فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال دوم، شماره‌ی ۵ (بهار ۱۳۹۲): صص ۱ – ۱۷

ارایه الگو مناسب برای تعاملات CERT مراکز نظامی

رضا کشاورز[۱]
علی ناصری[۲]
زین‌العابدین نوروزی[۳]

تاریخ دریافت: ۱۳۹۲/۰۲/۰۸
تاریخ پذیرش: ۱۳۹۲/۰۸/۱۰

چکیده

امروزه با پیشرفت فناوری اطلاعات و ارتباطات، این علم نوین به عنوان یکی از ارکان مهم در زیرساخت‌های حیاتی مبتنی بر فناوری اطلاعات تبدیل شده است و با افزایش اهمیت آن، حملات و آسیب‌پذیری‌های آن نیز افزایش یافته است. از این‌رو یکی از اجزای مهم امنیتی، CERT است که با داشتن یک برنامه مدون و از پیش تعریف شده باعث کاهش مخاطرات و هزینه‌ها می‌شود. به همین منظور پس از بررسی الگوهای CERT، به ارایه یک الگو جدید برای بهبود تعاملات بین اجزای CERT در پاسخ‌گویی رخداد پرداخته‌ایم که می‌تواند جهت افزایش سرعت گروه CERT در هنگام رویارویی و مهار یک رخداد و در راستای پدافند غیر عامل استفاده شود. از جمله مزیت این الگو، تبیین نقش افراد و منسجم ساختن ارتباط بین CERT و مرکز کنترل امنیت در پاسخ‌گویی به یک رخداد در زمان مناسب است.

کلید واژه‌ها: *مدیریت رخداد، پاسخ‌گویی به حادثه، مهار رخداد، CERT*

۱- کارشناس ارشد پدافند غیر عامل- Emai: Rezakeshavarz۹۲@yahoo.com
۲- دکتری پردازش دیجیتال - دانشگاه علم وصنعت
۳- دکتری رمز دانشگاه امام حسین علیه السلام

۱- مقدمه

پدافند غیر عامل در حوزه فناوری اطلاعات شامل کلیه اقدامات به منظور حفظ امنیت اطلاعات، ایمنی و پایداری شبکه، توسعه ظرفیت دفاع الکترونیکی و تقویت ضریب امنیت در حوزه‌های زیر ساخت ملی و حیاتی است (یزدان پناه،۱۳۹۰: ۲۴-۱۹) یکی از ابزارهای مهم مورد استفاده برای رسیدن به این اهداف، ایجاد گروه‌های فوریتی پاسخ‌گویی رایانه‌ای یا همان CERT[1] است. هنگامی که مشکلات امنیتی برای سازمان رخ می‌دهد، نکته بسیار مهم آن است که سازمان مزبور شیوه پاسخ‌گویی مناسب را بداند. در واقع سرعت در تشخیص، تحلیل و پاسخ‌گویی یک مشکل امنیتی، میزان خطر و هزینه ترمیم را کاهش می‌دهد. (J. West-Brown,۲۰۰۷: ۲۹۱) هر سازمانی باید بتواند حملات مربوط به سازمان خود را شناسایی و در کوتاه‌ترین زمان ممکن مهار نماید. این حملات شامل تلاش برای دست‌یابی به یک سامانه یا داده‌های آن، ممانعت از اجرای سرویس، استفاده غیرمجاز از سامانه برای پردازش یا ذخیره داده‌ها، تغییر سخت‌افزار یا نرم‌افزار، کدهای مخرب، از بین رفتن محرمانگی و جامعیت اطلاعات، سوءاستفاده از سامانه‌های اطلاعاتی و غیره است (Georgia Killcrece;۲۰۰۴). برخیCERTها بسته به نیازمندی‌ها و شرایط سازمان شامل مجموعه‌ای کامل از سرویس‌ها، شامل تجزیه و تحلیل، پاسخ‌گویی و عکس‌العمل نسبت به حملات، مواجهه و مدیریت آسیب‌پذیری، تشخیص نفوذ، ارزیابی ریسک، ایجاد سامانه‌های پشتیبان شبکه، تست نفوذ به شبکه، رایزنی‌های امنیتی و غیره می‌باشد (Penedo, David;۲۰۰۶:۲۷-۳۲).

۲- بیان مسئله

برای داشتن یک گروه امنیتی کارا و توسعه سرویس‌های CERT، درک صحیح از نیازمندی‌های سازمان، اطلاعات مشترک، سرعت تبادل اطلاعات، اطلاعات دقیق، نوع محصولات و سرویس‌ها بسیار مهم است. بعد از آن، می‌بایست الگوهای قابل اعتماد در پاسخ‌گویی بررسی شود و تلاش در جهت حصول سرویس‌های امنیتی هشداردهنده برای درک بهتر آسیب‌پذیری سامانه، صورت گیرد. هر چند که شالوده CERT پاسخ‌گویی سریع است اما مهم، این است که ساختار ذاتی و اصلی و نیازمندی‌های محیطی که در آن CERT اجرا خواهد شد و نیز جایگاهی که CERT برای مدیریت ریسک در آن محیط می‌تواند ایفا نماید را درک کنیم (J. West-Brown,۲۰۰۷: ۲۹۱) لذا با نگرش به مراتب فوق، شناخت شیوه‌های جدید در پاسخ‌گویی می‌تواند در دفاع غیر عامل نقش تعیین کننده‌ای ایفا نماید. داشتن یک الگوی مناسب و دقیق برای پاسخ‌گویی و ارایه سرویس در یک گروه CERT از اصول اولیه است، به طوری که امکان مدیریت و تأمین منابع مورد نیاز برای کاربران CERT فراهم گردد. طراحی سرویس، ساختار و نحوه تعاملات، یکی از ارکان اساسی برای ایجاد CERT در سازمان است (http://en.wikipedia.org). نیاز به الگویی مناسب در پاسخ‌گویی، منجر به طرح این سئوال می‌گردد که چگونه

۱. Computer Emergency Response Team

می‌توان با شناسایی و بررسی الگوهای موجود در دنیا به الگوی بهینه‌ای در پاسخ‌گویی به رخداد دست یافت؟ در این مقاله با تطبیق الگوهای سازمانی دیگر و سرویس‌های مورد نیاز، به تشریح نقش افراد در زمان وقوع رخداد رایانه‌ای پرداخته شده، سپس فرآیند نحوه مقابله با یک رخداد و ارتباط بین مولفه‌های مرکز عملیات امنیتی و CERT بیان گردیده، در نهایت الگوی مناسبی برای تعاملات CERT در زمان وقوع رخداد و در راستای اصول پدافند غیر عامل ارایه گردید.

