فصلنامه دیدگاههای حقوقی، دانشکده علوم قضائی و خدمات اداری
شماره بیست وسوم و بیست و چهارم، ۱۳۸۰، صص ۱۱۱-۹۹

جرایم رایانه‌ای و روش‌های مقابله و پیشگیری از آن

مهدی فهیمی*

«۱۳۸۰/۱۰/۲۴»

با گسترش فناوری‌های اطلاعاتی و ارتباطی و دسترسی عموم جامعه به شبکهٔ اینترنت، فضای جدیدی فراروی متخلفین جوامع قرارگرفته است. فضایی که در آن محدودیت هایی همچون مرزهای جغرافیایی، ملیت، بعد مسافت، زمان و... فاقد معنا و مفهوم است. در موقعیت جدید، جرایم رایانه‌ای از رشد و توسعهٔ چشمگیری برخوردار بوده است. مقاله حاضر با بهره‌گیری از سیاستهای جرایم رایانه‌ای کشورهای آمریکا، انگلستان، آلمان، فرانسه، کانادا، ژاپن، کره، سنگاپور، مالزی و هنگ کنگ و جامعه اروپا تهیه شده و به مهم‌ترین راهکارهای استفاده شده توسط این کشورها می‌پردازد. نظر به محدودیت حجم مقاله، در این نوشتار بیشتر به نقش پلیس اشاره شده و تأثیر دیگر سازمان‌ها در مقابله با جرایم رایانه‌ای فهرست و از طرح شده است.

واژه‌های کلیدی:
جرایم رایانه‌ای - پلیس - پیشگیری و مقابله - قانون گذار - سیستم قضایی - تأمین کنندگان خدمات اطلاعاتی - بخش خصوصی - امنیت اطلاعات - فناوری اطلاعات.

۱- مقدمه

در هر جامعه‌ای اشخاص متخلف، همواره در انتظار فرصت‌های مناسب و بهره برداری از موقعیت‌های فراهم شده هستند. این فرصت‌ها ممکن است بر اثر غفلت افراد یا سازمان‌ها باشد که در هر صورت برای متخلفین یک موقعیت به شمار رفته و منافعی را در بر خواهد داشت. امروزه با گسترش ارتباطات و دسترسی همگان به شاهراه‌های جهانی اطلاعات، غفلت‌های فردی یا سازمانی می‌تواند، موقعیت‌های متنوع‌تر، سهل

---

* - عضوگروه مدیریت تکنولوژی مجتمع دانشگاهی مهندسی صنایع

الوصول‌تر و پرسودتری را فراروی متخلفین قرار دهد. تا یک دههٔ قبل، نفوذ مراکز حساس دولتی مستلزم طرح ریزی گسترده و تأمین منابع مالی و انسانی قابل توجه بوده است ولی در عصر حاضر شرایط به کلی دگرگون شده است. در شرایط کنونی، یک کاربر ماهر به خوبی می‌تواند واحد کنترل ترافیک یک فرودگاه بین المللی را مختل کند، خدمات اضطراری مانند برق، آب، پزشکی و... را در یک منطقه تعطیل کند، حساب‌های بانکی شهروندان یا سازمان‌های خصوصی و دولتی را مورد دستبرد قرار دهد و حتی برخی تسلیحات دفاعی کشور را چنان چه به صورت مستقیم یا غیر مستقیم به اینترنت و یا یک خط تلفن معمولی وصل باشند، فعال نماید. جالب توجه این است که تجهیزات مورد نیاز همه این طرح‌ها عبارتند از: یک دستگاه رایانه، یک مودم و یک خط تلفن.

بررسی آمار جرایم رایانه‌ای جهان بیانگر این واقعیت است که طی سال‌های ۱۹۹۶ الی ۱۹۹۹، برخی از کشورها شاهد ۱۶۰۰٪ رشد در اینگونه جرایم بوده‌اند که شامل زمینه‌های نفوذ غیر قانونی، رمزشکنی، چاپ تصاویر یا تبلیغات مبتذل، خسارت به دیگران، تقلب در خریدهای اینترنتی، تعرض به حقوق مالکیت معنوی و دیگر موارد می‌شده است.

