چالش‌های گروه‌های آپا در ارائه خدمات با تمرکز بر فورنسیک دیجیتال

طلا تفضلی

عضو هیئت علمی موسسه تحقیقات ارتباطات و فناوری اطلاعات

و عضو مرکز هماهنگی آپا

tafazoli@itrc.ac.ir

چکیده

با توسعه فناوری اطلاعات و ارتباطات فرصتهای زیادی برای مهاجمان و مجرمین بر روی اینترنت فراهم شده است. نفوذ، دزدی، کلاهبرداری و جرائم سازمان‌یافته نمونه‌هایی از حوادث در فضای سایبر هستند. به منظور مدیریت حوادث و کاهش آنها، اقدامات پیشگیرانه و واکنشی به طور همزمان باید صورت گیرند. این دو دسته خدمات، از مهمترین ماموریت های مدیریت پاسخ به حوادث هستند که توسط گروه های موسوم به CERT انجام می گیرند. آپا نامی بومی برای این گروه ها است که به منظور انجام اقدامات واکنشی و پیش گیرانه در کشور شکل گرفته‌اند. این مراکز با چالشها و مشکلات متعددی روبرو می‌باشند. بازسازی آسیب‌پذیری های محصولات مختلف خارجی و همچنین فقدان برنامه‌نویسی امن و تولید محصولات داخلی امن و مشکلات مرتبط با رفع آسیب‌پذیری های آنها از جمله چالشهای مطرح برای این مراکز می‌باشد. یکی از مسائل بسیار مهم در پاسخگویی به حادثه بحث فورنسیک دیجیتال و پی‌جویی حادثه است. اولین پاسخگویان امنیتی باید در فرایند پاسخگویی، مسائل و چالشهای مطرح در زمینه فورنسیک دیجیتال را در نظر بگیرند.

کلمات کلیدی:

گروه‌های آپا، فورنسیک دیجیتال، فضای سایبر، معیارهای امنیتی

۱- مقدمه

افزایش روزافزون استفاده از فناوری اطلاعات و ارتباطات بر همه جنبه‌های زندگی اثر گذاشته و همانگونه که وسایل آسایش و راحتی را برای عموم فراهم کرده، به طور همزمان فرصتهای زیادی را برای مهاجمان فراهم نموده است. مهاجمان می‌توانند از هرگوشه‌ای از دنیا حمله نمایند و اغلب از میزبانهای بی‌گناه برای حمله استفاده می‌کنند. حملات و جرائم سازمان‌یافته در اینترنت به سادگی انجام می‌گیرند و مهاجمان می‌توانند در مدت زمان کوتاهی در شبکه‌ها نفوذ کرده و سرویس ها را از کار بیندازند.

اینترنت تبدیل به یک زیرساخت حیاتی مهم شده است، اما اینترنت فقط یک ابزار نمی‌باشد. سرویسهای ارتباطی بسیاری بر روی اینترنت ارائه می‌گردند و کاربردهای مختلفی در اینترنت توسط کاربران گوناگون استفاده می‌شوند، مانند بانکداری الکترونیکی، تجارت الکترونیکی، دولت الکترونیکی. حوادث امنیتی در این فضای جدید خسارت زیادی را به بار می‌آورند. به دلیل حوادث امنیتی، سیستم های برخط نمی‌توانند به خوبی کار کنند، ضررهای بزرگ مالی بوجود می‌آید، پرواز مسافران در فرودگاه به دلیل ویروس دچار مشکل می‌گردد و هر روزه خسارات بسیاری به دلیل این حوادث بوجود می‌آید. شبکه‌های نا امن به اعتماد کاربران آسیب می‌زنند و این بزرگترین خسارت به جامعه اطلاعاتی می‌باشد.

زیرساختهای سایبر به دلیل استفاده روزافزون از فناوری اطلاعات، نقش حیاتی پیدا کرده‌اند. با توسعه فناوری ها، آسیب‌پذیری های زیادی در تجهیزات و نرم‌افزارها بوجود آمده است. از آنجا که تهدیدات علیه زیرساخت حیاتی ملی فاوا-پایه از طریق این آسیب‌پذیری ها تاثیر زیادی را بر اقتصاد و امنیت جامعه می‌گذارد، به منظور حل آن نیاز به انجام اقدامات هماهنگی بین دولت و بخش خصوصی در داخل کشور و در میان سایر کشورها می‌باشد. تامین امنیت دارایی های اطلاعاتی در محیط به هم‌پیوسته کنونی چالش بزرگی است و با وجود سرویس های الکترونیکی مختلف و ابزارهای نفوذ متنوع، بسیار دشوارو پیچیده می‌باشد. یک راه‌حل کلی برای تامین امنیت سیستم ها، داده‌ها و شبکه‌ها وجود ندارد، بلکه برای نیل به این هدف استراتژی امنیتی چندلایه‌ای مورد نیاز می‌باشد. مطابق با استانداردهای مدیریت امنیت اطلاعات اقدامات پیشگیرانه و واکنشی به طور همزمان برای تداوم کسب و کار، حداقل نمودن ریسک ها و ماکزیمم نمودن سود بکار می‌روند. به همین منظور علاوه بر امن‌سازی سیستم ها، مدیریت ریسک و نصب کنترل های امنیتی، نیاز به مدیریت حوادث در فضای سایبر احساس می‌گردد. و گروههای آپا و واکنش فوری برای اطمینان از امنیت فضای سایبر ملی و پاسخگویی به حوادث در کشور مورد نیاز می‌باشند.