۳- روش‌شناسی پاسخ‌گویی به حوادث

یک روش شناسی در پاسخ‌گویی حوادث، قسمتی از یک چارچوب مدیریتی ارتباطی و خوب است که برای شناسایی و ارزیابی در فرآیند مدیریت رخداد به کار می رود. در این قسمت تعدادی از روش شناسی‌های مهم را از دیدگاه‌های مختلف بررسی می‌کنیم.

۳-۱- روش‌شناسی پاسخ‌گویی حوادث از دید SEI[۱]

این نوع، به عقیده کارشناسان SEI، مجموعه ای از توابع مدیریتی رخدادهاست. این الگویی است که با آن، شناسایی و ارزیابی مقایسه‌ای در فرآیند مدیریت حوادث رخداد در سازمان‌ها حاصل می‌شود. این الگو و نتایج شناسایی، ابزاری برای تقویت و ارزیابی الگویی مدیریت رخداد است که با هدف انسجام در پاسخ‌گویی به رخداد صورت می‌گیرد و شامل این مراحل است: ۱-آماده‌سازی ۲- محافظت ۳- آشکارسازی ۴- تریاژ ۵- پاسخ‌گویی

اطمینان و تاکید لازم در به‌کارگیری مناسب تجهیزات حفاظتی شبکه، در مرحله آماده‌سازی و محافظت است. گزارش رخدادها و آسیب‌پذیری‌ها، رصد شبکه، درخواست‌های عمومی و غیره همگی به عنوان ابزار آشکارسازی در مرحله بعد می‌باشد که پس از ترکیب و اطمینان از وقوع رخداد به قسمت تریاژ ارجاع می‌شود. واحد تریاژ، واحد گزارش‌گیری و جمع‌آوری اطلاعات از تمامی نقاط شبکه است. در نهایت، مرحله پاسخ‌گویی پس از ارایه راه‌کارهای لازم صورت می‌گیرد.

۳-۲- روش شناسی پاسخ‌گویی حوادث از دید NIST[۲]

یک روش شناسی در پاسخ‌گویی حوادث، قسمتی از یک چارچوب مدیریت ارتباطی مناسب است که با داشتن یک روش شناسی به صورت چندین ارایه مجزا از یکدیگر برای پاسخ‌گویی دقیق به یک رخداد است.

۱. Software Engineering Institute

۲. National Institute of standard and technology

مهم‌ترین این روش شناسی‌ها در چارچوب پاسخ گویی به رخدادها، توسط متخصصان دانشگاه دیپوال[1] با گروه مهندسی نرم افزار انستیتو کارنگی ملون[2] و NIST طراحی شده است که هدف از آن کوتاه‌تر کردن دامنه اثرات رخدادها است و شامل مراحل زیر است:

۱- آماده‌سازی	۲- تشخیص	۳- پاسخ‌گویی به حادثه
۴- جمع‌آوری	۵- محافظت	۶- آزمایش
۷- تحلیل	۸- بازرسی	۹- ارایه.

این الگو، قابل کاربرد به صورت بی‌درنگ و پس از حمله است. پنج مرحله اول بر ترافیک بی‌درنگ شبکه عمل می‌کند. مرحله آماده سازی تضمین می‌کند که تجهیزات نظارتی در جایگاه خود قرار دارد. مرحله تشخیص در کشف حمله کمک می‌کند و مرحله جمع‌آوری، بسته‌های شبکه را گرفته، صحت داده‌ها را تضمین می‌کند. پاسخ مناسب به حادثه بر اساس ماهیت حمله تولید می‌شود و در مرحله محافظت، درهم سازی داده‌ها ایجاد شده، یک نسخه از آن ساخته می‌شود. چهار مرحله بعد برای سناریوهای بی‌درنگ و پس از حمله کاربرد دارد.

رسیدگی پس از حمله، با مرحله آزمایش شروع می‌شود، به‌طوری‌که یک نسخه از فایل دریافتی مرحله آزمایش ورودی منابع مختلف را ترکیب و شاخص‌های حمله را شناسایی می‌کند. مرحله تحلیل با روش‌های استخراج داده، محاسبات نرم افزاری و آماری، الگوهای حمله را طبقه بندی می‌کند. مرحله بازرسی شامل ردیابی به عقب و شناسایی مهاجم می‌باشد. مرحله نهایی ارایه منجر به تعقیب قانونی مهاجم می‌شود (۲۷-Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi۲۰۱۰ :۱۴).

۳-۳- فرآیند پاسخ‌گویی از دید JPCERT[3]

فرآیند پاسخ‌گویی از دید CERT ژاپن بدین صورت است که درخواست‌ها و گزارشات به واحد تریاژ ارسال شده، پس از جمع‌آوری، برای پشتیبانی و بررسی به خبرگان، مهندسین و CSIRTها ارجاع می‌شود. همچنین بازخوردی را که از گزارشات دریافتی، مدیریت‌ها و دیگران دریافت شده است در تعامل با بخش بررسی و ارزیابی قرار می‌گیرد و پس از تجمیع نظرات و راه‌کارها از طریق واحد تریاژ، به مجمع CERT

۱. Depaul
۲. Carnegie Mellon
۳. jappanices CERT

اعلان رخداد می‌شود و در مجمع کلی CERT برای از بین بردن رخداد و آسیب‌پذیری اقدام می‌شود (Keisuke kamata, ۲۰۰۷:).

۴- محل استقرار و گزارش‌دهی CERT در سازمان

CERT از نظر جایگاه ساختمانی می‌تواند در موقعیت‌های متفاوتی قرار گیرد. درون مدیریت‌های فناوری اطلاعات یا مدیریت امنیت و حتی در مدیریت زیر ساخت به عنوان یک واحد می‌تواند قرار گیرد، یا اینکه به عنوان یک معاونت مستقل زیر نظر مستقیم مدیر کل قرار گیرد و این وابسته به اقتداری است که در سازمان برای آن تعریف می‌شود؛ به عنوان مثال CERT ایالات متحده یا همان US-CERT با توجه به نفوذ خود می‌تواند ارتش را به عکس‌العمل‌هایی وادار کند.

