نگاهی به درون مرکز مبارزه با جرم‌های سایبری یوروپل

هر روز یک چالش است

مرکز جرم‌های سایبری اروپا از نهادهای زیرمجموعه یوروپل (پلیس اتحادیه اروپا)، سریع‌تر از آن‌چه انتظار می‌رفت، رشد کرد. داگ درینک‌واتر(Doug Drinkwater) ضمن بازدید از دفاتر این مرکز در شهر لاهه هلند، در پی این بود که دریابد آن‌ها چگونه از الزامات قانونی برای مبارزه با مجرمان سایبری بهره می‌برند.

مرکز جرم‌های سایبری اروپا (European Cybercrime Centre)، به‌طور خلاصه EC3، در ساختمان چهاربرجه معروف پلیس اروپا، یوروپل (Europol)، در شهر لاهه هلند قرار دارد و 850 نفر از نیروهای قضایی از 28 کشور اتحادیه اروپا در آن حضور دارند. این مرکز در ژانویه 2013 با این هدف که در سال 2015 کاملاً عملیاتی شود، کار خود را آغاز کرد. مرکز یاد شده زیرمجموعه بخش ساز و کارهای یوروپل است که در کنار چند بخش دیگر شامل SOC، Info Hub، ضدتروریسم، راهبری و توان‌مندی‌ها به ایفای نقش می‌پردازد. مرکز EC3 نیز برای راهبردها و ساز و کارهایش بخش‌های اختصاصی خود را دارد. بخش ساز و کارها شامل زیرمجموعه‌های دیگری مانند هوش سایبری، سایبورگ (جرم‌های پیش‌رفته) و کلاهبرداری‌های مالی است. مجله SC با تروئل اورتینگ (Troels Oerting) رییس و پائول گیلن مدیر این مرکز و همچنین چند نفر دیگر از بازرسان جرم‌های سایبری در یوروپل دیدار کرد تا از عملکرد این واحد تا به این‌جا و نیز چالش‌هایی که پیش رو دارد آگاه شود.

اورتینگ تأیید می‌کند که او و گروهش باید به‌سرعت موارد گوناگونی را یاد بگیرند تا بتوانند به‌سرعت خود را با گسترش شتابنده جرم‌های سایبری هم‌گام کنند. او می‌گوید: «ما حالا تقریباً 70 نفر (نیروی انسانی) داریم.» اما پیش از بحران اقتصادی و بانکی قرار بود چندصد نفر در این مرکز کار کنند. با این همه، آن گونه که اورتینگ می‌گوید، یوروپل سال آینده برای افزایش شمار کارکنان این مرکز بودجه کافی و منابع بیش‌تری را به آن اختصاص خواهد داد. او اظهار می‌دارد که در استخدام این افراد باید سختگیر بود. کشف جرم دیجیتال فرآیند آسانی نیست، به‌ویژه که می‌توان گفت نیروهای قضایی در مقایسه با بخش‌های دیگر درباره امنیت اطلاعات تجربه کم‌تری دارند. اورتینگ می‌گوید، مشکل این است که نمی‌شود صرفاً یک نفر را از بخش مبارزه با قاچاق انسان به این‌جا منتقل کرد و سپس گفت: «خب، تو الان یک متخصص کامپیوتر هستی.» دیدگاه او این است که باید متخصصان را در این مرکز استخدام کرد: «در این صورت شاید کمی کندتر، اما با افرادی مناسب (این کار) رشد می‌کنیم.» در گستره مسئولیت‌های کنونی EC3 بخش راهبردها دیدی فراگستر و بالگردگونه دارد که وظیفه آن نظارت بر پیش‌گیری از جرم‌های سایبری، محافظت، پی‌گیری و راهبری است. بخش ساز و کارها که پائول گیلن مدیر آن است، با گروه‌های جرم‌های سایبری مبارزه می‌کند. این بخش در نابود کردن بات‌نت‌های نام‌آشنای Gameover Zeus و CryptoLocker