۲- طرح مشکل

اگر در جامعه ما یک کاربر خاطی با هر انگیزهٔ احتمالی، تصمیم به ورود به یکی از پایگاه‌های حیاتی کشور گرفته باشد و مثلاً به بخش کنترل پرواز فرودگاه،برنامه تهیه و پیش خرید بلیط مسافرین، نتایج کنکور سراسری، پرونده فردی افراد در تأمین اجتماعی، مرکز کنترل ترافیک، پایگاه ثبت احوال، بخش صدور رویداد و دیگر موارد مشابه نفوذ کند،تا چه میزان آمادگی برخورد با حوادث ایجاد شده را خواهیم داشت؟ اگر واقعاً موفق به کشف و شناسایی فرد خاطی شویم، ساز و کار مناسب به منظور اثبات جرم و تنظیم مستندات قابل ارایه در محاکم قضایی کدامند؟ سازمان رسیدگی کننده به این گونه جرایم مجازی و الکتریکی دارای چه ویژگیهایی خواهد بود؟

در یک چنین شرایطی وظیفه نهادهای مختلف کشور مانند قانون گذار، نیروی انتظامی، سیستم قضایی، شرکت مخابرات، شورای عالی انفورماتیک، سازمان‌های تأمین کننده خدمات اینترنتی،[1] بخش خصوصی و... چه خواهد بود؟

1- Informthlon service Providers (ISPs)

کدام سازمان‌ها مسئولیت مراقبت از اطلاعات حساس کشور را به عهده خواهند داشت؟ وظیفه حفظ آمادگی فنی و علمی برای مواجه شدن با تهاجمات رایانه‌ای در سطح ملی، به عهده کدام نهاد خواهد بود؟ طبعاً می‌توان سئوالات متعدد دیگری را به فهرست مشکلات فوق افزود. در این مقاله سعی خواهد شد تا با ذکر نمونه فعالیت‌های دیگر کشورها،به هر یک از موارد پیش گفته اشاره شود.

۳-گذری بر قوانین جرایم رایانه‌ای در جهان

بر اساس تقسیم بندی مؤسسه بین المللی مک کانل[1] جرایم رایانه‌ای به چهار گروه اصلی و ده نوع جرم مستقل تقسیم شده‌اند. این چهار گروه عبارتند از:

یک - جرایم مرتبط با داده‌ها: شنود الکترونیکی، تغییر داده‌ها، سرقت داده ها

دو - جرایم شبکه: اختلال در شبکه، خرابکاری در شبکه

سه - نفوذ: دسترسی غیر مجاز، انتشار ویروس

چهار - سایر موارد: همکاری در ارتکاب جرم، جعل رایانه‌ای، کلاهبرداری

مک کانل مقایسه‌ای بین وضعیت قوانین بالا در پنجاه و دو کشور جهان بعمل آورده است و مشخص شده است که:

۱- تنها کشور فیلیپین دارای قوانین جزایی لازم برای برخورد با هر ۱۰جرم است،

۲- هشت کشور بطور اساسی قوانین خود را روزآمد کرده‌اند. مانند: آمریکا،ژاپن و استرالیا،

۳- ده کشور بطور جزیی قوانین خود را روز آمد کرده‌اند مانند انگلستان، دانمارک، چین و شیلی،

۴- شانزده کشور قوانین خود را روزآمد سازی نکرده‌اند.

۵- هفده کشور فاقد قوانین مصوب برای مقابله با جرایم رایانه‌ای هستند، از جمله کشورهای کوبا و ایران.

