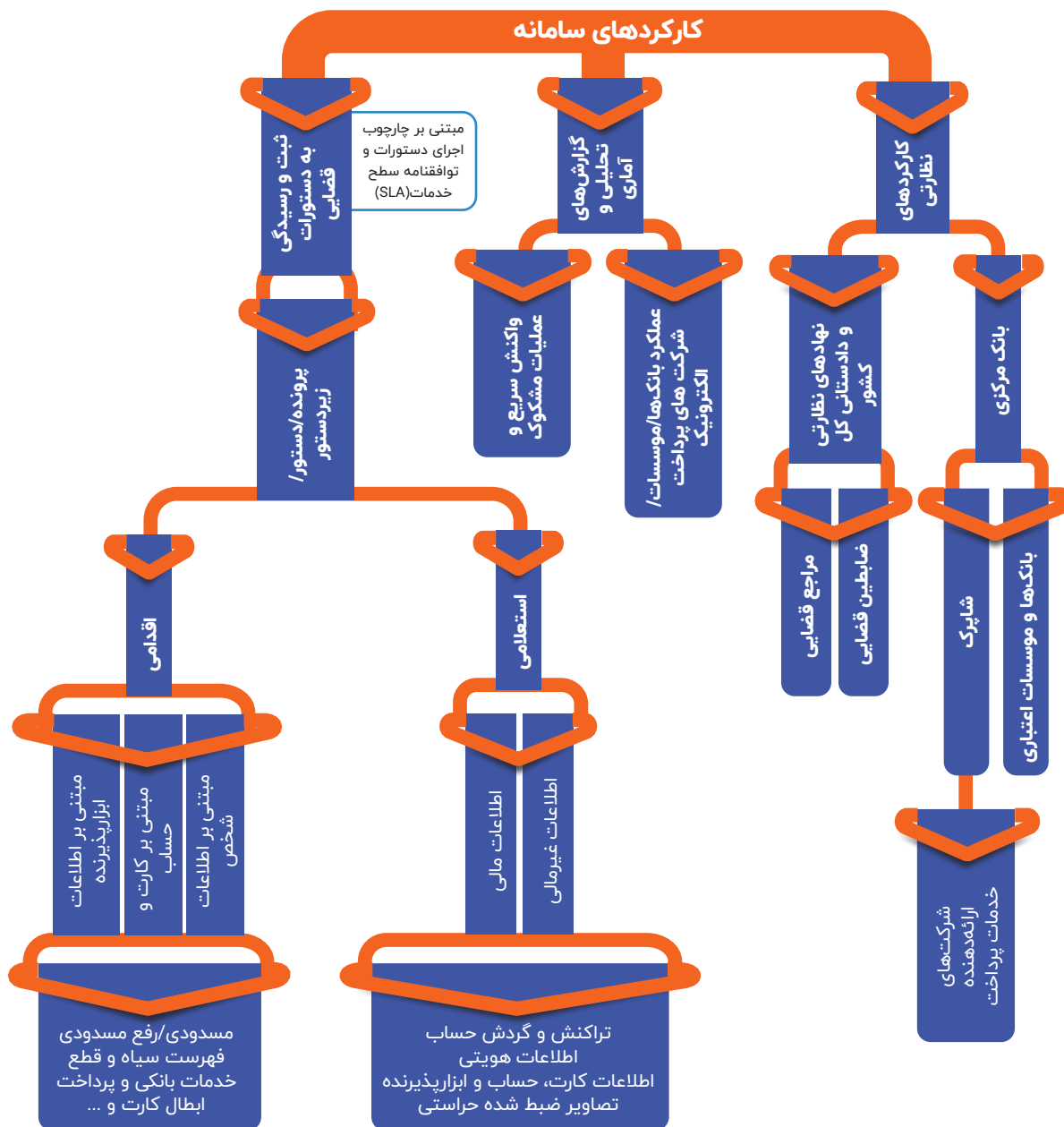
طبق مصوبه شورای پول و اعتبار، کاشف به‌عنوان اپراتور امنیت شبکه بانکی باید انجام وظیفه کند و بر اساس آن، ما می‌توانیم مرکز ارائه خدمات امنیتی مدیریت‌شده هم



آشنایی با سامانه سرآمد

سامانه رسیدگی آنی و مستمر دستورهای قضایی

ثبت کنندگان دستورات قضایی			
نهادهای حکومتی			
مراجع قضایی	مراجع و ضابطین قضایی		
	ضابطین قضایی		
	پلیس فتا	پلیس آگاهی	پلیس مبارزه با جرایم اقتصادی
بانک مرکزی		واکنش سریع	FIU عملیات مشکوک



■ ویژه‌نامه امنیت بانکداری ■ زمستان ۱۴۰۲ ■

زیرساخت



نظام، جایگاه معماری و انواع مراکز عملیات امنیت

مرکز عملیات امنیت (SOC) مجموعه‌ای از سامانه‌های نرم‌افزاری، سخت‌افزاری و کارشناسان خبره است که بر اساس رویه‌ای تعریف شده، مسئولیت تشخیص و فراهم‌سازی امکان پاسخگویی رودررو و / یا غیر رودررو با رخداد‌های امنیتی در حوزه خود را بر عهده دارد.

این مرکز ضمن رویارویی ناوابسته با رخداد‌های امنیتی شناخته‌شده، اطلاعات مربوط به رخداد‌های امنیتی پشتیبانی نشده رخداد‌های امنیتی که امکان رویارویی با آن‌ها در مرکز عملیات امنیت فراهم نشده باشد را به گروه گوهر مربوطه می‌فرستد و در مقابل رویه رویارویی با آن رخداد‌های امنیتی را از تیم گوهر دریافت و به صورت رودررو یا غیر رودررو اعمال می‌کند. مرکز عملیات امنیت مجموعه‌ای از سامانه‌های مدیریت ثبت رویداد همبستگی سنجی و پاسخگویی به رخداد‌ها است که برای یکپارچه‌سازی و ایجاد هماهنگی میان عناصر عملیاتی درگیر در تشخیص حمله‌ها و پاسخگویی به رخداد‌ها با استفاده از افراد خبره و روال‌های تعیین شده به تثبیت امنیت کمک مؤثری می‌کند. در ادامه این مقاله ابتدا جایگاه مراکز عملیات امنیت در سامانه افتا بیان می‌شود. سپس فناوری‌های کلیدی سامانه ملی عملیات امنیت در کشور، مشخص و در نهایت به معرفی ساختار و معماری مراکز عملیات امنیت و خدمات امنیتی مدیریت شده در فضای تبادل اطلاعات می‌پردازد.

در این مقاله بررسی کوتاهی از مفاهیم اولیه چرخه حیات و کاربردهای هوش تهدید سایبری انجام خواهیم داد و از آنجایی که به اشتراک گذاری هوش تهدید یکی از مهم‌ترین موضوعاتی است که در چرخه حیات آن مورد نظر است؛ لذا مزایا، چالش‌ها و استانداردهای آن نیز بررسی شده نهایتاً تحلیلی از جایگاه هوش تهدید سایبری در صنعت مالی ارائه می‌شود.

جایگاه مراکز عملیات امنیت

بر اساس اسناد بالادستی موجود در حوزه امنیت فضای تبادل اطلاعات، سامانه مراکز عملیات امنیت، یکی از سامانه‌های فرا بخشی حوزه امنیت فضای تبادل اطلاعات افتای کشور محسوب می‌شود که ارتباط بسیار نزدیکی با چهار سامانه فرا بخشی دیگر حوزه افتا دارد. این سامانه‌های فرا بخشی، عبارت‌اند از:

- ۱- سامانه تشخیص و رویارویی با رخداد‌های رایانه‌ای (سامانه پیشگیری، رویارویی و امداد افتا)
- ۲- سامانه ارزیابی و اعتبارسنجی محصولات و عرضه‌کنندگان خدمات افتا
- ۳- سامانه رویارویی با جرائم رایانه‌ای
- ۴- سامانه رویارویی با جاسوسی و تروریسم سایبری

بر این اساس، مراکز عملیات امنیت، اعتبار خود را از سامانه ارزیابی و اعتبارسنجی اخذ کرده و به عنوان واسط بین فضای تبادل اطلاعات (فضای مجازی) و سامانه تشخیص و رویارویی با رخداد‌های رایانه‌ای عمل می‌کنند. وظیفه اصلی این مراکز، تشخیص و رویارویی با حمله‌ها در فضای تبادل اطلاعات کشور و ممانعت از بروز رخداد‌های رایانه‌ای در اثر این نوع حمله‌ها است و برای تحقق این امر، رویارویی با حمله‌های شناخته‌شده را راساً و رویارویی با حمله‌های ناشناخته را پس از تحلیل و ارائه راهکار توسط سامانه تشخیص و رویارویی با رخداد‌های رایانه‌ای، انجام می‌دهند.

سامانه مراکز عملیات امنیت، همچنین حمله‌های تشخیص داده‌شده و ادله ثبت شده در این خصوص را برای بهره‌برداری، در اختیار دو سامانه رویارویی با جرائم رایانه‌ای و رویارویی با جاسوسی و تروریسم سایبری قرار می‌دهد. مؤلفه‌های مهم نظام ملی عملیات امنیت به منظور استقرار سامانه ملی عملیات امنیت در کشور، لازم است فناوری‌هایی مطابق با ساختار چهار لایه‌ای نمایش داده شده در شکل ۱ بومی شده و محصولات مرتبط با آن‌ها، تولید و عرضه شوند.

لایه اول: فناوری‌های تشخیص و پیشگیری از نفوذ؛ ابزار تشخیص و پیشگیری از نفوذ برای تشخیص حمله‌ها

حمله‌های تک‌مرحله‌ای، چندمرحله‌ای و توزیع‌شده و همچنین تشخیص و فراهم‌سازی امکان رویارویی مستقیم یا غیرمستقیم با رخدادهای امنیتی در حوزه قلمرو خود را بر عهده دارد. این مراکز ضمن، رویارویی مستقل با رخدادهای امنیتی شناخته‌شده، اطلاعات مربوط به رخدادهای امنیتی جدید (رخدادهای امنیتی که امکان رویارویی با آن‌ها در مرکز عملیات امنیت فراهم نشده باشد) را به تیم‌های گوهر مربوطه ارسال نکرده و در مقابل رویارویی با آن رخدادهای امنیتی را از تیم گوهر دریافت و به صورت مستقیم یا غیرمستقیم اعمال می‌کنند.

علاوه بر موارد فوق، تیم‌های گوهر دارای آزمایشگاه‌های بسیار مجهز در زمینه تشخیص آسیب‌پذیری‌ها، ارزیابی مخاطره‌ها و آزمایشگاه‌های مرتبط با جمع‌آوری ادله جرم می‌باشند.

لایه سوم: مراکز اشتراک‌گذاری و تحلیل اطلاعات و مرکز گردآوری، تحلیل و ادله جرم

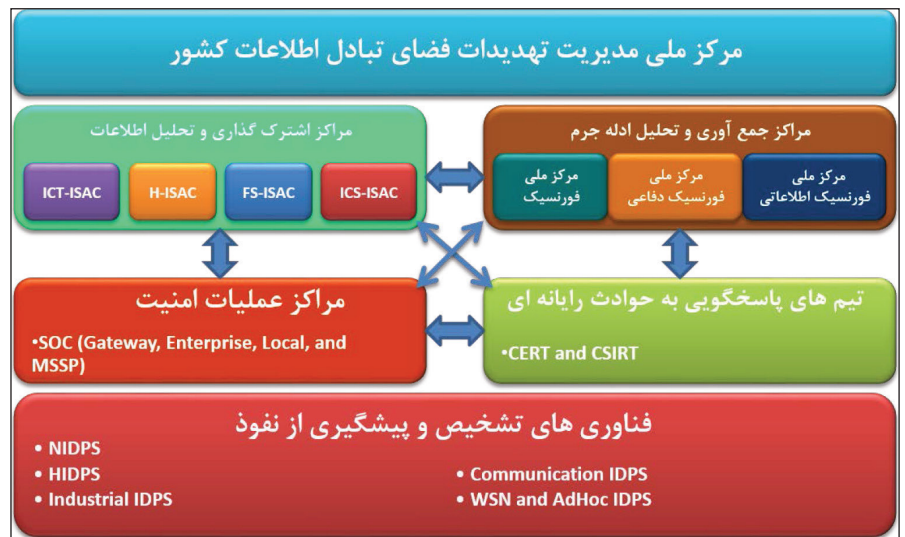
مرکز اشتراک‌گذاری و تحلیل اطلاعات^۴ یا به تعبیری لایه سوم، یک موجودیت عملیاتی است که عملیات گردآوری، تحلیل، نگهداری مناسب و انتشار اطلاعات مرتبط به حمله‌ها، رخدادهای آسیب‌پذیری‌ها و مخاطره‌های زیرساخت‌های حیاتی را به همراه قابلیت اعلان هشدار تهدیدات و گزارش دهی رخدادهای فراهم می‌کند. این مرکز توانایی کافی برای اشتراک‌گذاری اطلاعات درون قلمرو زیرساختی، بین قلمروها و حاکمیت و نیز ذینفعان حوزه خصوصی را دارد. این مراکز با تمامی مراکز عملیاتی امنیت کشور در حوزه خود شامل مراکز عملیات امنیت سازمانی، مراکز عملیات امنیت منطقه‌ای، مراکز گوهر و ماهر و ... به عنوان مجموعه‌ها یا از حسگرهای خود در ارتباط است و یک تصویر جامع از آسیب‌پذیری‌ها، نفوذها و رخدادهای امنیتی در سطح ملی ارائه می‌کند و مدیریت پاسخ به آن‌ها را بر عهده دارد.

لایه چهارم: مرکز ملی مدیریت تهدیدات فضای سایبری کشور

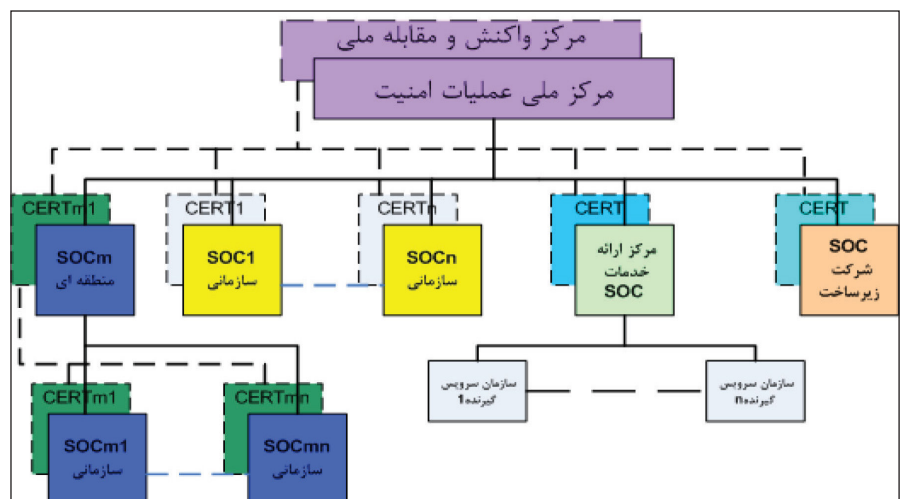
مرکز مدیریت تهدیدات و مخاطره‌های فضای تبادل اطلاعات کشور، مجموعه‌ها یا سامانه‌های نرم‌افزاری، سخت‌افزاری و کارشناسان خبره، جهت یکپارچه‌سازی و هماهنگی میان عناصر عملیاتی درگیر در امنیت فضای مجازی است. این مرکز وظیفه تعیین وضعیت سایبری، هدایت راهبردی، نظارت و هماهنگی پدافند سایبری افتا، پدافند غیرعامل، نظام رویارویی با تروریسم و جاسوسی سایبری و نظام رویارویی با جرائم سایبری را به منظور تشخیص یکپارچه، تحلیل متمرکز و واکنش سریع به حمله‌ها، مخاطره‌ها و رخدادهای امنیتی در سطح کشور بر عهده داشته و هدف اصلی آن تضمین تداوم امنیت اطلاعات و ارتباطات فضای مجازی شامل زیرساخت‌های ارتباطی کشور، شبکه اینترنت و شبکه ملی اطلاعات، شبکه دولت، شبکه بانک‌ها و سایر شبکه‌های سازمانی و منطقه‌ای داخلی است.

از طریق بررسی و تحلیل ترافیک و رویدادهای دریافتی به کار می‌روند. این ابزارها به دو دسته اصلی تقسیم می‌شوند. HIDPS و NIDPS که HIDPS ابزاری است که تشخیص حمله‌ها به یک میزبان خاص را بر عهده دارد و عمل حفاظت از داده‌های محلی آن میزبان را انجام می‌دهد، درحالی که IDPS یا HIDPS ابزار تشخیص و پیشگیری از نفوذ مبتنی بر شبکه است که ترافیک شبکه را پایش کرده و پروتکل‌های لایه‌های مختلف شبکه، انتقال و کاربرد را در جهت تشخیص فعالیت‌های ناهنجار و نفوذهای مهاجمین، تجزیه و تحلیل می‌کند.

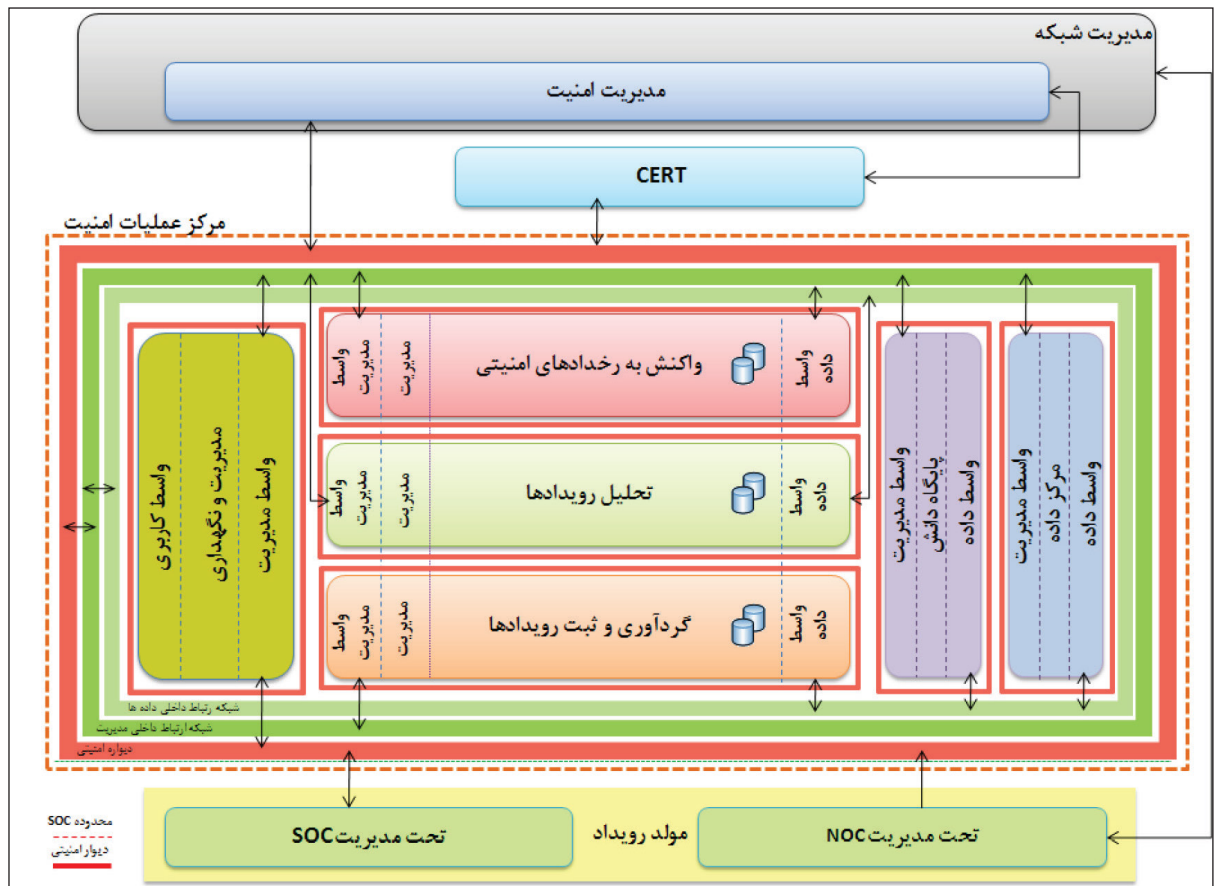
لایه دوم: مراکز عملیات امنیت و تیم‌های پاسخگویی به رخدادهای رایانه‌ای
مراکز عملیات امنیت مجموعه‌ای از سامانه‌های نرم‌افزاری، سخت‌افزاری و کارشناسان خبره است که بر اساس یک رویه تعریف‌شده مسئولیت تشخیص



شکل ۱- مؤلفه‌های مهم موردنیاز برای استقرار سامانه ملی عملیات امنیت



شکل ۲- انواع SOC و ارتباط آن‌ها با CERT



شکل ۳- معماری سیستمی مرکز عملیات امنیت

۳- الزامات فنی، اجرایی و امنیتی SOC

در حوزه مراکز عملیات امنیت، با توجه به جایگاه قرارگیری این مرکز، سه نوع مختلف آن تعریف شده است که شامل مرکز عملیات امنیت دروازه‌ای، سازمانی و منطقه‌ای است. در شکل ۲ ساختار قرارگیری آن‌ها آمده است:

این سه نوع از مراکز عملیات امنیت در زمانی که یک شبکه اختصاصی، یک سازمان یا مجموعه‌ای از شبکه‌ها نیازمند تأمین امنیت ارتباط خود هستند، انتخاب می‌شود. لازم به یادآوری است در زمانی که سازمان یا مؤسسه‌ای نخواهد برای نصب و راه‌اندازی یک مرکز عملیات امنیت هزینه‌ای صرف کند اما خواهان استفاده از خدمات SOC باشد، می‌تواند خدمات امنیتی مربوطه را از طریق یک مرکز عرضه خدمات امنیتی^۵ (MSSP) تأمین کند. در این صورت مرکز خدمات با یک CT-ISAC ارتباط خواهد داشت. در زمانی که یک شبکه خصوصی، یک شبکه پیرامونی (شبکه ملی)، ملزم به نصب و راه‌اندازی SOC سازمانی، دروازه‌ای و منطقه‌ای می‌شوند، متناسب با هر کدام از این مراکز، حسگرهای خاصی را استفاده کرده و از سیاست‌های امنیتی خاصی تبعیت می‌کنند. وظیفه و خدمت اصلی یک مرکز عملیات امنیت، مدیریت و پایش امنیت شبکه و خدمات حوزه قلمروی آن مرکز عملیات امنیت به صورت ۲۴ در ۷ در ۳۶۵ است.

این کار با پشتیبانی عملیاتی روزانه، مدیریت و نگهداری، به‌روزرسانی امضاها، مدیریت تغییرات و پیکربندی‌ها، نظارت و هشدار رخداد، حمله و تهدید، بررسی مخاطره‌پذیری امنیتی شبکه و سامانه‌ها و ارائه خدمت جمع‌آوری ادله جرم انجام می‌شود. به‌منظور انجام این وظایف توسط یک مرکز عملیات امنیت، الزاماتی (فنی، امنیتی، عملیاتی و اجرایی) به شبکه و سازمانی که استفاده‌کننده خدمات است، محول می‌شود که در ادامه این الزامات تشریح شده است. قبل از تشریح الزامات، معماری کلی یک مرکز عملیات امنیت ارائه می‌شود:

معماری ساختارمند مرکز عملیات امنیت

معماری ساختارمند مرکز عملیات امنیت در شکل ۳ نشان داده شده است. همانطوری که در این شکل دیده می‌شود واحدهای اصلی مرکز عملیات امنیت که در معماری عملیاتی به آن‌ها اشاره شد از طریق شبکه ارتباطات داخلی که با نوار سبز کمرنگ دیده می‌شود با یکدیگر ارتباط دارند. واسط داده‌ها در هر یک از واحدهای اصلی، وظیفه آماده‌سازی و تبدیل قالب اطلاعات، به فرمت قابل فهم در طرف مقابل را بر عهده دارد.

تمامی فرمان‌ها و اطلاعات مدیریت یا از طریق واسط مدیریت در هر واحد و از طریق شبکه داخلی مدیریت که

به رنگ سبز پررنگ نشان داده شده، با واحد مدیریت و نگهداری در تعامل است.

به علاوه به منظور امن سازی کلیه واحدها یک دیواره امنیتی برای هر یک از آنها تعبیه شده که آنها را در شکل با نوار سرخ رنگ باریک نشان داده ایم. ضمناً یک دیواره امنیتی، تمامی واحدهای مرکز عملیات امنیت را احاطه کرده است (نوار سرخ رنگ عریض) که امنیت ارتباطات خارجی را تضمین کند.

در ادامه، واحدها و وظایف آنها تشریح می شوند:

۱- واحد گردآوری و ثبت رویداد

با توجه به اینکه رویدادهای امنیتی شبکه در نقاط مختلفی از آن تولید می شوند، باید در یک نقطه مرکزی گردآوری شده و مکانیزمی برای انتقال آنها در نظر گرفته شود. پروتکل های انتقال رویداد، انجام این انتقال را هموار می سازند. تجهیزات یا منابع مولد رویداد در شبکه ممکن است از پروتکل های متفاوتی برای انتقال رویداد پشتیبانی کنند؛ بنابراین این واحد باید قابلیت توسعه برای پشتیبانی از پروتکل های گردآوری متفاوت را داشته باشد. این واحد، هشدارهای سامانه تشخیص نفوذ را دریافت کرده، ضمن نرمال سازی به واحد تحلیل و هم بسته سازی منتقل کرده و در بایگانی مرکزی نگهداری می کند. تمامی داده های موجود در مرکز عملیات امنیت، اعم از هشدارها، فرا هشدارها و رخدادها، گردآوری، تحلیل و رسیدگی می شوند و برای مدتی طولانی بایگانی و حفظ می شوند و امکان بازیابی و جستجو را هنگام نیاز فراهم می کند.

۲- واحد تحلیل و همبستگی سنجی

این واحد، وظیفه تحلیل و کشف ارتباط و همبسته سازی هشدارها و رخداد نماهای مختلف دریافت شده از واحد گردآوری و همچنین ثبت و تولید فرا هشدارهای متناظر آنها را بر عهده دارد. موتور همبستگی سنجی در مرکز عملیات امنیت، هشدارها و رخداد نماهای دریافتی از دستگاه های مختلف را در ساختار خود تجمیع، تحلیل و اولویت بندی نموده و حمله های شناسایی شده را در قالب تولید فرا هشدارهای متناسب گزارش می کند؛ بنابراین ارتباطات مختلف بین رخداد نماها و هشدارها که منجر به حمله شده اند، کشف شده و فرا هشدارهای لازم تولید خواهد شد. در نهایت فرا هشدارهای تولید شده به واحد واکنش ارسال می شوند. همچنین فرا هشدارها در بایگانی واحد گردآوری، ثبت و ذخیره می شوند.

۳- واحد واکنش و پاسخ به رخداد های امنیتی

واحد واکنش به رخداد های امنیتی وظیفه دارد فرا هشدارهای امنیتی ر بررسی کرده و در نهایت گزارش رخداد را تولید کند. در این واحد ابتدا فوریت رسیدگی به فرا هشدارهای امنیتی با استفاده از یک سامانه خبره تعیین می شود. سپس فرا هشدارهایی که رخداد تشخیص داده می شوند اولویت بندی و دسته بندی شده و بر اساس عواملی چون حساسیت و بیشینه زمان لازم برای رسیدگی

در صف زمان بندی قرار می گیرند. سپس این رخدادها وارد مرحله رسیدگی می شوند و بر اساس گردش کاری که برای آنها تعیین می شود، راهبرد رسیدگی به رخداد مشخص شده و پس از کسب مجوز، راهبرد به فرمان تبدیل شده و فرمان ها برای اجرا به مرکز عملیات شبکه یا تجهیزات شبکه ارسال می شود. در نهایت گزارش های مربوط به رخداد برای گروه های مرتبط فرستاده می شود. در تمامی مراحل تشخیص و رسیدگی به رخداد، یک سلسله درخواست و پاسخ با گروه های پایش، تحلیل و واکنش، امداد و جرم شناسی از طریق کنسول ردوبدل می شود. نتایج عملکرد واحد واکنش به رخداد های امنیتی در بایگانی واحد گردآوری و ثبت رویداد ذخیره می شود.

۴- واحد کنسول و درگاه ارتباطی

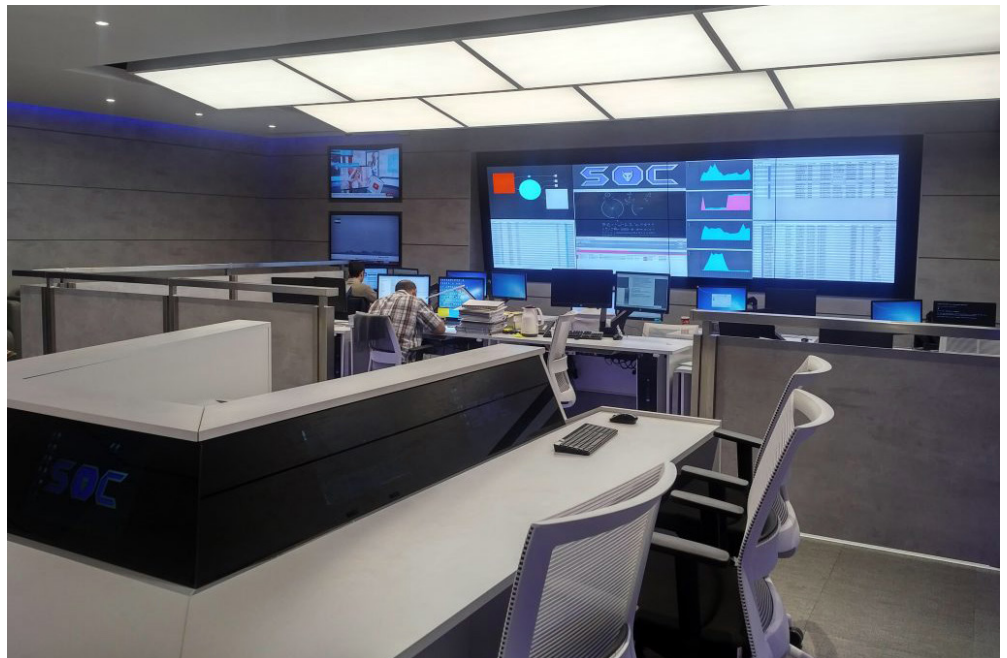
کنسول، واسطه ارتباطی سامانه با اجزای دیگر است. واحد کنسول با استفاده از زیر واحدهای کنسول در واحدهای دیگر خدمات را ارائه می دهد. هر زیر واحد برای یک گروه بیرونی خاص تعبیه شده است. زیر واحد نمایشگرها، اطلاعات لازم برای نمایش در نمایشگرهای پایگاه پایش را فراهم می کند. زیر واحد سازمان ها، کنسول ارتباطی سازمان های جامعه هدف با مرکز عملیات امنیت است. زیر واحد گزارش ها، ابزار پایگاه تحلیل و رویارویی برای ریشه یابی رخدادها محسوب می شود. زیر واحد اعمال، امکاناتی را به منظور پاسخ به رخدادها فراهم می کند. زیر واحد Ticketing رخداد های گزارش شده را به گروه پایش اطلاع داده، روال رسیدگی به آن توسط گروه پایش و تحلیل و رویارویی را کنترل می کند.

۵- واحد پایگاه دانش

پایگاه دانش مرکز عملیات امنیت واحدی است که وظیفه مدیریت دانش موجود در این مرکز را به عهده دارد. منظور از دانش در مرکز عملیات امنیت، اطلاعاتی است که واحدهای مختلف موجود در این مرکز به منظور انجام یکی از فرآیندهای گردآوری، تحلیل و رویارویی با رخداد های امنیتی به صورت دستی یا خودکار مورداستفاده قرار می دهند. این دانش نقطه اتکا واحدهای مختلف مرکز است؛ بنابراین باید درستی آن بررسی و ثابت شده باشد. واحد پایگاه دانش وظیفه مدیریت این دانش، اطمینان از درستی و عدم تناقض آن و مدیریت ارتباط اطلاعاتی میان واحدهای مختلف را به عهده دارد.

تعریف مرکز عرضه خدمات امنیتی مدیریت شده

در حالی که تنوع و پیچیدگی حمله های سایبری به صورت روزانه در حال تغییر است، تهدیدهای امنیتی که شبکه و دارایی های سازمان ها را هدف قرار می دهند نیز در حال گسترش است؛ بنابراین در این شرایط ضروری است که سازمان ها نسبت به تأمین امنیت اطلاعات خود حساسیت بیشتری نشان دهند. تصمیم گیری و سرمایه گذاری در حوزه امنیت در چارچوب مدیریت مخاطره ها قابل توجه است. در مدیریت مخاطره ها، نحوه برخورد با مخاطره، شامل پذیرش، کاهش یا اجتناب از وقوع آن مورد بررسی



قرار می‌گیرد. برون‌سپاری خدمات امنیتی، از طریق عقد قرارداد همکاری با مراکز ارائه خدمات امنیتی، امکان انتقال بار مسئولیت تشخیص و مواجهه با مخاطره‌های امنیتی را برای سازمان‌ها فراهم می‌کند. در این صورت درحالی‌که سازمان در قبال مخاطره‌های امنیت و کسب‌وکار مسئول است، در مدیریت مخاطره‌ها و روش برخورد با آن‌ها از همکاری و مشارکت یک مرکز تخصصی عرضه خدمات امنیتی بهره‌مند می‌شود.

مراکز عرضه خدمات امنیتی مدیریت شده^۷، بسته به توانایی‌های خود و نیاز بازار، خدمات متفاوتی ارائه می‌دهند. این خدمات طیف وسیعی را در برمی‌گیرد که مهم‌ترین آن‌ها در حوزه‌های زیر است:

■ مرکز عملیات امنیت

- تشخیص حمله‌ها، شناخت روند حمله‌ها، واکنش در مقابل حمله‌ها؛

- استقرار حسگرها، گردآوری داده‌ها و تحلیل داده‌ها؛

- پایش و تهیه گزارش‌های امنیت.

■ دفاع پیرامونی

- دفاع پیرامونی در مقابل حمله‌ها و تهدیدهای بیرون سازمان؛

نصب و راه‌اندازی تجهیزات Firewall-IDS/IPS

- پیکربندی امن تجهیزات ارتباطی بیرون سازمان مانند VPN و Router

■ امنیت نقاط پایانی

- رویارویی با تهدیدهای داخلی، کنترل میهمانان، کنترل دسترسی کاربران؛

- نصب و راه‌اندازی تجهیزات و راهکارها مانند ISE، VPN، VDI

■ مدیریت آسیب‌پذیری‌ها

- حفظ یکپارچگی، دفاع پیشگیرانه؛

- شناسایی و مدیریت آسیب‌پذیری‌ها (ارزیابی امنیت و آزمون نفوذپذیری به‌صورت دوره‌ای و مقاوم‌سازی) گارنتر خدمات مدیریت شده امنیتی را به این صورت تعریف می‌کند: «پایش یا مدیریت از راه دور فعالیت‌های امنیت فناوری اطلاعات، بدون استفاده از نیروی انسانی در محل ارائه خدمات و با استفاده از خدمات مشترکی که توسط مراکز عملیات امنیت از راه دور ارائه می‌شود.»