با تشکیل این گروهها و انجام اقدامات واکنشی، فرصتهای موجود برای انجام حملات سایبری کاهش می‌یابد. هم‌اکنون تلاشهای زیادی برای ایجاد سیستمهای امن و قابل اعتماد انجام گرفته است. اما زیرساخت های حیاتی بسیار پیچیده هستند و اقدامات پیشگیرانه کافی نمی‌باشند. بنابراین با ارائه سرویسهای واکنشی امکان کشف و پاسخگویی به حملات سایبری فراهم می‌گردد و اپراتورهای مختلف می‌توانند سریعا پس از حملات سایبری سرویسهای خود را بازیابی نمایند.

گروههای آپا و واکنش فوری امکان هماهنگی بین بخشهای مختلف جامعه برای کشف، پاسخگویی و بازیابی از حادثه را فراهم می‌کنند. دولت، ارائه دهندگان خدمات اینترنتی، آزمایشگاه ها، سازمانها و صنعت، فقط در صورت همکاری بین خود، می‌توانند بر مشکلات ناشی از حوادث امنیتی در مدت زمان مناسب و با سرعت قابل قبول فائق آیند. گروههای آپا و واکنش فوری امکان جمع‌آوری و تحلیل داده، ارائه اطلاعات فنی و پشتیبان برای آسیب‌پذیری ها، انجام تحقیقات مرتبط و هماهنگی برای پاسخگویی به حادثه را فراهم می‌نمایند.

۲- تاریخچه و تبیین وضع موجود گروههای آپا و واکنش فوری

آپا نام بومی CERT است که شامل همه گروههای واکنش فوری، تحلیل آسیب‌پذیری و هشدار می‌باشد. گروههای آپا از سال ۱۳۸۳ در مرکز تحقیقات مخابرات ایران شروع به فعالیت نمودند. ۸ مرکز تخصصی برای تحلیل آسیب‌پذیری های حوزه‌های سیستم‌عامل، پایگاه داده، نرم‌افزارهای کاربردی، سیستمهای رمزنگاری، شبکه، سرویسهای شبکه و تجهیزات بی‌سیم، هرزنامه و بدافزار تشکیل

گردیدند. در سطح دولت نیز مرکز ماهر بوجود آمد که cert دولتی است و هم اکنون در حال توسعه و ایجاد شعوب سازمانی خود بنام گروه‌های گوهر می‌باشد.

۳- مهمترین خدمات گروههای آپا و واکنش فوری

مهم‌ترین خدماتی که توسط گروه های آپا ارائه می شوند عموما در سه دسته واکنشی[1]، پیش گیرانه[2] و مدیریت کیفیت امنیت است که در مجموعه این خدمات، پاره ای موارد هستند که اهمیت بیشتری داشته و باید مورد اهتمام قرار گیرند. در زیر به بعضی از آنها به اجمال اشاره می‌شود:[۱]

الف- فعالیتهای رسیدگی به حادثه : در این نوع فعالیت ها که عمدتا مبتنی بر روش PDCERT صورت می گیرند مراحل آمادگی ، شناسایی ، نگهداشت، ریشه کنی، بازیابی و پی جویی همراه با فناوری ها، رویه ها و سیاست های مربوطه صورت می‌گیرند.