تحلیل مؤسسه مک کانل از وضعیت قوانین جرایم رایانه‌ای بین پنجاه و دو کشور بررسی شده به شرح زیر گزارش شده است:

یک- با اتکا به قوانین قدیمی و متعارف نمی‌توان با جرایم رایانه‌ای به مقابله

1- Mc Connell International Institute

پرداخت. این مشکلی است که بسیاری از سیستم‌های قضایی با آن مواجه هستند.

دو- مقررات جزایی برای هر جرم در کشورهای مختلف، متفاوت است ولی جهت‌گیری کلی قوانین در جهت مراقبت از پایگاه‌ها و داده‌های ملی و دولتی است.

سه - مجازات‌های سبک و ناکافی موجب بی اثر شدن تلاش‌ها خواهد شد. این مشکل می‌تواند آثار منفی اجتماعی و اقتصادی گسترده‌ای به دنبال داشته باشد.

چهار- اصلی مراقبت از خود باید به جامعه آموزش داده شود. نهادهای خصوصی و دولتی باید ابتدا خودشان از اطلاعات موجود مراقبت نموده و سپس در انتظار کمک دولت باشند.

پنج- قوانین چند گانه جهانی موجب کاهش قاطعیت در برخورد با مجرم می‌گردد.

شش - نیاز مبرم به یک الگوی رفتاری واحد در سطح بین المللی وجود دارد.

۴- راهکارهای احتمالی در مقابله و پیشگیری از جرایم رایانه ای

وظیفه نظام حاکم است که با توجه به روند تحولات جهانی، ابراز قانونی و اجرایی لازم را برای مقابله و پیشگیری از جرایم مهیا نماید. تجربه کشورهایی که حداقل یک دهه از عمر قانون گذاری و نهادهای اجرایی مقابله با جرایم رایانه‌ای آنها می‌گذرد، بیانگر این مهم است که:

الف - سعی کرده‌اند تا تعادلی بین نیازهای جامعه و ضمانت اجرایی لازم برای مجریان قانون به وجود آورند.

ب - نه تنها سه نهاد اصلی یعنی قانون گذار، نظام قضایی و پلیس و هم ردیف با دو نهاد دیگر است؟ بلکه سازمان‌ها و وزارت خانه‌های متعددی دست به دست یکدیگر داده تا طرح مبارزه با جرایم را از طریق آموزش عمومی و مقابله با مجرمین، به اجرا درآورند.

۴-۱- نقش و جایگاه قانون گذار

یک متخلف رایانه‌ای معمولاً احترامی برای حقوق فردی، قوانین مرزی، مقررات ایمنی، تبعیت ملی و... قایل نخواهد بود، بنابراین قانون گذار بر خلاف پرونده‌های متعارف، با چند مشکل اساسی از جمله مجازی بودن حادثه، حضور متخلف در خارج از مرزهای کشور، هماهنگی با دیگر نظام‌های قضایی در دستگیری و مجازات مجرم و مشکلاتی از این نوع، روبرو خواهد بود. به این منظور مروری بر تعاریف و قوانین دیگر

کشورها به منظور دستیابی به بهترین مقررات وضع شده، مفید خواهد بود. نکته دیگر این است که اگر اصطلاحات و عبارات مرتبط با موضوع، که معمولاً جدید و نوظهور هستند، به وضوح تعریف نشوند، قاضی و سیستم قضایی را در بررسی یک پرونده با مشکل مواجه خواهند کرد.

برای نمونه باید در متن قانون عباراتی هم چون جرم رایانه‌ای، رایانه، رمز نگاری، مراقبت از داده‌ها، فریب دادن رایانه، مکان ارتکاب جرم، انواع جرایم احتمالی، ملیت مجرم و دیگر عبارات مشابه با دقت تعریف و ارزیابی گردند. به عنوان نمونه به برداشت هایی که می‌توان از برخی از این اصطلاحات داشت؛ اشاره می‌گردد:

یک - جرم رایانه‌ای

جرم رایانه‌ای ممکن است هر یک از موارد زیر باشد:

الف - جرایمی که مستقیماً یک دستگاه رایانه یا سیستم‌های آن را مورد هدف قرار دهد، مانند نفوذ و رمز شکنی

ب - جرایمی که در آن‌ها از رایانه به عنوان یک رسانه استفاده می‌شود. مانند قمار از طریق اینترنت

ج - جرایمی که رایانه صرفاً محل حادث شدن جرم بوده است. مانند نمایش یک آگهی غیر مجاز به منظور جذب مشتری به محل فروش.