که گفته می‌شد چیزی حدود پانصد هزار دستگاه کامپیوتر را در سراسر جهان آلوده کرده بودند، به‌عنوان مرکز فرماندهی اتحادیه اروپا نقشی کلیدی داشت. همچنین، به آژانس ملی جرایم بریتانیا (NCA) کمک کرد تا زیرساخت‌های بدافزار Shylock را درهم بشکنند.
این گروه با صنایع بخش خصوصی نیز همکاری تنگاتنگی دارد، و نیز در قالب گروهی به‌نام Outreach از شرکای شرکت‌هایی مانند مایکروسافت، فیس‌بوک، توییتر، گوگل، آمازون و شرکت‌های امنیتی مانند مک‌آفی، کسپرسکی، سیمنتک و همچنین فدراسیون بانک اروپا و 21 بانک وابسته به‌شمار می‌رود. از دید اورتینگ این ارتباط‌ها حیاتی هستند؛ زیرا بیش‌ترین تخصص در حیطه امنیت سایبری را می‌توان در صنایع بخش خصوصی یافت. او می‌گوید مرکز متبوعش باید در زمینه فضای سایبری گام‌های عملی بردارد؛ زیرا در این باره اطلاعاتی ندارد. از این رو، در تلاش است تا خود را نه تنها با صنایع بخش خصوصی و کشورهای پیش‌رفته اتحادیه اروپا، بلکه با بازار شکوفنده فناوری هماهنگ نگه دارد. اینترنت اشیا، بزرگ‌داده و فناوری‌های پوشیدنی از جمله مواردی هستند که EC3 بر نگرانی‌های خود درباره آن‌ها تأکید دارد. البته مک‌آفی که یکی از شرکای EC3 است، اظهار می‌دارد که این گروه فعلاً فقط با جرم‌های سایبری روز سر و کار دارد؛ جرم‌هایی که سالانه 350 میلیون یورو برای اقتصاد جهانی زیان در پی دارند.
مشکل اصلی برای نیروهای قضایی و قانون‌گذاران، نبود مرزهای جغرافیایی در جرم‌های سایبری است. گروه‌های تبهکار اغلب صدها مایل دورتر از کشور هدف، حمله‌ای را علیه آن صورت می‌دهند و با استفاده از سرورهای پراکسی ترافیک اینترنتی خود را به حیطه‌هایی سوق می‌دهند که فراتر از حیطه مسئولیت نیروهای قضایی کشور هدف است. مبارزه با جرم‌های سایبری دگرگونی بزرگی را در نیروی پلیس پدید آورد و بازرسان را با مسئولیت‌هایی فراتر از مسئولیت‌های سنتی آن‌ها روبه‌رو کرد. با توجه به این که بررسی جرم‌های سایبری کار سختی است و برخی از کشورها توان‌مندی این را ندارند که از منظر حقوقی چنین جرم‌هایی را بررسی کنند، به EC3 روی می‌آورند.

[illegible]