ب- رصد تهدیدات ،تحلیل، هشداردهی و اعلان خطر

ج- مدیریت آسیب‌پذیری: دو دسته اصلی فعالیت‌های این بخش شامل :

- کشف آسیب‌پذیری ها: در این فعالیت به مهندسین کمک می‌شود که درک بهتری از آسیب‌پذیری ها و نحوه کشف آنها داشته باشند. هدف از این فاز آموزش مهندسین برای کشف و حذف آسیب‌پذیری های محصولات نرم‌افزاری قبل و هنگام تولید و انتشار آن می‌باشد.
- توسعه تکنیکهای برنامه‌نویسی امن به منظور کاهش آسیب‌پذیری نرم افزارها نیز در این حوزه مطرح می‌گردد.
- بازسازی[3] آسیب‌پذیری: patch کردن و بروزرسانی نرم-افزار یکی از راههای موثر برای اجتناب از آسیب‌پذیری ها می‌باشد. فرایند بازسازی آسیب‌پذیری شامل چهار مرحله جمع‌آوری اطلاعات درباره آسیب‌پذیری، تحلیل نرم‌افزار و استخراج آسیب‌پذیری و patch مربوطه، هماهنگی و افشاء و آشکارسازی آسیب‌پذیری می‌باشد.

د- تحلیل بد افزارها[4]: تحلیل بدافزارها شامل مراحل ذیر می‌باشند:

- دریافت اطلاعات و کپی‌های بدافزارها که در حملات سایبری و فعالیتهای غیرمجاز و مخرب استفاده شده‌اند.
- جمع‌آوری و ارزیابی اطلاعات از vendorهای ضد بدافزار (ارزیابی آنکه آیا انواع بدافزارها کشف و تحلیل شده‌اند)
- بررسی بدافزارها در محیط sandbox :
  - تحلیل طبیعت، مکانیزم، نسخه و استفاده از بدافزار(مانند پروفایلینگ شبکه، پروفایلینگ سیستم، مهندسی معکوس تحلیل در محیط هانی‌پات)
  - توسعه استراتژیهای پاسخگویی برای کشف، حذف و دفاع در برابر بدافزار
- همکاری با سایر افراد و سازمانها

۳-۱- مهمترین چالشها و مشکلات مرتبط با فعالیت‌های گروههای آپا و واکنش فوری

برخی از مهمترین چالشهای مطرح در ارائه خدمات گروههای آپا و واکنش فوری در ادامه شرح داده شده‌اند.

الف- چالشهای مطرح در زمینه پاسخگویی به حادثه:

- فرایند پاسخگویی به حادثه و فورنسیک دیجیتال باید با یکدیگر ترکیب گردند تا ادله دستخوش تغییر نشوند و استنادپذیری آنها از بین نرود. بنابراین پاسخگویان امنیتی باید با قواعد و قوانین فورنسیک دیجیتال و جمع‌آوری ادله استنادپذیر آشنا باشند. توضیح بیشتر در این‌باره در بخش‌های بعدی آمده است.
- فعالیتهای پاسخگویی به حادثه باید در کل سازمان به صورت هماهنگ انجام گیرد تا اطمینان حاصل شود که قابلیتهای سازگار و مناسب در زمان نیاز وجود دارند. همچنین داده‌های نفوذ باید در کل سازمان یکپارچه گردند و پیگیری آنها به صورت یکپارچه انجام گیرد.

[1] Reactive
[2] Proactive
[3] remediation
[4] Artifact handling

- یکی از مهمترین مسائل و چالشها برای مراکز آپا تولید و تست ابزارهای مناسب برای پی‌جویی و پاسخگویی به حادثه می‌باشد. این ابزارها شامل ابزارهای جمع‌آوری، تحلیل و پاسخگویی و همچنین جعبه ابزار پاسخگویان به حوادث می‌باشند.

ب- چالشهای مطرح در زمینه تحلیل، هشداردهی و اعلان خطر:

- ایجاد امکان تحلیل سایبری پیشگویانه: در سازمانها و ارگانهای مختلف و همچنین در سطح ملی باید امکان تحلیل سایبری پیشگویانه فراهم شود تا اثرات فعالیتهای شبکه معین شود، تهدیدات آینده پیشگویی گردند و حملات در جریان کشف شوند.
- ارتباطات قابل اعتماد به منظور به اشتراک‌گذاری اطلاعات در میان سازمانها و ارگانهای مختلف باید توسعه یابند.
- قابلیتهای تحلیلی و تکنیکی در سطح سازمانها و ارگانها باید ایجاد گردند و همه این فعالیتها باید در گروههای آپا و واکنش فوری مدیریت شوند.

