رویداد

دستور برای استخدام نیرو در حوزه امنیت اطلاعات

■ **ایسنا:** رییس سازمان فناوری اطلاعات از دستور رییس‌جمهوری برای جذب نیروهای انسانی در زمینه امنیت فناوری اطلاعات خبر داد. علی حکیم جوادی با اعلام این خبر گفت: مدتی است برای تامین امنیت بیشتر، رییس‌جمهور دستور جذب نیروهای انسانی مورد نیاز در زمینه امنیت فناوری اطلاعات را صادر کرده و قرار است این نیروها از طریق معاونت توسعه نیروهای ریاست‌جمهوری تامین شود. وی ادامه داد: محدودیتی برای جذب نیرو در این زمینه تعیین نشده و تنها گفته شده است که نیروهای مورد نیاز تامین شوند.

ارزیابی امنیتی محصولات حوزه فضای تبادل اطلاعات

■ **شرق:** براساس تصمیم اعضای کارگروه فاوا، وزارت ارتباطات و فناوری اطلاعات موظف شده است ضمن حمایت از طراحی و توسعه محصولات افتا و ضد بدافزار بومی درخصوص ارزیابی امنیتی انواع محصولات داخلی و خارجی فتا و صدور گواهی تایید محصولات نیز اقدامات لازم را انجام دهد. طی بخشنامه وزارت ارتباطات و فناوری اطلاعات به تمامی دستگاه‌های اجرایی موضوع ماده پنج قانون مدیریت خدمات کشوری ابلاغ شد که ضمن به کارگیری محصولات بومی افتا از تخصیص اعتبار برای خرید محصولات افتا و ضد بدافزارهایی که به تایید این وزارتخانه نرسیده است، خودداری کنند.

عضویت ایران در فدراسیون بازی‌های آسیا

■ **شرق:** بنیاد ملی بازی‌های رایانه‌ای به عضویت سازمان بازی‌های جدی سنگاپور (Serious Games Association) که برای مشارکت در توسعه بازی‌های جدی و فناوری شبیه‌سازی در سنگاپور و فراتر از آن در جنوب شرقی آسیا تاسیس شده، درآمد.این سازمان بر مباحثی نظیر کاربردهای مختلف بازی در زمینه‌های آموزشی و راهبردی شامل بخش خصوصی و دولتی، صنعت و آکادمیک متمرکز است. سازمان بازی‌های دیجیتال بر پایه یادگیری هنگ‌کنگ، سازمان ملی بازی‌های جدی و شبیه‌سازی هند، بنیاد ملی بازی‌های رایانه‌ای ایران و سازمان بازی‌های جدی ژاپن از اعضای فدراسیون بازی‌های جدی آسیا هستند.

نبرد ۲/۵ میلیارد دلاری «اپل» و «سامسونگ»

■ **فارس:** نبرد چندین ساله اپل و سامسونگ بر سر نقض حقوق مالکیت معنوی وارد یکی از مراحل سرنوشت ساز خود شده است. بر اساس گزارش گاردین، انتخاب اعضای هیات منصفه برای رسیدگی به این پرونده در سانفرانسیسکوی آمریکا از دیروز آغاز شده و انتظار می‌رود رسیدگی به پرونده یاد شده مدت زیادی به طول بینجامد. پیش از این مدیران عامل دو شرکت برای رسیدن به توافق با یکدیگر دیدار کرده بودند، اما نتوانسته بودند برای صلح با هم به راه‌حل قاطعی برسند. بعد از این شکست اپل دوباره شکایت از سامسونگ را آغاز کرد و خواستار دریافت ۲/۵ میلیارد دلار غرامت از سامسونگ شد. این شرکت اولین بار در سال ۲۰۱۱ از سامسونگ شکایت کرده و به علت کپی‌برداری از طراحی آی‌فن و آی‌پد خواستار دریافت غرامت شده بود.