با استناد به این تعریف، خدمات امنیتی مدیریت شده، شامل ارائه نیروی متخصص در محل، مشاوره و توسعه راه‌حل‌ها یا خدمات نمی‌شود، هرچند ممکن است شرکت‌های بزرگ این خدمات را در کنار خدمات اصلی MSSP ارائه دهند. همچنین فعالیت اصلی مراکز ارائه مدیریت شده امنیت در حوزه فعالیت‌های SOC است و تأکید آن بر ارائه خدمات به مشتریان متفاوت، از راه دور است.

مرکز عرضه خدمات امنیتی مدیریت شده، با استفاده از مرکز عملیات امنیت با دسترسی پذیری بالا^۸ به مشتریان متفاوت، خدمات از راه دور و به صورت ۲۴ در ۷ ارائه می‌دهد. این خدمات در پنج دسته قابل تعریف است:

■ مدیریت رخدادها^۹

■ تشخیص حمله‌ها

■ پایش رخدادها

■ ارائه راهکار رسیدگی به رخداد

■ گزارش‌های امنیت

این خدمات به نحوی ارائه می‌شوند که موارد زیر را پوشش دهند:

■ **محرمانگی اطلاعات:** اطمینان از دسترسی افراد مجاز به اطلاعات و داده‌ها

■ **دسترسی پذیری:** اطمینان از دسترسی افراد مجاز به اطلاعات در زمان موردنظر و با روش مناسب

بر وضعیت امنیت سازمان خود مسلط باشد و درعین حال مسئولیت نگهداری از اطلاعات امنیتی و بهبود و ارتقای سطح امنیت سازمان را برون سپاری کند. در حقیقت، مشتریان یک بسته خدمات شامل خدمات امنیتی مدیریت شده‌ای که متناسب با نیازهای سازمان هدف است، از مرکز عرضه خدمات امنیتی مدیریت شده اجاره می‌کنند و در مقابل هزینه‌ای برای اجاره و دریافت خدمات پرداخت می‌کنند. اصطلاحاً مرکز عملیات امنیت به صورت چند اجاره‌ای^۳ اداره و مدیریت می‌شود. منابع خدماتی تخصیص داده شده به هر مشتری پس از پایان قرارداد آزاد شده و قابل تخصیص به یک مشتری دیگر است.

۲- حفاظت، تضمین تداوم و ارتقاء امنیت اطلاعات مطابق نیاز کارفرما
مرکز عرضه خدمات امنیتی مدیریت شده، با پایش شبکه کارفرما، نگهداری پایگاه دانش بر اساس دارایی‌های هر مشتری و تحلیل اطلاعات در مرکز عملیات امنیت، امکان تشخیص حمله‌ها، ارائه راهکار رسیدگی و سامان‌دهی روال‌های امنیتی برای کارفرما را فراهم می‌کند. تضمین تداوم ارائه خدمات، پشتیبانی و نگهداری، همچنین به روزرسانی دوره‌ها پایگاه دانش، تداوم و ارتقای امنیت اطلاعات را برای کارفرما فراهم می‌کند.

۳- مقیاس پذیر و انعطاف پذیر در نوع و میزان خدمات
مراکز عرضه خدمات مدیریت شده باید امکان ارائه خدمات قابل انتخاب را به مشتریان متنوع و دارای نیازهای متفاوت داشته باشند. همچنین در حوزه فعالیت مرکز عملیات امنیت، توجه به ویژگی‌های شبکه کارفرما و انتخاب پیکربندی مناسب برای پوشش نرخ داده ورودی، تنوع تجهیزات و بستر ذخیره‌سازی، بسیار حائز اهمیت است. مرکز عملیات امنیت که در مرکز عرضه خدمات امنیتی مدیریت شده استفاده می‌شود، از معماری مقیاس پذیر در سطوح مختلف عملیاتی بهره‌مند است؛ بنابراین امکان عرضه خدمات برای نرخ ورودی متفاوت، تجهیزات متنوع و حجم اطلاعات و دوره‌های ذخیره‌سازی متفاوت، بر اساس نیاز مشتری امکان پذیر است.

■ **یکپارچگی:** اطمینان از عدم تغییر اطلاعات ذخیره شده یا در حال انتقال
■ **انکارناپذیری:** اطمینان از عدم انکار به تولید یا تغییر اطلاعات توسط تولیدکننده یا تغییردهنده آن
■ **اصالت:** اطمینان از اصالت کاربر استفاده کننده از اطلاعات

ویژگی‌های مرکز عرضه خدمات امنیتی مدیریت شده برای تشریح ویژگی‌های مرکز ارائه خدمات امنیتی مدیریت شده لازم است از دریچه نگاه مشتری به این موضوع پرداخته شود. مهم‌ترین هدف از ایجاد مرکز ارائه خدمات مدیریت شده امنیت، کاهش هزینه مالکیت (TCO)^۱ برای سازمان‌ها و صنایع است. امنیت اطلاعات، کسب و کار اصلی اکثر سازمان‌ها نیست و از طرفی پیچیده‌تر شدن حمله‌های سایبری، موجب نیاز سازمان‌ها به کسب مهارت بیشتر و تخصیص نیروی مضاعف برای رویارویی با تهدیدهای امنیتی شده است. همچنین کسب و کارهای امروزی نیاز به تأمین مداوم امنیت به صورت ۲۴ در ۷ دارند که با منابع محدود سازمان به سختی قابل تحقق است؛ بنابراین سازمان‌ها در صورتی به مراکز عرضه خدمات مدیریت شده امنیت روی می‌آورند که علاوه بر مزیت‌هایی برای تحقق نیازهای امنیتی هزینه‌های جاری آن‌ها را نیز کاهش دهد.

بر این اساس، مهم‌ترین ویژگی‌هایی که مرکز عرضه خدمات امنیتی مدیریت شده باید داشته باشد عبارتند از:

۱- ارائه خدمات به واسطه عضویت، نه مالکیت
ایجاد یک مرکز عملیات امنیت درون سازمان‌ها مستلزم خرید تکنولوژی، آموزش نیروی متخصص و اجرای فرآیندهای عملیاتی متعددی است که از توان بسیاری از سازمان‌های متقاضی خدمات امنیتی فراتر است. مرکز عرضه خدمات امنیتی مدیریت شده، امکان ارائه خدمات در قبال پرداخت حق عضویت را به سازمان‌ها می‌دهد.

هزینه دریافت خدمات بر اساس خدمات عرضه شده و توافقنامه سطح خدمات^{۱۱} محاسبه می‌شود. مشتری می‌تواند با هزینه‌ای به مراتب کمتر از راه اندازی مرکز عملیات امنیت، از طریق دریافت گزارش‌های لحظه‌ای،

پی‌نوشت

- 1- Security Operations Center
- 2- Host Based Intrusion Detection and Prevention System
- 3- Network Intrusion Detection and Prevention System
- 4- Information Sharing and Analysis Center
- 5- Managed Security Service Provider
- 6- Risk management
- 7- Managed Security Service Provider (MSSP)
- 8- High availability
- 9- Log management
- 10- Total Cost of Ownership
- 11- Service Level Agreement (SLA)
- 12- Multi-tenant

آشنایی با هوش تهدید سایبری

هوش تهدید سایبری

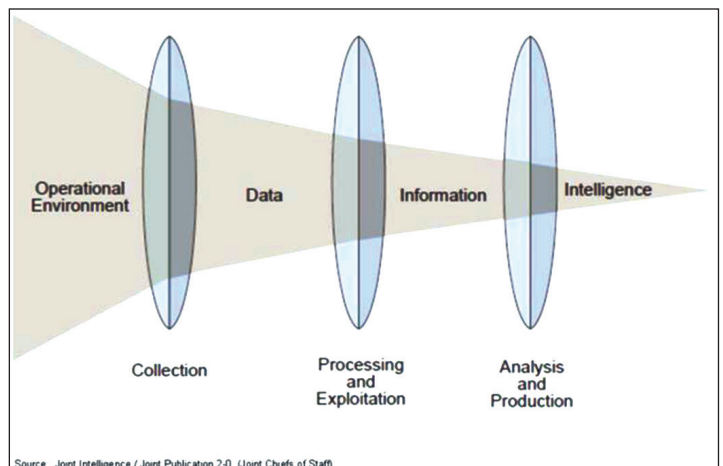
منبعی با پتانسیل ایجاد یک رخداد ناخواسته که ممکن است به سیستم با سازمانی آسیب برساند همچون حملات منع سرویس یا بدافزارهای مخرب تهدید نامیده می‌شوند. شناسایی به هنگام و ارزیابی صحیح تهدیدها یکی از پارامترهای موفقیت در مدیریت مخاطرات سازمان‌ها است. این موضوع هنگام مقابله با دشمن از اهمیت بیشتری برخوردار است به نحوی که معمولاً در رقابت‌ها و آوردگاه‌های مختلف بشری، کسی که از دانش بیشتری نسبت به دیگری برخوردار بوده برنده میدان شده است.

با این مقدمه هوش تهدید سایبری (Cyber Threat Intelligence: CTI) دانشی است بر پایه شواهد تهدید که در بردارنده وضعیت نشانگرها دلایل، سازوکارها، پیامدها و توصیه‌های قابل پیگیری در باره وجود یا به وجود آمدن خطر یا تهدیدی مرتبط با دارایی‌های سازمان است و می‌توان بر اساس دانش کسب شده اقدام یا تصمیم مناسبی را در پاسخ به تهدید به انجام رساند. در تعریفی دیگر با توجه به ارتباط بین داده اطلاعات و هوش (شکل ۱) هوش تهدید دانشی است که از استخراج و غنی شدن اطلاعات تهدید حاصل می‌شود. کیفیت هوش تهدید به ویژگی‌هایی همچون اولویت‌بندی به هنگام بودن ساخت‌یافتگی صحت و مرتبط بودن به سازمان، وابسته است.

دسته‌بندی‌های مختلفی از هوش تهدید همچون رسمی-غیررسمی، راهبردی-عملیاتی، راهبردی-تاکتیکی، راهبردی-عملیاتی-تاکتیکی-فنی شناسایی شده‌اند. اما گارتنر هوش تهدید را به دو دسته راهبردی و تاکتیکی به این نحو معرفی می‌کند.

هوش تهدید راهبردی: گزارش‌هایی قابل فهم که برای تشریح عوامل تهدید انگیزه‌ها تمایلات اهداف برنامه‌ها و کمپین‌های آن تولید می‌شوند. در حقیقت تولیدکننده و مصرف‌کننده این دسته از خروجی‌ها انسان است. این

گزارش‌های اخیر نشان‌دهنده آن است که پیچیدگی و خبرگی حملات سایبری رو به افزایش است عوامل تهدید در پنهان نمودن ردپای خود پیشرفته‌تر شده‌اند. بدافزارها قابلیت‌های گمنامی و رمزنگاری را اضافه کرده‌اند و هم‌زمان نگرانی از جنگ سایبری نیز بیشتر شده است. از طرفی بیشتر خبرگان امنیتی هم‌زمان هستند که دانستن و آگاهی بیشتر از تهدید می‌تواند به دفاع بهتر از سازمان‌ها کمک نماید. در این راستا هوش تهدید سایبری تلاش دارد تا با فراهم نمودن و به اشتراک‌گذاری به هنگام دانشی که بر پایه شواهد تهدید به دست می‌آید سازمان‌ها را در محافظت تشخیص و پاسخگویی به این تهدیدهای روزافزون یاری کند که به دو دسته راهبردی و فنی تقسیم می‌شوند. هوش تهدید راهبردی بیشتر انسان‌محور است و شامل گزارش‌هایی که در تصمیم‌گیری‌های ذاتا بلندمدت کاربرد دارد و هوش تهدید فنی ناظر است بر اطلاعاتی فنی از قبیل لیست IP‌های بدخواه که معمولاً در سیستم‌های اطلاعاتی استفاده می‌شوند. بر اساس مطالعه‌ای که توسط SANS در سال ۲۰۱۸ منتشر شده است. ۶۸ درصد پاسخ‌دهندگان از هوش تهدید سایبری استفاده می‌کنند و ۲۲ درصد نیز به کارگیری آن را در برنامه‌های آینده‌شان قرار داده‌اند. در این مقاله بررسی کوتاهی از مفاهیم اولیه چرخه حیات و کاربردهای هوش تهدید سایبری انجام خواهیم داد و از آنجایی که به اشتراک‌گذاری هوش تهدید یکی از مهم‌ترین موضوعاتی است که در چرخه حیات آن مورد نظر است؛ لذا مزایا، چالش‌ها و استانداردهای آن نیز بررسی شده نهایتاً تحلیلی از جایگاه هوش تهدید سایبری در صنعت مالی ارائه می‌شود.



شکل ۱- ارتباط بین داده، اطلاعات و هوش

آن بر تشخیص اولویت بندی اعلام هشدار و پاسخ سریع به رویدادهای امنیتی در سطح فنی و عملیاتی است. برای نمونه می توان به شناسایی آدرس کنترل فرمان (C&C) یک بدافزار و تغییر مورد نیاز در بیکر بندی تجهیزات امنیتی اشاره کرد. TTI را می توان به سه دسته نشانگرهای شبکه نشانگرهای میزبان و نشانگرهای رایانه تقسیم نمود. TTI اغلب توسط یک سیستم اطلاعاتی مشابه، SIEM، VM، WAP، UTM، IDPS یا EPP استفاده می شود که بیشتر تولیدکنندگان این محصولات ارائه فیدهای انحصاری خود را در دستور کار دارند نگاه نوین و متفاوت آن است که این محصولات، امکان استفاده از منابع مختلف TTI را در محصولات خود با به کارگیری استانداردهای به اشتراک گذاری اطلاعات تهدید فراهم کنند.

بر اساس مطالعه SANS در سال ۲۰۱۸ هوش تهدید سایبری برای اغلب سازمان های پاسخ دهنده مفید بوده است و تقریباً در تمامی مراحل فرآیندهای امنیتی سازمان کاربرد دارد و همان طور که در شکل ۲ مشاهده می شود بیشترین کاربرد سازمانی آن در تشخیص و ممانعت از حمله تهدید و پاسخگویی به رخداد است.

چرخه حیات هوش تهدید

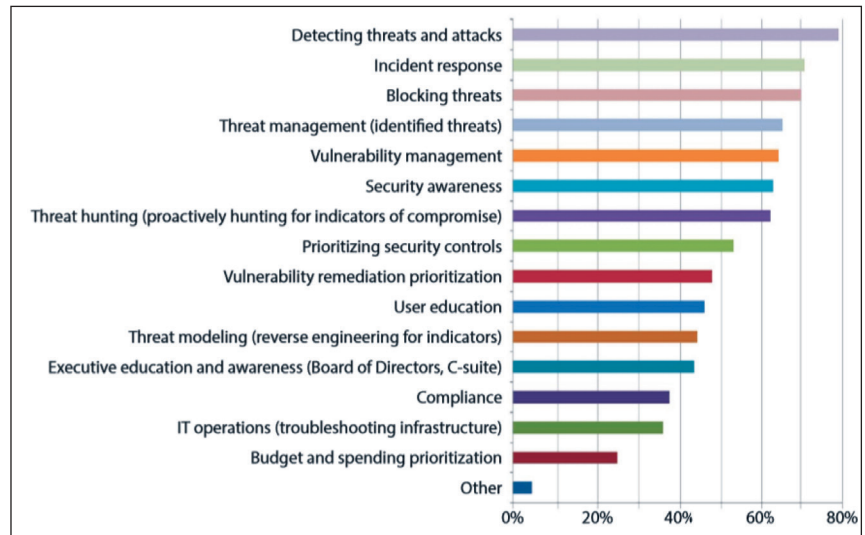
چرخه حیات هوش تهدید از سه مرحله اصلی فراهم سازی یا تولید، هم جوشی و انتشار هوش تهدید (شکل ۳) تشکیل می شود. اگر سازمانی بخواهد به سطح بلوغ در زمینه هوش تهدید برسد باید این چرخه را در سازمان ایجاد نماید. در این بخش مراحل کلان این چرخه را خیلی کوتاه توصیف می کنیم.

۱-۲ فراهم سازی یا تولید

در این مرحله فراهم سازی هوش تهدید از منبعی خارج از سازمان با ایجاد آن در داخل سازمان یا هر دو مدنظر است.

الف: فراهم سازی

منظور از فراهم سازی تهیه اطلاعات هوش تهدید تاکتیکی با راهبردی از منابع دیگری غیر از منابع داخل سازمان است که شامل استخراج از منابع متن منبع باز (OSINT) وبسایت های مرتبط با امنیت شبکه های اجتماعی و ...، خرید خدمت از فراهم کنندگان هوش تهدید، عضویت در انجمن ها و سازمان های متولی به اشتراک گذاری اطلاعات است. در اهمیت پایش OSINT جهت شناسایی تهدیدها به این مثال بسنده می شود که بر اساس پژوهش هایی که به عمل آمده است به طور میانگین اکسپلویت های جدید در روز قبل از آنکه به پایگاه داده ملی آمریکا (NVD) اضافه شود در شبکه تویتر منتشر می شوند.



شکل ۲. کاربردهای هوش تهدید در سازمان



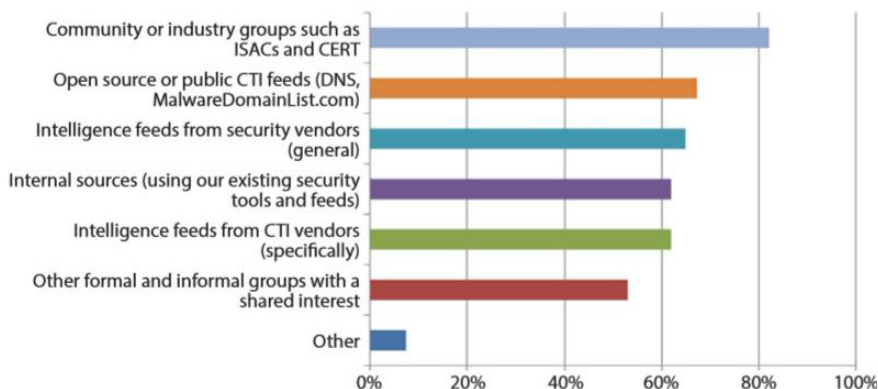
Source: Gartner (September 2016)

شکل ۳. چرخه حیات هوش تهدید

نوع از هوش معمولاً برای تصمیم های بلندمدت همچون تدوین برنامه ها و فرایندهای جدید امنیتی اعمال تغییرات و سرمایه گذاری در زیرساخت ها استفاده می شود. به عنوان مثال گزارشی تحلیلی که رشد حملات فیشینگ را در صنعت پرداخت با انتشار از طریق برنامه های موبایلی در شبکه های اجتماعی در دوره زمانی مشخصی نشان می دهد می تواند منجر به ایجاد سازوکارهای امنیتی جدید در روش های پرداخت شود.

هوش تهدید تاکتیکی (TTI): این دسته شامل

اطلاعات تهدید از جنس فنی است مشابه آدرس های IP یا دامنه های مخرب فهرست های درهم ساز بدافزارها آدرس های فیشینگ و دیگر اطلاعاتی که معمولاً ناظر به یک سیستم اطلاعاتی است و معمولاً فید نامیده می شوند. هوش تاکتیکی معمولاً با تصمیم هایی که ماهیت کوتاه مدت دارند برای نمونه دقیقه با ساعت مرتبط بوده. تمرکز



شکل ۴- مهم‌ترین منابع سازمان‌ها در خدمات هوش تهدید

در دستور کار قرار می‌گیرد. همچنین به اشتراک‌گذاری هوش تهدید با انجمن‌ها با سازمان‌های متولی دیگر نیز در این مرحله انجام خواهد شد.

بدیهی است که با توجه به مأموریت ابعاد میزان امنیت موردنیاز و برخی چالش‌ها و موانع توسعه کارآمد CTI همچون کارکنان کم‌تجربه و کمبود دانش فنی بودجه و زمان عدم امکان خودکارسازی و یکپارچه‌سازی و غیره ([۳]) پیاده‌سازی چرخه حیات CTI در هر سازمانی متفاوت خواهد بود. در این راستا گارتر متریس بلوغ تجارب هوش تهدید را در پنج سطح و از جنبه‌های ابزار کارکنان، منابع، فرآیندها و موارد کاربرد پیشنهاد کرده است.

جایگاه هوش تهدید در ساختارهای امنیت سازمان

مطالعه SANS نشان می‌دهد که نزدیک به ۴۳ درصد سازمان‌های پاسخگو از تیم رسمی CTI سود می‌برند. همچنین کارمندی که در این حوزه فعالیت می‌کنند به ترتیب ۵۳ درصد در مراکز عملیات امنیت، ۲۶ درصد در تیم‌های پاسخگویی به رخداد و ۳۲ درصد نیز در دیگر گروه‌های امنیتی حضور دارند. گارتر پیش‌بینی کرده است که تا سال ۲۰۲۰ نیمی از مراکز عملیات امنیت با اضافه کردن قابلیت‌های هوش تهدید و پاسخگویی به رخداد به SOC‌های مدرن تبدیل شوند با توجه به گزارش‌های مذکور و با نگاهی به مدل‌های مختلف مراکز عملیات امنیت به نظر می‌رسد که SOC به دلیل تجمیع اطلاعات رویدادها و رخدادهای داخلی سازمان‌ها محل مناسبی برای ایجاد چرخه حیات هوش تهدید در یک سازمان است. همچنین گارتر ۵ مدل SOC شامل مجازی، چندمنظوره، ترکیبی، اختصاصی و فرماندهی به شرح زیر معرفی کرده است و

ب: تولید

هوش تهدید به معنای آن است که سازمانی با استفاده از داده‌ها و اطلاعات در دسترس از منابع و زیرساخت‌ها و خدمات‌های اقدام به شناسایی و تولید اطلاعات هوش تاکتیکی با راهبردی نماید. منابع مورد استفاده شامل داده‌های شبکه همچون تجهیزات و امنیت شبکه و سیستم‌های پایش داده میزبان‌ها، همچون رویدادهای سیستم عامل و برنامه‌های کاربردی آنتی‌ویروس‌ها و مرورگرهای وب و دیگر منابع همچون SIEM‌ها، فرایندها و سیستم‌های گزارش‌دهی رخداد، ابزارهای فارتیک، خروجی تحلیل‌های باینری و مهندسی معکوس و ابزارهای کوزه‌عسل باشد.

در شکل ۴ مهم‌ترین منابع مورد استفاده در سازمان‌ها برای فراهم‌سازی با ایجاد CTI در مطالعه SANS نشان داده شده‌اند. مشاهده می‌شود که اغلب سازمان‌ها از گروه‌ها یا انجمن‌هایی همچون ISAC یا CERT سود می‌برند.

۳-۱ هم‌جوشی

هدف از مرحله هم‌جوشی تحلیل اطلاعات تهدید گردآوری شده جهت استخراج هوش تهدیدی با کیفیت‌تر و مرتبط‌تر است که خود از مراحل دیگری شامل مجتمع سازی، پاک‌سازی (ذخیره‌سازی، به‌نحوی که امکان جستجو فراهم شود)، غنی‌سازی (برای نمونه آدرس IP مشکوک و با استفاده از Whois اطلاعات بیشتری از آن فراهم شود)، همبسته‌سازی (مرتبط کردن المان‌های مختلف تهدید به یکدیگر است برای نمونه برقراری ارتباط یک IP مشکوک به URL بدافزار و حتی کمپین مربوطه)، اعتبارسنجی (مقایسه اطلاعات با اطلاعات دیگر منابع و همچنین فهرست‌های سفید و سیاه موجود می‌تواند به حذف یا اطمینان از صحت اطلاعات کمک نماید)، اولویت‌بندی (بر اساس اعتماد به منابع مرتبط بودن با مشاهدات، رخدادها و حوادث پیشین، اولویت‌بندی انجام می‌شود) و زمینه‌سازی برای استفاده نهایی از هوش تهدید ارتباط بین اطلاعات استخراج شده با دارایی‌های سازمان مشاهدات و رخدادها داخلی تعیین می‌شود) تشکیل شده است.

۴-۱ انتشار

در این مرحله اطلاعات هوش تهدید برای استفاده از ابزارهای امنیتی با برنامه ریزان و مدیران تصمیم‌گیر در سازمان منتشر می‌شود که بر اساس آن سلسله کارهایی همچون پیش‌بینی پیشگیری تشخیص و پاسخگویی

از فیدهای خریداری شده در محصولات استفاده می کنند. در سطح ۲ نیز فعالیت های هوش تهدید به کارکنان امنیتی تخصیص داده می شود. در سطح ۳ کارکنان تمام وقتی در تیم SOC یا CSIRT برای فعالیت های هوش تهدید در نظر گرفته می شوند و در سطح ۴ بلوغ تیمی اختصاصی در SOC با ایجاد نقش تحلیلگر تهدید به وجود می آید. نهایتاً در سطح پنجم از بلوغ هوش تهدید تیمی مستقل و متناظر با SOC با عنوان تیم هوش تهدید یا مرکزی با نام «مرکز هم جوشی هوش تهدید» ایجاد می شود.

به اشتراک گذاری اطلاعات تهدید

در هر مجموعه ای تهدیدهای مشترکی هستند که با پیش آمدن رخداد برای یکی از اعضاء. احتمال وقوع تهدید مشابه برای دیگر اعضای مجموعه بالاتر خواهد رفت. از طرفی با توجه به گستردگی و پیچیدگی تهدیدها که عاملان آن با انگیزه های مختلف سیاسی، اقتصادی، مالی و تروریستی، امنیت سازمان ها را به چالش می کشند و با عنایت به محدودیت منابع و بودجه های امنیتی سازمان ها، همکاری در تولید و به اشتراک گذاری اطلاعات هوش تهدید سایبری خصوصاً در هر بخش از صنعت ضروری به نظر می رسد که در چرخه حیات هوش تهدید نیز در مراحل فراهم سازی و انتشار به این موضوع توجه می شود. تصور نمایید که بانکی موفق به شناسایی آدرس C&C یک بدافزار

همان طور که دیده می شود در این دسته بندی فراهم سازی خدمات هوش تهدید و ارائه آگاهی آتی جزء خصوصیات اصلی SOC های مدل فرماندهی است:

- مدل مجازی برای سازمان های کوچک و معمولاً با راهبرد برون سپاری به یک MSSP است.

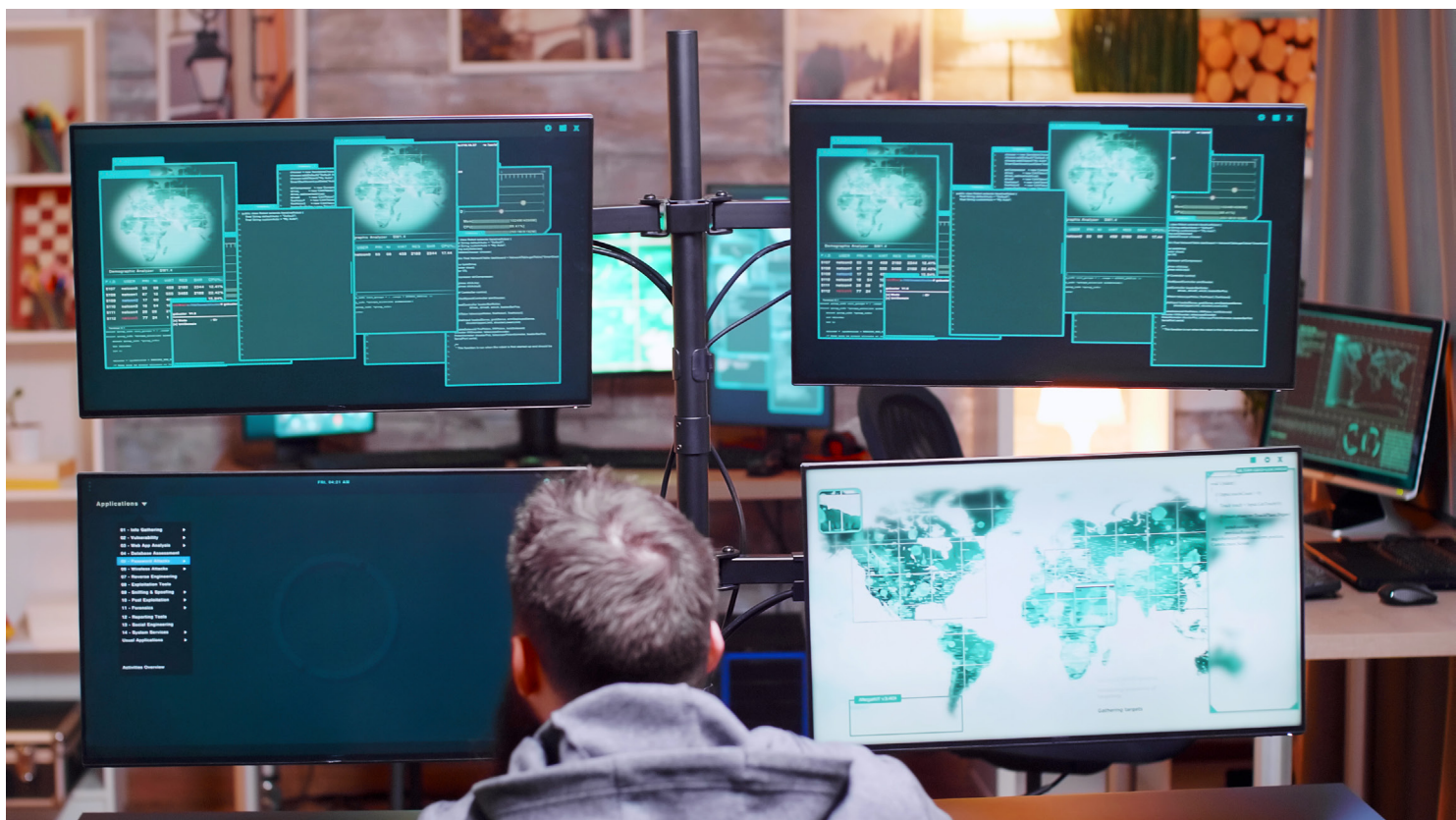
- مدل چندمنظوره برای سازمان های کوچک متوسط و بزرگی که دارای مخاطره پایین است کاربرد دارد و معمولاً کارکردهای امنیتی توسط تیم های عملیات آتی همچون NOC انجام می شوند؛

- مدل ترکیبی برای سازمان های کوچک و متوسط توصیه می شود که تیم امنیتی اختصاصی یا نیمه اختصاصی با همکاری یک MSSP یا دیگر واحدهای عملیات سازمان فعالیت های مورد نظر را انجام خواهد داد؛

- مدل اختصاصی نیز برای سازمان هایی با مقیاس بزرگ مخاطره بالا یا فراهم کنندگان خدمات توصیه می شود که کاملاً درون سپاری با امکانات اختصاصی است؛

- مدل فرماندهی نیز برای سازمان های حاکمیتی، نظامی، فراهم کنندگان خدمت یا سازمان هایی با ابعاد بسیار بزرگ توصیه شده و معمولاً هماهنگی بین SOC های دیگر را بر عهده دارد.

همچنین اگر با نگاه بلوغ فرآیندی به سازمان دهی هوش تهدید نگریسته شود می بینیم که معمولاً سازمان ها در سطح ۱ دارای کارکنانی مختص هوش تهدید نیستند و فقط



مناسب اهمیت دارد.

به اشتراک گذاری اطلاعات تهدید با محدودیتها و چالش‌هایی نیز مواجه است که می‌تواند باعث مشارکت نکردن اعضا در یک انجمن شود که برخی از مهم‌ترین آن‌ها به شرح زیر هستند:

■ بیم اعضاء از رعایت نشدن گمنامی و تأثیر منفی احتمالی بر کسب‌وکار یا سودجویی رقیب یکی از چالش‌های مهم این بحث است.

■ در برخی موارد، سازمان‌ها در اینکه چه اطلاعاتی محرمانه است و نباید آن‌ها را طبق قوانین بالادستی به اشتراک بگذارند. ابهام دارند.

■ کیفیت خدمات هوش تهدید چالش دیگری است که در همکاری و جلب مشارکت اهمیت دارد. برای نمونه در هوش تهدید، تاکنیکی برخی از فیدها تاریخ اعتبار کوتاهی دارند و برخی نیز ممکن است که تنها برای یک هدف مشخص استفاده شوند، برای نمونه IP‌های بات‌های قربانی با آدرس C&C یک بات نت که ممکن است به سرعت توسط مهاجم تغییر یابد؛ بنابراین، از یک طرف سرعت به اشتراک گذاری مطرح است و از طرف دیگر اعتبارسنجی که فرایند تحلیل را زمان‌بر می‌نماید.

■ مشارکت نکردن برخی اعضاء در یک گروه می‌تواند در مشارکت دیگر اعضا تأثیرگذار باشد که اینجا نیز، راهکارهای پاداش محور یا تنبیه محور دو رویکرد برای حل این مشکل هستند.

■ بی‌آنکه از الگوریتم‌های هوش مصنوعی و ابزارهای مناسب استفاده شود فرایند تحلیل داده‌های حجیم نیز امری دشوار است و نیازمند استفاده از این الگوریتم‌ها در چرخه حیات هوش تهدید سایبری است.

با توجه به دلایل پیش گفته در یک حوزه مشخص قابل اعتماد و با رعایت سیاست‌های امنیتی به اشتراک گذاری اطلاعات هوش تهدید سایبری رویکردی قابل توجه است و مزایای مختلفی از قبیل افزایش چابکی بهره‌گیری از آگاهی‌های درجا غنی شدن هوش تهدید بلوغ دانش و تجارب جمعی را در بر خواهد داشت.

استانداردهای به اشتراک‌گذاری اطلاعات

تهدید

نیازهایی همچون امکان تحلیل با رویکرد مشارکت محور ایجاد پایگاه دانش تهدید و خودکارسازی به اشتراک گذاری اطلاعات تهدید. افزایش کارایی و قابلیت‌های پاسخگویی به رخداد مهم‌ترین دلایل توسعه استانداردهای به اشتراک‌گذاری اطلاعات تهدید است. استانداردهایی مانند: OpenIOC (ساختاری برای ارائه هوش فنی) و IODEFS (استانداردی برای به اشتراک‌گذاشتن اطلاعات رخداد در تیم‌های CSIRT)، CyBox (برای توصیف مشاهدات)، MAEC (زبانی ساخت یافته برای گردآوری و به اشتراک‌گذاری اطلاعات بدافزارها)، CAPEC

یا تجربه یک حمله منع سرویس توزیع شده (DDoS) با استفاده از تجهیزات امنیتی خود شده است. این بانک با به اشتراک‌گذاری به هنگام اطلاعات تهدید می‌تواند اثرات احتمالی وقوع مجدد رخدادی مشابه را در صنعت بانکی کشور کاهش دهد.

در ادامه برخی از تیم‌ها، سازمان‌ها و شرکت‌هایی که در به اشتراک‌گذاری اطلاعات تهدید سایبری فعال هستند. معرفی می‌شود.

