نکات تحلیلی ایمیل از زاویه جزایی

نگاهی به جرائم سایبری

در شماره پیشین ماهنامه قضاوت، بحث تحلیل ابزاری یا تحلیل یک سرویس به جای پرداختن به دکترین یا تئوری در قالب بررسی مسائل ایمیل (پست الکترونیک) به قلم محمدحسن دزیانی ارائه شد. در این بخش قسمت سوم این مقاله را پی خواهیم گرفت و از زاویه جزایی به برخی نکات تحلیلی ایمیل (پست الکترونیک) اشاره خواهیم کرد. آنچه در این مقاله می آید فقط خلاصه و زمینه ورود به مباحث تفصیلی است و برای مطالعه بیشتر باید از منابع موجود و به ویژه کتاب بزرگ و ارزشمند مصور اینترنت استفاده کرد.

ب- جنبهٔ جزایی

از جنبه یا لحاظ جزایی باید بین مسائل ماهوی، شکلی، بین المللی و کشف علمی در عین ارتباط با هم، مرزی قائل شد و به تفکیک به هر یک پرداخت. از نظر ماهوی می توان به بحث عمد و بی مبالاتی، مسئولیت کیفری، عنصر مادی و . . . اشاره کرد. هم چنین در بحث ماهوی جرائم احتمالی باید ذکر شود که با یک تقسیم بندی جزئی تر می توان بحث ماهوی را به جزای عمومی و جزای اختصاصی تقسیم کرد.

الف - جزای ماهوی عمومی

در این سخن از عمد و بی مبالاتی و مسئولیت کیفری و بعداً عنصر مادی است البته در عنصر مادی است که عمد و بی مبالاتی مطرح می شود و بحث مسئولیت کیفری مقوله جدایی است.

۱- در برخی نظامهای قضایی و حقوقی زمانی که ایمیل در اختیار افراد ناصالح یا غیر مجاز قرار می گیرد مسئولیت کیفری تحقق پیدا می کند زیرا با این کار اطلاعات مهم لو می رود و حتی هکرها به اطلاعات سیستم می توانند دست یابند.

گاه رفتن به سایتهای ناشناس موجب تحقق مسئولیت می شود. در مورد افراد نظامی و امنیتی و انتظامی این امر بسیار کاربرد دارد زیرا این کار آنها سیستم کامپیوتری را به خطر می اندازد. هکرها به دنبال بدست آوردن شماره تلفن مورد استفاده سرور، ایمیل افراد مهم و حساس و . . . هستند. در غیر افراد مهم نیز در بحث جرائم سازمان یافته و . . . ، افراد عادی در معرض خطر هستند. طبعاً بی مبالاتی یا عمد موجب تخریب، جاسوسی و . . . می شود.

۲- گاه مسئولیت ناشی از عدم به کارگیری روالهای امنیتی است. در هر سیستم باید امنیت کافی تأمین شود حتی در قراردادهای مدیریت سیستم انفورماتیک یا به اصطلاح قرارداد برون سپاری این امر باید تأکید شود.

زیرا کوتاهی در انجام تعهدات از سوی مدیر انفورماتیک نه تنها موجب مسئولیت قراردادی و حتی مدنی بلکه موجب تحقق مسئولیت کیفری می شود این روالهای امنیتی را باید در صورت وجود، فعال کرد و در صورت نیاز نصب کرد در شرکت ها، سیستم های اداری و . . . این امر مهم تر و دارای لزوم بیشتری است ISPها یا همان تهیه کنندگان خدمات اینترنت باید چنین روالهای امنیتی را بکار گیرند وگرنه طیف وسیع مشتریان خود را با انواع مخاطرات مواجه می کنند یا در برابر مخاطرات تنها می گذارند. ایمیل یکی از پر مخاطره ترین سرویس ها است زمانی که روالهای امنیتی فعال نباشد یا در سطح کمی فعال باشد.

۳- گاه در اختیار گذاشتن ایمیل به صورت غیرمجاز موجب تحقق مسئولیت می شود.