برای کسب اطلاعات بیشتر، طی مطالعات انجام شده از گروه‌ها، محل استقرار سازمانی آن‌ها، پرسیده شد. اکثریت گروه‌ها یعنی ۴۱ درصد در واحد فناوری اطلاعات مستقر بودند و ۲۴ درصد به عنوان گروهی مجزا و خارج از سایر بخش‌ها به عملیات می‌پرداختند. درباره گزارش دهی به مدیریت، ساختار ثابت و مشخصی به دست نیامد و تنها نتایج زیر حاصل شد:

- ۳۸ درصد از شرکت کنندگان به فردی غیر از کارشناس فناوری اطلاعات سازمان، مدیر فناوری اطلاعات، مدیر CERT یا مدیر امنیت گزارش می‌دهند.
- ۳۱ درصد از شرکت کنندگان به کارشناس فناوری اطلاعات سازمان گزارش می‌دهند.

در بخش بانکی تمامی گروه‌ها به کارشناس فناوری اطلاعات گزارش ارائه می‌دهند (ENSIA : ۲۰۰۸).

۵- تطبیق الگوهای CERT در پاسخ‌گویی

۵-۱- الگوهای سازمانی از دیدگاه ENSIA[۱]

در الگوهای سازمانی از دیدگاه ENSIA، نحوه ارتباط بین بخش‌ها با یکدیگر و ساختار سازمانی و نیروی انسانی در پاسخ‌گویی به رخدادها به صورت زیر می باشد:

۵-۱-۱- الگوی تجاری مستقل

در این ساختار CERT کاملاً به طور مستقل عمل می‌کند و مدیر و کارمندان مستقلی دارد به نحوی که گاه حتی از لحاظ جغرافیایی نیز خارج از سازمان خود قرار می‌گیرد.

۱. European Network and Information Security Agency

۵-۱-۲- الگوی ادغام شده[۱]

در این ساختار یک نفر به عنوان سرپرست گروه معرفی می‌شود که با شناسایی متخصصان امنیت اطلاعات در موارد واکنشی یا پیش‌گیرانه استفاده می‌کند. در ضمن سرپرست گروه می‌تواند در شرایط خاص تقاضای نیروی انسانی بیشتر داشته باشد. الگوی ادغام شده در مواقعی مفید است که CERT در سازمان میزبان ایجاد شده است و قصد استفاده از امکانات واحد فناوری اطلاعات را دارد.

۵-۱-۳- الگوی تحقیقاتی

در این الگو تعدادی از مراکز تحقیقاتی و دانشگاهی را که در نقاط مختلف قرار گرفته‌اند و گاه کل کشور را پوشش می‌دهند، برای ارایه سرویس‌های CERT برای سازمان مادر و کلیه شعبه‌های آن در نظر گرفته می‌شود. معمولاً این مراکز به صورت مستقل از یکدیگر عمل می‌کنند و برای خود ساختار مجزایی دارند اما در ساختار CERT مرکزی یا مادر عمل می‌کنند. CERT مرکزی علاوه بر نقش هماهنگی بین CERTها، به عنوان پنجره یکتای ارتباط با محیط خارج از سازمان نیز محسوب می‌شود.

۵-۱-۴- الگوی داوطلبانه

در الگو داوطلبانه تعدادی از افراد و متخصصان در یک گروه و به صورت داوطلبانه به پشتیبانی از یکدیگر می‌پردازند و انگیزه شخصی مهم‌ترین عامل پیش‌برنده در این گروه است (ENSIA : ۲۰۰۸).

۵-۲- الگوی میتروپولوس برای پاسخ گویی به رخداد

در الگویی که توسط میتروپولوس[۲] ارایه شده است مدیر گروه می‌بایستی مسایل را به مدیر ارشد مستقیماً ارجاع دهد و مدیر ارشد هم به دیگران مسأله را اطلاع رسانی نماید. کارکنان میز پشتیبان[۳] برای اینکه هم در زمان پاسخ گویی به بازرسین توجیه باشند و هم برای حملاتی مانند حملات انکار سرویس[۴]، حملات بر روی سرویس دهنده وب، سرویس دهنده FTP[۵] و پست الکترونیکی نیز آمادگی لازم را داشته باشند، باید در این امر سهیم شوند. روابط عمومی می‌تواند با داشتن یک نسخه از رخدادهای انجام شده امکان پاسخ‌گویی و ارتباط با دیگران را دارا باشد که شامل ارتباط با قسمت‌های دیگر مثل پیمانکار است. بنابراین منابع انسانی هم می‌تواند برای یک عملکرد مناسب در زمان رخدادهای داخلی به‌کارگیری شود.

۱. Embedded
۲. Sarandis Mitropoulos
۳. Help desk
۴. Denial of service
۵. File Transport Protocol

بازرسی سازمان وظیفه مهمی دارد و آن زمانی است که مجبور به نگهداری اسرار برای مدتی، و تسهیل در ردیابی[1] رخداد به قسمت پاسخ‌گویی می‌باشد تا اجازه ندهد که اطلاعات به خارج از سازمان درز پیدا کرده، باعث ایجاد اثراتی در اذهان عمومی گردد. این گروه اغلب در خارج سازمان با دیگر افراد مرتبط امنیتی که بازرس حوادث امنیتی هستند با اعمال قوانین فوریتی در مورد رخدادهای جدی مشارکت می‌کنند (مثل سرقت تجهیزات IT، نسخه برداری غیرمجاز، نرم افزار یا دیتا و درج قوانین امنیتی که مورد نیاز است). مشاور قانونی سازمان در توسعه توانمندی‌های گروه پاسخ‌گویی شرکت نموده، مقررات زمان رخداد را وضع می‌کند. کارکنان سازمان بایستی آموزش داده شوند و مطابق سیاست‌ها، روش‌ها و راهبردها عمل نمایند. بنابراین کارکنان بایستی بدانند که در زمان به وجود آمدن یک رخداد چگونه عمل نموده، با چه کسی ارتباط برقرار نمایند. در بسیاری از مواقع رخدادهای امنیتی توسط کاربران معمولی کشف شده است. یک ارتباط سالم و سریع از طرف کاربران معمولی در مواقع ضروری در پاسخ‌گویی کارآمد خواهد بود. بر اساس اهمیت رخداد امنیتی، ممکن است که از دیگر قسمت‌های خارجی که می‌تواند نقش مهمی را در کشف و پاسخ‌گویی رخداد امنیتی داشته باشد استفاده کرد. مثلاً ISP[2] می‌تواند اطلاعات خوبی را در زمانی که قصد ردیابی یک ارتباط شبکه‌ای را از زمانی که ISP ها در حال برقراری ارتباط سامانه‌های سازمانی و شبکه خارج از سازمان هستند به دست آورد. و بالاخره گروهCERT و متخصصان بیرونی دیگر که می‌توان از دانش و تجربیات به دست آمده آن‌ها حداکثر استفاده لازم را برد (Sarandis Mitropoulos, ۲۰۰۸:)