سرمقاله نیویورک تایمز هک شد

■ **ایتنا:** هکرها با دستکاری در سایت روزنامه نیویورک‌تایمز، یک سرمقاله جعلی به نام این روزنامه معتبر منتشر کردند. بر اساس گزارش خبرگزاری فرانسه، این اقدام هکرها، خشم مسوولان این روزنامه پرسابقه را به دنبال داشته است.این سرمقاله غیرواقعی که به موضوع ویکی‌لیکس می‌پرداخت، با قلم بیل کلر (Bill Keller) سردبیر سابق نیویورک‌تایمز منتشر شد. آقای کلر در موضوعات مربوط به ویکی‌لیکس تحقیقاتی انجام داده و در این خصوص مقالاتی نیز به رشته تحریر درآورده است. پس از آن تیم بیلتون (Tim Bilton) سردبیر بخش فنی نیویورک‌تایمز که از شیطنت هکرها بی‌اطلاع بود، این مطلب را در توییتر منتشر کرد. پس از فاش شدن موضوع، آقای کلر با انتشار یک توییت گفت: یک سرمقاله غیرواقعی درباره ویکی‌لیکس به اسم من منتشر شده است. به دنبال آن آقای بیلتون پیام قبلی خود را حذف کرد. هنوز هویت فرد یا گروهی که دست به این اقدام موذیانه زده، مشخص نشده است.

وجین کسپرسکی:

ارتباطی با دولت پوتین نداریم

■ **فارس:** Eugene Kaspersky رییس شرکت کسپرسکی، بزرگ‌ترین موسسه امنیت سایبری روسیه اخبار منتشر شده در مورد روابط نزدیکش با دولت این کشور را رد کرد. بر اساس گزارش وایرد، اولین بار این سایت، اطلاعاتی را در مورد شرکت کسپرسکی منتشر کرد که نشان می‌داد کارشناسان امنیتی آن روابط نزدیکی با دولت روسیه و سرویس‌های امنیتی آن دارند. این اخبار و اطلاعات پس از آن منتشر می‌شود که رسانه‌های مختلف از روابط نزدیک شرکت‌هایی مانند گوگل، فیس‌بوک و مایکروسافت با کاخ سفید و سازمان جاسوسی سیا خبر می‌دهند. رییس کسپرسکی علت رجوع مقامات دولتی روسیه به این شرکت را تنها تخصص کارکنان آن عنوان کردند.

اجرای مصوبه سازمان تنظیم مقررات

۱۰ درصد کاربران؛ پیامک تبلیغی نمی‌خواهند

شرق: شیوه ارسال پیامک‌های تبلیغاتی و انبوه به تلفن‌های همراه نزدیک به ۶۰ میلیون ایرانی و افزایش روزافزون تعداد این پیامک‌ها بدون اجازه مشترکان در تمامی ساعات شبانه‌روز و حتی نیمه‌های شب، مورد انتقاد بسیاری از مشترکان بود که با این وجود سازمان تنظیم مقررات و ارتباطات رادیویی با تصویب طرحی اپراتورهای تلفن همراه را به کسب اجازه قبلی از مشترکان برای ارسال پیامک‌های انبوه تبلیغاتی، خبری و اطلاع‌رسانی مکلف و اعلام کرد که این مصوبه را در تاریخ ۱۹ بهمن به اپراتورهای اول، دوم و سوم تلفن همراه ابلاغ کرده است. به گزارش «مهر» پس از این مصوبه، اپراتورهای موبایل با ارایه دستورالعملی تمایل مشترکان برای دریافت این پیامک‌ها را بررسی کردند و با ارسال پیامکی از مشترکان خواستند که در صورت عدم تمایل به دریافت پیامک، موضوع را به اپراتور اعلام کنند. به دنبال استعلام پیامکی اپراتورهای موبایل از مشترکان برای تمایل یا عدم تمایل به دریافت پیامک‌های تبلیغاتی، اطلاع‌رسانی و خبری بالغ بر ۱۰درصد مشترکان تلفن همراه اعلام کرده‌اند که تمایلی به دریافت این پیامک‌ها ندارند. اما این در حالی است که با گذشت چندین ماه از ابلاغ مصوبه ممنوعیت ارسال پیامک‌های تبلیغاتی بدون موافقت مشترکان شواهد نشان می‌دهد که همچنان مشترکان موبایل اپراتورهای اول و دوم همچنان روزانه تعداد بی‌شماری پیامک‌های تبلیغاتی ناخواسته دریافت می‌کنند و این درحالی است مسوولان سازمان تنظیم مقررات و ارتباطات رادیویی گفته‌اند که اپراتورهای موبایل نسبت به ارسال پیامک برای تایید موافقت مشترکان اقدام کرده‌اند. و حتی کار به آنجا رسید که مسوولان سازمان تنظیم مقررات و ارتباطات رادیویی بیان کردند گزارش فعالیت اپراتورها را برای عدم اعمال این مصوبه به سازمان تعزیرات حکومتی می‌فرستیم. براساس مستندات حقوقی، ارسال پیامک بدون رضایت مشترک نوعی مزاحمت تلقی شده و با توجه به اینکه این مزاحمت توسط دستگاه‌های مخابراتی صورت می‌پذیرد وفق ماده ۶۴۱ قانون مجازات اسلامی قابل پیگرد خواهد بود.