برخی شرکتها و نهادها و . . . برای مقاصد خاص ایمیل به افراد می دهند و تأکید می کنند نباید افراد این ایمیل خاص را در غیر موارد مصرحه استفاده کنند. در صورت بی مبالاتی در انجام وظیفه یا در اختیار گذاشتن عمدی ایمیل خاص، مسئولیت محقق می شود.

۴- نوع دیگر بی مبالاتی و در نتیجه تحقق ←

مسئولیت کیفری در قضیه ISP ها و . . . دیده می‌شود اینها زمانی که از محتوای غیراخلاقی یا مجرمانه ایمیل توسط یک کودک یا والدین او یا پلیس مطلع می‌شوند باید محتوای مضر را بردارند و محو کنند در غیر این صورت دارای مسئولیت کیفری خواهند بود.

۵- نوع دیگر تحقق مسئولیت در عدم واکنش به گزارش توسط مقامات مربوطه، تهیه کنندگان خدمات اینترنت و . . . است حتی در سطح جهان خطوط آتش یا هات لاین هایی بصورت یک ارگان غیر دولتی ولی دارای اختیارات قابل توجه وجود دارند و در تعامل یا مقامات مربوطه و ارگانهای فنی قرار دارند.

این خطوط آتش به هنگام مواجه به برخی جرائم سایبری، در بخشی از روند تحقیق جنایی و تعقیب و حتی پیشگیری مشارکت می کنند. عدم توجه به گزارش هات لاین ها در خصوص ایمیل های با متوای مضر موجب تحقق مسئولیت کیفری می شود.

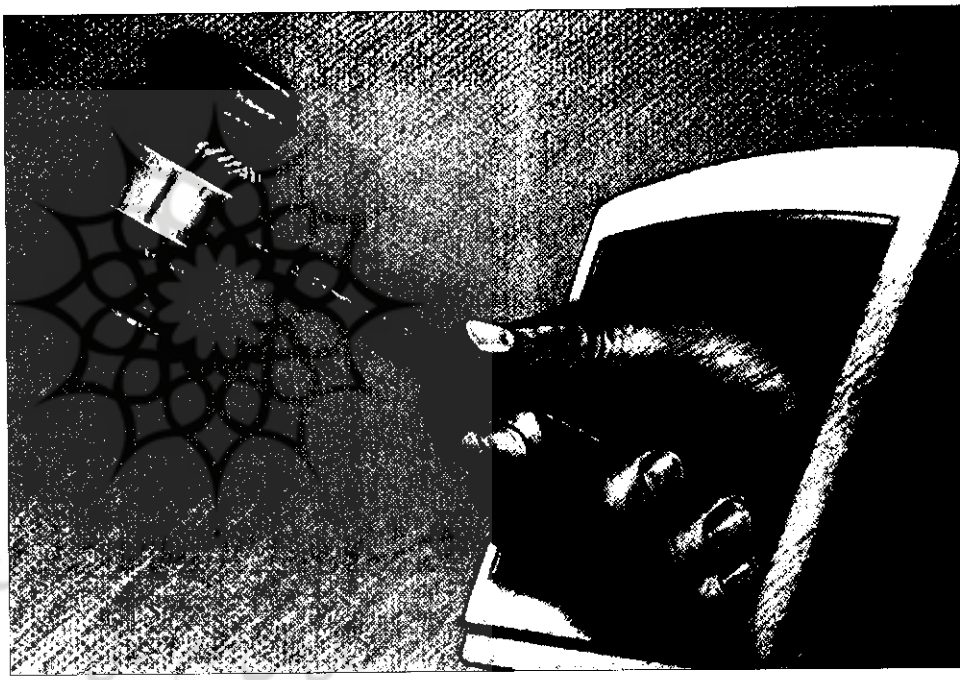
۶- درخصوص پست الکترونیک از زاویه دید و بحث عنصر مادی (جرائم مختلف) باید تصریح کرد این سرویس گاه در روش ارتکاب جرم مورد بحث قرار می گیرد. در پدیده هایی مانند کلاهبرداری از طریق فیشینگ «Phishing» از پست الکترونیک برای رسیدن به مقصود و مراد مجرمانه استفاده می شود. گاه ان سرویس وسیله ارتکاب است مثلاً در ارتکاب جرم کلاهبرداری از طریق اسکم «شیادی=scam» گاه نیز می تواند بعنوان جرم مستقل بسته به جرم ارتکابی مطرح شود مثلاً ایذاء و اذیت از طریق پست الکترونیک و . . .