ج- چالشهای مطرح در زمینه مدیریت آسیب‌پذیری

- یکی از اصول مهم برای مدیریت آسیب‌پذیری برنامه نویسی امن می‌باشد. متاسفانه هم‌اکنون سامانه‌های مختلفی در کشور تولید و عملیاتی شده‌اند بدون آنکه تکنیکهای تولید امن برنامه در آن رعایت گردیده باشد. این برنامه‌ها آسیب‌پذیریهای زیادی دارند و هم‌اکنون کارهای مهمی در کشور توسط این برنامه‌ها انجام می‌گیرد و این برنامه‌ها در معرض حملات سایبری می‌باشند.
- برای شرکتها و موسساتی که این نرم‌افزارها را تولید می‌نمایند و همچنین در ارگانهای تحویل‌گیرنده این محصولات باید فرهنگ‌سازی لازم انجام گیرد تا پس از تولید محصولات، شرکتها برای رفع آسیب‌پذیری‌های موجود در محصولاتشان همکاریهای لازم را بعمل آورده و خدمات کافی ارائه نمایند.
- مراکز cert دنیا، به منظور بازسازی آسیب‌پذیری‌ها با تولیدکنندگان نرم‌افزارها و تجهیزات مختلف مانند سیستمهای عامل، سیستمهای تشخیص نفوذ، دیوارهای آتش و ... در ارتباط می‌باشند و با همکاری با این مجموعه‌ها آسیب‌پذیریها را تحلیل و patchها را تولید می‌نمایند. گروههای آپا باید توانایی تحلیل آسیب‌پذیریها و patchهای تولید شده توسط این تولیدکنندگان و مراکز cert بین‌المللی را داشته باشند. به دلیل اینکه آسیب-پذیریها بسیار متنوع می‌باشند ایجاد چنین قابلیتی بسیار دشوار و هزینه‌بر می‌باشد.
- مدیریت patch در سازمانها به دلیل بزرگی شبکه و تنوع سخت‌افزارها و نرم‌افزارهای موجود در شبکه بسیار دشوار می‌باشد.

د- چالش‌های مطرح در زمینه تحلیل بدافزار

- تحلیل بدافزار از نظر زمانی بسیار حساس می‌باشد. در زمان انتشار بدافزار، این قطعات کد باید به سرعت تحلیل گردند و امضاهای سیستم‌های تشخیص نفوذ و ضد بدافزار برای آنها باید تولید شوند. همچنین راه‌حلهای محدودسازی و ریشه‌کنی آنها نیز باید به سرعت ایجاد می‌گردند.
- وجود پایگاههای داده‌ای از بدافزارها در مرکز آپای ملی به همراه سایر اطلاعات تکمیلی از قبیل زمان شناسایی آنها، فرد مسئول شناسایی و اعمال مرتبطی که برای آن قطعه بدافزار انجام گرفته لازم و ضروری است.
- ایجاد محیط sandbox و تهیه ابزارهای مناسب برای تحلیل بدافزار در مرکز آپا از مسائل مهم می‌باشد.

۴- ضرورت انجام فعالیت‌های فورنسیک دیجیتال در گروههای آپا و واکنش فوری

توسعه اینترنت و فناوری اطلاعات فرصتهای زیادی را برای مجرمین برای ارتکاب جرائم سایبر فراهم نموده است. در نتیجه حوادثی چون نقض سیاست امنیتی، جرائم سایبر، کلاهبرداری، جرائم مالی، پولشویی و ... به وقوع می‌پیوندند. نیاز به رویکردهای مناسبی برای مهار این حوادث به منظور ایجاد ادله دیجیتال استنادپذیر احساس می‌گردد. از آنجا که ادله دیجیتال شکستنی می‌باشند و به سادگی

تغییر می‌یابند، پیدا کردن این داده‌ها، جمع‌آوری، حفظ و ارائه آن در دادگاه چالش‌برانگیز می‌باشد. اولین پاسخگویان بـه حـوادث امنیتـی سایبری اغلب و همیشه پرسنل ICT می‌باشند که مهـارت کمـی در پی‌جویی سایبری دارند.

به فرایند جمع‌آوری، حفظ، تحلیل داده‌ها از کامپیوترها، شبکه‌ها و رسانه‌هـای ذخیـره‌سـازی و ارائـه ادلـه بـه دادگـاه بـا تضـمین استنادپذیری آن فورنسیک دیجیتال می‌گویند. مـدیریت حـوادث به همراه فورنسیک دیجیتال، فرایند پی‌جویی اتفاقـات بـه وقـوع پیوسته بر روی سیستمهای کـامپیوتری، شـبکه‌هـا و ...، تعیـین دامنه خسارت و اجتناب از وقوع مجدد آن حـوادث مـی‌باشـد. بـا توسعه‌ی روزافزون تجارت الکترونیکی و فناوری اطلاعات، جـرائم سایبر معمول و پیچیده گردیده‌اند. پاسخگویی به حادثـه رویکـرد سازمان‌یافته‌ای بـرای پـرداختن و مـدیریت پـس از وقـوع رخنـه امنیتی و حمله است. هدف، محدودسازی خسارت و کاهش زمان و هزینه‌های بازیابی از حادثه است.

