کاشف
مدیریت امن الکترونیکی
(سهامی خاص)

نشریه
امنیت بانکداری

شماره دوم، بهار ۱۴۰۳
نشریه تخصصی شرکت مدیریت امن الکترونیکی کاشف

امنیت اطلاعات

تحول دیجیتال بدون امنیت
واعتماد دیجیتال ممکن نیست

نگاهی به عملکرد دستاوردها
و برنامه های کاشف

پیاده سازی الزامات امنیت اطلاعات و بانکداری
درصرافی ها به یک ضرورت تبدیل شده است

فهرست

امنیت بانکداری

مدیریت امن الکترونیکی (سهامی خاص)

نشریه امنیت بانکداری

نشریه تخصصی شرکت مدیریت امن الکترونیکی کاشف

شماره دوم، بهار ۱۴۰۳

مدیر عامل: حسین قرایی

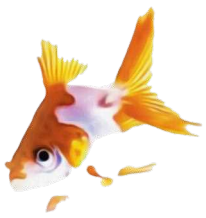
مجری طرح، گردآوری و ویراستاری: روابط عمومی شرکت کاشف

باهمکاری: موسسه مطبوعاتی بازار پول و ارز (ایبنا)

نشانی: تهران، خیابان ظفر، شماره ۴۱

تلفن: ۷۲۸۶۱۰۰۰

سایت و ایمیل: www.kashef.ir info@kashef.ir



سال نو مبارک

سرمقاله

تحول دیجیتال بدون امنیت و اعتماد دیجیتال ممکن نیست

محمدرضا فرزین
دبیرکل بانک مرکزی

تردیدی نیست که خدمات بانکداری و پرداخت الکترونیکی طی دو دهه اخیر در کشور ما از گستره و عمق قابل ملاحظه‌ای برخوردار بوده است. گذشته از ملاحظاتی که ممکن است درباره کیفیت و کمیت این خدمات مطرح باشد، ایجاد چنین منظومه‌ای از خدمات بانکی بر بستر فناوری اطلاعات جای افتخار و مباهات دارد و به ایران اسلامی جایگاهی ممتاز در میان کشورهای منطقه بخشیده است چرا که کمتر کشوری را می‌توان در دامنه جغرافیایی منطقه سراغ گرفت که از زیرساخت‌ها و خدماتی با این تنوع بهره‌مند باشد و طیف گسترده‌ای از ابزارها و سرویس‌های بانکی و پرداختی الکترونیکی در اختیار کاربران قرار داده باشد.

نکته بسیار مهمی که لازم می‌دانم در این مورد با مخاطبان این نوشته در میان بگذارم این است که خوشبختانه استفاده از ابزارهای الکترونیکی در حوزه بانکی از سوی جامعه ایرانی به خوبی پذیرفته شده تا جایی که دریافت ابزارها و خدمات پیشرفته‌تر را می‌توان یکی از مطالبات مردم دانست. این پذیرش و مطالبه بدون شک رخ نمی‌داد مگر در سایه اعتمادی که کاربران به پایداری و امنیت ابزارها دارند؛ پر واضح است که در صورت نبود این اعتماد، مردم به هیچ‌وجه و حتی با وجود ارائه رایگان این قبیل خدمات، حاضر به استفاده از آنها به‌ویژه در حوزه حساسی مانند دارایی‌های پولی خود نبودند. به همین دلیل نیز خدشه‌دار کردن این اعتماد به عنوان سرمایه‌ای اجتماعی که در موارد مختلفی به نهادهای حاکمیتی در اجرای دقیق‌تر، کم‌هزینه‌تر و سریع‌تر بسیاری از تصمیمات کلان کمک کرده و می‌کند، از جمله اهداف بدخواهان این مرز و بوم است و شاهد تلاش‌های فراوانی از سوی آنان در قالب حمله و آسیب‌رسانی به زیرساخت‌های فنی و تضعیف این اعتماد عمومی بوده و هستیم.

زیرساخت‌های بانکی کشور همواره به عنوان یکی از زیرساخت‌های حیاتی و استراتژیک کشور، همواره مورد سوءقصد بدخواهان و معاندان نظام مقدس جمهوری اسلامی ایران بوده و هست اما به لطف الهی و با کوشش متخصصان این مرز و بوم، تدابیر اندیشیده شده از سوی بانک مرکزی همواره سد محکمی در برابر این عناد و بدخواهی بوده و حافظ کیان نظام مقدس اسلامی و همچنین شبکه بانکی کشور بوده است.

در عین حال چنین شرایط خطیری صد البته مسئولیت نهادهای متولی در حوزه امنیت فناوری را به‌خصوص در حوزه بانکی صد چندان کرده و بانک مرکزی جمهوری اسلامی نیز با درک این حساسیت و اهمیت، تدابیر و برنامه‌های فراوانی برای ارتقای مستمر امنیت زیرساخت‌ها و خدمات بانکی و پرداختی را از طریق بازوهای فنی و اجرایی خود به اجرا گذاشته است که خوشبختانه نتایج و آثار مثبت این اقدامات در ارائه خدمات بانکی امن و به‌روز به مردم شریف ایران اسلامی مشهود است.

علاوه بر این موارد اما نکته مهمی که مایلم بر آن تأکید کنم این است که هدف اصلی از برقراری امنیت در خدمات بانکداری، ایجاد اعتماد است. این قدرت اعتماد است که کاربران را به استفاده از ابزارها و خدمات ترغیب می‌کند و امکان حکمرانی با اقتدارتر و بهتر را فراهم می‌آورد. ما باید باور کنیم که در دنیای امروز نگاه به مقوله امنیت اطلاعات تغییر کرده است. آنچه بیش و پیش از امنیت مورد توجه قرار می‌گیرد، اعتماد یا همان Trust است چرا که اعتماد، امنیت را به دنبال می‌آورد. باید باور کنیم و این باور را گسترش دهیم که «تحول دیجیتال بدون اعتماد دیجیتال امکانپذیر نیست» چرا که ممکن است یک سیستم امن باشد، ولی قابل اعتماد نباشد و بالعکس. لذا بانک مرکزی به عنوان نهاد رگولاتور به ویژه در یکسال اخیر، سعی و تلاش ویژه‌ای در توسعه این اعتماد به منظور دستیابی به حکمرانی دیجیتال در فضای اقتصادی و مالی کشور داشته و دارد که امیدواریم ثمرات همه این اقدامات، منجر به توسعه هرچه بیشتر خدمت‌رسانی به عموم مردم شریف ایران باشد.

یادداشت

نگاهی به عملکرد دستاوردها و برنامه‌های کاشف

دکتر حسین قرایی
مدیرعامل کاشف

در یک سال گذشته با تلاش و همکاری مدیران و همکاران کاشف، برنامه جدیدی در راستای تحقق اهداف و انتظارات بانک مرکزی تدوین شد. این برنامه شامل ارتقای حکمرانی امنیت اطلاعات، مدیریت مخاطرات و تطابق‌پذیری، ارتقای 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.

رویکرد کاشف در تدوین و اجرای این برنامه‌ها همانطور که رئیس کل محترم بانک مرکزی به دفعات اشاره کرده‌اند، ایجاد اعتماد و اطمینان در تمامی لایه‌ها و کاربران خدمات بانکداری و پرداخت الکترونیکی در کشور است. به‌این‌ترتیب علاوه بر افزایش سطح رضایتمندی و بهره‌وری، زمینه‌های لازم برای تحول دیجیتال در تمام عرصه‌های کشور فراهم خواهد شد. در این راستا تلاش داریم، آگاهی از خدمات و مسئولیت‌های کاشف را در حوزه‌های مختلف افزایش دهیم. بر همین اساس، ارتقای جایگاه شرکت در زیست‌بوم امنیت اطلاعات کشور از اولویت‌های ما بوده و هست.

در این خصوص، دریافت مجوز دانش‌بنیان شدن شرکت کاشف، دریافت مجوز انفورماتیک و مجوز آزمایشگاه ارزیابی امنیتی کاشف از افتای ریاست جمهوری بخشی از این تلاش‌ها بوده که طی یک سال گذشته در جهت دست‌یابی به این مهم صورت گرفته است. چشم‌انداز ما در کاشف تبدیل شدن به معتمدترین مرجع و عامل پیشران در ارتقای امنیت، پایداری و تاب‌آوری در زیست بوم تولید و تبادل اطلاعات بانکی است. علاوه بر این تلاش کردیم در سال ۱۴۰۲ برای حوزه‌های امنیتی کاشف شامل تنظیم مقررات، ارزیابی و اعتبارسنجی و رسیدگی به تهدیدها، پروژه‌های لازم را تعریف و عملیاتی کنیم و بر همین اساس نیز ۴۰ پروژه در قالب نیازمندی‌های بانک مرکزی به ثمر رسید. راه‌اندازی و عملیاتی شدن آزمایشگاه کاشف و انجام بیش از ۷۰ تست و ارزیابی در حوزه‌های وب، شبکه، برنامک‌های موبایل، برنامک‌های نماد و گواهی امضای دیجیتالی نیز از جمله اقدامات این شرکت بوده است که همگی در راستای تحقق این هدف است که کاشف به معتمدترین مرجع و عامل پیشران در ارتقای امنیت اطلاعات بانکی تبدیل شود. علاوه بر این پروژه‌ها، تدوین و اجرای برنامه جامع ارتقای امنیت بانک مرکزی و شبکه بانکی از اقدامات بسیار ضروری و مهمی است که کاشف در حال انجام آن است.

طراحی، توسعه و پیاده‌سازی سامانه سرآمد ۳ از دی ماه سال ۱۴۰۱ و رونمایی از آن در اول آبان ۱۴۰۲، راه‌اندازی و عملیاتی کردن مدیریت آسیب‌پذیری در شبکه و سامانه‌های بانک مرکزی، شبکه پرداخت و شبکه صرافی‌ها، انتشار نسخه جدید سامانه رادار و پیگیری منظم از بانک‌ها برای ارتقای مرکز عملیات امنیت در داخل بانک‌ها، راه‌اندازی فاز اول مرکز اشتراک‌گذاری و تحلیل اطلاعات بانکی (FS-ISAC) و همچنین ارتقای ماژول آسیب‌پذیری سامانه پیکار و هوش‌یار از دیگر اقدامات شرکت کاشف در یک سال اخیر بوده است.

یکی دیگر از مقولاتی که تلاش داریم در آن بیش از پیش فعالیت کنیم، فرهنگ‌سازی و توسعه دانش و آگاهی در حوزه امنیت اطلاعات است. در این راستا نیز گام‌های نهایی به منظور راه‌اندازی آکادمی امنیت بانکی توسط شرکت کاشف برداشته 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. پویش آسیب‌پذیری‌های بانکی (پاسبانک) یکی دیگر از مهم‌ترین پروژه‌های کاشف است. در این خدمت، آسیب‌پذیری‌های سامانه‌ها و دارایی‌های سایبری اعضای نظام بانکی و پرداخت کشور که در بستر اینترنت قابل رؤیت است، شناسایی‌شده و اطلاع‌رسانی‌ها، هماهنگی‌ها و پشتیبانی‌های فنی جهت رفع هرچه سریع‌تر آنها صورت می‌پذیرد. در مدت فعالیت این پویش تاکنون مجموعا ۲۲۱ آسیب‌پذیری خاص محصولات و خدمات نظام بانکی و پرداخت را شناسایی و اعلان کرده است. رؤیت آنی و دائم رخدادهای امنیتی زیرساخت بانکی و پرداخت (رادار) از دیگر اقدامات و مأموریت‌های کاشف است که تاکنون در مجموع ۳۰۸۰ رخداد از ۳۰ مؤسسه اعتباری در سامانه رادار ثبت و رسیدگی شده است.

آنچه در امنیت نظام بانکی اهمیت دارد ایجاد وحدت رویه در رسیدگی به رخدادها می باشد که کاشف با تلاش موفق به انجام آن شد و در همین راستا باهمکاری افتای ریاست جمهوری توانست " مرکز واکنش سریع به رخدادهای نظام بانکی" را افتتاح کند. تمام آنچه ذکر شد گوشه ای از تلاش‌های متخصصان و مهندسان ایرانی در شرکت کاشف است تا بتواند در خدمت سیاست‌های بانک مرکزی و نظام بانکی کشور باشد.

گفت و گو

معاون مدیرعامل در امور فناوری اطلاعات بانک ملت:

اهمیت استفاده از هوش مصنوعی در نظام بانکی

همانطور که رایانه‌ها و سایر دستگاه‌های دیجیتال برای تجارت ضروری شده‌اند، آنها نیز به طور فزاینده‌ای به هدف حملات تبدیل شده‌اند. برای اینکه یک شرکت یا یک فرد بتواند با اطمینان و اعتماد از یک دستگاه محاسباتی یا پلتفرم استفاده کند، ابتدا باید اطمینان حاصل شود که دستگاه به‌هیچ‌وجه در معرض خطر قرار نگرفته و همه ارتباطات ایمن خواهند بود. ساخت بستر امن برای تکنولوژی‌های روز در عین حال نیازمند توانمندی‌های نیرو انسانی و حتی آگاهی‌بخشی‌های عمومی است، با این حال در ایران مسأله دیگری نیز وجود دارد که می‌تواند بر ایجاد بستر امن تأثیر فزاینده‌ای داشته باشد و آن رگولاتوری است. درباره همه این موارد با رسول لطفی آذر؛ معاون مدیر عامل در امور فناوری اطلاعات بانک ملت به گفت‌وگو نشسته‌ایم که ماحصل این گفت‌وگو را در قالب این گزارش می‌خوانید.

رسول لطفی آذر؛ دربـاره مشکلات امنیت اطلاعات شبکه بانکی در توسعه فناوری‌های نوین گفت: موضوع امنیت به امری روزمره تبدیل شده به طوری که کنترل‌های معمول استاندارد را در امنیت ملاک قرار می‌دادیم؛ اما با رخدادهای امنیتی که در جامعه شاهد آن بوده‌ایم باید به توانمندسازی نیروی انسانی و به‌کارگیری ابزار و تکنولوژی جدید در حوزه امنیت نیز بپردازیم.

لطفی آذر با بیان اینکه فرهنگ‌سازی و آموزش از دیگر موضوعات مهم در حوزه امنیت است، تأکید کـرد: اگر نیروی انسانی و کاربران سیستم‌ها دچار روزمرگی شوند و تکنولوژی قابلیت‌های سیستم خود را فعال نکند، ادعای امنیت اطلاعات نمی‌تواند کارآمد باشد.

وی با اشاره به این موضوع که قابلیت‌های حوزه فناوری اطلاعات باعث پیشرفت بانک‌ها می‌شود، گفت: اگر بانک‌ها بخواهند چارچوب و استانداردهای امنیتی را رعایت نکنند در تداوم کسب‌وکار دچار مشکل خواهند شد؛ بنابراین تهیه و تنظیم برنامه‌های راهبردی همگام با توسعه فناوری اطلاعات در حوزه امنیت و زیرساخت مهم است.

معاون مدیر عامل در امور فناوری اطلاعات بانک ملت اظهار داشت: سیاست‌نامه و استانداردهای ابلاغی واحدهای نظارتی باعث می‌شود بانک‌ها به سمت توسعه امنیت در ساختار فناوری اطلاعات حرکت کنند.

.

بانک مرکزی درحفظ امنیت شبکه بانکی چه‌نقشی دارد؟

لطفی آذر با بیان اینکه رگولاتور باعث می‌شود که سازمان‌ها و بانک‌ها موضوع امنیت را جدی بگیرند، تأکید کرد: بانک مرکزی با نظارت عالی، تدوین سیاست‌نامه و تحلیل رخدادها و انتقال آنها به بدنه فنی سازمان‌های کشور؛ به حوزه فناوری اطلاعات بانک‌ها کمک می‌کند، البته هم‌اکنون سازمان و ارگان‌هایی که در کنار بانک مرکزی قرار دارند در حوزه سیاست‌گذاری و نظارت اثرگذار هستند و به توسعه امنیت در شبکه بانکی کمک می‌کنند.

وی افزود: رگولاتور به عنوان یکی از ناظران اصلی همواره چارچوب‌های استاندارد اتصال نظام بانکی به بازیگران جدید مثل فین‌تک و پرداخت‌یارها را تعیین می‌کند؛ چون توسعه سرویس و خدمات از طریق بازیگران جدید است.

لطفی آذر با اشاره به این موضوع که به هر میزان که کاشف در حوزه نظارت، ارزیابی و چارچوب‌های سیاست‌گذاری فنی فعال‌تر باشد بهتر است تأکید کرد: بانک‌ها باید چارچوب‌های امنیتی را مطابق سیاست‌گذاری به صورت ماهانه گزارش کنند و رگولاتور نیز مجموعه فعالیت‌های کلان حوزه آی‌تی (IT) را مانیتور می‌کند تا در نهایت شاهد اثرات مثبت این مجموعه اقدامات باشیم.

وی افزود: بودجه حوزه امنیت در کل نظام بانکی حالت سلیقه‌ای دارد و رگولاتور باید برای گذاشتن چارچوب در حوزه بودجه فناوری اطلاعات تجربه‌های سایر کشورها را مبنا قرار دهد، معمولا سازمان‌ها یا بانک‌ها تمایل دارند اپلیکیشن و زیرساختی را که خریداری کردند با حداقل هزینه به توسعه برسانند، طبیعتا این الگوها می‌تواند در تعیین بودجه برای حوزه امنیت سامانه‌های بانکی کارساز باشند.

شبکه بانکی در تأمین امنیت سایبری چه جایگاهی دارد؟

معاون مدیر عامل در امور فناوری اطلاعات بانک ملت با بیان اینکه تمامی بانک‌ها در چرخه حوزه خدمات، پرداخت و سرویس بانکی از امنیت سایبری و بانکداری تأثیر می‌گیرند، گفت: اگر بانکی آسیب ببیند سایر بانک‌ها و مشتریان سازمان‌های دیگر نیز ممکن است آسیب ببینند چرا که گاهی، رخدادهایی شکل گرفته که مشتریان تمامی بانک‌ها را تحت تأثیر قرار داده است؛ بنابراین موضوع امنیت یک کار جمعی است و مجموعه نظام بانکی باید تلاش کند که سرویس‌های امنیتی ارائه دهد تا سرویس و خدماتی که به مشتریان داده می‌شود از استانداردها تبعیت کند؛ در نتیجه موضوع امنیت در حوزه بانکداری کاری جمعی است.

لطفی آذر درباره نقش هوش مصنوعی در صنعت بانکداری تأکید کرد: هوش مصنوعی در احراز هویت و شناسایی رفتار مشتریان هنگام استفاده از خدمات بانکی می‌تواند جلوی بسیاری از سوءاستفاده‌ها و مشکلات امنیتی را بگیرد؛ بنابراین ما باید در استفاده از قابلیت هوش مصنوعی در چارچوب داده، نهادسازی کنیم. برای استفاده از هوش مصنوعی باید زیرساخت‌های مربوطه در حوزه اطلاعات فراهم باشد و نوعی توسعه فناوری و تکنولوژی را به کار بگیریم تا از قابلیت هوش مصنوعی در امنیت نیز استفاده کنیم. هرچند نباید فراموش کنیم که استفاده از هوش مصنوعی در صنعت بانکداری هم تهدید و هم مزیت محسوب می‌شود و بازیگران مختلف مانند فین‌تک‌ها از تکنولوژی استفاده می‌کنند تا سهم بانک‌ها از تراکنش‌های الکترونیکی را به حداقل برسانند.

معاون مدیر عامل در امور فناوری اطلاعات بانک ملت با اشاره به این موضوع که ما باید در به‌کارگیری هر تکنولوژی از قابلیت آن برای تسهیل و سرویس‌دهی به مشتریان استفاده کنیم، تأکید کرد: مشتریان از بانک هوشمندتر هستند و می‌توانند چابک‌تر از ابزارها برای دریافت خدمات بهینه استفاده کنند، بانک‌ها نیز با هدف توسعه خدمات به مشتریان از مزایای این ابزارها استفاده می‌کنند.

وی افزود: معمولا با مطرح شدن موضوع امنیت از سرعت کاسته می‌شود؛ ولی با این وجود سعی می‌شود که زودتر و چابک‌تر از رقبا عمل کنیم، با توجه به رخدادهایی که در کشور اتفاق افتاده در تلاش هستیم تا روش‌های جدیدی را برای خدمات به‌کار بگیریم و همچنین استفاده از تکنولوژی‌ها را برای ارتقا در دستور کار قرار دهیم.

معاون مدیر عامل در امور فناوری اطلاعات بانک ملت گفت: در حوزه امنیت اطلاعات، استفاده از ابزارهای نوین و مانیتورینگ ارائه خدمات، به‌روزکردن مجوزها و ارائه هشدار و رخداد در دستور کار بانک ملت است تا بتوانیم نگرانی‌های امنیتی از سمت بانک را مدیریت کنیم.

وی افزود: قیمت تمام شده سرویس و خدمات بسیار بالاست و هر چه قدر بخواهیم امنیت را در بانک‌ها ارتقا دهیم، هزینه‌ها نیز بیشتر می‌شود، از طرفی این تکنولوژی‌ها بومی نیستند و بومی کردن تکنولوژی نیز نیاز به سرمایه‌گذاری کلان دارد.

لطفی آذر تأکید کرد: اگر بتوانیم سیاست‌های تشویقی را برای ارتقای سیستم و سامانه‌های جدید توسط بانک مرکزی و حاکمیت برنامه‌ریزی کنیم؛ وابستگی‌ها در این حوزه به شدت کاهش پیدا می‌کند.

وی در پایان گفت: باید سیاست‌های حمایتی را برای سازمان‌هایی که در حوزه امنیت سرمایه‌گذاری و هزینه می‌کنند در نظر گرفت تا بتوانیم شاهد این سیاست‌ها در بدنه سازمان و بانک‌هایی که موفق عمل کردند باشیم. ضمن اینکه باید شناسایی کنیم که چندین راهبر در حوزه امنیت داریم تا از نظر جایگاهی مورد حمایت قرار بگیرند؛ بنابراین باید نیروهای توانمند در حوزه امنیت را شناسایی و برای آنها برنامه داشته باشیم.

> احراز هویت هم‌اکنون در حوزه خدمات غیر حضوری یک تجربه جدید است که در کشور ما شکل گرفته، همچنین شناسایی رفتار مشتریان در استفاده از خدمات می‌تواند جلوی سوءاستفاده‌ها را بگیرد. البته نباید فراموش کنیم که استفاده از هوش مصنوعی در صنعت بانکداری هم تهدید و هم مزیت محسوب می‌شود و بازیگران مختلف مانند فین‌تک‌ها از این تکنولوژی استفاده می‌کنند تا سهم بانک‌ها از تراکنش‌های الکترونیکی را به حداقل برسانند

گفت‌وگو

نقش هوش مصنوعی در امنیت نظام بانکی

بانک پارسیان در حوزه امنیت چه برنامه‌هایی دارد؟

نظام بانکی کشور، به خصوص در این سال‌های اخیر، در زمینه بانکداری دیجیتال و پس از آن ایجاد امنیت در بانکداری، تلاش‌های خوبی انجام داده و بسیاری از بانک‌ها به سمت داشتن نقشه راه مناسب با شرایط‌شان رفته‌اند. با اینحال به خاطر انتظاراتی که از صنعت بانکداری می‌رود و همچنین به دلیل سرعت تغییرات در علم و فناوری، این سؤال پیش می‌آید که آیا بانکداری ایران علی‌رغم همه تلاش‌ها، به سرعت جهانی تغییرات می‌رسد؟ و در این راه با چه چالش‌هایی مواجه است؟ در ادامه سری گفت‌وگوهای نشریه امنیت بانکداری این بار با مسعود پشمچی؛ معاون فناوری اطلاعات بانک پارسیان به گفت‌وگو نشستیم و نظرات ایشان را جویا شدیم.

مسعود پشمچی؛ معاون فناوری اطلاعات بانک پارسیان با بیان اینکه بانکداری دیجیتال از نقاط قوت نظام بانکی به حساب می‌آید، گفت: بانکداری دیجیتال علاوه بر نقاط قوت تهدیدهایی مانند حملات سایبری ایجاد می‌کند و چون ایران طی چند سال اخیر در جنگ سایبری بوده؛ بنابراین نظام مالی و اقتصادی نیز ممکن است مورد حمله سایبری قرار بگیرد.

وی افـزود: موضوع حریم خصوصی از دیگر مشکلات و چالش‌های این حوزه به شمار می‌آید؛ چون بانک‌ها به عنوان نماد اعتماد مردم باید زیرساخت‌هایی را فراهم کنند تا از اطلاعات مردم نگهداری کنند؛ اما به علت تحریم‌ها مشکلاتی برای به‌کارگیری فناوری‌های نوین وجود دارد، همچنین منابع انسانی و مهاجرت نیروی انسانی نخبه نیز چالش‌های زیادی در حوزه فناوری اطلاعات و امنیت ایجاد کرده است.

تکنولوژی در حل مشکلات امنیت بانکی چه نقشی دارد؟

پشمچی اظهار داشت: پیشرفت تکنولوژی و حملات سایبری ارتباط دوطرفه‌ای دارند؛ چون با استفاده از پیشرفت تکنولوژی می‌توانیم حملات امنیتی را مدیریت کنیم و با بهبود زیرساخت‌ها و استفاده از فناوری‌های نوین، سطح امنیت را ارتقا دهیم. از طرف مقابل، پیشرفت تکنولوژی در اختیار هکرها قرار می‌گیرد و هکرها نیز با استفاده از فناوری‌های روز تنوع حملات خود را بیشتر می‌کنند، البته سازمان‌ها به خصوص بانک‌ها باید با ارتقای زیرساخت‌های خود بتوانند بر حملات هکرها غلبه کنند این زیرساخت‌ها شامل بلاکچین و امضای دیجیتال می‌شود.

معاون فناوری اطلاعات بانک پارسیان تأکید کرد: رگولاتور باید نقش حمایتی و نظارتی بر نظام بانکی داشته باشد و با تنظیم اسناد بالادستی و ابلاغ استانداردها در زمینه حفظ امنیت کمک کند، همچنین در اجرای پروژه و تدوین بودجه نیز اقدام به پشتیبانی کند.

وی افزود: وجود چندین نهاد بالادستی باعث اتلاف منابع و زمان شده به‌طوری که در حوزه امنیت و فناوری اطلاعات تعداد زیادی نهاد ناظر مانند افتا، کاشف، فتا و .... داریم؛ بنابراین حوزه فناوری اطلاعات بانک‌ها زمان زیادی را برای به پاسخگویی به سؤال‌های مختلف این نهادها صرف می‌کند، البته در برخی از موارد تناقض‌هایی در دستورالعمل و ابلاغیه‌ها نیز مشاهده می‌شود، در نتیجه یکپارچه‌سازی و یکی کردن واحدهای نظارتی، مهمترین حمایت بخش رگولاتور از نظام بانکی است. البته باتوجه به تحریم و نوسانات نرخ ارز دستیابی به تکنولوژی سخت و دارای هزینه است؛ بنابراین بانک مرکزی می‌تواند در حوزه هزینه‌ها نیز کمک کننده باشد.

وی افـزود: نظام بانکی گاهی درگیر سود و زیان است؛ بنابراین اولویت امنیت در جایگاه پایین‌تری قـرار می‌گیرد؛ در نتیجه اگر هزینه‌های حوزه امنیت با موضوع متعادل‌سازی کارمزد خدمات نوین حل شود اولویت امنیت نزد مدیران بانکی افزایش پیدا می‌کند، همچنین تدوین چارچوب‌های امنیتی به صورت یکپارچه و تعیین سطح بلوغ بانک‌ها به حوزه فناوری اطلاعات کمک می‌کند.

پشمچی با بیان اینکه نظام بانکی در کشور بر اساس فناوری است، گفت: بیشترین میزان سرمایه‌گذاری در حوزه فناوری در نظام بانکی صورت می‌گیرد و سطح ارائه خدمات نوین در این نظام نسبت به سایر کسب‌وکارها بالا است. در حوزه امنیت نیز سرمایه‌گذاری‌هایی صورت گرفته و حضور شرکت‌هایی مثل کاشف و شاپرک به استانداردسازی سطح امنیت کمک کرده است، همچنین حضور افراد نخبه باعث افزایش امنیت سیستم بانکی شده است.

وی افزود: ۴۹ درصد از مدیران بانکی در سطح جهان استفاده از هوش مصنوعی برای مقابله با تهدیدات امنیت سایبری را در برنامه خود گنجانده‌اند و پیش‌بینی می‌شود تا سال ۲۰۲۷ سالیانه به صورت متوسط ۲۴ درصد بودجه استفاده از هوش مصنوعی در امنیت سایبری افزایش پیدا کند؛ بنابراین در سطح مدیران ارشد موضوع استفاده از هوش مصنوعی در مقابله با تهدیدات سایبری جایگاه ویژه‌ای خواهد داشت؛ البته در سمت هکرها نیز حملات پیچیده‌ای با استفاده هوش مصنوعی صورت می‌گیرد.