۶- سرویس‌ها و ساختار پیشنهادی CERT مراکز نظامی

۶-۱- مأموریت

گروه CERT مراکز نظامی عموما با هدف کنترل موثر رخداد، پیش‌گیری از رخداد، بهبود امنیت با تعریف مخاطرات و حوادث، پایش شبکه، محافظت منابع داده، ترویج دانش رایانه کاربران، پشتیبانی و ترویج امنیت سایبری به‌کارگیری می‌شود.

۶-۲- الگوی سازمانی CERT مراکز نظامی

CERT به الگوهای مختلفی تقسیم می‌شود که عبارت است از: ۱-گروه امنیتی ۲- داخلی (توزیع شده داخلی، متمرکز داخلی و ترکیبی) ۳- هماهنگ کننده. در جدول (۱) نقاط قوت و ضعف این الگوها به اختصار بیان شده است. پس از مطالعه و تحقیق در ساختارهای گوناگون نظامی دنیا، الگوی پیشنهادی برای

۱. Tracing

۲. Internet service provider

CERT مراکز نظامی پیشنهاد گردید. با توجه به گسترش جغرافیایی و تجهیزات فناوری اطلاعات در مراکز نظامی و تعدد گردان‌ها و تیپ‌های نظامی و وجود رده‌های عمده، مانند نیروهای دریایی، زمینی، هوایی، مراکز تحقیقاتی، موسسات آموزشی و غیره، از گستردگی و پراکندگی بسیار بالایی برخوردار هستند؛ لذا برای مدیریت بهینه گروه CERT در مراکز نظامی، الگوی CERT در دو لایه پیشنهاد می‌شود: ۱- لایه درونی، که مختص مراکز نظامی‌های استانی- ایالتی، ستاد نیروها و مراکز تحقیقاتی است و به صورت الگوی ترکیبی با یکدیگر تعامل دارد. ۲- لایه بیرونی، که این لایه مختص فرماندهی فناوری اطلاعات مراکز نظامی بوده، با CERT ملی به صورت هماهنگ کننده تعامل می‌نماید.

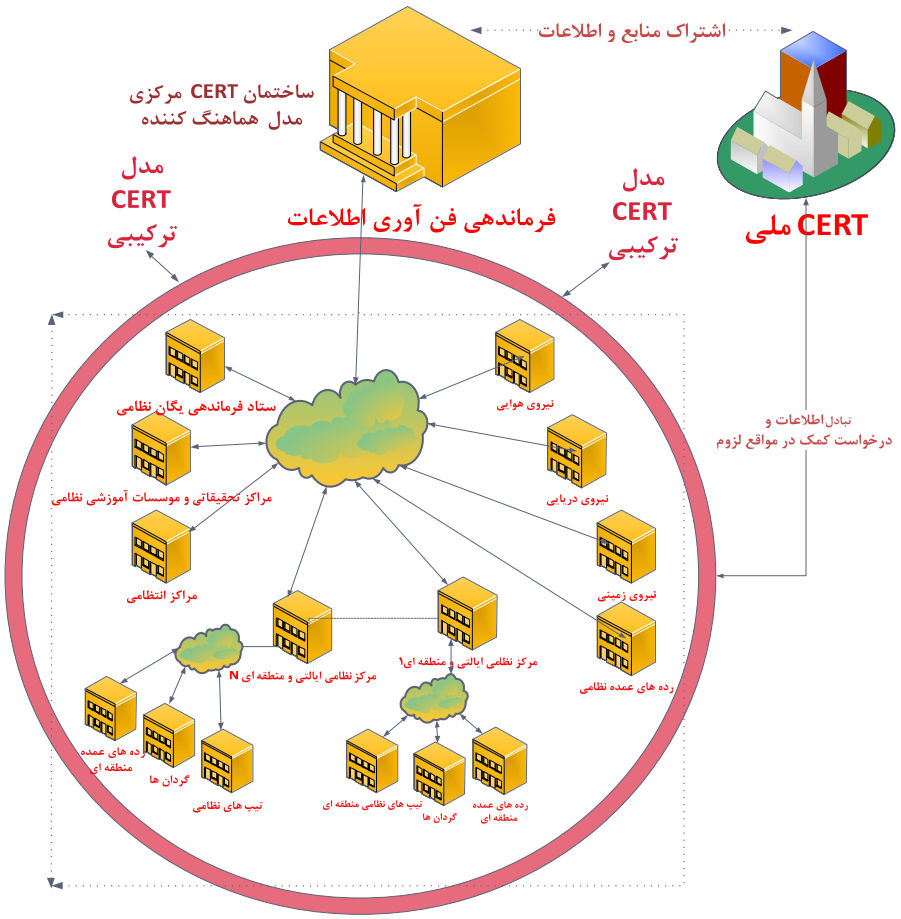
جدول ۱- مقایسه نقاط قوت و ضعف الگوهای CERT [۳،۲و۷]