اورتینگ می‌گوید که آن‌ها در این مرکز در ساز و کارها مشارکت و رؤسای آن‌ها در بخش جرم‌های سایبری با یوروپل همکاری خواهند داشت. آن‌ها می‌توانند نیازمندی‌های فناورانه خود را به EC3 اعلام کنند. یکی از مشکلات اتحادیه اروپا در ارتباط با کشورهایی است که بیرون از حیطه قضایی این اتحادیه به‌شمار می‌روند و ممکن است از تحویل دادن هکرهای مظنون خودداری کنند. اورتینگ با گفتن این مورد که «برخی کشورها هرگز مجرمان خود را به ما تحویل نخواهند داد.» می‌پرسد: «آیا در چنین مواردی باید کل پرونده را به آن کشور تحویل داد؟ آیا آن‌ها پرونده را خواهند پذیرفت و به دادگاه تحویل خواهند داد؟ چقدر باید صبر کرد؟» به‌نظر او باید در پی یک سیستم گزارش‌دهی بود که هیچ حیطه‌ای را از قلم نیاندازد، هم‌پوشانی نداشته باشد و آن وقت است که می‌توان سیستمی داشت که در آن با کشورهای مورد اشاره که جرم‌ها در آن‌ها شکل می‌گیرند، همکاری کرد.
به گفته اورتینگ، هم‌اکنون 85 درصد پرونده‌های تحت بررسی در EC3 به جرم‌هایی مربوط است که ریشه آن‌ها روسی‌زبانان هستند. او انتظار دارد که با افزایش کاربران اینترنت در افریقا، هندوستان و چین که شمار جهانی کاربران این شبکه را ظرف سه تا چهار سال آینده از 9/2 میلیارد نفر کنونی به حدود 4 میلیارد نفر خواهد رساند، این رویه تغییر کند. پائول گیلن که بخش ساز و کارها را در این مرکز مدیریت می‌کند و مدت زیادی در مقام مدیر واحد بررسی جرم‌های کامپیوتری (CCIU) در سرویس پلیس ایرلند (Garda Síochána) کار کرده، با تأیید این موضوع که منابع کنونی آن‌ها محدود است، می‌گوید، سرشان خیلی شلوغ است. به گفته او: «اگر مقدار منابع دو، سه یا چهار برابر بود، بدیهی است می‌توانستیم کار بیش‌تری انجام دهیم. اما در حال حاضر با کلی کار سرمان کاملاً شلوغ است، کارهایی واقعاً جالب.» این کارها در سطوح گوناگونی جای می‌گیرند. بعضی در مرحله شکل‌گیری و برخی توسعه‌یافته هستند. گیلن تأیید می‌کند که گروه او هر روز با چالش‌های گوناگونی روبه‌رو است، اما امیدوار است که بخش نوبنیان J-Cat بتواند به آن‌ها کمک کند.
وقتی بخش J-Cat در ماه جولای گذشته تشکیل شد، گیلن که گروهی از بازرسان را مدیریت می‌کند، داوطلبانه درباره سختی‌های مبارزه با جرم‌های سایبری سخن گفت و اظهار داشت که آن‌ها فقط با مشارکت هم می‌توانند کارها را پیش ببرند. او گفت: «ما موفقیت‌ها و شکست‌هایی خواهیم داشت، اما باید با هم کار کنیم.» به گفته گیلن، وجود 23

زبان و 28 محدوده قضایی در گستره مرزهای اروپا، سطح شناسایی جرم‌های سایبری و نبود ساز و کاری برای ارائه گزارش‌های جهانی تنها برخی از مشکلات روزانه‌ای است آن‌ها با آن روبه‌رو هستند. به مشکلات قانونی مواردی مانند گردآوری شواهد کافی برای ارائه دادخواست به دادگاه را نیز بیافزایید. به گفته گیلن، تفاوت شواهد در فضای سایبری با شواهد در جهان فیزیکی (برای مثال، قاچاق مواد مخدر) این است که در جهان فیزیکی شواهد فیزیکی نیز وجود دارند. آن‌ها یک جایی خواهند بود و کسی آن‌ها را خواهد خرید، گردآوری خواهد کرد، به کار خواهد برد، خواهد فروخت و از آن پول درخواهد آورد. یک صنعت کامل آن را احاطه کرده است. در موارد سایبری شواهد ناپایدار هستند. آن‌ها داده‌ها هستند که می‌توانند دستکاری شوند، حذف شوند، از رسانه‌ای به رسانه دیگر منتقل شوند، نابود شوند و چیزی به آن‌ها افزوده شود. این باعث می‌شود که شواهد سایبری اتکاناپذیر، غیردقیق، و در بدترین حالت ضمن دادخواهی غیرقابل قبول باشند یا شاید بدتر، در اثر نابودی دیگر موجود نباشند.
هم گیلن و هم اورتینگ سیستم گزارش‌دهی را یکی از مشکلات کنونی می‌دانند؛ زیرا هیچ رویه استانداردی برای این کار وجود ندارد. اورتینگ می‌گوید: «ما می‌کوشیم با سیستم قضایی قرن 19 به جنگ جرایم قرن 21 برویم.» او به ساز و کارهای کنونی در بررسی جرم‌های سایبری اشاره می‌کند که دنباله‌روی همان ساز و کاری است که از آن در بررسی جرم‌های فیزیکی استفاده می‌شود؛ یافتن شواهد و پرس‌وجوی پلیس برای به‌دست آوردن اطلاعات. ضمن این که انجام همین بررسی‌ها نیز در برخی کشورها ممکن است و در بعضی دیگر از کشورها بدون دستور دادگاه نمی‌توان چنین کاری کرد. وقتی از اورتینگ پرسیده شد که آیا با مسئولان قضایی در کمیسیون اروپا در ارتباط است یا نه، گفت که او اغلب جرایم سایبری را برای همه قدرت‌های این اتحادیه که با آن‌ها دیدار داشته باشد توضیح می‌دهد، اما تأیید می‌کند که مشکلات درخصوص قانون‌گذاری پابرجا است و می‌افزاید هرچند در این حیطه مشکلاتی وجود دارد، اما این‌ها مواردی هستند که در حیطه مسئولیت‌های سیاست‌مداران جای می‌گیرند.