۱۰ درصد مشترکان تمایل به دریافت پیامک تبلیغاتی ندارند

پیشتر مسوولان سازمان تنظیم مقررات و ارتباطات اعلام کرده بودند که موافقت یا عدم موافقت با دریافت پیامک‌های تبلیغاتی حداکثر ظرف یک هفته آینده از تمامی مشترکان اپراتورهای موبایل در کشور استعلام خواهد شد. اما اپراتورهای موبایل برای برخی مشترکان پیامک استعلام دریافت را ارسال کرده بودند اما بعد از ۲۴ ساعت مجددا ارسال پیامک‌های تبلیغاتی برای این مشترکان آغاز شد، که در این‌باره حسن رضوانی بیان کرد در این زمینه به اپراتورهای موبایل تذکر داده شد و این موارد نیز هم‌اکنون اصلاح شده است. معاون نظارت و اعمال مقررات سازمان تنظیم مقررات و ارتباطات رادیویی افزود: این موضوع مربوط به برخی شرکت‌های طرف قرارداد اپراتورهای موبایل بود که با تذکر و هشدار به جریمه حل و فصل شده است. البته این مقام مسوول در نهایت از تعیین تکلیف نهایی پیامک‌های ارسالی تبلیغاتی به مشترکان خبر داده و گفته بود مواردی که با اعتراض مشترکان روبه‌رو شده بود نیز پاسخ داده خواهد شد. اینک با گذشت دو ماه از اظهارات مسوولان رگولاتوری، حسن رضوانی بیان کرد این مصوبه هم‌اکنون در کل کشور اجرایی شده و شواهد و مستندات ارایه‌شده نشان می‌دهد که مشترکان مشکلی بابت دریافت این پیامک‌ها ندارند. او می‌افزاید: تنها به دلیل برخی اشکالات در سیستم فنی، پیامک استعلام از تمایل دریافت پیامک به تعداد معدودی از مشترکان نرسیده و در سیستم به ثبت نرسیده است و چنانچه به هر دلیلی مشترکان موبایل اس‌ام‌اس استعلام دریافت پیامک را از اپراتور دریافت نکرده‌اند باید با تماس با مرکز تماس و امور مشترکان اپراتورها تمایل یا عدم تمایل خود را برای دریافت این پیامک‌ها گزارش کنند. به گفته او براساس مستندات ارایه‌شده از سوی اپراتور اول تلفن همراه تنها ۱۰ درصد مشترکان این اپراتور از ۳۲ میلیون مشترک فعال در این شبکه تمایلی به دریافت پیامک تبلیغاتی نداشته‌اند و این خدمات برای این تعداد مشترکان هم‌اکنون مسدود شده است. در همین حال از اپراتور دوم نیز خواسته‌ایم مستندات خود را در اجرای این طرح به سازمان تنظیم مقررات و ارتباطات رادیویی ارایه دهد. معاون سازمان رگولاتوری ادامه می‌دهد: از بستر شبکه اپراتور دوم پیامک تبلیغاتی ارسال نمی‌شود و تنها پیامک‌های اطلاع‌رسانی این اپراتور است که چنانچه مشترکان تمایلی به دریافت این پیامک‌ها نداشته باشند، می‌توانند با تماس با مرکز تماس این اپراتور نسبت به قطع این خدمات اقدام کنند.