■ تیم‌های پاسخگویی به رخدادهای سایبری (CSIRTs): یکی از وظایف تیم‌های پاسخگویی به رخدادهای، گردآوری و به اشتراک‌گذاری اطلاعات تهدید با ذی‌نفعان است. CSIRT با توجه به حوزه مأموریتشان می‌توانند سازمانی، بخشی، ملی یا حتی بین‌المللی باشند.

■ مراکز تحلیل و به اشتراک‌گذاری اطلاعات (ISACs): ISACها مراکزی غیرانتفاعی هستند که رسمی یا دستور ریاست. جمهوری آمریکا در سال ۱۹۹۸ باهدف گردآوری تحلیل و انتشار اطلاعات تهدید در بخش خصوصی ایالات متحده تشکیل شد و همچنین تبادل اطلاعات دوطرفه بین بخش خصوصی و دولتی را نیز بر عهده گرفت. بدیهی است که این مراکز تنها در ایالات متحده کاربرد دارند و کشورهای دیگر نیز بر اساس سیاست‌های خویش نهادهای مشابهی را برنامه‌ریزی می‌کنند.

■ سازمان تحلیل و به اشتراک‌گذاری اطلاعات (ISAO) در سال ۲۰۱۵ به دلیل رشد تهدیدها و همچنین به دلیل آن‌ها

■ ISACها نمی‌توانستند به تمامی شرکت‌ها و سازمان‌های آمریکا پوشش دهند فرمانی برای ایجاد ISAO صادر شده است.

■ استاد راهنمایی برای ایجاد چنین سازمان‌هایی با ذکر قابلیت‌ها و خدمات مورد انتظار آن‌ها ارائه کرده است.

■ فراهم‌کنندگان خدمات و محصولات هوش تهدید خدمات و محصولات هوش تهدید توسط برخی شرکت‌های تجاری ارائه می‌شود که نوع و سطح خدمات آن‌ها بسیار متنوع است. در ادامه نمونه‌هایی

از این خدمات با ذکر نام یک شرکت در مقابل آن معرفی می‌شوند: تشخیص فیشینگ (PhishMe)،

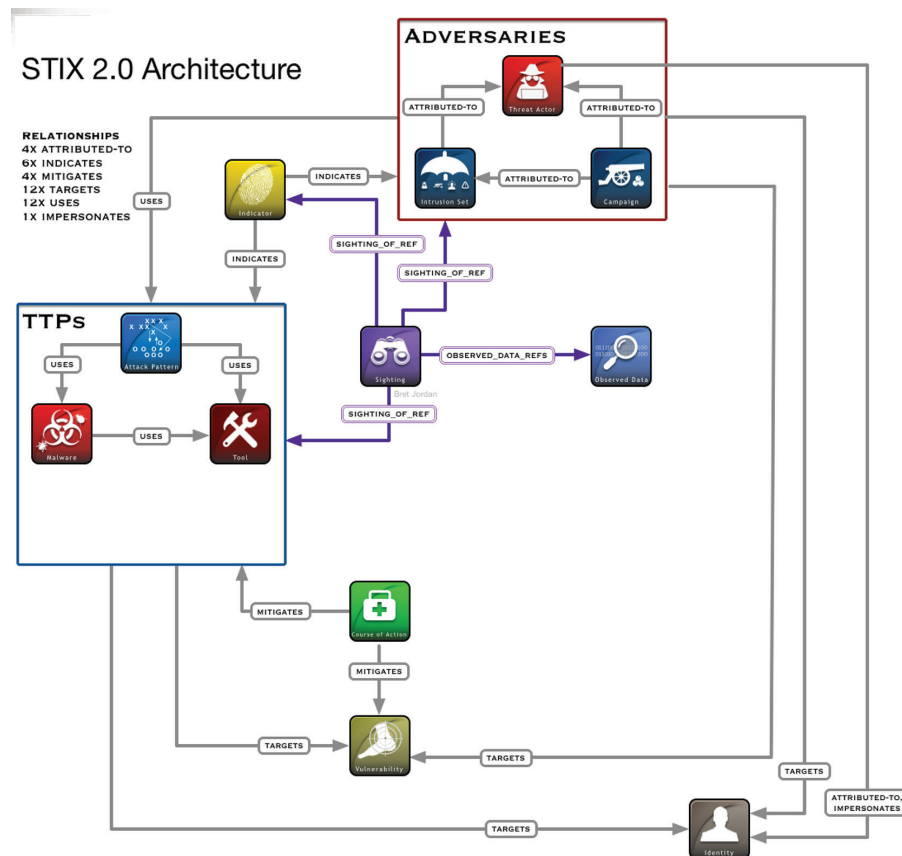
پایش شبکه‌های اجتماعی (Recorded Future)، اولویت‌بندی آسیب‌پذیری‌ها با توجه به شرایط سازمان

(Kenna Security)، پایش برند (BrandProtect)، پایش وب عمیق و تاریک باهدف ارائه هشدارهای پیش

از وقوع یا آگاهی‌های درجا (Digital Shadows)، شناسایی برنامه‌های جعلی (PhishLab)، رصد تهدید

و پاسخگویی به رخداد (iSight). در این راستا بررسی پارامترهای مختلفی همچون گستره پوشش تهدیدها

عمق و دقت قابلیت توسعه محدود جغرافیایی با حوزه کسب‌وکار سطوح دانش و تجربه در انتخاب فراهم‌کننده



شکل ۵

الگوی حمله: تاکتیک‌ها فن‌ها و رویه‌هایی (TTP) است که روش‌های دشمن برای به مخاطره انداختن یک هدف را توصیف می‌نماید.

کمپین: گروهی از رفتارهای خصمانه که بیانگر مجموعه حملات با فعالیت‌های مخرب علیه یک هدف مشخص در بازه زمانی معینی است و معمولاً دارای اهدافی کاملاً تعریف شده است.

سلسله کار: سلسله فعالیت‌هایی که برای جلوگیری با پاسخ به حمله انجام می‌شود.

هویت: می‌تواند معرف افراد سازمان‌ها و گروه‌های حقیقی یا دسته‌هایی از افراد سازمان‌ها و گروه‌ها، برای نمونه: بخش مالی باشد.

نشانه‌گر: نشانه‌گرها شامل الگویی هستند که برای تشخیص فعالیت‌های مشکوک و یا مخرب به کار می‌روند.

مجموعه نفوذ: مجموعه‌ای گروه‌بندی شده از رفتارهای خصمانه و منابعی با مشخصات مشترک که به‌یقین توسط یک سازمان (عامل تهدید برنامه‌ریزی شده باشد). یک مجموعه نفوذ ممکن است شامل کمپین‌های متعدد و آیا فعالیت‌های دیگری که همگی به‌واسطه خصوصیت

(پایگاه دانشی از الگوی حملات) و STIX-TAXII برخی از مهم‌ترین تلاش‌ها در این حوزه به شمار می‌روند. STIX زبانی برای توصیف اطلاعات هوش تهدید و TAXII نیز قرارداد لایه برنامه‌کاربردی برای تبادل CTI روی https هست که اخیراً نسخه دوم آن توسط OASIS منتشر شد. این استاندارد با وجود پیچیدگی در پیاده‌سازی از مقبولیت برخوردار بوده و بسیاری از استانداردها و را در درون خود جای می‌دهد که بیانگر جامعیت آن است. همچنین به نظر می‌رسد که STIX/TAXII مثال بارزی از هوش تهدید ماشین خوانا (MRTI۴۱) است که امکان به اشتراک‌گذاری خودکار اطلاعات تهدید را فراهم می‌نماید که توسط تعداد و طیف قابل قبولی از فروشندگان محصولات امنیتی و مراکز ISAC پشتیبانی می‌شود. STIX زبانی مبتنی بر گراف بوده و مهم‌ترین مزیت آن انطباق با رویکردهای تحلیلی است که امکان ارائه‌ای سازگار انعطاف‌پذیر ساخت‌یافته و پیمانه‌ای از اطلاعات هوش تهدید را فراهم می‌کند. این استاندارد از ۱۲ شیء دامنه که هر شیء دارای مشخصات و ارتباطی در گراف است تشکیل می‌شود. توصیفی مختصر از این اشیاء در ذیل آمده است:



بدافزارها، این ابزارها و آيا بسته‌های نرم‌افزار روی سیستم‌ها یافت می‌شود و اهداف قانونی برای کاربران دارند.

آسیب‌پذیری: اشتباهی در نرم‌افزار که ممکن است هکر به‌موجب آن به سیستم با شبکه دسترسی یابد.

شکل ۵ معماری STIX 2.0 را که بیانگر ارتباط بین اشیاء است، نشان می‌دهد.

به‌طورکلی گارنتر به سازمان‌ها توصیه می‌نماید که هنگام خرید محصولات امنیتی قابلیت استانداردهای باز هوش تهدید در نظر گرفته شود. و حتی فراتر از آن به فروشندگان محصول برای اضافه کردن چنین قابلیت‌های فشار آورده شود

سکوهای هوش تهدید

گسترده‌گی و پیچیدگی حملات سایبری و به دنبال آن حجم عظیمی از اطلاعات که در منابع مختلف تهدید منتشر می‌شوند از یک طرف و از طرف دیگر نیاز به اشتراک‌گذاری خودکار و به‌هنگام اطلاعات تهدید و یکپارچه‌سازی آن با دیگر محصولات امنیتی برخی پیشران‌های تولید ابزارهایی همچون سکوهای هوش تهدید (TIP) برای جایگزینی روش‌های سنتی تبادل اطلاعات شده است. TIP بنا دارد که سازمان‌ها را در چرخه حیات هوش تهدید شامل

مشترکی که نشانگر یک عامل تهدید است و به هم مرتبط هستند. باشد.

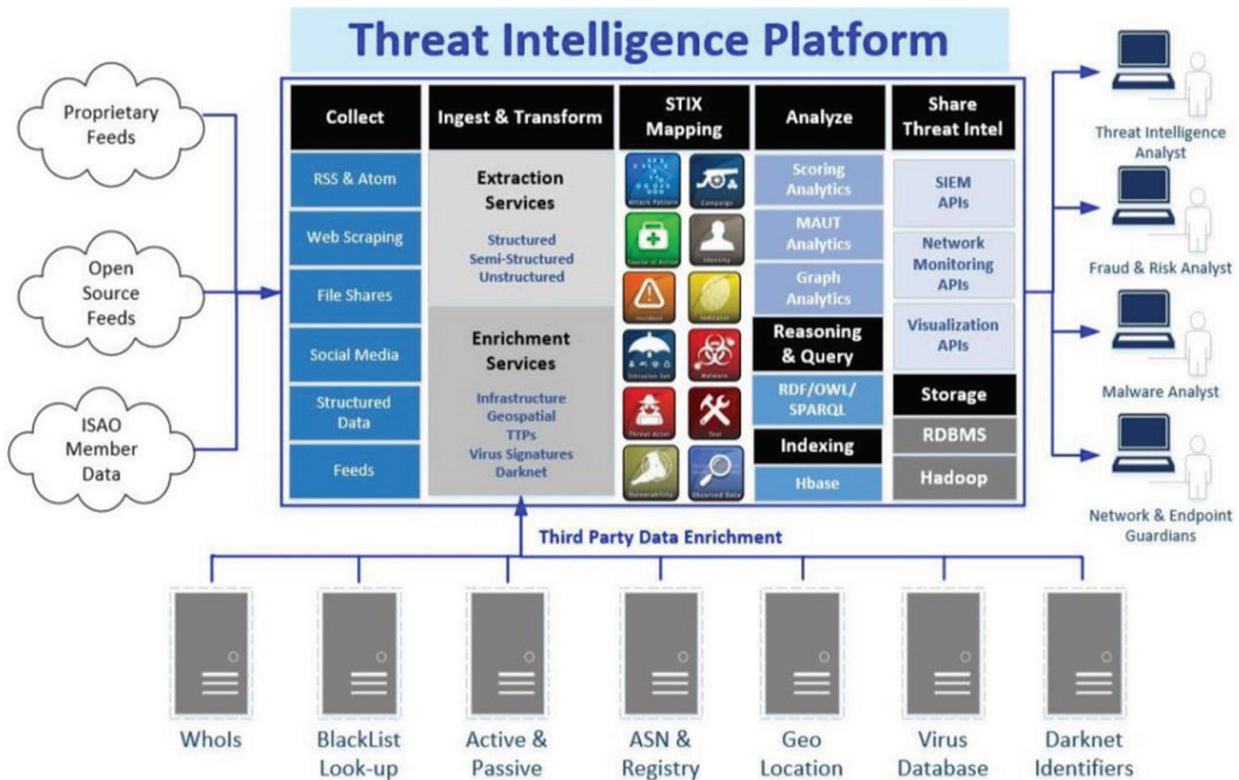
بدافزار: نوعی از TTP که با نام‌های کد مخرب و نرم‌افزار مخرب نیز شناخته می‌شود.

داده دیده‌شده: بیانگر اطلاعاتی است که روی سیستم‌عامل‌ها و شبکه‌ها دیده‌شده است مانند آدرس IP اتصال به شبکه فایل و یا کلیدهای رجیستری

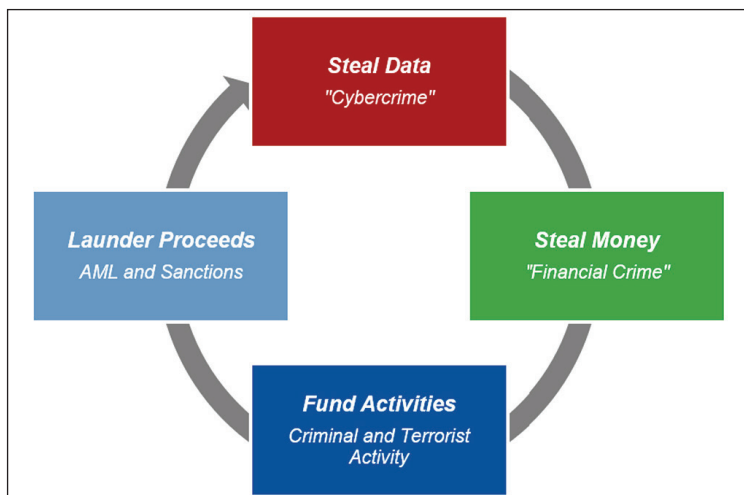
گزارش: برای گروه‌بندی و تهیه روایتی از تهدید سایبری جامع استفاده می‌شود و مجموعه‌ای از هوش تهدید است که روی یک یا چند موضوع متمرکز است. مانند توصیف یک عامل تهدید بدافزار یا فن حمله با سایر جزئیات مرتبط

عامل تهدید: افراد گروه‌ها و سازمان‌های حقیقی که به‌یقین اعمالی با اهداف تخریبی انجام می‌دهند. عامل تهدید است. عامل تهدید یک مجموعه نفوذ «نیست ولی ممکن است آن‌ها را در طول زمان پشتیبانی یا با آن‌ها همکاری کند. عامل تهدید منابع خود و احتمالاً منابع مجموعه نفوذ را برای انجام حمله و اجرای کمپین علیه اهداف به کار می‌برد.

ابزار: نرم‌افزارهای قانونی که ممکن است توسط عاملین تهدید برای انجام حملات به کار برده شوند. برخلاف



شکل ۶- سکوی هوش تهدید ایدئال



شکل ۷- چرخه حملات کلاهبرداری مالی

گردآوری پاک‌سازی غنی‌سازی تحلیل و انتشار کمک کند. براساس بررسی‌های SANS، میزان ۵۷درصد پاسخ‌دهندگان از TIP استفاده می‌کنند که ۱۷درصد نسبت به پارسال رشد داشته است. همچنین طبق همین مطالعه، استفاده از ابزارهای دیگری همچون SIEMها و سکوهایی فارتزیک برای گردآوری و مدیریت هوش تهدید نیز پرکاربرد است. محصولات Threatelligence

، ThreatConnect، CRITS، TruSTAR، MISP Looking Glass، EclecticIQ، نمونه‌ای از این سکوها است که برخی متن‌باز و برخی تجاری هستند. در شکل ۶ قابلیت‌های یک سکوی هوش تهدید ایدئال نمایش داده شده است.

به‌تازگی مطالعه‌ای درباره TIP توسط ENISA منتشر شده است و ضمن برشمردن قابلیت‌های آن

گردآوری پاک‌سازی غنی‌سازی تحلیل و انتشار کمک کند. براساس بررسی‌های SANS، میزان ۵۷درصد پاسخ‌دهندگان از TIP استفاده می‌کنند که ۱۷درصد نسبت به پارسال رشد داشته است. همچنین طبق همین مطالعه، استفاده از ابزارهای دیگری همچون SIEMها و سکوهایی فارتزیک برای گردآوری و مدیریت هوش تهدید نیز پرکاربرد است. محصولات Threatelligence

FinCERT بانک مرکزی روسیه نیز اقدام به هماهنگی در پاسخگویی به رخدادها در نظام بانکی می‌نماید که فعالیت آن در همین راستا ارزیابی می‌شود. همچنین بررسی‌های گارت‌تر در تعامل با فراهم‌کنندگان خدمات هوش تهدید تجاری نشان می‌دهد که مشتری سنتی آن‌ها دولت و بخش مالی است؛ هرچند که این مشتریان استفاده از گروه‌هایی مشابه FS-ISAC را مفیدتر و ارزان‌تر ارزیابی کرده‌اند. از طرف دیگر گویا فناوری نیز تلاش خود را برای همگرایی راهکارهای مقابله با تهدیدهای سایبری و مالی به انجام خواهد رساند و شاید به همین دلیل است که برخی از ارائه‌کنندگان خدمات هوش تهدید، همچون IntSights و RSA، Threat Metrix، TruSTAR گردآوری هوش تهدید سایبری در کنار فیدهای کلاهبرداری مالی را در خدمات و محصولات خود قرار داده‌اند و برخی از آن‌ها نسل آینده هوش تهدید را برای خدمات خود برگزیده‌اند و سطح پیشرفته‌ای از خدمات خود را که با کسب‌وکار مرتبط است به هوش کلاهبرداری تعبیر می‌کنند.

جمع‌بندی و نتیجه‌گیری

هوش تهدید سایبری دانشی بر پایه شواهد تهدید از قبیل الگوی حمله عامل تهدید کمپین ابزارها نشانگر آسیب‌پذیری ... است که با بهره‌گیری از آن سازمان‌ها در تمامی مراحل چرخه حیات حمله اعم از پیش‌بینی جلوگیری تشخیص و پاسخگویی به هنگام توانمندتر خواهند شد. همچنین CTI می‌تواند مؤسسات مالی را افزون بر مدیریت تهدیدهای سایبری در مدیریت کلاهبرداری مالی نیز یاری کند. بنابراین وجود چرخه حیات CTI شامل فراهم‌سازی با تولید هم‌جوشی و انتشار در مؤسسات مالی و اعتباری با تمرکز بر مدیریت داده مشارکت محور و منسجم و با همکاری تیم‌های مختلف امنیتی شامل تهدید سایبری کلاهبرداری و ضد پول‌شویی توصیه می‌شود. همچنین با توجه به آن که شاید استفاده از خدمات CTI شرکت‌های تجاری و انجمن‌های خارجی به دلایل امنیتی و حتی کارایی با محدودیت همراه خواهد بود ایجاد مراکز هوش تهدید سایبری با مراکز به اشتراک‌گذاری اطلاعات تهدید با مشخصات کسب‌وکاری موردنیاز زیست‌بوم بانکی کشور با بهره‌گیری از مراکز عملیات امنیت سلسله مراتبی ضروری به نظر می‌رسد در این راستا شرکت‌های خصوصی نیز با بررسی کسب‌وکارهای مشابه می‌توانند خدمات و محصولات هوش تهدید همچون تشخیص فیشینگ پایش شبکه‌های اجتماعی و وب عمیق و تاریک، سکوها هوش تهدید ارائه گزارش‌های راهبردی و فیدهای فنی و غیره را در برنامه‌های خود قرار دهند و با به‌کارگیری استانداردهای بازی مشابه STIX/TAXII در محصولات امنیتی خود زیرساخت‌های لازم برای به اشتراک‌گذاری و استفاده از هوش تهدید ماشین خوانا را فراهم کنند.

یادآوری کرده است که هم‌اینک این ابزارهای نوپدید محدودیت‌هایی نیز دارند که برخی از مهم‌ترین آن‌ها شامل موارد زیر است. بیشتر این محصولات بر گردآوری داده تمرکز دارند و قابلیت‌هایشان برای فازهای هم‌جوشی و تحلیل محدود است. بیشتر سکوها هوش تهدید کنونی بر هوش فنی تمرکز یافته‌اند و کمتر به دیگر زمینه‌های هوش تهدید توجه دارند که علت آن پیاده‌سازی نادرست استانداردهایی همچون STIX است و در برابر برخی تولیدکنندگان محدودیت‌های این استانداردها را دلیل این امر می‌دانند.

هوش تهدید سایبری در صنعت مالی

آمارها بیانگر آن هستند که افزون بر تهدیدهای سایبری تعداد و پیچیدگی حملات کلاهبرداری مالی نیز رو به افزایش است. رشد ۱۳۵ درصدی فروش داده‌های بانکی در بازار وب تاریخ رشد ۹۱ درصدی حمله فیشینگ برای آدرس‌های رایانامه متعلق به بانک‌ها و افزایش ۱۴۹ درصدی دزدیده شدن اطلاعات کارت‌های اعتباری نمونه‌ای از این آمارها است. حال پرسش اینجا است که آیا تهدید سایبری با کلاهبرداری مالی در صنعت پرداخت مرتبط است؟ پاسخ آن است که چرخه حملات کلاهبرداری مالی شکل (۷) بیشتر با جرائم سایبری در دیدن داده‌های با ارزش شروع می‌شود و با جرائم مالی، دزدیدن پول، فعالیت‌های مجرمانه تروریستی و پول‌شویی ادامه می‌یابد. عملاً تهدیدهای سایبری پیشرفته همچون حملات فیشینگ و بدافزارهای موبایلی مشابه اسلحه‌ای در فرآیند کلاهبرداری مالی استفاده می‌شود.

با توجه به آن‌که در شرایط حاضر عمدتاً ابزارها، فناوری‌ها و ساختار مدیریتی تشخیص و پیشگیری از کلاهبرداری با امنیت سایبری مجزا است و روش‌های مذکور بیشتر برپایش تراکنش متمرکز است؛ بنابراین کلاه‌برداران می‌توانند از این شکاف استفاده کنند. در این راستا، توسعه کرانه‌های راهکارهای تشخیص و جلوگیری از کلاهبرداری و ارتباط آن با دیگر حوزه‌های امنیتی رقم خورده است و توصیه می‌شود که مدیران مخاطره و امنیتی سازمان‌های مالی بر مدیریت داده با نگاه مشارکت محور و منسجم و بر همکاری تیم‌های مختلف امنیتی شامل تیم‌های تهدید سایبری کلاهبرداری و ضد پول‌شویی تمرکز کنند. در این حال مستقل از آنکه یک فناوری یکپارچه برای تشخیص حملات سایبری و کلاهبرداری ایجاد شود. هوش تهدید سایبری می‌تواند مؤسسات مالی را در تشخیص و مانعیت از کلاهبرداری‌های مالی که در چرخه آن‌ها از حملات سایبری استفاده می‌شود. بازی کند.

FS-ISAC در بخش خدمات مالی آمریکا و SWIFT ISAC در حوزه زیرساخت‌های سوئیفت نمونه‌ای از تلاش‌ها در ایجاد مراکز هوش تهدید در بخش مالی است. افزون بر آن CSIRT‌های برخی بانک‌های مرکزی همچون

■ ویژه‌نامه امنیت بانکداری ■ زمستان ۱۴۰۲ ■

مورد کاوی





ریکاردو فریرا

سرپرست بخش امنیت اطلاعات شرکت فوریت

سیر تکامل امنیت سایبری در بانکداری

تحولات بانکداری در پیوند با نوآوری‌های دیجیتالی، خطرات بی‌سابقه‌ای را برای امنیت سایبری به همراه داشته است. همان‌طور که در گزارش‌های اخیر مشخص شده، حوادث سایبری می‌توانند عملکردهای کلیدی اکوسیستم مالی را مختل کنند، بنابراین مدیریت ریسک و تکیه بر پروتکل‌های شبکه ایمن بسیار مهم است. از آنجایی که مجرمان سایبری بی‌وقفه به دنبال سودجویی هستند، نقض داده‌ها بیشتر و پیچیده‌تر شده و آسیب‌پذیری بخش بانکی را بیش از پیش نمایان می‌سازد.

رویکردهای قانون‌گذاری، مانند EU DORA یا G7 و گزارش‌های رسیده از سایر بانک‌های مرکزی و رگولاتورها، بر اهمیت حیاتی انعطاف‌پذیری سایبری در بخش بانکداری تأکید می‌کنند. این نوع قوانین و مقررات، اقداماتی واکنشی در برابر تهدیدات قدیمی و استراتژی‌های پیشگیرانه برای پیش‌بینی و کاهش خطرات آینده هستند. تداوم سیر دیجیتالی‌سازی، افزایش وابستگی به طرف‌های سوم و تنش‌های ژئوپلیتیکی نشان می‌دهد که چشم‌انداز در حال تحول تهدیدات سایبری نیازمند پاسخی قوی از سوی مؤسسات مالی است.

ارزهای دیجیتال بانک مرکزی (CBDC) لایه دیگری بر این پیچیدگی اضافه می‌کنند. هم‌زمان با افزایش تراکنش CBDCها، فرصت‌هایی برای شمولیت مالی و نیز چالش‌های امنیت سایبری به وجود می‌آید.

زیان مالی در برابر حملات سایبری هستند و درعین حال، تقاضا برای بیمه سایبری از عرضه پیشی خواهد گرفت.

ارزش امنیت سایبری برای بخش بانکداری

مؤسسات مالی برای اینکه در این محیط رقابتی و انعطاف پذیر باقی بمانند، باید به مسیر نوآوری ادامه دهند و اطمینان حاصل کنند که این نوآوری ها از ایمنی لازم برخوردارند. دو روی سکه تأمین امنیت، با توجه به گسترش سطح حمله - که ناشی از ظهور بانکداری دیجیتال، اخلاکگران فین تک و معرفی CBDC ها و مدرن سازی سیستم های محوری آن هاست - چالش برانگیزتر می شود. الزامات کلیدی امنیت سایبری برای بانکداری عبارت اند از:

■ **پایش:** رصد همیشگی و جامع شبکه با گسترش بانکداری تلفن همراه، اینترنت اشیا و استقرار ابر بسیار مهم است. از آنجایی که چشم انداز تهدیدات سایبری پیچیده تر می شود، رصد شفاف تمام فعالیت های شبکه برای جلوگیری از نقض اطلاعات و مدیریت خطرات امنیت سایبری بسیار مهم است.

■ **اتوماسیون و کارآمدی عملیاتی:** دوران راه حل های چندگانه و مجزا در حال رنگ باختن است. امنیت سایبری مدرن، مستلزم راهکارهای یکپارچه ای است که بتواند با توسعه اتوماسیون، نیاز به تنظیمات دستی و نظارت مداوم را کاهش دهد. پیاده سازی policy as code می تواند این فرایند را ساده تر کرده و تضمین کند که خطمشی های امنیتی به طور مداوم و خودکار در سراسر شبکه امن اجرا می شوند.

■ **انعطاف پذیری:** ساختار متنوع فناوری اطلاعات که شامل استقرار در محل و چند ابری است، به کنترل ها و خطمشی های امنیتی بسیار سریع نیاز دارد. همان طور که مؤسسات مالی پیچیدگی های تحول دیجیتال را تجربه می کنند، راه حل های امنیتی آن ها، از جمله policy as code، باید قابل انطباق بوده و تضمین کنند که خطمشی های امنیتی با تغییرات زیرساخت ها هماهنگ هستند.

■ **گزارش انطباق:** انطباق با مقررات رگولاتوری فقط یک تمرین و علامت زدن موارد نیست. بنا بر تأکید بانک های مرکزی و سایر مقامات ناظر بر مقررات انعطاف پذیری سایبری، تیم های امنیتی باید بین پایبندی به این مقررات و دفاع فعالانه در برابر تهدیدات سایبری تعادل برقرار کنند. به کارگیری policy as code نیز می تواند به کمک کدگذاری و اتوماسیون بررسی های خطمشی به تضمین انطباق کمک کند.

در نهایت، عنصر انسانی را نمی توان نادیده گرفت. وراي استفاده از فناوری پیشرفته، مؤسسات مالی به متخصصان ماهری نیاز دارند که بتوانند از پتانسیل پلتفرم ها و سیستم های جدید استفاده کنند. محدود بودن متخصصان در حوزه های خاص و نیز دانش ناکافی در درک محصولات، فرایندها و سیستم های پیچیده چالش های بیشتری را ایجاد می کند.

مثلا شرکت فورتی نت برای حل این مشکل، یکی از بزرگ ترین و گسترده ترین برنامه های آموزشی در صنعت

در این چشم انداز رقابتی، جایی که بانک های سنتی، اخلاکگران فناوری مالی و بانک های دیجیتال رقیب بومی برای سهم بازار تلاش می کنند، ارائه یک تجربه دیجیتالی یکپارچه بسیار مهم است. با این حال، مؤسسات در حالی که برای دستیابی به نوآوری رقابت می کنند نباید از آسیب پذیری های بالقوه غافل شوند. پذیرش فناوری های دیجیتال یک ضرورت است، اما اطمینان از اینکه چنین فناوری هایی توانایی مقابله با تهدیدات همیشگی در حال تکامل را دارند نیز بسیار مهم است.

افزایش ریسک سایبری برای بانکها

از آنجایی که بانک ها و ارائه دهندگان خدمات مالی در مسیر رشد و نوآوری قرار دارند، اتخاذ یک رویکرد جامع در جهت امنیت سایبری که بر اساس آخرین معیارهای مقرراتی و اطلاعات تهدیدات شکل گرفته باشد، برای اطمینان از پیشرفت پایدار و ایمن بسیار مهم خواهد بود.

امنیت سایبری در بانکداری

در چشم انداز بانکداری دیجیتال که به سرعت در حال تحول است، تیم های امنیت سایبری در خط مقدم یک نبرد پیچیده قرار دارند. مخصوصاً بخش مالی در برابر تهدیدات سایبری، از جمله نقض قابل توجه داده ها، آسیب پذیر است. بخش مالی، هدف محبوب تبهکارانی است که به دنبال سودجویی مالی، راز و رمزهای تجارت یا اختلال آفرینی در خدمات هستند که در نهایت به تبلیغات اجتماعی یا سیاسی منجر می شود. بر اساس گزارش جدید اینتریل، جرائم مالی و سایبری در حال حاضر مهم ترین نگرانی سیاست های جهانی است.

بسته به شدت حمله و بانک خاص هدف گرفته شده، یک نقض داده موفقیت آمیز می تواند منجر به آسیب جدی به برند شود. بر اساس گزارش آژانس امنیت سایبری اتحادیه اروپا (ENISA)، ماهانه بیش از ۱۰ ترابایت داده به سرقت می رود و بیش از ۶۰ درصد سازمان ها ممکن است با درخواست های باج روبرو شده باشند. گزارش دیگری نشان می دهد که در سال ۲۰۲۲ وسیع ترین هک رمزرها روی داده است.

از آنجایی که دیجیتالی سازی در صنعت بانکداری به یک ضرورت تبدیل شده، هم زمان با آن خطرات امنیتی نیز افزایش می یابد و تیم های اجرایی باید از انعطاف پذیری عملکردهای تجاری خود، انطباق با مقررات دولتی و صنعتی و اثربخشی زیرساخت های امنیت سایبری خود برای محافظت از سطح حمله در حال گسترش اطمینان حاصل کنند.

ارائه دهندگان خدمات مالی باید بتوانند در برابر هجوم نقض داده ها، باج افزارها، بدافزارها، حملات فیشینگ و حملات مهندسی اجتماعی که رشد چشمگیری در پیچیدگی، تکرار و شدت داشته اند از خود دفاع کنند. چالش های مقابله با تهدیدات با گسترش سطح حمله به لحاظ وسعت و پیچیدگی، افزایش می یابد. گزارشی در چشم انداز جهانی ریسک سایبری، بیان می کند که رگولاتورها و بیمه گران در حال انجام اقداماتی برای کاهش



صندوق بین‌المللی پول تصویر نگران‌کننده‌ای از چشم‌انداز نظارتی ترسیم می‌کند. این نظرسنجی با پوشش ۵۱ کشور، نتایج زیر را نشان داد:

■ ۵۶ درصد از بانک‌های مرکزی یا مقامات نظارتی فاقد استراتژی ملی سایبری اختصاصی برای بخش مالی هستند.

■ ۴۲ درصد فاقد مقررات خاص امنیت سایبری یا مدیریت ریسک هستند و در کمال تعجب ۶۸ درصد، فاقد بخش تخصصی مدیریت ریسک در بخش نظارتی خود هستند.

■ ۶۴ درصد دستورالعملی در خصوص حوادث امنیت سایبری ارائه نداده و آزمون و بررسی را اجباری نکرده‌اند.

■ ۵۴ درصد فاقد نظام یا سیستم اختصاصی برای گزارش حوادث سایبری هستند.

■ ۴۸ درصد فاقد مقررات خاص در مورد جرائم سایبری هستند.

در حالی که این آمار ممکن است تصویری تیره‌وتار ارائه دهد، ضروری است که مقررات و الزامات امنیتی را به جای محدودیت، به‌عنوان کاتالیزوری برای نوآوری و مدیریت ریسک در نظر بگیریم. به‌عنوان مثال، مک‌کنزی با برجسته‌سازی پتانسیل تجزیه‌وتحلیل داده‌ها در بانکداری، بر این باور است که نتایج این تحلیل‌ها می‌تواند تا سالانه یک میلیارد دلار برای برخی از بانک‌های بزرگ، به کاهش هزینه مدیریت ریسک منجر شود. این صرفه‌جویی‌ها شامل کاهش جریمه‌ها، بالا رفتن دقت گزارش انطباق، مدیریت بهینه داده‌های حساس و کاهش خطرات مختلف دیگر است.

از آنجایی که بخش بانکداری به تکامل دیجیتالی خود ادامه می‌دهد، ایجاد تعادل بین نوآوری، تهدیدات امنیت سایبری و انطباق با مقررات بسیار مهم خواهد بود. پذیرش این فاکتورهای سه‌گانه می‌تواند فرصت‌های بی‌سابقه‌ای را ایجاد کند تا یک چشم‌انداز مالی ایمن، سازگار و آینده‌نگر تضمین شود.

را ارائه داد و متعهد شد که تا سال ۲۰۲۶ یک میلیون نفر را تحت آموزش قرار دهد تا شکاف مهارت‌های مرتبط با امنیت سایبری کاهش یابد. سایر مشارکت‌های استراتژیک شامل همکاری با مجمع جهانی اقتصاد برای ارائه دوره‌های آموزشی از طریق مرکز آموزشی امنیت سایبری است.

همان‌طور که بخش بانکداری به سیر دیجیتالی خود ادامه می‌دهد، اتخاذ رویکردی جامع، آگاهی بخش و سریع‌الانتقال نسبت به امنیت سایبری، سازگارپذیری و پیشروی در نوآوری‌های دیجیتالی برای همگرایی شبکه و امنیت، آموزش مجدد مهارت به نیروی کار و اتوماسیون امور، محورهای موفقیت محسوب خواهند شد. اطمینان از برخورداری از یک شبکه ایمن و مدیریت مؤثر ریسک در مواجهه با نقض احتمالی داده‌ها و تهدیدات در حال تحول بسیار مهم است.