یکی دیگر از مشکلاتی که کم‌تر آشکارا درباره آن سخن گفته شده است، امکانات بسیار اندک بعضی کشورهای اروپایی در بررسی جرم‌های سایبری است. کریستین مارک لیفلندر، مشاور سیاست‌گذاری دفاع سایبری بخش چالش‌های امنیتی پیش‌رفته ناتو، گفته بود که برخی از کشورهای اروپای شرقی برای مقابله با جرایم سایبری امکانات بسیار کم‌تری دارند. برخی کشورها حتی مجوز ENCASE هم ندارند که لازمه بازرسی کامپیوترهای شخصی/ درایوهای سخت است.
گیلن نیز می‌گوید، در حال حاضر برای کسی که درباره فضای سایبری به‌دنبال اطلاعات است، پلیس بهترین گزینه نیست. این اطلاعات را باید از شرکت‌های بخش خصوصی، قربانیان جرایم سایبری، مؤسسه‌های مالی، آی‌اس‌پی‌ها، شرکت‌های میزبانی‌شده و... دریافت کرد. از نظر او چنین شرکت‌هایی تخصص بیش‌تری دارند و می‌توانند به آن‌ها که ظرفیت کم‌تری دارند مشاوره دهند. او می‌گوید: «نمی‌توانیم تحمل کنیم که در این زنجیره پیوند ضعیفی وجود داشته باشد. باید مطمئن شویم که همه به پیش می‌آیند.»
در خلال گزارش خبرنگار SC Magazine، بازرسان EC3 وارد اتاق می‌شوند و درباره هر چیزی از تجارب مورد نیاز گرفته تا تازه‌ترین تهدیدها به گفت‌وگو می‌پیوندند. پس‌زمینه کاری آن‌ها متفاوت است، اما بیش‌ترشان در کشورهای خود در واحدهای جرایم سایبری پیش‌رفته کار کرده‌اند. زبان مشترک آن‌ها انگلیسی است. آن‌ها می‌گویند از جمله