دو- رایانه

یکی از وسیع‌ترین و متنوع‌ترین تعاریف در متن قوانین کشورها، عبارت رایانه و سیستم‌های رایانه است. باید مشخص شود که منظور از رایانه چیست؟ تعاریف موجود در برخی موارد به گونه‌ای است که قضاوت و برداشت را به عهده محکمه گذاشته است. به عنوان نمونه، مشخص نیست که منظور از رایانه دستگاه و تجهیزات سخت‌افزاری، اطلاعات و داده‌های موجود در یک رایانه، و یا نرم افزارهای پردازش، ذخیره، بازیابی و نشر اطلاعات است.

سه - رمزنگاری

روش‌های رمز نگاری در سال‌های اخیر به شدّت دستخوش دگرگونی شده است. افراد برای اطلاعات خصوصی و تجارت الکترونیکی ممکن است نیاز به استفاده از رمزنگاری داشته باشند. از طرفی متخلفین نیز برای مراقبت از اطلاعات خود از این فناوری بهره می‌گیرند. بنابراین اگر مجری قانون مجهز به تکنیک‌های رمزنگاری در

چارچوب تعیین شده نباشد، به سختی می‌توان وارد اطلاعات متخلفین شده و اسناد لازم برای محکمه را آماده کرد.

با بررسی که به عمل آمده است، معمولاً قوانین جرایم رایانه‌ای از سوی شورایی با حضور نمایندگان زیر و در مدت زمانی در حدود شش و هشت ماه تدوین شده است. هر چند که ترکیب شورا متناسب با ساختار حکومتی هر کشور اندکی متفاوت می‌باشد، ولی مهم‌ترین نمایندگان شورا عبارتند از:

۱- نماینده سازمانهای امنیتی، به عنوان رئیس شورا (۲ نفر)
۲- شورای عالی انفورماتیک (۳-۲ نفر)
۳- شرکت مخابرات (۳ نفر)
۴- وزارت کشور (۶-۴نفر)
۵- وزارت صنایع (۴-۳ نفر)
۶- دیوان عدالت اداری (۳ نفر)
۷- پلیس (۶-۴نفر)
۸- قوه قضائیه (۶-۴نفر)
۹- وزارت بازرگانی (۴-۳ نفر)
۱۰- وزارت اقتصاد و دارایی (۶-۴ نفر)
۱۱- برخی نمایندگان بخش خصوصی (ISPs)

۴-۲- نقش و جایگاه پلیس

با بررسی اجمالی واحد جرایم رایانه‌ای در ۱۰ ادارهٔ پلیس، در سطح جهان، مشاهده شد که بخش‌های اصلی تشکیل دهنده این واحدها به شرح زیر می‌باشند:

۱- دریافت شکایتهای اینترنتی
۲- مراقبت از کودکان
۳- تخلفات تجاری
۴- جاسوسی اطلاعاتی اعم از صنعتی / تجاری
۵- آگاه سازی جامعه: شامل مدارس، عموم جامعه، واحدهای تجاری و صنعتی، واحدهای حراست سازمان‌ها و...
۶- تخلفات مخابراتی
۷- سرقت سخت‌افزار و نرم افزار

۸- عملیات (مراحل کشف تا مدرک نگاری یک جرم)

فهرست جامعی از اهداف و وظایف مشخص برای هر یک از واحدهای بالا اعلام شده است. به عنوان مثال، در زمینهٔ آگاه سازی عمومی جامعه، ادارات پلیس حداقل به اقدامات زیر می‌پردازند:

۱- برگزاری سخنرانی برای دانش‌آموزان، مربیان و اولیاء

۲- چاپ و نشر مواد فرهنگی در مدارس از طریق بروشور، mouse pad، برچسب و پوستر

۳- همکاری با آموزش و پرورش در طراحی مباحث امنیتی - اخلاقی در تهیه طرح درس فناوری اطلاعات

۴- گنجاندن متن قانون در کتب درسی

۵- سخنرانی برای کارکنان و مدیران صنایع و بنگاههای تجاری

۶- همکاری با ISPs در ارسال تذکر به اعضای خاطی شبکه اینترنت

۷- حضور در همایش‌های عمومی مرتبط با امنیت اطلاعات

۸- حضور در نمایشگاه‌های رایانه‌ای با هدف آموزش و آگاه سازی

۹- ارسال تذکرات ویژه برای مشترکین با پهنای باند وسیع‌تر[1] (آنها بیشتر در معرض خطر هستند)

همچنین در زمینهٔ کشف تا اثبات و رسیدگی به یک جرم، فرآیند پیچیده‌ای توسط کارشناسان پلیس طی خواهد شد. این فرآیند با بهره‌گیری از فناوری‌های جدید و تجهیزات پیشرفته سخت‌افزاری و نرم‌افزاری، باید قابلیت پرداختن به کشف و شناسایی مجرم، شناخت روشهای استفاده شده توسط مجرمین، شناخت روش‌های پیشگیری و مقابله و روش‌های مستند سازی و اثبات جرم را داشته باشد. از طرفی باید توجه داشت که اطلاعات زمان و مکان ارتکاب جرم به راحتی قابل تغییر هستند، لذا مجریان قانون نیاز به روشها و تجهیزات بازیابی شرایط را دارند. در این رابطه یکی از روشهای معمول، «منجمد کردن اطلاعات[2]» از راه دور نام دارد که توسط ابزار خاصی توسط مجری قانون صورت می‌پذیرد.[3]

1- Wider Width of Band

2- Information Freezing

۳- اطلاعات بالا با بهره‌گیری از وظایف و ساختار اداره پلیس، ازمنابع شماره (۴، ۵، ۶، ۷، ۸، ۹) تهیه شده است.

۴-۳- نقش تأمین کنندگان خدمات اطلاعاتی (ISPs)

بسیاری از جرایم رایانه‌ای بااستفاده از تار جهان گستر (WWW) صورت می‌پذیرد، لذا تأمین کنندگان خدمات اینترنت یا (ISPs) نقش به سزایی در مقابله و پیشگیری جرایم رایانه‌ای دارند.

معمولاً در بررسی یک تخلف بوجود آمده از طریق اینترنت، دو دسته اطلاعات مورد نیاز هستند:

۱- اطلاعات مربوط به حساب مشتری و

۲- اطلاعات مربوط به هر جلسه ارتباط از طریق شبکه.

فهرست اطلاعات مرود نیاز توافق شده توسط محققین پرونده‌های جرایم رایانه‌ای، بالغ بر ۱۴ مورد برای اطلاعات در هر ارتباط و ۲۱ مورد برای حساب مشترکین می‌باشد.

۴-۴- نقش بخش خصوصی در مقابله با جرایم رایانه ای

نهادهای مجری قانون بدون مشارکت و مساعدت افراد جامعه نمی‌توانند با جرایم بطور مؤثر و بینادی مقابله نمایند. این بخش به بررسی نقش شهروندان و بخش خصوصی، در مقابله و پیشگیری از جرایم رایانه‌ای می‌پردازد. برخی از اقدامات بخش خصوصی در کشورهای مطالعه شده، عبارتند از:

۱- یک اصل مهم و زیر بنایی این است که «هر فرد یا سازمان، خود مسئول مراقبت از داده‌ها و پایگاه خویش است، قبل از اینکه دولت برای وی فکری بکند.»