تأثیرات قانون‌گذاری در امنیت سایبری

اگرچه بخش بانکداری به‌منزله چراغ راهنمای ثبات مالی است، اما به‌طور فزاینده‌ای با چالش‌های دوگانه تضمین امنیت سایبری قوی و پایبندی به مقررات در حال تحول، دست‌وپنجه نرم می‌کند. در عین حال که مؤسسات مالی در تلاش برای برآورده کردن خواسته‌های مشتریان و مقابله با خطرات امنیت سایبری هستند، باید هزارتوی قوانین سخت‌گیرانه حفظ حریم خصوصی و امنیت داده‌ها را نیز بررسی کنند. این اقدامات نظارتی، همراه با گسترش چشم‌انداز دیجیتال، به‌طور اجتناب‌ناپذیری هزینه‌های عملیاتی را به‌ویژه در حوزه انطباق برای بانک‌های شرکتی و خرده‌فروشی افزایش داده است.

ارتقای امنیت و انطباق با استانداردهای بانکداری که با نیاز به حفاظت از داده‌های حساس شخصی، حفظ یکپارچگی تراکنش‌ها و حفظ سلامت اقتصادهای ملی و جهانی همراه است ضروری به نظر می‌رسد. با این حال، نظرسنجی اخیر

مدیریت بهینه امنیت سایبری در صنعت بانکداری

مدیریت تهدیدات سایبری در فضای بانکداری کنونی چیزی ورای اقدامات فنی است و رویکردی جامع و کلی‌نگر را در برمی‌گیرد. با این حال، بسیاری از مؤسسات مالی برای سنجش خطرات امنیت سایبری ابزارهای محدودی در اختیار دارند، به‌ویژه هنگام یکپارچه‌سازی با فناوری‌های دیجیتال جدید.

قوانین نظارتی اخیر بر انعطاف‌پذیری عملیاتی تأکید می‌کند و از چارچوب مدیریت ریسک در سطح جهانی حمایت می‌کند. این همگرایی بین‌المللی به دنبال استانداردسازی رویکردها و یکپارچه‌سازی هرچه بیشتر آنهاست. یکی از جنبه‌های قابل توجه این مقررات، بررسی دقیق ارائه‌دهندگان طرف سوم، با توجه به اهمیت روزافزون آنها در اکوسیستم مالی است.

از آنجا که بانک‌ها همیشه در انتخاب فروشنده فناوری اطلاعات محتاط بوده‌اند، ظهور استارت‌آپ‌های نوآور، راه‌حل‌هایی امیدوارکننده ارائه می‌دهد. با این حال، راه‌حل‌های جدید هم باید با دقت لازم تحت تعدیل قرار گیرند، به خصوص زمانی که ارتباطات طرف سوم امکان آسیب‌پذیری‌های امنیت سایبری را محتمل می‌سازد. با تکامل دیجیتال شدن بانک‌ها، یک رویکرد هماهنگ برای مدیریت ریسک که مقررات جهانی و یکپارچگی با طرف سوم را در نظر می‌گیرد برای یک بخش بانکی ایمن و مترقی ضروری است.

چالش‌های امنیت سایبری بانکی

در گذشته بانک‌ها به‌عنوان نهادهای مجزا فعالیت می‌کردند. بخش‌های مجزا، که هرکدام دارای اهداف منحصر به فرد خود بودند و به صورت مستقل فعالیت می‌کردند. چنین رویکردی مانع پیشرفت بود و موجبات نارضایتی مشتریان را فراهم می‌کرد. بانک‌های سنتی، به داشتن فرایندهای دست‌وپاگیر شهرت پیدا کرده‌اند، به‌ویژه زمانی که مشتریان به دنبال خدمات یا پشتیبانی جدید هستند. پیاده‌سازی یک پلتفرم یکپارچه که داده‌ها را متمرکز می‌کند و شکاف را بین سیستم‌های مختلف پر می‌کند، می‌تواند به‌طور مؤثر با چالش‌های ناشی از این عملکردهای مجزا مقابله کند. با این حال، مجزا بودن بخش‌های اطلاعاتی، خطرات امنیت سایبری، نقض داده‌ها و نگرانی‌های مربوط به انطباق را فراتر از ناکارآمدی‌های عملیاتی تقویت می‌کنند که همگی در چشم‌انداز بانکی امروزی، مسائل بفرنجی هستند.

یکپارچگی زیرساخت‌های فناوری اطلاعات و حجم وسیعی از داده‌هایی که در آن نگهداری می‌شود یکی از نگرانی‌های اصلی در سیر تکامل دیجیتال بانک‌هاست. از طرفی رسیدگی به بدهی‌های فنی بسیار مهم است. این بدهی اغلب مربوط به فراهم آوردن محصولات جانبی فناوری‌های نوین است که باید بر فراز زیرساخت‌های قدیمی قرار گیرند. برای عبور از این چالش‌ها، بانک‌ها باید واحدهای اختصاصی یا تیم‌های حرفه‌ای و مجرب در نظر

بگیرند که بر نوآوری و اطمینان از رقابتی ماندن محصولات قابل ارائه متمرکز باشد. شفاف‌سازی مسئولیت‌ها برای این پروژه‌های نوآورانه بسیار مهم است.

دورانی که امنیت فناوری اطلاعات در بانکداری یک موضوع خطی بود، سپری شده است. اکوسیستم بانکی امروزی شامل ده‌ها یا حتی صدها هزار دستگاه به‌هم‌پیوسته است که از رایانه‌ها گرفته تا تجهیزات اینترنت اشیا (IoT) را شامل می‌شود و هنگامی که گستردگی کانال‌های اجتماعی، خدمات ابری و اپلیکیشن‌های تلفن همراه در نظر گرفته شود، سطح حمله احتمالی برای نقض داده‌ها و خطرات امنیت سایبری به‌طور تصاعدی افزایش می‌یابد. حال این سؤال مطرح می‌شود که در کشاکش این پیچیدگی‌های گسترده، بانک‌ها چگونه می‌توانند از امنیت شبکه اطمینان حاصل کنند؟

اگرچه سازمان‌های مالی به ابتکارات دیجیتال شدیداً نیازمندند، اما این کار الزام اتکا به امنیت مقیاس‌پذیر و راهکارهای انطباقی را بیشتر می‌کند. در این سیر تحول و تکامل بانکداری، معیارهای ارائه‌شده به‌واسطه راهکار نرم‌افزار به‌عنوان خدمت (Software As a Service) به‌ویژه در بخش بانکداری خرده‌فروشی، ضرورت خود را بیشتر نشان می‌دهد. در واقع سازمان‌ها باید بتوانند به سرعت با چالش‌ها و تهدیدهای جدیدی که در حوزه دیجیتال به وجود می‌آیند سازگار شوند.

راهکار مناسب امنیتی

صرف نظر از اینکه یک سازمان دارای فناوری پیشرفته یا قدیمی باشد، آسیب‌پذیری‌های زیرساخت می‌توانند به اهداف اصلی مجرمان سایبری تبدیل شود. از آنجایی که این تبهکاران بی‌وقفه در حال سوءاستفاده از نقاط ضعف هستند، مؤسسات مالی در معرض زیان‌های مالی قابل توجه، از دسترس خارج شدن عملیات، آسیب برند و جریمه‌های دولتی قرار دارند. بنابراین مدیران مؤسسات مالی باید انعطاف‌پذیری و امنیت کلی مؤسسات خود را در اولویت قرار دهند.

مؤسسات مالی باید با ایجاد همگرایی بین شبکه و امنیت، یک راهکار شبکه‌ای ایمن بیافرینند تا بتوانند از پس چالش‌های پیش رو برآیند. آن‌ها می‌توانند با ادغام محصولات امنیتی مختلف در یک پلتفرم امنیت سایبری یکدست، از هوش تهدید و خدمات امنیتی یکپارچه استفاده کنند. ویژگی‌های کلیدی یک راهکار امنیتی ایده‌آل عبارت‌اند از:

- **رصد:** نظارت جامع بر کل سطح حمله دیجیتال
- **حفاظت پیشرفته:** مکانیسم‌های دفاعی در برابر تهدیدات وسیع و پیچیده
- **هوشمندی یکپارچه:** یکپارچگی در ساختار هوشمند فناوری اطلاعات
- **خودکارسازی:** استفاده از فناوری برای رفع کمبود استعدادهای انسانی ماهر
- **انطباق ساده:** تسهیل فرایندها برای اطمینان از پایبندی به مقررات حفظ حریم خصوصی داده‌ها



احراز هویت صوتی، گامی برای افزایش امنیت

حرفه‌ای، نمی‌تواند پنچ مکالمه تلفنی مختلف را هم‌زمان نگه دارد؛ اما آن‌ها می‌توانند هم‌زمان از چندین دستگاه چت کنند یا حتی این کار را به ربات‌های قابل برنامه‌ریزی واگذار کنند.

این نیاز روزافزون به ایمن‌سازی مؤثر تعامل Omni Channel یا چندکاناله، یکی از عواملی است که سازمان‌ها را به جایگزینی فرایندهای احراز هویت ضعیف و مبتنی بر دانش با بیومتریک صوتی سوق می‌دهد. عامل دیگر، فشار ناشی از دوره‌های چالش‌برانگیز مالی است.

بسیاری از مدیران مراکز تماس به دنبال راهکارهایی برای ارائه عملکردهای سریع‌تر و کارآمدتر هستند. آن‌ها برای کاهش میانگین زمان رسیدگی، سبک کردن فشار کاری کارکنان و فعال کردن خدمات خودایمنی برای تعاملات پرخطر با مشتریان، به پتانسیل بیومتریک صوتی روی آورده‌اند.

آن‌ها به راه‌حل‌های احراز هویت صوتی نیاز دارند که کاملاً اثبات شده باشند و کارآمدی خود را در کسب‌وکار نشان دهند. آن‌ها همچنین به راهکارهایی با میزان دقت بسیار بالا نیاز دارند که به‌واسطه آن‌ها زمان برای هشدارهای کلاهبرداری قلبی و رد کردن مشتری قلبی تلف نمی‌شود. هم‌زمان با رواج فزاینده بیومتریک صوتی، کلاهبرداران حرفه‌ای شروع به سرمایه‌گذاری روی زمان و منابع بیشتری برای فرار و فریب فناوری کرده‌اند. درحالی‌که چنین تکنیک‌هایی هنوز در مراحل ابتدایی خود هستند، شاهد افزایش حملات با استفاده از گفتار مصنوعی و ضبط‌شده بوده‌ایم که تحت عنوان «دیپ‌فیک» صدا شناخته می‌شود.

دورنمای کلاهبرداری مجازی به سرعت در حال تغییر است؛ بنابراین ما باید احراز هویت صوتی را سریع‌تر توسعه دهیم.

از آنجایی که راه‌ها و کانال‌های ارتباطی دنیای دیجیتال فرصت‌های سوءاستفاده جدیدی برای کلاهبرداران فراهم آورده‌اند، مدیران مراکز تماس تلاش می‌کنند تا با صرف هزینه و منابع کمتر، کارایی بیشتری داشته باشند. هم‌اکنون سازمان‌ها به دنبال استفاده از حسگر بیولوژیک صدا هستند تا پیشگیری مؤثرتر و کارآمدتری در برابر حملات جعل هویت و نیز احراز هویت مشتری ارائه دهند؛ اما آن‌ها برای ایمن‌سازی موفقیت‌آمیز هر کانال، صرفه‌جویی در هزینه‌ها و مقابله با تهدیدات نوظهور به راهکاری نیازمندند که هم عملاً اثبات شده و هم پیشرفته باشد.

گفته می‌شود نیاز، مادر هر اختراعی است و در مورد نوآوری نیز این گفته صدق می‌کند. با وجود دورنمای همیشه در حال تحول کلاهبرداری، ضروری به نظر می‌رسد که سرعت تکامل راهکارهای هوشمند پیشگیری از کلاهبرداری از سرعت پیشرفت سودجویان فزونی یابد.

در شرکت نوآنس (Nuance)، تیم‌های تحقیق و توسعه پیشرو دائماً در حال ارتقا و تقویت هوش مصنوعی امنیتی هستند تا از تهدیدات مدرن جلوتر بمانند و در دو سال گذشته، شاهد برخی تغییرات تحول‌ساز بوده‌ایم.

از آنجاکه برندها و مشتریان آن‌ها به کانال‌های دیجیتالی، از چت زنده گرفته تا برنامه‌های تلفن همراه، تمایل پیدا کرده‌اند، کلاهبرداران نیز از آن‌ها عقب نمانده‌اند. در بسیاری از موارد، آن‌ها با امنیت ضعیف‌تر و فرصت‌های تازه سودجویی مواجه شده‌اند. برای مثال، یک کلاهبردار

می‌توان ده‌ها هزار تعامل را در چند دقیقه تجزیه و تحلیل کرده و به نتایج مرتبط‌تر و دقیق‌تری دست یافت. نوآنس همچنین موفق شده نرخ خطای بسیار پایین موتور را حتی پایین‌تر هم ببرد، بنابراین تعداد کمتری از پذیرش‌ها و ردهای جعلی را شاهد خواهید بود.

و البته، نوآنس به تقویت قابلیت‌های ضد جعل Nuance Lightning Engine ادامه داده تا وضعیت امنیتی سازمان را در سایه تهدیدات در حال ظهور تقویت کند. مدل هوش مصنوعی نوآنس اکنون در تشخیص گفتار زنده انسان از گفتار مصنوعی یا ضبط‌شده در زمان واقعی بسیار کارآمد است حتی اگر حمله بسیار پیچیده باشد. نوآنس طی سال ۲۰۲۲ همکاری‌هایی با تیم تحقیقاتی هوش مصنوعی شناختی مایکروسافت داشته تا الگوریتم تشخیص گفتار مصنوعی را تنظیم کند و به مشتریان امکان تشخیص صداهای مصنوعی قدرتمند را در زمان واقعی ارائه دهد، درست مانند صداهایی که توسط مدل‌های پیشرفته هوش مصنوعی مولد ایجاد شده‌اند. در نتیجه این تلاش‌ها اکنون نرخ دقت تشخیص الگوریتم به ۸۶ درصد یافته است. افزودن قابلیت Conversation Print که الگوهای زبانی یک فرد را تجزیه و تحلیل می‌کند، میزان تشخیص را تا ۹۹ درصد بالا می‌برد.

آینده بیومتریک صوتی

همه این قابلیت‌ها امروزه در دسترس هستند. Nuance Lightning Engine در قلب راهکار امنیتی بیومتریک نوآنس، یعنی Nuance Gatekeeper قرار دارد. Nuance Gatekeeper بخشی از پلتفرم مرکز تماس دیجیتال مایکروسافت است که از هوش مصنوعی و تجزیه و تحلیل عمیق برای ساده کردن خدمات و افزایش رضایتمندی مشتریان استفاده می‌کند؛ ام Gatekeeper همچنان یک ابر بومی با پلتفرم نامعلوم (platform agnostic) است و با مرکز تماس پیشرو به‌عنوان خدمت (CCaaS) کار می‌کند که جنسیس، آوایا، سیسکو و آمازون کانکت را ارائه می‌دهد.

به زبان ساده، Gatekeeper ساخته شده تا اطمینان حاصل شود که می‌توان از مزایای بهترین راهکارهای احراز هویت و ضد کلاهبرداری در هر زیرساختی بهره‌مند شد.

نوآوری مستمر برای مبارزه با تهدیدات همیشه در حال تغییر

مشاهده سازمان‌های زیادی که به دنبال بیومتریک صدا هستند تا از کلاهبرداری در کانال‌ها جلوگیری کنند و مرکز تماس کارآمدتری داشته باشند بسیار جالب توجه است؛ اما برای رسیدن به این دو هدف، نیازمند راهکارهایی هستیم که می‌دانیم نتایج واقعی و نوآوری مستمر را به ارمغان می‌آورند.

این آخرین پیشرفت‌های نوآنس برای Gatekeeper است. این دستاوردها بر میزان سرعت و دقت راهکارهای مربوط به صدا افزوده‌اند و از کلاهبرداری‌ها پیشگیری کرده و درها را بر روی تهدیدهای نوظهور می‌بندند.

ضرورت استمرار نوآوری

در صورتی که راهکار بیومتریک صوتی برای شناسایی این تهدیدها و یک قدم جلوتر نگه داشتن شما به‌طور مداوم در حال تکامل است، دیپ‌فیک‌ها مشکل‌چندانی به شمار نمی‌آیند.

کمپانی نوآنس در اوایل دهه ۲۰۰۰ پیشگام بیومتریک صوتی فعال و غیرفعال (اکتیو و پسیو) بود و راهکارهای آن نمایاننده یک تکنولوژی با ریسک بالا بودند. Nuance Lightning Engine که در واقع قلب تپنده راهکارهای محسوب می‌شود یک مدل هوش مصنوعی اختصاصی است که از شبکه‌های عصبی عمیق و تجزیه و تحلیل ویژگی‌های صدای انسان برای احراز هویت مشتریان و شناسایی کلاهبرداران در کانال‌ها استفاده می‌کند.

با جدیدترین و نهمین نسل این موتور، پیشرفت‌های قابل توجهی انجام شده که به سازمان‌ها کمک می‌کند تا سیستم دفاع خود را تقویت کنند، کارایی خود را بهبود بخشند و استانداردهایی را برای آینده فناوری بیومتریک صوتی معین کنند.

پیشگیری واقعی از کلاهبرداری Omni Channel

قبلاً، دقت سخن‌نگاری (voiceprints) مانعی برای استفاده از بیومتریک جهت احراز هویت در خارج از مرکز تماس بوده است.

به لطف تازه‌ترین پیشرفت‌ها در شرکت نوآنس، یک سخن‌نگاری که از طریق تلفن استاندارد ضبط شده است، اکنون می‌تواند به‌عنوان مدلی بسیار دقیق که از احراز هویت یکپارچه در کانال‌های دیجیتال پشتیبانی می‌کند، ایفای نقش نماید. این بدان معناست که مشتری پس از ثبت نام و تعریف سخن‌نگار خود، می‌تواند از صدای خود برای احراز هویت در هر کانالی، خواه تلفن گویا یا برنامه تلفن همراه و یا وبسایت، استفاده کند.

عملیات و تجربیات ساده و پربازده

Nuance Lightning Engine در حال حاضر محصولی پیشرو با سرعت، دقت و میزان موفقیت بالا در احراز هویت است. هم‌ثبت نام و هم احراز هویت مشتری اکنون سریع‌تر از همیشه انجام می‌پذیرد. به‌عنوان مثال، این برنامه با نرخ احراز هویت ۹۵ درصد، می‌تواند مشتریان را بر اساس یک صوت ۵ ثانیه‌ای ثبت نام کرده و آن‌ها را در نیم ثانیه احراز هویت کند.

افزایش قابلیت‌های کشف کلاهبرداری

شرکت نوآنس همچنین قابلیت‌های پیشگیری از کلاهبرداری هوشمند بر اساس مدل هوش مصنوعی را ارتقا داده است.

ویژگی انحصاری خوشه‌بندی بیومتریک آن به تیم‌های شناسایی اجازه می‌دهد تا با تجزیه و تحلیل جنبه‌های مختلف تعاملات تماس و چت، کلاهبرداران ناشناخته قبلی را شناسایی کنند. با جدیدترین نسل این برنامه اکنون

زمین بازی تغییر خواهد کرد هوش مصنوعی رفتار محور در امنیت اطلاعات

الیور پاترسون، سرپرست بخش مدیریت محصول در گروه امنیتی VIPRE، در خصوص اینکه هوش مصنوعی چگونه می‌تواند نقش تعیین‌کننده‌ای در تغییر روند بازی امنیت سایبری داشته باشد، مباحثی را ارائه داده است.

امروزه تضمین امنیت سایبری مستلزم پشتکار و استقامت بی‌حد و حصری است. ضرر و زیان ناشی از کلاهبرداری‌هایی که از طریق ایمیل جعلی تجاری (BEC) صورت می‌گیرد ۷۵ برابر (۲/۷ میلیارد دلار) بیشتر از حملات باج‌افزاری (۳۴/۳ میلیون دلار) است. مجرمان از هیچ اقدامی فروگذار نمی‌کنند و حملات Malspam و بدون ما کرویک رویه جدید در این جهت است که بر اساس آن ارسال ایمیل‌های فیشینگ با کدهای QR یک تاکتیک جدید برای تطمیع قربانیان بوده که در نتیجه آن خانواده بدافزار Qakbot (یک نوع بدافزار بسیار زیان‌بار و مخرب) به سرعت در حال توسعه و تکثیر است.

قابلیت هوش مصنوعی مبتنی بر رفتار، به زودی زمین بازی امنیت سایبری را تغییر خواهد داد. با این اوصاف، ضروری است که اقدامات امنیتی و زیربنایی در بالاترین سطح در دستور کار قرار گیرند. برخلاف تصور عمومی، برای به‌کارگیری مؤثر قابلیت هوش مصنوعی رفتار محور، باید چارچوب‌های امنیتی مبتنی بر فناوری‌هایی که قبلاً امتحان خود را پس داده‌اند قوی باشد.

ایمیل هنوز بزرگ‌ترین تهدید است

مجرمان همچنان ترجیح می‌دهند حملات را از سطح ایمیل انجام بدهند و از این‌رو محافظت همه‌جانبه و قوی از ایمیل و به‌کارگیری قابلیت‌هایی که بتواند منبع اصلی ارسال را شناسایی کند حیاتی است. فرض کنید که ایمیلی حاوی یک پیوست دریافت می‌کنید که برای باز کردن آن باید تصمیم بگیرید. در این شرایط شرکت‌ها باید امکانات لازم برای تجزیه و تحلیل ایمیل تا منبع اصلی آن را داشته باشند تا از غیر جعلی بودن آن اطمینان حاصل کنند؛ آیا فرمت پیوست قانونی است؟ لینک موجود در ایمیل / پیوست اشاره به چه چیزی دارد؟ اگر لینک به یک تبلیغ هدایت



شود، آیا احتمال دارد لینک فیشینگ باشد؟ از طرف دیگر، اگر لینک به یک وب‌سایت برود، آیا آن سایت معتبر است یا احتمال خطر وجود دارد؟ آیا وب‌سایت یک صفحه مایکروسافت است؟ اگر چنین است می‌تواند یک علامت خطر باشد چراکه مجرمان قادرند وب‌سایت‌هایی با ظاهر بسیار معتبر را به معنای واقعی کلمه در زمان واقعی و درست در زمانی که در مرورگر کاربر دانلود می‌شوند، اسکرپت کنند.

امروزه، بسیاری از شرکت‌ها مجذوب راه‌حل‌های متعدد امنیتی مبتنی بر هوش مصنوعی برای ایمیل‌ها شده‌اند که در حال حاضر به بازار راه پیدا کرده‌اند. آن‌ها راهکارهایی دقیق و مناسب با نقطه تمرکز محدود هستند. آن‌ها فقط به بخش کوچکی از نوع خاصی از مشکل می‌پردازند. تهدیدها همواره در حال دگرگونی هستند زیرا مجرمان دائماً از تکنیک‌های جدید برای فریب دادن استفاده می‌کنند.

تهدیدات نقطه پایانی

ترجیحی، شناسه‌های ایمیل استفاده شده به غیر از ایمیل تجاری، الگوهای ترافیک ایمیل، دستگاه‌های مورد استفاده برای ورود به سیستم، سبک نوشتن در ایمیل‌ها، فرمت پیوست‌ها و غیره وجود نداشته باشد، راهکار هوش مصنوعی برای شناسایی و کاهش تهدید شناسی ندارد. بنابراین، آموزش سیستم‌های هوش مصنوعی بر پایه داده‌های ترکیبی شامل طیف گسترده‌ای از منابع خارجی دقیق و معتبر در کنار ورودی‌های راهکارهای خاص، حیاتی است. زمانی که سیستم‌های امنیتی هوش مصنوعی بر مبنای داده‌های مناسب تحت آموزش قرار گیرند، هزاران منبع رخنه با رویکردهای فناوری رفتارمحور قابل شناسایی هستند. به‌عنوان مثال، تشخیص و تجزیه و تحلیل جهت‌گیری و هدف ایمیل‌ها بر اساس نمایه‌های تاریخی افراد ممکن است. آیا از این ایمیل بوی نوعی الزام و اجبار ناآشنا به مشام می‌رسد که ممکن است نشانه‌ای هشداردهنده از نیتی سوء باشد؟

به همین ترتیب، از قابلیت مولد هوش مصنوعی می‌توان برای تحقیقات جرم‌یابی استفاده کرد تا مشخص شود آیا انواع خاصی از حوادث به‌طور مکرر روی داده و سابقه مشابه دارند یا اینکه یک رویداد جدید هستند یا اینکه سازمان قبلاً مانند آن‌ها را تجربه کرده است و حتی اگر هنوز نتوان نام یک حادثه را روی آن گذاشت چگونه کاربران تحت تأثیر این اقدامات قرار می‌گیرند. به‌واسطه این ابزار، صرفه‌جویی در زمان و هزینه برای تیم‌های امنیتی بی‌سابقه خواهد بود. همه این وظایف در مدل‌های پردازش زبان طبیعی و یادگیری ماشینی تا حد زیادی قابل انجام خواهند بود که سبب می‌شود هوش مصنوعی مبتنی بر رفتار برای تغییر روند بازی‌های امنیتی مورد استفاده قرار گیرد. علاوه بر هزینه بررسی و کشف به موقع حملات، میانگین زمان بازیابی و هزینه تحقیقات نیز به میزان قابل توجهی کاهش می‌یابد.

آگاهی‌رسانی امنیتی ضروری است

توصیه ما به شما این است که صرف‌نظر از میزان پیشرفته بودن یک فناوری، تکیه صرف به راهکارهای فناوری یک استراتژی پرخطر است. در این میان هوشیاری کارکنان نیز امری ضروری است. همیشه امکان تلاش برای رخنه و خرابکاری وجود دارد و کارکنان باید به دانش مناسبی برای شناسایی یک تهدید بالقوه مجهز باشند. یک لینک مخرب مثال خوبی است. اگر آن‌ها به‌طور ناخواسته روی لینک مخرب یا حمله فیشینگ یا مهندسی اجتماعی کلیک کرده باشند، حتماً باید با راهکارهای کاهش فوری تأثیر نقض داده بر سازمان آشنا باشند و اقدامات اصلاحی را صورت دهند. به زبان ساده هیچ جایگزینی برای این راهکارها وجود ندارد. غفلت از انجام این اقدامات بسیار مهم می‌تواند به‌راحتی تبدیل به یک اشتباه پرهزینه شود. این دیدگاه که هوش مصنوعی را می‌توان «روشن» کرد تا این فناوری به‌طور جادویی، امنیت شما را تأمین کند یک اشتباه بزرگ است.

تهدیدها همیشه فقط از طریق ایمیل‌ها ایجاد نمی‌شوند. نقاط پایانی (Endpoint) مانند مرورگرها و صفحات وب، راهکارهای اشتراک‌گذاری اسناد طرف سوم، سیستم‌های کنترل دسترسی به شبکه، سند باکس (محیط آزمایشی امن و مجزا)، رمزگذاری و بسیاری موارد دیگر وجود دارند که می‌توانند در معرض خطر باشند؛ بنابراین، اقداماتی مانند ایجاد محافظت به‌واسطه ضدویروس، نظارت بر ترافیک شبکه، مدیریت آسیب‌پذیری و غیره بسیار مهم هستند. در چنین شرایطی، به‌کارگیری فناوری‌های موجود مانند پردازش زبان طبیعی و یادگیری ماشینی بسیار مهم و مؤثر است. در واقع، امروزه از این تکنیک‌ها به‌طور گسترده‌ای برای توقف فعالیت بدافزار و باج‌افزار روز صفر که لزوماً مبتنی بر فایل نیستند، استفاده می‌شود. داده‌های این فناوری‌ها نیز برای آموزش فناوری‌های جدید هوش مصنوعی به کار می‌آید.

امنیت مبتنی بر هوش مصنوعی رفتارمحور

امنیت مبتنی بر هوش مصنوعی رفتارمحور برای رویکرد امنیت سایبری چندلایه از مرحله نخست اقدامات مجرمان برای شناسایی یعنی فیشینگ تا باج‌افزار و حمله بدون امضا (less signature) و حملات روز صفر که تاکنون نظیر آن دیده نشده است، راه‌حلی مؤثر ارائه می‌کند.

اساس به‌کارگیری چنین فناوری، دسترسی به حجم وسیعی از داده‌ها شامل تمام نسخه‌های فرمت‌های هوش مصنوعی برای هر جنبه امنیتی از سند باکس، نقطه پایانی و نظارت بر فرآیند گرفته تا بدافزار و شناسایی فیشینگ لینک عمیق و مبدأ تاریخ کاربر است.

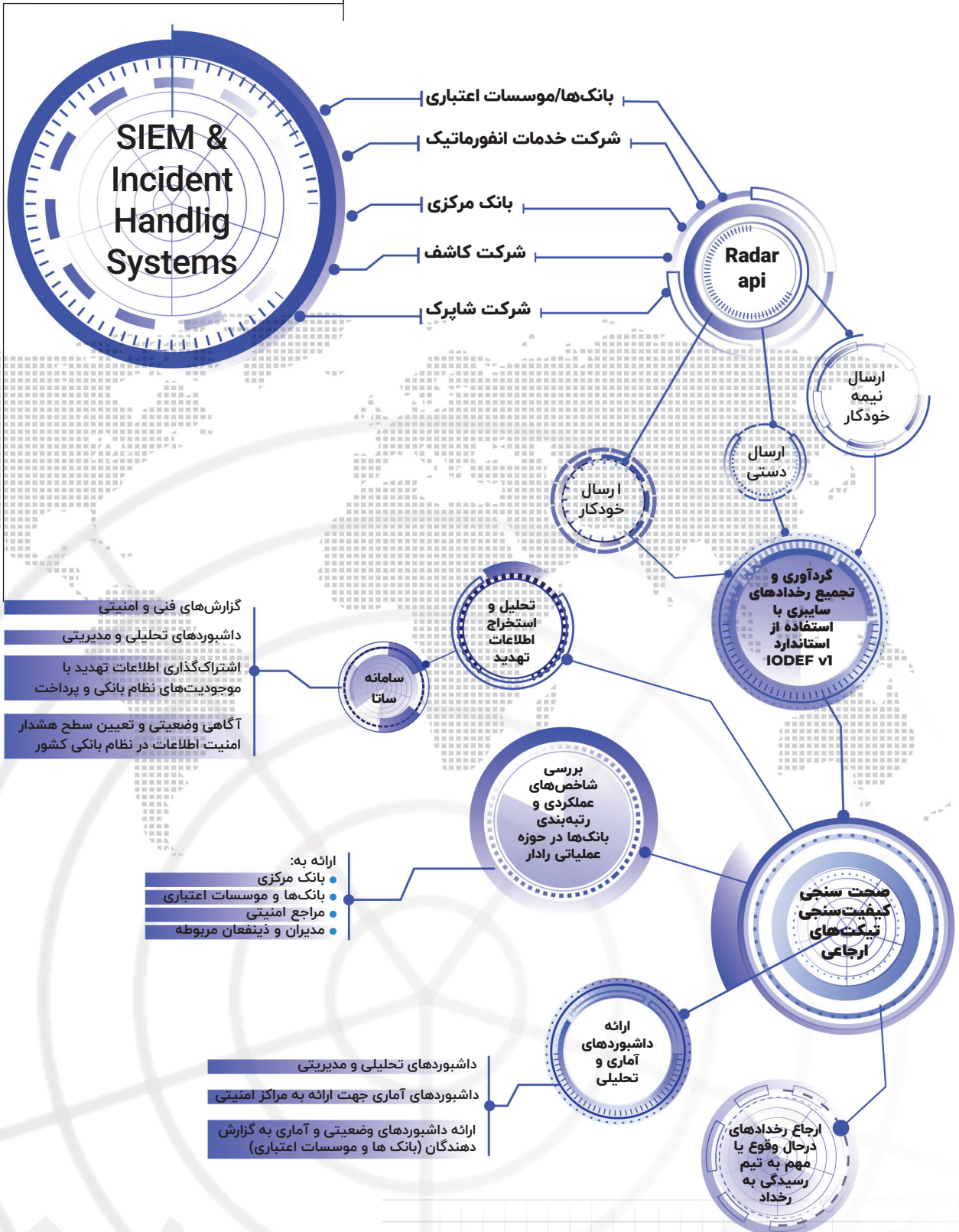
هوش مصنوعی واقعاً چیست؟ اساساً یک موتور جست‌وجوی عظیم است که با استفاده از زبان طبیعی، اطلاعاتی را ارائه می‌کند تا حول تصویری از آنچه در یک محیط در حال روی دادن است و نقطه‌ای که باید روی آن تمرکز شود، مفاهیم و نگرش‌هایی را ارائه دهد و در نهایت از رخنه‌ها و دستبردهای امنیتی جلوگیری کند.

شرکت‌هایی که به دنبال ایجاد امنیت مبتنی بر رفتار هستند باید اطمینان حاصل کنند که داده‌های ورودی موتور هوش مصنوعی داده‌های داخلی و خارجی دقیقی باشند. به‌عنوان مثال، اگر رفتار کارکنان در مورد ایمیل‌ها فقط بر مبنای کاربری آن‌ها در سازمان فعلی و در حوزه‌های خاصی مانند لینک‌ها، فایل‌های اجرایی، فایل‌های مخرب، ماگروها و مواردی از این قبیل تجزیه و تحلیل شود، قابلیت راهکارهای هوش مصنوعی برای مقابله با حمله ایمیل جعلی تجاری (BEC) و ارائه تصویر دقیقی از رفتار آنلاین را محدود می‌سازد.

علاوه بر این، فرض کنید که یک کارمند تازه‌کار، لینک فیشینگ جدیدی را دریافت می‌کند که شرکت قبلاً نظیر آن را ندیده است. اگر در یک شرکت هیچ تعریفی در خصوص رفتار و واکنش کارمند در برابر مقولاتی چون آدرس‌های IP که فرد از آن‌ها برای مکاتبه استفاده می‌کند، مرورگر

آشنایی با سامانه رادار

سامانه رؤیت آنی و دائم رخدادهای امنیتی





بر اساس گزارش موسسه گلوبال مارکت اینسایتز، انتظار می‌رود بازار جهانی نئوبانک‌ها از سال ۲۰۲۲ تا ۲۰۲۸ با نرخ رشد سالانه ۴۵ درصد رشد کند و تا سال ۲۰۲۸ اندازه این بازار به بیش از ۶۰۰ میلیارد دلار برسد. پدیده نئوبانک صنعت بانکداری سنتی را مختل کرده است و به مصرف‌کنندگان یک تجربه بانکی راحت‌تر و شخصی‌سازی شده ارائه می‌دهد. نئوبانک‌ها در واقع بانک‌های دیجیتالی هستند که تمام و کمال به صورت آنلاین و بدون نیاز به شعب فیزیکی فعالیت می‌کنند. اما نئوبانک‌ها فقط به خاطر راحتی انجام امور طراحی نشده‌اند، بلکه نوآوری و برآوردن نیازهای در حال تکامل مصرف‌کنندگان در یک چشم‌انداز مالی به سرعت در حال تغییر را در نظر دارد. همگام با پیشرفت فناوری، پتانسیل نئوبانک‌ها برای تغییر طرز تفکر ما در مورد بانکداری نیز افزایش می‌یابد.