ارتباط فناوری‌های نوین با امنیت در شبکه بانکی

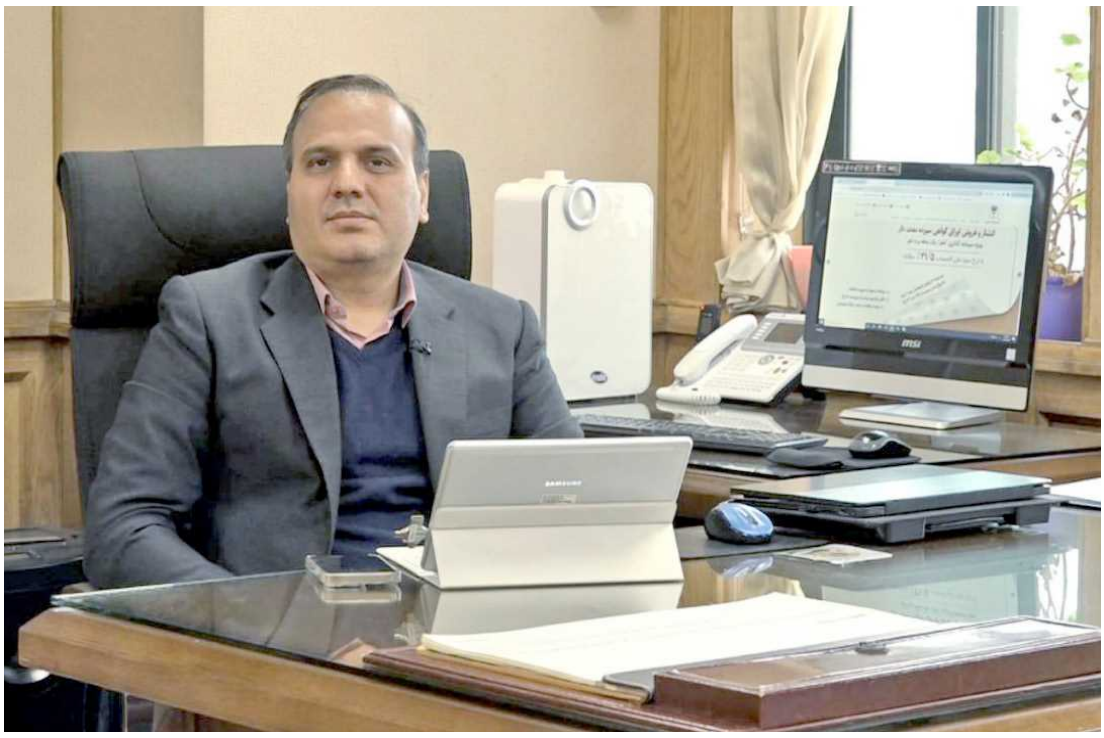
معاون فناوری اطلاعات بانک پارسیان بیان کرد: سرویس جدید یا خدمت نوینی که در سیستم بانکی ارائه می‌شود توسط اعتماد در بین مردم فراگیر می‌شود. به عنوان مثال زمانی که کارت در اوایل دهه هشتاد وارد نظام بانکی شد؛ چون هنوز مردم اعتمادی به آن نداشتند استقبال خوبی صورت نگرفت؛ البته بخشی از آن به زیرساخت و عدم فرهنگ‌سازی مربوط است؛ بنابراین مهم‌ترین شرط لازم برای استفاده از خدمات بانکی در بین مردم امنیت و اعتمادسازی است.

وی افـــزود: استفاده از خدمات نوین و تکنولوژی‌های جدید برای ارتقای سطح اعتماد در تبادلات مالی مشتریان یکی از اهداف نظام بانکی است و در همین زمینه بانک پارسیان سرویس‌های جدیدی را مورد بهره‌برداری قرار داده تا سطح امنیت تبادلات مالی مشتریان را ارتقا دهد.

پشمچی تأکید کرد: امضای دیجیتال، سفته و چک الکترونیک سرویس‌هایی بودند که بانک پارسیان به عنوان پیشرو در اختیار مشتریان قرار داد تا با این عمل ارائه خدمات به مشتریان تسهیل شود، همچنین بانک پارسیان برای آگاهی بخشی در حوزه امنیت نیز تلاش‌های زیادی در دو سطح کاربران و همکاران انجام داده است.

معاون فناوری اطلاعات بانک پارسیان اظهار داشـت: همچنین در ارتقای امنیت زیرساخت‌های نرم‌افزاری و سخت‌افزاری، پروژه‌های مختلفی اجرا شده یا در دست اجرا است به عنوان مثال پروژه SOC را اجرا کرده‌ایم و در حال تعمیم‌دادن به کل بانک‌ها هستیم، همچنین cert و به‌روزرسانی ISMS در دست اجرا است و امیدواریم بتوانیم با این اقدامات سطح امنیت بانک پارسیان را در وضعیت مطلوب برای ارائه خدمات نگه داریم.

> یکپارچه‌سازی و یکی کردن واحدهای نظارتی، مهم‌ترین کمکی است که از رگولاتور انتظار داریم، البته باتوجه به تحریم و نوسانات نرخ ارز دستیابی به تکنولوژی سخت و دارای هزینه است؛ بنابراین بانک مرکزی می‌تواند در حوزه هزینه‌ها نیز کمک کننده باشد



گفت و گو

حمیدرضا فاطمی مدیرعامل صرافی رادین در گفت‌وگو با نشریه امنیت بانکداری گفت:

پیاده‌سازی الزامات امنیت اطلاعات و بانکداری در صرافی‌ها به یک ضرورت تبدیل شده است

سامانه «جامع راهبری امنیت اطلاعات شرکت‌های صرافی» یا همان «صرافبان»، یکم شهریورماه در شرکت کاشف راه‌اندازی شد و در دسترس صرافی‌های کل کشور قرار گرفت. این سامانه که در راستای مأموریت‌های محول‌شده به کاشف به‌عنوان «اپراتور امنیت بانکی» طراحی شده است، یکی از لوازم و ضرورت‌های امن‌سازی بستر مبادلات صرافی‌های کل کشور است. پیوستن به سامانه مدیریت آسیب‌پذیری اکنون جزء الزامات امنیتی صرافی‌هاست؛ که از سوی بانک مرکزی پیگیری می‌شود. در این بین برخی صرافی‌ها در حرکتی پیشرو و ازآنجایی که لزوم امنیت را درک کرده بودند زودتر از دیگران به این جرگه پیوستند، درهمین راستا، پای تجربه یکی از این صرافی‌ها، نشستیم. با حمیدرضا فاطمی مدیرعامل صرافی رادین درباره آنچه بر صرافی‌ها رفته است و همچنین انتقادات و پیشنهادات این سازوکار بانک مرکزی گفتگو کرده ایم.

روایت شما از سال‌های گذشته جامعه صرافان در حوزه امنیت چیست؟

به سال ۱۳۹۶ برمی‌گردم که ابتدای سناریوی تغییر قیمت ارز بود، از بهمن ماه همان سال تکانه‌های افزایشی قیمت ارز را شاهد بودیم به گونه‌ای که صف‌های طولانی جلوی صرافی‌ها شکل می‌گرفت، چراکه قرار بود عرضه ارز توسط بانک مرکزی انجام شود.

پیش از این سامانه سنا وجود داشت که برخی صرافی‌ها خرید و فروش عادی ارز را در آن ثبت می‌کردند اما الزامی برآن وجود نداشت، شکل الزام‌آور آن بعد از این اتفاقات کلید خورد.

آن‌سال بعد از چند ماه که اولین دستورالعمل بانک مرکزی آمد، صرافی‌ها وضعیت معلقی داشتند و اجازه انجام هیچ عملیاتی را نداشتند. در واقع این چند ماه سکوی پرتابی شد برای اینکه بانک مرکزی وارد بحث پلتفرم کردن انجام عملیاتش با ایجاد سامانه‌ای به نام نیما شود، برای آنکه عرضه ارز و ارزهای حاصل از صادرات در یک بستر با پایه وب انجام شود.

تجربه خوبی بود شاید این تغییر به خودی خود سالها طول می‌کشید اما با این اتفاقات در یک زمان کوتاه این سازوکار پیاده شد. آنجا بود که کلمه امنیت در جامعه صرافان متولد شد.

به هرحال قرار بود یک عرضه عمومی اتفاق بیفتد و اطلاعات زیـادی در دسترس قرار می‌گرفت. همه چیز قرار بود ثبت و ضبط شود و کانالی برای خریدار و فروشنده ایجاد شود. از نظر من این همان نقطه عطفی است که ما امروز داریم درباره‌اش حرف می‌زنیم.

بعد از آن بود که صرافی‌ها توانستند از کسب‌وکار کوچک محلی خود خارج شوند و بتوانند با مشتریانی از شهرهای متفاوت کار کنند، اینگونه بازار صرافی‌ها گسترش یافت.

به نظر می‌رسد آنجا پذیرشی مبنی بر اینکه کارها به سمت دیجیتال‌شدن بروند شکل گرفت. باید توجه داشت که این اتفاقات با فشار زیاد و زمان کم رخ داد و مشخصاً نیازمند زمان بود تا به بلوغ و پختگی و راهکارهای جدید برسد.

پلتفرم نیما، بسیار مهم بود. چون در آن همه

جزییات و اطلاعات معاملات ارز کشور ثبت می‌شد واهمیت داشت که امنیت آن به خوبی تأمین شود.باید گفت که این امر یکسری تبعات هم (مثل برخی کلاهبرداری‌ها و..) به دنبال داشت که به نظرم طبیعی بود و هزینه توسعه بود. البته این موارد سریع رفع شد و دستورالعمل‌های لازم آمد و مدیریت شد.

پس از این تجربیات، امروزه واکنش جامعه صرافی‌ها به امنیت چیست و چه سازوکاری برای ایجاد امنیت خود اندیشیده‌اند؟

صرافی‌ها چون در یک پلتفرم دیگری تعامل را انجام می‌دادند، ذهنیتی درباره این موضوع نداشتند که آسیب‌پذیری‌ها چگونه می‌تواند به شبکه آنها رسوخ کند و اطلاعات آنها مورد سوءاستفاده قرار گیرد، و نسبت به این موضوع دانشی نیز نداشتند و امروزه فقط چند صرافی در تهران با مکانیزم فناوری بخش آی‌تی کار می‌کنند این وضعیت در شهرستان‌ها وخیم‌تر است.

چرا صرافی‌ها با اجرای الزامات امنیتی بانک مرکزی چالش دارند؟

چون می‌پندارند که این الزامات هزینه است در حالی‌که این اتفاق هزینه‌کرد نیست و برای ایجاد بستر امن انتقال اطلاعات ضروری است. ما خیلی از هزینه‌ها را پرداخت می‌کنیم اما به عنوان هزینه نمی‌بینیم. مثلاً پرداخت بیمه خودرو برای زمان تصادفات پیش نیامده، این هزینه این اطمینان را به ما می‌دهد که اگر اتفاقی رخ داد، راه برون‌رفتی داشته باشیم. این پذیرفته شده است و به عنوان یک سرمایه‌گذاری درنظرگرفته می‌شود، اما در مورد هزینه برای امنیت در جامعه صرافی‌ها این فحوا و منطق به تازگی و به علت اجبار در حال شکل‌گیری است؛ اگر کاشف این اقدام را شروع نمی‌کرد صرافی‌ها تا چند سال آینده هم به این سمت حرکت نمی‌کردند.

آیا طی سال‌های اخیر حمله سایبری جدی در جامعه صرافی‌ها وجود نداشته که به اندازه کافی برای اقدام جهت امنیت، اقناع کننده باشد؟

من تجربه خودم را می‌گویم، که به دیگر صرافی‌ها هم تسری پیدا می‌کند. سال ۹۹ در سه بخش به ما حمله سایبری شد که شناسایی و به پلیس فتا ارجاع شد. در این حمله بسیار تلاش شده بود تا ورود پیدا کنند و شاید اگر کمی تعلل می‌کردیم و زیرساختی نمی‌داشتیم، اطلاعات ما لو می‌رفت. این تجربه باعث شد ما بخواهیم به آزمایشگاه مراجعه کنیم تا بتوانیم جلوی اتفاقات بعدی را بگیریم. همین یک مورد کافی است برای اینکه عزم‌مان را برای امنیت صرافی جذب کنیم.

> خیلی صریح بگویم در صرافی کارها همزمان و در حضور مشتری انجام می‌شود و اگر شبکه و سرورهای ما دایم آماده نباشد اطلاعات شخصی-هویتی مشتریان‌مان که ارزشمندترین دارایی ماست مورد سوءاستفاده قرار می‌گیرد

خیلی صریح بگویم در صرافی کارها همزمان و در حضور مشتری انجام می‌شود و اگر شبکه و سرورهای ما دایم آماده نباشد، اطلاعات شخصی-هویتی مشتریان‌مان که ارزشمندترین دارایی ماست مورد سوءاستفاده قرار می‌گیرد. آنجاست که باید سیستم خود را از دسترس خارج کرده و به مشتری پاسخگو نباشیم و این صدمه جبران‌ناپذیری بر برند و اعتبار و اعتماد به شما خواهد زد. به‌هرحال در مجموعه ما همه اتفاقات برخط است و مدیریت پشتیبانی خدمات به صورت دیجیتال انجام می‌شود، پس از این لحاظ برای ما امنیت اولویت دارد.

شما به اهمیت اطلاعات شخصی-هویتی اشاره کردید، رادین برای امن نگه‌داشتن این اطلاعات چه کرده است و از کجا اطمینان پیدا می‌کند که مسیرش درست و امن است؟

سال ۹۹ بود که ما با چند شرکت حوزه امنیت مذاکره کردیم. واکنش چنین شرکت‌هایی جالب بود، آنها در واقع خواسته ما را کوچک می‌شمردند و اهمیت موضوع حتی برای چنین شرکت‌هایی روشن نبود. اینکه یک صرافی به دنبال آزمایشگاه تست نفوذ و مشاوره امنیت است برای آنها تعریف نشده بود. اما ما به دنبال بهبود و توسعه و ایجاد اطمینان از روش‌های امنیتی خود بودیم و هستیم. اما در آن‌سو این مهم تعریف نشده است یا عددهای انجام این کار را در مقیاس‌های بزرگ و غیرقابل پرداخت بیان می‌کنند که کار را دشوار می‌کند.

درنهایت در حد و توان خود یکسری راهکار را پیاده‌سازی کرده‌ایم. در واقع تا قبل از اینکه اتفاقی بیفتد ما کار را پیش می‌بریم اما نکته اینجاست که آن متخصصی که از بیرون ما را می‌بیند می‌تواند آسیب‌های جدی را تشخیص دهد. تا قبل از اینکه سامانه آسیب‌پذیری‌های جدی بیابد اگر خطری هم رخ مـی‌داد ما متوجه‌اش نمی‌شدیم. کاری نمی‌توانستیم بکنیم لذا ورود کاشف در حل این دست مسائل کمک بزرگی کرد. واقعیت این است که ما خیلی جلوتر از آمدن این دستورالعمل احساس نیاز کرده بودیم و زمانیکه این الزام آمد خوشحال شدیم. چون کار را برای ما راحت‌تر می‌کرد.

اشکالاتی که متوجه الزامات امنیتی بانک مرکزی برای صرافی‌ها می‌دانید چیست؟

ما انتظار داریم نیازهای واقعی یک صرافی جهانی را درک کنند و بر اساس آن برنامه‌ریزی کنند و یک حرکت روبه‌جلو باشد به طور خلاصه بگویم؛ منتظر چشم‌اندازهایی با حضور قوی فین‌تک هستیم.

صرافی‌ها نیاز دارند که به دنیای بیرون دسترسی داشته باشند و بالا بردن دیوارها و محدودکردن می‌تواند قسمتی از ایجاد امنیت باشد و نه همه آن. الزامات باید منعطف و براساس نیازهای صرافی‌ها طراحی شود. یکی از اشکالاتی که امیدواریم در پروتکل‌های آتی اصلاح شود این است که انتقال اطلاعات از طریق فلش و از طریق سیستم دیگر حذف شود. چون این روند از نظر ما ایجاد خطر می‌کند.

مسأله بعدی این است که ما دوتا مانیتور و دوتا شبکه روی میزهایمان داریم، یکی شبکه امن است و دیگری شبکه اختصاصی خودمان که به اینترنت آزاد وصل است و هرکاری که می‌کنیم باید دوبار انجام شود.

چنین پروسه‌ای نیازمند چندبار چک کردن است پس درصد خطا را بالا می‌برد و هزینه مالی و زمانی و استهلاک ایجاد می‌کند. همچنین شاهد هستیم خود بانک مرکزی برای دسترسی داشتن به یکسری اطلاعات نیازمند اینترنت است (هرچند اینترنت داخلی) تا بتوانند به طور «برخط » خروجی داشته باشند. مسأله دیگر این است که برای ثبت اجماع تراز روزانه صرافی‌ها و ارسال به بانک مرکزی باید یک کارمند را موظف کنیم تا به صورت دستی این لیست را وارد کند.

در حالی‌که می‌توانیم با یک خروجی از پلتفرم خودمان این آمار را دقیق ارائه دهیم!

ما به نوعی مجازهستیم پنج شعبه داشته باشیم برای اینکه این شعب کار کنند نیازمند یک سیستم متمرکز و شبکه است از سوی دیگر این اجازه را ندارم بر روی دیتاسنتر بروم یا بر روی cloud کارم را توسعه دهم. به عبارتی از طریق این الزامات، دست‌هایتان برای توسعه بسته است.

با همه این توضیحات من به بلوغ این روش فکر می‌کنم؛ چون مطمئن هستم این ابتدای مسیر است و دوستان در کاشف باید صبور باشند چون تغییرات طی زمان رخ می‌دهد و درعین حال حجم تغییرات خیلی سریع است و نیازمند بالا رفتن سطح آگاهی در جامعه صرافی‌ها هستیم.

.

شما در ارتباط مستقیم با مشتریان‌تان شاهد تقاضاهایی از جنس امنیت هستید؟

بله مردم درخواست و توقعات بسیار بالاتری از آنچه موجود است دارند. زمانیکه اعتماد مشتری خدشه‌دار شود، بلافاصله اعتراض می‌کند. مشتریان شاهد ارائه خدمات متنوعی در صرافی‌های دنیا هستند پس به حقوق و گستره خدمات آشنایی دارند. این را براساس تحقیق می‌گویم.

درسایت صرافی رادین بخشی گذاشته بودیم که ایده مشتریان را دریافت کنیم. شما با مطالعه این ایده‌ها متوجه می‌شدید توقعات و آگاهی مشتریان تا کجاست. اما از آن طرف با صرافی‌هایی مواجه‌ایم که حتی برای سهولت امور حاضر نیستند یک نرم‌افزار ساده اداری بخرند، و اصولاً به توقعات مشتری وقعی نمی‌نهند.

الزامات امنیتی بانک مرکزی را دارای چه امتیازهایی می‌بینید؟

الزامات امنیتی کاشف سبب شد تا جامعه صرافی‌ها از بی‌نظمی خارج شود. مقوله اطلاعات برای صرافی‌ها ارزشمند شد و وارد دنیای دیگری شدند.

هرچند این الزامات حاکمیتی و بالادستی است اما ما را وادار به حرکت روبه‌جلو کرده و مجبور می‌کند نسبت به دارایی‌هایی که دارند وسواس بیشتری داشته باشند.

همچنین عملکرد کاشف منجر به تزریق دانش، خرد و آگاهی در این صنف شد و ریل‌گذاری‌هایی انجام داد تا در مسیر رسیدن به استانداردهای دنیا قرار بگیریم.

همایش‌های ماهانه شرکت کاشف را دارای چه تأثیراتی می‌دانید و آیا از برگزاری آنها رضایت دارید؟

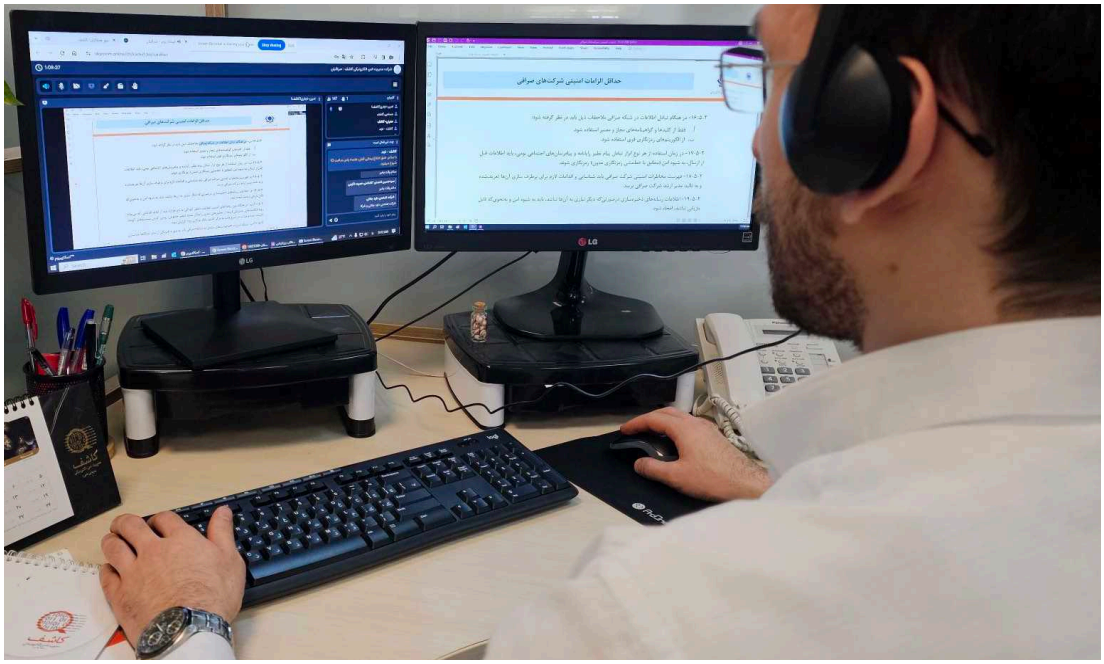
همایش‌های کاشف دارای تأثیرات مثبتی است با این حال انتظار داریم که همایش‌ها به صورت سطح‌بندی شده برگزار شود تا آن کسی که از سطح مقدماتی عبور کرده هم بتواند استفاده کند. درعین حال امیدواریم مستمر و با یک سناریوی تعریف شده ادامه داشته باشد.

تیم این پروژه علی‌رغم تجربه جدیدی که در این خصوص درحال رخ دادن است دارای افرادی پویا، پیگیر، باانگیزه و باسوادی هستند که از همکاری با آنها لذت بردم.

همایش ششم پروژه امن سازی صرافی ها برگزار شد

ششمین همایش آگاهی‌رسانی و آموزشی در راستای پیاده‌سازی الزامات امنیتی صرافی‌ها روز چهارشنبه تاریخ ۱۴۰۲/۱۲/۰۹ برگزار شد. طی ماه‌های اخیر شش همایش آنلاین با حضور تعداد قابل توجهی از صرافی‌های سراسر کشور برگزار شد، در این همایش‌ها متخصصین کاشف به آموزش الزامات امنیتی پرداخته و گام‌های اجرایی پروژه امن‌سازی را تبیین کردند. همچنین طریقه تکمیل چک لیست خود اظهاری انطباق با الزامات توضیح داده شد و سامانه صرافیان و طریقه کاربری آن شرح داده شد. در هر همایش به پرسش‌های فنی و مشکلات مطرح شده از سوی صرافی‌ها پاسخ داده شد.

شایان ذکر است همایش‌ها تا زمان آموزش کامل سند، حداقل الزامات امنیتی صرافی‌ها به‌صورت عمومی برای تمام صرافی‌ها برگزار می‌شود، پس از آن برای صرافی‌هایی که در مراحل اولیه پیاده‌سازی الزامات هستند، همایش‌های عمومی ادامه پیدا می‌کند و برای صرافی‌هایی که در پیاده‌سازی الزامات پیشرو هستند، همایش‌های تخصصی برگزار خواهد شد.



گفت و گو

در گفت‌وگو با تیم «پروژه امنیت صرافی‌های کاشف» مورد بررسی قرار گرفت؛

ممیزی و انطباق‌سنجی امنیت صرافی‌ها

حدود ۷۰۰ صرافی در کشور وجود دارد که معاملات ارزی کشور را انجام می‌دهند با این حال تا چندی پیش سازوکار یکپارچه‌ای برای نظارت بر زیرساخت و شبکه‌های آنها وجود نداشت، تا اینکه بانک مرکزی به دنبال پیاده‌سازی الزاماتی جهت بهبود وضعیت امنیت صرافی‌های کشور برآمد. با این حال طی تمام این سالها صرافی‌ها وارد دنیای دیجیتال شدند و حتی به مدد متخصصان آی‌تی توانستند شبکه‌های زیرساخت را در صرافی خود برپا کنند؛ اما مقوله امنیت، مسأله متفاوتی از اقدامات فناورانه و شبکه را دنبال می‌کند که گاهی اشتباه درک شده و یکسان پنداشته می‌شود. کاشف به عنوان بازوی امنیتی بانک مرکزی ۳۰ مرداد ۱۴۰۲، اولین نشست با صرافی‌ها را با عنوان «راهبری امنیت اطلاعات در شرکت‌های صرافی»، برگزار کرد و تاکنون شش همایش به منظور پاسخگویی و روشن‌سازی فرآیند «امن‌سازی صرافی‌ها» برگزار کرده است، همچنین تمام مراحل گام به گام برای پیوستن به این پروتکل، در سامانه‌ای به نام صرافیان به طور کامل توضیح داده شد. در این پرونده مناسب دیدیم با اعضای تیم «پروژه امنیت صرافی‌ها» واحد نظارت کاشف که به عبارتی همان گروه نظارت پروژه‌های بانکی به ریاست ابراهیم نجد است، مصاحبه‌ای گروهی انجام دهیم و از آنها بخواهیم به چالش برانگیزترین سؤالات این حوزه پاسخ دهند

خیلی‌ها می‌پرسند آیا پیاده‌سازی الزامات امنیتی بانک مرکزی برای تمام صرافی‌ها لازم‌الاجرا است؟

نجد: بله، دامنه کاربرد سند حاضر، تمامی شرکت‌های صرافی اعم از سهامی خاص (بانکی) و تضامنی دارای مجوز معتبر از بانک مرکزی ج.ا.ا است.

بر اساس تحقیقی که کرده‌ام از شما زیاد پرسیده می‌شود که آدرس سامانه صرافیان چیست؟ و از چه طریق امکان دسترسی به سامانه وجود دارد؟

حسن شکری‌پور: بله، سؤال متداولی است، امکان دسترسی به سامانه صرافیان تنها از طریق نورنتا برقرار است. آدرس سامانه صرافیان sarafsec.kashef.ir است و جهت مشاهده سامانه صرافیان از طریق نورنتا، ابتدا باید تنظیمات DNS شبکه نورنتا را مطابق «سند راهنما» - آمده در سامانه صرافیان- تغییر بدهند.

در صورتی که مدیرعامل صرافی تغییر کرده باشد آیا امکان ثبت نام وجود دارد؟

اتحاد: خیر، به‌منظور ثبت‌نام، ابتدا اطلاعات مدیرعامل جدید صرافی را از طریق ایمیل، به آدرس sarafsec@kashef.ir ارسال فرمایند.

امکان بازیابی رمزعبور در صورت فراموشی رمز یا حذف پیامک اولیه وجود دارد؟

اتحاد: بله، یک ایمیل با موضوع درخواست «بازیابی رمز عبور» به آدرس ایمیل sarafsec@kashef.ir ارسال بفرمایند.

چه اطلاعاتی باید برای استعلام حراستی مدیران فناوری اطلاعات ارسال شود؟

شکری‌پور: نام، نام‌خانوادگی، شماره موبایل و کد ملی مدیر فناوری اطلاعات (مسئول IT) صرافی خود را در یک نامه رسمی ثبت بفرمایید. سپس نامه مهر و امضاء شده به‌علاوه کپی پشت و روی کارت ملی و کپی تمامی صفحات شناسنامه مدیر فناوری اطلاعات (مسئول IT) را به‌صورت

فیزیکی به کاشف ارسال بفرمایید.

گاهی پس از ثبت‌نام این پیغام دیده می‌شود که «کاربر صرافی غیرفعال می‌باشد» در چنین مواقعی چه باید کرد؟

مسلمی: به منظور فعالسازی، ضروری است مدیر صرافی، پس از ثبت‌نام با شماره تلفن ۷۲۸۶۱۴۳۵ تماس بگیرد تا راهنمایی لازم انجام شود.

آقای نجاری شما به عنوان مدیر پروژه «امنیت صرافی‌ها» حتما درباره ویژگی‌های thin client نظرات را شنیده‌اید، توضیحی در این خصوص دارید؟

نجاری: خب deviceهای قوی‌تر و بزرگتر و البته گرانتری وجود دارد که قابلیت‌های بسیار بیشتری دارند؛ اما ما در این مرحله از کار، یک device متوسط‌الحال را انتخاب کردیم که به کسی فشار نیاید.(می‌خندد) با این حال در حال آزمودن برخی روش‌ها برای ارتقای عملکرد این device هستیم.

بسیاری می‌پرسند که چرا باید چک لیست خوداظهاری الزامات را تکمیل کنند؟

مسلمی: پس از اتمام زمان تکمیل چک لیست خوداظهاری الزامات توسط صرافی‌ها، مجموع نتایج توسط کاشف به بانک مرکزی ج.ا.ا ارائه خواهد شد. لازم به ذکر است این پاسخ‌ها در جهت سنجش وضعیت فعلی امنیت صرافی‌های کشور توسط بانک مرکزی است. کسی نمی‌تواند این مسأله را انکار کند که این مسیر موجب امن‌شدن بیشتر و نظارت راحت‌تر بانک مرکزی می‌شود و احتمال رخ دادن مخاطرات سایبری را کم می‌کند.