۲- تقویت نرم افزارهای ضد ویروس و توزیع آن به قیمت مناسب در جامعه همچنین طراحی نرم افزارهای ضد ویروس ویژه برای امنیت اطلاعات سازمانهایی که شبکه‌های ارتباطی حساسی دارند.

۳- سازمان هایی که دست آورد محققین آنها در قالب «حقوق مالکیت معنوی» نمود دارد، باید از نرم افزارهای مراقبتی لازم بهره گرفته تا دسترنج آنها به راحتی از طریق اینترنت قابل انتقال نباشد.

۴- طراحی و توزیع فیلترهای ویژه (دایه:nanny) بطوریکه اولیاء از دسترسی کودکان و نوجوانان به پایگاههای غیر ضروری و غیر مجاز اطمینان خاطر داشته باشند.

۵- پیشگیری از تهاجمات رایانه‌ای و تحمل هزینه‌های سرسام آور، از طریق تهیهٔ نسخهٔ پشتیبانی (Backup) مستمر از داده‌ها.

۶- دسترسی‌ها: بهره‌گیری از مقررات ساده و متعارف امنیتی در دسترسی کارکنان و مشتریان به اطلاعات، مانند:

- تغییر مستمر رمز عبور افراد
- ممنوعیت استفاده از رمز عبور دیگران
- قطع ارتباط در محیط اینترنت، قبل از اتصال به شبکه اینترنت.

۷- بهره‌گیری از نسخه اصلی نرم افزارها در عوض کپی‌های ارزان قیمت موجود در بازار.

۴-۵- نقش دولت در مقابله و پیشگیری از اشاعه جرایم رایانه ای

متقابلاً دولت باید فرهنگ امنیت اطلاعاتی و همکاری متقابل را در بین افراد و نهادهای بخش خصوصی اشاعه دهد. این مهم می‌تواند با فعالیتهای زیر انجام پذیرد:

۱- تبیین جایگاه امنیت اطلاعات در استراتژی همکاری بین دولت و بخش خصوصی

۲- در تدوین قانون و تهیهٔ لوایح، باید از مشارکت و معاونت بخش خصوصی بهره گرفته شده تا قوانین واقع بینانه‌تر تهیه شده و از ضمانت اجرایی بیشتری برخوردار باشد.

۳- نهادهای مجری قانون معمولاً در جریان چگونگی شکل گرفتن یک جرم و راههای نفوذ متخلفین قرار می‌گیرند. لازم است تا این اطلاعات دسته بندی شده و بطور مستمر به آگاهی تهیه کنندگان نرم‌افزار، سخت‌افزار و صنایع تولید کنندهٔ ادوات مخابراتی و ارتباطی برسد. بدیهی است که این اطلاعات تدابیر جدیدی را در طراحی و تولید فراهم خواهد نمود. متقابلاً صنایع IT کشور نیز باید دستگاه‌های مجری قانون را در جریان روند رو به رشد و پدیده‌های نو ظهور قرار دهند.

۴- دولت باید بطور مستمر آمادگی مقابله با تهاجمات رایانه‌ای در بخش خصوصی را ارزیابی و تحلیل نماید. لذا نیاز به استانداردهای پذیرفته شدهٔ ملی وجود دارد.

۵- ترویج فرهنگ اخلاق کار در فضای اطلاعاتی
(Information ethics / cyberethics)

۶- بهره‌گیری از تدابیر امنیتی پیشگیرانه به منظور به حداقل رساندن خسارات ناشی از تهاجمات رایانه‌ای.

اشاعه اخبار و فرهنگ «بهترین روشهای مدیریتی» بین سازمان‌ها، به ویژه آنهایی که بیشترین تماس را با مشتری دارند. مانند بانکداری الکترونیکی، فروشگاههای اینترنتی، صنعت بیمه و...