فرصت‌ها و تهدیدهای نئوبانک‌ها

دیجیتالی فاقد شعبه فیزیکی استفاده می‌شود. این بانک‌ها تمام خدمات بانکی سنتی مانند حساب‌های جاری، حساب‌های پس‌انداز و وام دادن را ارائه می‌دهند و شما به راحتی می‌توانید امور مالی خود را از طریق تلفن هوشمند یا رایانه مدیریت کنید.

ظهور نئوبانک

ظهور نئوبانک‌ها دست کمی از برخورد شهاب سنگ با زمین ندارد! تغییر مسیر به این سمت را می‌توان به پیامدهای بحران مالی ۲۰۰۸ نسبت داد که اعتماد به بانک‌های سنتی به پایین‌ترین حد خود رسید. مصرف‌کنندگان به دنبال جایگزین‌هایی برای سیستم بانکداری سنتی بودند و نئوبانک‌ها به عنوان یک گزینه مناسب ظاهر شدند.

نئوبانک‌ها توانستند با تکیه بر فناوری، تجربه بانکداری شفاف‌تر و در دسترس‌تری را ارائه دهند و نسل جدیدی از مشتریان را جذب کنند که به دنبال رویکردهای مدرن بانکداری مانند انتقال پول دیجیتال بودند.

امروز

در سال ۲۰۲۳، با معرفی روش‌های سرآمد پرداخت دیجیتال، نئوبانک‌ها به طور فزاینده‌ای محبوب شده‌اند و تعداد بسیاری از مصرف‌کنندگان برای نیازهای مالی خود به آن‌ها مراجعه می‌کنند. طبق مطالعات اخیر، ۴۹ درصد از نسل میانسالان و ۵۳ درصد از مشتریان نسل زد از نئوبانک‌ها برای نیازهای بانکی خود استفاده می‌کنند.

با افزایش محبوبیت نئوبانک‌ها، توجه بانک‌های سنتی نیز به آن جلب شده و بسیاری از آن‌ها برای رقابت با نئوبانک‌ها در طرح‌های تحول دیجیتال سرمایه‌گذاری می‌کنند. نئوبانک‌ها به این طوفان انقلابی در صنعت بانکداری ادامه خواهد داد و تجربه بانکداری ساده‌تر و شخصی‌شده‌تری را به مشتریان ارائه می‌دهد.

به گفته یکی از مشتریان نئوبانک «من دوست دارم بتوانم امور مالی خود را در حال قدم زدن مدیریت کنم. بتوانم پول را انتقال دهم، صورتحساب‌ها را پرداخت کنم و همه هزینه‌هایم را از طریق تلفنم پیگیری کنم؛ و نئوبانک یعنی همه این‌ها.

مزایای نئوبانک

نئوبانک نسبت به بانکداری سنتی مزایای فراوانی دارد. در اینجا برخی از مزایای کلیدی نئوبانک‌ها فهرست شده است:

■ راحتی

نئوبانک نیاز به شعب فیزیکی بانک را از بین می‌برد و به شما امکان می‌دهد امور مالی خود را از هر کجا و در هر زمان مدیریت کنید.

■ شخصی‌سازی

نئوبانک‌ها برای ارائه توصیه‌های مالی به شما، بر اساس



در این مطلب، آینده نئوبانک و رویکردهای نوظهور و فرصت‌های پیش رو را بررسی خواهیم کرد. این مطلب دیدگاه‌های ارزشمندی را در مورد دنیای بانکداری نوین و چگونگی مفید بودن آن ارائه می‌دهد.

مروری بر نئوبانک در سال ۲۰۲۳

صبح از خواب بیدار می‌شوید، گوشی هوشمند خود را برمی‌دارید و حساب بانکی‌تان را چک می‌کنید. متوجه می‌شوید که شب گذشته مبلغی به حساب شما واریز شده است، بنابراین به سرعت این مقدار وجه را به حساب سرمایه‌گذاری خود منتقل می‌کنید، اجاره خود را پرداخت می‌کنید و امتیاز اعتباری خود را بررسی می‌کنید. همه این‌ها در عرض چند دقیقه انجام می‌شود، بدون اینکه از جای خود حرکت کنید. این قدرت نئوبانک است. نئوبانک اصطلاحی است که برای توصیف بانک‌های

عادات هزینه و اهداف مالی تان از هوش مصنوعی و یادگیری ماشینی استفاده می کنند.

■ کاهش هزینه

نئوبانک‌ها در مقایسه با بانک‌های سنتی اغلب کارمزد کمتر و نرخ بهره بالاتری ارائه می دهند.

■ افتتاح سریع و راحت حساب بانکی

با نئوبانک می‌توانید در عرض چند دقیقه حساب باز کنید بدون اینکه از خانه بیرون بروید.

چالش‌های امنیت سایبری در فین‌تک و نئوبانک

چالش‌های بزرگ امنیت سایبری برای برنامه‌های فین‌تک و نئوبانک که شامل نقض اطلاعات، هک، حملات فیشینگ و سرقت هویت می‌شود، متخصصان را نگران کرده است. فاجعه امنیت سایبری اکویفا کس بیش از ۱۴۷ میلیون مشتری را تحت تأثیر قرار داد. چند تجربه تلخ امنیت سایبری منجر به نقض داده‌ها و هموار کردن مسیر برای مجرمان سایبری شد. یکی از دلایل اصلی آن ناتوانی یک شرکت پیشرو در صنعت فین‌تک برای شناسایی و اصلاح یک آسیب‌پذیری بود در حالی که پچ‌های برطرف کردن این آسیب‌پذیری، بیش از شش ماه در دسترس بودند.

همچنین اکویفا کس نتوانست اکوسیستم خود را بخش‌بندی کند و همین مسئله به هکرها امکان دسترسی آسان به چندین سرور را داد. نام‌های کاربری و رمزهای عبور نیز به صورت متن رمز نشده در دسترس بودند که سیستم را آسیب‌پذیرتر می‌کرد. اکویفا کس همچنین در دوباره‌سازی گواهی رمزگذاری برای یکی از ابزارهای داخلی خود ناکام بود که هکرها را قادر ساخت تا داده‌ها را به مدت چند ماه استخراج کنند.

شرکت کپیتال وان نیز به همین ترتیب به دلیل آسیب‌پذیری‌های سیستم خود قربانی یک حمله سایبری شد. مهاجم سایبری با دسترسی به سرورهای AWS شرکت توانست صد میلیون برنامه کارت اعتباری را به سرقت ببرد. مهاجم اطلاعات دزدیده شده را در Github منتشر کرد و امنیت شرکت را به سخره گرفت و خبر آن به رسانه‌های اجتماعی درز کرد.

دلیل اصلی چنین حمله‌ای، ناکامی این شرکت در ایمن‌سازی فضای ابری خود از طریق راهکار نظارت بر سطح حمله بود. از سوی دیگر، یک فایروال با پیکربندی نادرست نیز وجود داشت که به نقض داده‌ها کمک کرد.

حملات مشابهی در مؤسسات مالی JP Morgan Chase، Flagstar Bank، Westpac Banking Corporation، The First American Financial Corporation و بسیاری از شرکت‌های دیگر گزارش شده است.

آمار و ارقام چالش‌های امنیت سایبری

بیش از سیصد هزار کاربر اندروید، اپلیکیشن‌های بانکداری جعلی را از طریق گوگل پلی دانلود کرده‌اند. به دلیل مجوزهای تنظیم شده روی این اپلیکیشن، بازیگردانان تروجان از این فرایند برای نقض داده‌ها و آلوده کردن گوشی‌های هوشمند کاربران سوءاستفاده می‌کنند.

میانگین کل هزینه‌ای که برای بازیابی و بازسازی فرایندها پس از حمله باج‌افزار نیاز است نزدیک به ۲ میلیون دلار برآورد می‌شود. همچنین داده‌ها نشان می‌دهد که در سال ۲۰۲۰ فقط ۸ درصد از مشاغلی که باج‌افزار پرداخت کردند، داده‌های خود را پس گرفتند. باج‌افزار یکی از مخرب‌ترین روش‌های مورد استفاده هکرها و عامل سود جستن آن‌ها از آسیب‌پذیری‌های برنامه‌های فین‌تک است.

جی پی مورگان چیس، یک شرکت پیشرو مالی، بودجه‌ای ۶۰۰ میلیون دلاری را برای سرمایه‌گذاری در امنیت سایبری اختصاص داده است. این شرکت بیش از سه هزار کارمند را در بخش امنیت سایبری خود استخدام کرده تا اطمینان حاصل کند که در همه جنبه‌ها از سیستم‌هایش در برابر هکرها و مجرمان سایبری محافظت می‌شود.

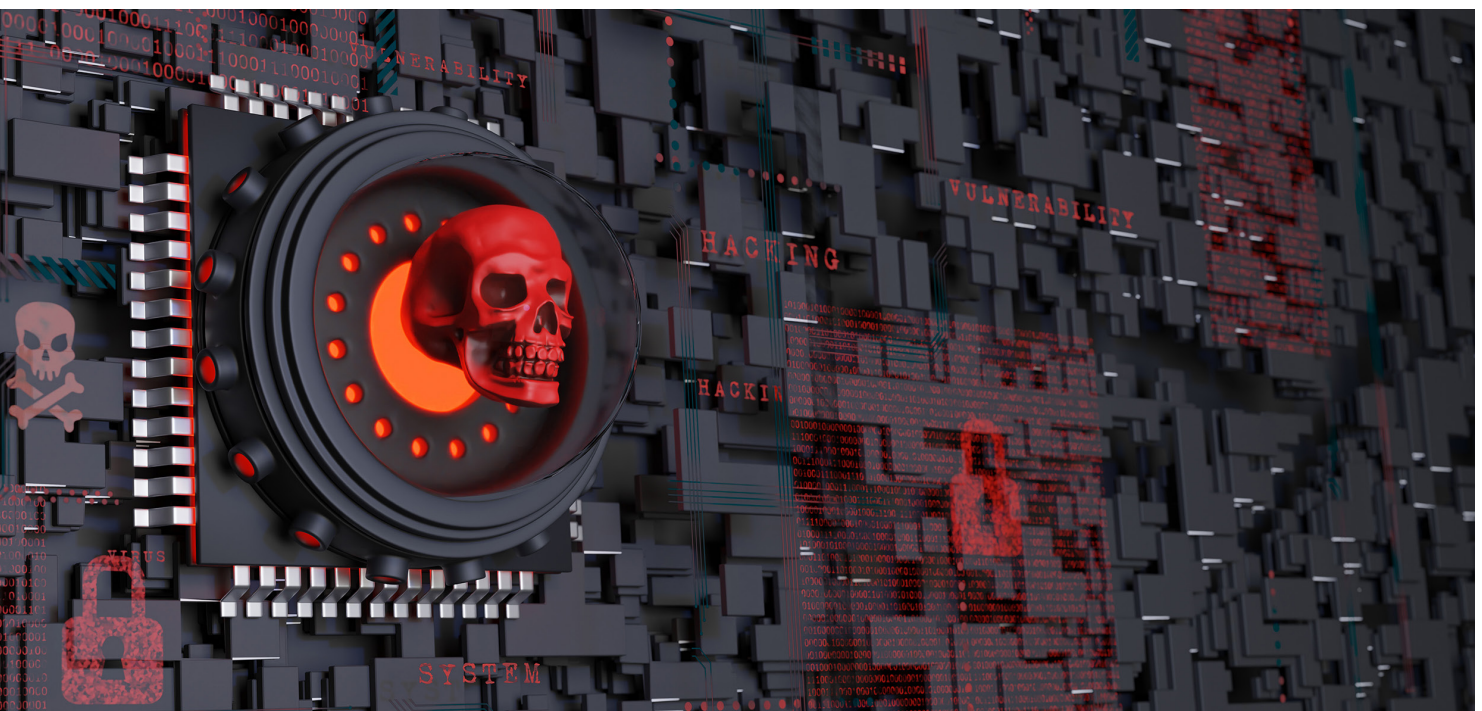


بزرگ‌ترین چالش‌های امنیت سایبری در فین‌تک

رشد فین‌تک و نئوبانک‌ها منجر به افزایش حملات سایبری نیز شده است. با اینکه فین‌تک‌ها و نئوبانک‌ها مزایای بسیاری دارند، اما امنیت یکی از نگرانی‌های اصلی آن‌ها است که بسیاری را هنوز در مورد استفاده از خدمات آن‌ها مردد نگه داشته است.

امروزه چالش‌های امنیت سایبری در نئوبانک‌ها موضوع روز است. در حالی که برخی این چالش‌ها را به عدم وجود واسطه نسبت می‌دهند اما ممکن است بیشتر به طراحی و زیرساخت راه‌حل‌ها مربوط باشد.

در ادامه به برخی از مهم‌ترین چالش‌های امنیت سایبری که فین‌تک و نئوبانک‌ها با آن مواجه هستند، اشاره می‌کنیم.



بانک‌ها با پلتفرم‌هایشان به چندین API سفارشی نیاز دارد که خطرات امنیتی را در یک سیستم بالا می‌برد. بدون دقت لازم و آزمایش دقیق، مجرمان می‌توانند از چندین حفره در یک سیستم سوءاستفاده کنند. علاوه بر این، اغلب نئوبانک‌ها از انجام آزمایش‌های منظم برای اطمینان از ایمن بودن نقاط پایانی API در برابر هرگونه آسیب‌پذیری و تهدید کوتاهی می‌کنند. حتی یک پیچ کوچک می‌تواند به آن‌ها در حل یک چالش امنیتی بزرگ کمک کند. جدا از این سه، فین‌تک با چالش‌های فیش‌سینگ، حملات انکار سرویس (DDoS)، بدافزارها و سایر تهدیدهایی که می‌توانند یک سیستم را در معرض خطر قرار دهند و باعث نقض داده‌ها شوند، مواجه است. با معرفی هوش مصنوعی، مجرمان سایبری در شناسایی آسیب‌پذیری‌ها مجبورند روش‌های بسیار پیچیده‌تری را امتحان کنند. با این حال، شرکت‌ها باید از هوش مصنوعی به نفع خود استفاده کرده و از آن برای محافظت در برابر کلاهبرداری استفاده کنند.

نتیجه

اپلیکیشن‌های فین‌تک و نئوبانک در حال حاضر یکی از اهداف مجرمان سایبری هستند. چنانچه آسیب‌پذیری‌ها رفع نشوند، می‌توانند باعث ایجاد مشکلات اساسی در یک سیستم شده و هزینه‌های زیادی را بر شرکت‌ها تحمیل کنند. شرکت‌ها باید جلوتر از مهاجمان سایبری حرکت کنند و با در اختیار گرفتن یک تیم امنیت سایبری اختصاصی که توانایی ارزیابی شرایط و رفع مشکلات در زمان بروز را داشته باشد آمادگی لازم را برای خود فراهم کنند.

عدم آمادگی برای مقابله با باج‌افزار

یکی از چالش‌های اصلی اپلیکیشن‌های نئوبانک عدم آمادگی آن‌ها برای مقابله با حملات باج‌افزار است. آن‌ها فاقد قابلیت‌های فناوری اطلاعات برای تأمین امنیت خود در برابر تهدیدات مخرب باج‌افزار هستند. هرکدام می‌توانند ترافیک ناخواسته را به شبکه ارسال کنند و ارائه خدمات به کاربران واقعی را متوقف کنند تا مجرمان امکان اخاذی از شرکت‌های مالی را پیدا کنند. باج‌افزار یکی از شایع‌ترین و مهم‌ترین چالش‌هایی است که کارشناسان امنیت سایبری در دنیای مدرن تجارت سعی در حل آن دارند.

بودجه محدود امنیت سایبری

یکی دیگر از چالش‌های امنیت سایبری که شرکت‌های فین‌تک و نئوبانک با آن مواجه هستند، محدود بودن بودجه‌های امنیت سایبری است. از آنجایی که بیشتر این‌ها استارت‌آپ هستند، پول لازم برای تأمین ایمنی هر مرحله از فرایند را ندارند. قد و قواره آن‌ها بسیار کوچک‌تر از سیستم‌های بانکداری سنتی است و همین دلیل آن‌ها را از سرمایه‌گذاری در امنیت سایبری منصرف می‌کند. اکثر شرکت‌ها برای صرفه‌جویی در هزینه‌های امنیتی به فروشندگان و شرکت‌های مشاوره مهندسی محصولات نرم‌افزاری طرف سوم متکی هستند.

حفره‌های یکپارچه‌سازی

یکی از چالش‌های فنی امنیت سایبری برای شرکت‌های فین‌تک، حفره‌های یکپارچه‌سازی است. یکپارچه‌سازی

■ ویژه‌نامه امنیت بانکداری ■ زمستان ۱۴۰۲ ■

راهکار





در نقش مشاور کنار بانک‌ها ایستاده‌ایم

واحد نظارت شرکت کاشف در چهار بخش ممیزی و انطباق سنجی، آزمایشگاه ارزیابی و انطباق سنجی، پایش مخاطرات که متولی راه‌اندازی مرکز وسعت هم هست و بخش نظارت پروژه‌های بانکی که به‌تازگی راه‌اندازی شده، فعالیت می‌کند. میثم نجار، معاون واحد نظارت شرکت کاشف، درباره وظایف و عملکرد این واحد توضیح می‌دهد.

واحد نظارت کاشف دارای چهار بخش است. یکی نظارت بر روی محصولات و خدمات حوزه پولی و بانکی کشور که در آزمایشگاه با ابزارها و دانش موجود، محصولات این حوزه را بررسی می‌کنند. در بخش ممیزی هم امور ممیزی و انطباق سنجی با الزاماتی که در این حوزه طراحی و تدوین شده‌اند صورت می‌گیرد. کار دیگری که در این بخش انجام می‌شود موضوع حاکمیت امنیت با تدوین الزامات و دستورالعمل‌هاست. بخش پایش مخاطرات هم سعی در شناسایی ریسک‌های حوزه بانکی دارد تا الگوریتم‌هایی برای تشخیص و احتمالاً تعدیل آن‌ها پیشنهاد دهد. یکی از کارهای دیگری که در یکی دو سال اخیر انجام می‌دهد موضوع کشف تقلب است که تراکنش‌های مشکوک را شناسایی و به بانک مرکزی اعلام می‌کند.

کاشف باید سبب بزرگی از پروژه‌های بانک مرکزی را اجرا کند و برای سامان دادن به گام‌های اولیه پروژه و تعیین متولی آن، بخش جدیدی به نام نظارت پروژه‌های بانکی راه‌اندازی شد که از آغاز یک پروژه تا نظارت فنی بر اجرای آن را برعهده بگیرد. با همین منطق، چند پروژه را جلو بردیم و شاهد نظم و بهبود خوبی در سرعت پیشبرد کارها بودیم؛ مخصوصاً زمانی که پروژه به مگا پروژه تبدیل می‌شود. اکنون مهم‌ترین پروژه‌ای در حال انجام در این بخش برای MSSP (Managed Security Service Provider) برای

نظارت و ارزیابی امنیتی صرافی‌ها بر بستر خوداظهاری‌های آن‌هاست. در همین راستا و قبل از آن، سامانه مدیریت تهدید صرافی‌ها برای بانک مرکزی انجام داده شده بود. گام اول ما در این نظارت بر محصولات برای بانک مرکزی تعریف شده است. موضوع (project management office) PMO که استانداردهای مدیریت پروژه را تعریف، تضمین و حفظ می‌کند، قبلاً در کاشف تعریف شده بود اما TMO یعنی مدیریت فنی پروژه را قبلاً در کاشف نداشتیم. در مورد برخی از پروژه‌های بانک مرکزی مشخص است که باید در چه واحد تخصصی اجرا شوند ولی برای تعیین جزئیات و نحوه اجرای برخی از این پروژه‌ها نیاز به بررسی بیشتر است. نکته دیگر هم این است که در یک سبب پروژه، آن‌ها نسبت به همدیگر تقدم و تأخر دارند مثلاً اینکه آیا این‌ها همگی قابلیت اجرای هم‌زمان دارند، آیا می‌توان با منابع موجود کنونی کاشف از آن‌ها استفاده کرد، آیا لازم است برای پروژه، جذبی صورت بگیرد و جایگاه آن در نقشه استراتژیک امنیت بانک مرکزی کجاست یعنی چقدر می‌تواند بانک

بین مشتری و بانک شکل نمی‌گیرد. از یک سو برای ایجاد ساختار و بستری امن جهت ارائه خدمات بانکی، استانداردهای مختلفی وجود دارد و از سوی نهادهای حاکمیتی متعددی مثل مرکز مدیریت راهبردی افتا، سازمان پدافند غیرعامل، سازمان حراست کل کشور و ... هر کدام دستورالعمل‌های خودشان را در مورد بانک‌ها دارند که اجرائی آن‌ها الزامی است. از این رو این چارچوب کنترلی را تهیه کرده‌ایم که همه این الزامات و استانداردها در آن یکپارچه و یکدست بشود. همچنین این چارچوب کنترلی بر مبنای ریسک‌هایی تدوین شده که یک بانک می‌تواند به زیرساخت حیاتی مالی و پولی کشور تحمیل کند. عواملی چون تعدد شعب و میزان ارائه خدمات بر بستر وب می‌توانند در این مورد، تعیین‌کننده باشند و اینکه هر بانکی بر اساس شرایط و ویژگی‌های خود باید چه الزاماتی را مدنظر قرار بدهد. این چارچوب کنترلی دارای ۱۳۰۶ الزام، ۶ حوزه و ۱۶ زیرحوزه است. برای مثال، یکی از حوزه‌هایی که در سال‌های اخیر، بانک‌ها خیلی از آن متأثر شده‌اند تأمین خدمات است که معمولاً بانک‌ها آن را برون‌سپاری می‌کنند و زیرساخت آن بیرون سازمان است. متأسفانه اکثر حملات سایبری از همین جا صورت می‌گیرند. یکی از موضوعاتی که در چارچوب کنترلی به بانک‌ها توصیه کرده‌ایم الزاماتی است که باید در این مورد به آن‌ها دقت کنند چون بر اساس آمار، بیشترین ریسک را به آن‌ها تحمیل کرده است.

در حال حاضر بابت عدم استفاده از این چارچوب در بانک‌ها اقدام تبیهی صورت نمی‌گیرد. نگاه ما به بانک‌ها یک نگاه حمایتی، پرسش و پاسخ و مشاوره‌ای است و بانک مرکزی باید تصمیم بگیرد که به چه صورت و با چه استراتژی، الزام به اجرای این چارچوب را در بانک‌ها مورد پیگیری قرار دهد؛ اما کاری که ما در کاشف انجام می‌دهیم صرفاً نقش حمایتی و پشتیبانی از بانک‌هاست و برای آن،

مرکزی را نسبت به تهدیدات پیرامونش مصون کند بر اساس ابلاغیه‌های بانک مرکزی و مرکز مدیریت راهبردی افتا، اپلیکیشن‌هایی که به هاب فناوران یا همان سامانه تابش اتصال پیدا می‌کنند باید حتماً گواهی‌نامه کاشف را دریافت کرده و سالانه تمدید کنند. ما متعهدیم گزارش این کار را به بانک مرکزی، شاپرک و همچنین متولی یا سازنده آن اپلیکیشن بدهیم. بانک مرکزی، ما را در بخش زیرساخت کلید عمومی PKI به عنوان ارزیاب و ممیز معرفی کرده است. همچنین برای سامانه‌هایی که بانک‌ها تحت عنوان RA، RO و CA تولید می‌کنند و یا هنگام راه‌اندازی سرویس نماد و اتصال به آن، موظفیم بررسی‌های لازم را انجام داده و نتیجه آن را به بانک مرکزی اعلام کنیم. همچنین سرویس‌هایی که باید به سامانه کهربا و چکاد بانک مرکزی متصل شوند باید ابتدا در آزمایشگاه کاشف ارزیابی شوند و تأییدیه دریافت کنند.

تدوین الزامات چارچوب کنترلی

ما برای ایجاد امنیت در بانک‌ها و مؤسسات پولی، پروژه مهمی در واحد انطباق سنجی داشتیم تحت عنوان تدوین الزامات چارچوب کنترلی. بانک‌ها، علاوه بر رسالت و کسب‌وکار تعریف شده‌شان، یک سری استانداردهایی هم برای فعالیت‌ها و ارائه خدمات دارند. از طرفی هم برای اینکه خدمات خود را در سریع‌ترین زمان ممکن به مشتری ارائه بدهد آن‌ها را روی بستر اینترنت آورده‌اند تا بتوانند خدماتشان را در لحظه و در هرجایی ارائه بدهند. چنین ساختاری برای اینکه در اختیار مشتری قرار بگیرند علاوه بر زیرساخت فنی به زیرساخت و الزامات امنیتی هم نیاز دارد. اگر خدمت ارائه شده توسط بانک، امن نباشد طبیعتاً هیچ اعتمادی



استعلام‌هایی که از بانک‌ها می‌گیریم قابل ارائه است. طبیعتاً بقیه نهادهای متناظر مثل مرکز مدیریت راهبردی افتا هم علاقه‌مند به دریافت این گزارش‌ها هستند و این انتظار را از بانک مرکزی و کاشف دارند که به صورت جدی این قضیه را پیگیری کنند و باید بتوانند گزارش‌هایی که برای انجام رسالت خود نیاز دارند از ما دریافت کنند.

ساختن امنیت یک هنر است

درباره MSSP یا مرکز مدیریت شده امنیت، دو نگرانی بزرگ در کشور وجود دارد. نخست اینکه آیا سرویس دهنده، امکان سرویس دهی به حجم زیادی از مشتریان آن را دارد و دوم اینکه، تجمیع اطلاعات ضمن اینکه خیلی ارزشمند است می‌تواند یک تهدید جدید هم ایجاد کند. فرض کنید شما شرکتی کوچک در حال ارائه خدمات گسترده‌ای بر بستر وب هستید تا با کم‌هزینه‌ترین حالت ممکن، بتوانید از طریق بازار رقابتی جدیدی که بر بستر اینترنت شکل گرفته و البته امنیت آن هم قابل اتکا نیست، در سریع‌ترین زمان ممکن خدمات خود را به کاربران نهایی در هر نقطه‌ای ارائه دهید. نمونه آن در دنیا و در ایران فراوان است؛ اما یکی از چیزهایی که شرکت‌ها را از پا درمی‌آورد همین امنیت اطلاعات است. شما ترجیح می‌دهید برای حفظ امنیت، نفرت و فناوری مفصل و پرهزینه‌ای را به کار بگیرید یا اینکه خدماتی متناسب با نیاز خود بخرید؟ MSSP مانند بنگاه‌های ارائه خدمات آی تی عمل می‌کند و سرویس‌های مانیتورینگ، پایش، شناسایی و غیره ارائه می‌دهد. ایدئال در MSSP آن است که fully automated service ارائه شود تا شرکت‌ها بتوانند پکیج‌های سرویس‌های موردنظرشان را انتخاب کرده و در کنار سرویسی که می‌دهند، بگذارند. دسترس پذیری سرویس، هم خیلی مهم است و موضوع دیگر در مورد امنیت یک سرویس این است که باید امنیت آن را بسازید و بالا ببرید و نمی‌توانید یک باره آن را ایجاد کنید. مورد دیگر هم اینکه ساخت و ساز امنیت، یک هنر است و همه این هنر را ندارند. MSSP می‌تواند سرویسی مناسب را پیشنهاد بدهد و فارغ از برند و تکنولوژی به کاررفته در آن، تضمین کند که می‌توان از آن استفاده کرد یا خیر.

کسب‌وکاری که در حوزه امنیت ایجاد می‌کنیم یک نهاد متولی دارد که الزامات و قواعد آن را مشخص کرده است. هر کسی که متولی این موضوع می‌شود باید این نظام‌نامه را ایجاد کند و نگرانی نهاد ناظر این است که MSSP نظام‌نامه را ندارد. نهاد ناظر چون قواعد لازم را برای رگولاتوری ندارد مایل به ایجاد آن نیست اما نیاز به ایجاد آن در بازار به گونه‌ای است که باید راه بیفتد. رگولاتوری می‌تواند به جای اینکه مانع ایجاد آن بشود با استفاده از ظرفیت‌های نخبگان، کاشف و پژوهشگاه فناوری اطلاعات و ارتباطات و غیره در مورد نظام‌نامه آن اقدام کند.

نه برنامه تشویقی داریم و نه اقدام تنبیهی. کاشف در نقش یک مشاور به بانک، برنامه و آموزش ارائه می‌دهد که بتواند این الزامات را اجرا کند و اگر مشکلی داشتند با برگزاری جلسات و مشاوره به آن‌ها کمک می‌کند.

چارچوب کنترلی در فروردین ماه ۱۴۰۲ توسط مرکز مدیریت راهبردی افتا به عنوان یک مستند لازم‌الاجرا به بانک‌ها ابلاغ شد. برای تسهیل کار بانک‌ها یک سامانه اختصاصی هم بر اساس همین چارچوب کنترلی، طراحی و تدوین کردیم که اگر بانکی مایل به دریافت این خدمت باشد در اختیارشان می‌گذاریم تا بتوانند روی تمام این الزامات، مدیریت داشته باشند و از آن استفاده کنند. پیاده‌سازی چارچوب کنترلی در کوتاه مدت کار آسانی نیست و جذب نیروی انسانی متخصص، ارتقای دانشی کارکنان و استفاده از تکنولوژی‌های به روز برای ارائه بهتر خدمات از جمله پیش‌نیازهایی است که بانک‌ها باید به آن‌ها توجه کنند.

این استاندارد، یک سری بایدو نباید را مشخص می‌کند، اما تقدم و تأخر آن نیاز به سفارشی‌سازی یا به عبارتی نیاز به تن‌دوخت دارد و هر بانکی باید بتواند، آن را متناسب‌سازی کند. بانک‌ها با شرکت در دوره‌هایی که در کاشف برای آن‌ها تدارک می‌دهیم می‌آموزند که باید چگونه از آن استفاده کنند.

در بانک مرکزی هم به یک کمیته راهبری نیاز داریم تا ببینیم که این چارچوب کنترلی را چگونه باید جلو ببرند و این کار باید به صورت مشارکتی و فعال بین کسانی که می‌خواهند استراتژی و راهبرد را مدیریت کنند، شکل بگیرد. برای ممیزی پیاده‌سازی چارچوب کنترلی در بانک‌ها، از طریق خوداظهاری‌های دوره‌ای از بانک‌ها استعلام می‌گیریم و وضعیت سنجی می‌کنیم. این یک مسیر بسیار طولانی و مستمر است که باید با کمک سه رکن بانک مرکزی، بانک‌ها و شرکت کاشف پیش برود و پیشرفت کند چارچوب کنترلی یک استاندارد خشک و مطلق نیست و باید انعطاف‌پذیر باشد؛ بنابراین از هم‌اکنون با تشکیل یک تیم، تحقیق و توسعه این چارچوب را بر اساس تغییرات استانداردهای بین‌المللی و دستورالعمل‌های جدیدی که نهادهای بالادستی می‌دهند در دستور کار قرار داده‌ایم تا با تغییرات اکوسیستم مالی، کسب‌وکارها، استانداردها و تکنولوژی همگام باشیم و قاعدتاً به روزرسانی سامانه آن هم باید بر اساس تغییرات این چارچوب صورت بگیرد.

طبیعی است که باید گزارش‌های ادواری از وضعیت اجرای چارچوب کنترلی در کل بانک‌های کشور به بانک مرکزی ارائه شود. اکنون برای معاونت فناوری‌های نوین بانک مرکزی، بخشی از این ممیزی‌ها، انطباق سنجی‌ها، خوداظهاری‌های بانک‌ها و روند پیشرفت را پیاده‌سازی کردیم و امکان رصد لحظه‌ای آن فراهم است. همچنین گزارش ادواری و منظم آن به شیوه‌های مختلف در قالب

مدیریت عملکرد با متد OKR و اهمیت آن در افزایش بهره‌وری نیروی انسانی

برنامه‌ریزی OKR، این سازمان‌ها کوشیده‌اند که چارچوبی را برای اهداف خود تعیین کنند. به وسیله OKR می‌توان با تعریف اهداف و نتایج اصلی و کلیدی، فرایندهای سازمانی را مدیریت کرده و به سمت موفقیت حرکت کرد. پیاده‌سازی سیستم OKR یکی از مهم‌ترین گام‌های موفقیت است که همه مدیران باید به آن توجه داشته باشند.

اجرای نمودن مدیریت عملکرد در سازمان با متد OKR فقط زمانی به درستی عمل کرده و باعث افزایش بهره‌وری خواهد شد که اولاً فرایندهای سازمان و علی‌الخصوص فرایندهای منابع انسانی از بلوغ مناسبی برای اجرای کردن آن برخوردار بوده و در ثانی پشتیبانی لازم به منظور پیاده‌سازی OKR توسط عالی‌ترین سطوح سازمان وجود داشته باشد؛ بنابراین، پیش از اقدام، باید شرایط سازمان به دقت بررسی شود. برای اطلاع از آمادگی سازمان خود برای پیاده‌سازی فرآیند مدیریت عملکرد با متد OKR، باید عواملی در نظر گرفته شوند که مهم‌ترین آن‌ها به شرح زیر است:

■ پذیرش و شفافیت: همه مدیران و کارکنان باید پذیرای شفافیت در فرایندها باشند؛ بنابراین، یکی از شروط پیاده‌سازی OKR، پذیرش و آمادگی کارکنان برای ایجاد تغییرات است.

■ چشم‌انداز و مأموریت: چشم‌انداز (آینده آرمانی) تصویری از آینده است که یک مجموعه قصد دارد در زمان مشخصی به آن دست یابد یا به عبارتی دیگر آرزوهای آتی و اهداف مجموعه در شرایط کنونی است که می‌خواهد زمانی به آن‌ها دست یابد. مأموریت عبارت است از فلسفه وجودی و یا نقشی که یک مجموعه در قبال جامعه خود، برعهده گرفته تا با ایفای آن و ارائه خدمات مورد نظر، نیازهایی از جامعه را برآورده سازد. به عبارت دیگر می‌توان گفت، مأموریت یک بیان کلی از نیت مجموعه است که با استفاده از نقطه نظرات مدیران ارشد آن مجموعه، تعریف و تصریح شده و در قالب «بیانیه مأموریت» مجموعه ارائه می‌گردد.

■ فرهنگ سازمانی: در سازمان شما باید فرهنگ پذیرش و قدردانی نهادینه شده باشد. این مسئله باعث می‌شود که در فرایند برنامه‌ریزی OKR، اشتباهات منجر به یادگیری شوند.

■ رهبری مناسب: یکی از مهم‌ترین عناصر پیاده‌سازی OKR مربوط به سبک رهبری سازمان است. در فرآیند مدیریت عملکرد با متد OKR، هدف به جای توییح و مچ‌گیری بر توسعه و یادگیری متمرکز است.