ب - جزای ماهوی اختصاصی

شاید یکی از پر مطلب ترین و حجیم ترین بخشهای بحث پست الکترونیک نوع جرم ارتکابی باشد. از آنجا که این جرائم متعدد و هریک مستلزم شرح زیاد است . در این بخش فقط به فهرست این مطالب اشاره می کنیم.

۱ - در جرائم علیه تمامیت معنوی اشخاص

از ذکر استفاده از پست الکترونیک برای ارتکاب جرائم علیه تمامیت جسمانی اشخاص اجتناب می کنم. زیرا در این خصوص آنچه اهمیت دارد حصول نتیجه است بنابراین بکارگیری پست الکترونیک یا . . . اثری در جرم ندارد . اما در جرائم علیه تمامیت معنوی اشخاص به دلیل تغییر در عنصر مادی و البته الزامات کشف جرم سایبری، دادرسی کیفری سایبری و بعلت ماهیت این جرائم، می توان به جرائم خاص قایل شد خواه به عنوان جرم مستقل یا عنصر جرم دیگر. در این گروه میتوان به افترا، توهین و فحاشی، مزاحمت و ایذاء سایبری «cyber stalking» اشاره کرد.



افترا فارغ از فرم و شکل کلاسیک آن یعنی اسناد جرم به نحو ارتجالی به غیر از طریق نطق در مجامع و . . . در این حالت یعنی حالت سایبری می تواند به شکل بولتن الکترونیک، محتوای افتراآمیز، از طریق پست الکترونیک و . . . ارتکاب یابد. یعنی از پست الکترونیک برای ارسال یا در دسترس قراردادن مطالب افتراآمیز خواه در اصل فایل یا به صورت فایل همراه استفاده می شود. گاه از پست الکترونیک برای مطالبه حاوی فحاشی و توهین استفاده می شود مطلبی که می تواند تعدادی را ناراحت کند یا حتی فردی را برنجاند و به شکل پست الکترونیک ارسال می شود. حتی ارسال پیام ها یا محتواهای ناخواسته «spam» در این گروه قرار می گیرد.

لزومی ندارد محتوای پست الکترونیک منفی و مضر باشد بلکه عدم وجود رضایت دریافت کننده برای تحقق مزاحمت کفایت می کند.

۲- در جرائم علیه امنیت و آسایش عمومی

در این جرائم از پست الکترونیک برای جاسوسی، تروریسم سایبری، سابوتاژ، تشویش اذهان عمومی، دعوت به براندازی و ارتباط با بیگانه استفاده می شود. بویژه در مواردی که امنیت به حد پائین و ناکافی وجود دارد، پست الکترونیک با محتوای رمزنگاری شده و به گونه ای که از فیلترها رد شود، از بهترین و سهل الوصول ترین ابزار جاسوسی است.

با این وسیله ارسال، اطلاعات محرمانه به تنهایی یا با فایل ضمیمه شده صورت می گیرد. در قضیه فعالیت گروه القاعده حتی مشخص شده اینها به همراه فایل های حاوی پورنوگرافی (تصاویر مستهجن) و . . . ارسال اطلاعات و . . . اقدام کرده اند و . . . برای تروریسم سایبری یکی از بهترین وسایل، پست الکترونیک است و از این طریق اقدام به ایذاء، تهدید، ارسال حجم زیاد پست الکترونیک، اخبار مربوط به تهدید به بمب گذاری و حتی زمان عملی شدن آن، نشر اکاذیب و . . . می شود.