۴-۶- مراقبت از سامانه‌های اطلاعاتی حساس کشور

در هر جامعه‌ای خدماتی وجود دارند که در حفظ امنیت و آرامش آن جامعه نقش مؤثری دارند. چنانچه اطلاعات این بخش‌های خدماتی دچار خدشه شود. آرامش جامعه با مشکل جدی مواجه خواهد شد. از جمله این اطلاعات عبارتند از: پایگاه مرکز کنترل راههای کشور (اعم از شهری یا بین شهری)،مرکز کنترل نیرو، شبکه ملی مخابرات، نظام بهداشت و درمان و اورژانس‌ها، سیستم‌های دفاعی، سیستم‌های بانکی و تجاری و... در کشورهای پیشرو مرکزی تحت عنوان مراقبت از سامان‌های اطلاعاتی حساس مسئولیت شناسایی پایگاههای کلیدی کشور و ایجاد بسترهای امنیتی مناسب برای آنها را به عهده دارد.

۴-۷- نیروهای واکنش سریع رایانه ای

امروزه تهاجمات رایانه‌ای خود جلوه دیگری از جنگ سرد یا به عبارتی عرصه پنجم جنگ‌ها را پس از زمین، هوا، دریا و فضا، تشکیل می‌دهد.

در برخی از کشورهای جهان مرکزی تحت عنوان مرکز واکنش سریع رایانه‌ای عهده دار«حفظ برتری کشور در شناسایی و ابداع آخرین روش‌های تهاجمات رایانه‌ای و هشدار به سازمان‌های دولتی و ملی» می‌باشد. معمولاً اعتبارات تحقیقاتی این مراکز توسط وزارت دفاع و نیروهای پلیس هر کشور تأمین می‌گردد.

۴-۸- تدوین اجرای طرح ملی آموزش عمومی جامعه

در آموزش‌های عمومی تأکید بر رعایت اخلاق بسیار مهم و تعیین کننده است. چرا که با ظهور پدیدهٔ تار جهان گستر (www) کوچکترین مزاحمت و تهاجم فردی می‌تواند در تمام دنیا منتشر شود. برای نمونه، ویروس منتشر شده از کشور فیلیپین، موسوم به ویروس عشق، در سال ۲۰۰۰،بالغ بر ۱۰ میلیارد دلار خسارت به بار آورد! در این حادثه، اطلاعات پایگاه بسیاری از سازمان‌ها محو شد.

بررسی سیاست‌های اعمال شده از جانب کشورهای پیشرو، بیانگر این مهم است که در این کشورها، آگاه سازی عموم نسبت به امنیت و اخلاق در فضای رایانه‌ای، طی یک برنامهٔ ملی و یکپارچه، و با مشارکت نهادهای سیاست گذار، اجرایی، قضایی،

بنگاه‌های تجاری و رسانه‌های عمومی صورت می‌پذیرد.

باید توجه داشت که اجرای طرح ملی فناوری اطلاعات و نیز طرح مقابله و پیشگیری از جرایم رایانه‌ای، بدون حضور بخش خصوصی غیر ممکن خواهد بود. این مهم تأکید تمامی کشورهایی است که در این بررسی مورد مطالعه قرار گرفته‌اند. طرح ملی آموزش عمومی معمولاً با مشارکت سازمان‌های زیر طراحی و اجرا شده و عملکرد همهٔ اعضاء در قبال اعتبارات دریافتی بطور مستمر ارزیابی شده و باید به مجری طرح پاسخگو باشند.

این سازمان‌ها عبارتند از:

- ادارهٔ پلیس
- سازمان‌های امنیتی دفاعی
- وزارت پست و تلگراف
- شرکت مخابرات
- شورای انفورماتیک کشور
- وزارت بازرگانی
- وزارت صنایع
- وزارت آموزش و پرورش
- وزارت آموزش عالی
- دفتر حمایت از حقوق و اطلاعات شهروندان
- سازمان ملی بهره وری
- سازمان حمایت از مصرف کنندگان
- انجمن‌های ملی مخابرات، رایانه، حقوق
- دانشکده‌های برق - رایانه و حقوق

نتیجه‌گیری

۱- فناوری‌های اطلاعاتی و ارتباطی فضای جدیدی را برای متخلفین جامعه فراهم کرده‌اند. لذا بر سیاست گذاران و مدیران جوامع است که برای این مشکل جدید راهکارهای قانونی و اجرایی تدارک ببینند.