بچندتا اصطلاح در سند ارائه شده از سوی بانک مرکزی دیده می‌شود که بد نیست توضیحی درباره آن بدهید: مثلاً منظور از «مدیریت امنیت اطلاعات فعال» چیست؟

معینی: مدیریت امنیت اطلاعات فعال به استراتژی و فرآیندهایی اشاره دارد که به منظور پیشگیری از تهدیدات امنیتی و مدیریت مؤثر ریسک‌های امنیتی در یک سازمان اجرا می‌شود. این رویکرد نه تنها از وقوع حوادث امنیتی جلوگیری می‌کند بلکه در صورت وقوع، از اثرات ناخواسته آنها کاسته و به سازمان این امکان را می‌دهد تا

به سرعت به وضعیت عادی بازگردد.

و «موجودیت‌های متصل به شبکه صرافی» یعنی چی؟

معینی: تمامی دارایی‌هایی که به شبکه صرافی متصل شده‌اند. این دارایی‌ها شامل ایستگاه‌های کاری، سرورها (نظیر سرور سیستم حسابداری، سرور اتوماسیون اداری، سرور دامین، فایل سرور و سایر سرورهای داخلی صرافی)، دوربین‌های نظارتی و تجهیزات مرتبط با آن، تجهیزات شبکه، برنامه‌های کاربردی و تجهیزات ذخیره‌ساز است.

آیا امکان برگزاری همایش‌ها به صورت سطح بندی شده وجود دارد؟

مسلمی: فعلاً خیر چون ما در مرحله آموزش هستیم و مرحله عمومی را طی می‌کنیم. ما موظفیم به حداقل اطمینان از این مسأله برسیم که تمام الزامات به درستی فهمیده شده است و بعد درباره ابزارها صحبت می‌کنیم و همچنین بند به بند الزامات را بازخوانی می‌کنیم و توضیح می‌دهیم. لذا بهتر است در این مرحله همه با هر سطحی از امنیت حضور داشته باشند، چون می‌تواند برای هرکسی با هر سطحی سؤالاتی ایجاد کند.

برخی می‌گویند ما اقداماتی انجام داده‌ایم و نیازی به ارائه این الزامات نداریم، جواب شما چیست؟

نجاری: این فرآیند دلبخواهی نیست، یک الزام حاکمیتی است و البته ما یعنی کاشف اصراری هم نداریم که حتماً بیایید و این کار را بکنید. اگر از امنیت خودتان مطمئن هستید، ما می‌آییم و ممیزی را انجام می‌دهیم و به بانک مرکزی گزارش می‌دهیم، اگر نتیجه مثبت بود که چه عالی، به هر حال، ما فقط موظف به بررسی و گزارش‌دهی هستیم. ممیزی و انطباق‌سنجی صورت گرفته از سوی کاشف نهایتا وضعیت صرافی‌ها را تحت تاثیر قرار خواهد داد.

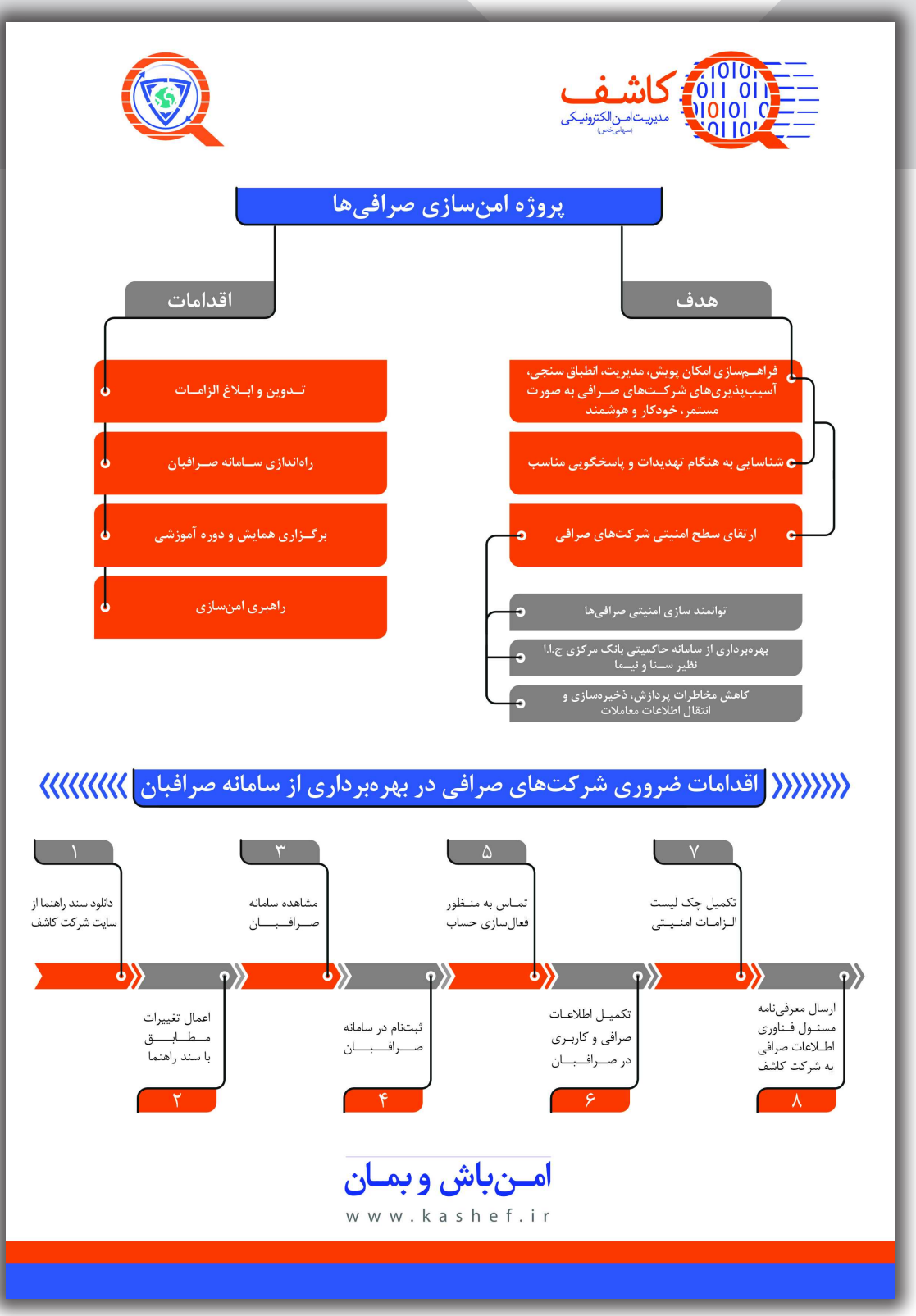
اینکه جهت استفاده از این سامانه نیازمند قطع اینترنت هستند یک چالش است و این ادعا وجود دارد که می‌تواند خطر بیشتری را به لحاظ جابه‌جا کردن اطلاعات توسط فلش ایجاد کند، یا یکسری فرآیندها دوباره کاری شود؟ پاسخ شما چیست؟

نجاری: متوجه نیازهای صرافی‌ها هستیم که می‌خواهند به اینترنت آزاد دسترسی داشته باشند برای گسترش کسب‌وکار، گاهی به خاطر حفظ امنیت و بقای کسب‌وکار ناچار به اعمال روش‌هایی هستیم که برای سادگی و توسعه کار چالش ایجاد می‌کنند، از طرفی جابه‌جا کردن اطلاعات از طریق فلش تنها راهکار موجود نیست، در نهایت کاشف و بانک مرکزی همچنان درحال بررسی این مسأله هستند.

بزرگترین چالش شما از شروع پروژه چه بوده است؟

با توجه به اینکه قبل از این پروژه، اقدام جدی بر روی امنیت صرافی‌ها انجام نشده بود ابهامات زیادی از سمت صرافی‌ها وجود داشت. این ابهامات به دلیل نگرانی‌های در ارتباط با سخت شدن فرایند کسب‌وکاری صرافی‌ها و شاید هزینه‌های این اقدامات بود. اما با گذشت زمان و آگاهی‌رسانی‌های کاشف، این مقاومت کاهش پیدا کرد و تبدیل به همکاری جهت یافتن راهکارهای جدید شد.

اینفوگرافی: پروژه امن‌سازی صرافی‌ها



یادداشت

امضای دیجیتال و احراز هویت

شاهین نوروزی
■ مدیرعامل شرکت پندار کوشک ایمن

امروز فناوری اطلاعات بسیار در دسترس، آسان و به تبع آن فراگیر شده است. اکثر افراد به‌راحتی در تلفن همراه خود می‌توانند از امکان فناوری اطلاعات استفاده کنند و اکثرا با کارکردها و روش کار آن آشنا هستند. این امر باعث شده کسب‌وکارها و صنایع مختلف، خدمات خود را در بستر فناوری اطلاعات ارائه کنند و به این ترتیب هم تعداد مشتریان خود را افزایش دهند، هم گستره جغرافیای توزیع خدمات خود را توسعه دهند و هم هزینه‌های خود را بصورت قابل توجهی کاهش دهند. با توسعه خدمات در بستر فناوری اطلاعات، موضوعات احراز هویت، انکارناپذیری و استنادپذیری اسناد و عملیات الکترونیک و محرمانگی اطلاعات مطرح و اهمیت آن بیش از پیش روشن شد و کسب‌وکارهای مختلف و به‌خصوص دولتها برای حل آن اقدام به تدوین دستورالعمل و قوانین کردند. اصلی‌ترین چیزی که باید بدانیم؛ تفاوت بین سه مفهوم احراز هویت، انکارناپذیری و استنادپذیری اسناد و عملیات الکترونیک و محرمانگی اطلاعات و کارکردهای هریک و ابزار تأمین آن است. در ادامه به توضیح هریک پرداخته شده است.

احراز هویت چیست؟

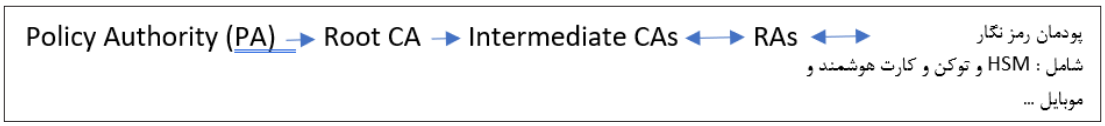
احراز هویت؛ شناسایی یک فرد و تصدیق هویت وی است. از انـواع روش‌هـای احراز هویت، می‌توان به کلمه و رمز عبور، رمز یکبار مصرف یا اثرانگشت یا تصویر چهره و... را نام برد که هرکدام کاربرد و قدرت و قابلیت اطمینان متفاوتی دارند. قوی‌ترین نوع احراز هویت مبتنی بر خواص بیومتریک است. مثل اثر انگشت و تصویر چهره که براساس اطلاعات پایه که معمولا توسط حاکمیت تهیه و جمع آوری شده است صورت می پذیرد. طبیعی است اطلاعات جمع آوری شده توسط حاکمیت به عنوان مثال برای شهروندان اطلاعات هویتی هر فرد در ثبت احوال کشور مبتنی بر نظام قابل قبول انجام شده و قابل اعتماد است. در دنیای فناوری اطلاعات برای احراز هویت از اطلاعات پایه حاکمیتی و هوش مصنوعی استفاده می‌شود. با ترکیب آنها، اثبات حضور یک فرد و هویت وی تصدیق می‌شود؛ اما بدیهی است اثبات حضور به معنای انجام یک عمل نیست و برای اثبات انجام یک عمل توسط یک فرد نیاز به ادله بیشتری است. در واقع احراز هویت دقیق و قابل اعتماد یک فرد به معنای استنادپذیری یا انکارپذیری یا محرمانگی عملیات و اطلاعات نیست و فقط حضور فرد را ثابت می‌کند.

انکار ناپذیری و استنادپذیری اسناد و عملیات الکترونیک چیست؟

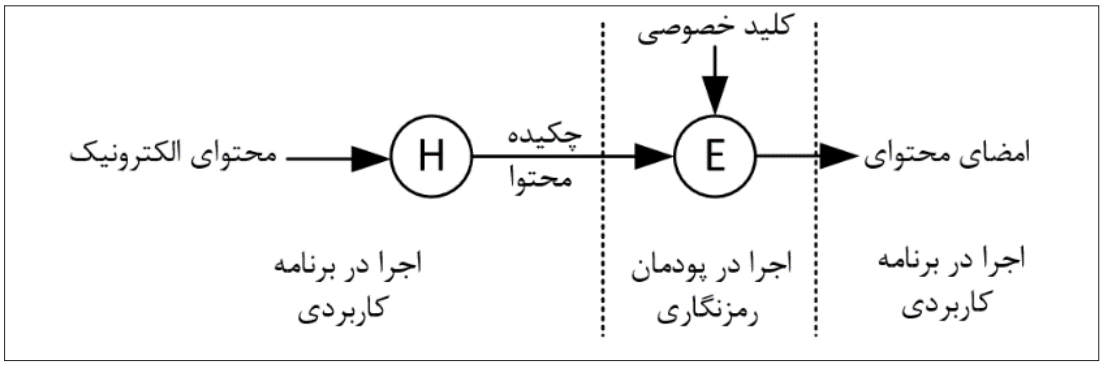
چناچه یک سند یا عمل در دنیای الکترونیک به گونه‌ای ثبت و ذخیره شده باشد که در هر زمان به‌توان هویت انجام‌دهنده آن را تشخیص داد و اثبات کرد عمل به اراده وی انجام شده و زمان انجام دقیق عمل را مشخص و ثابت کرد اطلاعات از زمان تولید تاکنون تغییر نکرده است، در نتیجه انجام‌دهنده عمل نمی‌تواند فعل خود را منکر شود و به اصطلاح این سند یا عمل استنادپذیر است. پایه‌های استنادپذیری، قوانین حاکم بر کشورها است و در کشور ما نیز پایه‌های این امر، قانون تجارت الکترونیک مصوب ۱۳۸۲ و قانون دادرسی الکترونیک مصوب ۱۳۹۳ و آیین‌نامه‌های مرتبط با این قوانین است.

سؤال اصلی این است که با چه ابزاری در دنیای فناوری اطلاعات می‌توان انکارناپذیری و استنادپذیری اسناد و عملیات الکترونیک

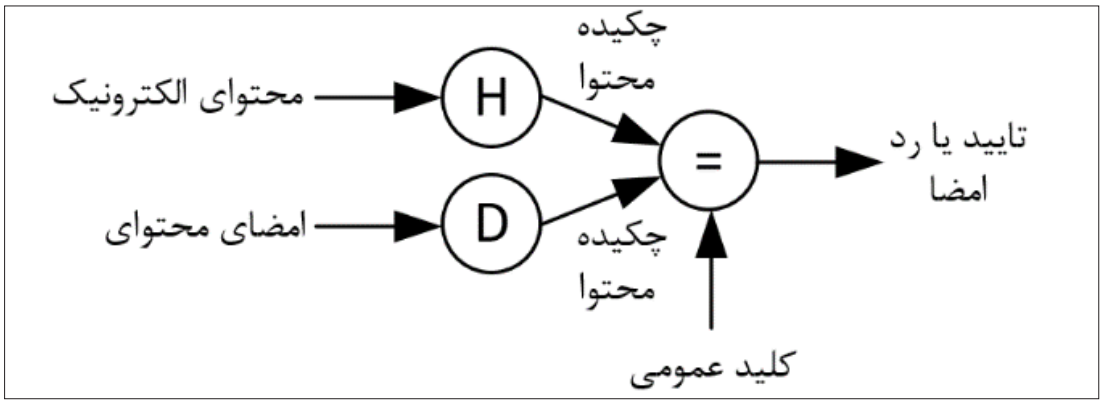
> پایه‌های استنادپذیری قوانین حاکم بر کشورها است و در کشور ما نیز پایه‌های این امر قانون تجارت الکترونیک مصوب ۱۳۸۲ و قانون دادرسی الکترونیک مصوب ۱۳۹۳ و آیین‌نامه‌های مرتبط با این قوانین می‌باشد



شکل ۱: پودمان رمزنگار



شکل ۲: فرآیند امضای دیجیتال



شکل ۳: فرآیند تصدیق امضا

را فراهم آورد. یکی از بهترین ابزار، امضای دیجیتال است. به کمک امضای دیجیتال می‌توان به راحتی هویت انجام‌دهنده عمل و زمان آن را مشخص کرد و در صورت رعایت قوانین مرکز دولتی ریشه در زمان اعطای گواهی و استفاده از آن، اعمال اراده آن قابل اثبات است و از همه مهمتر تغییر یا عدم تغییر اطلاعات قابل تشخیص خواهد بود. در واقع ثبت امضای دیجیتال برروی یک محتوا (از جنس سند یا عملیات) انکارناپذیری و استنادپذیری را به همراه خواهد داشت.

اما امضای دیجیتال چگونه این قابلیت را فراهم می‌کند؟ برای پاسخ این سؤال باید نحوه کارکرد و عناصر لازم برای امضای دیجیتال را دقیق بشناسیم.

چگونه قابلیت امضای الکترونیک مطمئن برای یک فرد فراهم می‌شود؟

هر فرد برای اینکه بتواند امضای الکترونیک انجام دهد نیاز به داشتن گواهی الکترونیک دارد. گواهی الکترونیک طبق قوانین کشور در یک نظام اعتبارسنجی و اعتبار بخش تولید می‌شود. این نظام در شکل ۱ ارائه شده است.

PA یا Policy Authority، مرجع قانونگذاری این حوزه است که در کشور ما تحت عنوان شورای سیاستگذاری زیرساخت کلید عمومی شناخته می‌شود و بر اساس قانون تجارت الکترونیک شکل گرفته و دبیرخانه آن مرکز توسعه تجارت الکترونیکی ایران است و مسئولیت تصویب قوانین این حوزه و اعتبار بخشی به مرکز ریشه و مراکز میانی را دارد.

RCA یا مرکز دولتی ریشه، مرجع صدور گواهی برای مراکز میانی و تهیه و تدوین‌کننده اسناد و قوانین حوزه زیرساخت کلید عمومی و بازوی اجرایی PA جهت ارزیابی، تأیید و رد عملکرد مراکز میانی است.

ICA (Intermediate Certificate Authority) مرکز میانی صدور گواهی الکترونیک؛ در واقع مراکزی هستند که مسئولیت صدور گواهی الکترونیک برای اشخاص را به عهده دارند و به متقاضیان انواع گواهی، سرویس می‌دهند. این مراکز جهت ثبت نام و احراز هویت متقاضیان از دفاتر ثبت نام (RA) استفاده می‌کنند.

(Registration Authority) مرجع ثبت نام و احراز هویت متقاضی گواهی و تأییدکننده صلاحیت اخذ گواهی برای متقاضی گواهی است. مراکز ثبت نام موظفند برای احراز هویت از مکانیزم‌های مورد تأیید بر اساس اطلاعات پایه حاکمیتی مثل کارت ملی برای احراز هویت حضوری و سرویس‌های مختلف موجود در کشور مثل سرویس‌های ثبت احوال، کد پستی، شاهکار، ثنا و غیره... برای احراز هویت غیر حضوری استفاده کنند.

در این نظام یک متقاضی گواهی الکترونیک یک زوج کلید منحصر به فرد در پودمان رمز نگاری (Cryptography module) خود تولید کرده و فقط کلید عمومی خود را در اختیار مرجع ثبت نام قرار می‌دهد. نقطه

قوت این نظام در همین نکته است که کلید خصوصی فقط در اختیار متقاضی گواهی است و به هیچ عنوان در این نظام، غیر از متقاضی گواهی هیچ عنصر دیگری برای اعتبارسنجی و اعتباربخشی به کلید خصوصی نیاز ندارد. مرجع ثبت نام، اطلاعات هویتی متقاضی را بررسی (به صورت حضوری یا غیرحضوری مطابق با قوانین) و در صورت صحت اطلاعات و تأیید صلاحیت، متقاضی جهت اخذ گواهی، اطلاعات هویتی و کلید عمومی را به مرکز صدور گواهی می‌دهد. مرکز صدور گواهی پس از اعتبارسنجی اطلاعات، یک گواهی حاوی اطلاعات هویتی مطابق پروفایل‌های کشوری و کلید عمومی و تاریخ اعتبار و یکسری اطلاعات دیگر مطابق استاندارد X۵۰۹ آن را در اختیار مرکز ثبت نام قرار داده و مرکز ثبت نام این گواهی را به متقاضی گواهی می‌دهد. در این لحظه متقاضی گواهی دارای یک گواهی الکترونیک بوده و از این پس می‌تواند از طریق این گواهی و کلید خصوصی خود هر محتوای الکترونیک را امضا کند.

همانگونه که در نظام صدور گواهی الکترونیک مشخص شد؛ امنیت گواهی الکترونیک به نحوه تولید و نگهداری کلید خصوصی است که برای آن توسط مرکز دولتی ریشه، قوانین و دستورالعمل‌های مشخصی وجود دارد و صادرکننده گواهی هیچ نقشی در امنیت کلید ندارد و فقط مسئولیت اعتبارسنجی متقاضی و اعتبار بخشی به گواهی تولید شده را دارد.

این مدل اعتماد بسیار کارکردی بوده و باعث می‌شود حتی در نظام جهانی نیز مستقل از صادرکننده گواهی بتوان به امضای یک شخص اعتماد کرد. بدیهی است هرکسی باید در هر اکوسیستم از گواهی مورد اعتماد از آن اکوسیستم استفاده کند به عنوان مثال در کشور ما گواهی که زنجیره آن که به مرکز دولتی ریشه ختم می‌گردد و در این زنجیره قابلیت اعتبارسنجی است می‌تواند در اکوسیستم خدمات الکترونیک کشور و نظام حقوقی کشور کار کند، به این ترتیب برای امضای اسناد بانکی یا بیمه یا سلامت نیاز به تأسیس مرکز میانی خاص در هر حوزه نیست؛ بلکه از هر مرکز میانی در زنجیره اعتماد کشور می‌توان در تمام حوزه‌های بانکی، بیمه، سلامت، بورس و ... استفاده کرد؛ آنچه مهم است کاربرد گواهی است نه مرکز صدور آن، این امر موجب پویایی و توسعه‌پذیری و از همه مهمتر باعث حضور مؤثر بخش خصوصی در نظام اعتبار بخشی الکترونیکی می‌شود و این روشی است که در تمام دنیا تجربه شده و دولتها تلاش کردند به منظور سهولت و رونق این حوزه PA, RCA را حاکمیتی و سایر عناصر را در بخش خصوصی توسعه دهند. این مدل مشابه دفاتر اسناد رسمی به عنوان بخش خصوصی در نظام اعتبارسنجی و اعتباربخشی اسناد کاغذی است.

> از آنجا که جهت امضای یک محتوای الکترونیک فقط چکیده آن، به پودمان منتقل می‌شود محرمانگی اطلاعات نیز در این نظام تضمین می‌شود نکته قابل توجه و قدرت امضای دیجیتال این است که برای اعتبارسنجی امضا فقط به کلید عمومی نیاز است در نتیجه اولا همه می‌توانند در اکو سیستم خدمات الکترونیک یک محتوای امضا شده را تصدیق یا رد کنند و برای این امر نیاز به حضور امضا کننده نمی‌باشد

امضای الکترونیک چیست و چگونه انکارناپذیری و استناد را فراهم می کند؟

همانطور که بیان شد یک فرد برای اینکه بتواند یک محتوای الکترونیک را امضا کند، باید گواهی الکترونیکی در زنجیره اعتماد مورد قبول حاکمیت یعنی زنجیره اعتماد منتهی به مرکز دولتی ریشه داشته باشد. به این ترتیب فرد دارای گواهی می‌تواند در طول مدت اعتبار گواهی هر چند بار که لازم باشد اسناد الکترونیک را امضا کند. امضای الکترونیک یک عملیات رمزنگاری برروی چکیده یک محتوای الکترونیک است که در شکل ۲ آورده شده.

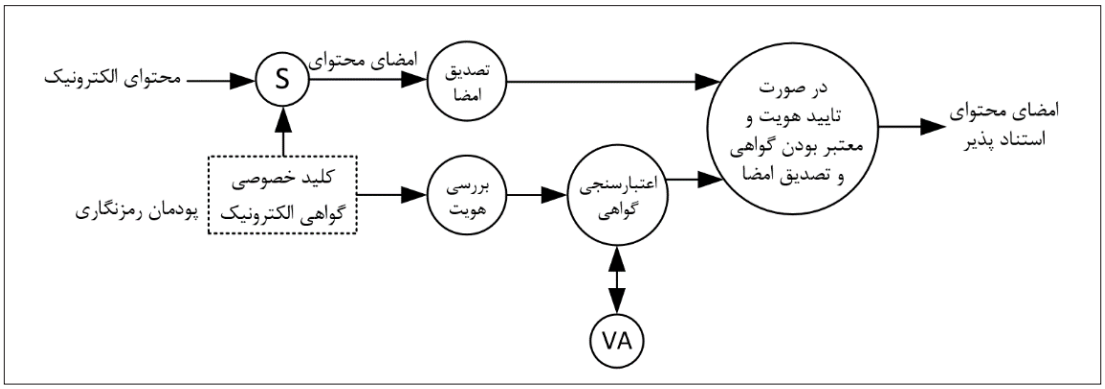
فرآیند امضای دیجیتال

همانگونه که مشخص است در فرآیند امضا، کلید خصوصی جهت رمزنگاری چکیده اطلاعات استفاده می‌شود. از آنجا که کلید خصوصی در نظام تولید گواهی فقط در اختیار صاحب گواهی است و به هیچ عنوان در صورت رعایت قوانین مرکز دولتی ریشه و استفاده از پودمان رمزنگاری مورد تأیید این مرکز در اختیار غیر قرارنمی‌گیرد و دسترسی به آن حداقل به صورت دو عامل یعنی داشتن پودمان و دانستن رمز آن امکانپذیر است استفاده از آن توسط صاحبش غیرقابل‌انکار است و صاحب گواهی در صورت گم شدن یا سرقت پودمان به عنوان عنصر داشته در احراز دو عامله، باید مراتب را بلافاصله به مرکز میانی صادرکننده گواهی اطلاع دهد. در غیر این صورت مسئولیت سوءاستفاده از آن توسط دیگران مستقیماً به عهده صاحب گواهی است. این نظام اعتماد در مورد گواهینامه رانندگی، شناسنامه، گذرنامه، پلاک خودرو و غیره نیز در قانون مدنی کشور وجود دارد.

از آنجا که بـرای امضای یک محتوای الکترونیک، فقط چکیده آن به پودمان منتقل می‌شود، محرمانگی اطلاعات نیز در این نظام تضمین می‌شود. نکته قابل توجه و قدرت امضای دیجیتال این است که برای اعتبارسنجی امضا فقط به کلید عمومی نیاز است؛ در نتیجه اولاً همه می‌توانند در اکو سیستم خدمات الکترونیک یک محتوای امضا شده را تصدیق یا رد کنند و برای این امر نیاز به حضور امضاکننده نیست. در شکل ۳ فرآیند تصدیق امضا ارائه شده است.

همانگونه که در فرآیند اعتبارسنجی مشخص است با کوچکترین تغییر در محتوای الکترونیکی نتیجه ارزیابی امضا رد خواهد شد و به این ترتیب هر تغییری در محتوای الکترونیک قابل تشخیص است.

تا اینجا نقش کلید خصوصی و عمومی در



شکل ۴: فرآیند امضا در یک سامانه

امضای دیجیتال مشخص و معلوم شد که به کمک این دو کلید می‌توان اثبات کرد یک محتوا توسط کدام کلید خصوصی در کدام پودمان امضا شده و محتوای امضا شده تغییر کرده است یا خیر. عنصری که هویت امضاکننده را مشخص می‌کند، گواهی الکترونیک است.

همان طور که قبلاً بیان شد گواهی حاوی اطلاعات هویتی مالک آن و کلید عمومی وی است که توسط یک مرکز صدور گواهی اعتبارسنجی و امضا شده است؛ در واقع توسط یک مرکز صدور گواهی به گواهی اعتبار بخشیده شده است. به این ترتیب می‌توان گفت هر سندی که با کلید عمومی داخل یک گواهی اعتبارسنجی شود توسط فردی که هویت آن در گواهی درج شده، امضا شده و از آنجا که پودمان نگهدارنده کلید خصوصی متناظر با کلید عمومی مندرج در گواهی در اختیار صاحب آن است، فرد امضاکننده در صورت عدم اعلام سرقت یا مفقودی پودمان، مسئول امضای خود بوده و نمی‌تواند منکر عمل خود شود.

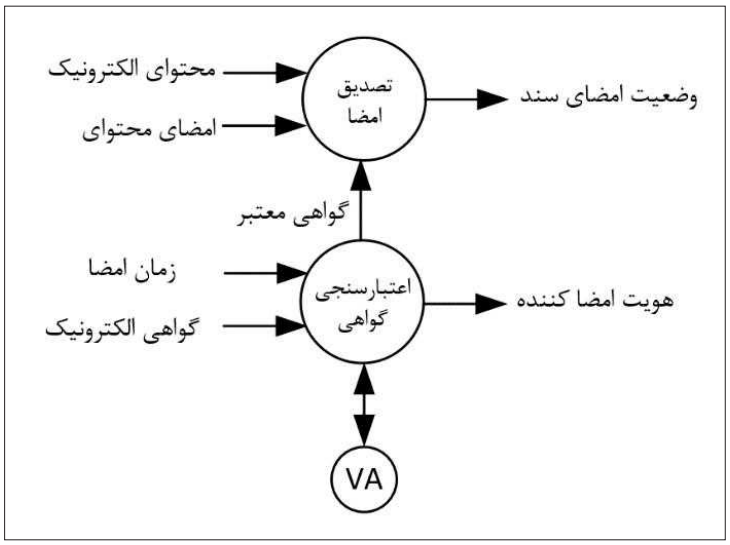
برای تکمیل زنجیره اعتماد و تحقق انکارپذیری و استناد پذیری اسناد و عملیات الکترونیک لازم است سامانه‌های استفاده کننده از گواهی الکترونیک نیز مطابق قوانین این حوزه عمل کنند.