۴-۱- کاربردهای فورنسیک دیجیتال

فناوری به مثابه شمشیر دولبه‌ای است، همانگونه که برای مقاصد تجاری و اقتصادی استفاده مـی‌شـود، و بـه دسـتگیری مجـرمین سایبر کمک می‌نماید، ابزارهای مختلفی که بـه ضـابطین قضـایی برای پی‌جویی پرونده‌های جرائم سـایبر و جمـع‌آوری ادلـه جـرم کمک می‌کند، مجرمین نیز از فناوری برای پنهان کـردن ردپـای خود استفاده می‌نمایند، مثلا دیسکها را پاکسازی کرده تا امکـان بازیابی داده‌ها را از بین ببرند.

روشها و ابزارهای فورنسیک در موارد ذیل بکار می‌روند:

- ضابطان قضایی: روشها و ابزارهای فورنسیک بر جمع‌آوری و تحلیل ادله و پیگرد مجرمین تمرکز دارند.
- سازمانها، کسب‌وکارها و بانکها: ایـن ارگانهـا بـرای تعیـین منشاء حادثه، علت، زمان وقـوع، نحـوه و چگـونگی وقـوع حادثه از شیوه‌های فورنسیک استفاده می‌نمایند.
- دانشگاهها: دانشگاهها با انجام تحقیقات دقت نتایج، روشها و ابزارهای فورنسیک را با روشـهای قابـل تکـرار و دقیـق اثبات می‌نمایند.
- دادگاهها: دادگاهها ادله و پرونده‌ها را به دقت با توجـه بـه قوانین موشکافی می‌نمایند.

زمانیکه سیستمها و دارایی‌های مهـم مـورد حملـه قـرار مـی‌گیرنـد، متخصصـین امنیتـی و پاسـخگویان بـه حادثـه بایـد بتواننـد ادلـه الکترونیکی را به صـورت اسـتنادپذیر جمـع‌آوری نماینـد. مجـرمین سایبری و کارمندان امین و متقلب ادله را در رسانه‌های ذخیره‌سازی مخفی، پنهان یا رمزنگاری می‌نمایند و اینکار را با برنامه‌هایی کـه بـه صورت رایگان و یا تجاری در دسترس می‌باشند انجام می‌دهند. ایـن حملات ممکن است نشانگر واقعه‌ای بزرگتر باشند. حسـابهای بـانکی ممکن است هک شوند و یا اطلاعات کارتهای اعتباری دزدیده شوند. زمانیکه چنین جرائمی به وقوع می‌پیوندند، ماموران پـی‌جـویی بایـد مجرمین را بیابند. متخصصین کامپیوتری از روشهای مختلفـی بـرای کشف داده‌هایی که در کامپیوترها، PDAها، کارتهای SIM، اعتباری و ... وجود دارد یا برای بازیابی داده‌های حذف شده و رمزنگاری شده و یا اطلاعات فایلهای خسارت دیده استفاده مـی‌نماینـد. گـم‌نـامی و شبه‌نامی در فضای سایبر ردیابی اشخاص را دشوار نموده است.

۴-۲- چالشهای فورنسیک دیجیتال

به طور سنتی، به نقض عمدی قوانین حقوقی که توسط قـانون قابـل تنبیه است، جرم می‌گویند. جرم در مرزهای یک بخش، ایالت، کشور که قلمرویی را تشکیل می‌دهنـد بـه وقـوع مـی‌پیونـدد. مـثلا وقتـی کلاهبرداری به وقوع می‌پیوندد، یکی از مسائل مهم آنست کـه جـرم در کجا به وقوع پیوسته بنابراین پی‌جـویی و پیگـرد در قلمـرو مـورد نظر انجام می‌گیرد. ضابطان قضایی باید بدانند که مجرم و قربـانی در زمان وقوع جرم در کجا با یکـدیگر تمـاس داشـته‌انـد تـا اختیـارات پی‌جویی و پیگرد مشخص شوند.

یکی از وجوه تمایز مهم بین جرائم سایبری و سـنتی در بـدون مـرز بودن و گم‌نامی این جرائم است. به دلیل وجود شبکه‌ها، جرائم سایبر ممکن است در نواحی، مناطق یا کشورهای مختلف به وقوع بپیوندند. ترسیم تصویر واقعی جرم برای ماموران پـی‌جـویی دشـوار مـی‌باشـد زیراکه المانهای مختلف در مکانهای مختلفی قرار دارند.