بمب پستی یعنی ارسال چند هزار پست الکترونیک به منظور از کار انداختن صندوق پستی الکترونیکی به دو قصد یا منظور صورت می گیرد: برخی برای معارضه با نظام و مقابله با یک نهاد یا سازمان دولتی یا وابسته به دولت این روش استفاده می کنند که در این صورت بمباران از طریق پست الکترونیک یا بمب پستی الکترونیکی، از مصادیق یا روش های ارتکاب سابوتاژ (خرابکاری) محسوب می شود. اگر این قصد معارضه نباشد مورد از مصادیق تخریب سایبری است.

از این ابزار و سرویس یعنی پست الکترونیک برای تشویق اذهان عمومی و حتی دعوت به براندازی نیز استفاده می شود به گونه ای که رابرت موگابه را دچار چالش سیاسی کرد. طبعا هرگونه ارتباط با بیگانه نیز از این طریق میسر است. یکی از بخشهای مهم قانون میهن پرستی «patriot» آمریکا بخش پست الکترونیک ناقض یا تهدیدکننده امنیت ملی است.

۳- ارتکاب برخی جرائم علیه اموال

دو مورد از مهم ترین استفاده ها از پست الکترونیک برای ارتکاب تخریب سایبری و کلاهبرداری سایبری است. در زمینه تخریب قبلاً به بمب پستی اشاره شد. اما در کلاهبرداری صور مورد استفاده گسترده تر است. Scam که فاعل آن را scammer می گویند و به معنای شیادی است از روش های کلاهبرداری سایبری از طریق پست، الکترونیک است.

در این روش به فرد اطلاع می دهند در قرعه کشی یا در بازی بخت آزمایی (لاتاری و . . .) برنده پول شده (مثلا ۲۵۰ هزار یورو) و باید برای انجام مراحل مالیاتی و کمرگی مبلغی (مثلا ۵۰ هزار دلار) به حساب وزارت دارایی فلان کشور به آدرس مرقوم در پست الکترونیک پول بریزد . یا با معرفی خود بعنوان مدیرعامل یا رئیس بانک، از فرد دارای حساب بانکی (ملی کارت، عابر بانک و . . .) خواسته می شود جهت اشتباه در برداشت یا واریز وجه به حساب او ، شماره کارت، گذر واژه و . . . را آن مقام چک کند یعنی برای او ایمیل کند تا آن طرف حساب را درست کند و از این راه مرتکب با دانستن شماره کارت و رمز فرد و با یک کارت جعلی می تواند اقدام به برداشت پول کند و . . . امروزه به این روش ، روش «phishing» اضافه شده و از این طریق اطلاعات مالی فرد و . . . دریافت و سوء استفاده می شود .

همچنین روش جدید شیادی ، پیام ناخواسته یا «spam - scam» برای کلاهبرداری سایبری استفاده می شود که به ویژه از طریق پست الکترونیک انجام می شود . نکته ای که مغفول ماند اینکه در سابوتاژ و نیز تخریب بسته به انگیزه و قصد مرتکب، از ایمیل برای ارسال ویروس، بمب، کرم و . . . استفاده می شود و . . .

۴- منافی عفت

یکی از موارد شایع استفاده از ایمیل برای پورنوگرافی بطور خاص و جرائم جنسی بطور عامل است . معمولا تصاویر مستهجن از این طریق ارسال می شوند خواه بین مجرمان اصلی، خواه از سوی تهیه کننده برای مشتریان این گونه عکس ها و . . . در عین حال از ایمیل برای ارسال تصویرهای پورنوگرافی جهت ایذاء و اذیت دیگران بویژه زنان و کودکان استفاده می شود، خیلی از افراد از دیدن چنین تصاویری ناراحت می شوند و البته یادمان نرود که پورنوگرافی در فضای سایبر بر عکس پورنوگرافی کلاسیک مرسوم شامل صوت، تصویر و نوشته مستهجن است .