چرخه عملیات در یک برنامه کاربردی برای امضا یا اعتبارسنجی امضا به طور کلی مطابق زیر است. بدیهی است این فرآیند اجزای زیادی دارد که در این نوشته مجال بحث آن نیست. (شکل ۴ و۵)

همانگونه که در فرآیند امضا و تصدیق امضا در سامانه‌های کاربردی مشاهده می‌کنید، در این فرآیند عنصری با عنوان VAوجود دارد.

(Validation Authority)

این عنصر توسط مرکز میانی صادرکننده گواهی عرضه می‌شود و آدرس آن در گواهی الکترونیک بصورت قابل اعتماد درج شده است. یک سامانه کاربردی برای انجام عملیات



شکل ۵: فرآیند اعتبارسنجی و تصدیق امضا

امضا و تصدیق آن باید مطابق فرآیند فوق اقدام کنند.

در این فرآیند اجزای متعددی جهت رعایت قوانین وجود دارد از جمله آن می‌توانWYS (what you see, what you say) را نام برد که در این فرآیند آورده نشده جهت اعتماد به سامانه‌های کاربردی طبق قوانین کشور سامانه‌ها باید در آزمایشگاه‌های مورد تأیید مرکز دولتی ریشه مورد ارزیابی و تأیید قرار گیرند.

نکته بسیار مهمی که باید بدانید و به آن توجه کنید این است که فرآیند امضا یک فرآیند در سمت کلاینت است و به هیچ عنوان نمی‌توان ادعا کرد که این فرآیند در کلاینت مطابق قوانین انجام شده است یا خیر؛ لذا نظام اعتبارسنجی گواهی و تصدیق امضا در سامانه‌های کاربردی اهمیت بالایی دارد. از آنجا که مدیریت و کنترل فرآیند امضا در سمت کلاینت قابل اعتماد نیست، تمام نظام‌های مبتنی بر زیرساخت کلید عمومی در دنیا جهت اعتبارسنجی و اعتماد به اسناد الکترونیک امضا شده، فرآیند امضا را ناامن فرض کرده و در فرآیند اعتبارسنجی و تصدیق امضا است که به سند و امضای آن اعتماد می‌کنند.

همانگونه که مشاهده کردید به طور کلی در فرآیند امضا و تصدیق امضا در اکوسیستم زیرساخت کلید عمومی عناصر مختلفی شامل RA، ICA، سامانه کاربردی، VA و پودمان رمزنگاری نقش دارند.

روابط بین این نقشها مطابق استانداردهای مرکز دولتی ریشه و استانداردهای جهانی انجام می‌پذیرد.

بدیهی است در صورتی که هر یک از این عناصر استانداردها را بطور کامل رعایت نکرده باشند، نمی‌توانند در اکو سیستم نقش کاملی داشته باشند و باعث می‌شوند بخشی از این اکوسیستم کارایی و یکپارچگی خود را از دست بدهد.

گفت و گو

سعید آزادی ابد، مدیرگروه ارزیابی محصولات و خدمات شرکت کاشف مطرح کرد:

از ارزیابی عملکرد و امنیت محصولات و خدمات بانکی تا مدیریت پروژه‌های اعتبارسنجی امنیت سایبری در آزمایشگاه امنیت سایبری کاشف

طبق گزارش IBM Cost of a Data Breach، میانگین جهانی هزینه نقض داده در سال ۲۰۲۱، بالغ بر ۴,۲۴ میلیون دلار بوده است. همچنین این بالاترین میانگین هزینه هر تخلف در ۱۷ سال گذشته است. این واقعیت جدید امنیت داده‌ها، تسلط بر امنیت سایبری را در زمینه فناوری اطلاعات مهم‌تر می‌کند. آزمایشگاه‌های سایبری این امکان را برای صاحبان کسب‌وکار که دارای سایت و اپلیکیشن‌های مختلف هستند فراهم می‌کند تا به سناریوهای زندگی واقعی نزدیک‌تر شوند و به آنها کمک می‌کند بینشی از آینده امنیت سایبری شغلی خود پیدا کنند. از آنجایی که سطح حمله سایبری لایه‌های متفاوتی دارد رویکردهای متفاوتی نیز می‌طلبد. مثلاً برای شناسایی تهدیدات احتمالی و ردیابی مهاجم، نیاز به راه‌اندازی آزمایشگاه‌های امنیت سایبری وجود دارد. اساساً، آزمایشگاه‌ها یک فضای اختصاصی پیشرفته هستند که برای نظارت، شناسایی و غیرفعال کردن مسائل امنیتی طراحی شده‌اند. همچنین آزمایشگاه‌های امنیت سایبری در یک محیط کنترل شده قرار دارند که در آن کارشناس سایبری سناریویی بلادرنگ برای انجام تست نفوذ ایجاد می‌کند. همه اینها در یک فضای ایزوله و بدون تأثیر بر شبکه‌های دیگر اتفاق می‌افتد.

در همین رابطه و اختصاصاً برای کسب وکارهای دارای امکان پرداخت و داد و ستد مالی که می‌تواند سلامت نظارت بانک مرکزی را ارتقا دهد، شرکت کاشف آزمایشگاه سایبری خود را راه‌اندازی کرد، درباره جزییات و عملکرد این آزمایشگاه با مدیرگروه ارزیابی محصولات و خدمات شرکت کاشف، سعید آزادی ابد به گفت‌وگو نشستیم:

آزمایشگاه نفوذ و اعتبار سنجی کاشف چه زمانی و برحسب چه فرآیندی شکل گرفت؟

آزمایشگاه ارزیابی و اعتبار سنجی کاشف در اسفند ماه سال ۱۴۰۰ در راستای تدوین و اجرای برنامه جامع ارتقای امنیت بانک مرکزی و شبکه بانکی راه‌اندازی شد.

در آزمایشگاه کاشف چه لاین های کاری و چه نوع تست هایی وجود دارد؟

در آزمایشگاه مدیریت امن الکترونیکی کاشف سه لاین وجود دارد:

پروژه‌های مبتنی بر نرم‌افزار(لاین وب): ارزیابی عملکردی، تست امنیتی

پروژه‌های مبتنی بر نرم‌افزارهای موبایل(لاین موبایل): ارزیابی عملکردی، تست امنیتی

پروژه‌های مبتنی بر زیرساخت کلید عمومی PKI: ارزیابی عملکردی، تست امنیتی، ممیزی فنی

که در بستر این سه لاین شاخص‌های ارزیابی و تست متدهای مرتبط با توجه به نوع محصولات تدوین شده است. همچنین آزمایشگاه کاشف به عنوان آزمایشگاه مورد تأیید افتا در حوزه بانکی نیز اقدام به ارزیابی عملکردی و امنیتی می‌کند.

پروژه‌های اعتبارسنجی چگونه در کاشف مدیریت می‌شوند؟

یکی از اقدامات صورت گرفته طی یک سال اخیر در آزمایشگاه کاشف، تدوین فرآیندهای مختلف در لایه‌های گوناگون بوده است. طی این مدت آزمایشگاه اقدام به تدوین حدوداً ۲۵ فرایند در لایه‌های مختلف کرده است که موارد ارزیابی و اعتباربخشی نیز شامل آنها می‌شود.

نیازهای عمده شرکت‌های درخواست کننده از شما چه بوده است؟

حفظ امنیت داده‌های حساس، ارائه راهکارهایی برای توسعه امن.

سرتیفیکت کاشف چگونه به آنها اطمینان خواهد داد، چه ضمانت اجرایی دارد؟ درصد اطمینان به این تست‌ها از لحاظ فنی چگونه است؟

به طورکلی هیچگاه نمی‌توان با قطعیت در خصوص امنیت ۱۰۰٪ صحبت کرد. با احتساب این واقعیت آزمایشگاه کاشف تمام تلاش خود را به‌کارگرفته که حداکثر انطباق محصولات به استانداردهای امنیتی را مورد ارزیابی قرار دهد. در این راستا از تجارب امنیت تهاجمی چندین ساله در این مجموعه کمک گرفته شده است تا ارزیابی امنیتی و انطباق سنجی مبتنی بر استانداردها با حداکثر کیفیت و انطباق صورت پذیرد.

عمده آسیب‌هایی که کشف کرده‌اید چیست و در چه دسته‌ای از شرکت‌ها بیشتر دیده می‌شود؟

عموماً به علت پیچیدگی بالای منطق کسب‌وکار سامانه‌ها، عمده مخاطرات مشاهده شده در حوزه سامانه‌ها بوده است.

الزامات بین المللی که طی فرایند تست ها به کار گرفته می شوند چه هستند؟

استانداردهای حوزه رمزنگاری و امنیتی محصولات شامل:
FIPS, NIST, MASVS, MSTG ISO 15408 , ISO 27000, PCI, ASVS (WSTG)S

اصلی ترین الزامات مربوط به تست موبایل MASVS و راهنمای تست آن MSTG و همچنین PCI نظام پرداخت (ISO 27002) است.

اصلی‌ترین الزامات مربوط به وب ASVS و راهنمای تست آن WSTG است.

همچنین الزامات مرتبط با رمزنگاری استانداردهای FIPS در چهارچوب امنیتی NIST است.

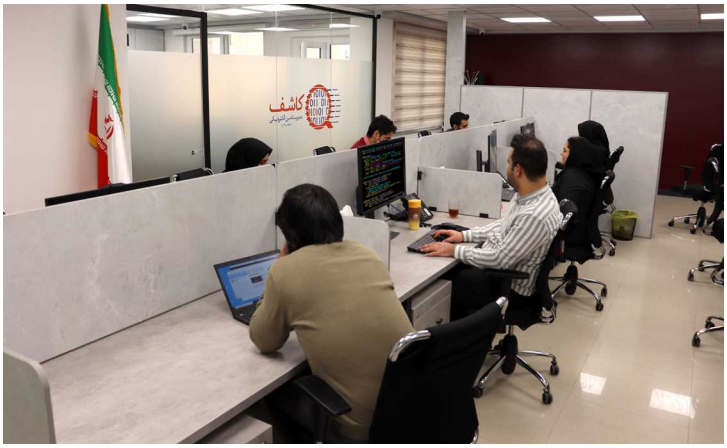
شایان ذکر است شرکت مدیریت امن الکترونیکی کاشف گواهی ISO17025 و ISO 15408 را در آزمایشگاه پیاده‌سازی و اجرا کرده است.

آیا فرآیند تست مجدد دارید و این فرآیند چه زمانی و چگونه انجام می‌شود؟

در آزمایشگاه مدیریت امن الکترونیکی کاشف پس از ارسال گزارش ارزیابی، متقاضی سه ماه مهلت برای رفع عدم انطباق‌های گزارش شده و ارجاع محصول به آزمایشگاه برای تست مجدد دارد.

همچنین تست‌های دوره‌ای با توجه به نوع محصولات وجود دارد که در بازه‌های تعریف شده متقاضی محصول را برای ارزیابی به آزمایشگاه ارائه می‌دهد. به عنوان مثال با توجه به سند «طرح ارزیابی امنیتی محصولات» گواهی‌های صادر شده توسط سازمان فناوری اطلاعات و مرکز مدیریت راهبردی افتا دو ساله است.

در سطح بین‌المللی چه ابزارها و لایسنس‌هایی استفاده می‌شود و آزمایشگاه کاشف چقدر به آن نزدیک است؟



امروزه بسیاری از سازمان‌های معتبر از نرم افزار لایسنس معتبر استفاده می‌کنند. ابزارهای مورد استفاده در آزمایشگاه کاشف نیز از این اصل امنیتی مستثنی نیست. ابزارهای مورد استفاده در ازمایشگاه کاشف همگی در سطح جهانی جایگاه بالایی دارد از جمله استفاده از لایسنس ابزارهای لیدر گارتنر در حوزه امنیت جهت بهره‌وری بالاتر مورد استفاده قرار می گیرد.

در سطح داخلی، آزمایشگاه کاشف بین آزمایشگاه‌های حوزه افتا در چه جایگاهی قرار دارد و آیا تابه حال مقایسه‌ای صورت گرفته است؟

آزمایشگاه کاشف به عنوان تنها آزمایشگاه در حوزه پولی و مالی در بین آزمایشگاه‌های مرکز مدیریت راهبردی افتا مطرح شده است؛ سطح ارزیابی در آزمایشگاه‌های افتا EAL۱ می‌باشد اما باتوجه به زیرساخت‌ها و پتانسیل فنی موجود در آزمایشگاه کاشف، پتانسیل ارزیابی در سطح بالاتر از EAL۱ وجود دارد.

> آزمایشگاه کاشف به عنوان تنها آزمایشگاه در حوزه پولی و مالی در بین آزمایشگاه‌های مرکز مدیریت راهبردی افتا مطرح شده است؛ سطح ارزیابی در آزمایشگاه‌های افتا EAL۱ می‌باشد اما باتوجه به زیرساخت‌ها و پتانسیل فنی موجود در آزمایشگاه کاشف پتانسیل ارزیابی در سطح بالاتر از EAL۱ وجود دارد

> نگاه ما امن‌سازی شبکه بانکی و پرداخت است و آزمایشگاه کاشف از سوی بانک مرکزی و با یک نگاه حاکمیتی موظف شده است که در سطح نرم‌افزارها مستقیم و غیرمستقیم وارد شود. از نگاه بانک مرکزی مجموعه‌های پولی بانکی موظف‌اند در یکسری از خدمت‌های خاص، تأییدیه آزمایشگاه کاشف را داشته باشند. از این باب نگاه ما انجام وظیفه است با این حال اگر در شش ماهه گذشته به عملکرد این گروه نگاه کنیم، حدود ۲۶ ارزیابی در حوزه موبایل و نماد به اتمام رسیده یا در حال ارزیابی هستند

در لاین آزمایشگاه موبایل و اپلیکیشن‌ها آماری وجود دارد که به ما بگوید طی شش ماه گذشته چند درخواست وجود داشته است؟

نگاه ما امن‌سازی شبکه بانکی و پرداخت است و آزمایشگاه کاشف از سوی بانک مرکزی و با یک نگاه حاکمیتی موظف شده است که در سطح نرم‌افزارها مستقیم و غیرمستقیم وارد شود. از نگاه بانک مرکزی مجموعه‌های پولی بانکی موظف‌اند در یکسری از خدمت‌های خاص، تأییدیه آزمایشگاه کاشف را داشته باشند. از این باب نگاه ما انجام وظیفه است با این حال اگر در شش ماهه گذشته به عملکرد این گروه نگاه کنیم، حدود ۲۶ ارزیابی در حوزه موبایل و نماد به اتمام رسیده یا در حال ارزیابی هستند.

در حوزه وب نیز حدود ۲۰ سامانه به اتمام رسیده یا در حال ارزیابی است. همچنین در شش ماه گذشته، ارزیابی درخواست‌های ارجاع شده از سوی مرکز مدیریت راهبردی افتا شروع شده است.

گفت و گو

رئیس گروه ممیزی و انطباق‌سنجی واحد نظارت شرکت کاشف:

تناقضی در اجرای چارچوب کنترلی و اجرای پروژه‌های تعریف شده در بانک ها و مؤسسات اعتباری وجود ندارد

در کشور ما هر بانک یا موسسه اعتباری به دلیل تفاوتی که در دیدگاه‌هایشان نسبت به موضوع امنیت وجود دارد، به دنبال پیاده‌سازی چارچوب امنیتی دلخواه خود است، چارچوب‌هایی مانند ISO270001، SWIFT، PCI-DSS طرح امن‌سازی زیرساخت‌های حیاتی کشور در برابر حملات سایبری (افتا) و .... بدین ترتیب شاهد هستیم که در نظام بانکی کشورمان اتفاق‌نظر و وحدت رویّه‌ای در انتخاب و پیاده‌سازی چارچوب‌های امنیتی در کار نبوده است. «چارچوب کنترل‌های امنیتی سازمانی و سامانه‌های اطلاعاتی بانکی» طراحی و تدوین شده به دست کارشناسان کاشف، درواقع تجمیع چارچوب‌های امنیتی شناخته‌شده و مرسوم جهان با الزامات امنیتی موجود در کشورمان است و بدین طریق، هر یک از بانک‌های کشور که این چارچوب را به کار گیرد، در عمل از مجموع توانمندی‌های آن چارچوب‌ها به‌طور یکجا و منسجم برخوردار است.بانک های کشور علی رغم اطلاع از این مزیت و حضور در نشست‌های تخصصی سوالات و دغدغه هایی داشتند که لازم بود به صورت صریح پاسخ داده شود. به این منظور در گفتگویی با وحید دوست‌محمدی، مدیر پروژه «چارچوب کنترل‌های امنیتی سازمانی و سامانه‌های اطلاعات بانکی» شرکت کاشف، به این سوالات پرداخته‌ایم.

رویکرد بانک مرکزی برای هماهنگی بین نهادهای تنظیم‌گر در حوزه امنیت اطلاعات چیست؟

یکی از اهداف مهم پروژه چارچوب کنترل‌های امنیتی، تجمیع تمامی الزامات امنیتی کاربردپذیر نهادهای تنظیم‌گر در حوزه امنیت اطلاعات است. بانک مرکزی از طریق برگزاری جلسات متعدد با تمامی ذینفعان حوزه امنیت اطلاعات در کشور به دنبال ایجاد وحدت رویه در حوزه امنیت اطلاعات در نظام بانکی کشور است. در این راستا هدفی که توسط بانک مرکزی دنبال می‌شود ایجاد یک پنجره واحد برای ابلاغ تمامی الزامات امنیتی از درگاه واحد بانک مرکزی ج.ا.ا است.

علت تدوین چارچوب کنترل‌های امنیتی از جانب بانک مرکزی ج.ا.ا. چه بوده است؟

«مرکز مدیریت راهبردی افتای ریاست جمهوری» به‌عنوان متولی زیرساخت‌های حیاتی کشور، «نقشه راه کلان»ی را با عنوان «طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری» تدوین و ابلاغ کرد و هر یک از سازمان‌های مادر- تخصصی مانند: وزارت نفت، بانک مرکزی، وزارت نیرو و... ملزم شدند تا مطابق با نقشه‌راه کلان یادشده، طرحی سفارش‌شده تدوین کنند.
در این راستا، بانک مرکزی ج.ا.ا به‌عنوان متولی نظام بانکی کشور تدوین چارچوب کنترلی را در دستور کار خود قرار داد و طرح امن‌سازی بومی‌شده‌ای را برای نظام بانکی کشور تدوین کرد. چارچوب کنترلی در بردارنده تمامی الزامات بالادستی در حوزه امنیت اطلاعات بوده و برای تأمین تمامی نیازمندی‌های امنیتی بانک‌ها و مؤسسات اعتباری از استانداردها و به‌روش‌های امنیتی نیز استفاده کرده است. انتظار می‌رود با پیاده‌سازی کنترل‌های امنیتی چارچوب کنترلی هر یک از بانک‌ها و مؤسسات اعتباری و نیز نهادهای تنظیم‌گر به اهداف امنیتی خود برسند.

مراجع تدوین چارچوب کنترل‌های امنیتی کدام یک از استانداردهای بین‌المللی است؟ آیا از منابع داخلی نیز در تدوین آن بهره برده شده است؟

چارچوب کنترلی برگرفته از معتبرترین استانداردهای بین‌المللی همچون: NIST، PCI-DSS، ISO 27001، SWIFT، FFIEC و همچنین الزامات، ابلاغیه‌ها و دستورالعمل‌های نهادهای تنظیم‌گر داخلی (نظیر مرکز مدیریت راهبردی افتا) در حوزه امنیت است.

آیا پس از پیاده‌سازی چارچوب کنترلی می‌توان برای دریافت گواهینامه سیستم‌های مدیریتی نظیر ISMS اقدام کرد؟

از آنجایی که چارچوب کنترلی دربرگیرنده استانداردهای بین‌المللی امنیتی منتخب و الزامات بالادستی است، بنابراین با پیاده‌سازی چارچوب کنترلی در واقع استاندارد ۲۷۰۰۱ نیز پیاده‌سازی شده است و امکان اقدام برای دریافت گواهینامه در دامنه پیاده‌سازی چارچوب کنترل‌های امنیتی وجود دارد.

برنامه اجرایی و روش پیاده‌سازی چارچوب کنترل‌های امنیتی سازمانی و سامانه‌های اطلاعاتی به چه صورت خواهد بود؟

مستندات راهنما در راستای پیاده‌سازی چارچوب کنترل‌های امنیتی سازمانی و سامانه‌های اطلاعاتی بانکی توسط مرکز کاشف تهیه و بصورت مستمر و به فراخور نیاز در اختیار بانک‌ها و مؤسسات اعتباری قرار خواهد گرفت.

رویکرد بانک مرکزی ج.ا.ا. در خصوص اقدامات قبلی بانک‌ها و مؤسسات اعتباری و نحوه یکپارچه‌سازی آن با چارچوب کنترلی به چه صورت خواهد بود؟ وضعیت پروژه‌های جاری حوزه امنیت اطلاعات در بانک‌ها و مؤسسات اعتباری به چه صورت خواهد بود؟

هریک از پروژه‌های امنیتی در حال اجرا در بانک‌ها و مؤسسات اعتباری، همچنان قابل اجرا خواهند بود و در صورت همراستایی با اهداف کنترل‌های مندرج در چارچوب، می‌توانند نیازمندی‌های اجرایی این کنترل‌ها را پوشش دهند؛ فلذا تناقضی در اجرای چارچوب کنترلی و نیز اجرای پروژه‌های تعریف شده در بانک‌ها و مؤسسات اعتباری وجود ندارد.

آیا کارگاه‌های آموزشی و جلسات توجیهی چارچوب کنترلی ادامه‌دار خواهد بود؟

بله، بانک مرکزی ج.ا.ا. و مرکز کاشف، کارگاه‌های آموزشی و جلسات تخصصی مشخصی را در هر یک از مراحل پیاده‌سازی چارچوب کنترلی برگزار کرده و جزو مقررات است که در تمامی مراحل پیاده‌سازی چارچوب، راهنمایی‌های لازم را در اختیار بانک‌ها و مؤسسات اعتباری قرار دهد. همچنین هریک از بانک‌ها و مؤسسات اعتباری در صورت نیاز، می‌توانند درخواست برگزاری جلسات اختصاصی با مرکز کاشف را طی یک نامه رسمی به این مرکز اعلام کرده و با انجام هماهنگی‌های لازم به این مهم دست پیدا کنند.

> در این راستا، بانک مرکزی ج.ا.ا به‌عنوان متولی نظام بانکی کشور تدوین چارچوب کنترلی را در دستور کار خود قرار داد و طرح امن‌سازی بومی‌شده‌ای را برای نظام بانکی کشور تدوین کرد. چارچوب کنترلی در بردارنده تمامی الزامات بالادستی در حوزه امنیت اطلاعات بوده و برای تأمین تمامی نیازمندی‌های امنیتی بانک‌ها و مؤسسات اعتباری از استانداردها و به‌روش‌های امنیتی نیز استفاده کرده است.

آیا در خصوص اجرای چارچوب کنترل‌های امنیتی سازمانی و سامانه‌های اطلاعاتی بانکی، فرآیندهای ممیزی هم انجام خواهد شد؟

مسلماً بله، بانک مرکزی ج.ا.ا. و مرکز کاشف در حال ایجاد نظام ممیزی امنیتی بانک‌ها و مؤسسات اعتباری است که در هماهنگی کامل با نظام ممیزی موجود در کشور (افتا) است و به‌صورت یکپارچه با آن انجام خواهد شد.

فرآیند ممیزی توسط چه کسانی انجام خواهد شد؟

ممیزی توسط مرکز کاشف بانک مرکزی با حضور سایر ذینفعان نظیر اداره کل امنیت اطلاعات بانک مرکزی به‌عنوان متولی امنیت، اداره سلامت و مرکز حراست برگزار خواهد شد. همچنین نمایندگان سایر نهادهای تنظیم‌گر نظیر مرکز افتا و پدافند غیرعامل نیز در صورت نیاز تیم ممیزی را همراهی خواهند کرد. هدف نهایی از برگزاری این ممیزی‌ها، انجام یکپارچه ممیزی و پیگیری تمامی معیارهای ممیزی است که توسط تمامی ذینفعان تدوین و ابلاغ شده است.

ممیزی‌های صورت گرفته از سوی بانک مرکزی در چه تواترهای زمانی انجام خواهد شد؟

طبق برنامه‌ریزی‌های صورت گرفته، حداقل هر ۶ ماه یک‌بار ممیزی‌ها در محل (On-Site) انجام خواهد شد. بدیهی است این بازه زمانی بسته به شرایط بانک‌ها و مؤسسات اعتباری و نیازمندی‌های نهادهای تنظیم‌گر قابل تغییر خواهد بود.

آیا با پیاده‌سازی چارچوب کنترلی دیگر ممیزی‌های مستقل از سوی سایر نهادهای تنظیم‌گر انجام نخواهد شد؟ چرا با وجود چارچوب کنترلی همچنان برخی از الزامات از سوی سایر نهادهای تنظیم‌گر ارسال، ابلاغ و پیگیری می‌شود؟

تمامی تلاش‌ها و هماهنگی‌های لازم با نهادهای تنظیم‌گر حوزه امنیت در کشور همچون مرکز افتا، پدافند غیرعامل، مرکز ملی فضای مجازی، مرکز حراست و سایر نهادهای موجود در بانک مرکزی ، در خصوص انجام ممیزی‌های یکپارچه از طریق پنجره واحد بانک مرکزی در حال پیگیری است و امید است در آینده نزدیک این مهم به‌طور کامل محقق شود.

در بانک و مؤسسه اعتباری کدام واحد ذینفع اجرای این پروژه است؟

هر یک از بانک‌ها و مؤسسات اعتباری با توجه به ساختار داخلی خود می‌توانند مسئولیت اجرای پروژه چارچوب کنترلی را به هر یک از واحدهای سازمانی خود محول کنند و مرکز کاشف یا بانک مرکزی در این خصوص ملاحظه‌ای نخواهد داشت. همچنین هریک از بانک‌ها و مؤسسات اعتباری باید برای اجرای پروژه چارچوب کنترلی کارگروه اجرایی خود را به صورت رسمی به بانک مرکزی و مرکز کاشف معرفی کنند. پیشنهاد می‌شود اعضای این کارگروه متشکل از ذینفعان کلیدی حوزه امنیت اطلاعات نظیر فناوری اطلاعات، امنیت اطلاعات، حراست باشد. نکته‌ای که باید مورد نظر قرار گیرد این است که در جلسات مشترک با مرکز کاشف صرفاً اعضای کارگروه که به طور رسمی معرفی شده‌اند امکان شرکت خواهند داشت و حضور مدیر پروژه در تمامی نشست‌ها ضروری است؛ بنابراین مدیر پروژه چارچوب کنترلی باید زمان، منابع و اختیارات کافی برای تصمیم‌سازی در نشست‌های مشترک را داشته باشد.

تعیین محدوده اجرای چارچوب کنترلی چگونه خواهد بود؟

محدوده اجرای چارچوب کنترلی بر اساس سامانه‌های اطلاعاتی تعیین خواهد شد و نهاد

تنظیم‌گر (بانک مرکزی ج.ا.ا با هماهنگی سایر نهادهای تنظیم‌گر نظیر مرکز مدیریت راهبردی افتا، پدافند غیرعامل، سازمان حراست کل) نسبت به تعیین و ابلاغ سامانه‌های اطلاعاتی دارای اهمیت اقدام خواهد کرد. هریک از بانک‌ها و مؤسسات اعتباری نیز می‌توانند در کنار سامانه‌های اطلاعاتی دارای اهمیت که از طرف نهاد تنظیم‌گر تعیین شده است نسبت به تعیین سامانه‌های اطلاعاتی که براساس شاخص‌های داخلی دارای اولویت هستند اقدام کنند.

منظور از سامانه اطلاعاتی در چارچوب کنترلی چیست؟

سامانه اطلاعاتی مجموعه‌ای از دارایی‌های (منابع) اطلاعاتی است که برای گردآوری، پردازش، نگهداری، استفاده، اشتراک، توزیع و ساماندهی اطلاعات، در کنار و در ارتباط با یکدیگر قرار گرفته و کار می‌کنند. منابع اطلاعاتی شامل اطلاعات و منابع مرتبط با آن مانند کارکنان، تجهیزات، منابع مالی، فناوری‌های اطلاعاتی و ارتباطی است..