	گروه امنیتی	توزیع شده داخلی	متمرکز داخلی	توزیع شده و متمرکز داخلی	هماهنگ کننده
نقاط قوت	-هیچ نقطه قوتی به دلیل نبود حل و فصلی مشاهده نمی شود	-تمرکز در مسوولیت -یکپارچگی در ماموریت -داشتن پایگاه داده متمرکز -داشتن دیدگاه جامع -قابلیت نیروهای محلی	-داشتن کارکنان متمرکز و اختصاصی و آموزش دیده -شناسایی حمله های هدفدار -داشتن پایگاه داده قوی -پشتیبانی آموزشی قوی مراکز سهولت در حفظ تیم	-داشتن نیروهای متمرکز و توزیع شده -داشتن پایگاه قوی داده -یکپارچگی در ماموریت -مسولیت متمرکز و تلفیقی -پشتیبانی آموزشی قوی رده ها -سهولت در پیاده سازی دستورالعملها	-دارای کارکنان اختصاصی و کارآزموده -دارای یک واحد قوی گزارش دهی -دارای واحدی متمرکز برای تحلیل اطلاعات -دارای یک پایگاه داده قوی -وجود تریاژ در خارج سازمان -پشتیبانی قوی آموزشی رده ها
نقاط ضعف	-نبود ضمانت اجرایی -عدم مشارکت گروه ها -هزینه کمتر و لی آسیب بیشتر -عدم هماهنگی پرسنل -دشواری در تعیین مسول رسیدگی	-کمبود نیروی متخصص -نبود فیدبک برای صحت انجام کارها -عدم مقیاس گذاری در مناطق بزرگ -دشواری در حفظ یکپارچگی -امکان تحمیل مسوولیت مازاد -نیاز به پشتیبانی مدیریت -به روز نگه داشتن اطلاعات افراد	-دشواری هماهنگی با سایتهای شعب -ایزوله بودن از نظر پرسنل -دشواری حفظ پشتوانه مالی -دشواری در اطاعت پذیری رده ها -امکان کمبود نیرو برای پشتیبانی لازم -زمان طولانی برای انجام فرامین -به روز نگه داشتن اطلاعات افراد	-دشواری در مدیریت و هماهنگی -دشواری حفظ منابع مالی -نیاز شدید به پشتیبانی مدیریت -امکان کمبود منابع انسانی و مالی برای پشتیبانی لازم -نیاز به خرید یک سیستم ردیابی قوی -امکان ایزوله بنظر رسیدن اعضای متمرکز -نیاز به استخدام نیرو و تجهیزات	-دشواری هماهنگی با رده ها -ایزوله بودن از نظر بقیه -امکان پشتیبانی مالی رده ها -پیچیدگی تعیین تعداد کارکنان -دشواری پوششی مدیریت -ثابت نبودن کارشناسان رده ها -عدم ارسال بموقع رده ها -نبود فیدبک از اجرای اخطارها -زمانبری اجرای فرامین -نیاز به خریداری سیستم ردیابی قوی -جلب اعتماد رده های تحت پوشش -به روز نگه داشتن افراد

لذا با توجه به پراکندگی و نیاز به داشتن یکپارچگی در مأموریت و انسجام بیشتر، پاسخ‌گویی سریع به رخدادها، مسوولیت متمرکز و تلفیقی و پشتیبانی بهتر رده‌ها و دیگر نیازمندی‌ها و با توجه به جدول (۱)، مقایسه نقاط قوت و ضعف الگوها، الگوی ترکیبی (ادغام متمرکز و توزیع‌پذیر) را می‌توان برای مراکز نظامی‌های استانی- ایالتی و ردهای عمده که در سطح مناطق پخش هستند در نظر گرفت. هر چند که الگوی متمرکز نیز تا حدی می‌توانست مناسب باشد ولی به علت پراکندگی نقاط، اتلاف زمان برای شناسایی و از بین بردن رخداد این گزینه را نفی می‌کند لذا الگوی ترکیبی که برای سازمان‌های بزرگ و پراکنده به بهترین نحو عمل می‌کند و دارای ویژگی‌هایی است که سازگاری آن با وضعیت مراکز نظامی مطابقت دارد پیشنهاد می‌گردد. همچنین ویژگی‌های عمده الگوی ترکیبی برای مراکز نظامی‌های استانی-ایالتی و رده‌های عمده عبارت است از:

- تشکیل بخش متمرکز CERT به صورت هسته‌ای پایدار از افراد متخصص
- توزیع تعدادی از کارمندان موجود در موقعیت‌های راهبردی مراکز نظامی و دیگر رده‌ها
- جمع آوری، ترکیب و پی گیری تمامی گزارش‌ها توسط اعضای گروه مرکزی
- تحلیل مناسب و کارا و تدوین راهبردهای مهار رخدادها توسط گروه مرکزی
- پیاده‌سازی راهبردهای تدوین شده در هسته مرکزی، توسط اعضای پراکنده گروه
- پاسخ‌گویی سریع‌تر به رخدادها توسط اعضای توزیع شده گروه در سطح مراکز
- انتقال مهارت و دانش به حوزه‌های مسوولیت توسط اعضای پراکنده گروه

فرماندهی فناوری اطلاعات مراکز نظامی نیز با توجه به متولی بودن برقراری امنیت اطلاعات، به عنوان CERT هماهنگ کننده برای برقراری ارتباط بین CERTهای مراکز نظامی‌های استانی- ایالتی و دیگر مناطق گزینه مناسبی خواهد بود. بنابراین در CERT مراکز نظامی، الگوی سازمانی ترکیبی برای مراکز نظامی استانی ـ ایالتی و رده‌های عمده و الگوی هماهنگ کننده برای فرماندهی کل مراکز نظامی پیشنهاد می‌گردد. شکل (۱) الگوی پیشنهادی ترکیبی و هماهنگ کننده را برای CERT مراکز نظامی نشان می‌دهد.



شکل ۱- الگوی پیشنهادی CERT ترکیبی و هماهنگ کننده برای مراکز نظامی

۶-۳- سرویس‌های اصلی و خدمات تکمیلی CERT

سرویس‌های هر CERT بر مبنای مأموریت، اهداف، محدوده عملکرد و جایگاه سازمانی آن متفاوت است. مسلماً رسیدگی به حادثه، هدف اصلی این سرویس‌ها را تشکیل می‌دهد. با در نظر گرفتن مأموریت و مطالعه در اهداف CERT برای عموم مراکز نظامی، سرویس‌های مورد نیاز مطابق جدول (۲) می‌باشد که در دو بخش سرویس‌های اصلی و سرویس‌های فرعی ارایه می‌شوند. هر چند که پیشنهاد می‌شود در مرحله آغاز سرویس‌های اصلی راه‌اندازی شود و پس از شکل‌گیری و تقویت CERT، سرویس‌های فرعی نیز راه‌اندازی گردد.