۲- به منظور مهار کردن جرایم رایانه‌ای در سطح جهانی، لازم است تا کلیه کشورها: دارای قوانین مصوب بوده و سعی شود قوانین حتی المقدور همگرایی داشته باشند. در این رابطه اقدام به ایجاد یک الگوی جهانی ضروری به نظر می‌رسد.

۳- قوانین جرایم رایانه‌ای و نیز طرح ملی آموزش عمومی در کشورهای بررسی شده، توسط شورایی متشکل از سازمان‌های علمی، صنعتی، تجاری، امنیتی و خدماتی تدوین می‌گردد.

۴- مشارکت عموم جامعه، بویژه بخش خصوصی، ضمانت اجرایی قوانین و طرح آموزش ملی را قویاً تقویت می‌نماید.

۵- در بسیاری از کشورها مراکزی تحت عنوان «مرکز مراقبت از سامانه‌های

حساس اطلاعاتی» و مراکز واکنش سریع رایانه‌ای فعالیت می‌کنند. این مراکز از جانب دانشکده‌های برق، رایانه و حقوق حمایت علمی و از جانب سازمان‌های دفاعی و امنیتی، حمایت‌های مالی و سیاسی دریافت می‌کنند.

۶- دولت‌ها ضمن ایجاد بستر قانونی، اجرایی و قضایی برای رسیدگی به امر جرایم رایانه‌ای، موظف به ایجاد اطمینان از گردش اطلاعات مناسب بین سازمان‌های دولتی سیاستگذار، مجریان قانون و بخش خصوصی هستند. از جمله وظایف خطیر دولت‌ها، ترویج فرهنگ «رعایت اخلاق در محیط زندگی و کار، در فضای اطلاعاتی جدید» است.

۷- با روند فزآینده ظهور، گسترش و دسترسی ارزان قیمت شهروندان به فناوری‌های اطلاعاتی، همچنان شاهد رشد آمار جرایم رایانه‌ای و پیچیده‌تر شدن روشهای ارتکاب جرم خواهیم بود. بی توجهی به این مهم در آینده‌ای نزدیک،فعالیت‌های علمی، صنعتی و اقتصادی جامعه را دچار صدمات جبران‌ناپذیر نموده و امنیت اجتماعی کشور را دستخوش تهدید جدی خواهد کرد.

علاج حادثه پیش از وقوع باید کرد
دریغ سود ندارد چو رفت کار از دست
به روزگار سلامت سلاح جنگ بساز
وگرنه سیل چو بگرفت،سد نشاید بست

منابع

1- www. gcsb.gov.n2/infos/infos.O2htm

۲- خبرنامه انفورماتیک، شورای عالی انفورماتیک کشور، سال شانزدهم، فروردین ماه ۱۳۸۰، شماره ۷۷.

3- www. making - a - difference.org

4- http://www.Co.mo.md. us/services/ police

5- http://www.facci.org

6- http://www.rcflwny.org/intro.htm

7- http://www.mcctf.org

8- http://www.troopers. state.ny.us/crim Inv/comuter crime.html

9- http://www.ifccfvi.gov/strategy/fraudtips.asp

10- www.Info.gov.hk/gia/general

11- http://europaoeuoint/ISPO/internet polices site/crime

12- www.mossbyrett.of.no/index.html

13- www.crime.research.org

14- www.aic.gov.au/con ferences/other/cybercrimes

15- http://cyhercrimes.net/shelldraft

۱۶- سعدی، مصلح الدین، کلیات سعدی، انتشارات فروغی، چاپ چهارم، ۱۳۷۱.