آیا در خصوص چارچوب کنترلی، ساختار مدیریتی و اجرایی در بانک مرکزی/کاشف وجوددارد؟

بله، در بانک مرکزی ساختارهای مدیریتی و اجرایی برای راهبری و مدیریت پروژه چارچوب کنترلی در نظر گرفته شده است. شاید به‌توان گفت که مهمترین رکن این ساختار که نمود بیرونی نیز دارد کارگروه اجرایی مشترکی است که بین بانک مرکزی، مرکز کاشف و نمایندگان بانک‌ها و مؤسسات اعتباری شکل می‌گیرد. جلسات این کارگروه حداقل به‌صورت ماهیانه در محل مرکز کاشف تشکیل می‌شود و روند پیشرفت پروژه در بانک‌ها و مؤسسات اعتباری مورد بررسی قرار می‌گیرد. همچنین در صورتی که بانک‌ها و مؤسسات اعتباری در هریک از گام‌های پیاده‌سازی پروژه چارچوب با ابهاماتی مواجه شوند می‌توانند با نمایندگان مرکز کاشف که در طی جلسات فی مابین به ایشان معرفی شده است در ارتباط باشند.

روال به‌روزرسانی چارچوب کنترلی چگونه خواهدبود؟

پروژه توسعه و به‌روزرسانی چارچوب کنترل‌های امنیتی در مرکز کاشف در حال اجراست و در قالب این پروژه نسخ جدید استانداردها و مراجع به‌کاربرده شده در چارچوب، همواره در حال تحلیل و بررسی است. در صورت وجود تغییرات اساسی، ابلاغ و انتشار نسخه جدید و به‌روزرسانی‌شده انجام خواهد شد. همچنین در صورت تغییر بخشی از کنترل‌های چارچوب کنترلی، ممکن است صرفاً کنترل‌ها مرتبط با همان دسته و زیردسته به‌روزرسانی شود و نیازی به ارائه یک نسخه جدید از کل سند چارچوب کنترلی نباشد. برای مثال ممکن است که بانک مرکزی به دلیل یک الزام بالادستی جدید یا انعکاس درس‌آموخته‌های حاصل از یک رخداد امنیتی، به دنبال ابلاغ الزامات مشخصی در حوزه «مدیریت حوادث» باشد، در این صورت، صرفاً الزامات جدید که در کنترل‌های ابلاغ شده قبلی پوشش داده نمی‌شوند در قالب کنترل‌های جدید چارچوب کنترلی به بانک‌ها و مؤسسات اعتباری ابلاغ خواهند شد.

> مهمترین رکن این ساختار که نمود بیرونی نیز دارد کارگروه اجرایی مشترکی است که بین بانک مرکزی، مرکز کاشف و نمایندگان بانک‌ها و مؤسسات اعتباری شکل می‌گیرد

نحوه تعامل بانک‌ها و مؤسسات اعتباری با بانک مرکزی چگونه خواهد بود؟ آیا باید به‌طور مستقیم با کاشف در ارتباط هستند یا با بانک مرکزی؟ برای تعامل با مرکز کاشف با کدام گروه و از طریق چه کانالی می‌توان ارتباط گرفت؟

در پروسه مکاتبات بین بانک‌ها و مؤسسات اعتباری، نامه‌ها، گزارش‌ها و... برای بانک مرکزی و رونوشت هریک از آنها به‌منظور تسریع در فرآیند رسیدگی به مکاتبات، برای مرکز کاشف نیز ارسال می‌شود.

جهت اخذ راهنمایی‌های لازم در خصوص پروژه چارچوب کنترلی امکان برقراری ارتباط مستقیم با کارگروه‌های فنی تعریف شده در «مدیریت نظارت/گروه ممیزی و انطباق‌سنجی» مرکز کاشف از طریق شماره تماس ۷۲۸۶۱۴۰۰-۰۲۱ وجود دارد. همچنین نمایندگان مرکز کاشف در جلسات مشترک با بانک‌ها و مؤسسات اعتباری معرفی می‌شوند و صرفاً مدیران پروژه (که به طور رسمی توسط بانک ها معرفی شده‌اند) می‌توانند با نماینده کاشف در ارتباط باشند.

آیا برای راهبری چارچوب کنترلی در بانک‌ها و مؤسسات اعتباری ساختار اجرایی خاصی باید در بانک و مؤسسه اعتباری ایجاد شود؟

بله، لازم است پروژه «چارچوب کنترل‌های امنیتی» در بانک/مؤسسه اعتباری تعریف و «مدیر پروژه» در این خصوص تعیین و اطلاعات ایشان به‌منظور برقراری ارتباطات آتی، به بانک مرکزی و مرکز کاشف اعلام شود.

همچنین لازم است کارگروه‌های اجرایی موردنیاز در بانک و مؤسسه اعتباری تشکیل و اطلاعات اعضا برای بانک مرکزی و مرکز کاشف ارسال شود.

آیا در حال حاضر سامانه‌ای در کشور وجود دارد که بتواند کل فرآیندهای چارچوب کنترلی را پیاده‌سازی کند؟

تاکنون هیچ‌گونه درخواستی مبنی بر اخذ تأییدیه یا مجوزهای موردنیاز در خصوص انتشار سامانه‌ای مرتبط با چارچوب کنترل‌های امنیتی دریافت نشده و چنین سامانه‌ای توسط هیچ‌یک از شرکت‌های بخش خصوصی تهیه و منتشرنشده‌است.

در این راستا، مرکز کاشف اقدام به تهیه ابزار سرابان برای پشتیبانی از پروژه چارچوب کنترلی کرده که پس از انجام مراحل آزمون و نهایی‌سازی آن و پس از دریافت تأییدیه های

پادکشف

صدای اختصاصی کاشف

شرکت کاشف یکی از مسئولیت‌های خود را ارتقای سطح دانش عمومی برای استفاده امن از ابزارها و خدمات بانکداری و پرداخت الکترونیکی می‌داند و در همین راستا نیز تلاش دارد با تفکیک مخاطبان و کاربران این خدمات، آگاهی‌های لازم را برای افزایش سواد جامعه با استفاده از ظرفیت‌های متنوع ارتباطی در اختیار کاربران قرار دهد.

یکی از ابزارهای ارتباطی که طی سال‌های اخیر سهم و نقش بسیاری در آگاهی‌بخشی و انتقال دانش به طیف‌های مختلف جامعه داشته و دارد، پادکست است. در همین راستا هم تهیه و نشر «پادکشف» در برنامه‌های روابط عمومی شرکا کاشف قرار گرفت و اکنون خوشبختانه دو اپیزود از آن منتشر شده است. قابل بیان استکه در قسمت‌های مختلف پادکشف که ماهانه منتشر خواهد شد به موضوعات مرتبط با امنیت در حوزه بانکداری و پرداخت الکترونیکی، روش‌های امن استفاده از ابزارها، شیوه‌های تقلب و... بپردازیم تا با استفاده از قابلیت‌های این پلتفرم، ارتباط نزدیک‌تری با کاربران و مخاطبان برقرار کنیم.

روابط عمومی کاشف به عنوان تهیه‌کننده پادکشف در مسیر تولید محتوای هر قسمت به شدت مشتاق و علاقمند همکاری با کارشناسان، مسئولان و دغدغه‌مندان حوزه امنیت است و از هر گونه همکاری استقبال خواهد کرد. بسیار امیدواریم که پادکشف، اقدام مفیدی برای ارتقای دانش و سواد عمومی در استفاده از ابزارهای پرداخت و بانکداری الکترونیکی باشد و اطمینان خاطر بیشتری برای مردم عزیزمان به ارمغان بیاورد.

شما می توانید اپیزود صفر پادکشف با موضوع فیشینگ و اپیزود اول «پادکشف» با موضوع امنیت اپلیکیشن‌های بانکی را، در پلتفرم castbox و کانال رسمی شرکت کاشف در تلگرام بشنوید.

پادْکَشف

پادکست اختصاصی شرکت کاشف

مقاله

راهگشایی فنون تاب‌آوری سایبری؛

اولویت پژوهشی شرکت کاشف

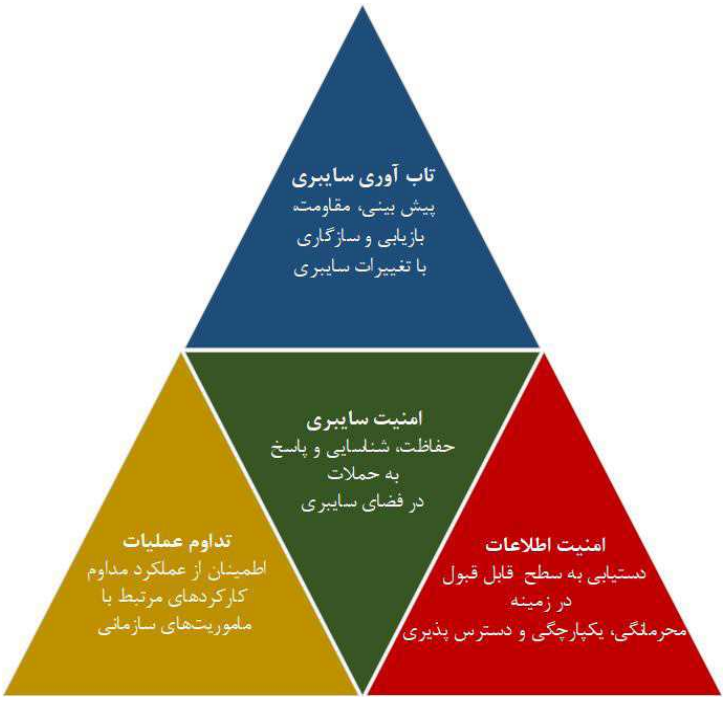
ساناز دهقانی
کارشناس ممیزی و انطباق‌سنجی شرکت کاشف

تلاش‌های امنیت اطلاعات در بسیاری از بانک‌ها و مؤسسات اعتباری غیربانکی، معطوف به انطباق با الزامات امنیتی ابلاغی نهادهای بالادستی یا اخذ گواهینامه‌های مرتبط است. فارغ از مسأله کمبود نیروی کار امنیت سایبری که بانک‌ها و مؤسسات اعتباری را محدود به انجام اقداماتی صرفاً برای انطباق با الزامات می‌کند؛ در برخی از مؤسسات اعتباری، امنیت معادل انطباق با الزامات و پیاده‌سازی کنترل‌های امنیتی تلقی می‌شود در حالی که یک سازمان منطبق با استانداردها و الزامات امنیت سایبری لزوماً تاب‌آور نیست.

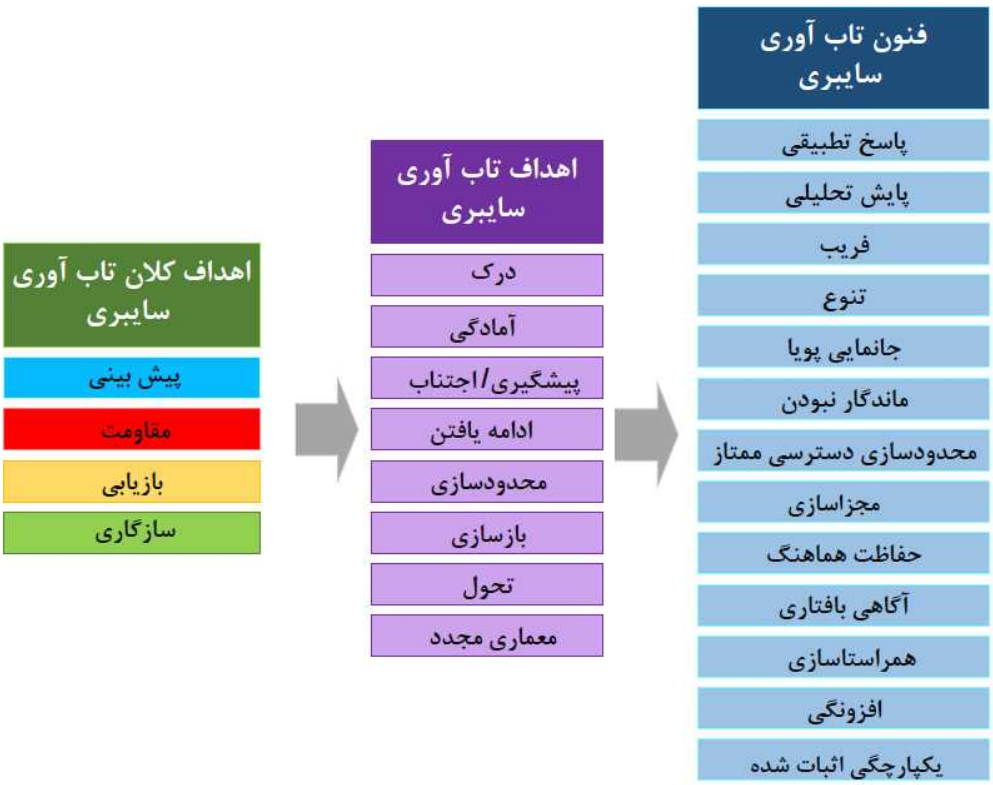
تاب‌آوری سایبری به معنای توانایی سازمان برای پیش‌بینی، مقاومت، بازیابی و سازگاری با شرایط نامطلوب، حملات، فشارها (برای نمونه بار کاری بالا و غیرمنتظره) و به‌خطرافتادن سامانه‌های مورد استفاده در منابع سایبری است و در نهایت، هدف از تاب‌آوری سایبری، دستیابی به مأموریت یا اهداف کسب‌وکاری وابسته به منابع سایبری است. هر چند تاب‌آوری سایبری بر پایه امنیت اطلاعات بنا می‌شود اما رویکرد آن متفاوت است، امنیت اطلاعات بر دستیابی به اهداف محرمانگی، یکپارچگی و دسترس‌پذیری تا سطح قابل قبول (با استفاده از حفاظت محیطی و اجرای کنترل‌های داخلی) متمرکز است؛ در حالی که تاب‌آوری سایبری فرض می‌کند که شرایط نامطلوب در حال اتفاق افتادن است، برای نمونه مهاجمان مستقر هستند تا کارکردها را متوقف یا کند کنند، داده‌ها را تخریب، دستکاری یا جعل کنند، اطلاعات حساس را به سرقت ببرند و به طور کلی تضمین انجام مأموریت‌ها و کارکردهای کسب‌وکاری را مختل کنند. به بیان دیگر تاب‌آوری سایبری فرض را بر این قرار می‌دهد که اقدامات امنیتی کافی انجام شده است، اما مهاجمان احتمال حضور در شبکه یا سامانه‌های سازمان را دارند. به این منظور تاب‌آوری سایبری بر پایه‌های امنیت سایبری که مبتنی بر حفاظت، تشخیص و پاسخ به حملات است نیز بنا می‌شود. بنابراین امنیت اطلاعات، امنیت سایبری و تداوم عملیات، شالوده‌های تاب‌آوری سایبری هستند. (شکل ۱)

طبق تعریف رایج تاب‌آوری سایبری که پیش‌تر تبیین شد، چهار هدف کلان: پیش‌بینی (Anticipate)، مقاومت (Withstand)، بازیابی (Recover) و سازگاری (Adapt) از مفهوم تاب‌آوری سایبری استخراج می‌شود. با توافق واژه «تهاجم» برای شرایط نامطلوب، حملات، فشارها و به‌خطرافتادن سامانه‌های مورد استفاده در منابع سایبری، اهداف کلان تاب‌آوری سایبری اینگونه تعریف می‌شوند؛ پیش‌بینی؛ حفظ وضعیت آمادگی آگاهانه در مقابل تهاجم.

در این تعریف «آمادگی آگاهانه» معطوف به طرح‌ریزی تداوم و طرح‌های کاهش و رسیدگی به رویدادهای تهدیدآمیز و همچنین کشف آسیب‌پذیری‌ها و به‌خطرافتادن‌های زنجیره تأمین است و یقیناً هوش تهدیدات سایبری می‌تواند اطلاعات مؤثری برای «آمادگی آگاهانه» فراهم کند.



شکل ۱: شالوده‌های تاب‌آوری سایبری



شکل ۲: اهداف و فنون تاب‌آوری سایبری در سطح سامانه‌های عملیاتی

مقاومت؛ تداوم کارکردهای کسب‌وکاری و مأموریت‌های اصلی علی‌رغم تهاجم.

برای دستیابی به این هدف باید مأموریت‌های اصلی و کارکردهای کسب‌وکاری سازمان و به تبع آن، زیرساخت، شبکه، خدمات سامانه‌ها و فرآیندهای پشتیبان نیز به درستی شناسایی شوند. توجه به این نکته حائز اهمیت است که حیاتی بودن منابع و قابلیت‌های کارکردهای اساسی در طول زمان می‌تواند تغییر کند.

بازیابی؛ بازگرداندن مأموریت یا کارکردهای کسب‌وکاری حین و پس از تهاجم.

در هدف کلان بازیابی، اگر چه بازگرداندن کارکردها و داده‌ها می‌تواند افزایشی باشد، اما چالش اصلی این است که چه میزان از اعتماد بر کارکردها و داده‌ها در فرآیند بازیابی می‌تواند حکمفرما باشد. برای نمونه در زمان بازیابی، دیگر تهدیدات چه میزان مداخله خواهند کرد و مهاجمان از شرایط سردرگمی بازیابی به چه میزان منتفع شده و جای پای خود را در سامانه‌ها چقدر محکم‌تر خواهند کرد.

سازگاری؛ اصلاح مأموریت یا کارکردهای کسب‌وکار و/یاصلاح مأموریت یا کارکردهای کسب‌وکار/ یا قابلیت‌های پشتیبان در پاسخ به تغییرات پیش‌بینی‌شده فنی، عملیاتی یا محیط تهدیدات.

در توضیح هدف کلان فوق، لازم است به یاد داشته باشیم که تغییر در زمان‌های متفاوت و مقیاس‌های گوناگون رخ می‌دهد؛ بنابراین تطبیق‌پذیری راهبردی و تاکتیکی ضروری است. تغییرات از محیط فنی، خدمات و محصولات جدید و فناوری‌های نوظهور مانند هوش مصنوعی تا تغییرات مقرراتی، همه باید از جنبه تغییر در سطح حمله (Attack surface) نیز تحلیل شوند.

برای بررسی دقیق‌تر موضوع مورد بحث، پس از تبیین تعریف و اهداف کلان تاب‌آوری سایبری، لازم است از سطح سازمانی و فرآیندهای کسب‌وکاری به سطح سامانه‌ها نیز وارد شویم و اهداف کلان را به اهداف موردنیاز ذی‌نفعان برای تضمین مأموریت‌ها در سطح سامانه‌های موجود در محیط عملیاتی ترجمه کنیم؛ این اهداف شامل موارد ذیل است:

پیشگیری یا اجتناب(Prevent or Avoid): ممانعت از اجرای موفق حمله یا تشخیص مناسب تهاجم.

آمادگی (Prepare): نگهداشت مجموعه اقدامات واقع‌بینانه برای مقابله با تهاجم پیش‌بینی‌شده یا مورد انتظار.

ادامه یافتن(Continue): بیشینه‌سازی مدت زمان اجرای کارکردهای کسب‌وکاری یا مأموریت‌های اصلی حین تهاجم.

محدودسازی(Constrain): محدود کردن خسارت ناشی از تهاجم.

بازسازی (Reconstitute): بازیابی هر چه بیشتر مأموریت یا کارکرد کسب‌وکاری پس از تهاجم.

درک(Understand): نگهداشت نمایه‌های مفیدی از مأموریت و وابستگی‌های کسب‌وکاری و همچنین وضعیت منابع با توجه به احتمالات وقوع تهاجم.

تحول (Transform): اصلاح مأموریت یا کارکردهای کسب‌وکار و فرآیندهای پشتیبان آنها برای اداره تهاجم و رسیدگی مؤثرتر به تغییرات محیطی.

معماری مجدد (Re-Architect): اصلاح معماری‌ها برای اداره تهاجم و رسیدگی مؤثرتر به تغییرات محیطی.

نخستین بار، مایتره، در «چارچوب مهندسی تاب‌آوری سایبری» برای اهداف تاب‌آوری سایبری، فنونی (Techniques) را ارائه داد و امروزه مورد اقتباس نهادهای استانداردسازی مانند مؤسسه ملی فناوری و استانداردها (NIST) نیز قرار گرفته‌اند. فنون تاب‌آوری سایبری، مجموعه‌ای از فناوری‌ها، فرآیندها و روش‌هایی است که قابلیت‌های لازم را برای دستیابی به یک یا چند هدف تاب‌آوری سایبری فوق، فراهم می‌کند. این فنون چهارده‌گانه به اختصار در ذیل ترسیم و معرفی شده‌اند. (شکل ۲)

۱- پاسخ تطبیقی (Adaptive Response): به‌کارگیری مجموعه اقدامات چابک در مدیریت مخاطرات.

۲- پایش تحلیلی(Analytic Monitoring): پایش و تحلیل طیف گسترده‌ای از ویژگی‌ها و رفتارها به صورت مداوم و هماهنگ.

۳- آگاهی بافتاری (Contextual Awareness):

ساخت و نگهداشت نمایه فعلی از وضعیت مأموریت‌های سازمانی یا کارکردهای کسب‌وکار با درنظرگرفتن رویدادهای تهدیدآمیز و اقدامات مربوطه.

۴- حفاظت هماهنگ

(Coordinated Protection): حصول اطمینان از اینکه سازوکارهای حفاظتی، به شیوه‌ای هماهنگ و اثربخش عمل کنند.

۵- فریب (Deception): پنهان‌کردن دارایی‌های حیاتی از دید مهاجم از طریق گمراه‌کردن یا گیج‌کردن یا در معرض قرار دادن دارایی‌های آلوده برای مهاجم.

۶- تنوع (Diversity): ناهمگون‌سازی به منظور کمینه‌کردن نقاط شکست رایج، به ویژه رویدادهای تهدیدآمیزی که از آسیب‌پذیری‌های رایج بهره می‌برند.

۷- جانمایی پویا (Dynamic Positioning): توزیع یا موقعیت‌یابی پویای کارکردها یا منابع سامانه.

۸- ماندگار نبودن (Non-Persistence): ایجاد و فعال نگه داشتن منابع تنها در صورت نیاز یا برای مدت محدود.

۹- محدودسازی دسترسی ممتاز

(Privilege Restriction): محدودسازی دسترسی‌های ممتاز بر پایه مشخصه‌های کاربران، عناصر سامانه‌ها و عوامل محیطی.

۱۰- هم‌راستاسازی (Realignment): سازماندهی مجدد سامانه‌ها و نحوه استفاده از منابع به طوری که نیاز کارکردهای کسب‌وکاری یا مأموریتی تأمین شود، مخاطرات موجود یا مورد انتظار کاهش یابد و با تحولات فنی، عملیاتی و محیط تهدیدات تطبیق حاصل شود.

۱۱- افزونگی (Redundancy): تهیه چندین نمونه محافظت‌شده از منابع حیاتی.

۱۲- مجزاسازی (Segmentation): تعریف و جداسازی عناصر سامانه بر اساس حیاتی بودن و قابلیت‌اعتماد.

۱۳- یکپارچگی اثبات‌شده

(Substantiated Integrity): استفاده از سازوکارهایی برای اطمینان از اینکه آیا عناصر حیاتی سامانه دچار تغییر شده‌اند یا خیر.

۱۴- قابل پیش‌بینی نبودن

(Unpredictability): ایجاد تغییرات به طور تصادفی و غیرقابل پیش‌بینی.

با تشریح ضرورت تاب‌آوری سایبری و فنون متناظر برای دستیابی به آن اهداف و در راستای اهداف کلان شرکت کاشف در زمینه ارتقای توانمندی نظام بانکی در پیشگیری از رخدادهای امنیتی و ارتقای قابلیت شناسایی و پاسخگویی هماهنگ به تهدیدها و رخدادهای امنیت اطلاعات، یکی از راهبردهای اصلی پژوهش و نوآوری در مدیریت توسعه خدمات شرکت کاشف، راهگشایی فنون تاب‌آوری سایبری برای نظام بانکی تعریف شده است؛ مقصود از راهگشایی، بسته به فنون یادشده، تهیه ابزارهای راهنما، توسعه خدمات کسب‌وکاری مرتبط، ارائه خدمات، تدوین توصیه‌نامه‌های فنی یا برگزاری کارگاه‌های آموزشی است. از مجموعه فنون چهارده‌گانه، تکنیکی که هم‌اکنون پروژه آن در حال اجرا است، تکنیک «فریب» است.

طبق تعاریف فنون تاب‌آوری سایبری یادشده، فریب، پنهان کردن دارایی‌های حیاتی از دید مهاجم از طریق گمراه‌کردن یا گیج‌کردن یا در معرض قرار دادن دارایی‌های آلوده برای مهاجم است. با استفاده از فریب، دارایی‌های مهم از دید مهاجم مخفی شده یا مهاجم با دارایی غیرواقعی گمراه یا گیج خواهد شد؛ نتیجه این امر، نامطمئن شدن مهاجم از نحوه ادامه کار، به تأخیر افتادن تأثیر حمله، افزایش خطر کشف شدن حمله و شناسایی مهاجم است. همچنین باعث می‌شود که مهاجم منابع خود را نادرست هدایت کرده یا هدر دهد و در نهایت روش کار خود را فاش گرداند.

طبق تعاریف فنون تاب‌آوری سایبری یادشده، فریب، پنهان کردن دارایی‌های حیاتی از دید مهاجم از طریق گمراه کردن یا گیج کردن یا در معرض قرار دادن دارایی‌های آلوده برای مهاجم است. با استفاده از فریب، دارایی‌های مهم از دید مهاجم مخفی شده یا مهاجم با دارایی غیر واقعی گمراه یا گیج خواهد شد؛ نتیجه این امر، نامطمئن‌شدن مهاجم از نحوه ادامه کار، به‌تأخیرافتادن تأثیر حمله، افزایش خطر کشف شدن حمله و شناسایی مهاجم است

توجه به این نکته حائز اهمیت است که به هیچ‌عنوان هانی‌پات و فریب سایبری مترادف نیستند ولی فریب سایبری را می‌توان تکامل‌یافته هانی‌پات‌ها دانست. هانی‌پات‌ها معمولاً دامنه محدودی دارند و شناسایی آنها برای مهاجمان حرفه‌ای آسان است. ثابت شده است که هانی‌پات‌ها اثر خاصی در تشخیص ندارند. در تعاریف پیش‌گفته فریب، از جمله تعریف ارائه‌شده توسط NIST، از چهار واژه برای توصیف و تمایز فریب استفاده می‌شود: مبهم‌سازی (Obfuscation)، اطلاعات نادرست (Disinformation)، هدایت نادرست (Misdirection) و آلوده‌سازی (Tainting).

«مبهم‌سازی» به پنهان‌کردن، تبدیل‌کردن یا به طریق دیگری مبهم‌کردن اطلاعات اشاره دارد. مهاجمان نمی‌دانند که کدام اهداف واقعی و کدام‌یک فریب هستند. مبهم‌سازی یک تاکتیک دفاعی ارزشمند است، به‌ویژه هنگامی که با رهگیری حمله و هدایت مجدد همراه باشد و در عین حال اطلاعات نادرست به مهاجم می‌دهد تا تلاش‌های وی را از مسیر خارج کند.

«اطلاعات نادرست» به ارائه عمدی اطلاعات گمراه کننده به مهاجم با استفاده از هر یک از انواع تکنیک‌ها اشاره دارد. یکی از روش‌های اطلاعات نادرست که به صراحت به آن اشاره شده، معرفی اعتبارنامه‌ها و توکن‌های نادرست به محیط است.

«هدایت نادرست» با عنوان حفظ منابع یا محیط‌های فریب و هدایت مهاجم به آن منابع یا محیط‌ها تعریف شده است.

«آلوده‌سازی» شامل گنجاندن قابلیت‌های پنهان در منابع است، مانند افزودن ورودی‌هایی به DNS حافظه پنهان شبکه یک سازمان که به دارایی‌ها و میزبان‌های فریبنده اشاره می‌کنند. این ورودی‌ها اعتبار سامانه‌های فریب را افزایش می‌دهند درحالی‌که به مهاجم اهداف بالقوه‌ای را ارائه می‌دهند که خود این اهداف تله هستند.

امروزه تکنیک فریب، به سکوهای فریب تبدیل شده است که شامل منابع فریبنده، برنامه‌های کاربردی، داده‌ها، پایگاه داده و غیره برای شناسایی جامع تهدید هستند. علاوه‌بر این، سکوهای فریب سایبری مدرن می‌توانند تحلیل‌های گسترده‌ای از حملات و قابلیت‌های خودکارسازی پاسخ ارائه دهند. این راه‌حل‌ها، پیچیدگی مدیریت و عدم مقیاس‌پذیری که در هانی‌پات‌ها وجود دارد را حذف کرده‌اند تا شرکت‌ها (اعم از کوچک و بزرگ) بتوانند محیط‌های فریب را به‌راحتی در سراسر شبکه‌های ابری و داخلی مستقر و مدیریت کنند. با توجه به مختصات برشمرده شده برای تکنیک فریب، پروژه در حال اجرا، بر شناسایی و توسعه سکوهای فریب تمرکز داشته و همزمان امکان‌سنجی، تله‌گذاری برای سناریوهای حمله مبتنی بر تکنیک‌های مایتره با استفاده از قابلیت‌های این سکوها در دست انجام است. امیدواریم فرآورده‌های حاصل از این راهبرد پژوهشی، دستاورد مطلوبی در راستای تاب‌آوری نظام بانکی باشد.