■ کارکنان به‌عنوان مهم‌ترین سرمایه هر سازمان به حساب می‌آیند. به همین منظور سازمان‌های امروزی برای افزایش بهره‌وری کارکنان خود اقدام به تدوین، برنامه‌ریزی و اجرای فرایندهای مختلف می‌کنند. بهره‌وری نیروی انسانی را حداکثر استفاده مناسب از نیروی انسانی به منظور حرکت در جهت اهداف سازمان با کمترین زمان و حداقل هزینه دانسته‌اند.

عوامل متعددی در افزایش بهره‌وری نیروی انسانی مؤثرند. از جمله این عوامل می‌توان به شناخت و توجیه شغل، حمایت سازمانی، دادن بازخورد و اصلاح عملکرد، آموزش و توسعه شایستگی، نظام جبران خدمات و ... اشاره کرد. از میان تمامی ابزارهای یادشده، به جرأت می‌توان گفت که در سازمان‌های پیشرفته و پیچیده امروزی، ارزیابی و مدیریت عملکرد مهم‌ترین ابزار مدیریتی برای افزایش بهره‌وری نیروی انسانی است. هیچ فرآیند مدیریتی دیگری نیست که چنین تأثیری بر مسیر حرفه‌ای کارکنان داشته باشد. اگر از ارزیابی و مدیریت عملکرد به درستی استفاده شود، قدرتمندترین ابزاری است که به هدایت انرژی افراد به سوی اهداف استراتژیک سازمان کمک خواهد کرد.

مدیریت عملکرد (Performance Management) که مفهومی متفاوت از ارزیابی عملکرد (Performance Evaluation) است، به‌عنوان فرآیند ارتباط و بازخورد مداوم بین مدیران و کارکنان در جهت نیل به اهداف سازمان تعریف می‌شود. به تعبیری دیگر مدیریت عملکرد به مدیران کمک می‌کند تا انتظارات خود را از کارمندان به‌طور دقیق به آن‌ها منتقل کنند تا اطمینان حاصل کنند که همه کارکنان در باره فعالیت‌های جاری خود، اهداف بلندمدت، مسئولیت‌ها، پروژه‌ها و همچنین نحوه انجام دادن آن کارها به درک درستی رسیده‌اند.

در ادامه لازم است نگاهی به OKR داشته باشیم. OKR مخفف عبارت Objective & Key Results بوده و به معنای اهداف و نتایج کلیدی تعریف می‌شود. هدف صرفاً همان چیزی است که باید محقق شود. نتایج کلیدی نیز مجموعه‌ای از معیارهاست که پیشرفت به سمت هدف را اندازه‌گیری می‌کند. در این مدل، روش‌هایی برای تعریف و پیگیری اهداف و ارزیابی نتایج آن‌ها معمولاً به صورت فصلی و سالانه وجود دارد.

شرکت‌های پیشروی جهان از مدل OKR برای اندازه‌گیری دقیق نتایج و دستیابی به اهداف خود استفاده می‌کنند. شرکتی مانند گوگل و یا آمازون موفقیت بی‌سابقه خود را مدیون مدل OKR هستند. با استفاده از

هدف‌گذاری و برنامه‌ریزی عملکرد:

برخلاف نظام‌های سنتی ارزیابی عملکرد که شاخص‌های ارزیابی بدون دخالت کارمند تدوین می‌شد و در اکثر مواقع با سمت و سوی اهداف شرکت همخوان نبود، در نظام مدیریت عملکرد با متد OKR، برنامه‌ریزی عملکرد که از چشم‌انداز و اهداف اصلی سازمان مایه می‌گیرد، در سطح فرد با مشارکت مستقیم کارمند انجام می‌شود؛ بنابراین برنامه‌ریزی عملکرد نوعی بحث و گفتگو میان مدیر و کارمند (ارزیاب و ارزیابی‌شونده) است که در خصوص موضوعات ذیل توافق انجام می‌شود:

- توافق بر روی مسئولیت‌های اصلی فرد
- توافق در خصوص اهداف و مقاصد که کارمند باید به آن‌ها دست یابد.
- مشخص کردن مهم‌ترین شایستگی‌هایی که کارمند در طول دوره ارزیابی باید از خود نشان دهد.
- تدوین طرح توسعه فردی مناسب برای تعیین اهداف درستی که منجر به بهره‌وری گردد الزام است از بیانیه مأموریت، چشم‌انداز و ارزش‌های سازمان تا راهبردها و برنامه‌های سازمان و برنامه‌های عملیاتی واحد، اهداف شغل، خواسته‌ها و ... استفاده شود.
- پیش از پیاده‌سازی مدیریت عملکرد با متد OKR باید مشخص باشد که چه اهداف معینی دنبال می‌شود. لزومی ندارد که این اهداف برای پیاده‌سازی مدیریت عملکرد در یک دوره طولانی باشند؛ در واقع می‌توان اهدافی را تعیین کرد که به‌مرور دچار تحول شده و به‌روزرسانی شوند. از این طریق، همیشه می‌توان خود را با تغییرات وفق داده و به شکل موثقتری اهداف را دنبال کرد.

انجام ارزیابی با حمایت و مربی‌گری مدیر:

بعد از مرحله برنامه‌ریزی عملکرد، زمان انجام کار توسط کارمند است. در این دوره کارمند و مدیر وظایفی دارند که اگر به‌درستی انجام شود منجر به افزایش بهره‌وری کارکنان خواهد شد. ذکر این نکته مهم است که یکی دیگر از تفاوت‌های نظام جدید مدیریت عملکرد با نظام‌های سنتی این است که در نظام‌های سنتی که عمدتاً با عنوان ارزیابی عملکرد نامیده می‌شوند، کارکنان در طول دوره ارزیابی رها شده و حمایتی در راستای کسب اهداف دریافت نمی‌کنند ولی در فرآیند مدیریت عملکرد مدیر (ارزیاب) دو نقش مهم را بر عهده دارد: اول ایجاد محیط انگیزشی برای به حداکثر رساندن عملکرد کارمند و دوم رفع موانع عملکرد. ارائه بازخورد از رفتار و عملکرد کارمندان در این مرحله اهمیت ویژه‌ای دارد. همه مدیران وظیفه دارند عملکرد افراد واحد خود را پیگیری کرده و در مواقع لزوم در خصوص اصلاح و بهبود عملکرد با کارکنان خود صحبت کنند.

نقش OKR در این مرحله نیز پررنگ است. چراکه اهداف فرد با اهداف سازمان همسو گردیده و این موضوع باعث افزایش انگیزه کارکنان در اجرای وظایف و مسئولیت‌های محوله خواهد شد.

ارزیابی عملکرد و ارائه بازخورد به منظور اصلاح و بهبود

عملکرد:

مدیر در پایان دوره ارزیابی، رفتار و عملکرد کارکنان را در مقایسه با آنچه توافق و در مورد آن هدف‌گذاری شده بود ارزیابی می‌نماید. به منظور اثربخش بودن ارزیابی عملکرد، مدیر مسئولیت‌هایی به شرح ذیل دارد:

- مرور مجدد توافق‌نامه عملکرد شامل مرور فهرست اصلی شایستگی‌ها، اهداف بلندمدت، اهداف کوتاه‌مدت و مسئولیت‌های اصلی شغل
- مرور وقایع ثبت‌شده در طول دوره ارزیابی به منظور یادآوری نقاط قوت و قابل‌بهبود کارمند. در مرحله ارزیابی عملکرد، مدیر در ابتدا به‌تنهایی اقدام به تکمیل فرم ارزیابی عملکرد کارکنان نموده و در مرحله بعد با دقت و جزئیات به کارمند نشان می‌دهد که کارمند در کدام عملکردها و رفتارها در حد انتظار و قابل‌قبول بوده و در



کدام رفتارها و عملکردها ماورای انتظار و استاندارد عمل کرده است و بالاخره در کدام رفتارها و عملکردها ضعیف بوده و اهداف و انتظارات را تأمین نکرده است. در نهایت با بازنگری در عملکرد، تعریف برنامه‌های توسعه‌ای به منظور تقویت نقاط قابل‌بهبود و بهبود چرخه عملکرد، فرآیند برای دوره بعدی از نو آغاز می‌گردد.

سخن پایانی

امروزه سازمان‌های مطرح دنیا و سازمان‌های بزرگ کشور از مدیریت عملکرد با رویکرد OKR استفاده می‌کنند تا با افزایش بهره‌وری نیروی انسانی تغییرات مثبتی را در سطح سازمان ایجاد کرده و به شکل مؤثری به سمت اهداف خود حرکت کنند. موفقیت در اجرائی نمودن مدیریت عملکرد با متد OKR به اجرای مراحل دقیقی نیاز دارد. آموزش و فرهنگ‌سازی مطلوب برای کلیه کارکنان، استفاده از نرم‌افزار مدیریت عملکرد و پشتیبانی مطلوب توسط عالی‌ترین مقام سازمان، موفقیت پیاده‌سازی این فرآیند را تضمین خواهد کرد.

هدف ما رسیدگی مستمر به رخدادهای بانکی است

معاون واحد مدیریت ماهر بانکی کاشف می گوید که این بخش، عملیات امنیتی دو حوزه رخدادهای بانکی و رخدادهای سایبری را پیگیری می کند. آنچه در ادامه آمده است صحبت های بهرام یعقوب زاده آشوریان است که به تشریح سامانه ها و عملکرد این بخش می پردازد.

ماهر بانکی، مسئول رسیدگی به تمام ناهنجاری ها و اختلالاتی است که در حوزه رخدادهای بانکی و رخدادهای سایبری در نظام بانکی رصد و شناسایی شده است و یا ممکن است بطور بالقوه اتفاق بیفتد؛ تا جاییکه از رفع کامل تهدید اطمینان حاصل نماید.

از رصد تا شناسایی

در حقیقت کار ما با رصد فضای تهدیدات امنیت اطلاعات در نظام بانکی و پرداخت شروع می شود و بعد به پایش تهدیدات با استفاده از حسگرهای تشخیص نفوذ به کار گرفته شده در موجودیت های نظام بانکی هم می رسیم. رصد با پایش تفاوت دارد. رصد زمانی است که ما در فضای تبادل اطلاعات به دنبال تهدیدات می گردیم. ما در فضای تهدید جست و جو می کنیم. در اقیانوسی از اتفاقات و اخبار غواصی می کنیم تا آن چیزی هایی را که به خودمان و تهدیدات نظام بانکی و پرداخت مربوط می بینیم جمع آوری کنیم. مثلاً می خواهیم ببینیم آیا روی محصولات سیسکو که در نظام بانکی ما استفاده می شود آسیب پذیری جدیدی آمده است یا نه. باید CVE آن را شناسایی کنیم و روزانه به بانکها اطلاع بدهیم. این کار همان رصد آسیب پذیری های عمومی بر روی محصولات پرکاربرد است. از طرف دیگر به دنبال آسیب پذیری های خاص خدمات و محصولات لبه شبکه بانکی می گردیم. این خدمت که با نام پویبش آسیب پذیری های بانکی (پاسبانک) ارائه می شود، بصورت جعبه سیاه و موردی به شناسایی نقاط ضعف و آسیب پذیری های فناورانه و منطقی بر روی محصولات و خدمات قابل مشاهده از بستر اینترنت می پردازد. مثلاً فلان بانکی که اینترنت بانک و موبایل بانک دارد آیا با تهدید از بستر اینترنت مواجه هست یا نه و همان طور که هکر و مهاجم، آن تهدید را می بیند ما هم آن را ببینیم و پیش از آنکه از آن آسیب پذیری سوء استفاده شود، آنرا رفع کنیم. این می شود اشراف اطلاعاتی در فضای تهدیدات سایبری که ما به آن می گوئیم رصد تهدیدات.

اما پایش، مربوط می شود به آن حملاتی که به سمت دارایی هایمان می آیند و حسگرهای ما آنها را شناسایی می کنند. فایروالها، هانی پاتها، SOCها و... همان ابزارها و حسگرهایی هستند که وقوع تهدید بر روی دارایی های ما را شناسایی می کنند. در واقع در خدمات رصدی، ما به سراغ

اتفاقات می رویم و در خدمات پایشی، اتفاقات به سراغ می آیند. این گونه که به شبکه حمله می شود و سنسورهای ما باید این حملات را تشخیص بدهند.

تلاش ما در ماهر بانکی این است که ظرفیت های پایش و شناسایی تهدیدات را هم برای بانک مرکزی و هم برای نظام بانکی تقویت کنیم؛ یعنی ما نقش رگولاتوری و تنظیم گری را برای هماهنگی و قانون گذاری و تعیین و تبیین الزامات ایفا می کنیم؛ اینکه باید چه چیزهایی را و چگونه شناسایی کرد و به چه نحوی باید مانع آنها شد. البته تا کید می کنم که ما عملیات داخل بانک را پایش نمی کنیم. ما تهدیدات را برایشان رصد می کنیم، اما پایش بر عهده ی خود بانک است، چون سنسورهای آنها را در اختیار نداریم. ولی کاری که انجام می دهیم این است که داریم ظرفیت های پایش بانکها را با ارائه الزامات، پرسش نامه ها و رتبه بندی کردن بانکها بر اساس توانایی های تشخیصی آنها بالا می بریم. یعنی سعی می کنیم انطباق بانکها را هرچه بیشتر با این الزامات و قانون گذاری های صورت گرفته نزدیک کنیم.

از هماهنگی تا واکنش سریع

وقتی که نظام بانکی یک اتفاق را به ما گزارش می دهد وظیفه ما نشان دادن واکنش سریع به آن رخداد است و در این مورد مسئولیت داریم. موضوع هماهنگی و واکنش به رخداد یکی از خدمات واکنشی است که در همه دنیا به آن اهمیت بسیاری داده می شود و آن این است که بتوانیم اطلاعات مربوط به اتفاقی که برای یک بانک افتاده به بانکهای دیگر منتقل کنیم و درس آموخته ها خیلی سریع اشتراک گذاشته شود. ما در ماهر بانکی در قالب خدمات واکنشی، خدمات پیش دستانه و خدمات مدیریت کیفیت امنیت مطابق با چارچوب های استاندارد خدمات هماهنگی در واکنش به رخداد را ارائه می دهیم. در واقع خدمات CERT کاشف بعنوان ماهر بانکی (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای) بنحوی فرادست گوهرها (واکنش هماهنگ رخدادهای رایانه ای) قرار می گیرد که ذیل بانکها کار می کنند و در حقیقت هماهنگی آنها را برعهده دارد. این نقش بسیار پررنگی است و با توجه به جایگاه کاشف در صنعت امنیت نظام بانکی، نقش خیلی مهمی است. بویژه با توجه به نقش اپراتور امنیت این موضوع پررنگ تر هم می شود و توقع مراجع امنیتی در این حوزه نیز رو به افزایش است.

واکنش به رخدادهای یک جنبه دیگر هم دارد و آن امداد سایبری و عملیات فارتیک در محل است. بانکها بسیار مایل هستند که بتوانیم در فارتیک به آنها کمک کنیم. اینجا کاشف دو نگاه دارد. یکی نگاهی با عنوان گزارش دهنده به مراجع امنیتی و دیگری با نگاه همدلانه و مسئولانه به موجودیت های نظام بانکی. ما برای کمک به نظام بانکی هم ظرفیت های خوبی را از نیروی انسانی متخصص تا تجهیزات پیشرفته ایجاد کرده و امیدواریم به هنگام وقوع رخداد بتوانیم با انرژی و پتانسیل زیادی نسبت به ارائه این خدمات اقدام کنیم.

کار دیگر ماهر بانکی، تحلیل بدافزار است که اگر نمونه ای از بدافزار در هر کدام از موجودیت های نظام بانکی

گذاری اطلاعات تهدید مورد استفاده قرار می‌گیرند.
«پیکار» با فیشینگ و برنامه‌های جعلی

در ماهر بانکی، انواع سازوکارها و دامنه‌های فیشینگ و برنامه‌های جعلی و مخرب را هم رصد می‌کنیم که برای دادستانی موضوع قابل توجهی است. برای رصد فیشینگ یک سری بازوهای اجرایی نیز داریم که در کل کشور توزیع شده‌اند، یعنی مراکز آپای دانشگاهی که تیم‌های بزرگی متشکل از نیروهای متخصص باتجربه و همچنین دانشجویان را در اختیار دارند. آنها فضای مجازی و شبکه‌های اجتماعی را وا کاوی می‌کنند و هر جایی دامنه‌ای ببینند که با هدف فریب کاربران و کلاهبرداری ایجاد شده، آن را به سامانه پیکار اعلام می‌کنند. در واقع پیکار، سامانه جدید رصد ما است. مثلاً دامنه‌های شناسایی شده برای فیلتر شدن توسط کارگروه مصادیق مجرمانه اعلام می‌شوند یا سرورهای میزبان آن به پلیس فتا اعلام می‌شود تا مورد پیگرد قرار گرفته و بسته شوند. بازیگران تهدید در این حوزه از کمپین‌های تبلیغاتی و فضای شکل گرفته در اذهان عمومی نیز سوء استفاده می‌کنند و با ارسال پیامک‌های جعلی اقدام به فیشینگ قربانیان می‌کنند. فرض کنید دولت اعلام می‌کند قصد دارد به همه اقشار، سهام عدالت بدهد و کلاهبرداران به سرعت با ارسال پیامک‌ها و ترغیب افراد به نصب برنامه‌ها یا ورود به صفحات جعلی، وارد عمل می‌شوند و اطلاعات هویتی یا بانکی افراد را سرقت می‌کنند. ما برای شناسایی و مسدودسازی کل فرآیند کلاهبرداری وارد عمل می‌شویم.

چرخه شناسایی تا اشتراک گذاری از «رادار» تا «ساتا»

کاشف، سامانه‌ای را به اسم «رادار» (رویت آبی و دائم رخداد) راه‌اندازی کرده است. از طریق این سامانه، کاشف مجموعه‌ای از رخداد‌های نظام بانکی و شاخصه‌های تهدیدات به کارگرفته شده در آنها را از موجودیت‌های نظام

شناسایی شود، چه حین رخداد و چه بنا به ارجاع بانک، آنها را تحلیل و رسیدگی کرده و واکنش متناسب را نشان می‌دهیم. ماهر بانکی بصورت مستمر روند بدافزارهای فعال در دنیا، منطقه و کشور را دنبال می‌کند و گزارش‌های تحلیلی دوره‌ای و موردی در اختیار نظام بانکی قرار می‌دهد.

اشتراک‌گذاری اطلاعات تهدیدات

بعد از همه اینها برای اینکه به‌واسطه جایگاه مرکز کاشف، بتوانیم بقیه بانک‌ها را هم از این اطلاعات تهدید بهره‌مند کنیم باید کاری انجام دهیم. اینجاست که موضوع اشتراک‌گذاری و هوش تهدید پیش می‌آید و برای آن در حال توسعه‌ی سامانه اشتراک‌گذاری اطلاعات تهدیدات امنیتی (ساتا) را تعریف کردیم. ساتا در واقع پلتفرم زیرساختی Threat Intelligence است. این سامانه که با همت تیم توسعه خدمات کاشف، توسعه می‌یابد به زودی در دسترس قرار می‌گیرد و در حال حاضر واحد ماهر، این سرویس را با ابزارهای خارجی و اوپن سورس ارائه می‌دهد. اتفاقی که می‌افتد این است که ما همه شاخصه‌های تهدیدات (IOC) استخراج شده از رخداد‌های ارجاع شده به ماهر بانکی کاشف در قالب سامانه رادار را غنی‌سازی می‌کنیم و در کنار اطلاعاتی که از رصد و پایش بدست آمده یا در قالب خوراک از منابع اطلاعات تهدید در دنیا، منطقه و کشور بدست آمده است را همبسته‌سازی می‌کنیم و دانش تولید شده را با بانک‌ها به اشتراک می‌گذاریم.

صدای «رسا» در فضای تهدید

سامانه رصد سریع اخبار (رسا) برای رصد اخبار فضای تهدید ایجاد شده است. قبل از این، ماهر بانکی کاشف روزانه از بین چند صد میلیون خبر، از طریق دسته‌بندی کلیدواژگان و با بکارگیری نیروی انسانی، اخبار مهم و مرتبط با حوزه تهدیدات کاشف استخراج و رسیدگی می‌شد. اما در سامانه رسا این کار با ظرفیت‌های هوش مصنوعی و یادگیری عمیق تا حد قابل توجهی بصورت خودکار انجام می‌شود. این سامانه مرتبط بودن اخبار با تهدیدات حوزه امنیت و فضای بانکی و همچنین میزان اعتبار اخبار را تشخیص می‌دهد. تهدیدات شناسایی شده در اخبار جهت رسیدگی و اشتراک



راستای الزامات مورد انتظار اطمینان حاصل کرده و به بانک بازخورد بدهیم.

سپری برای بانکها

موضوع استقبال و تمایل بانکها به استفاده از سرویسهای ما چه از لحاظ ساختاری و چه از لحاظ رویه‌ای و نیروی انسانی بیش از همه برمی‌گردد به رویکرد ما در نظام بانکی به عنوان تنظیم‌گر حوزه امنیت اطلاعات. ما لازم است اعتماد نظام بانکی را به نحوی جلب کنیم که اگر کاشف از آنها اطلاعاتی خواست بدانند قرار نیست با استفاده از آن اطلاعات آنها را زیر سوال ببرد بلکه می‌خواهد با این اطلاعات به کمک آنها بیاید که اتفاقی برایشان نیفتد. این برمی‌گردد به رویکرد ما که هم بخش نظارت و هم ماهر بانکی کاشف در این موضوع خیلی نقش دارند؛ اینکه ما کنار بانکها احساس بشویم و نه روبروی آنها.

ما باید ضعف‌هایشان را ببینیم تا آنها را رفع کنیم. یعنی با بودن کاشف در کنار خودشان احساس مثبتی از اعتماد و امنیت داشته باشند و ظرفیت و توانمندی‌هایشان را از طریق کاشف با سایرین در این نظام به اشتراک بگذارند. برای تبدیل شدن به یک پلتفرم اشتراک‌گذاری اطلاعات، اعتمادسازی بسیار مهم است. ما باید بتوانیم کاشف را به پلتفرم قابل اعتمادی برای بانکها تبدیل کنیم که بانکها از طریق آن با همدیگر ارتباط داشته باشند و نگران نباشند که اطلاعاتی که با سایر بانکها در میان می‌گذارند مزیت‌های رقابتی‌شان را از بین ببرد و بدانند که این ارتباطات بصورت دوجانبه و جنبه سازنده دارد.

توانمندسازی در «آکادمی امنیت»

یکی از محورهای استراتژیک و راهبردی کاشف همیشه توانمندسازی نیروی انسانی متخصص در نظام بانکی بوده است. یکی از پروژه‌هایی که مدیریت کاشف به دنبال آن است، ایجاد آکادمی امنیت برای نظام بانکی است. این آکادمی می‌تواند هم از ظرفیت‌های آموزشی نیروهای کاشف، بانکها و همچنین خبرگان حوزه امنیت در بخش خصوصی استفاده کند و با اشراف به نیازمندی‌های عملیاتی بانکها، نگاهی کاربردی به مسئله آموزش داشته باشد. توانمندسازی ظرفیت‌های تخصصی موجودیت‌های نظام بانکی هم‌راستا با اهداف و مأموریت‌های حاکمیتی کاشف است. اگر بانکی بتواند رخدادی را بهتر شناسایی و مدیریت کند، کاشف در مأموریت خود موفق عمل کرده و در ارتقای امنیت صنعت بانکی توفیق داشته است.

آنچه در بانکها دیدیم

در شناسایی و رسیدگی به آسیب‌پذیری‌های خاص خدمات و محصولات بانکی به مواردی برخورد کرده‌ایم که نمونه‌های جالبی برای بازگ کردن هستند. مثلاً بانکی را دیدیم که سامانه گرافیکی تمام ماشین‌های حمل پول به صورت لایو در هر خیابانی و در هر شهری به سادگی از طریق وب در دسترس بود؛ که بسیار خطرناک بوده و در صورت سوء استفاده‌ی بدخواهانه، تبعات آن می‌توانست بسیار فراتر از حوزه سایبری باشد. یا مثلاً مواردی را داشتیم که کپی کامل از سامانه نرم‌افزاری یک بانک روی وبسایت در یک فایل زیپ شده بارگذاری شده و اصطلاحاً جا مانده بود. ظاهراً برنامه‌نویس می‌خواست آیدیتی را انجام دهد ولی بعد فراموش کرده بود که فایل را حذف کند.

بانکی گردآوری و برای مراجع امنیتی و بانک مرکزی، تجمیع و داشبورد می‌کند. همچنین شاخصه‌های تهدیدات مثل آدرس مهاجم و روش حمله و غیره استخراج شده و به سامانه اشتراک‌گذاری اطلاعات تهدیدات امنیتی (ساتا) می‌فرستد تا با غنی‌سازی خوراکها و فیدها، اطلاعات تحلیلی را به خود بانکها برگرداند و سایر ذی‌نفعان را بصورت پیش‌دستانه از تهدید مطلع کند.

«وسعت» در «سرآمد»

ماهر بانکی همچنین وظیفه‌ی رسیدگی به دستورات قضایی را نیز برعهده دارد و واسطه‌محوری و نقطه اتصال بین دو نهاد بزرگ دولتی یعنی نظام قضایی با نظام بانکی است. این خدمت که در قالب سامانه‌ی سرآمد عملیاتی می‌شود، در واقع ظرفیت ثبت و رسیدگی سریع و آنلاین ۲۴ ساعته دستورات قضایی را مطابق با توافقات سطح خدمات (SLA) فراهم می‌کند.

فعالیت دیگر ماهر بانکی ارائه خدمات، رصد سکوه‌های قمار و شرط‌بندی، انواع تقلب و کلاهبرداری و سایر وجوه عملیات مشکوک بانکی است که در قالب خدمات مرکز وسعت (واکاوی سریع عملیات مشکوک) ارائه می‌شود. اگر بخواهم به طور کلی و خلاصه بگویم استفاده سوء از زیست بوم و ابزارهای نظام بانکی و پرداخت را شناسایی و با آنها مقابله می‌کنیم. درگاه پرداخت جعلی، استفاده غیرمجاز از ابزارهای پرداخت، کارت‌های اجاره‌ای، روش‌های پول‌شویی، تقلب و کلاهبرداری و... مصادیق ناهنجاری‌های پولی و بانکی هستند که در سامانه «پیکار» تجمیع و گردآوری شده و بخشی را به سمت دادستانی ارجاع می‌دهد و بخشی را به بانک مرکزی، تا تبدیل به دستورات قضایی واکنشی شوند و نهایتاً توسط سامانه «سرآمد» به رسیدگی در نظام بانکی منتج شوند.

به این ترتیب چرخه کاملی از رصد فضای تهدید، پایش و شناسایی، تحلیل و رسیدگی و نهایتاً اشتراک‌گذاری اطلاعات را در هر دو حوزه رخدادهای بانکی و سایبری برعهده‌ی ماهر بانکی کاشف است. بخشی که همچنان قدری جای کار دارد و مهجور مانده و باید بیشتر به آن پرداخته شود اشتراک‌گذاری اطلاعات تهدیدات بانکی است که هنوز کم‌رنگ است. یعنی باید به سمت اشتراک‌گذاری اطلاعات تقلب و کلاهبرداری با مردم، نظام بانکی و نظام پرداخت برویم.

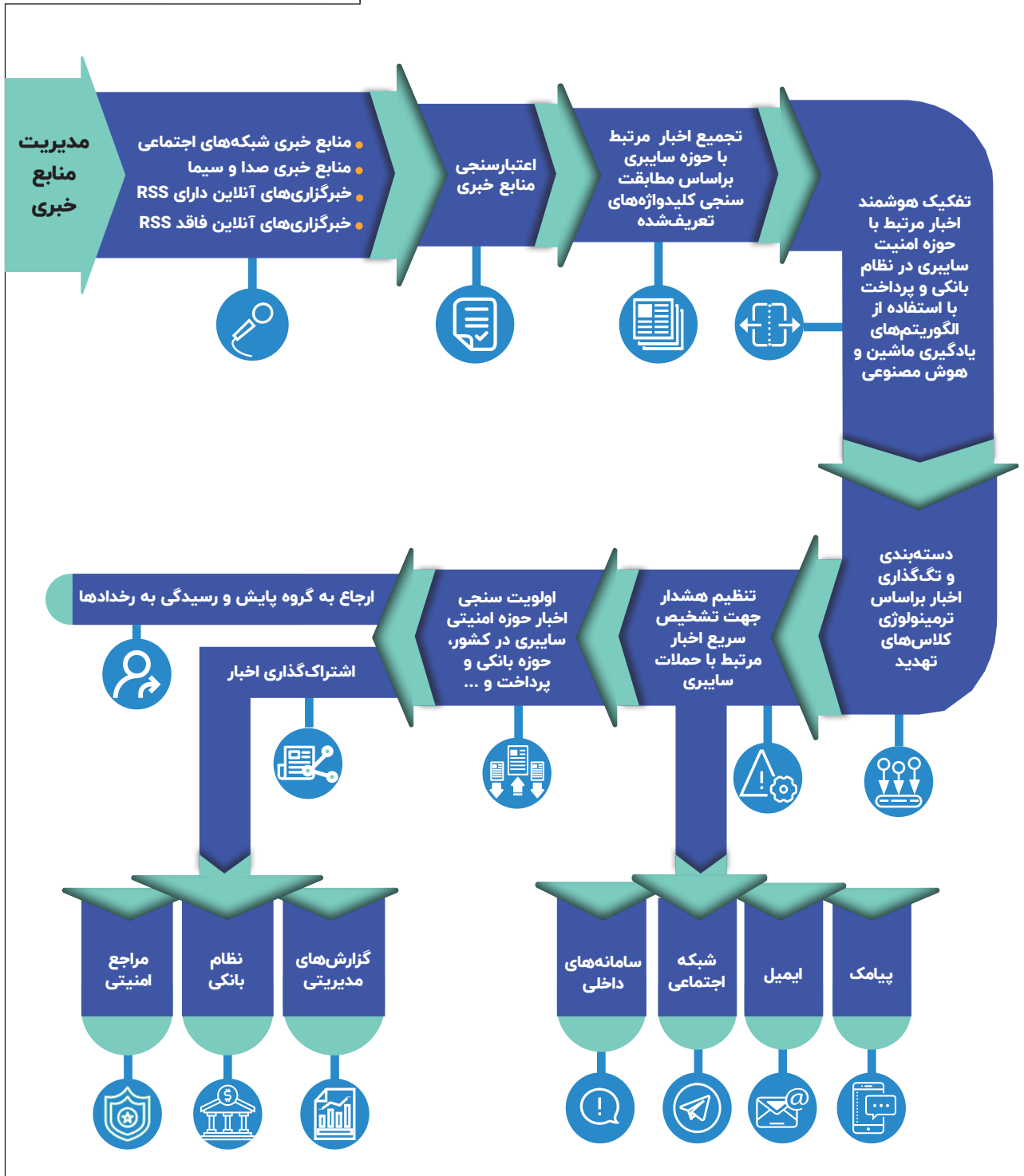
به‌عنوان مشاور در کنار بانک هستیم

یکی دیگر از وظایف جدید ماهر بانکی، ارائه خدمات مدیریت شده امنیت اطلاعات (MSSP) است. ما به‌طور کلی می‌بایست بتوانیم وظایف حاکمیتی را از وظایف ارائه خدمات مدیریت شده امنیت تفکیک کنیم. در واقع همانگونه که کاشف در راستای وظایف حاکمیتی خود به بانک می‌گوید که باید با فلان الزام امنیتی منطبق باشی، در حوزه ارائه خدمات مدیریت شده امنیت نیز می‌تواند بانک را توانمند کند که به این هدف برسد. به عنوان مثال ماهر بانکی به بانک می‌گوید که باید بتواند در زمینه مثل SOC مطابق با الزامات ارائه شده توسعه پیدا کند، اما برخی بانکها این توان و ظرفیت را ندارند و به کمک نیاز دارند. پس می‌توانیم هم به عنوان مشاور در کنار بانک قرار بگیریم و هم بعنوان ناظر از پیشبرد پروژه‌های آنها در



آشنایی با سامانه رسا

سامانه رصد سریع اخبار



مهندس سجاد طرهانی

سامانه‌هایی که از درون نیازها سر برمی آورند

اینجا واحدی است که سامانه‌های زیادی از دل آن سر برآورده‌اند تا هر کدام ابزاری باشند برای تسهیل ارائه خدمات کاشف به نظام بانکی کشور. واحد توسعه خدمات، وظایفی را از واحد طرح و برنامه سابق به ارث برد و پیش‌بینی شده که بتواند در حوزه توسعه محصولات و خدمات نقش آفرینی کند و در حال حاضر، واحدهای خود شرکت، مشتری اصلی آن محسوب می‌شوند. تمام کارهایی که در این واحد انجام می‌شود برای این است که سامانه‌های اطلاعاتی مورد نیاز واحدهای عملیاتی را برای انجام مأموریت‌ها و ارائه خدماتشان فراهم کند.

چگونه به رسا و رادار رسیدیم

«رسا» یکی از سامانه‌هایی است که برای واحد ماهر بانکی کاشف توسعه یافته است و وظیفه آن رصد و پایش سریع اخبار در فضای عمومی اخبار، خبرگزاری‌های رسمی و غیررسمی و شبکه‌های اجتماعی است و تلاش می‌کند اطلاعات مرتبط با امنیت اطلاعات نظام بانکی را گردآوری کند که بر اساس آن‌ها تصمیم‌گیری‌هایی انجام شود یا اشتراک‌گذاری اطلاعات صورت گیرد که بهره‌بردار آن در حال حاضر سازمان داخلی کاشف است ولی این قابلیت را دارد که در اختیار ذینفعان بیرونی هم قرار گیرد.

سامانه بعدی «رادار» است که کارکرد آن رؤیت‌آنی و دائم رخدادهای امنیتی است، بهره‌بردار این سامانه نیز واحد ماهر بانکی است. منشأ این سامانه درخواست نهادهای بالادستی بانک مرکزی بوده که می‌خواستند از رخدادهایی

سجاد طرهانی، مدیر واحد توسعه خدمات کاشف است. او توضیح می‌دهد که واحد توسعه خدمات، وظیفه پژوهش، نوآوری، طراحی و توسعه محصولات و خدمات شرکت و پشتیبانی از آن‌ها را برعهده دارد. پای صحبت‌های او بنشینیم و ببینیم در واحد توسعه خدمات شرکت کاشف چه می‌گذرد.