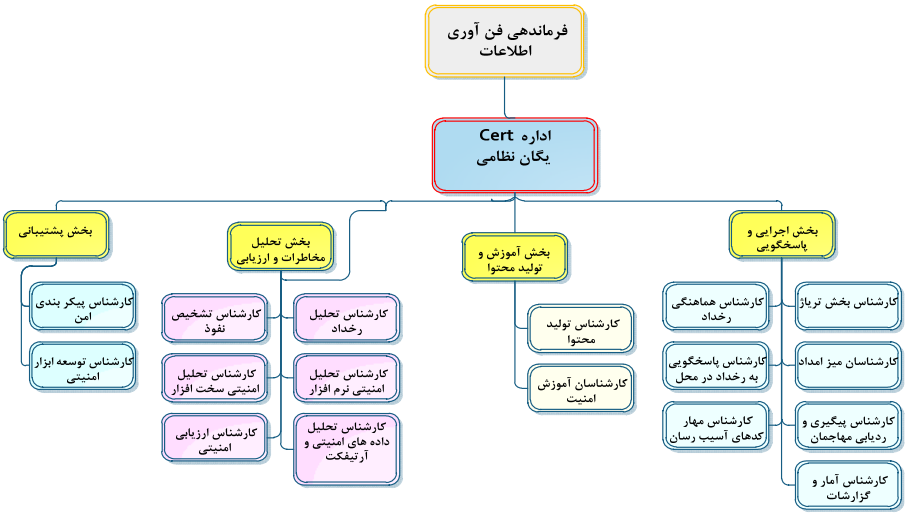
جدول ۲- سرویس‌های خدمات اصلی و فرعی CERT مراکز نظامی

	سرویس‌های اصلی	سرویس‌های فرعی
۱	هشدارها و اخطارها	پاسخ‌گویی به رخداد در محل
۲	تحلیل رخداد	سرویس‌های تشخیص نفوذ
۳	پشتیبانی پاسخ‌گویی به رخداد	تحلیل حفره‌های امنیتی و آثار باقی‌مانده از حمله
۴	هماهنگی در پاسخ‌گویی به رخداد	ممیزی یا ارزیابی امنیتی
۵	هماهنگی در پاسخ‌گویی به حفره‌های امنیتی و آثار باقی‌مانده	تنظیم، پیکربندی و نگهداری ابزارها، نرم افزارها و زیر ساخت های امنیتی
۶	اعلان‌ها	توسعه ابزارهای امنیتی
۷	پایش فناوری	
۸	انتشار اطلاعات مرتبط با امنیت	

۶-۴- ساختار پیشنهادی CERT در مراکز نظامی

ساختار مناسب از دیدگاه ENSIA، ساختاری است که دارای شرایط زیر باشد (۲۷-۱۴: ۲۰۱۰ Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi): ۱- دارای انعطاف پذیری مناسب گروه ۲- استفاده از نیروهای کارآمد و با توانائی‌های بالا در تحلیل وقایع ۳- توانایی پاسخ‌گویی یک گروه به صورت ۲۴×۷ ۴- چینش مناسب و سعی در استفاده حداکثری از نیروهای تمام وقت. با توجه به سرویس‌های مورد نیاز در CERT مراکز نظامی، جهت اجرای بهینه سرویس‌ها، نیاز به ساختاری مناسب می‌باشد؛ لذا چهار بخش زیر برای ایجاد CERT ضروری است که تعداد نیروی انسانی برای هر کدام از این بخش‌ها بستگی به استعداد سازمان مربوطه دارد. همچنین پیکربندی این بخش‌ها به همراه کارشناس یا کارشناسان لازم در شکل (۲) نشان داده شده است:

۱- بخش اجرایی و پاسخ‌گویی برای کنترل رخداد و مدیریت پاسخ‌گویی
۲- بخش تحلیل مخاطرات برای تحلیل رخدادها و کدهای مخرب
۳- بخش پشتیبانی برای توسعه ابزارهای امنیتی و مدیریت پیکربندی
۴- بخش آموزش و تحقیق برای مشاوره و آموزش و تولید محتوا

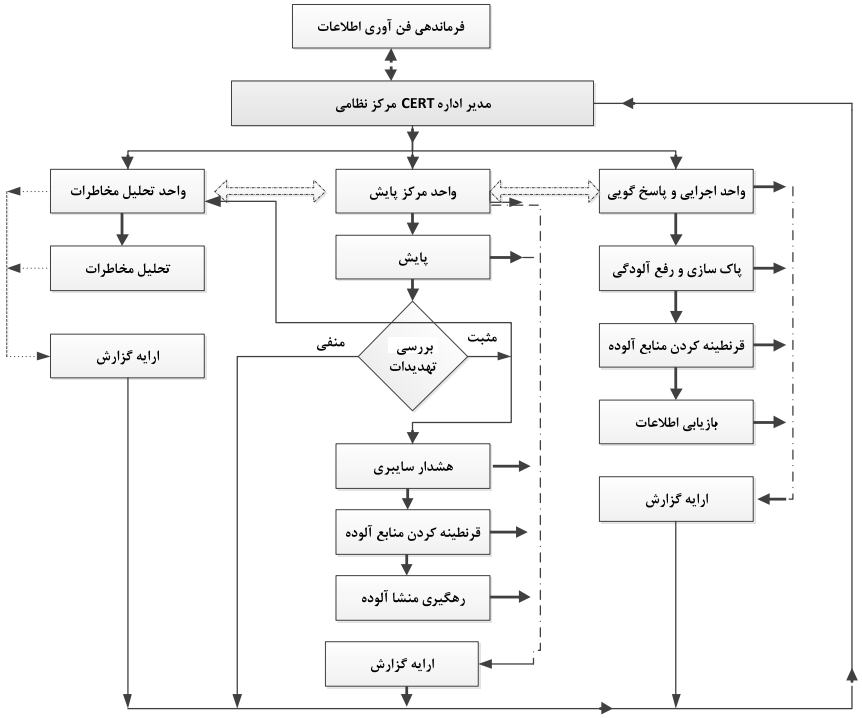


شکل ۲- ساختار پیشنهادی و بخش‌های مورد نیاز CERT در مراکز نظامی

۷- الگوی فرآیند نحوه مقابله با یک رخداد و ارتباط بین مؤلفه‌ها

برای داشتن یک گروه منسجم و هماهنگ در برابر رخدادهای امنیتی و حملات سایبری بهتر است که الگوی مناسبی را به عنوان فرآیند مقابله با یک رخداد امنیتی تعریف گردد. بدیهی است که با داشتن الگو و فرآیندی از پیش تعریف شده، سرعت در واکنش و پاسخ‌گویی بهینه خواهد شد. در این الگو، نحوه برقراری ارتباط بین CERT و واحد پایش که به عنوان مرکز عملیات امنیتی[۱] است و در نقش بازوی اجرایی CERT عمل می‌نماید، مشخص شده است (شکل ۳). واحد مرکز پایش، در قسمت مانیتورینگ، ضمن رصد تمامی نقاط شبکه، در صورت بروز هشداری به واحد تحلیل مخاطرات و واحد اجرایی اطلاع رسانی می‌کند؛ و آن‌ها نیز بر حسب وظیفه از پیش تعریف شده اقدام به تحلیل، قرنطینه نمودن منابع آلوده، پاک‌سازی و رفع آلودگی می‌نمایند.