> **به دنبال استعلام پیامکی اپراتورهای موبایل از مشترکان برای تمایل یا عدم تمایل به دریافت پیامک‌های تبلیغاتی، اطلاع‌رسانی و خبری بالغ بر ۱۰درصد مشترکان تلفن همراه اعلام کرده‌اند که تمایلی به دریافت این پیامک‌ها ندارد. اما شواهد نشان می‌دهد که مشترکان همچنان پیامک‌های تبلیغاتی ناخواسته دریافت می‌کنند**

پیامک‌های تبلیغاتی را مسدود نکنید

در مقابل مسوولان شرکت مخابرات بر این عقیده‌اند تعداد پیامک‌های تبلیغاتی که برای کاربران تلفن همراه ارسال می‌شود آنقدر نیست که باعث شکایت مشترکان شود. به گفته داوود زارعیان میانگین ارسال پیامک انبوه و تبلیغاتی برای هر مشترک کمتر از دو پیامک در هفته است و این آمار نشان می‌دهد تعداد این پیامک‌ها آنقدر نیست که باعث شکایت تعداد زیادی از مشترکان شود. مدیرکل روابط عمومی شرکت مخابرات ایران بیان می‌کند پیامک‌های تبلیغاتی پس از ساعت ۱۲ شب ارسال نمی‌شود و امکان دریافت آن در ساعات نیمه‌شب بعید به نظر می‌رسد، مگر آنکه موبایل مشترک مقصد خاموش بوده یا خارج از محدوده سرویس‌دهی باشد که پیامک در سیستم ذخیره شده و بعد از این زمان به مشترک می‌رسد. او تاکید کرد در صورتی که پیامک تبلیغاتی مشترکان غیرفعال و مسدود شود دیگر هیچ‌گونه اخطار یا حتی پیام اطلاع‌رسانی و آموزشی نیز دریافت نخواهند کرد. زارعیان در ادامه همچنان بر عدم انسداد پیامک‌های تبلیغاتی تاکید داشته و می‌گوید: هیچ اپراتوری خدمات‌دهی خود را محدود نمی‌کند و زمانی می‌توان این کار را انجام داد که این سرویس‌دهی برای مشترک هزینه‌ای داشته باشد اما با وجودی که پیامک‌هایی که ارسال می‌شود برای مشترک هزینه‌ای دربرندارد و حتی ضروری بوده و آسیب‌رسان نیست به نظر نمی‌رسد نگرانی در پی داشته باشد.

گذرگاه

استراتژی امنیت ملی سایبری ایران

محمد خالدی: ابزارهایی که می‌توان به درستی نام سلاح سایبری را بر آنها گذاشت، نشان می‌دهند که سرمایه‌گذاری دولتی، انجام فعالیت‌های تمرینی و مانور سایبری (نظیر آنچه در مورد استاکس‌نت و فلیم انجام گرفت)، هدف‌گیری روی صنایع خاص یا مناطق خاص، واردآوردن آسیب‌های فیزیکی و انجام تخریب در محیط واقعی از جمله رویکردهای این قبیل سلاح‌هاست که مروری بر سیر حملات و تحرکات دیپلماتیک که به موازات آن انجام گرفته است نکات کلیدی را برای ما آشکار خواهد کرد.

به گزارش سیتنا براساس آمار تاکنون ۳۲ کشور در دنیا، ساختار دفاع سایبری خود را تشکیل داده‌اند و ۱۴۰کشور در حال مطالعه روی توسعه دفاع ملی در کشور خود هستند. در آمریکا با وجود جایگاه ابرقدرت سایبری، طبق نظرسنجی انجام‌شده توسط لیبرمن ریسرچ گروپ ۷۴درصد از مردم آمریکا بالاترین میزان احساس خطر را در رقابت با تروریسم اتمی و میکروبی و... از ناحیه تروریسم سایبری داشته‌اند و با توجه به نشانه‌ها و حساسیت‌هایی که پیشتر توسط کارشناسان بررسی شده است، احتمال پیاده‌سازی سناریوی ۱۱ سپتامبر سایبری در سطح بالایی قرار دارد. کشورهایی مانند روسیه و چین نیز، با درک حساسیت موضوع، سرمایه‌گذاری چشمگیر و توجه و اقدامات ویژه‌ای در این حوزه کرده‌اند، به نحوی که روسیه در سال‌های ۲۰۰۷ و ۲۰۰۸ در طول چند ساعت نظام مدیریتی - حکومتی کشورهای استونی و گرجستان را بدون شلیک یک گلوله از کار انداخت.

چین نیز همواره فارغ از تحرکاتی چون راه‌اندازی شبکه ملی و حتی گوگل ملی، پای ثابت عملیات ویژه سایبری و جاسوسی سایبری در سطح بسیار پیشرفته بوده است.

در سطوح تکنیکی نیز می‌توان از شاخص‌ترین رخدادها همچون بدافزار «دوکو»، «استاکس نت» و «فلیم» نام برد.

