بررسی شاخص های ارزیابی عملکرد مراکز گوهر

هانیه کارخانه، دانشجوی کارشناسی ارشد EMBA، دانشگاه علم و صنعت ایران، عضو پژوهشکده ICT شرکت ایزایران، h_karkhane@iust.ac.ir
(محمد فتحیان،عضو هیئت علمی دانشکده مهندسی صنایع دانشگاه علم و صنعت ایران، (fathian@iust.ac.ir

چکیده

امروزه یکی از نیازمندی‌های شناخته‌شده سازمان‌ها، تامین امنیت سیستم‌های اطلاعات می‌باشد. در واقع هر سازمانی نیازمند پاره‌ای اقدامات پیشگیرانه جهت جلوگیری از ورود و فعالیت هکرهای شبکه و نرم‌افزارهای مخرب می‌باشد. اما واقعیت این است که هرگز نمی توان جلوی ورود تمامی افراد و نرم افزارهای غیرمجاز و فعالیت آنها را به طور کامل گرفت. لذا سازمان‌ها علاوه بر اقدامات پیشگیرانه، نیازمند اتخاذ اقدامات واکنشی به منظور برخورد با ورود احتمالی این افراد و نرم‌افزارها می‌باشند. یکی از راه‌حل‌هایی که سازمان‌ها و شرکت‌های بزرگ به این منظور به کار می‌برند ایجاد گروه‌واکنش‌هماهنگ‌رخداد می‌باشد که با نام اختصاری گوهر از آنها یاد می‌شود. در این مقاله به مطالعه و بررسی فرآیندهای کاری گوهر و شاخصهای ارزیابی هر یک از این فرآیندها پرداخته می‌شود. بالا بودن کارآیی گوهر از نظر اقتصادی اهمیت فراوانی دارد زیرا از یک سو هزینه فرایندهای کاری را کاهش می‌دهد و از سوی دیگر با کوتاه کردن زمان از کار افتادگی سیستمها، هزینه‌های ناشی از آن را کاهش می‌دهد. در این مقاله در بخش شناسایی فرآیندها و معیارها از روش مطالعات کتابخانه‌ای و در جهت انتخاب شاخص‌های ارزیابی از روش تحقیق پیمایشی و پرسشنامه بهره برده‌ایم . ارزیابی پایایی و روایی پرسشنامه ها به روش بازآزمایی و آلفای کرونباخ انجام گرفته است.

کلید واژه ها: گروه واکنش هماهنگ رخداد۱ (گوهر)؛ ارزیابی عملکرد؛ فرایندهای کاری

1 Computer Security Incident Response Teams(CSIRT)

مقدمه

یک گوهر که معادل فارسی واژه CSIRT یا سرت سازمانی انتخاب گردیده است، یک سازمان خدماتی است که مسئول دریافت، مرور و پاسخگویی به گزارشات ارسالی و فعالیتهای مربوط به مشکلات و رویدادهای کامپیوتری است. سرویس های این سازمان معمولا برای محدوده مشخصی تعریف می شود که می تواند یک شرکت، اداره‌ی دولتی، سازمان آموزشی یا یک منطقه یا کشور باشد.[۱و۲]

سرویس های گوهر را می توان به ۳ دسته کلی تقسیم نمود: [۱و۳و۴]

- ✓ سرویس های واکنشی

این سرویس ها بوسیله یک رویداد یا یک درخواست، مانند گزارش به خطر افتادن یک میزبان، گسترش کدهای مخرب، آسیب پذیری نرم‌افزار یا موردی که توسط یک سیستم تشخیص نفوذ یا سیستم ثبت وقایع تشخیص داده شده است، فعال می شوند. سرویس های واکنشی مولفه اصلی کار گوهراست.

- ✓ سرویس های پیشگیرانه

این سرویس ها اطلاعاتی را فراهم می آورد که کمک به آماده سازی، محافظت و تامین ایمنی سیستمهای حوزه عمل در پیش بینی حملات، مشکلات و رویدادها می نماید. کارایی این سرویس ها مستقیماً تعداد حوادث را در آینده کاهش می دهد.

- ✓ سرویس های مدیریت کیفی امنیت

این سرویس ها تقویت کننده سرویس هایی است که درحال حاضر به خوبی بنا شده اند و مستقل از مدیریت رویدادها می باشند وبه صورت سنتی بوسیله قسمت های دیگر سازمان مانند بخش های فناوری اطلاعات، بازرسی یا آموزش، انجام می شوند.این سرویس ها عموماً پیشگیرانه اند اما غیر مستقیم به کاهش تعداد حوادث کمک می کنند. زیر سرویس های هر یک از این سرویس ها در تصویر شماره ۱ ذکر شده است.

تصویر شماره۱- سرویس‌های گوهر

ما در این مقاله بر آنیم تا معیارهایی را برای ارزیابی و اندازه گیری کارآیی تیمهای گوهراستخراج نماییم. این معیارها بر اساس تحقیقات پیمایشی حاصل شده است.

ساختار ادامه مقاله به این صورت است که بخش ۲ به بررسی کارهای مرتبط می پردازد، بخش ۳ به تشریح روش تحقیق اختصاص دارد، بخش ۴ نتایج به دست آمده را ارائه می نماید و بخش ۵ به جمع‌بندی و ارائه پیشنهاداتی برای کارهای آتی تخصیص داده شده است.