روندهای کلیدی کنونی در جرم‌های سایبری، استفاده از Tor برای مکاتبه‌های سایبری مجرمانه، افزایش بات‌نت‌های در حال کار، و سرورهای دستور و کنترل (C&C) است. همچنین، در کلاهبرداری‌های مربوط به کارت‌های EMV، مبالغ سرقتی در کشورهایی که از EMV پشتیبانی نمی‌کنند، به پول نقد تبدیل می‌شوند.
جاپ ون اوس، سرپرست بخش سایبورگ در EC3، درباره نقش خود در یوروپل طی هفت سال گذشته می‌گوید: «فکر می‌کنم جرم‌های سایبری چیزی است که باید در سطح بین‌المللی حل شود؛ از این رو، وقتی شانس این را یافتم که در سال 2007 در این‌جا کار کنم، قدر این موقعیت را دانستم و هنوز این‌جا هستم. فکر می‌کنم یک دگرگونی بزرگ این است که هم‌اینک جرم‌های سایبری به‌صورت روزانه و خیلی زیاد در همه سطوح در دستور جلسه‌های اقتصادی و بانکداری قرار می‌گیرند. اینک همه اظهار می‌دارند که چنین مشکلی وجود دارد و به‌سرعت در حال رشد است.»
مارسین اسکورنک، مدیر بخش «پایانه»، یک افسر پلیس لهستانی بود و یک سال بعد به بخش جرایم مالی سازمان‌یافته یوروپل منتقل شد و اکنون کار او پایش کلاهبرداری‌های مرتبط با پرداخت‌های مالی است؛ حیطه‌ای که به گفته او از مواردی مانند جعل کارت‌های مالی به هک کردن سامانه‌های خودپرداز متمایل شده است. همه بازرسان روز خود را با پایش «الگوها» در این فضا آغاز می‌کنند و می‌گویند تروجان‌های بانکی، سرویس‌های ناشناس‌ساز، و جرم سایبری در قالب سرویس (Cyber-crime-as-a-service) از جمله رایج‌ترین جرم‌های سایبری هستند. این مورد آخر در گزارش اخیر ارزیابی تهدیدهای جرایم سازمان‌یافته اینترنتی مورد اشاره قرار گرفت و اورتینگ می‌گوید که شمار بدافزارنویسان زبده خیلی کم است. گیلن با تشبیه بازرسان خود به تیم فوتبال می‌گوید: «هر کسی تجارب متفاوتی دارد.» به گفته اورتینگ، EC3 هم‌اکنون با سه دانشگاه در سطح کارشناسی ارشد امنیت سایبری مشغول همکاری است.

گسترش در آینده

از دید گیلن، اتحادیه اروپا از حیث این گونه جرم‌ها دارد به یک سد بدل می‌شود. او می‌گوید: «می‌توانم خودمان را ببینم که با همکاری هم، به‌گونه‌ای مؤثر به یک نیروی یک‌پارچه در برابر جرم‌های سایبری تبدیل می‌شویم.» و می‌افزاید: «در ده سال آینده خودمان را در شرایطی می‌بینم که کارکنان بسیار بیش‌تری داریم و جرم‌های سایبری را در سطح اتحادیه اروپا به‌صورت دقیق بازرسی می‌کنیم.» به گفته او، شاید زمانی برسد که این همکاری به ایالات متحده و دیگر کشورها و شرکت‌های شریک نیز گسترس یابد.
اورتینگ بر این باور است که مکانیسم‌های گزارش‌دهی و قانون‌گذاری باید ارتقا پیدا کند تا بتواند در برابر جرم‌های سایبری بایستد. اما این موضوع را نیز مورد تأکید قرار می‌دهد که باید اینترنت را به‌صورت یک منبع مشترک مانند آب پیرامون خود در نظر بگیریم. این شبکه به کسی تعلق ندارد. ما نباید هیچ‌گونه آلودگی را در اینترنت بپذیریم. باید نحوه محافظت از اینترنت را بیابیم. در این‌جا است که نقطه مشترک با چینی‌ها و روسی‌ها نیز خودش را نشان می‌دهد؛ زیرا آن‌ها نیز چنین چیزی را می‌خواهند. به گفته او، آن‌ها همواره جاسوسی یکدیگر را خواهند کرد، اما دست‌کم می‌توان با جرم‌های سایبری سازمان‌یافته مبارزه کرد و درباره آن به توافق رسید. این چیزی است که EC3 می‌کوشد انجام دهد.

منبع:

تاریخ انتشار:
07 بهمن 1393

نشانی منبع: https://www.shabakeh-mag.com/security/232