مجرمین می‌دانند که چگونه جرائم سـایبر را مرتکـب شـوند کـه ردپایی از خود به جای نگذارند و بنابراین متخصصـین فورنسـیک

کامپیوتری باید دانش سطح بالاتری از سخت‌افزار و نرم‌افزار کامپیوتری داشته باشند.

دنیای درحال تغییر فناوری، چالش دیگری برای فورنسیک دیجیتال می‌باشد. از یک طرف ابزارهای مختلف فورنسیک باید مرتبا توسعه یابند و ارزیابی شوند تا با فناوری‌های جدید سازگار باشند و از طرف دیگر دادگاهها باید قوانین و آیین‌نامه‌های جدیدی را تدوین نمایند تا ادله دیجیتال و سایر موارد مربوط به فناوریهای جدید را پوشش دهند. این ابزارها باید به دقت تست گردند تا ادله تولید شده توسط ابزارها استنادپذیر باشند و در دادگاهها برای اثبات دعوی بکار روند. برای تست ابزارها و روشهای فورنسیک دیجیتال سه رویکرد مختلف وجود دارد: کد برنامه آزمایش گردد، از ابزار دیگری برای فورنسیک دیجیتال استفاده شود تا اطمینان حاصل شود که نتایج بدست آمده مشابه می‌باشند و از تستهای فورمال برای تست ابزارها استفاده شود. بهترین و موثرترین روش برای ارزیابی ابزارها استفاده از مرور peer می‌باشد یعنی از ابزار دیگری برای تست استفاده شود و نتایج با یکدیگر مقایسه گردند.

متخصصین فورنسیک دیجیتال نه تنها باید ادله دیجیتال را پی‌جویی و جمع‌آوری نمایند، بلکه باید نتایج را به یکدیگر مرتبط نموده و به صورت واضحی در دادگاهها ارائه دهند. مامور پیگرد و قاضی ممکن است درک مناسبی از محاسبات نداشته باشند. بنابراین نتایج و پرونده باید به نحوی در دادگاه ارائه شود که برای قاضی قابل درک باشد و منجر به نتیجه‌گیری غلط نشود.

سازمانها و کسب و کارها تمایلی به افشاء حملاتی که تجربه می‌کنند، ندارند و معمولا این حوادث را به صورت داخلی مدیریت می‌نمایند بالاخص بانکها و موسسات مالی به دلیل ترس از افشاء آسیب‌پذیریها و احتمال وقوع حملات بعدی، لطمه به شهرت، از دست رفتن اعتماد عمومی و ازدست رفتن مشتریان اطلاعات حملات را افشاء نمی‌نمایند.

مدیریت نادرست داده‌های فورنسیک ممکن است کل پرونده را نابود نماید یا پی‌جویی را معلق کند، بنابراین داده‌ها و اطلاعات باید توسط متخصص آموزش‌دیده فورنسیک سایبر جمع‌آوری گردد. بنابراین برای سیستم‌های برخطی که ماموریت حیاتی دارند، باید تیم متخصصی وجود داشته باشد که در زمانهای بحرانی پس از وقوع حادثه بتوانند کمک کنند و مطمئنا در این حوزه کمبود پرسنل وجود دارد.

اگر قوانین یک کشور هیچ سیستم و رویه‌ای را برای جمع‌آوری و ذخیره‌سازی ادله دیجیتال در محل نداشته باشند، جرائم سایبر تعقیب و تنبیه نمی‌گردند و کارهای ماموران پی‌جویی استنادناپذیر است و تلف می‌گردد. همچنین در محیطهای شبکه‌ای مجرمین ممکن است از تنبیه سرباز بزنند چنانچه جرائم را از کشورهایی مرتکب شوند که قوانین درستی برای پیگرد ندارند و یا امکان پیگرد موفق در این کشورها وجود ندارد.

۵- مدل پیشنهادی برای پاسخگویی به حادثه و فورنسیک دیجیتال

همانگونه که در بخشهای قبلی ذکر شده، پاسخگویی به حادثه واکنش سازمان به عمل غیرقانونی یا غیرقابل قبول برعلیه اجزاء کامپیوتر یا شبکه سازمان می‌باشد. پاسخگویی به حادثه توسط گروههای آپا و یا در سطح سازمانها انجام می‌گیرد. در حین پاسخگویی به حادثه همانگونه که در مدل نشان داده شده، ادله دیجیتال نیز جمع‌آوری می‌گردند. ضابطان قضایی یا پاسخگویان به حادثه باید قوانین ادله را درنظر بگیرند تا بتوانند از دعوی خود در دادگاهها دفاع نمایند. ضابطان قضایی و پاسخگویان امنیتی ادله دیجیتال را به صورتهایی چون logهای شبکه، مستندات، ویدئو و تصویر و ... جمع‌آوری می‌نمایند. در برخی موارد نیاز به تحلیل تمام بیتهای ادله وجود دارد. در چنین شرایطی تصویربرداری نقش مهمی در اعتبار ادله دارد. در شکل ۱ متدولوژی پاسخگویی به حادثه به همراه فورنسیک دیجیتال معرفی شده است.[۴]

در این متدولوژی فرایند پاسخگویی به حادثه در هفت مرحله شرح داده می‌شود. اینک شرح مختصری از هر مرحله ارائه می‌شود.