است، پلیس فتا و معاونت امور فضای مجازی عملاً برای شناسایی و مقابله با آن‌ها با روش‌های سنتی دچار مشکل بودند و این سامانه سعی داشت، ضعف‌های هماهنگی و اطلاع‌رسانی به موقع را در این حوزه به حداقل برساند. سال ۹۷ که این تفاهم‌نامه امضا شد ما یک سامانه اولیه داشتیم که بیشتر یک کارتابل نامه‌نگاری بود و مشکلات خاص خودش را داشت. مثلاً قاضی چون با ادبیات نظام بانکی آشنایی نداشت دستوری در سامانه ثبت می‌کرد که بخشی از آن مربوط به PSPها بود و بخش دیگری، مربوط به بانک بود و این ناآشنایی با سازوکارهای ایجاد و انتقال تراکنش‌های بانکی، مشکلاتی ایجاد کرده بود. همچنین صحت سنجی و گزارش‌گیری از داده‌های آن سامانه به دلیل شباهت آن با سامانه‌های تبادل نامه و دشواری در استخراج اطلاعات از آنچه بین مرجع قضایی و بانک صورت می‌گرفت، کار آسانی نبود. تقریباً یک سال و نیم که گذشت شرکت تصمیم گرفت که این رویه را بهبود دهد و با توجه به نیازهای ذی‌نفعان، کل این فرایند را از لحاظ مدیریت داده‌ها ساختاریافته‌تر کند تا در گام‌های بعدی امکان پاسخگویی به انتظارات مراجع قضائی و انتظامی فراهم شود. از مهم‌ترین اقدامات انجام شده در این خصوص، ساخت یافته کردن داده‌ها، صحت سنجی و اعتبارسنجی داده‌ها در زمان ثبت داده‌ها توسط کاربران، مسیریابی خودکار دستورهای قضائی براساس اطلاعات وارد شده و محاسبه فرصت‌های پاسخگویی مجریان دستورهای قضائی بود. شاید بتوانم به جرئت بگویم که سرآمد تنها سامانه بین نهادهای دولتی است که کسب‌وکار بانکی را به فرآیندهای مراجع قضایی و انتظامی ترجمه کرده است.

گزارش دهی بدون خطا با صراف‌بان

واحد نظارت نیز یکی دیگر از بهره‌برداران سامانه‌های اطلاعاتی است. برای مثال سامانه «صراف‌بان» که طراحی و توسعه آن در واحد ما انجام شده است. زمان کوتاهی حدود یک ماه از طرح مسئله تا اینکه سامانه‌ای در اختیارشان قرار بگیرد طول کشید و هنوز هم در حال بهبود و توسعه آن هستیم. سامانه صراف‌بان برای ساماندهی امنیت اطلاعات صرافی‌های کشور طراحی شده است که در بستر آن، رگولاتور و بازوی رگولاتور، یعنی کاشف، بتواند الزامات امنیتی تدوین شده را به آن‌ها ابلاغ کند و گزارش اقدامات را به صورت سیستمی از آن‌ها دریافت کند. سامانه دیگری که برای واحد نظارت داریم «سرابان» یا سامانه راهبری امنیت بانکی است که قبلاً برون‌سپاری شده و پشتیبانی آن در این واحد انجام می‌شود و نسخه‌های

که در نظام بانکی توسط اعضای نظام بانکی شناسایی و رسیدگی شده‌اند، اطلاع داشته باشند. همه بانک‌ها موظف هستند رخدادهایی که شناسایی می‌کنند را در این سامانه ثبت کنند. هم‌اکنون همه بانک‌ها به این سامانه متصل هستند و رخدادهایشان را در این سامانه ثبت و ضبط می‌کنند.

گامی فراتر از گزارش دهی

سامانه دیگری که در این حوزه داریم سامانه «پیکار» نام دارد که برای ثبت، گزارش دهی و رسیدگی به رخدادهای بانکی توسعه یافته است. در قیاس با رادار، که صرفاً سامانه‌ای برای گزارش دهی رخدادهای سایبری محسوب می‌شود، در سامانه پیکار به جز فرآیند گزارش دهی رخدادهای غیرسایبری، اقداماتی هم در زمینه رسیدگی به آنها انجام می‌شود. در ادبیات ما رخدادهای بانکی (غیرسایبری) از این جنس هستند که از خدمات و ابزارهای بانکی یا سوءاستفاده می‌شود و یا جعل صورت می‌گیرد و نگاه ما بیشتر نگاه کسب‌وکار بانکی است، مثلاً از یک کارت بانکی سوءاستفاده می‌شود و یا از ابزارهای بانکی در قمار و شرط‌بندی استفاده می‌شود. برای همین، سامانه‌ای ایجاد کرده‌ایم که اگر واحدهای عملیاتی شرکت کاشف و پیمانکارهای ما رخدادهایی از این جنس را مشاهده کردند، اطلاعات رخداد ثبت کرده و در مرحله بعد وارد فرایند رسیدگی شود. برای مثال، اطلاعات درگاه مورد سوءاستفاده قرار گرفته را به صورت سیستمی برای مراجع ذی‌صلاح ارسال می‌کنیم تا در مورد آن تصمیم‌گیری کنند یا اطلاعات کارت‌ها را برای تصمیم‌گیری به مراجع قضایی ارسال می‌کنیم و آن‌ها در مورد ابطال یا تعلیق یا سایر اقدامات تصمیم‌گیری می‌کنند.

کارتابل نامه‌نگاری که «سرآمد» شد

سامانه دیگری که هم‌اکنون توسط واحد ماهر بانکی مورد بهره‌برداری قرار گرفته است، سامانه «سرآمد» نام دارد که برای رسیدگی آنی و مستمر به دستورات قضایی طراحی و توسعه یافته است. این سامانه بر اساس تفاهم‌نامه‌ای ایجاد شد که بین معاونت امور فضای مجازی دادستانی کل کشور، بانک مرکزی و کاشف منعقد شد. پیرو تفاهم‌نامه منعقد شده، به کاشف سپرده شد تا یک بستر الکترونیکی برای تبادل دستورات قضایی میان مراجع قضایی و انتظامی و نظام بانکی و پرداخت ایجاد کند. با توجه به اینکه سرعت وقوع جرائم سایبری و همچنین گم کردن رد پول توسط ابزارهای الکترونیکی، متفاوت از روش‌های سنتی

خوبی تشریح کرده و راه حل‌ها را به صورت شفاف بیان می‌کنند به گونه‌ای که فرد تصمیم‌گیر و مجری به راحتی از آن استفاده می‌کند. هدف ما در پژوهش و نوآوری رسیدن به این نقطه است.

ارتباط مستمر و باکیفیت

سامانه تیکت‌گذاری هم یکی از سامانه‌هایی است که در حال طراحی و توسعه است و در نهایت میز خدمت کاشف خواهد شد. این سامانه در آینده تا جای ممکن، مشتریان تمام سرویس‌ها را از یک درگاه یا پلتفرم با ما مرتبط می‌کند. ولی چون کسب‌وکارها مختلف‌اند و خدمات هم متفاوت هستند، انجام آن به زمان قابل توجهی نیاز دارد و در حال حاضر، آن را برای یکی دو موضوع پیش می‌بریم. تمام سامانه‌ها زیر چتر پشتیبانی ما قرار دارند و تیم پشتیبانی ما برخط هستند. بهینه‌سازی فرایندها و تبادل اطلاعات و تعاملات یکی از کارهای مهم ما در زمینه پشتیبانی است.

آکادمی امنیت؛ گامی برای آموزش

در چند سالی که شرکت تأسیس شده است و با توجه به اولویت‌ها، آموزش یکی از حوزه‌هایی بوده که کمتر به آن پرداخته شده، ولی در یک سال اخیر سعی کردیم به موضوع آموزش توجه ویژه‌تری داشته باشیم و نتیجه این شد که برای تأسیس آکادمی امنیت برنامه‌ریزی کنیم. مهارت‌هایی که نیروی انسانی در دانشگاه کسب می‌کند متناسب با بازار کار نیست و آموزش‌ها نیز کفایت لازم را ندارند. در آکادمی امنیت سعی داریم بتوانیم سه محور اصلی را پوشش دهیم. نخست، ارائه دوره‌های آموزشی تخصصی برای آن دسته از متقاضیانی که می‌خواهند در مدتی کوتاه و معین، مهارتشان را در یک یا چند حوزه تخصصی ارتقا بدهند. دوم، برنامه‌های تنظیم کنیم برای کسانی که می‌خواهند بلندمدت‌تر به مسیر شغلی خود پردازند، آموزش‌هایی ببینند و در نهایت تبحر و سطوحشان را مشخص می‌کنیم و محور سوم، بحث آگاهی‌رسانی است برای عموم جامعه و مخاطبان خدمات شبکه بانکی.

ساتا؛ مجموعه هر آنچه می‌خواهیم

در توسعه خدمات یک سامانه مهم به اسم «ساتا» هم داریم که در دست پیاده‌سازی است. سامانه اشتراک‌گذاری و تحلیل اطلاعات امنیتی. در چند سال آتی قرار است از تمام اطلاعاتی که در سامانه‌هایمان در حوزه نظام بانکی گردآوری می‌کنیم، ارزش افزوده‌ای ایجاد کنیم به این صورت که تقاطع‌هایشان کشف شود و اگر نیاز است یک سری غنی‌سازی‌هایی روی آن‌ها انجام شده و در نهایت اطلاعات خوبی برای اشتراک گذاشتن تهیه شود؛ از اطلاعات فنی گرفته تا راهبردهای امنیت اطلاعات. یکی از اهداف مهم این سامانه ارائه آگاهی وضعیتی امنیت نظام بانکی است.

آتی آن را به صورت درون‌سپاری پیش خواهیم برد. در واقع سرابان، مدل پیشرفته‌تر صراف‌بان است که برای بانک‌ها و موسسات اعتباری غیربانکی طراحی و توسعه یافته است. در این سامانه بانک‌ها و موسسات اعتباری غیربانکی اطلاعات مربوط به فرایند مدیریت ریسک در سامانه‌های اطلاعاتی پراهمیت خود را بر اساس چرخه‌ای که کاشف تعریف کرده در سرابان ثبت و ضبط می‌کنند. در بطن سامانه سرابان، چارچوب کنترل‌های امنیتی کاشف نیز به کار رفته است. این چارچوب در واقع فهرستی جامع از کنترل‌های امنیت فناوری اطلاعات که برای نظام بانکی تدوین شده است.

از نمونه‌های موفق دنیا الگو می‌گیریم

ما از نمونه‌های جهانی در مورد همه سامانه‌هایمان الگوبرداری کرده ایم و در مواردی هم با توجه به نیازهای داخلی که داشته ایم، اختصاصی‌سازی کردیم. برای مثال در قسمتی از چرخه مدیریت ریسکی که در سامانه سرابان پیاده‌سازی شده است، مدل استفاده شده برگرفته از مدل پیاده‌سازی شده است، RMF (Risk Management Framework) است، در حوزه طبقه‌بندی امنیت اطلاعاتی که بخشی از RMF محسوب می‌شود، یک سند کاملاً به طبقه‌بندی امنیتی اطلاعاتی می‌پردازد. ولی ما در آنجا نوآوری هم داشتیم و آن را با IFW ادغام کردیم و روشگان خاص نظام بانکی را ایجاد کردیم.

مواردی هم بوده که اصلاً الگوی جهانی مشابهی نداریم مثل سامانه سرآمد که کاربرد و مسئله خاص ماست و تمام فرآیند طراحی، توسعه و بهره‌برداری از آن توسط همکاران ما در کاشف شکل گرفته است.

چگونه نوآوری کنیم

کاشف، جایی است که باید دانش کاربردی در حوزه امنیت اطلاعات تولید کند و در اختیار نظام بانکی قرار دهد. دانش کاربردی می‌تواند در سطوح مختلف سازمان به کار آید، از لایه‌های مدیریتی سطح بالا برای تبیین راهبردها و اهداف کلان امنیتی گرفته تا لایه‌های فنی شامل پیکربندی تجهیزات، دستورالعمل‌های امنیتی و غیره. در این حوزه ما به شرکت‌های امنیتی بزرگ دنیا نگاه می‌کنیم و می‌بینیم که مسائلی را به





بزرگ‌ترین چالش امنیت کمبود نیروی انسانی است

احسان گیلانی، مدیر واحد مدیریت فناوری اطلاعات کاشف است. او درباره عملکرد اصلی این واحد که پشتیبانی فناوری شرکت کاشف است، توضیح می‌دهد و به تشریح پروژه‌هایی می‌پردازد که در این واحد انجام شده و یاد در دست اقدام هستند.

نیازهای فناورانه آن‌هاست که ما باید تأمین کنیم. همچنین سیستم‌ها و کامپیوترهای کارکنان کاشف نیاز به نگهداری و به‌روزرسانی دارد و همه این امور در زمره فعالیت‌های این واحد است.

با توجه به پتانسیل‌های موجود و جنس پروژه‌ها، خدمات خارج از سازمان هم ارائه می‌دهیم که البته در حال حاضر، این خدمات فقط شامل بانک مرکزی می‌شود و به زیرساخت آن مرتبط است.

واحد مدیریت فناوری اطلاعات شرکت کاشف در حال حاضر دو زیرگروه دارد. زیرگروه توسعه و نگهداری زیرساخت که آنچه تا کنون گفتیم بخشی از وظایف این زیرگروه است. دیگری زیرگروه امنیت است که تمام امور اجرایی امن‌سازی بسترهای الکترونیکی کاشف را برعهده دارد. این وظیفه خطیر و مهمی است و باید همواره، چه

هر سازمانی نیازهای روزمره فناورانه دارد. از رایانه‌ای که روی میز کارکنان است تا سرورهایی که اطلاعات در آنها نگهداری می‌شوند و هرآنچه که باید بر بستر وب صورت گیرد؛ از نصب یک برنامه کاربردی معمولی تا به‌روزرسانی‌های امنیتی خیلی حساس و مهم. کارهایی که می‌توانند فهرست بلندبالایی باشند از وظایفی که شاید کوچک به نظر برسند، اما امنیت یک سازمان در قلب آنها ریشه دوانده است.

کاشف هم از این موضوع مستثنی نیست. مشتریان اصلی ما، واحدهای مختلف کاشف هستند و ما معمولاً سرویس‌دهنده به واحدهای دیگر هستیم. در شرکت کاشف، واحدهای صف را داریم که به بانک‌ها و بانک مرکزی خدماتی ارائه می‌دهند و باید امکانات لازم برای این خدمات‌دهی در اختیارشان قرار بگیرد. بخشی از این نیازها،

اطلاع‌رسانی مربوط به آسیب‌پذیری‌های سیستم‌های بانک مرکزی را در برمی‌گیرد.

TVM تمام شبکه را به صورت خودکار اسکن کرده و نقاط ضعف موجود را شناسایی می‌کند و درباره عدم اعمال به‌روزرسانی‌ها و وصله‌های امنیتی هشدار می‌دهد و درجه اهمیت و میزان خطرناک بودن آن آسیب‌پذیری (CVSS) را هم گزارش می‌کند تا متولی آن سیستم یا شبکه بتواند بر اساس درجه اهمیت و به‌ترتیب اولویت، درباره به‌روزرسانی سیستم‌عامل و یا هر دارایی آسیب‌پذیر دیگر اقدام کند. فرایند اجرا به این شکل بوده پس از انتخاب محصول و برگزاری مناقصه و خرید لایسنس‌های مربوطه، خودمان نصب و راه‌اندازی آن را برای بانک مرکزی انجام دادیم و در حال حاضر هم ارائه مشاوره فنی به بانک مرکزی برعهده ماست.

امن‌سازی بستر مجازی‌سازی

یکی از پروژه‌های بزرگی که در دست داریم امن‌سازی بستر مجازی‌سازی است که به اختصار NSX خوانده می‌شود و از این تکنولوژی استفاده می‌کند. قبلاً به این شکل بوده که این پروژه‌ها توسط پیمانکاری که کاشف مشخص می‌کرد انجام می‌شد و ما مدیریت آن پیمانکار را تا زمانی که پروژه به سرانجام برسد، برعهده داشتیم؛ اما پروژه NSX با آموزش‌هایی که به تیم فناوری اطلاعات کاشف داده شده‌است، توسط آنها پیش می‌رود؛ زیرا از طرفی، این پروژه از لحاظ اطلاعات فنی و دانش تکنولوژی در سطح خیلی بالایی قرار داشت و با توجه به روند مهاجرت، تعداد

در برابر حملات شبکه‌ای تکنیکی و فنی و چه حملات مهندسی اجتماعی، هوشیاری لازم را داشته باشد. وظیفه اجرایی‌سازی و رعایت سیاست‌های کلان و الزامات تعیین‌شده از سوی مرکز ملی انفورماتیک، مرکز مدیریت راهبردی افتا و نهادهای ذی‌ربط نیز برعهده همین زیرگروه است.

پروژه محافظت از نقاط انتهایی

پروژه محافظت از نقاط انتهایی (EPP: Endpoint Protection) پروژه‌ای بود که اوایل پاییز و در موعد مقرر به پایان رسید. هدف از آن حفاظت در برابر مشکلات و آسیب‌پذیری‌ها و تهدیداتی است که معمولاً از سمت کلاینت‌ها و دستگاه‌ها و ایستگاه‌های کاری به وجود می‌آید و در واقع ترکیبی از روش‌های پیشگیرانه برای شناسایی عملیات مشکوک است که آنها را تحلیل و گزارش می‌کند. اکنون آن را روی پانصد نقطه نهایی بانک مرکزی اجرا کردیم و در سال‌های بعد به همه سیستم‌های بانک مرکزی گسترش پیدا می‌کند.

پروژه TVM

یکی دیگر از پروژه‌هایی که تقریباً سه‌ماه پیش توسط زیرگروه امنیت این واحد به اتمام رسید پروژه TVM بانک مرکزی بود که اسکن آسیب‌پذیری‌ها و



اطلاعات است. پروژه امن‌سازی ایمیل، پروژه دیگری است که در آینده اجرا خواهد شد. ایمیل یکی از منابعی است که بیشتر اطلاعات سازمان‌ها از طریق آن نشت پیدا می‌کند و بنابراین، امن‌سازی ایمیل‌ها هم در دستور کار قرار دارد و مراحل تحقیقاتی این پروژه در حال انجام است. به دلیل عملکرد خوب و روند پیشرفتی که پروژه‌ها داشته‌اند پروژه‌هایی از جمله امن‌سازی فایروال‌ها و دیتابیس‌ها برای بانک مرکزی و ارتقای اکتیو دایرکتوری بانک مرکزی نیز برعهده واحد فناوری اطلاعات کاشف گذاشته شده‌اند. ناظر یکی از پروژه‌های ما، واحد امنیت بانک مرکزی و در بقیه موارد، واحد زیرساخت فناوری اطلاعات بانک مرکزی است. بهینه‌سازی WAF‌های بانک مرکزی هم توسط گروه امنیت به تازگی آغاز شده است.

چالش‌های پیش رو

عمده‌ترین چالشی که در پیاده‌سازی پروژه‌هایمان داریم مربوط به نیروی انسانی متخصص است. با توجه به روند مهاجرت، تعداد نیروی انسانی متخصص در حوزه فناوری خیلی کم شده و هزینه جذب همین تعداد اندک هم خیلی بالاست.

چالش بعدی این است که در برخی موارد به دلیل تحریم نمی‌توانیم بعضی دستگاه‌ها یا نرم‌افزارها را به‌طور مستقیم تهیه کنیم. غالباً هم نرم‌افزارهای بومی در حوزه مدنظر یا وجود ندارند یا کیفیت و ویژگی نرم‌افزارهای مشابه خارجی را ندارند و یا به‌روز نیستند. در حالی که در بحث امنیت، سرعت پاسخ‌دهی خیلی مهم است و مزیت ایجاد می‌کند یکی از بزرگ‌ترین اقداماتی که برای کاشف انجام دادیم حفظ استقلال کاشف با توجه به منافع شرکت و به دور از نگاه متعصبانه بود که بسته به منافع شرکت راجع به اینکه برای کدام کارهایمان در داخل شرکت هزینه کنیم، تصمیم‌گیری شود.

بحث گسترش دیتاستر کاشف و نیز توسعه ITSM هم از کارهایی هستند که در کاشف و برای توسعه آن، روی آنها تمرکز داریم. ما همچنین به دنبال توسعه NOC و SOC کاشف در قالب واحدهای مستقل هستیم.

شرکت کاشف در مسیر رشد و در حال پوست‌اندازی است و شیب رشد آن در سال‌های اخیر و به‌ویژه یک‌سال اخیر بیشتر شده و همه همکاران برای ارتقای آن، سختکوشانه و شبانه‌روزی زحمت می‌کشند. قدر متخصصان زحمتکش را می‌دانیم و سعی داریم آنها را در مسیر خودشان هدایت کنیم و با کمک به رشد آنها به عنوان یک شرکت موفق در زمینه تربیت نیروی متخصص این حوزه شناخته بشویم.

افراد مسلط روی این محصول و تکنولوژی در کل کشورمان انگشت‌شمار بود و از سوی دیگر بانک مرکزی، اطلاعات بسیار حساسی دارد و انتخاب و وابستگی به یک پیمانکار، خطرات و ریسک‌های امنیتی زیادی به همراه داشت. با این وصف، اکنون ضمن انجام یک پروژه بسیار مهم و بزرگ در سطح بانک مرکزی در حال تربیت نیروی انسانی و ارتقای سطح دانش گروه‌مان نیز هستیم. برای این کار با زبده‌ترین متخصصان مشاور کشور در زمینه آموزش و انتقال تکنولوژی و طراحی آغاز همکاری کردیم تا بدون اینکه اطلاعات حیاتی منتقل شود، دانش لازم منتقل شود. در ساختار مجازی‌سازی معمولاً همه ماشین‌های مجازی می‌توانند با همدیگر ارتباط داشته باشند ولی چون این ارتباط، مجازی است معمولاً از دایره آن سرورها خارج نمی‌شود، مگر اینکه این ترافیک‌ها توسط ارتباطات VLAN‌های خاصی تفکیک شود که تا سوییچ یا روتر بالادستش بیاید و برگردد. معمولاً این ترافیک‌ها تا مدتی ناشناخته می‌ماند؛ یعنی ماشین‌های مجازی با شبکه‌ای در بیرون، ترافیک ردوبدل می‌کند ولی دیده نمی‌شود و هیچ شفافیتی روی این قضیه وجود ندارد بنابراین کنترل وجود مخاطره امنیتی، تقریباً غیرممکن خواهد شد. معمولاً تعداد ماشین‌های مجازی در ساختار مجازی‌سازی خیلی زیاد و بیشتر از تعداد سرورهای عادی است. کاری که NSX انجام می‌دهد مانند این است که روی هر ماشین‌های مجازی یک فایروال گذاشته شده باشد. همچنین قابلیت انجام یک سری از کارهای فایروال‌های نسل جدیدتر را هم دارد.

برنامه‌های آینده

امن‌سازی پایگاه‌های داده، یکی از پروژه‌های آینده ما است. پایگاه داده یکی از نقاط بسیار حساس هر سازمانی محسوب می‌شود و معمولاً هر کاری که هکرها و نفوذگران می‌کنند در نهایت برای دسترسی به داده‌هاست. این اطلاعات در سطح سامانه‌ها معمولاً در پایگاه داده قرار دارد و بنابراین در این پروژه، DAM (Database Activity Monitoring) یا به بیان دیگر DAP (Database Audit and protection) سر راه دیتابیس‌ها و سایر سیستم‌هایی که می‌خواهند از دیتابیس استفاده کنند قرار می‌گیرد و تمام جست‌وجوها و دسترسی‌هایی را که به فایروال اتفاق می‌افتد پایش، کنترل و محدود می‌کند و هشدارهای لازم را در مورد اتفاقات می‌دهد. اکنون در فاز تحقیقات این پروژه قرار داریم. پروژه‌های امنیتی مثل ISMS هم جزء کار واحد فناوری

اهداف کلان کاشف



دکتر حسین قرایی گرکانی

شناخت مدل‌های مرجع CERT / CSIRT

قسمت اول

امنیت اطلاعات به معنای حفظ محرمانگی، صحت/جامعیت و دسترس پذیری اطلاعات یکی از مسائل بسیار حساس و حیاتی در زمان استفاده از اینترنت در انجام امور روزانه است. باید توجه داشت که سطح بالای امنیت، علاوه بر سه ویژگی مهم امنیت (CIA)، به ایجاد اطمینان و حسابرسی^۱ نیز می‌پردازد.

برای تأمین امنیت در تمامی حوزه‌ها، جلوگیری از منع سرویس، کشف کلاهبرداری‌های مالی و سایر موارد مشابه، تیم‌های مختلفی در کنار یکدیگر فعالیت می‌کنند. این تیم‌ها در حالت کلی به‌عنوان تیم امنیت فناوری اطلاعات سازمان شناخته می‌شوند. در کنار این گروه، تیم پاسخ به حوادث اضطراری رایانه‌ای و تیم پاسخ به حوادث امنیت کامپیوتر دو رکن اصلی امنیت در سازمان هستند. CERT و CSIRT به‌عنوان دو بخش اصلی با هدف تأمین امنیت بسیار مشابه هم هستند. هر دو می‌توانند در قالب تیم‌های رسمی یا پراکنده عمل کنند، وظایف نسبتاً مشابهی دارند و بر اساس ساختار سازمان و میزان اهمیت امنیت در آن، ممکن است هر دو تیم و یا تنها یکی از تیم‌ها در آن وجود داشته باشد.

در این مقاله به بررسی مدل‌های مرجع برای شناخت سرویس‌ها، فرآیندها و وظایف CSIRT (CERT/CC) و هماهنگ‌کننده CSIRT پرداخته می‌شود.

مقدمه

امنیت اطلاعات به معنای حفظ محرمانگی، صحت/جامعیت و دسترس پذیری اطلاعات یکی از مسائل بسیار حساس و حیاتی در زمان استفاده از اینترنت در انجام امور روزانه است. باید توجه داشت که سطح بالای امنیت، علاوه بر سه ویژگی مهم امنیت (CIA)، به ایجاد اطمینان^۱ و حسابرسی^۲ نیز می‌پردازد.

برای تأمین امنیت در تمامی حوزه‌ها، جلوگیری از منع سرویس، کشف کلاهبرداری‌های مالی و سایر موارد مشابه، تیم‌های مختلفی در کنار یکدیگر فعالیت می‌کنند. این تیم‌ها در حالت کلی به‌عنوان تیم امنیت فناوری اطلاعات سازمان شناخته می‌شوند. در کنار این گروه، تیم پاسخ به حوادث اضطراری رایانه‌ای و تیم پاسخ به حوادث امنیت کامپیوتر دو رکن اصلی امنیت در سازمان هستند. شکل ۱ جایگاه CSIRT را در سازمان و در مقایسه با تیم امنیت فناوری اطلاعات نشان می‌دهد.



شکل ۱- جایگاه CSIRT در سازمان

CERT و CSIRT به‌عنوان دو بخش اصلی با هدف تأمین امنیت بسیار مشابه هم هستند. هر دو می‌توانند در قالب تیم‌های رسمی یا پراکنده عمل کنند، وظایف نسبتاً مشابهی دارند و بر اساس ساختار سازمان و میزان اهمیت امنیت در آن، ممکن است هر دو تیم و یا تنها یکی از تیم‌ها در آن وجود داشته باشد. اما در بررسی تفاوت‌های این دو تیم، بزرگ‌ترین اختلاف آن‌ها در وظایف و مسئولیت‌ها است. CERT معمولاً با انجمن‌هایی در

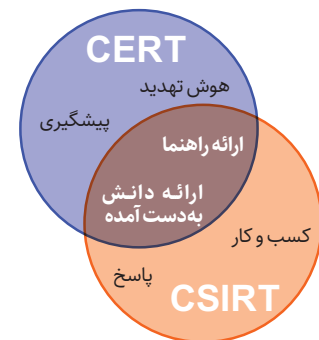
1 Assurance

2Accountability

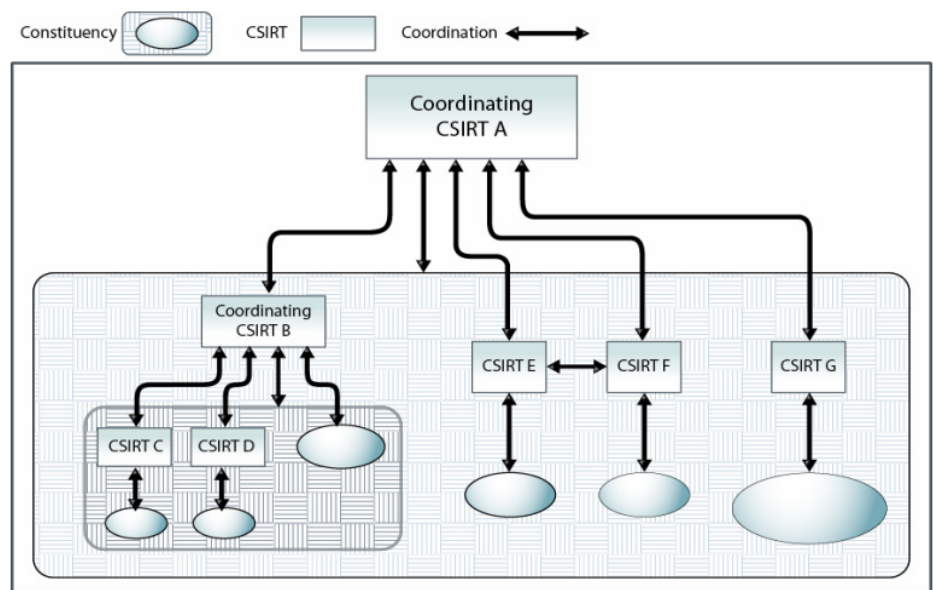
حوادث رخ داده دور هم جمع می‌شوند. حال پس از انجام بررسی‌های مورد نیاز، در صورت کشف مقصر بروز رخداد امنیتی این تیم می‌تواند در خصوص آنها پیگیری قانونی انجام دهد و حتی در بدترین حالت فعالیت خاکی را تعلیق/حذف کند.

برای روشن‌تر شدن اشتراکات و تفاوت‌های عملکرد این دو تیم، مجموعه وظایف آن‌ها در شکل ۲ آمده است. مفهوم CERT در سال ۱۹۸۸ ایجاد شد. در پاسخ به حمله کرم کامپیوتری Morris که هزاران سرور را بر روی اینترنت تحت تأثیر قرار داد، دارپا مجموعه‌ای را با همکاری دانشگاه کارنگی ملون به نام CERT/CC به معنای مرکز هماهنگی تیم پاسخ به حوادث کامپیوتری^۳ ایجاد کرد. هدف CERT/CC کمک به حفاظت از اینترنت و تأمین امنیت در بستر اینترنت از طریق جمع‌آوری و توزیع اطلاعات مربوط به آسیب‌پذیری‌های امنیتی حیاتی است. مشابه این مرکز در برخی کشورهای دیگر نیز به وجود آمد. حال مفهوم CERT به تمامی تیم‌های پاسخ به اضطراری که با تهدیدات سایبری مواجه هستند اشاره می‌کند. امروز از CSIRT به جای CERT/CC استفاده می‌شود. البته باید توجه داشت که وظیفه اصلی CERT به اشتراک‌گذاری اطلاعات برای کمک به سایر تیم‌های پاسخ به اضطرار برای مواجهه با مسائل امنیتی در محدوده خودشان است. به عبارت دیگر می‌توان گفت، CSIRT‌ها می‌توانند متشکل از چندین CERT باشند. سطح بالاتری از CSIRT‌ها نیز تعریف می‌شود که به نام هماهنگ‌کننده‌های CSIRT مطرح شده و در لایه مدیریتی بالاتر ایفای نقش می‌کند. ارتباط CSIRT‌ها با سایر نظیرهای این حوزه (البته به صورت عمومی که بر اساس بیان دانشگاه کارنگی ملون می‌تواند بر روی تمامی سکتورها مانند سکتور مالی اعمال شود) در شکل ۳- آمده است.

حوزه اینترنت فعالیت می‌کنند تا بتوانند وظایف خود را در حوزه حوادث امنیتی مربوط به میزبان‌ها به صورت ساده‌تر انجام دهند، گام‌های پیشگیرانه برای افزایش آگاهی انجمن در خصوص مسائل امنیت کامپیوتری بردارند و پژوهش‌هایی که با هدف بهبود امنیت سیستم‌های موجود انجام شده است را ارزیابی کنند. CERT معمولاً به صورت ۲۴ ساعته برای پاسخ‌گویی به آسیب‌پذیری‌های امنیتی همکاری فنی را فراهم می‌آورد. این در حالی است که سرویس‌های CSIRT مسئول دریافت، بازبینی و پاسخ به گزارش‌های حوادث امنیتی است. با توجه به نقش‌هایی که برای CSIRT تعریف می‌شود، می‌توان گفت این تیم شباهت بسیار بیشتری به هدف پروژه جاری دارد. سطح سرویس‌دهی این تیم بسیار گسترده است، به عبارت دیگر سرویس‌های این تیم می‌تواند در محدوده قلمرو یک سازمان با شعب زیاد و یا حتی کاربری باشد که از طریق اینترنت پرداخت انجام می‌دهد. همان‌طور که بیان شد این تیم می‌تواند به صورت رسمی و یا پراکنده باشد، اگر تیم رسمی برای سازمان وجود داشته باشد، تمامی فرآیندهای پاسخ به رویدادهای امنیتی توسط این تیم به‌عنوان عملکرد هسته‌ای انجام می‌شود. از طرفی تیم پراکنده، به اقتضای



شکل ۲- نقش‌های اصلی CERT و CSIRT



شکل ۳- ارتباط نظیرهای CSIRT‌ها

عملیاتی است، CERT/CC قرار می‌گیرد که وظیفه آن انتشار، تحلیل، بررسی و نتیجه‌گیری از اطلاعاتی است که از لایه پایین‌تر دریافت کرده و آن‌ها را سایر CERTها انتشار می‌دهد. CSIRT/CC در گام بعدی مسئول اتصال CERT/CCها به همدیگر و تصمیم‌گیری، تحلیل و انتشار در سطح بالاتر است. در ادامه شرح وظایف این سه دسته از دیدگاه مؤسسات مرجع به شکل مقابل مورد بررسی قرار می‌گیرد:

معرفی CERT از دیدگاه ENISA

در سراسر محیط عملیاتی سازمان، وقفه‌ها به صورت منظم رخ می‌دهند. این وقفه‌ها ممکن است به سبب اقدامات عمدی علیه سازمان رخ دهند مانند حمله انکار سرویس یا انتشار یک ویروس کامپیوتری و همچنین به دلیل اقداماتی که سازمان کنترلی بر روی آن‌ها ندارد، مانند سیل یا زلزله. حوادث ناگوار بدون توجه به سازمان یا موارد دیگر به طور قابل توجهی می‌تواند بر ظرفیت‌های عملیاتی مرتبط با توانایی سازمان تأثیر گذارد. برای مدیریت

در این گزارش به بررسی مدل‌های مرجع برای شناخت سرویس‌ها، فرآیندها و وظایف (CERT/CC) CSIRT و هماهنگ‌کننده CSIRT پرداخته می‌شود.