اینفوگرافی: سامانه سهند

اینفوگرافی: سامانه سرابان کاشف

مقاله

امنیت و حریم خصوصی در سیستم‌های مبتنی بر یادگیری ماشین

حمید هرس‌مالی
کارشناس گروه پایش و کنترل مخاطرات شرکت کاشف

سیستم‌های نرم‌افزاری در معرض انواع حملات امنیتی قرار دارند و تلاش‌ها برای ایمن‌کردن سیستم‌های نرم‌افزاری از یک طرف و از طرف دیگر تلاش‌ها برای شکستن این اقدامات امنیتی از سابقه تاریخی طولانی برخوردار است. از جمله این اقدامات می‌توان به موارد زیر اشاره کرد: عوامل مخرب سعی می‌کنند به اطلاعات خصوصی دسترسی پیدا کنند (حمله محرمانه)، ممکن است سعی کنند داده‌ها یا خروجی‌های سیستم را دستکاری کنند (حمله یکپارچگی) یا ممکن است به سادگی کل سیستم را از بین ببرند (حمله در دسترس بودن).

با به‌کارگیری یادگیری ماشین در سامانه‌های نرم‌افزاری، ما با نگرانی‌های امنیتی بیشتری روبرو هستیم، زیرا باید نگران داده‌ها (داده‌های آموزشی، داده‌های استنتاج، هایپرپارامترها) و مدل‌ها باشیم.

همچنین علاوه بر نگرانی‌های معمول حفظ حریم خصوصی که در سامانه‌های نرم‌افزاری وجود دارد، یادگیری ماشین تهدیدات حریم خصوصی جدیدی را معرفی می‌کند. مدل‌ها ممکن است اطلاعات خصوصی را از مقادیر زیادی داده‌های خام استنتاج کنند، برای مثال مدل‌های یادگیری ماشین در شرکت‌های تجارت الکترونیک که وضعیت سلامت مشتری را از داده‌های خرید از داروخانه یا مراکز درمانی پیش‌بینی می‌کنند بدون اینکه مشتری اطلاعاتی در مورد وضعیت سلامتی خود اظهار کرده باشد.

الزامات امنیتی در سیستم‌های مبتنی بر یادگیری ماشین؛ برای یک پروژه خاص، الزامات امنیتی آنچه از یک پروژه انتظار می‌رود را تعریف می‌کند، معنای ایمن بودن ممکن است بین پروژه‌ها متفاوت باشد.

■ **الزامات محرمانگی:** محرمانگی در مورد کنترل دسترسی به اطلاعات است، محرمانه بودن به سادگی نشان می‌دهد که داده‌های حساس فقط توسط افرادی که مجاز به استفاده از آن هستند قابل دسترسی باشند.

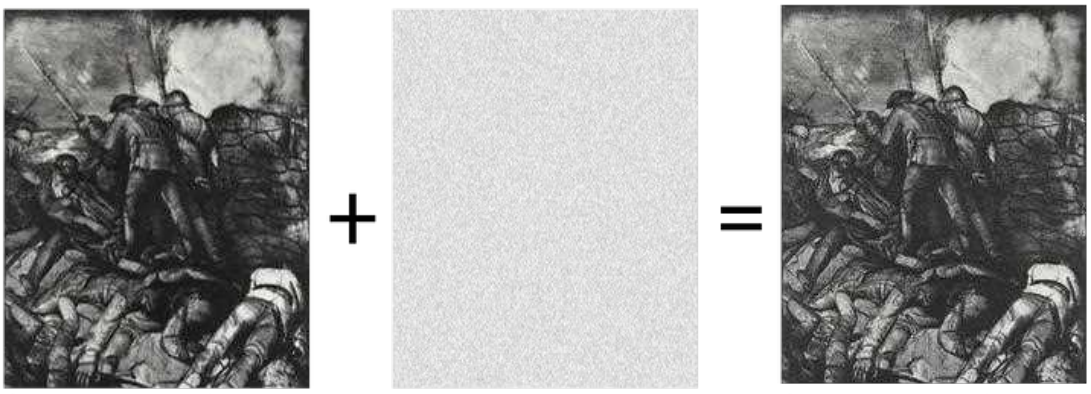
در تنظیمات یادگیری ماشین، ممکن است لازم باشد در نظر بگیریم که چه کسی قرار است به داده‌های آموزشی، مدل‌ها و داده‌های استنتاج و تله‌متری دسترسی داشته باشد.

■ **الزامات یکپارچگی:** یکپارچگی به معنی محدود کردن ایجاد و اصلاح اطلاعات به کسانی است، که مجاز به انجام این کار هستند. با وجود یادگیری ماشین، دوباره باید نگران داده‌های آموزشی، مدل‌ها و داده‌های استنتاج و تله‌متری باشیم. به عنوان مثال، ممکن است بخواهیم مطمئن شویم که فقط توسعه‌دهندگان در تیم مرتبط مجاز به تغییر مدل مورد استفاده هستند.

■ **الزامات در دسترس بودن:** کاربران مخرب ممکن است سعی کنند کل سیستم را از کار بیاندازند یا آن را آنقدر کند یا نادرست کنند که اساساً بی‌فایده شود و احتمالاً خدمات مهمی که کاربران به آنها متکی هستند متوقف کنند. با وجود یادگیری ماشین، عوامل مخرب ممکن است خدمات مرتبط با استنتاج مدل را به منظور کندکردن یا از دسترس خارج کردن آن مورد هدف قرار دهند. همچنین ممکن است سعی کنند دقت مدل را تا حدی کاهش دهند که خروجی مدل قابلیت به کارگیری را نداشته باشد.

انواع حملات مرتبط با یادگیری ماشین و راه‌های مقابله با آن

در حالی که امنیت در یک سیستم نرم‌افزاری مهم و چالش‌برانگیز است، یادگیری ماشین استراتژی‌های حمله جدیدی را معرفی می‌کند. چهار حمله رایج را مورد بحث قرار می‌دهیم.



شکل ۱:

حملات فرار(Evasion attacks) یا نمونه‌های متخاصم (adversarial exam-ples)

متداول‌ترین حمله مورد بحث روی مدل‌های یادگیری ماشین، حملات فرار است که معمولاً به عنوان نمونه‌های متخاصم شناخته می‌شوند. به طور خلاصه، در یک حمله فرار، مهاجم ورودی (داده‌های استنتاج برای مدل) را طوری ایجاد می‌کند که مدل در زمان استنتاج یک پیش‌بینی دلخواه را تولید کند. معمولاً ورودی به گونه‌ای ساخته می‌شود که برای یک ناظر انسانی بدون مشکل به‌نظرمی‌رسد، اما مدل را به یک پیش‌بینی «اشتباه» فریب می‌دهد. حملات فرار اغلب برای دور زدن الزامات امنیتی یکپارچگی به‌کارگرفته می‌شود.

شکل ۱ مثالی از حمله خصمانه به مدلی که تصاویر خشونت را در نقاشی تشخیص می‌دهد، جایی که نویز به سختی قابل درک به ورودی اضافه می‌شود، نتیجه پیش‌بینی را تغییر می‌دهد. استراتژی‌های متعددی برای دشوارتر کردن حملات فرار وجود دارد.

- **بهبود مرز تصمیم‌گیری:** هر چیزی که مرز تصمیم مدل را بهبود بخشد، در وهله اول فرصت نمونه‌های متخاصم را کاهش می‌دهد. این امر شامل جمع‌آوری داده‌های آموزشی بهتر و ارزیابی مدل برای یادگیری میانبر است.
- **آموزش با نمونه‌های متخاصم:** از مثال‌های خصمانه برای سخت‌ترکردن مدل و بهبود مرزهای تصمیم‌گیری استفاده کنید. یک استراتژی متداول این است که نمونه‌های متخاصم را جستجو کنید که معمولاً با داده‌های آموزشی یا داده‌های تله‌متری به عنوان نقطه آغاز شروع می‌شود و نمونه‌های متخاصم یافت شده را با برچسب‌های صحیح به داده‌های آموزشی اضافه می‌کنید. به این ترتیب، داده‌های آموزشی را در نزدیکی مرز تصمیم‌گیری به صورت تدریجی اصلاح می‌کنیم.
- **تصفیه ورودی:** در برخی موارد، می‌توان از دانش دامنه (یا اطلاعات حملات گذشته) برای شناسایی بخش‌هایی از فضای ورودی که به مسأله بی‌ربط هستند و می‌توانند در زمان آموزش و استنتاج پاکسازی شوند، استفاده کرد.
- **محدود کردن دسترسی به مدل:** محدودکردن دسترسی به مدل، محدود کردن تعداد درخواست‌های استنتاج، و عدم ارائه امتیاز اطمینان (دقیق) همگی باعث می‌شوند جستجو برای حملات خصمانه هزینه بیشتری داشته باشد. در حالی که برخی از حملات هنوز امکان‌پذیر است، به جای جستجوی بسیار کارآمد در شیب مدل، عوامل مخرب ممکن است مجبور باشند به نمونه‌های کمی برای یادگیری و حملات کمی برای امتحان کردن تکیه کنند.
- **مدل‌های اضافی:** مدل‌های چندگانه کمتر احتمال دارد که مرزهای تصمیم‌گیری مشابهی را که مستعد نمونه‌های متخاصم یکسان هستند، بیاموزند. ممکن است فریب چندین مدل به طور همزمان برای عوامل مخرب گران‌تر شود و اختلاف بین پیش‌بینی‌های مدل ممکن است ما را نسبت به پیش‌بینی‌های غیرقابل اعتماد و حملات خصمانه احتمالی آگاه کند.
- **اطلاعات اضافی:** در برخی از سناریوها، اطلاعات را می‌توان به صورت اضافی رمزگذاری کرد و حمله به مدل‌ها برای هر کدگذاری همزمان را دشوارتر می‌کند.
- **بررسی استحکام:** بررسی‌های استحکام در زمان استنتاج می‌تواند ارزیابی کند که آیا ورودی دریافتی بسیار نزدیک به مرز تصمیم است و بنابراین ممکن است یک حمله باشد.

همه این رویکردها می‌توانند یک مدل را سخت‌تر و حملات را دشوارتر کنند، اما با توجه به فقدان مشخصات در یادگیری ماشین، هیچ رویکردی نمی‌تواند به طور کامل از پیش‌بینی‌های اشتباهی که ممکن است در حملات خصمانه مورد سوءاستفاده قرار گیرند، جلوگیری کند. هنگام در نظر گرفتن امنیت، مهندسان باید تصمیمات مبادله‌ای دشواری بین امنیت و دقت، بین امنیت و هزینه آموزش، بین امنیت و هزینه استنتاج، بین امنیت و مزایای ارائه شده به کاربران و غیره اتخاذ کنند.

حملات مسمومیت(Poisoning attacks)

حملات مسمومیت، حملات غیرمستقیم به یک سیستم شامل مدل یادگیری ماشین هستند که سعی در تغییر مدل با دستکاری داده‌های آموزشی دارند. حملات مسمومیت غیرهدفمند سعی می‌کنند پیش‌بینی مدل را با استفاده از داده‌های آموزشی تولیدشده نادرست نشان دهند و الزامات در دسترس بودن را زیر پا بگذارند. در مقابل، حملات مسمومیت هدفمند با هدف دستکاری مدل برای دستیابی به یک پیش‌بینی مطلوب (یک برچسب خاص) برای ورودی هدفمند خاص انجام می‌گیرد، اساساً ایجاد یک درب پشتی و شکستن الزامات یکپارچگی را به دنبال دارد.

راه‌های مقابله

متداول‌ترین دفاع در برابر حملات مسمومیت بر روی شناسایی و حذف موارد پرت در داده‌های آموزشی و شناسایی برچسب‌های نادرست متمرکز است. با این حال، دفاع باید کل سیستم و نحوه جریان داده‌ها در داخل سیستم، و اینکه چه داده‌هایی می‌تواند مورد دسترسی یا تحت تأثیر عوامل مخرب قرار گیرد را در نظر بگیرد. این مهم است (الف) زمانی که کاربران می‌توانند مستقیماً بر داده‌ها تأثیر بگذارند، مثلاً با بارگذاری یا گزارش محتوا، و (ب) زمانی که اطلاعات به طور غیرمستقیم از رفتار کاربر جمع آوری می‌شود. به طور کلی مکانیسم‌های دفاعی زیادی وجود دارد، از جمله:

- **بهبود استحکام برای نقاط پرت**
- **بررسی مجموعه داده‌های خارجی**

- **افزایش اعتماد به داده‌ها و برچسب‌های آموزشی**
- **مخفی‌کردن و ایمن‌کردن موارد داخلی**
- **منشأ ردیابی**

حملات استخراج مدل

محرمانه نگه‌داشتن مدل‌ها دشوار است. هنگامی که به کاربران اجازه می‌دهد از طریق یک API با مدل تعامل داشته باشند، عوامل مخرب می‌توانند به سادگی با پرس‌وجوی مکرر مدل، اطلاعات زیادی درباره مدل استخراج کنند. با پرس‌وجوهای کافی، مهاجم می‌تواند یک مدل جایگزین در نتایج پیش‌بینی‌شده بیاموزد که ممکن است با دقت مشابهی عمل کند. این مدل دزدیده شده ممکن است سپس در محصولات خود مورد استفاده قرار گیرد یا ممکن است به عنوان پایه‌ای برای انجام حملات فرار یا مسمومیت یا کارآمدتر استفاده شود.

راه‌های مقابله

سرقت مدل را می‌توان با محدود کردن نحوه پرس‌وجو کردن مدل سخت‌تر کرد. اگر یک مدل فقط به صورت داخلی در یک محصول استفاده شود، جستجو و مشاهده برای عوامل مخرب دشوارتر است. اگر پیش‌بینی‌های مدل قبل از نمایش نتایج به کاربران به‌شدت پردازش شوند عوامل مخرب فقط می‌توانند در مورد رفتار کلی سیستم بیاموزند، اما ممکن است زمان سخت‌تری برای شناسایی رفتار خاص مدل داخلی داشته باشند.

وارونگی مدل و حملات استنتاج عضویت

هنگامی که عوامل مخرب به یک مدل دسترسی دارند، می‌توانند سعی کنند اطلاعات را از داده‌های آموزشی با حملات وارونگی مدل و حملات استنتاج عضویت استخراج کنند و الزامات محرمانگی را زیر پا بگذارند. از آنجایی که مدل‌ها اغلب بر روی داده‌های خصوصی آموزش می‌بینند، عوامل مخرب ممکن است قادر به سرقت اطلاعات باشند، هدف یک حمله وارونگی مدل بازسازی داده‌های آموزشی مرتبط با یک پیش‌بینی خاص است.

راه‌های مقابله

راه‌های مقابله در برابر حملات وارونگی مدل و حملات استنتاج عضویت معمولاً بر کاهش بیش از حد برازش در طول آموزش مدل، اضافه کردن نویز به امتیازات اطمینان پس از استنتاج و الگوریتم‌های یادگیری ماشین جدید که تضمین‌های حریم خصوصی (محدود) خاصی را ایجاد می‌کنند، متمرکز است. از آنجایی که این حملات با استفاده از تعداد پرس‌وجوهای زیاد از مدل متکی هستند، باز هم طراحان سیستم می‌توانند از استراتژی هایی مانند محدود کردن نرخ و شناسایی سوءاستفاده برای افزایش هزینه مهاجم استفاده کنند.

حفظ حریم خصوصی داده‌ها در سیستم‌های مبتنی بر یادگیری ماشین

حفظ حریم خصوصی به توانایی یک فرد یا گروه برای کنترل اطلاعات مربوط به آنها و نحوه استفاده از اطلاعات مشترک اشاره دارد. در سیستم‌های نرم‌افزاری، حریم خصوصی معمولاً به این بستگی دارد که کاربران انتخاب می‌کنند چه اطلاعاتی را با سیستم نرم‌افزاری به اشتراک بگذارند و تصمیم می‌گیرند که چگونه سیستم می‌تواند از آن اطلاعات استفاده کند. بسیاری از حوزه‌های قضایی درجاتی از حریم خصوصی را به عنوان یک حق مدون معرفی می‌کنند، یعنی کاربران باید انتخاب‌های خاصی را در مورد اینکه چه اطلاعاتی به اشتراک گذاشته می‌شود و چگونه استفاده می‌شود، حفظ کنند. در عمل، سیستم‌های نرم‌افزاری اغلب با درخواست یا الزام آنها به موافقت با سیاست‌های حفظ حریم خصوصی به عنوان شرط استفاده از سیستم، مجوزهای گسترده‌ای را از کاربران درخواست می‌کنند.

حریم خصوصی با امنیت مرتبط است، اما برابر نیست. حریم خصوصی به این موضوع مربوط می‌شود که آیا اطلاعات به اشتراک گذاشته می‌شوند یا نه و برای اطمینان از اینکه اطلاعات فقط به صورت مورد نظر استفاده می‌شود، به امنیت نیاز است. به عنوان مثال، راه‌های مقابله‌ی امنیتی مانند کنترل دسترسی و رمزگذاری داده‌ها کمک می‌کند تا اطمینان حاصل شود که اطلاعات توسط بازیگران غیرمجاز خوانده و استفاده نمی‌شود. در حالی که امنیت برای دستیابی به حریم خصوصی لازم است، کافی نیست: یک سیستم می‌تواند از طریق اقدامات خود وعده‌های حفظ حریم خصوصی را زیر پا بگذارد، بدون اینکه عوامل مخرب دفاع امنیتی را برای افشای اطلاعات محرمانه زیرپا بگذارند.

تهدیدات حریم خصوصی ناشی از یادگیری ماشین

یادگیری ماشین در پیش‌بینی اطلاعات از داده‌های خام که برای هدف دیگری به اشتراک گذاشته شده‌اند، قدرتمند است. برای مثال، الگوریتم‌های یادگیری ماشین می‌توانند سن، جنسیت، نژاد و گرایش سیاسی احتمالی را از طریق چند عبارت جستجو یا پست در سایت اشتراک‌گذاری تصویر اجتماعی ما پیش‌بینی کند. علاوه بر این، یادگیری ماشین می‌تواند محرمانه نگه‌داشتن داده‌ها را بسیار چالش برانگیز کند،

> محدود کردن دسترسی به مدل، محدود کردن تعداد درخواست‌های استنتاج، و عدم ارائه امتیاز اطمینان (دقیق) همگی باعث می‌شوند جستجو برای حملات خصمانه هزینه بیشتری داشته باشد. در حالی که برخی از حملات هنوز امکان پذیر است، به جای جستجوی بسیار کارآمد در شیب مدل، عوامل مخرب ممکن است مجبور باشند به نمونه های کمی برای یادگیری و حملات کمی برای امتحان کردن تکیه کنند

بنابراین سیستم را به روی تهدیدات امنیتی جدید باز می‌کند: داده‌ها در مکان‌های اضافی ذخیره می‌شوند و توسط فرآیندهای مختلف پردازش می‌شوند، که همه آنها ممکن است مورد حمله قرار گیرند، و مدل‌ها می‌توانند داده‌های آموزشی را به خاطر بسپارند و حملات وارونگی مدل می‌توانند داده‌های آموزشی را استخراج کنند. بنابراین سیستم را به روی تهدیدات امنیتی جدید باز می‌کند: داده‌ها در مکان‌های اضافی ذخیره می‌شوند و توسط فرآیندهای مختلف پردازش می‌شوند، که همه آنها ممکن است مورد حمله قرار گیرند و مدل‌ها می‌توانند داده های آموزشی را به خاطر بسپارند و حملات وارونگی مدل می‌توانند داده‌های آموزشی را استخراج کنند.

> برخی از قوانین اخیر حفظ حریم خصوصی، مانند GDPR در اتحادیه اروپا، مجازات‌های قابل توجهی را برای نقض‌هایی که توسعه‌دهندگان شروع به جدی گرفتن می‌کنند، تهدید می‌کند

سیاست‌های حفظ حریم خصوصی

خط مشی حفظ حریم خصوصی سندی است که توضیح می‌دهد چه اطلاعاتی توسط یک سیستم نرم‌افزاری جمع آوری می‌شود و چگونه می‌توان از اطلاعات جمع‌آوری شده استفاده و به اشتراک گذاشت. به نوعی، این مستندات عمومی از تصمیمات حفظ حریم خصوصی در سیستم است. در حالت ایده‌آل، یک خط‌مشی حفظ حریم خصوصی به کاربر اجازه می‌دهد تا در مورد استفاده از یک سرویس و موافقت با قوانین جمع‌آوری، پردازش و اشتراک‌گذاری داده‌ها مشورت کند. فراتر از خط‌مشی‌های گسترده حریم خصوصی، یک سیستم ممکن است کنترل‌های حریم خصوصی کاربر را نیز در اختیار کاربر بگذارد تا بتوانند تصمیمات دقیق‌تری در مورد نحوه استفاده از داده‌های خود بگیرند.

به طور کلی، اخیراً تلاش‌هایی برای تنظیم حریم خصوصی نسبت به تنظیم بسیاری از حوزه‌های دیگر مهندسی مسئول، مانند انصاف و شفافیت وجود دارد. علاوه بر این، برخی از قوانین اخیر حفظ حریم خصوصی، مانند GDPR در اتحادیه اروپا، مجازات‌های قابل توجهی را برای نقض‌هایی که توسعه‌دهندگان شروع به جدی گرفتن می‌کنند، تهدید می‌کند. با این حال، فراتر از انطباق اولیه با حداقل مقررات قانون، ما دوباره باید به مهندسان مسئول برای محدود کردن جمع‌آوری و اشتراک‌گذاری داده‌ها به آنچه ضروری است، برای انتقال شفاف خط‌مشی‌های حفظ حریم خصوصی و ارائه کنترل‌های معنادار حریم خصوصی با پیش‌فرض‌های معقول تکیه کنیم. حفظ حریم خصوصی پیچیده است و ارزیابی ریسک‌های حریم خصوصی زمانی که خطرات ناشی از جریان‌های داده ناشناخته در یک سیستم، از جمع‌آوری داده‌ها از منابع مختلف، استنباط‌های انجام‌شده با مدل‌های یادگیری ماشین، یا از دفاع امنیتی ضعیف در سیستم به وجود می‌آیند، می‌تواند دشوار باشد.

روش‌های حفظ حریم خصوصی در یادگیری ماشین

رویکردهای رمزنگاری

(Cryptographic Approaches): این تکنیک شامل استفاده از الگوریتم‌های رمزنگاری برای رمزنگاری داده‌های حساس است. با اعمال رمزنگاری، داده‌های حساس به صورت رمزنگاری شده ذخیره می‌شوند و تنها کسانی که دارای کلید رمزنگاری هستند، قادر به بازگشایی داده‌ها می‌شوند.

رمزگذاری هممورفی

(Homomorphic Encryption): رمزگذاری کاملاً هممورفیک، محاسبات روی داده‌های رمزگذاری شده را با عملیاتی مانند جمع و ضرب، که می‌تواند به عنوان پایه‌ای برای توابع دلخواه پیچیده‌تر مورد استفاده قرار گیرد، امکان پذیر می‌کند.

مدارهای مخدوش (Garbled Circuits):

با فرض یک راه‌اندازی دوطرفه بین دو نفر که می‌خواهند نتیجه یک تابع محاسبه شده روی ورودی‌های خصوصی آنها را به دست آورند، نفر اول می‌تواند تابع را به یک مدار درهم تبدیل کند و این مدار را همراه با ورودی مخدوش خود ارسال کند. نفر دوم نسخه مخدوش ورودی خود را از نفر اول دریافت می‌کند بدون اینکه او چیزی در مورد ورودی خصوصی نفر دوم بداند (مثلاً با استفاده از انتقال فراموشی). نفر دوم اکنون می‌تواند از ورودی مخدوش خود با مدار درهم استفاده کند تا نتیجه تابع مورد نیاز را به دست آورد (و می‌تواند به صورت اختیاری آن را با نفر اول به اشتراک بگذارد).

پردازنده‌های امن (Secure Processors):

ایده اصلی شامل همکاری چندین مالک داده برای انجام یکی از وظایف یادگیری ماشین با سرور محاسباتی است که وظیفه یادگیری ماشین را روی یک مرکز داده دارای SGX فعال می‌کند.

رویکردهای درهم‌سازی

(Perturbation Approaches): این روش شامل محو کردن یا جایگزینی داده‌های حساس با داده‌های غیرحساس است. به عنوان مثال، جایگزین کردن نام افراد با نام‌های جعلی یا حذف اطلاعات شناسایی شخصی می‌تواند به حفظ حریم خصوصی کمک کند.

حریم خصوصی تفاضلی

Differential Privacy (DP): تضمین می‌کند که هر دنباله‌ای از خروجی‌ها (پاسخ به پرس‌وجوها) اساساً به یک اندازه احتمال دارد اتفاق بیفتد، خواه رکورد خاصی در مجموعه داده گنجانده شده باشد یا نه.

داده‌های حریم خصوصی محلی

(Local DP): هنگامی که طرف‌های ورودی اطلاعات کافی برای آموزش یک مدل یادگیری ماشین ندارند، ممکن است بهتر باشد از رویکردهایی استفاده شود که به DP محلی (LDP) متکی هستند. با LDP، هر طرف ورودی داده‌های خود را مختل می‌کند و فقط این نمای مبهم از داده‌ها را منتشر می‌کند.

کاهش داده (DR)

: DR با بازنمایی داده‌ها به یک ابر صفحه با ابعاد پایین‌تر حریم خصوصی را افزایش می‌دهد. چنین تبدیلی زیان‌بار است زیرا بازیابی داده‌های اصلی دقیق از یک نسخه با ابعاد کاهش‌یافته ممکن نیست.

منابع

Boulemtafes, A., Derhab, A., & Challal, Y. (2020). A review of privacy-preserving techniques for deep learning. Neurocomputing, 384, 21-45.

Mohassel, Payman, and Yupeng Zhang. "Secureml: A system for scalable privacy-preserving machine learning." In 2017 IEEE symposium on security and privacy (SP), pp. 19-38. IEEE, 2017.

Xu, R., Baracaldo, N., & Joshi, J. (2021). Privacy-preserving machine learning: Methods, challenges and directions. arXiv preprint arXiv:2108.04417.

Al-Rubaie, M., & Chang, J. M. (2019). Privacy-preserving machine learning: Threats and solutions. IEEE Security & Privacy, 17(2), 49-58.

Xu, K., Yue, H., Guo, L., Guo, Y., & Fang, Y. (2015, June). Privacy-preserving machine learning algorithms for big data systems. In 2015 IEEE 35th international conference on distributed computing systems (pp. 318-327). IEEE.

J. Morris Chang, Di Zhuang, G. Samaraweera, G. Dumindu Samaraweera. Privacy-Preserving Machine Learning. book 2023

مجمع شرکت کاشف برگزار شد

با برگزاری جلسه مجمع عمومی صاحبان سهام شرکت کاشف برای سال مالی منتهی به آذر ۱۴۰۲، کلیه صورت‌های مالی این شرکت مورد تائید و تصویب قرار گرفت.

به گزارش روابط عمومی شرکت کاشف، در مجمع عمومی عادی سالانه این شرکت که با حضور کلیه سهامداران و نمایندگان بانک مرکزی در دی ماه برگزار شد، صورت‌های مالی و عملکرد این شرکت تصویب شد و ترکیب حقوقی جدید هیأت مدیره شرکت کاشف نیز پس از رأی‌گیری در این خصوص، مورد تصویب قرار گرفت.

در ابتدای این جلسه دکتر ماهیار که به عنوان نماینده شرکت ملی انفورماتیک ریاست مجمع را برعهده داشت، در بیاناتی ضمن تقدیر از اقدامات انجام شده، بر عملیاتی کردن برنامه‌های شرکت کاشف و توسعه آن تاکید کرد. دکتر قرایی، مدیرعامل شرکت کاشف نیز در این جلسه ضمن ارائه گزارش اقدامات و پیشرفت پروژه‌های شرکت کاشف تصریح کرد: در یکسال گذشته با تلاش و همکاری مدیران و همکاران، برنامه‌های جدیدی در راستای تحقق اهداف و انتظارات شرکت ملی انفورماتیک و بانک مرکزی در شرکت کاشف، تدوین و پیاده‌سازی شده است.

تقدیر بانک مرکزی از شرکت کاشف

بانک مرکزی از اقدامات شرکت کاشف برای پیاده‌سازی حداقل الزامات امنیتی در صرافی‌ها و برگزاری دوره‌های آموزشی مؤثر تقدیر کرد.

به گزارش روابط عمومی کاشف، اداره امنیت بانک مرکزی جمهوری اسلامی طی نامه‌ای به مدیرعامل کاشف از «عملکرد مطلوب و دقت نظر همکاران آن شرکت در خصوص حداقل الزامات امنیتی در صرافی‌ها و برگزاری همایش‌های آموزشی و رفع ابهامات موجود» تقدیر و تشکر کرد. در این نامه اظهار امیدواری شده است «در پرتو عنایت حق تعالی و تلاش و اهتمام آن مدیریت، گامی مؤثر در جهت بهبود و ارتقای امنیت در نظام بانکی کشور برداشته شود.»

تقدیر بانک مرکزی از شرکت کاشف

گفتنی است که پروژه «تدوین دستورالعمل امن‌سازی صرافی‌ها» از ۱۴۰۱ تا آغاز سال ۱۴۰۲ در واحد نظارت کاشف به انجام رسید.

همچنین، پروژه دیگری در همین زمینه با عنوان «اجرای دستورالعمل امن‌سازی و راه‌اندازی سامانه مدیریت آسیب‌پذیری در صرافی‌ها» از اوایل امسال (۱۴۰۲) در حال اجرا است و با تقدیر بانک مرکزی روبه‌رو شده است.