به هر حال در پی این موارد و بسیاری از زدوخوردهای پنهان و آشکار دیگر، سطح عمل و نتایج به‌دست‌آمده به حدی از اهمیت می‌رسد که موضع‌گیری‌های رسمی و دیپلماتیک را برمی‌انگیزد. نگاهی به سه حمله بزرگ سایبری به کشورمان که به وسیله بدافزارهای «استاکس نت»، «دوکو» و «فلیم» انجام گرفت، نشان می‌دهد که ابزارهای به کارگرفته‌شده در این حملات به مرور تکمیل شده‌اند و هر بار بر درجه تخریب آنها افزوده شده است.

از دیدگاه فنی پیچیدگی‌های فوق‌العاده بالای بدافزارها، هوشمندی در طراحی و به‌کارگیری، خلاقیت در نحوه عملکرد و سازگاری با فناوری‌های امنیتی شناخته‌شده و رایج، نشان از آن دارد که این ابزارها به وسیله دولت‌ها و با اهداف خاص طراحی و اشاعه داده شده‌اند.

به این ترتیب جنگ سایبری در نگاه غربی‌ها نه‌تنها گزینه‌ای محتمل بلکه عملا جنگی تمام‌عیار است که مدتی نیز از شروع آن می‌گذرد. به موازات اقدامات در حوزه‌های تکنیکی و عرصه‌های دیپلماتیک، غرب فعالیت خود را برای چارچوب‌بندی و تعیین خطوط قرمز و تحمیل آن به دیگر بازیگران آغاز کرده است. به نحوی که پس از دو سال فشار از سوی پنتاگون برای ارایه پیش‌نویس قواعد جنگ سایبری آمریکا، سرانجام این دستورالعمل‌ها در ماه‌های قبل تنظیم شد و به امضای باراک اوباما رسید و در پی آن اعلام شد که هرگونه حمله سایبری از سوی کشورهای دیگر اقدام جنگی بوده و با حمله نظامی پاسخ داده خواهد شد. در واقع وی در تبعیض آشکار دیگری در عرصه بین‌المللی خود را مجاز به پاسخگویی به این به اصطلاح جنگ متمدنانه دانسته و از طرفی به‌صورت پیش‌دستانه از خوف حملات تلافی‌جویانه کشورهایی مانند ایران به تهدید و ارعاب جهانی می‌پردازد تا از این رهگذر خود را در حاشیه امن قرار دهد.

با توجه به مطالب فوق است که باید در رهبری جبهه مقاومت، اتخاذ رویکردی هوشمندانه در حوزه سایبر در دستور کار قرار گیرد تا در آینده علاوه بر قرارگیری در موقعیت کلیدی و برتر، بتوان هزینه منازعات و شکست دشمن را به حداقل ممکن کاهش داد. اما آنچه مهم است، تدوین «استراتژی امنیت ملی سایبری» کشور است که نیاز به آن به صورت روزافزون احساس می‌شود.

تدوین «استراتژی امنیت ملی سایبری» دربرگیرنده چهار حوزه امنیت ملی: سیاسی-امنیتی، فرهنگی- اجتماعی، اقتصادی و نظامی که نحوه تصمیم‌گیری، هدایت و کنترل امور را از سطح تکنیک تا استراتژیک در حوزه‌های سلبی- ایجابی، آفندی- پدافندی و خارجی- داخلی کشور پوشش دهد، بسیار ضروری به نظر می‌رسد.

این طرح باید ماموریت‌ها، وظایف، الزامات و اصول و فرمول‌های هدایت راهبردی، ایجاد ساختارهای نوین، خط مشی‌ها، رویه‌ها، پروتکل‌ها و چارچوب چینش و هماهنگی و هدایت یکپارچه عناصر را از بالا به پایین پوشش دهد و توسعه تاکتیک‌ها و تسلیحات ویژه این جنگ را در دستور کار قرار دهد. با تدوین و اجرایی کردن این طرح در ذیل و راستای «استراتژی بزرگ» کشور است که می‌توان کنش‌ها و واکنش‌های کشور را در حوزه سایبر و تمامی حوزه‌های مربوط به نحوی تنظیم کرد.

