



هشدار پلیس فتا به فعالان اقتصادی درباره کلاهبرداری‌های مالی سایبری

نشست ارائه‌ی راهکارهای مالی سایبری، در خصوص کلاهبرداری از فعالان اقتصادی و مدیران صنایع، با حضور رئیس پلیس فتا فرماندهی انتظامی استان آذربایجان شرقی و جمعی از فعالان اقتصادی در اتاق بازرگانی تبریز برگزار شد.

به گزارش روابط عمومی اتاق بازرگانی تبریز، سید باقر شریف زاده، رئیس شورای راهبردی مرکز پژوهش‌های اتاق بازرگانی تبریز، با اشاره به اهمیت برگزاری این نشست گفت: امروزه بخش قابل توجهی از فرآیندهای بنگاه‌های اقتصادی، از جمله انعقاد قراردادهای، پرداخت‌ها، ارتباط با مشتریان و مدیریت زنجیره تأمین، به بسترهای دیجیتال منتقل شده است؛ تحولی که در کنار فرصت‌های متعدد، تهدیدها و مخاطرات جدیدی را نیز برای کسب و کارها به همراه دارد.

وی افزود: دیجیتالی شدن فرآیندها موجب افزایش سرعت، شفافیت و راندمان فعالیت‌های اقتصادی شده است، اما در مقابل، کوچک‌ترین خطا یا بی‌توجهی در این حوزه می‌تواند زمینه‌ساز بروز مشکلات و خسارت‌های جدی برای بنگاه‌های اقتصادی شود.

شریف زاده با اشاره به افزایش شیوه‌های کلاهبرداری در فضای مجازی اظهار کرد: استفاده از ایمیل‌ها، تماس‌های تلفنی و پیامک‌های جعلی، هک سیستم‌ها و سایر روش‌های کلاهبرداری سایبری، ضرورت آشنایی مدیران و فعالان اقتصادی با راهکارهای پیشگیری و ارتقای امنیت سایبری در بنگاه‌ها را بیش از گذشته آشکار کرده است.

وی با تأکید بر ضرورت همراهی مدیران با تحولات فناوری گفت: مدیران ارشد باید به سرعت تغییرات‌آور داشته باشند و این نگاه باید در سطوح کلان مدیریتی کشور نیز وجود داشته باشد.

رئیس شورای راهبردی مرکز پژوهش‌های اتاق بازرگانی تبریز با اشاره به تحولات ناشی از انقلاب صنعتی و شتاب بالای تغییرات فناوری افزود: سازمان‌ها اگر نتوانند خود را با این تغییرات هماهنگ کرده و الزامات آن را در ساختار و فرآیندهای خود اجرا کنند، محکوم به شکست خواهند بود.

وی همچنین تعدد سامانه‌های مورد استفاده بنگاه‌های اقتصادی را یکی از مشکلات موجود عنوان کرد و گفت: تعدد سامانه‌ها، فعالان اقتصادی را با مشکلات جدی مواجه کرده و در مواردی فرآیند فعالیت بنگاه‌ها را مختل کرده است.

شریف زاده در پایان خواستار پیگیری این موضوع از سوی رئیس پلیس فتای استان شد.

سه عامل اصلی جرایم سایبری؛ ناآگاهی، طمع و اعتماد بیش از حد

سرهنگ اکبر محمدجعفری، رئیس پلیس فتا فرماندهی انتظامی استان آذربایجان شرقی، در این نشست با اشاره به اهمیت امنیت سایبری برای فعالان اقتصادی گفت: اکنون تقریباً تمامی مراودات اقتصادی وارد حوزه فضای مجازی شده است؛ از این رو، امنیت سایبری برای فعالان اقتصادی اهمیت ویژه‌ای دارد.

وی با تأکید بر لزوم یادگیری فعالان اقتصادی در این حوزه، جهت حفظ دارایی و کسب و کار، افزود: مورد اول مختص ایمیل شرکت‌ها است که از طریق تغییر حروف در ایمیل‌های ارسالی جعلی و مشابه ایمیل‌های قبلی، شماره حساب‌هایی به افراد دارای مراودات اقتصادی فرستاده می‌شود. عدم دقت کافی در آدرس ایمیل باعث می‌شود واریزی به شماره حساب کلاهبردارها صورت بگیرد. لذا هر بار شماره حساب جدید فرستاده می‌شود، باید چک شود.

وی مورد بعدی کلاهبرداری را باج‌افزارها عنوان کرد و گفت: فایل‌هایی که با عنوان پی‌دی‌اف در قالب تبلیغات فرستاده می‌شود، باید دقت شود که به شکل باج‌افزار نباشد؛ چراکه با دسترسی به فایل‌های اصلی، آن‌ها را لاک کرده و افراد برای باز شدن آن‌ها مجبور به پرداخت مبالغی می‌شوند.