از ایمیل برای اغوا و تحریک دیگران برای مقاصد جنسی نیز استفاده می شود . معمولا کودکان یا جوانان را تشویق به دیدن یا تهیه چنین تصاویری از خود یا دوستانشان می کنند و حتی پاداش مالی برای این کارها تعیین می کنند .

گاه از طریق ایمیل برای باندهای مجرمانه پورنوگرافی عضوگیری می کنند یا افراد را تشویق به گرفتن فیلم حاوی چنین تصاویری می کنند . نیز به خاطر داشته باشیم رفتن به سایتهای مضر، دادن ایمیل به آنها و گذرواژه یا رمز و . . . موجب لو رفتن اطلاعات شخصی و مشکلات بعدی می شود .

۵- تطهیر نامشروع (پول شویی)

از ایمیل برای پول شویی نیز استفاده می شود . مرتکب یا دارنده وجوه غیرقانونی و کثیف (عواید حاصل از جرم) بدوا ایمیل برای یک نفر در محل یا کشور دیگری می فرستد و از او می خواهد شماره حساب خود را در اختیار او بگذارد و شرط می کند که به ازاء صد هزار دلاری که ناشناس می فرستد او باید بعد از چند وقت پنج یا ده هزار دلار آن را برای خودش نگه دارد و باقی را از طریق سستم معتبر قانونی به حساب قانونی مرتکب بفرستد و با این مکانیسم پول کثیف تبدیل به پول تمیز می شود .

البته در این گونه ایمیل ها باید مواظب کلاهبرداری نیز باشیم زیرا آنها بدوا شرط می کنند که دریافت کننده باید حساب ارزی درست کند یا مبلغی به صورت ارز برای آنها حواله کند تا مطمئن شوند آدم خوبی است که البته ارسال پول همانا و از دست دادن مال نیز همان .

۶- قاچاق

از ایمیل برای تبادل اطلاعات مجرمانه، از جمله اطلاعات مالی، زمان تحویل یا ترانزیت کالای قاچاق و . . . استفاده می شود و برای ایمن کردن آن و مصون ماندن از تعقیب پلیس، از رمزنگاری یا . . . استفاده می شود . معمولا کشف این مورد سخت تر است .

از ایمیل برای تبادل اطلاعات مجرمانه نیز از جمله اطلاعات مالی، زمان تحویل یا ترانزیت کالای قاچاق و... استفاده می شود و برای ایمن کردن آن و مصون ماندن از تعقیب پلیس، از رمزنگاری یا ... استفاده می شود

۷- مواد مخدر

چند سالی است که فضای سایبر مورد استفاده مجرمان مواد مخدر بویژه قاچاقچیان قرار گرفته است . در مورد قبلی اشاره شد اما بطور تفضیلی تر می توان اشاره ای به لیست توزیع افراد، تبادل اطلاعات مشتریان، اعلام نیاز مشتری از طریق ایمیل، زمان و نحوه ترانزیت موادمخدر، نحوه انتقال وجوه مجرمانه ... کرد .

۸- در دیگر جرائم

اگر چه به ذکر اندکی از جرائم سایبری که در آنها ایمیل مورد استفاده قرار می گیرد اشاره ای داشتیم اما بدنیست بدانیم در جرائم غیر سایبری براساس اطلاعات پلیس جنایی (مثلا اف بی آی) به هنگام پی جویی باید به وجود ایمیل توجه شود و آن را در شمار دلایل در جرائم مختلف از کلاهبرداری، قتل، خودکشی گرفته تا جرائم سازمان یافته غیر سایبری در نظر گرفت .

با مختصر مطالبی که در بحث ماهوی (جزای عمومی و اختصاصی ذکر شد) باید به بحث جزای شکلی یا همان آئین دادرسی کیفری پرداخت که انشاءالله در شماره بعد پی خواهیم گرفت .