بازیکده

راز کارآگاه ویژه

مجید نوردوست: سبک بازی‌های ماجراجویی به صورت سنتی دارای داستان‌هایی بسیار زیبا و چالش‌برانگیز هستند، اما در این مدت شاهد این موضوع بودیم که داستان در این سری از بازی‌ها نقش کمرنگ‌تری داشته و حتی سبک ماجراجویی به سمت سبک اکشن هم پیش رفته است. حال استودیوی اوکراینی Frogwares سازنده بازی The Testament of Sherlock Holmes قصد دارد تا بازی‌ای بسیار چالش‌برانگیز را خلق کند که سبک بازی‌های ماجراجویی را به دوران طلایی‌اش بازگرداند. اولین چیزی که در این بازی نظر شما را به خودش جلب می‌کند، پیشرفت گرافیکی آن است که در مقایسه با نسخه‌های قبلی بهتر شده است. انیمیشن‌ها نرم و روان‌تر شده‌اند و حالت طبیعی‌تری به خودشان گرفته‌اند. کسانی که به این دلیل نسخه قبلی را بازی نکرده‌اند، امیدوار باشند که می‌توانند این نسخه را تجربه کنند. روند بازی به شکلی است که بازیکنان می‌توانند حالت دوربین بازی را بین دو حالت اول‌شخص و سوم‌شخص تغییر دهند یا حتی می‌توانند آن را به صورت ۲/۵بعدی و به صورت Point and Click بازی کنند. در حالت سوم‌شخص می‌توانید دوربین را دور شخصیت بازی حرکت دهید تا بتوانید زاویه دلخواه را به دست بیاورید. همچنین باید به این موضوع اشاره کنیم که گرافیک بازی همچنان المان‌های نسخه Jack the Ripper را دارد. اضافه شدن قابلیت انتخاب حالت دوربین بازی، باعث شده که این نسخه روی کنسول‌ها بهتر اجرا شود و بازیکنان مشکلی با کنترل شخصیت بازی نداشته باشند. در نسخه قبلی این بازی، ناشر فرانسوی آن، یعنی شرکت Focus Home Interactive بازخوردهای زیادی را از بازیکنان نسخه Xbox 360 دریافت کرد که فضای بازی باید به شکل 3D باشد، چراکه اکنون این سبک گرافیک به خوبی می‌تواند جذابیت بازی‌های ماجراجویی را زیاد کند و به جذب مخاطب‌های بیشتر به سمت این سبک نیز کمک می‌کند. در نسخه قبلی، معماهای بسیار سختی در بازی وجود داشتند که برای حل کردن آنها باید زیاد فکر می‌کردید و محیط بازی را به دقت مورد بررسی قرار می‌دادید. همین موضوع باعث می‌شد که مدت‌زمان بازی بسیار طولانی باشد و حتی خیلی‌ها بازی را تا انتها ادامه ندهند. بعد از سه نسخه از این سری که شباهت‌های زیادی به یکدیگر داشتند، بد نیست طرفداران بدانند که در Testament با قابلیت‌های پیش‌بینی‌شده کمتری مواجه می‌شوند و همچنین بازی به شکل خاصی روی خود شخصیت هولمز تمرکز دارد. این موضوع از همان بخش آموزشی بازی به چشم می‌آید که شخصیت هولمز را در اتاق مجللی مشاهده می‌کنید. بعد از اینکه او با بررسی محیط، سرنخ‌های مهمی به‌دست می‌آورد، به حالت Exposition Mode می‌رود تا یک گردنبند را از داخل جعبه‌ای بسته پیدا کند. صبح روز بعد، بازی به خیابان B Baker Street 221 می‌رود. واتسون (Watson) دوست همیشگی هولمز در حال روزنامه خواندن است و به او اعداد مرموزی را نشان می‌دهد که فکر می‌کند نقشی را در ماجرای جدید آنها ایفا می‌کند. در روزنامه‌ای که واتسون در حال خواندن آن است، به این موضوع نیز اشاره شده که گردنبندی که پیدا کرده‌اند، تقلبی بوده است. پس از مدتی سربازرس باینس (Baynes) همراه با گردنبند از راه می‌رسد و اینجاست که اولین معمای کوچک بازی را باید حل کرد. باید گردنبند را از زوایای مختلف مورد بررسی قرار دهید و چند علامت مختلف روی آن پیدا کنید که باعث می‌شوند تقلبی بودن آن ثابت شود. از اینجا به بعد، داستان بازی شکل مرموز خودش را نمایش می‌دهد. آنها به دنبال بررسی گردنبند و روزنامه‌ای که خبر تقلبی بودن آن را چاپ کرده، می‌روند و پس از مدتی سرنخ، آنها را به یک کشیش محلی می‌رسانند. اما کمی قبل از اینکه آنها به کشیش دسترسی پیدا کنند، کشیش به شکل بیرحمانه‌ای به قتل می‌رسد. از این قسمت به بعد تحقیقات اصلی آغاز می‌شود و باید با استفاده از چیزهای بسیار معمولی یا سرنخ‌های بسیار پیش پا افتاده، معماهای بازی را حل کنید. هولمز فکر می‌کند که کشته شدن کشیش به دلیل اخاذی او بوده و باید به هدف اصلی قاتل پی برد. البته هولمز در این بین درگیر ماجراهای دیگری می‌شود که اطلاعات زیادی از آنها منتشر نشده. اینها ماجراهایی هستند که بیشتر به خود شخصیت هولمز مربوط می‌شود. بازیکنان در این بازی با دو روند مرموز روبه‌رو خواهند شد. یکی ماجرای قتل کشیش و دیگری اتفاقاتی که برای خود هولمز در بازی رخ می‌دهد و همچنین پیش‌زمینه‌هایی از اتفاقات رخ‌داده در بازی داده می‌شوند که نقش مهمی را ایفا می‌کنند. سازندگان به این موضوع اشاره می‌کنند که بازی آنها بین ۱۰ تا ۱۵ ساعت طول می‌کشد و بازیکنان در این نسخه با ماجراهای بسیار خوبی روبه‌رو خواهند شد.