- آماده‌سازی پیش از حادثه: این فاز حتی در زمانیکه حادثه به وقوع نپیوسته انجام می‌گیرد. در این فاز سازمان و تیم مدیریت حوادث برای حادثه آماده می‌گردند. آماده‌سازی سازمان با پیاده‌سازی معیارهای امنیتی میزبان‌بنیاد و

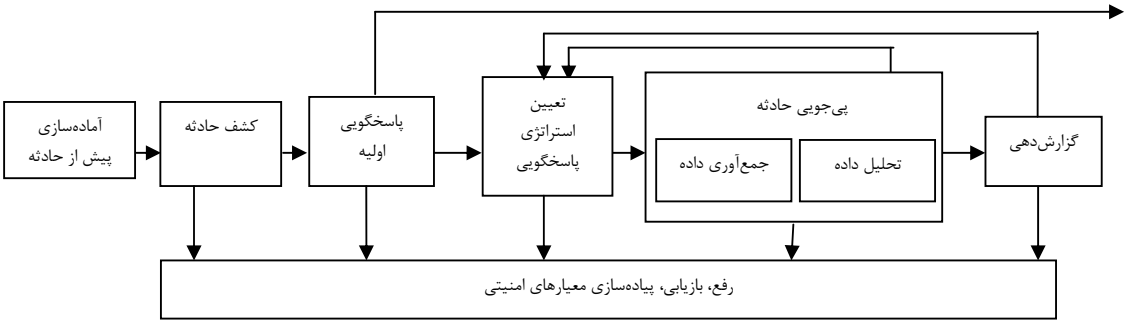
شبکه بنیاد انجام می‌گیرد. تیم مدیریت حوادث نیز باید ابزارهای لازم برای مدیریت حادثه را تهیه نمایند.

- کشف حوادث: کشف حادثه یکی از اجزاء مهم پاسخگویی به حادثه می‌باشد. هر فردی از مدیر سیستم یا کارمند که لزوما دانش فنی لازم درباره سیستم ندارد، می‌تواند حادثه را کشف نماید. در این فاز مشخص می‌شود به چه کسی باید درباره وقوع حادثه اطلاع داد.
- پاسخگویی اولیه: در این فاز پی‌جویی اولیه اطلاعات آغاز می‌گردد و شرح اولیه‌ای از حواشی حادثه ثبت می‌شود. جمع‌آوری باید به نحوی انجام شود که امکان تعیین استراتژی پاسخگویی مناسب فراهم شود. مصاحبه با افراد درگیر در حادثه و بررسی logهای موجود در سیستمها، نمونه‌ای از این اطلاعات می‌باشند.
- تعیین استراتژی پاسخگویی: بر اساس اطلاعات کسب‌شده از حادثه، بهترین استراتژی پاسخگویی تعیین می‌شود و تایید مدیریت گرفته می‌شود. هدف این فاز تعیین استراتژی پاسخگویی است که به بهترین شکل با شرایط انطباق دارد و کل شرایط را در نظر می‌گیرد. برخی از شرایط عبارتند از: بحرانی بودن سیستمهای آسیب‌دیده، نوع مهاجم مورد ظن و کل خسارتی که در سیستم ایجاد شده است. همچنین سیاستهای پاسخگویی سازمان نیز باید در نظر گرفته شوند.
- پی‌چویی حادثه: در طی پی‌جویی حادثه، انواع مختلفی از ادله مربوط به حادثه جمع‌آوری می‌گردند تا رویدادهای مربوط به حادثه امنیتی بازسازی شوند. این بازسازی، اطلاعاتی را درباره چه چیزی اتفاق افتاده، چه زمانی، چگونه، چرا و توسط چه کسی در اختیار قرار می‌دهند. جمع‌آوری داده‌ها به دو دسته جمع‌آوری داده‌های فرار و ماندگار تقسیم می‌گردد.
- گزارش‌دهی: پس از آنکه پی‌جویی حادثه امنیتی خاتمه یافت، همه یافته‌ها و نتایج باید در گزارشی به صورت دقیق مستند گردند. در این گزارش همه فعالیتهای پی‌جویانه مستند می‌گردند و همه نتایج بدست آمده به طور کامل شرح داده می‌شوند.
- رفع: در این فاز معیارهای امنیتی و تغییرات رویه‌ای صورت می‌گیرد، درسهای آموخته شده ثبت می‌گردند و fixها و راه‌حلهای طولانی مدتی برای مسائل مشخص شده توسعه می‌یابد.