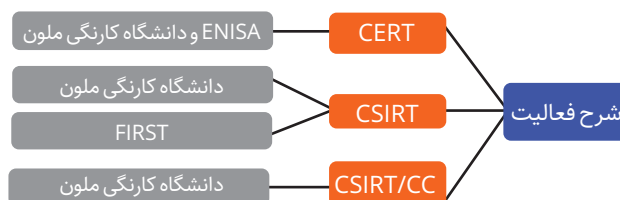
بررسی مدل‌های مرجع برای (CERT/CC) CSIRT

همان‌طور که پیش‌تر نیز بیان شد برای بررسی نقش‌ها و وظایف تیم‌های پاسخ‌گویی به حوادث، می‌توان آن‌ها را در سه دسته کلی قرار داد که شامل CSIRT، CERT، (CERT/CC) و CSIRT/CC است. هرکدام از این تیم‌ها دارای مأموریت‌هایی هستند که در جدول ۱ آمده است. بر اساس اهداف و مأموریت‌های تعریف‌شده در شکل (۲) برای CSIRTها، سه نوع کلی CSIRT معرفی شده است که در سه سطح هماهنگی، سازمانی و فنی تعریف می‌شود که به نظر می‌رسد سطح فنی به CERTها، سازمانی به CERT/CC و هماهنگی به CSIRT-CC اشاره دارد. با اطلاع از اهداف و چشم‌اندازهای این مؤسسات،

اهداف (مأموریت‌ها)	تیم (مؤسسه)
• بهبود امنیت تمامی محصولات فناوری اطلاعات که در محدوده فعالیت تیم می‌گنجد	CERT (۲)
• ارائه یک دیدگاه جامع روش‌های حمله، آسیب‌پذیری‌ها و تأثیر حملات بر روی شبکه و سیستم‌های اطلاعاتی و همچنین ارائه رویه‌ها و جزییات اطلاعات حوادث و آسیب‌پذیری‌ها • ایجاد یک زیرساخت تخصصی امنیتی مناسب که به حملات به سیستم‌های متصل به اینترنت پاسخ دهد و بتواند از سیستم‌های خود در برابر خطرات امنیتی محافظت کند • ارائه روش‌هایی ارزیابی، بهبود و حفظ امنیت و قابلیت اطمینان سیستم‌های شبکه • همکاری با فروشندگان به جهت بهبود امنیت محصولات • پاسخ سریع به موارد امنیتی موجود در اینترنت • ارائه خدمات به‌عنوان یک نقطه کانونی جهت گزارش آسیب‌پذیری‌ها و حوادث امنیتی • افزایش آگاهی از مسائل امنیتی • ایجاد مدل‌هایی به‌منظور کمک به دیگر تیم‌های واکنش به حوادث	CSIRT یا CERT/CC (۵) (۶) (۷) (۸) (۹)
• دریافت دانش کامل در مورد تهدیدات امنیتی در جهان • ارتباط با سایر CSIRTها و انتشار اطلاعات • ایجاد یک web of trust بین تمامی CSIRTها	CSIRT/CC (۲)

جدول ۱- اهداف مؤسسات CERT، CSIRT و CSIRT-CC

انعطاف‌پذیری عملیاتی سازمان باید در هر زمانی که ضروری است از وقفه‌های احتمالی جلوگیری کند و همچنین از پیوستگی عملیات هنگام وقوع خرابی اطمینان حاصل یابد. باین وجود، به این دلیل که تمام وقفه‌ها قابل جلوگیری نیستند، سازمان باید توانایی شناسایی رخدادهایی که می‌تواند بر عملیات سازمان تأثیر بگذارد را داشته باشد و به‌طور مناسب به آن‌ها پاسخ دهد. یک سازمان باید دارای سرویس‌ها و فرآیندهایی به‌منظور شناسایی اختلالات بالقوه، تجزیه و تحلیل آن‌ها و تعیین زمان به‌موقع پاسخگویی به آن‌ها باشد. محدوده فرآیند مدیریت و کنترل حوادث، توجه سازمان را بر روی چرخه حیات حادثه، از تشخیص رخداد تا



شکل ۳- ساختار ادامه مستند در خصوص شرح وظایف مؤسسات

مشخص می‌شود CERT یک واحد درون سازمان برای پاسخگویی به حوادث امنیتی است که در سطح کاملاً فنی به رسیدگی به آسیب‌پذیری‌ها، حملات و حوادث پرداخته و به سطوح بالاتر گزارش می‌دهد. در سطح بالاتر که سطح

دسته‌بندی سرویس‌های CERT

با توجه به جدول یک دسته‌بندی مرسوم برای سرویس‌های کسب‌وکار CERT نشان داده شده است که این دسته‌بندی توسط CERT/CC در دانشگاه کارنگی ملون ارائه شده است که در ادامه هر کدام شرح داده می‌شود.

۱- سرویس‌های واکنش‌گرایانه

این سرویس‌ها در صورت وقوع یک حادثه مانند گزارش آلوده شدن یک سیستم، پخش شدن کدهای آلوده، آسیب‌پذیری نرم‌افزار و یا هر خطر اعلامی توسط سیستم‌های تشخیص نفوذ یا رخداد نگاری، فعال می‌شوند. این دسته از سرویس‌ها مجموعه خدمات هسته‌ای و اساسی CSIRT محسوب می‌شوند.

اعلام هشدار و اخطار

این سرویس برای انتشار اطلاعات به اجزاء اصلی در پاسخ به مشکلات امنیت شبکه مانند نفوذ، آسیب‌پذیری یا اخطار امنیتی، وجود ویروس در کنار فراهم‌سازی راه‌کارهای

تجزیه و تحلیل و پاسخ به آن، متمرکز می‌کند. یک سازمان طرح مدیریت حادثه را ایجاد می‌کند و منابع مناسب را به آن اختصاص می‌دهد. همچنین یک سازمان مجموعه معیارهایی را برای تعیین زمانی که حوادث اتفاق می‌افتد مورد توجه قرار می‌دهد و قابلیت شناسایی رخدادها و گزارش دهی آن‌ها را ایجاد می‌کند. فعالیت‌های پشتیبانی مانند ارتباطات، ثبت و ردگیری رخدادها و حفظ شواهد رخداد و حادثه تعریف و ایجاد می‌شود. مهم‌تر از همه، سازمان، بازنگری پس‌ا حادثه را انجام می‌دهد تا مشخص شود که چه چیزی می‌تواند از مدیریت حوادث آموخته شود.

مدیریت حوادث با شناسایی رخداد، تریاژ و تجزیه و تحلیل آغاز می‌شود. یک رخداد می‌تواند بر دارایی‌های سازمانی تأثیر گذارد و ممکن است منجر به اختلال در یک عملیات شود. یک رخداد ممکن است نیازی به پاسخ رسمی از سازمان نداشته باشد و به صورت مشکل جداگانه‌ای باشد که نهایتاً قابل حل است.

سرویس‌های CERT		
سرویس‌های مدیریت کیفیت امنیت	سرویس‌های پیش‌گیرانه	سرویس‌های واکنش‌گرایانه
<ul style="list-style-type: none"> تجزیه و تحلیل ریسک^{۱۵} طرح بازیابی حوادث و تداوم کسب‌وکار^{۱۶} مشاور امنیت^{۱۷} ایجاد آگاهی^{۱۸} آموزش و یادگیری^{۱۹} ارزیابی و تأیید محصول^{۲۰} 	<ul style="list-style-type: none"> اعلان عمومی^۸ پایش فناوری^۹ ارزیابی یا حسابرسی امنیتی^{۱۰} بیکربندی و نگهداری از ابزارها، تجهیزات، زیرساخت‌ها و سرویس‌های امنیتی^{۱۱} توسعه ابزارهای امنیتی^{۱۲} سرویس‌های تشخیص نفوذ^{۱۳} انتشار اطلاعات امنیتی^{۱۴} 	<ul style="list-style-type: none"> اعلام هشدار و اخطار^۴ رسیدگی به حادثه^۵ تحلیل حادثه پاسخ‌گویی به حادثه در سایت پشتیبانی پاسخ‌گویی به حادثه هماهنگی پاسخ‌گویی به حادثه رسیدگی به آسیب‌پذیری^۶ تحلیل آسیب‌پذیری پاسخ‌گویی به آسیب‌پذیری هماهنگی پاسخ‌گویی به آسیب‌پذیری رسیدگی به آرتیفکت^۷ تحلیل آرتیفکت پاسخ‌گویی به آرتیفکت هماهنگی پاسخ‌گویی به آرتیفکت

جدول ۲- انواع سرویس‌های CERT

- Alerts and Warnings
- Incident Handling
- Vulnerability Handling
- Artifact Handling
- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and Maintenance of Security Tools, Applications and Infrastructure
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination
- Risk Analysis
- Business Continuity and Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education Training
- Product Evaluation or Certification



حادثه بر روی زیرسرویس‌های موجود در سازمان تعریف می‌شود. در حالت کلی، منظور از تحلیل حادثه، بررسی تمامی آرتیفکت‌ها، آسیب‌پذیری‌ها و شواهد مرتبط با حادثه‌ای است که رخ داده است. هدف از این بخش یافتن محدوده حادثه، ذات وقوع حادثه و راهبردهایی که برای رفع آن می‌توان در پیش گرفت. تیم CERT با تحلیل آسیب‌پذیری و آرتیفکت می‌تواند تحلیل کامل و به‌روزی را در مورد سیستمی که مورد حمله قرار گرفته است فراهم آورد. CERT تمامی شواهد مربوط به حادثه را به‌منظور یافتن روند حمله، ارتباط بین فعالیت‌ها، الگوی حمله و یا امضای نفوذ همبسته سازی می‌نماید. دو زیر سرویس که در این بخش توسط تیم CERT ارائه می‌شود - البته بر اساس اهداف، مأموریت‌ها و چشم‌اندازهای سازمان - به شرح زیر است:

- جمع‌آوری مدارک فارتیک^{۲۱}: جمع‌آوری، مستندسازی، نگهداری و تحلیل شواهد از سیستم‌هایی که مورد نفوذ قرار گرفته‌اند، با هدف شناسایی تغییرات ایجاد شده بر روی سیستم توسط این زیرسرویس انجام می‌شود تا بتوان رویدادهایی که منجر به بروز این حمله موفق بر روی سیستم شده‌اند مجدداً بازسازی و در نتیجه شناسایی شوند. این جمع‌آوری اطلاعات باید به شکلی انجام گیرد که زنجیره جرم‌شناسی قابل استنادی را بر اساس شواهد در دادگاه‌ها فراهم نموده و ادله دادگاه‌پذیر داشته باشد. فعالیت‌هایی که در این زیرسرویس انجام می‌شود شامل تهیه تصویر کاملی^{۲۲} از هارد درایو سیستم آلوده، بررسی تغییرات صورت گرفته بر روی سیستم شامل فایل‌ها و برنامه‌های جدید و موارد مشابه، بررسی برنامه‌های در حال اجرا و پورت‌های باز و در نهایت بررسی

کوتاه‌مدت برای رفع مشکل امنیتی، مورد استفاده قرار می‌گیرد. هدف اصلی این سرویس مهیا کردن راهنمایی برای محافظت از سیستم‌ها و بازیابی سیستم‌هایی است که مورد نفوذ قرار گرفته‌اند. در این سرویس، اطلاعات ممکن است توسط مرکز CERT، CSIRT یا توسط سایر فروشندگان خدمات امنیتی و یا متخصصان امنیتی ایجاد شده باشد.

۲- رسیدگی به حادثه

این سرویس به فرآیند دریافت، تریاژ و پاسخ‌گویی به درخواست‌ها و گزارش‌ها و تجزیه و تحلیل حوادث و رویدادها گفته می‌شود. فعالیت‌های پاسخ‌گویی می‌تواند شامل موارد زیر باشد:

- اقدامات مورد نیاز جهت محافظت از سیستم‌ها و شبکه‌هایی که توسط مهاجمان تهدید می‌شوند.
- فراهم کردن راه‌حل‌ها و استراتژی‌های کاهش مخاطرات با در نظرگیری هشدارهای مرتبط.
- جستجو برای فعالیت‌های نفوذ در تمام نقاط شبکه.
- پیویش ترافیک شبکه.
- نصب وصله^{۲۳} و اصلاح سیستم‌ها.
- تدوین راهبرد مناسب برای سایر پاسخ‌ها یا رویه‌ها. از آنجا که فعالیت‌های رسیدگی به حادثه به روش‌های مختلف و توسط CERT‌های گوناگون پیاده‌سازی می‌شوند، این سرویس بر اساس نوع فعالیت‌های انجام شده و نوع کمک‌های داده شده به شکل زیر دسته‌بندی می‌شود:
- تجزیه و تحلیل حادثه: سطوح مختلفی برای تحلیل

21 Paching

22 Forensic Evidence Collection

23 Bit-Image

بخش حقوقی، منابع انسانی و دایره قانونی است. این بخش از سرویس نیز نیازی به حضور فیزیکی در محل ندارد.

۳- رسیدگی به آسیب‌پذیری

این سرویس شامل دریافت اطلاعات و گزارش‌ها در مورد آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری، تحلیل ماهیت و اثرات آسیب‌پذیری و ایجاد استراتژی‌های پاسخ برای شناسایی و تعمیر آسیب‌پذیری است. در ابتدا، CERT یک تجزیه و تحلیل و بازرسی فنی از آسیب‌پذیری‌های احتمالی در نرم‌افزار و سخت‌افزار انجام می‌دهد. در گام بعد، CERT پاسخی را تولید می‌کند که شامل وصله‌ها، تعمیرات و روش‌های جایگزین موقت^{۲۷} است. در آخر، CERT اطلاعات و خدمات مورد نیاز در خصوص نحوه اصلاح یا کاهش آسیب‌پذیری را با سایر ذینفعان به اشتراک می‌گذارد. سه زیرسرویس (فرآیند) اساسی که در این سرویس وجود دارد به شرح زیر است:

■ **تحلیل آسیب‌پذیری:** تیم CERT می‌تواند تحلیل و آزمون فنی بر روی آسیب‌پذیری‌های سخت‌افزار و نرم‌افزار انجام دهد. این تحلیل شامل صحت‌سنجی وجود آسیب‌پذیری، آزمون فنی آسیب‌پذیری نرم‌افزاری و سخت‌افزاری و تحلیل چگونگی سوءاستفاده از آسیب‌پذیری است. تحلیل سئورس‌کد، استفاده از دیباگر برای اطمینان از چگونگی وقوع آسیب‌پذیری یا شبیه‌سازی آسیب‌پذیری و جمله در یک سیستم شبیه‌ساز از مواردی است که در این بخش انجام می‌شود.

■ **پاسخ‌گویی به آسیب‌پذیری:** این سرویس تبیین پاسخ دقیق برای رفع آسیب‌پذیری و یا کاهش آن، هدف اصلی این سرویس است. این کار شامل توسعه وصله‌های امنیتی و یا تحقیق در خصوص وصله‌ها، راه‌کارهای رفع آسیب‌پذیری و سایر فعالیت‌های جانبی برای کاهش آسیب‌پذیری و اطلاع‌رسانی به سایر شعب و بخش‌ها در خصوص راهبردهای کاهش است.

■ **هماهنگی پاسخ‌گویی به آسیب‌پذیری:** تیم CERT سایر شعب بانکی و مالی و سایر بخش‌های درگیر در خصوص سازمان اصلی را در مورد وجود آسیب‌پذیری مطلع ساخته و اطلاعات مربوط به چگونگی رفع یا کاهش آسیب‌پذیری را به آن‌ها اعلام می‌دارد. تیم CERT اطمینان حاصل می‌کند که راهبرد کاهش و پاسخ‌گویی به آسیب به‌طور کارآمد پیاده‌سازی شده است. برقراری ارتباط با فروشندگان محصولات، سایر CERTها و CSIRTها، متخصصان فنی، افرادی که در کشف آسیب‌پذیری دخیل بوده‌اند و هیئت خبره مجموعه، از سایر اقداماتی است که در حوزه هماهنگی صورت می‌گیرد. عمده فعالیت‌های این سرویس شامل موارد زیر است: (۱) ساده‌سازی تحلیل آسیب‌پذیری یا گزارش آسیب‌پذیری، (۲) هماهنگ‌سازی زمان انتشار مستندات، وصله‌ها و راه‌کارهای رفع آسیب‌پذیری، (۳) تبیین تحلیل فنی صورت گرفته از طرف‌های مختلف.

وجود روت‌کیت یا تروجان و سایر بدافزارها بر روی سیستم آلوده است. اعضای از تیم که این فعالیت را انجام می‌دهند، معمولاً برای دفاع از ادله جرم، در دادگاه حاضر می‌شوند.

- ردیابی^{۲۴} یا رصد^{۲۵}: این زیرسرویس به معنای رصد و پایش مهاجم اصلی و شناسایی سیستم‌هایی است که مهاجم به آن‌ها دسترسی پیدا کرده است. عمده فعالیت‌های این بخش شامل موارد زیر است: (۱) رصد و پایش چگونگی ورود مهاجم به سیستم‌های سازمان و شبکه مربوطه، (۲) یافتن سیستمی که امکان نفوذ مهاجم را فراهم کرده است، (۳) محل آغاز حمله، (۴) فهرست سیستم‌ها و ادواتی است که برای گسترش حمله مورد استفاده قرار گرفته است و (۵) تلاش برای شناسایی هویت اصلی مهاجم در صورت امکان. این بخش از فعالیت‌ها که در سرویس انجام می‌شود معمولاً با همکاری متخصصان بخش حقوقی، فراهم‌کنندگان اینترنت و سایر سازمان‌های دخیل در این حوزه انجام می‌شود.

■ **پاسخ‌گویی به حادثه در سایت (محل):** تیم CERT می‌تواند به سازمان، بخش یا تیمی که سیستم‌های آن مورد حمله قرار گرفته است کمک مستقیم در -محل^{۲۶} ارائه دهد. برای این کار تیم به صورت فیزیکی در محل حاضر شده، سیستم‌های حمله شده را تحلیل می‌کند و به بازبانی و تصحیح سیستم در صورت امکان می‌پردازد. همان‌طور که بیان شد این کار با حضور فیزیکی انجام می‌شود، لذا ممکن است متخصصان تیم، مسیری را برای حضور در محل مسافرت نمایند.

■ **پشتیبانی پاسخ‌گویی به حادثه:** تیم CERT از طریق مستندات، تلفن و یا ایمیل می‌تواند به تیم قربانی برای رفع مشکل و بازبانی از فاجعه کمک کند. این کار شامل کمک فنی در جمع‌آوری اطلاعات از سیستم‌ها، فراهم‌سازی اطلاعات تماس و تبیین راهبردهایی برای رفع مشکل است. این بخش از سرویس نیازی به حضور فیزیکی در محل ندارد.

هماهنگی پاسخ‌گویی به حادثه: CSIRT (که به‌عنوان هماهنگ‌کننده CERT به حساب می‌آید)، به هماهنگ‌سازی پاسخ به حادثه در بین سایر طرف‌های درگیر در حادثه می‌پردازد. این طرف‌های درگیر معمولاً قربانی، سایر شعب درگیر در حمله، تمامی شعبی است که برای تحلیل حمله نیاز به حضور آن‌ها وجود دارد، طرف‌هایی که کمک‌های فناوری اطلاعات ارائه می‌دهد، فراهم‌کنندگان خدمات اینترنت، سایر CERTها و CSIRTها و سرپرست سیستم و اینترنت در سایت را شامل می‌شود. فعالیت هماهنگی می‌تواند شامل جمع‌آوری اطلاعات تماس، اطلاع به سایت در خصوص هویت احتمالی مهاجم، جمع‌آوری آمار و ارقام در مورد تعداد شعبی که مورد حمله قرار گرفته‌اند و نیز ساده‌سازی اشتراک‌گذاری اطلاعات باشد. البته بخش دیگری که در این زیرسرویس قابل انجام است، هماهنگی با

24 tracing

25 tracking

26 On site

27 workarounds



متوسط تا طولانی مدت مانند کشف آسیب پذیری های جدید یا ابزار نفوذ را گزارش می دهد. این سرویس دینفعان را قادر می سازد تا از سیستم ها و شبکه شان در برابر مشکلات جدید کشف شده محافظت نمایند.

۲- پایش فناوری

CERT پیشرفت های فنی جدید، فعالیت های نفوذ و گرایش های مرتبط را به منظور در شناسایی تهدیدات آینده رصد و بررسی می کند. عناوین مورد بررسی می تواند شامل قوانین شرعی و قانونی، تهدیدهای سیاسی و اجتماعی و فناوری های نوظهور باشد. این سرویس شامل خواندن ایمیل های امنیتی، وبسایت های امنیتی و اخبار کنونی و مقالات علمی در حوزه های علمی، فنی، سیاست به منظور استخراج اطلاعات مرتبط با امنیت سیستم ها و شبکه ها است. همچنین این سرویس می تواند به منظور کسب اطمینان از دستیابی به بهترین و دقیق ترین اطلاعات با نهادهای معتبر فعال در این زمینه ها ارتباط قرار کند. نتایج این سرویس ممکن است نوعی اعلان، رهنمود یا توصیه و پیشنهاد برای مشکلات امنیتی باشد.

۳- ارزیابی و حسابرسی امنیتی

این سرویس بر اساس نیازمندی های تعریف شده توسط سازمان یا استانداردهای صنعتی، زیرساخت امنیتی یک شرکت را به صورت دقیق و جزئی مورد تحلیل

۴- رسیدگی به آرتیفکت

آرتیفکت به هر فایل یا شیئی که با هدف حمله به سیستم ها یا شبکه ها یا تضعیف اقدامات امنیتی بر روی سیستم قربانی قرار گرفته است، گفته می شود. آرتیفکت ها می تواند شامل ویروس های کامپیوتری، برنامه اسپ تروجان، کرم ها اسکرپیت های مخرب و یا تول کیت ها^{۲۸} باشد. رسیدگی به آرتیفکت با دریافت اطلاعات مرتبط با آرتیفکت و یک نسخه از آرتیفکتی که در حمله یا فعالیت غیرمجاز مورد استفاده قرار گرفته است شروع می شود. به محض دریافت اطلاعات آرتیفکت بررسی می شود و بر اساس ماهیت، مکانیسم، ورژن و استفاده از آرتیفکت استراتژی های پاسخ دهی برای تشخیص، حذف و مقابله با این آرتیفکت توسعه داده می شود. این سرویس با عنوان سرویس بررسی بدافزار^{۲۹} نیز شناخته می شود که تجزیه و تحلیل، پاسخگویی و هماهنگی محصولات آرتیفکت ها را بر عهده دارد. تحلیل آرتیفکت ها یک مهارت کاملاً تخصصی است که تمامی مراکز CERT آن را ارائه نمی دهند. زمانی که بدافزار شناسایی شود، تمامی مراکز CERT با هماهنگی یکدیگر یک وصله یا نرم افزار ضد ویروس را ایجاد می کنند (۱۲). سه زیرسرویس (فرآیند) اساسی که در این سرویس وجود دارد به شرح زیر است:

■ **تحلیل آرتیفکت:** تیم CERT هرگونه تحلیل فنی بر روی آرتیفکت های یافته شده بر روی سیستم را انجام می دهد. شناسایی نوع فایل، ساختار آرتیفکت، مقایسه آرتیفکت یافته شده با آرتیفکت های شناخته شده موجود، مهندسی معکوس برای یافتن کد و تحلیل متن و موارد مشابه از جمله اهداف اصلی تحلیل آرتیفکت است.

■ **پاسخگویی به آرتیفکت:** این سرویس شامل انجام فعالیت های مربوط به شناسایی و از بین بردن آرتیفکت و جلوگیری از امکان نصب آرتیفکت از مواردی است که در این بخش انجام می شود. ایجاد امضایی که بتواند این نوع آرتیفکت را در ابزار ضد بدافزار تشخیص دهد از نمونه کارهای فنی است که در این بخش انجام می شود.

■ **هماهنگی پاسخگویی به آرتیفکت:** اشتراک گذاری و ترکیب^{۳۰} نتایج تحلیل مربوط به راهبردهای شناسایی آرتیفکت که توسط افراد مختلف، CERT های مختلف یا سایر متخصصان امنیت انجام شده است، از جمله فعالیت های این بخش است.

۵- سرویس های پیش گیرانه

این دسته از سرویس ها اطلاعات و راهنماهایی را برای آماده سازی، حفاظت و امن سازی سیستم های مجموعه پیش از وقوع حمله، مشکل یا حادثه فراهم می کند. خروجی این سرویس ها باعث کاهش حادثه ها در آینده می شود.

۱- اعلان عمومی

این سرویس شامل هشدارهای نفوذ، اخطارهای آسیب پذیری و مشاوره های امنیتی است. چنین اعلان هایی به طور مداوم پیشرفت های جدید با تأثیر

28 toolkits

29 malware handling

30 synthesizing

این سرویس رهنمودها و روش‌های مناسبی را برای پیکر بندی و نگهداری امن ابزارها، برنامه‌های کاربردی و زیرساخت محاسباتی عمومی که توسط CERT مورد استفاده قرار می‌گیرد، شناسایی یا مهیا می‌کند. علاوه بر عرضه رهنمودها، CERT ممکن است به روزرسانی و نگهداری از ابزارها و سرویس‌های امنیتی مانند IDS، سیستم‌های نظارت و پویس شبکه، فیلترها، پویس‌ها^{۳۱}، دیوارهای آتش، شبکه‌های مجازی خصوصی، کامپیوترهای شخصی، لپ‌تاپ‌ها و سایر تجهیزات بی‌سیم را انجام دهد. این سرویس شامل مدیریت هرگونه مشکل مرتبط با پیکر بندی و ابزارها و برنامه‌هایی است که بنا به گفته CERT یک سیستم را از حملات و آسیب‌پذیری مصون نگه می‌دارد.

۵- توسعه ابزارهای امنیتی

این سرویس شامل توسعه ابزارهای جدید و خاص محور است که توسط CERT و یا سازمان‌های مرتبط با CERT توسعه داده می‌شود. این سرویس می‌تواند شامل توسعه وصله‌های امنیتی برای نرم‌افزارهای سفارشی‌شده، و یا توزیع نرم‌افزارهای امن برای امن‌سازی میزبان‌های در معرض خطر باشد. همچنین این سرویس دربرگیرنده توسعه ابزارها و اسکریپت‌هایی است که عملکرد ابزارهای امنیتی کنونی را بهبود می‌دهد، از جمله این ابزارها می‌توان به یک پلاگین^{۳۲} جدید برای آسیب‌پذیری یا کاوش شبکه، اسکریپت‌هایی که استفاده از فناوری رمزنگاری را آسان می‌کند یا مکانیسم‌های توزیع‌شده خودکار اشاره کرد.

۶- سرویس‌های تشخیص نفوذ

این سرویس شامل بررسی رخدادهای دریافتی از IDS و تحلیل و پاسخ‌دهی به رویدادهایی است که سیاست‌های تعریف‌شده را نقض می‌کند. تشخیص نفوذ و تحلیل رخدادهای امنیتی مرتبط، وظیفه حساس و پرمخاطره‌ای است، زیرا نه تنها وظیفه تشخیص محل قرارگیری حس‌گرها در محیط را بر عهده دارند، بلکه وظیفه جمع‌آوری و تحلیل حجم زیادی از داده‌های دریافتی را بر عهده دارند. در بسیاری از موارد، ابزارهای خاص و دانش فنی ویژه‌ای جهت ترکیب و تفسیر اطلاعات و شناسایی هشدارها، حملات و رخدادهای شبکه‌ای اشتباه و پیاده‌سازی استراتژی‌های کاهش و کمینه‌سازی چنین رخدادهایی مورد نیاز است. بعضی از سازمان‌ها اقدام به برون‌سپاری این فعالیت به مراکز عرضه خدمات امنیتی مدیریت‌شده^{۳۳} می‌کنند که نیروی متخصص و ابزارهای کافی برای ارائه این سرویس را در اختیار دارند.

۷- انتشار اطلاعات امنیتی

این سرویس باهدف کمک به بهبود امنیت مجموعه‌ای



و بررسی قرار می‌دهد. همچنین این سرویس می‌تواند اقدامات امنیتی سازمانی را نیز مورد بازبینی قرار دهد. ارزیابی و حسابرسی می‌تواند به روش‌های مختلفی عرضه شود که شامل موارد زیر است:

- مرور و بررسی زیرساخت: بازبینی دستی پیکر بندی سخت‌افزار و نرم‌افزار، روتر، فایروال، سرور و کامپیوترهای شخصی به منظور اطمینان از تطابق با استانداردها و خط‌مشی‌های سازمان.
- بازبینی به روش‌ها: مصاحبه با کارمندان و سرپرستان سیستم‌ها و شبکه به منظور اطمینان از این که فعالیت‌های امنیتی آن‌ها با سیاست‌ها و استانداردهای سازمان تطابق دارد.
- استفاده از پویس‌گرهای ویروس و آسیب‌پذیری برای شناسایی سیستم‌ها و شبکه‌های آسیب‌پذیر.
- انجام تست نفوذ به منظور سنجش میان امنیتی سیستم‌ها و شبکه
- دریافت رضایت مدیر سطح بالاتر برای انجام این ممیزی‌ها و حسابرسی‌ها ضروری است. برخی از ممیزی‌ها ممکن است بر اساس سیاست‌های سازمان منع قانونی داشته باشد. این سرویس می‌تواند توسط خود تیم CERT انجام شده و یا به صورت پیمانکاری به یک شرکت ثالث ارجاع داده شود.

۴- پیکر بندی و نگهداری از ابزارها، تجهیزات، زیرساخت‌ها و سرویس‌های امنیتی

31 wrapper

32 plug-in

33 managed security service providers

گروه‌های CSIRT می‌توانند به منظور ارائه مشاوره و راهنمایی برای بهترین روش‌های امنیت در پیاده‌سازی مؤلفه‌های عملیات کسب‌وکار مورد استفاده قرار گیرند. یک گروه CERT با ارائه این سرویس در ارائه توصیه‌نامه‌ها یا شناسایی نیازمندی‌ها برای حصول، نصب یا امن سازی سیستم‌های جدید، ادوات شبکه، برنامه‌های کاربردی نرم‌افزاری یا فرآیندهای کسب‌وکار سازمانی درگیر می‌شوند. این سرویس ارائه راهنمایی‌ها و کمک‌هایی به منظور توسعه سیاست‌های امنیتی کلان و سازمانی را شامل می‌شود. همچنین این سرویس به قانون‌گذار یا دیگر بدنه‌های دولت مشاوره می‌دهد.

۴- ایجاد آگاهی

گروه‌های CERT قادر به شناسایی موقعیت‌هایی هستند که اجزای اصلی در آن به اطلاعات و راهنمایی‌های بیشتری برای تطبیق بهتر با روش‌های امنیتی پذیرفته‌شده و سیاست‌های امنیتی سازمانی نیاز دارند. با افزایش آگاهی امنیتی افراد وابسته، نه تنها درک و آگاهی آن‌ها از مسائل امنیتی بیشتر می‌شود بلکه به آن‌ها در انجام عملیات روزانه به روشی امن‌تر کمک می‌کند. این موضوع می‌تواند وقوع حملات موفق را کاهش دهد و احتمال تشخیص و گزارش حملات را برای اجزای اصلی افزایش دهد و در نتیجه میزان تلفات و زمان‌های بازیابی را کاهش دهد.

گروه‌های CERT با انجام این سرویس به دنبال موقعیت‌هایی به منظور افزایش آگاهی وضعیتی از طریق توسعه مقالات، پوسترها، نشریه‌های خبری، وب‌سایت‌ها یا دیگر منابع اطلاعاتی هستند که بهترین شیوه‌های امنیتی را شرح می‌دهند. فعالیت‌ها نیز شامل زمان بندی جلسات و سمینارها به منظور به روز بودن اجزای اصلی با تداوم رویه‌های امنیتی و تهدیدات سیستم‌های سازمانی است.

۵- آموزش و یادگیری

این سرویس اطلاعاتی را درباره مسائل امنیتی کامپیوتر از طریق سمینارها، کارگاه‌های کاری، دوره‌های آموزشی و کمک آموزشی به اجزای اصلی ارائه می‌دهد. موضوعات این بخش شامل دستورالعمل گزارش‌های حوادث، روش‌های مناسب پاسخگویی، ابزار پاسخگویی به حوادث، روش‌های پیشگیری از حوادث و اطلاعات ضروری دیگر به منظور حفاظت، تشخیص گزارش و پاسخ به حوادث امنیتی کامپیوتری است.

۶- ارزیابی و تأیید محصول

برای این سرویس یک گروه CERT، ابزارها، برنامه‌های کاربردی و یا سرویس‌های دیگر محصول را به منظور اطمینان از امنیت آن‌ها مطابق با روش‌های پذیرفته‌شده توسط CERT و شیوه‌های امنیتی سازمانی ارزیابی می‌کند. ابزارها و برنامه‌های کاربردی بررسی شده می‌توانند به صورت محصولات تجاری و یا منبع باز باشند

کامل از اطلاعات مفید و در دسترس را برای ذینفعان فراهم می‌آورد. این اطلاعات می‌توانند شامل موارد زیر باشند:

- گزارش راهنمایی‌ها و اطلاعات تماس برای CERT
 - بایگانی رخدادها، هشدارها و سایر اعلان‌ها
 - مستندسازی درباره بهترین شیوه‌های رایج
 - راهنمایی امنیت کامپیوتر عمومی
 - سیاست‌ها، روندها و چک‌لیست‌ها
 - وصله اطلاعات توزیع شده
 - لینک فروشنده
 - آمارهای رایج گزارش حوادث
 - اطلاعات دیگری که می‌تواند امنیت کلی را بهبود دهد.
- این اطلاعات می‌تواند به وسیله CERT یا سایر اجزای سازمان مانند بخش IT، منابع انسانی و بخش‌های دیگر توسعه یابد و منتشر شود.

۶- سرویس‌های مدیریت کیفیت امنیت

این بخش از سرویس‌های CSIRT در حوزه فعالیت‌های تمامی واحدهای درگیر در مجموعه مانند واحد فناوری اطلاعات، ممیزی و آموزش قرار می‌گیرد. در صورتی که واحدهای پیش‌گفته با CSIRT در حوزه‌های کاری خود همکاری نمایند، می‌توان گفت که نتیجه آن می‌تواند به بهبود دید عمومی سازمان در مقابل تهدیدها، ضعف‌های سیستم‌ها و... منجر شود.

۱- تجزیه و تحلیل ریسک

CERTها قادر به تجزیه و تحلیل و ارزیابی ریسک‌ها هستند. این گروه‌ها می‌توانند توانایی سازمان‌ها در ارزیابی تهدیدات، ارائه ارزیابی کمی و کیفی مناسب ریسک‌ها به منظور ارزیابی اطلاعات و همچنین ارزیابی استراتژی‌های پاسخگویی و حفاظت را بهبود بخشند. گروه‌های CERT با انجام این سرویس به فعالیت‌های تجزیه و تحلیل ریسک‌های امنیتی اطلاعات برای سیستم‌های جدید و فرآیندهای کسب‌وکار یا ارزیابی تهدیدات و حملات در برابر دارایی‌ها و سیستم‌ها کمک خواهند کرد.

۲- طرح بازیابی حوادث و تداوم کسب‌وکار

بر اساس رخدادها، گذشته و پیش‌بینی‌های آینده رویه‌های امنیتی یا حوادث به وجود آمده، بیشتر حوادث در اثر اختلال جدی در کسب‌وکار است. بنابراین باید تلاش شود تا برنامه‌ریزی‌ها در جهت توصیه‌ها و تجارب گروه CERT به منظور بهبود پاسخگویی به حوادث برای اطمینان از تداوم کسب‌وکار باشد. گروه‌های CERT با انجام این سرویس در طرح بازیابی حوادث و تداوم کسب‌وکار برای رخدادها، مرتبط با حملات و تهدیدات امنیتی، درگیر می‌شوند.

۳- مشاور امنیت



امن باش و بمان

www.kashef.ir