سرهنگ اکبر محمدجعفری به اهمیت گزینش کارکنان بخش سایبری در مجموعه اشاره کرد و افزود: شخص حسابدار در مجموعه یا افراد فامیل نمی‌توانند به عنوان امنیت سایبری انتخاب شوند. این فرد باید در قبال حفظ داده‌ها قرارداد حقوقی و فنی داشته باشد و همچنین باید در داخل کشور باشد؛ چراکه افراد امنیت شبکه در خارج از کشور می‌توانند آسیب جدی به شرکت وارد کنند.

وی بک‌آپ‌گیری اطلاعات را یکی دیگر از راه‌های امنیت سایبری بیان کرد.

رئیس پلیس فتا استان درباره نقش دوربین‌های مداربسته در امنیت سایبری گفت: این دوربین‌ها باید مک‌فیلت‌ر باشند و همه به آن دسترسی نداشته باشند. برای مثال، نقشه نصب دوربین مداربسته وجود دارد که در کجاها بهتر است نصب شوند.

وی افزود: درباره بررسی دوره‌ای تراکنش‌های مالی، حسابدار باید حداقل هر دو هفته یک بار درباره نوسان‌ها و دادوستدهای شرکت گزارش دهد.

سرهنگ محمدجعفری گفت: اینکه رمزهای اکانت‌ها در اختیار چه کسانی قرار می‌گیرد، موضوع مهمی است. از آنجا که امروزه اغلب سیستم‌های بانکی مجازی هستند، لازم است این فضا مهم شمرده شود. برای مثال، قرارگیری رمز اکانت‌های صفحات تلگرامی، اینستاگرامی، واتس‌آپی و... در اختیار چه کسانی و یا چند نفر قرار می‌گیرد، موضوع مهمی است.

وی ادامه داد: موضوعی که اخیراً برای افراد حوزه صنعت بیشتر اتفاق افتاده است، اخذ کدهای دسترسی بوده است که برای مثال، لیست افراد هک می‌شود و برایشان کدی فرستاده می‌شود که از این طریق، حساب‌های افراد هک شده و خالی یا انتقال داده می‌شود.

سرهنگ محمدجعفری شماره تماس ۰۹۶۳۸۰ را شماره اختصاصی پلیس فتا برای جرایم مالی سایبری عنوان کرد و افزود: سایت «کلیک امن» نیز کانال این سازمان است که مطالبی در حوزه امنیت سایبری در اختیار افراد قرار می‌دهد.

سرهنگ محمدجعفری نیز در پایان به سه مورد که منجر به ایجاد جرم‌های سایبری می‌شود اشاره کرد و گفت: عدم آگاهی، طمع و اعتماد بیش از حد، سه موردی است که منجر به جرایم در این حوزه می‌شود و اهمیت حوزه سایبری از حفاظت فیزیکی بیشتر است.

ضرورت ایجاد جایگاه مدیریت اطلاعات سایبری در بنگاه‌های اقتصادی

سرگرد تورج جعفری، معاون رئیس پلیس فتا، در خصوص باج‌افزارها توضیح داد: نحوه عملکرد باج‌افزارها به این شکل است که داده‌ها را رمزنگاری می‌کند و فرد نمی‌تواند به

آن‌ها دسترسی داشته باشد که برای حل این مشکل نیز می‌توان اقداماتی انجام داد. از جمله اینکه برخی گروه‌های تجاری و برخی آزاد وجود دارند که فعالیتشان در این حوزه است که دیکریپت می‌کنند که این اقدام تا بالای ۶۰ درصد توسط پلیس فتای استان و با دستور قضایی انجام می‌گیرد.

سرگرد جعفری همچنین درباره پیگیری بین‌المللی در این خصوص گفت: خوشبختانه پلیس سایبری ایران زیرمجموعه اینترپل قرار دارد و از طریق IGC که مستقر در سنگاپور است، می‌توان این جرایم را به صورت بین‌المللی پیگیری کرد. در استان نیز در پلیس آگاهی قرار دارد.

وی در رابطه با ادمین شبکه‌های مجازی و مشکلات مربوط در این حوزه توضیح داد: در قراردادهایی که بسته می‌شود، دسترسی‌ای که داده می‌شود نباید مسئولیت‌زا باشد و انتشار باید در اختیار خود شرکت باشد. قرارداد بایستی با تیم محتوا بسته شود.

معاون عملیات سایبری استان به اهمیت ویژه هوشمندسازی و استفاده از CIO در شرکت‌ها تأکید و بیان کرد: باید حتماً پوزیشنی در شرکت‌ها به عنوان مدیر اطلاعات سایبری اطلاعات (CIO) به وجود بیاید که در این مورد می‌توان از هوش مصنوعی استفاده کرد. برای مثال، N&N یکی از پلتفرم‌های هوش مصنوعی در این زمینه است که در حوزه انتشار محتوا مورد استفاده قرار می‌گیرد.

وی درباره مزایای هوشمندسازی گفت: از خطای انسانی جلوگیری می‌کند، تجمیع‌کننده بوده و همچنین جرم‌یابی را خیلی راحت می‌کند و کتابخانه جامع دارد.