۵-۱- وظایف اولین پاسخگویان حوادث برای جمع-آوری داده‌های فرار و ماندگار

داده‌های فرار در حافظه سیستم، ذخیره‌سازی می‌گردند (مانند رجیسترها، cache، RAM) و چنانچه برق سیستم قطع شود، سیستم خاموش و یا راه‌اندازی مجدد شود، از بین می‌روند. جمع-آوری این داده‌ها بسیار مهم می‌باشند. اولین قدم در پاسخگویی به حادثه جمع‌آوری داده‌های فرار و تحلیل نتایج برای تعیین اقدامات بعدی است. اولین پاسخگویان امنیتی نقش مهمی را در جمع‌آوری این داده‌ها دارند. مدیران سیستم‌ها و شبکه‌ها معمولا اولین پاسخگویان امنیتی می‌باشند. آنها باید به حادثه رسیدگی بنمایند و ریشه اصلی حادثه را مشخص کنند. آنها باید مجموعه ابزاری برای جمع‌آوری داده‌های فرار داشته باشند. [۳]

به هنگام جمع‌آوری داده‌های فرار از سیستم live، باید درجه فرار بودن داده‌ها در نظر گرفته شود. داده‌هایی باید ابتدا جمع‌آوری شوند که شانس بالاتری برای تغییر یا از دست رفتن داشته باشند. رجیسترها و cache، جداول مسیریابی، جدولarp ، جدول پروسه‌ها، آمار kernel و اتصالات، فایلهای سیستمی موقت نمونه‌هایی از داده‌های فرار می‌باشند.



شکل ۱- فرایند پاسخگویی به حادثه

اولین پاسخگویان امنیتی در جمع‌آوری داده‌های فرار ممکن است دچار دو اشتباه ذیل گردند:

- خاموش کردن یا راه‌اندازی مجدد ماشین
- فرض اینکه بیشتر قسمنتهای کامپیوتر مورد ظن قابل اعتماد می‌باشند.

داده‌های ماندگار پس از آنکه سیستم خاموش شد، بدون تغییر باقی می‌مانند. این داده‌ها بر روی دیسکهای سخت و رسانه‌های ذخیره-سازی جابجا شدنی قرار دارند. اگرچه داده‌های ماندگار طبیعت پایداری دارند اما برای جمع‌آوری آنها رعایت احتیاطهایی لازم و ضروری است. اولین پاسخگویان باید قبل از انجام هرگونه عملی بر روی کامپیوتر مورد ظن از داده‌های ماندگار آنها تصویربرداری نمایند تا مطمئن شوند که این داده‌ها دستخوش تغییر نمی‌شوند و استنادپذیری ادله به مخاطره نمی‌افتد.

۶- جمع‌بندی و نتیجه‌گیری

به منظور مبارزه با جرائم سازمان‌یافته، نفوذها و حملات سایبری و کدهای بدخواه اقدامات متعددی در کشور باید صورت گیرند. تشکیل و تقویت گروههای آپا و واکنش فوری یکی از اقدامات مهم و ضروری در این زمینه می‌باشد. پس از آنکه مکانیزمهای امنیتی سیستم‌ها به مخاطره می‌افتند و حوادث به وقوع می‌پیوندند، رسیدگی به حادثه، بازیابی سیستم‌ها، تعیین دامنه حادثه و پی‌جویی حملات و جرائم از مهمترین اقدامات می‌باشند. با تقویت گروههای آپا و واکنش فوری با ایجاد قابلیتهای تحلیل حوادث و بدافزارها، پی‌جویی حوادث و حملات و تحلیل آسیب‌پذیریها قدرت کشور در بازیابی از حادثه و تداوم خدمات و سرویسها افزایش یافته و امنیت و اعتماد تامین می‌گردد.

مراجع

[1] Cert Operational Gaps, ENISA, 2011.
[2] Information Security Challenges to Improving DOD's Incident Response Capabilities, GAO, 2001.
[3] Richard Nolan, Colin O'Sullivan, Jake Branson, Cal Waits, First Responder's guide to computer forensics, CERT training and Education, 2005.
[4] Kevin Mandia, Chris Prosise, Matt Pepe, Incident Response and computer forensics, McGraw-Hill, 2003.