دیدگاه

بررسی جرم تحصیل و افشای اسرار تجاری الکترونیک

گلسارا پویان
وکیل پایه یک دادگستری

■ امروزه فضای مجازی این امکان را به تجار و معامله‌گران داده تا بدون نیاز به صرف هزینه‌های گزاف برای سفر به اقصا نقاط عالم، با مراجعه به تارنمای طرف مقابل یا ارسال و دریافت رایانامه، معامله کنند و در عصر اطلاعات، نحوه نگاهداری اسناد و مدارک شرکت‌ها و بنگاه‌های تجاری نیز دستخوش تغییرات اساسی شده است. از این رو در کنار محاسن این پیشرفت، کارکردهای منفی آن را نیز نباید از نظر دور داشت، چراکه کم حجم بودن فایل‌ها و در بسیاری مواقع مشترک بودن حق دسترسی به اطلاعات حساس تجاری یا ارسال آن از طریق اینترنت، خطر دسترسی رقبا و افشای اسرار تجاری را بالا برده است. سوال اینجا است که با توجه به نوین بودن شیوه‌های حفظ اسرار تجاری، آیا قانون‌گذار چاره‌ای برای دستاندازی به این اسرار اندیشیده است؟ خوشبختانه جواب مثبت است؛ مواد ۶۴، ۶۵و ۷۵ قانون تجارت الکترونیک، حربه قانون‌گذار برای مقابله با این روند به شمار می‌آیند، ماده ۶۴ این قانون جرم تحصیل و افشای اسرار تجاری را چنین تعریف می‌کند که: «به منظور حمایت از رقابت‌های مشروع و عادلانه در بستر مبادلات الکترونیکی، تحصیل غیرقانونی اسرار تجاری و اقتصادی بنگاه‌ها و موسسات برای خود یا افشای آن برای اشخاص ثالث در محیط الکترونیکی جرم محسوب و مرتکب به مجازات مقرر در این قانون خواهد رسید.». شرایط اثباتی این جرم نیز به شرح ذیل است:

برای تحقق هر جرم سه عنصر مادی، معنوی و قانونی باید فراهم باشد، با توجه به متن مواد قانونی یاد شده، عنصر مادی این جرم با دو فعل مثبت و مادی تحصیل و افشا محقق می‌شود و موضوع جرم نیز اسرار تجاری الکترونیک است، صرف‌نظر از ماهیت الکترونیک بودن آنها، چه اطلاعاتی را می‌توان اسرار تجاری قلمداد کرد؟ به‌طور خلاصه اسرار تجاری از دیدگاه سازمان بین‌المللی مالکیت فکری، اطلاعات محرمانه‌ای هستند که دارای چنان ارزش تجاری‌ای هستند که سری نگاه داشته شده و به این منظور تدابیر امنیتی ویژه‌ای اندیشیده شده باشد. البته قانون‌گذار نیز در ماده ۶۵ همان قانون، با رعایت کلیات تعریف سازمان جهانی مالکیت فکری و با عنایت به شکل ویژه (الکترونیکی بودن) این اسرار، آن را تعریف می‌کند. نکته مهم در دو تعریف، تاکید روی شیوه نگاهداری و ارزش معاملاتی این اسرار است، یعنی چنانچه اطلاعات قابل معامله به صورت نامناسب نگهداری و در دسترس عموم قرارداده شده باشند و به سرقت روند، این جرم محقق نمی‌شود. نکته دیگر درخصوص فعل مجرمانه، بحث رابطه مجرم با بنگاه است، گاه فردی به دلیل رابطه استخدامی یا حقوقی‌ای که با یک شرکت (بنگاه تجاری) دارد، به‌طور مجاز به اسرار تجاری دسترسی پیدا می‌کند، بنابراین این فرد با پشت کردن به اعتماد یا قراردادهای محرمانگی‌ای که میان وی با آن بنگاه‌ها وجود دارد، این اطلاعات را افشا می‌کند، در اینجا عنصر تحصیل اطلاعات خودبه‌خود محقق شده و عنصر مجرمانه را تنها عمل افشاگری تشکیل می‌دهد، اما درخصوص آن دسته اشخاصی که دارای این دسترسی اولیه نیستند، هر دو فعل تحصیل و افشا می‌تواند موضوعیت داشته باشد، چراکه از دید قانون‌گذار تحصیل اسرار تجاری متعلق به غیر، به قصد افشا؛ خود جرم است و به طریق اولی آن هنگام که فرد اسرار تجاری رقیب را غیرقانونی تحصیل کرده و افشا می‌کند نیز این جرم محقق می‌شود. لازم به ذکر است که برای تحصیل یا افشای اسرار تجاری الکترونیک تنها راه‌های استفاده از بدافزارهای رایانه‌ای مد نظر قانون‌گذار نبوده و نکته قابل توجه این است که اگر نحوه تحصیل این اسرار، خود جرمی مستقل باشد، برای نمونه فرد برای ورود به ساختمان شرکت، حرز- در اصطلاح حقوق جزایی عبارت است از: تخریب، سوراخ کردن، شکافتن، کندن حصار و در و قفسه و صندوق و هر حافظ دیگر از این قبیل_ را شکسته و رایانه‌ای را سرقت کند، علاوه بر مجازات جرم یاد شده به مجازات سرقت نیز محکوم خواهد شد. (موضوع مواد ۴۶ و ۴۷ قانون مجازات اسلامی) افشای این اسرار نیز منحصر به روش‌های مجازی یا الکترونیکی نیست و هر نوع روشی را در بر می‌گیرد.

درخصوص رکن معنوی این جرم باید به قسمت اول ماده ۷۵ توجه کرد که می‌گوید: «هرکس به منظور رقابت، منفعت یا ورود خسارت به بنگاه‌های تجاری...، اسرار تجاری آنان را برای خود تحصیل کرده یا برای اشخاص ثالث، افشا کند...» بنابراین علاوه بر قصد عام- انجام عمل مجرمانه - این جرم نیازمند اثبات قصد خاص هم است، یعنی مجرم باید از ارتکاب عمل خود قصد رقابت ناعادلانه، منفعت‌طلبی یا وارد آوردن خسارت به بنگاه را داشته باشد. در نهایت رکن قانونی این جرم را مواد ۶۴، ۶۵و ۷۵ قانون یادشده تشکیل می‌دهند و مجازات این جرم نیز در صورت وجود و اثبات دو رکن مادی و معنوی (به شرح یادشده) حبس شش‌ماه تا دو سال و نیم و جزای نقدی معادل ۵۰میلیون ریال است. بنابراین در صورتی که شرکتی با چنین وضعیتی روبه‌رو شود، می‌تواند از دستگاه قضایی انتظار مجازات مجرم را داشته باشد، به این ترتیب است که قانون‌گذار گامی بسیار موثر برای حفاظت شیوه‌های نوین تجارت برداشته و امید می‌رود تا شاهد این روند مثبت درخصوص سایر مظاهر نوین فناوری که نیازمند وضع قوانین خاص هستند، نیز باشیم.