«پادکشف» صدای اختصاصی شرکت کاشف منتشر شد

شرکت کاشف یکی از مسئولیت‌های خود را ارتقای سطح دانش عمومی برای استفاده امن از ابزارها و خدمات بانکداری و پرداخت الکترونیکی می‌داند. در همین راستا از «پادکست» ابزار ارتباطی محبوب سالهای اخیر برای آگاهی بخشی و انتقال دانش به طیف‌های مختلف جامعه بهره برده است. با همین هدف اپیزود صفر «پادکشف » منتشر شد و متعاقب استقبال خوب از آن در شبکه تلگرامی کاشف، برآن شدیم تا با تلاش بیشتر جهت ارتقا سطح کار اپیزود اول را با عنوان «امنیت نرم‌افزارهای بانکی» تولید کنیم. زین پس شما در کست باکس می‌توانید پادکشف را بشنوید و از اطلاعات روز دنیا در حوزه امنیت بانکداری آگاه شوید.

پادکَشف
پادکست اختصاصی شرکت کاشف

گزیده‌خبرهای زمستان

دبیرکل بانک مرکزی در بازدید از کاشف:

خدمات‌وسرویسهای کاشف به‌نظام‌بانکی،قابل‌توجه‌وشایسته‌قدردانی است

دبیر کل بانک مرکزی با حضور در شرکت کاشف از نزدیک در جریان اقدامات، برنامه‌ها و امکانات این شرکت در راستای حفظ و ارتقای امنیت بسترهای بانکی و پرداختی کشور قرار گرفت.

به گزارش روابط عمومی کاشف، دکتر محمد طالبی در این بازدید که با همراهی امین مهاجر مدیر ارشد امنیت بانک مرکزی و علیرضا ماهیار مدیرعامل شرکت ملی انفورماتیک صورت گرفت، اقدامات انجام گرفته توسط نیروهای متخصص کاشف را در ارتقای سطح امنیت حوزه بانکی بسیار مؤثر دانست و گفت: کشور ما از نظر زیرساخت‌های بانکداری و پرداخت الکترونیکی خوشبختانه در منطقه و حتی نسبت به بسیاری از کشورهای دنیا در جایگاه قابل تأملی برخوردار است و با وجود همه محدودیت‌های موجود، فاصله چندانی با استانداردهای بین‌المللی ندارد.

دکترطالبی با بیان اینکه کاشف کار سخت و چندجانبه‌ای را در صیانت از شبکه بانکداری و پرداخت الکترونیک کشور، بر دوش دارد گفت: بخش‌هایی مانند نظارت‌های دوره‌ای، تست‌های ارزیابی و انطباق‌سنجی، بسیار مهم‌اند و قادرند همانند سد و دژ محکمی در مقابله با تهدیدات و رخدادهای امنیتی در نظام پولی کشور باشند.

شرکت‌ملی‌انفورماتیک‌درگروه‌رایانه‌وفعالیت‌های‌وابسته‌اول‌شد

به گزارش روابط عمومی شرکت ملی انفورماتیک، این شرکت در همایش رتبه بندی شرکت‌های برتر ایران IMI100 در گروه رایانه و فعالیت‌های وابسته موفق به کسب رتبه نخست شد.

سازمان مدیریت صنعتی در سال ۱۴۰۲ برای بیست و ششمین سال متوالی شرکت‌های برتر ایران را رتبه‌بندی کرد. در این رتبه‌بندی ۵۰۰ شرکت بزرگ و موثر در اقتصاد کشور طی همایشی که در دوم بهمن ماه سال برگزار شد، معرفی شدند.

رتبه‌بندی IMI100 در سال نخست (۱۳۷۷) با رتبه‌بندی ۱۰۰ شرکت برتر ایران از نظر شاخص میزان فروش (درآمد) آغاز شد و در سال‌های بعد از آن با توجه به استقبال خوب شرکت‌ها و برای پاسخگویی به درخواست آنها، به تدریج تعداد شرکت‌های فهرست به ۵۰۰ شرکت افزایش یافت. همچنین تعداد شاخص‌های مورد بررسی نیز به ۳۳ شاخص افزایش یافت.

مقاله

مدیریت پروژه‌های امنیت اطلاعات بر اساس تطبیق PMBOK و استانداردهای حوزه امنیت اطلاعات

یاسر خرمشاهی
کارشناس برنامه‌ریزی و مدیریت پروژه شرکت کاشف

مدیریت پروژه های امنیت اطلاعات

یکی از عوامل مهم موفقیت در ابعاد مختلف پروژه‌های سازمانی، استفاده اثربخش و کارا، از فرآیند مدیریت پروژه است. استقرار نظام جامع و عملیاتی مدیریت پروژه، مسیری است که در جهت اتخاذ تصمیمات مدیریتی و کاهش هزینه‌ها و بهبود کیفیت و ایجاد سیاست‌های متناسب با پـروژه، افزایش بهره‌وری منابع انسانی و تسهیل ارتباط میان ذینفعان و مجریان طرح‌ها قرار دارد. موفقیت یک پروژه امنیت اطلاعات نیز مستلزم یک رویکرد مدیریتی مستمر و منظم است. مدیریت پروژه امنیت اطلاعات از طریق ساختار PMO، جریان‌های اطلاعاتی و روندهای مدیریتی را ایجاد می‌کند که به CISO اجـازه می‌دهد تا به سمت نقشی استراتژیک‌تر حرکت کند و به جای فعالیت مداوم در حالت بحران، بر بهبود مستمر تمرکز کند. مدیریت مناسب در این نوع پروژه‌ها می‌تواند تا حد زیادی در کاهش مشکلات پروژه نقش داشته باشد.

ضرورت به‌کارگیری استانداردها

استفاده از استانداردها، راهنماها و متدولوژی‌های معتبر برای همزبانی افراد درگیر در پروژه و اطمینان از اجرای درست اقدامی ضروری است. بکارگیری این استانداردها، افراد داخل پروژه را در اجرای پروژه و پیشبرد اهداف آن یاری نموده و سازمان را به یک نظام هماهنگ و یکپارچه مبدل می‌کند.

مدیریت پروژه های امنیت اطلاعات بر اساس استانداردها

در مدل تهیه شده جهت مدیریت پروژه‌های امنیت اطلاعات بر اساس استاندارد PMBOK با توجه به مشخصات پروژه‌ها و فرآیندهای وابسته به این نوع پروژه‌ها، چهار فرآیند تعیین نیازها و انتظارات مشتری، طرح‌ریزی جریان‌های کاری، کارگروهی و در نهایت ارزیابی و اختتام کار در نظر گرفته شده است که کلیه این فرآیندها با یکدیگر مرتبط می‌باشند. طبق بررسی‌های به‌عمل آمده فرایند مدیریت پروژه امنیت اطلاعات را مطابق با سری ISO27000 به فلوچارت مذکور اضافه نموده و به شرح آن می‌پردازیم.

مرحله اول :

مدیریت تدارکات پروژه امنیتی:

مدیریت تدارکات در هر پروژه‌ای، کالا و خدمات مورد نیاز جهت انجام آن پروژه را از خارج از آن سازمان تامین می‌کند. در خصوص پروژه‌های امنیتی نکته در این است که این موضوع دلیلی برای ارتباط نفرات دخیل در پروژه امنیتی

فرایندهای مدیریت پروژه‌های امنیت اطلاعات	مرحله اول	فرایند تعیین نیاز ها و انتظارات مشتری	مدیریت تدارکات پروژه امنیتی مدیریت محدوده پروژه های امنیتی
	مرحله دوم	فرایند طرح ریزی جریان‌های کاری	مدیریت هزینه پروژه امنیتی مدیریت زمان پروژه امنیتی
	مرحله سوم	فرایند کار گروهی	مدیریت ریسک پروژه امنیتی مدیریت ارتباطات پروژه امنیتی مدیریت منابع انسانی پروژه
	مرحله چهارم	ارزیابی و اختتام کار	مدیریت یکپارچگی پروژه امنیتی مدیریت کیفیت پروژه امنیتی

با خارج از سازمان است. لذا شناخت و اعتماد سازمان مجری، به افـراد تدارکات بسیار ضروری است. چرا که از همین ارتباطات ساده، اطلاعات یک پروژه امنیتی می‌تواند فاش شود و بر سرنوشت آن پروژه تاثیر بگذارد. در گام اول باید نیازهایی از پروژه که می‌توان آنها را از خارج سازمان پروژه تامین کرد شناسایی شده و تعیین شود که آیا این تدارک انجام شود یا خیر؟، در صورت پاسخ مثبت چگونگی انجام باید مشخص شود، مقدار تدارک و زمان آن نیز باید معین شود. پس از آن باید برای پشتیبانی از این درخواست تدارکات، اسناد آن آماده‌سازی شوند. در گام بعدی باید از فروشندگان آتی تدارکات پیشنهادهای بهاء و طرح‌های پیشنهادی در مورد چگونگی تحقق نیازهای پروژه اخذ شود. پس از این کار باید برای انجام امور تدارکات یک منبع تدارکات در خارج از سازمان را انتخاب نمود، که برای این انتخاب باید بر اساس معیارهای مهم برای سازمان پروژه ارزیابی از منبع انجام شده و انتخاب آن صورت پذیرد. در پروژه‌های امنیتی یا پروژه‌های غیرامنیتی که کاربرد امنیتی دارند اینکه سازمان پروژه از منبع تدارکات در خارج از سازمان چه میزان شناخت دارد و چه میزان به آن اعتماد دارد یکی از اصلی‌ترین ملاک‌های ارزیابی منابع تدارکات در پروژه‌های امنیتی است. در گام نهایی باید طی روشی، اطمینان حاصل نمود که عملکرد فروشنده(منبع تدارکات) الزامات پیمان را محقق می‌سازد. و با صحت‌سنجی محصول و ثبت و به‌روزآوری سوابق به منظور انعکاس بهتر نتایج نهایی، فرآیند اجرای تدارکات را خاتمه داد.

■ مدیریت محدوده هزینه پروژه امنیتی :

مدیریت محدوده پروژه‌های امنیتی در واقع یعنی تعیین مرز اینکه چه کاری را می‌توان به شرکت‌های اقماری داد و چه کاری باید حتماً در انحصار تیم خود مجموعه امنیتی باشد. پس از اینکه با کار کارشناسی دقیق و گسترده محدوده امور مربوط به تیم خود مجموعه و شرکت‌های اقماری مشخص شد گام بعدی تصویب رسمی پروژه است که شروع کار در اینجاست. در گام بعدی، این پروژه تصویب شده باید مستندسازی شود و هریک از بخش‌های آن به تفصیل شرح داده شود. نکته اینکه هر بخش از این مستند فقط باید در اختیار کسی قرار گیرد که باید آن کار را انجام دهد و کل آن فقط باید در اختیار تیم مدیریت پروژه باشد.

در تدوین بخش‌ها باید تا حد ممکن هر بخش مستقل از دیگری باشد لیکن بخش‌ها از محدوده اصلی کار خارج نشوند تا قابل کنترل و مدیریت باشند. پس از شفاف شدن حد و مرزهای اصل پروژه و بخش‌های آن، گام بعدی پذیرفتن رسمی این محدوده‌ها توسط سازمان‌ها یا اشخاص حقوقی ذی‌نفع در پروژه است.

نتیجه این گام آن است که هریک از بخش‌های این کار امنیتی از نگاه مسئولیت‌های مختلف مورد بازبینی امنیتی قرار می‌گیرد و در صورت عدم مشکل تأیید می‌شود. در گام پایانی نوبت به اتفاقاتی می‌رسد که محدوده پروژه امنیتی را تغییر می‌دهند و آنهایی که این محدوده را تغییر نمی‌دهند. اگر یک اتفاق رخ دهد که تیم مدیریت پروژه امنیتی تأیید کند که در محدوده پروژه اثرگذار است، آنچه که تاکنون بیان شد باید از ابتدا مورد بازبینی قرار گیرد. در گام پایانی باید افرادی در جلسه تصمیم‌گیری حضور داشته باشند که در آن سازمان از مقام بالایی برخوردار باشند تا بتوانند مسئولیت و تبعات تصمیمات متخذه را بر عهده بگیرند.

مرحله دوم :

■ مدیریت هزینه پروژه امنیتی :

مدیریت هزینه پروژه‌ها در برگیرنده فرآیندهای مورد نیاز برای حصول اطمینان از تکمیل پروژه با بودجه مصوب است. حال با توجه به اینکه در تمام سازمان‌ها علاقه زیادی به کاهش هزینه‌های تمام شده هر پروژه وجود دارد، ممکن است رقیبان به روش‌های مختلف حاضر باشند حتی بخشی از یک پروژه امنیتی را رایگان انجام دهند، فقط برای اینکه درون تیم نفوذ کرده و اطلاعات کسب کنند. در مدیریت هزینه پروژه‌های امنیتی توجه به این نکته بسیار ضروری است. در این راستا باید برنامه‌ریزی کرد که چه منابعی و از هر منبع چه میزان و در چه زمانی برای انجام فعالیت‌های پروژه مورد نیاز است. در گام بعدی برای منابع مورد نیاز باید یک برآورد هزینه انجام داد تا به‌توان یک تخمین از هزینه کل پروژه را بدست آورد. سپس باید این هزینه را به تک تک فعالیت‌ها یا بسته‌های کاری جهت تشکیل مبنای هزینه برای اندازه‌گیری عملکرد پروژه شکست و به هریک تخصیص داد و پس از آن در صورت وقوع هر نوع تغییر احتمالی، باید این تغییر توسط ذی‌نفعان پروژه مورد توافق قرار گیرد و هزینه مبنای تغییر یافته تشخیص داده شود و این تغییرات واقعا در لحظه وقوع مدیریت وکنترل شوند.

■ مدیریت زمان پروژه امنیتی:

همان‌طور که می‌دانید هر کاری که در عمل به طولانی شدن زمان اجرا برخورد کرد، در حاشیه قرار خواهد گرفت و کارهای مهم‌تر از آن برای آن سازمان به وجود خواهد آمد. در این بین احتمال فاش شدن اطلاعات و اسناد پروژه به علت طولانی شدن زمان اجرا بسیار زیاد می‌شود. پس در مدیریت زمان پروژه‌های امنیتی باید از به‌وقوع پیوستن تعلل در کار جلوگیری کرد. مدیریت زمان در هر پروژه‌ای دربرگیرنده فرآیندهای مورد نیاز جهت حصول اطمینان از تکمیل به‌موقع پروژه است. برای انجام این مدیریت باید بدانیم کل پروژه شامل چه کارهایی است و هر کار نیز شامل چه بخش‌هایی است. تمام این موارد باید شناسایی شوند و مستندات آنها تولید گردد که بهترین منبع برای این کار ساختار شکست کار(WBS) است.

مرحله سوم :

■ مدیریت ریسک پروژه امنیتی:

این نوع مدیریت بر پروژه‌ها تضمین می‌کند که آثار مثبت رویدادها به میزان حداکثر، و آثار منفی آن به میزان حداقل بر پروژه تأثیر بگذارد و در آن فرآیندهایی وجود دارد تا ریسک‌های پروژه شناسایی، تحلیل و نسبت به آنها واکنش مناسب اتخاذ شود. لیکن در پروژه‌های امنیتی رویدادهایی که تأثیرگذار هستند ویژگی‌های خاصی دارند که از جمله آنها می‌توان به این مطلب اشاره کرد که باید خیلی سریع به آن رویدادها پاسخ داد و در صورت از دست دادن زمان و طولانی شدن فرآیند پاسخ دهی، پاسخ قبلی در زمان فعلی راه حل مناسبی نخواهد بود. پس سرعت عمل در واکنش مناسب به ریسکی که شناسایی شده و تحلیل مناسب روی آن انجام شده است مطلب بسیار مهمی است. شناسایی ریسک فرآیندی تکرارپذیر است که در مقاطع زمانی مختلف باید انجام شود. سپس باید ریسک‌های شناسایی شده را تحلیل کنیم تا تأثیر و شانس وقوع آنها سنجیده شود. به این وسیله ریسک‌ها را بر اساس آثار بالقوه آنها بر اهـداف پـروژه اولویت‌بندی می‌کنیم. سپس باید تحلیل عددی احتمال هر ریسک و پیامدهای آن بر اهداف پروژه را برای داشتن تحلیل کمی ریسک استخراج کنیم. در گام بعدی باید اقداماتی انجام داد تا فرصت‌ها افزایش و تهدیدها کاهش یابد و برای انجام این کار باید افراد یا قسمت‌هایی به منظور پذیرش مسئولیت هر واکنش به ریسک شناسایی و تعیین گردند. با این کار در واقع برنامه‌ریزی واکنش به ریسک را انجام داده‌ایم. این برنامه باید با شدت ریسک متناسب باشد، در مواجهه با چالش‌ها از نظر هزینه‌ای اثربخش باشد، برای موفقیت‌آمیزبودن به هنگام باشد، با توجه به شرایط پروژه واقع بینانه باشد، مورد توافق همه قسمت‌های درگیر باشد و توسط یک شخص مسئول پذیرفته شده باشد. در گام آخر باید یک کنترل و نظارت بر ریسک‌ها داشت که شامل فرآیند پیگیری ریسک‌های شناسایی شده، نظارت بر ریسک‌های باقیمانده و شناسایی ریسک‌های جدید، اطمینان از اجرای برنامه‌های ریسک و ارزیابی اثر بخشی آنها در کاهش ریسک است. آنچه واضح است اینکه حوزه مدیریت ریسک حساس‌ترین حوزه مدیریت یک پروژه امنیتی است که در صورت مدیریت صحیح نتایج مثبت پروژه و در صورت سهل‌انگاری لغو پروژه را در پی دارد.

مدیریت ارتباطات پروژه امنیتی:
مدیریت ارتباطات در پروژه‌ها تنظیم‌کننده روابط بین افراد، نظرات و اطلاعاتی است که برای موفقیت پروژه لازم هستند. حال در پروژه‌های امنیتی آنچه از این موضوع اهمیت دارد این است که اگر پازل اطلاعات ذهنی افراد پروژه در کنار یکدیگر قابلیت تکمیل شدن داشته باشد، آنگاه احتمال فاش شدن ماهیت پروژه وجود دارد که باید از وقوع آن جلوگیری کرد. در گام اول باید برای این ارتباطات برنامه‌ریزی کنیم. در گام بعدی برای آگاهی از نحوه مصرف منابع در راستای اهداف پروژه باید اطلاعات عملکردی پروژه به منظور گزارش‌دهی گردآوری شود و در نهایت باید نتایج پروژه مستندسازی شده تا محصول پروژه توسط سرمایه‌گذار پذیرش رسمی شود.

مدیریت منابع انسانی پروژه امنیتی:
در پروژه‌ها معمولاً مدیریت منابع انسانی دربرگیرنده فرآیندهایی است که برای دستیابی به اثربخش‌ترین کاربری از افراد درگیر در پروژه لازم است. آنچه که در مورد پروژه‌های امنیتی در این بخش اهمیت دارد این است که تمام تیم نیروی انسانی پروژه باید کارمندان رسمی آن سازمانی باشند که قصد اجرای یک پروژه امنیتی را دارد و در صورت ضعف در دانش فنی برای این تیم کلاس آموزشی درنظر گرفته شود. زیرا دانش فنی کار را می‌توان با کلاس آموزشی به یک نفر انتقال داد لیکن اعتماد و اطمینان به یک نیروی سازمانی، با برگزاری کلاس آموزشی تأمین نمی‌شود. برای انجام این مهم در گام اول باید اقدام به شناسایی، مستندسازی و واگذاری نقش‌ها و مسئولیت‌ها در پروژه کرد که هر کدام از آنها می‌تواند به افراد یا گروه‌های کاری واگذار شود.

مرحله چهارم:

مدیریت یکپارچگی پروژه امنیتی:
در این بخش فرآیندهایی از استاندارد PM-BOK مطرح است که اطمینان می‌دهد هماهنگی مناسبی بین عناصر مختلف پروژه امنیتی اتفاق می‌افتد. برای کنترل این هماهنگی کار را در سه بخش انجام می‌دهیم:
۱- تدوین برنامه‌ای برای این کنترل: برنامه‌ای که بتواند عناصر مختلف پروژه امنیتی را کنترل و هماهنگ کند. ۲- اجرای این برنامه: در اجرای برنامه‌های تدوین شده، دقت در اجرا ضامن کیفیت خروجی کار است. ۳- کنترل تغییرات احتمالی: در کنترل تغییرات قدم نخست تشخیص و تعیین این مطلب است که یک تغییر رخ داده است. پس از آن کنترل و مدیریت آن تغییر دارای اهمیت است و در نهایت حصول اطمینان از اینکه آن تغییر پذیرفته شده است یا خیر.

مدیریت کیفیت پروژه امنیتی:
مدیریت کیفیت پروژه‌ها دربرگیرنده فرآیندهایی است برای تأمین اطمینان اینکه نیازهایی که پروژه به خاطر آنها تعهد شده است حتماً حاصل می‌شوند. نکته مهم برای پروژه‌های امنیتی در این است که اگر کیفیت کار پایین بیاید نمی‌گوییم کار با کیفیت پایینی انجام شده. بلکه ممکن است کاهش کیفیت، کل اصل کار پروژه را لغو کند، آن هم به دلیل مسائل امنیتی. پس تأمین کیفیت پروژه در پروژه‌های امنیتی اهمیتی دو چندان دارد.

جمع بندی

هدف از این مقاله بررسی مدیریت پروژه‌های امنیت اطلاعات بر اساس استاندارد PM-BOK و استانداردهای حوزه امنیت اطلاعات بوده است. در این راستا، لزوم مدیریت خاص در این نوع پروژه‌ها، بر اساس یک استاندارد معتبر، مورد توجه قرار گرفت. لذا استاندارد مؤسسه PMI ، به عنوان بستر اصلی مورد توجه قرار گرفت. در ادامه نیز بررسی مدل مدیریتی این نوع پروژه‌ها براساس استاندارد PMBOK مشتمل بر چهار فرآیند اصلی (تعیین نیازها و انتظارات مشتری، فرآیند طرح ریزی جریان‌های کاری ، فرآیند کار گروهی و نیز فرآیند ارزیابی و اختتام کار) تدوین شد و با وارد کردن مراحل امنیت اطلاعات طبق استانداردهای سری ISO 27002 مدلی جهت مدیریت این نوع پروژه‌ها مشتمل بر ۹ فرایند جزئی بیان شد.

۱- بهترین‌ها در امنیت اطلاعات / جرج ال استفانک / ترجمه و نگارش: دکتر علیرضا پورابراهیمی ، دکتر عباس طلوعی اشلقی /انتشارات دانشگاه آزاد اسلامی واحد الکترونیکی / ۱۳۹۹

۲- آشنایی با ISMS و استانداردهای امنیتی ISO 27001 و ISO 27002 / نویسنده: حیدر علی کورنگی /۱۳۸۶

۳- راهنمای مدیریت پروژه / تألیف انجمن مدیریت پروژه PMI / مترجمین: سیدحسین اصولی، نجابت، علی بیاتی، حسین ناصری، علی افخمی شرکت/۱۳۸۴

۴- Prince آشنایی با استانداردهای جهانی مدیریت پروژه / نویسندگان: علیرضا معینی، احمد شفیعی و محمود شفیعی/ دانشگاه علم و صنعت ایران/ ۱۳۸۴ / دومین کنفرانس بین‌المللی مدیریت پروژه

۵- معرفی استانداردهای مدیریت پروژه/ نویسنده: محمد زین العابدین/پایگاه اطلاع رسانی پیمان کاری عمومی ایران/ ۱۳۹۰/ مجله تخصصی قرب

۶- مقایسه استانداردهای مدیریت پروژه در دنیا/ نویسندگان: عباس آزادی مقدم آرانی و سیدمهدی فراهانی / گروه پژوهشی آریانا/۱۳۸۶/سومین کنفرانس بین‌المللی مدیریت پروژه.

7- Risk Analysis and Security Countermeasure Selection / by Thomas L.Norman / CRC Press , Taylor & Francis Group , an informa business / 2010 / ISBN 978-1-4200-7870-1

8- ITIL V3 and Information Security / by : Jim Clinch / White Paper , 2009

9- Information Security Management Metrics : A Definitive Guide to Effective Security Monitoring and Measurement / by W.Krag Brotby , CISM / CRC Press , Taylor & Francis Group , an informa business / 2009

10- Management Information Systems : James A.O´ Brien , George M.Markas / Ninth edition / Mc Grow Hill / 2009

11- Project Management Frameworks: Comparative Analysis. Al-Maghraby, Rania. Istanbul, Turkey : s.n., Nov 2010, IPMA 2010 World Congress.

12- Comparison between ISO 21500 and PMBOK, Guide 5th Edition. Wojnar, Katarzyna. 2013, Theoretical background and practical usage of ISO 21500 in IT projects., p. 11. 34

13- Roles in information security e A survey and classification of the research area. Fuchs, L, Pernul, G and Sandhu, R. 2011, Elsevier, p. 748

14- OCLC - Project risk management,2012. Cervone, H. Frank. [ed.] mahmood madineh negah. s.l. : Systems & Services:International digital library perspectives Vol. 22 No. 4, pp. 256-262

15- Project management in the information systems and information technologies industries. Hartman, Frnacis and Rafi, Ashrafi A. 2002, Project Management Journal, p. 5

16- Project management: key tool for implementing strategy. Longman, Andrew and Mullins, Jim . 2004, Emerald, p. 55.

اینفوگرافی: چارچوب ناظر

مقاله

نگاهی اجمالی به یک چارچوب مدیریت ریسک تقلب

فریده شفیعی

کارشناس گروه پایش و کنترل مخاطرات شرکت کاشف

در عصر کنونی اغلب ارتباطات شکل دیجیتالی به خود گرفته‌اند و در شبکه بانکی نیز تراکنش‌های بسیار بیشتری روی دستگاه‌های دیجیتالی انجام می‌شود. با وجود بسیاری مزایای فوق‌العاده، پیشرفت‌های اخیر زمینه برخی مشکلات جدی همچون تقلب را نیز به همراه داشته‌اند. با توجه به فراگیری تقلب و پیامدهای منفی وابسته به آن، بحث‌هایی در زمینه سرمایه‌گذاری صحیح زمان و منابع در جهت پیشگیری و تشخیص تقلب وجود دارد.

یکی از راهبردهای استاندارد در مدیریت و مقابله با تقلب شامل پیشگیری، شناسایی و پاسخ به تقلب است (شکل ۱). تکنیک‌های پیشگیری از تقلب شامل معرفی سیاست‌ها، روش‌ها و کنترل‌های در جهت کاهش انجام تقلب و همچنین فعالیت‌هایی مانند آموزش و آگاهی از تقلب هستند، به نحوی که قادر باشیم رخداد تقلب را متوقف کنیم. در این یادداشت به مرور مفاهیم تقلب، ریسک، ریسک تقلب و الزامات کلی اصول مدیریت ریسک خواهیم پرداخت. در انتها نیز در مورد اجزای کلیدی یا یک چارچوب استاندارد مقابله با تقلب بحث خواهیم کرد.

تقلب چیست؟

براساس تعریف انجمن بازرسان خبره تقلب، هر عمل غیرقانونی که با فریب، پنهان‌کاری یا نقض اعتماد همراه باشد، را تقلب می‌نامیم. این اعمال وابسته به خشونت یا زور فیزیکی نیستند. تقلب توسط افراد و شرکت‌ها برای به‌دست آوردن پول، اموال یا خدمات، برای جلوگیری از پرداخت پول و از دست دادن خدمات، برای حفظ مزایای شخصی یا مزایای شرکتی انجام می‌شود. تقریباً تمام فعالیت‌های متقلبانه با سرقت یا فریب همراه است.

ارکان یا مثلث تقلب چیست؟

مجموعه‌ای از عوامل که در فرآیندهای متقلبانه مشترک هستند، به مثلث تقلب معروف است. مثلث تقلب براساس نظریه یک جرم‌شناس به نام دونالد کرسی در دهه ۱۹۴۰ پیشنهاد شد. کرسی تحقیقات گسترده‌ای روی تقلب انجام داده است. نتایج تحقیقات کرسی به آنچه که امروز تحت عنوان مثلث تقلب مشهور است، منتج شد. سه مؤلفه مثلث تقلب (شکل ۲) عبارت است از: انگیزه، فرصت، و توجیه‌پذیری.

مهم‌ترین انگیزه انجام تقلب را می‌توان حرص، طمع یا نیاز مالی بیان کرد. عموما فرصت انجام تقلب در سازمان‌هایی که دارای کنترل‌های داخلی ضعیف، امنیت ضعیف روی دارایی‌ها، ترس اندک از افشای آن و احتمال پایین تشخیص، یا سیاست‌های غیرشفاف در مورد رفتارهای قابل قبول دارند، بیشتر رخ می‌دهد. اگرچه بسیاری از افراد جامعه به دلیل باور به قانون، ترس از شرمنده‌شدن یا طردشدن توسط افراد دیگر جامعه از قانون پیروی می‌کنند، با این حال برخی افراد دیگر رفتارهای متقلبانه خویش را با دلایلی نظیر لزوم آن توجیه می‌کنند.