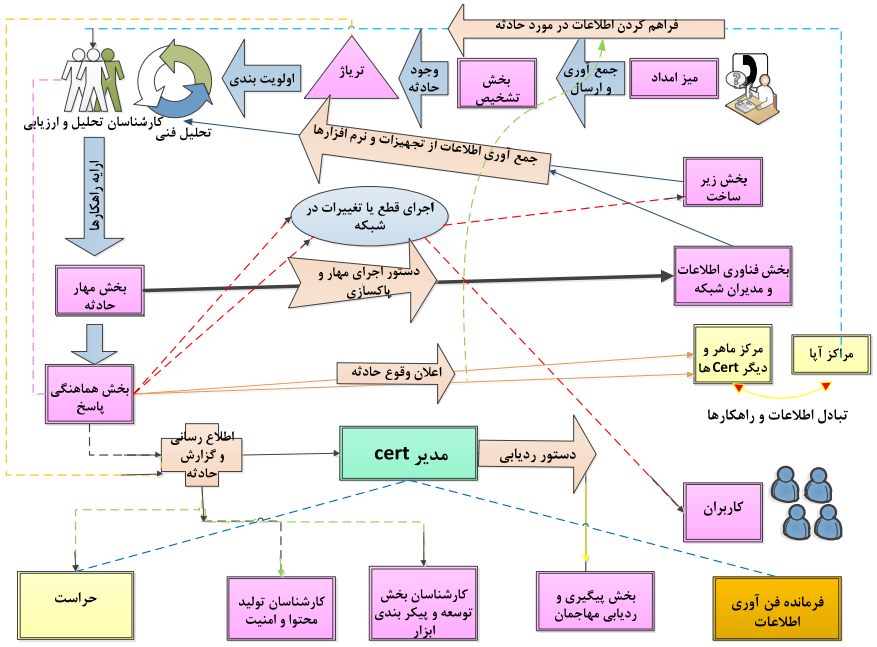
۱. security operation center (SOC)



شکل ۳- فرآیند نحوه مقابله با یک رخداد و ارتباط بین مؤلفه‌های مرکز عملیات امنیتی و CERT

۸- ارایه الگوی مناسب برای تعاملات CERT در حین بحران

در هنگام مواجهه با یک حادثه مشکوک یا رخداد، داشتن یک روش مناسب برای گروه CERT ضروری است. این روش و جریان کاری شمایی کلی از مسوولیت‌ها، وظایف، سرویس‌ها، ساختار سازمانی و دیگر مطالب گفته شده در برنامه‌های یک گروه CERT را نمایان می‌سازد. در این الگو (شکل ۴)، پس از مواجه با یک حادثه مشکوک که توسط کاربران از طریق پست الکترونیکی، فاکس، تلفن، پرتال سازمانی و دیگر موارد ممکن به کارشناسان میز امداد گزارش می‌شود. این کارشناسان، گزارشات دریافتی را به بخش تشخیص اعلان می‌نمایند. بخش تشخیص با بهره‌گیری از کارشناسان موجود، موارد را مطالعه کرده، پس از دریافت گزارشات دیگر از نرم افزارها و سخت افزارهای مانیتورینگ مرکز عملیات امنیتی، آن‌ها را ترکیب نموده، در صورت اطمینان از وجود یک حادثه یا رخداد امنیتی و پس از ثبت در پایگاه داده CERT، آن را به بخش تریاژ اطلاع می‌دهد.



شکل ۴- روال‌ها و جریانات کاری بخش‌ها در هنگام رویارویی با یک رخداد

بخش تریاژ، پس از دسته بندی، اولویت بندی و ثبت در پایگاه داده گزارشات حادثه، به مدیر CERT و بخش فنی تحلیل و ارزیابی، گزارش می‌دهد. بخش فنی با بررسی و مقایسه با حوادث پیش آمده قبلی، سعی در رفع آن می‌نماید. بخش فنی و ارزیابی مخاطرات در صورت پیدا کردن راه‌کار به بخش مهار حوادث اطلاع رسانی می‌کند در غیر این صورت به بخش هماهنگی پاسخ اطلاع می‌دهد. بخش هماهنگی پاسخ نیز از ماهر و دیگر CERT ها درخواست کمک می‌نماید و آن‌ها نیز پس از یافتن راه‌کار به بخش فنی اطلاع می‌دهند و پس از پیدا کردن راه‌کار، به بخش مهار حوادث اطلاع رسانی می‌شود. بخش مهار حوادث نیز به فناوری اطلاعات دستور مهار و ترمیم را اعلام می‌کند و به بخش هماهنگی پاسخ نیز اطلاع می‌دهد. بخش هماهنگی نیز به مدیر CERT اطلاع و گزارشی از برطرف شدن حادثه را می‌دهد. مدیر CERT، به بخش ردیابی، دستور پیدا کردن مهاجمین را می‌دهد. همچنین به بخش‌های تولید محتوا، حراست سازمان، توسعه پیکربندی و امنیت اطلاع داده می‌شود. طرح فوق به صورت آزمایشی با اجزای گروه CERT پیشنهادی، اجرا گردید و در مراحل مختلف با فرض اینکه میز پشتیبان وجود رخدادی را اعلام نموده است برای همه حالات، مشترک در نظر گرفته شد و با تغییر و جابجایی یا حذف قسمتی، زمان پاسخ‌گویی به

یک رخداد با یکدیگر مقایسه گردید که زمان پاسخ‌گویی طرح فوق نسبت به بقیه حالات و تغییرات اعمال شده، کمتر بود.

محاسن قابل ذکر در این الگو، نسبت به الگوهای دیگر مانند الگو میتروپولوس، عبارتند از:

۱- کارکنان میز امداد، از ارسال گزارش‌های مشکوک به مدیر CERT به صورت مستقیم خودداری می‌نمایند و گزارشات خود را به واحد تریاژ ارسال می‌نمایند. واحد تریاژ نیز گزارشات را از میز امداد، مرکز عملیات امنیتی، SIEM[1] و غیره دریافت نموده، با مراجعه به پایگاه داده در صورتی که این رخداد قبلاً در سامانه ثبت نشده باشد آن را به بخش تحلیل مخاطرات امنیتی ارجاع نموده، مدیر CERT را نیز در جریان حادثه قرار می‌دهد. در واقع، این الگوی حجم کاری را در زمان رخداد بین اعضای CERT تقسیم می‌نماید و باعث می‌شود مدیر CERT، فرصت بیشتری جهت تصمیم‌گیری و بهبود روابط بین اجزا داشته باشد.

۲- در این الگو، در حین رخداد به دلیل بالا بودن ریسک، از کارکنان سازمان برای برطرف کردن حوادث استفاده نمی‌شود و اصولاً نقشی برای آن‌ها در نظر گرفته نمی‌شود و محوریت اجرای مأموریت به نیروهای گروه واگذار شده است؛ ولی در الگوهایی مانند میتروپولوس برای کارکنان سازمان نیز وظایفی لحاظ شده است.

۳- در این الگو با ادغام مدیریت CSIRT[2] و مدیریت توانایی پاسخ‌گویی حوادث[3]، ضمن متمرکز نمودن CERT، باعث بهبود سرعت واکنش، کاهش زمان پاسخ‌گویی و افزایش انسجام و توانایی CERT به یک رخداد خواهد شد.

۹- نتیجه‌گیری

با توجه به اینکه CERT نسبت به گروه‌های امنیتی موجود در سازمان‌ها، تمرکز بیشتری در مدیریت و امکان پاسخ‌گویی سریع‌تری در برابر رخدادهای امنیتی دارد؛ لذا تاکید می‌شود از CERT برای پیش‌گیری از حملات نرم افزاری در شبکه‌های رایانه‌ای جهت پاسخ‌گویی سریع‌تر و مدیریت سرویس‌ها، به‌کارگیری شود. در این مقاله ضمن بررسی الگوهای مختلف پاسخ‌گویی CERT در دنیا و کمبود الگویی استاندارد در پاسخ‌گویی به رخداد، الگو جدیدی برای مراکز نظامی طراحی گردید. سپس الگوی سازمانی CERT مراکز نظامی، ساختار سازمانی پیشنهادی، سرویس‌های خدمات اصلی و تکمیلی و فرآیند نحوه برخورد با رخداد، ارایه گردید. لزوم به‌کارگیری واحد تریاژ و نقش کلیدی آن در جمع‌آوری اطلاعات از قسمت‌های مختلف

۱. Security Information Event Management

۲. omputer Security Incident Response Team

۳. Incident Response Capability

مانند میز پشتیبان، مرکز عملیات امنیتی و غیره، برای تسریع در پاسخ‌گویی به رخداد نقش بسزایی دارد. همچنین سازمان‌ها به اهمیت بالای امنیت در شبکه‌های رایانه‌ای خود پی برده‌اند لذا به سرعت در حال راه‌اندازی واحد CERT و واحد مرکز عملیات امنیتی[1] هستند. در تحقیقاتی که صورت گرفت بعضی از سازمان‌ها این دو واحد را مجزا از یکدیگر قرار می‌دهند و اعتقادی به ادغام آن‌ها تحت یک مرکز واحد ندارند؛ لذا با توجه به الگوی ارایه شده در پاسخ‌گویی پیشنهاد می‌شود CERT و مرکز عملیات امنیتی با یکدیگر ترکیب شده، به علت نیاز به مدیریت هوشمند توسط منابع انسانی، مرکز عملیات امنیتی به عنوان بازوی اجرایی در CERT قرار گیرد.

۱. security operation center (SOC)

کتابنامه

یزدان‌پناه، محمود (زمستان ۱۳۹۰)؛ ***شبیه‌سازی و پیاده‌سازی یک رمز جریانی خود هم‌زمان بومی (CPS۳) جهت امنیت در تبادل اطلاعات محرمانه***؛ فصلنامه علمی- ترویجی پدافند غیرعامل؛ شماره ۴

J. West-Brown, Moira. Stikvoort, Don. Kossakowski, Klaus-Peter. Audrey. Killcrece, Georgia. Ruefle, Robin. Zajicek, Mark(۲۰۰۷); "Handbook for Computer Security Incident Response Teams (CSIRTs)". CMU/SEI-۲۰۰۳-HB-۰۰۲. U.S: Software Engineering Institute, Carnegie Mellon University. CSIRTs. page.۲۹۱. Available at<http://www.sei.cmu.edu/reports/۰۳hb۰۰۲.pdf>,.

Software Engineering Institute(۲۰۰۵), Building CSIRT capabilies, carrnegi mellon university, Pittsburgh,PA۱۵۲۱۳,

Emmanuel S. Pilli, R.C. Joshi, Rajdeep Niyogi,(۲۰۱۰) ; "Network forensic frameworks: Survey and research challenges, *Digital Investigation"*, vol. ۷, pp- ۱۴-۲۷.

Keisuke kamata,(۲۰۰۷)., "Creating CSIRT", JPCERT/coordination center, japan

European network and information security agency (ENSIA)(۲۰۰۸); " A STEP- BY- STEP APPROACH ON HOW TO SET UP A CSIRT".

Sarandis Mitropoulos, Dimitrios Patsos, Christos Douligeris"(۲۳ September ۲۰۰۸); " On Incident Handling and Response; A state-of-the-art approach.

Georgia Killcrece(August ۲۰۰۴); "Steps for Creating National CSIRTs.", CERT® Coordination Center, Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University.

Penedo, David(Aug ۲۰۰۶); "Technical Infrastructure of a CSIRT". Cote d'Azur: *Internet Surveillance and Protection, ICISP '۰۶. International Conference, pp.* ۲۷ – ۳۲.

Available at < http://en.wikipedia.org/wiki/SQL_injection>(۱۲ Feb ۲۰۱۰).