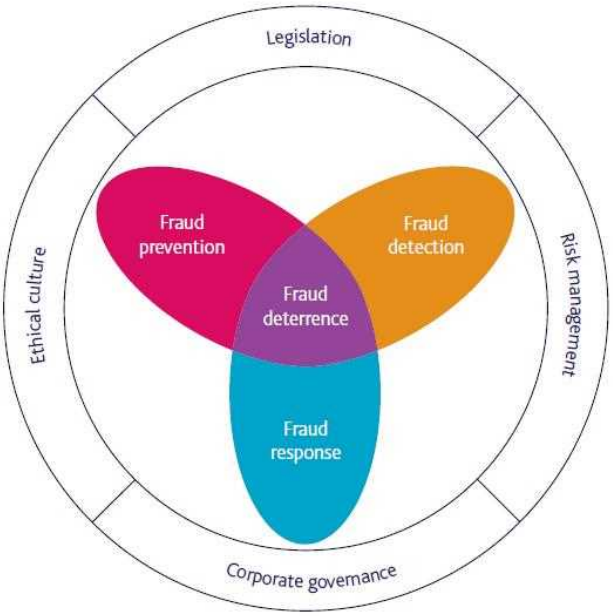
ریسک تقلب چیست؟

آسیب‌پذیری سازمان در هنگام رسیدن به اهداف خویش از جانب افراد/عوامل درون یا بیرون سازمان.

انواع ریسک تقلب:

ریسک ذاتی[۶]: ریسک‌هایی که پیش از آنکه هرگونه اقدام مدیریتی در جهت کاهش آن رخ دهد، موجود است.

ریسک‌های باقیمانده بعد از انجام اقدامات



شکل ۱- راهبرد مقابله با تقلب [۴]

شکل ۲ مثلث تقلب [۴]

مدیریتی در جهت کاهش یا حذف آنها.

مدیریت ریسک[۸] چیست؟

مدیریت ریسک فرآیند درک و سازماندهی کردن ریسک‌هایی که یک سازمان به طور ناگزیر در تلاش برای دستیابی به اهداف سازمان با آنها مواجه است. برای سازمان، ریسک‌ها در حقیقت حوادث محتملی است که می‌توانند اهداف سازمان را تحت تأثیر قرار دهند. به بیان بهتر، مدیریت ریسک عبارت از بیان تهدیدات و برنامه‌ریزی در جهت کاهش دادن آنها است. تقلب یکی از مهم‌ترین ریسک‌هایی است که کسب‌وکار را تهدید می‌کند، نه تنها از دیدگاه سلامت مالی، بلکه به لحاظ تصویر و شهرت سازمان. در این راستا ابتدا به معرفی چرخه مدیریت ریسک [۴] پرداخته و سپس سعی خواهیم کرد ارتباط آن را با مدیریت ریسک تقلب بررسی کنیم.

چرخه مدیریت ریسک[۹] چیست؟

چرخه مدیریت ریسک (شکل ۳) یک فرآیند تعاملی شامل شناسایی ریسک‌ها، ارزیابی تأثیر آنها و اولویت‌بندی اقدامات برای کاهش و کنترل ریسک‌ها است. گام‌های چرخه مدیریت ریسک عبارتند از:

- ایجاد یک گروه مدیریت ریسک و تعیین اهداف
- شناسایی حوزه‌های ریسک
- درک و ارزیابی اندازه ریسک
- توسعه راهبرد پاسخ به ریسک
- پیاده‌سازی راهبردها و تخصیص مسئولیت‌ها
- پیاده‌سازی و نظارت بر کنترل‌های پیشنهادی
- مرور و اصلاح فرآیند و انجام دوباره آن

اینک برخی پرسش‌های قابل بحث در زمینه رویکرد سازمان شما در ارتباط با مدیریت ریسک و مدیریت ریسک تقلب را بیان خواهیم کرد.

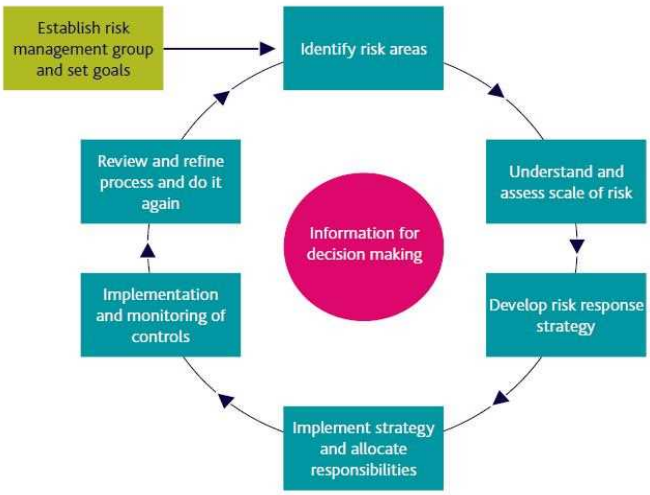
۱- آیا سازمان شما از یک مدل خاص مدیریت ریسک پیروی می‌کند؟ اگر بله، کدام؟ آیا فکر می‌کنید این مدل به اندازه کافی ریسک‌هایی که سازمان با آن مواجه است را برطرف می‌کند؟ چرا و چرا نه؟

۲- برخی از ریسک‌هایی که سازمان شما با آن مواجه است را بیان کنید؟ ریسک تقلب در سلسله مراتب ریسک‌هایی که سازمان شما با آن مواجه است، کجا قرار می‌گیرد؟

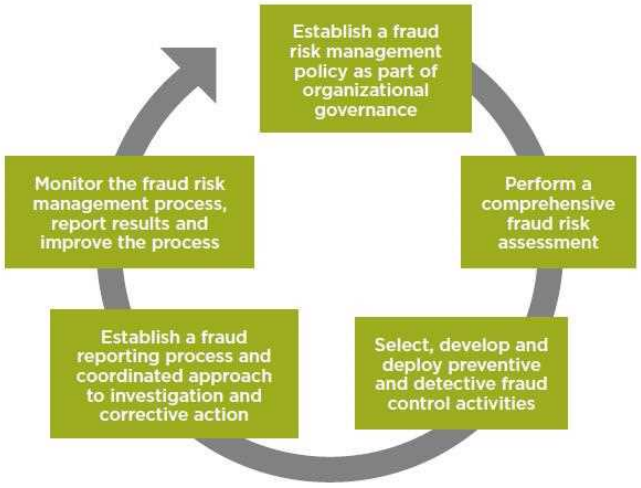
۳- آیا سازمان شما دارای یک عملکرد رسمی مدیریت ریسک است؟ اگر چنین است، آیا طرح‌های مقابله با تقلب در طرح‌های مدیریت ریسک ادغام شده‌اند؟

۴- سازمان شما چگونه ریسک‌هایی را که در فرآیند مدیریت ریسک شناسایی می‌شوند، دسته‌بندی می‌کند؟

در سال ۱۹۹۲، کمیته سازمان‌های حامی کمیسیون تردوی (COSO) چارچوب یکپارچه کنترل داخلی خود (چارچوب اصلی) را منتشر کرد. چارچوب اصلی به صورت گسترده مورد پذیرش قرار گرفت و در سراسر جهان استفاده شد. این چارچوب به عنوان یک مرجع استاندارد در زمینه طراحی و اجرای کنترل‌های داخلی و ارزیابی اثر بخشی آنها مورد استفاده قرار گرفته است. کوزو چارچوب اصلی را در سال ۲۰۱۳ و با بهره‌گیری از چارچوب منتشر شده سال ۲۰۰۸ مؤسسه حسابداران رسمی آمریکا ، مؤسسه حسابرسان داخلی ، و انجمن بازرسان خبره تقلب مورد بازبینی و اصلاح قرار داد. چارچوب سال ۲۰۱۳ شامل ۱۷ اصل است. این ۱۷ اصل با پنج مؤلفه کنترل داخلی مرتبط هستند و برای کاربر در طراحی و اجرای سیستم‌های کنترل داخلی و همچنین برای درک الزامات کنترل داخلی مؤثر شفافیت ایجاد می‌کنند. در سال ۲۰۱۶ کوزو با حمایت مؤسسه ACFE راهنمای مدیریت ریسک تقلب را به نحو سازگار با چارچوب ۲۰۱۳ توسعه داده و منتشر کرد. راهنمای مذکور به عنوان بهترین شیوه برای سازمان‌ها در ارزیابی تقلب‌ها مورد استفاده قرار می‌گیرد. این راهنما شامل اطلاعاتی بیش از اطلاعات مورد نیاز برای انجام ارزیابی ریسک تقلب است، به‌ویژه شامل راهنمایی در مورد ایجاد یک برنامه کلی مدیریت



شکل ۳- چرخه مدیریت ریسک CIMA [۴]



شکل ۴- فرآیند مدیریت ریسک تقلب کوزو [۳]

ریسک تقلب است؛ بنابراین برای سازمان‌هایی که مایل به ایجاد یک رویکرد جامع‌تر برای مدیریت ریسک تقلب هستند، مفید است. به عبارت بهتر، چارچوب مذکور شامل مجموعه‌ای جامع از شیوه‌های پیشرو است که به عنوان راهنمای مدیران در هنگام توسعه‌ی فعالیت‌های مقابله با تقلب به شیوه‌ای راهبردی و مبتنی بر ریسک استفاده می‌شود. (شکل ۴)

اینک سعی خواهیم کرد به تشریح فرآیند مدیریت ریسک تقلب کوزو (شکل ۴) به صورت مختصر بپردازیم. چارچوب مدیریت ریسک تقلب کوزو شامل یک برنامه کامل به شرح زیر است:

■ **ایجاد سیاست مدیریت ریسک تقلب به عنوان بخشی از حاکمیت سازمان:** سازمان یک برنامه مدیریت ریسک تقلب را ایجاد و ابلاغ می‌کند که انتظارات هیأت مدیره و مدیریت ارشد و تعهد آنها به یکپارچگی بالا و ارزش‌های اخلاقی در مورد مدیریت ریسک تقلب را نشان می‌دهد.

■ **اجرای جامع ارزیابی ریسک تقلب:** سازمان یک ارزیابی جامع ریسک تقلب را انجام می‌دهد تا الگوهای تقلب خاص و ریسک‌هایی آن را شناسایی کند، احتمال وقوع و اهمیت آنها را ارزیابی کند، فعالیت‌های کنترلی تقلب موجود را بررسی و ارزیابی کند و اقداماتی برای کاهش ریسک‌های تقلب احتمالی را پیاده‌سازی کند.

■ **انتخاب، توسعه و استقرار فعالیت‌های کنترلی پیشگیرانه و شناسایی‌کننده تقلب:** سازمان اقدام به انتخاب، توسعه و استقرار فعالیت‌های کنترلی پیشگیرانه و شناسایی کننده تقلب می‌کند تا ریسک فعالیت‌های متقلبانه‌ای را که رخ داده یا در زمان معلوم شناسایی نشده، کاهش دهد.

■ **ایجاد فرآیند گزارش‌دهی تقلب و اختصاص رویکرد بررسی و تصحیح کننده فعالیت:** سازمان یک فرآیند ارتباطی برای به‌دست آوردن اطلاعات در مورد تقلب‌های محتمل ایجاد می‌کند و یک رویکرد مختص به آن برای بررسی و اقدامات اصلاحی درجهت رسیدگی مناسب و به موقع تقلب مستقر می‌کند.

■ **نظارت بر فرآیند مدیریت ریسک تقلب، گزارش نتایج و بهبود فرآیند:** سازمان ارزیابی‌های مداوم را انتخاب، توسعه و اجرا می‌کند تا مشخص کند که آیا هریک از ۵ اصل مدیریت ریسک تقلب وجود دارد؟ عملکرد دارد؟ و نواقص برنامه مدیریت ریسک تقلب را به موقع با طرفین مسئول انجام اقدامات اصلاحی از جمله مدیریت ارشد و هیأت مدیره انتقال می‌دهد.

منابع

ACFE (Association of certified Fraud Examiners), Fraud Risk Management.

Wells, J. T., International fraud handbook, John Wiley & Sons, Inc., Hoboken, New Jersey, 2018.

COSO (Committee of Sponsoring Organizations of the Treadway Commission), Fraud Risk Management Guide, 2016

CIMA (Chartered Institute of Management Accountants), Fraud risk management – a guide to good practice, 2008.

پاورقی

1- Association of Certified Fraud Examiners (ACFE)
2- Donald Cressey
3- Motivation
4- opportunity
5- Rationalization
6- Inherent risk
7- Residual risk
8- Risk management
9-CIMA (Chartered Institute of Management Accountants) office Terminology 2005
10- The risk management cycle
11- The committee of Sponsoring Organizations of the Treadway Commission (COSO)
12- The American Institute of Certified Public Accountants (AICPA)
13- The Institute of Internal Auditors (IIA)
14- The Association of Certified Fraud Examiners (ACFE)
15- Fraud Risk Management Guide

مقاله

کاشف بازیگر و متولی ISAC در سطح زیرساخت بانکی و پرداخت

لیلا فتحی
■ رییس گروه پژوهش و نوآوری شرکت کاشف

بخش بانکی یکی از زیرساخت‌های حیاتی هر کشور است که نبض اقتصاد و توسعه آن محسوب می‌شود. یکی از اساسی‌ترین مسائل پیش‌روی این زیرساخت مورد هدف قرارگرفتن توسط عوامل تهدید مختلف به‌صورت مستقیم یا غیرمستقیم از طریق سایر زیرساخت‌های مرتبط (همانند زیرساخت‌ها نیرو، سلامت، فاوا، انرژی و ...) است. اهمیت حیاتی این زیرساخت، ایجاب می‌کند مخاطرات ناشی از آسیب‌پذیری‌ها و تهدیدات برآورد شده علیه این بخش در کمینه‌ترین حالت ممکن باشند.

رویکرد سنتی توسعه امنیت، مبتنی بر شناخت و رفع آسیب‌پذیری‌های شناخته‌شده است. این رویکرد، تضمین‌کننده کاهش یا رفع مخاطرات ناشی از تهدیدات ناشناخته یا مبتنی بر نفوذ و حضور مهاجمان و متخاصمین در درون استحکامات دفاعی نیست.

بر این اساس رویکرد تلفیق امنیت فعال با رویکرد پیش‌کنشی و تاب‌آوری ذاتی بسیار مورد توجه قرار گرفته است. این رویکرد، مبتنی بر شناسایی و شکار تهدیدات و مقابله با آنها در فازهای پیش از تهاجم است. ایجاد این رویکرد و مواجهه با بردارهای تهدید، مستلزم همکاری بازیگران و ذینفعان و هماهنگی با آنها است. این هماهنگی با بهره‌گیری از رویکرد اشتراک‌گذاری میسر می‌شود.

ضمن اینکه تجربیات قبلی ذینفعان در کشف، حفاظت، بازدارندگی، پیشگیری، مقابله یا رهایی از تهاجمات و بازیابی پس از آنها می‌تواند در صورت تکرار یک تهاجم، به‌تناسب مورداستفاده قرار گیرد. از سوی دیگر، توسعه استحکامات دفاعی با رفع آسیب‌پذیری‌های شناخته‌شده نیز می‌تواند با اتکاء به همکاری اطلاعاتی (با رعایت شرایط آن مانند رعایت حریم خصوصی و التزام به چارچوب‌های قانونی) ارتقا یابد.

در این راستا و تحقق فرآیندهای اشتراک‌گذاری، کشورهایی همانند کشورهای عضو اتحادیه اروپا، ایالات‌متحده آمریکا، ژاپن و کره اقدام به راه‌اندازی مراکزی تحت عنوان ISAC جهت محافظت از زیرساخت‌های حیاتی در برابر تهدیدهای سایبری کردند. از آنجا که یکی از مهم‌ترین زیرساخت‌های حیاتی، مالی است این مرکز شکل گرفته در سطح زیرساخت مالی عنوان FS-ISAC را دارد. از جمله مأموریت‌های مهم این مراکز بهره‌مندی از پیاده‌سازی سازوکارهای اشتراک‌گذاری برای ارتقای آگاهی وضعیتی و ایجاد هماهنگی در پاسخگویی به تهدیدها و مخاطرات سایبری است. در واقع این مراکز بسترهای مهم حیات، رشد و پویایی در ایجاد امنیت و تاب‌آوری سایبری تلقی می‌شوند و مجموعه‌ای مشتمل بر سامانه‌های هوشمندی تهدیدها و آگاهی‌وضعیتی با عملکرد ملی در سطح زیرساخت حیاتی (راهبردی-عملیاتی) و کارگروه‌های تحلیل و ایجاد هماهنگی هستند.

این مرکز عالی‌ترین نهاد مرجع در خصوص

۱) تعیین وضعیت امنیت سایبری و ارائه هشدارها و تدوین راهبردهای عملیاتی لازم،

۲) ایجاد، ارتقا و به‌اشتراک‌گذاری آگاهی وضعیتی در سطح ملی، به‌صورت به‌هنگام یا به اقتضای هر مخاطره،

۳) تشخیص یکپارچه، تحلیل متمرکز و راهبری منسجم پیشگیری و واکنش به مخاطرات سایبری (در قلمرو زیرساخت) و

۴) ایجاد امکان تصمیم‌گیری کم‌مخاطره در حوزه مخاطرات سایبری است.

هدف از ارائه این مقاله توصیف مأموریت‌های کاشف به‌عنوان بازیگر ISAC در سطح نظام بانکی پرداخت است.

کاشف بازیگر و متولی ISAC در سطح زیرساخت بانکی و پرداخت

بر اساس بیانیه مأموریت و اهداف شرکت کاشف مهمترین وظایف عملکردی این شرکت به‌عنوان متولی مرکز ISAC به شرح موارد زیر است:

۱- ایجاد، ارتقا و اشتراک‌گذاری آگاهی وضعیتی دقیق، جامع و به‌هنگام از طریق:

- دریافت اطلاعات مربوط به آگاهی‌وضعیتی (وضعیت مخاطره، تهدید، وضعیت عملیاتی) از مراکز عملیات امنیت سازمان‌ها؛
- دریافت اطلاعات تکمیلی هر مخاطره شامل دارایی‌ها، تهدیدها، آسیب‌پذیری‌ها، حملات و آثار از هر حوزه میدانی درگیر (سازمان‌ها)؛
- دریافت انواع سطوح هوشمندی (اطلاعات، دانش، آگاهی، خرد) از منابع باز، آزاد و عمومی و مراکز تحقیقاتی؛
- پردازش تحلیل کلیه سطوح هوشمندی دریافتی به‌صورت تلفیقی (خودکار و انسانی)؛
- ایجاد تصویر جامع وضعیتی، تعیین وضعیت امنیت سایبری و ارایه هشدارهای مرتبط؛
- استخراج و اشتراک‌گذاری آگاهی‌وضعیتی موردنیاز برای تصمیم‌سازی و تصمیم‌گیری عملیاتی و همچنین اصلاح یا به‌روزرسانی اهداف

راهبردی و سیاست‌های کلان در خصوص مدیریت مخاطرات

۲- هماهنگی و هدایت متمرکز مدیریت مخاطرات سایبری در سطح نظام بانکی و پرداخت براساس چارچوب نظامات امنیت سایبری کشور از طریق:

- هماهنگی مانورهای عملیاتی جهت ایجاد آمادگی در سطح نظام بانکی و پرداخت؛
- هماهنگی ارزیابی دوره‌ای و اقتضایی مخاطرات سایبری در سطح نظام بانکی و پرداخت؛
- تشخیص و ارزیابی مخاطرات سایبری؛
- تصمیم‌سازی و کمک به تصمیم‌گیری راهبردی در خصوص مدیریت مخاطرات سایبری؛
- تعیین بازیگران (متولیان اصلی و همکاران) در خصوص هر مخاطره سایبری؛
- ایجاد هماهنگی بین بازیگران در خصوص مدیریت مخاطرات سایبری؛
- کمک به شروع، هماهنگی، ترمیم، بازسازی یا آمادگی اضطراری در شرایط بحران یا شرایط اضطراری؛
- تحلیل جامع، عمیق و دقیق مخاطرات سایبری و آثار آنها و ارائه نیازمندی‌ها و پیشنهادات اصلاح سیاست‌ها، اهداف و راهبردهای کلان در راستای بهبود و ارتقای طرح‌ها، برنامه‌ها و همچنین دانش و هوشمندی در موارد مشابه یا آتی؛
- پشتیبانی از پیگیری قضایی و احقاق حقوق قانونی در سطح ملی یا بین‌المللی.
- نقش‌آفرینی در راستای تحقق سکوی همکاری متقابل بین ذینفع مرتبط در حوزه مخاطرات ملی سایبری-فیزیکی در چارچوب نظام‌های مصوب از طریق:
- ایجاد امکان تجمیع سامانه ساتا «بازوی فناورانه همکاری، اشتراک‌گذاری و ایجاد آگاهی‌وضعیتی» با دیگر سامانه‌های مشابه و ایجاد سامانه یکپارچه گزارش‌دهی برای دفاع سایبری و مقابله با جرائم سایبری در قالب یک پنجره واحد؛
- فراهم‌آوری امکان اعمال سیاست‌ها، قوانین و مقررات در حوزه اشتراک‌گذاری اطلاعات در سطح راهبردی و عملیاتی؛
- ایجاد سازوکارهای تصمیم‌سازی کم‌مخاطره در شرایط بروز رخداد و حساس و بحرانی
- ایجاد بستر مشارکت مراکز تحقیقاتی و دانشگاهی در تحقق اهداف

بنابر وظایف بیان شده، معماری عملیاتی کاشف به‌عنوان متولی ISAC مشتمل بر سه عملیات کلان پردازش آگاهی وضعیتی، هماهنگی مدیریت مخاطرات و مدیریت/امنیت داخلی است که در ادامه اجزا و فرایند کلان آن بیان شده است.

شکل ۱: عملیات پردازش آگاهی وضعیتی

شکل ۲: عملیات هماهنگی مدیریت مخاطرات (واکنش و درمان مخاطره)

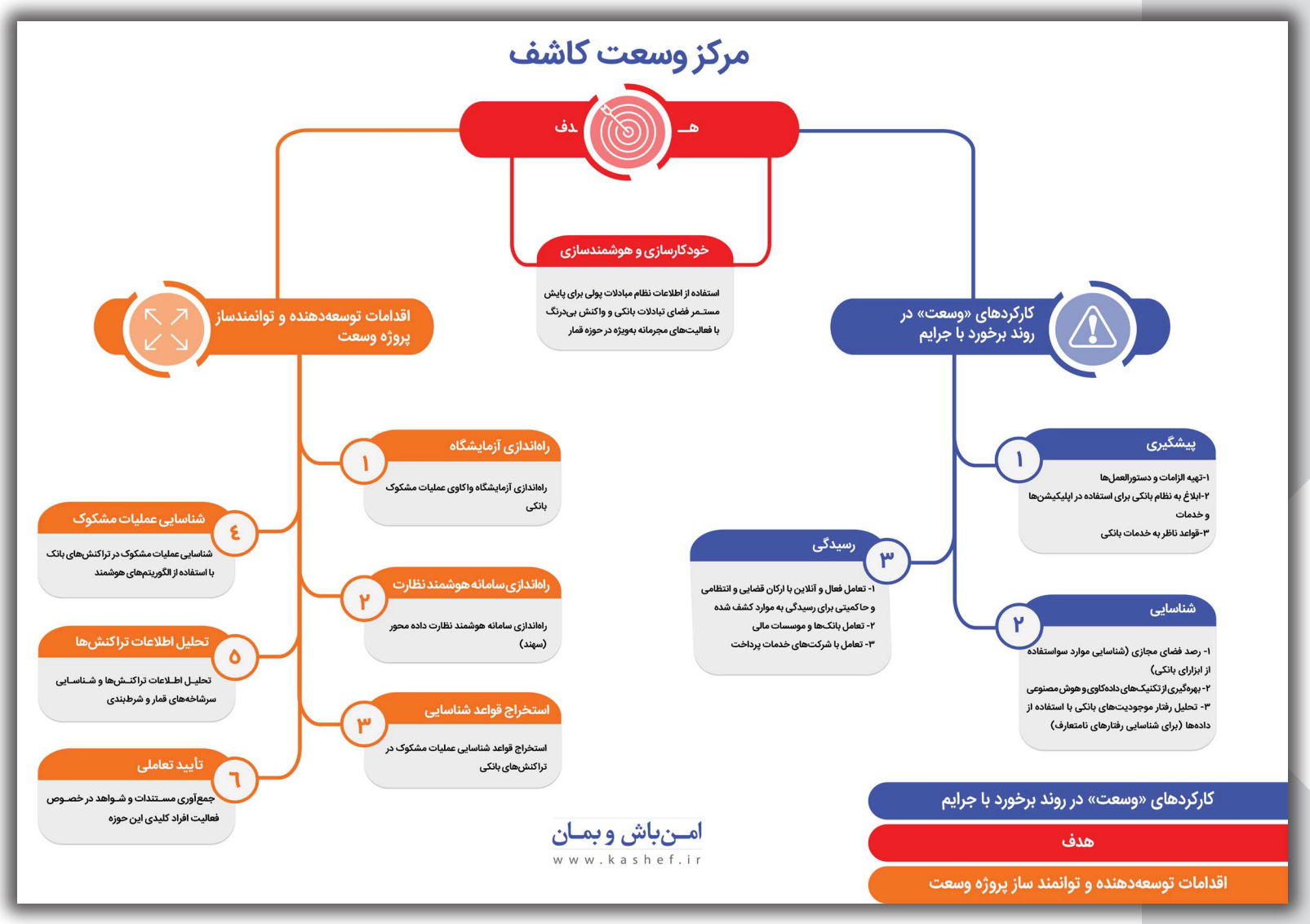
شکل ۳: عملیات هماهنگی مدیریت مخاطرات (پیشگیری)

پاورقی

1- Information Sharing and Analysis Center (ISAC)


کاشف
مدیریت امن الکترونیکی
ماموریت رادار
در راستای الزام شورای عالی فضای مجازی مبنی بر راه‌اندازی سریع و کوتاه مدت سامانه‌ای بومی جهت جمع‌آوری متمرکز رخدادهای امنیتی در زیرساخت بانکی و پرداخت کشور، مقرر گردید سامانه رادار با عاملیت مرکز کاشف در بانک مرکزی توسعه داده شود.
اهداف عملیاتی پروژه
جمع‌آوری متمرکز رخدادهای امنیتی
تحلیل رخدادها و ارائه گزارش‌های یکپارچه
اشتراک‌گذاری با نهادهای بالادستی
بانک
Event
Security Log
Alerts
SIEM
ExploitTarget
Observable
Intrusion Set
SOC & CERT
رخدادهای امنیتی
امن باش و بمان
www.kashef.ir

اینفوگرافی: مرکز وسعت کاشف



فراخوان همکاری با نشریه
«امنیت بانکداری»

شرکت کاشف در راستای تحقق بخشی از اهداف و ماموریتهای خود، که آگاهی‌رسانی و فرهنگ‌سازی است، در دهمین سال تاسیس و پس از بلوغ و کسب تجربه‌های کاربردی و موثر، اقدام به چاپ نشریه تخصصی کرده است. نشریه‌ای که در آن سعی می‌شود مباحث فنی و به‌روز دنیا در آن منعکس شود.

همچنین نشریه امنیت بانکداری سعی دارد تا از دانش و تجربیات مدیران این زیست‌بوم در مطالب این نشریه استفاده کند.

نشریه امنیت بانکداری در کنار اندک رسانه‌های حوزه بانکداری و با رویکرد تخصصی در حوزه امنیت سایبری و بانکداری، می‌تواند پنجره‌ای باشد برای آگاهی‌بخشی و گفتن و شنیدن از مفاهیم جاری در امنیت بانک‌ها.

در همین راستا و برای هم‌افزایی دانش و تجارب از همه متخصصان، کارشناسان و مدیران این حوزه دعوت می‌شود مطالب خود را با موضوعات مرتبط با فعالیت‌های امنیت بانکداری در قالب مقاله، یادداشت، گزارش پروژه و ... از طریق ایمیل به واحد روابط عمومی شرکت کاشف ارسال نمایند info@kashef.ir یا جهت اطلاعات بیشتر با شماره (۰۲۱۷۲۸۶۱۴۷۹) تماس حاصل فرمایند.

قابل توضیح است این نشریه فصلنامه بوده و مطالب ارسالی شما در صورت تایید با نام شما منتشر خواهد شد.

نشریه

امنیت بانکداری

رویکرد کاشف در تدوین و اجرای این برنامه‌ها همانطور که رئیس کل محترم بانک مرکزی به دفعات اشاره کرده‌اند، ایجاد اعتماد و اطمینان در تمامی لایه‌ها و کاربران خدمات بانکداری و پرداخت الکترونیکی در کشور است. به‌این‌ترتیب علاوه بر افزایش سطح رضایتمندی و بهره‌وری، زمینه‌های لازم برای تحول دیجیتال در تمام عرصه‌های کشور فراهم خواهد شد. در این راستا تلاش داریم، آگاهی از خدمات و مسئولیت‌های کاشف را در حوزه‌های مختلف افزایش دهیم. بر همین اساس، ارتقای جایگاه شرکت در زیست‌بوم امنیت اطلاعات کشور از اولویت‌های ما بوده و هست.

دریافت مجوز دانش‌بنیان شدن شرکت کاشف، دریافت مجوز انفورماتیک و مجوز آزمایشگاه ارزیابی امنیتی کاشف از افتای ریاست جمهوری بخشی از این تلاش‌ها بوده که طی یک سال گذشته در جهت دست‌یابی به این مهم صورت گرفته است. چشم‌انداز ما در کاشف تبدیل شدن به معتمدترین مرجع و عامل پیشران در ارتقای امنیت، پایداری و تاب‌آوری در زیست بوم تولید و تبادل اطلاعات بانکی است.

www.kashef.ir