مروری بر ادبیات موضوع و کارهای مرتبط

بر پایه گزارشی از Killcrece و همکارانش در[۵] با استفاده از یک نظرسنجی در میان تعدادی از گوهرها، نشان دادند که گوهر ها میتوانند شامل چه سازماندهی، ساختار و فرآیندهایی شوند. این یک منبع با ارزش در شناسایی فرایندهای کاری در گوهرها بوده ، و نشان می‌دهد که بر اساس نوع فعالیت یک گوهرچه فرآیندهای کاری نیاز است.

West-Brown و همکارانش [۶] یک بررسی برروی عملکردها و وظایف مختلفی که یک گوهر داشته اند. و تحقیق آنها به عنوان راهنمایی برای کسانی است که تصمیم به راه اندازی یک تیم داشته‌اند، مناسب است . در این تحقیق بیان می کند بر اساس نیاز و قوانین سازمان نحوه استقرار، تنظیم کارکرد و وظایف یک

گوهرچگونه باشد. این سند در مورد وظایف و عملکرد گوهرها اطلاعات مهمی میدهد ، اما شرایط مورد استفاده در این سند لزوما مطابق با شرایط انجام توسط تیم در هنگام عمل نیست.

Wack [۷] لیستی از اعمال و وظایف یک گوهرهنگام رویارویی با حادثه را ارائه میکند ، اما در مورد دلایل وضرورت آنها هیچ توضیحی ارائه نمی‌دهد.در واقع این سند عمدتا به مبحث مدیریت فرآیندها و همچنین فرآیندهایی که برای ایجاد یک گوهر نیاز دارد پرداخته و هیچ نوع توضیحی در مورد عملکرد مستقیم بهنگام رسیدگی به حادثه ارائه نمی‌کند. این بدان معنی است که این سند برای بررسی و شناسایی فرایندهای کاری درهنگام رسیدگی به حوادث مناسب نبوده اما جهت بررسی فرایندها در حوزه مدیریت حادثه مناسب است.

در [۹] ، Schultz و Shumway یک راهنما ارایه کردند که به نحوه رسیدگی به حوادث به شکلی سازمان یافته در هر سازمان می پردازد. آنها از شرایط و عملکردهای بیشتری از فرآیندهای گوهردر مقایسه با موارد استفاده شده در [۵ ، ۶] را پوشش میدهند. فرآیندهای اصلی آنها آماده تر ، تشخیص پذیرتر و واکنش پذیر تر از موارد استفاده شده در[۵ ، ۶] میباشد. دربخش [۸] بر روی هر دو واقعه ی رسیدگی به حادثه و مدیریت حادثه متمرکز میشویم. استفاده از شرایط مختلف نیاز به این دارد که هر گوهر شرایط مورد استفاده در تیم را بدرستی توصیف کند. اگر هر تیم این کار را بدرستی انجام دهد پیداکردن روش ها و پروسه های مقایسه تیم های مختلف با هم راحت تر میشود.

شولتز [۹] ادعا می کند که یک گوهردر چهار مرحله تکامل می یابد: اولیه ، انتقال ، استقرار و پس از استقرار. او استدلال می کند که اکثر گوهرها در مرحله انتقال، در نهایت دریکسری حلقه ها گیر میکنند، زیرا آنها قادر به ارائه خدمات در یک وضعیت پایا و کاملا کارآمد نیستند و فقط اطلاعاتی که از منابع دیگر می آید را تکرار میکنند. او پیشنهاد تغییراتی جهت دریافت یک گوهرموثر را داد که بطور مداوم در حال بهبود امنیت در سازمان است. باید عواملی که باعث میشود یکگوهر در این حلقه نگه داشته شود و راه کارهایی که کمک میکند از این حلقه خارج شود را دقیقا شناسایی نماییم. این عوامل میتواند برای اندازه گیری محدوده تکامل گوهرکه توسط شولتز شرح داده شده مورد استفاده قرار میگیرند.

در [۱۰] Alberts و همکارانش فرآیندهای کاری را در یک گوهر به پنج فرآیند اصلی تقسیم کردند: آمادگی/ثبات/ بهبود مستمر، حفاظت از زیرساخت ، شناسایی ، ارزیابی و پاسخ. بعلاوه در این گزارش نشان میدهد که چه عملکردی برعهده کدام بخش از فرآیند قرار گرفته است.سند [۱۰] سهم مهمی برای شناسایی فرایندهای کاری دریک گوهردارد.

در [۱۱] ، لوکاس و مولر متدولوژی پاسخ به حادثه را در هفت مرحله توصیف می‌کنند. این مراحل شامل مراحلی همانند متدهای نویسنده های مختلف روی موضوعات بسیار مشابه و حتی استفاده از روشهای مختلف گفته شده در متدهای متفاوت نیز می باشد. نویسندگان در [۱۲] همچنین یک روش هفت مرحله ای را توصیف می‌کنند که از شرایط متفاوت تری در سازماندهی فعالیت ها استفاده می‌کنند کمی متفاوت تر از آنچه در [۱۱] اتفاق میفتد.

Pelkariو Chuvakin در [۱۳] یک روش شش مرحله ای را توضیح دادند. روش آنها مانند بسیاری از فعالیتهایی است که در روشهای دیگر شرح داده شده، اما برخی از فعالیت های جدید در آن گنجانده شده است.

رایت در [۱۴] به اهمیت سیاستهای پاسخ به حادثه پرداخته و چگونگی طراحی یک سیاست مفید را تشریح مینماید. بعلاوه، این مقاله مراحل لازم جهت ساخت پروسه پاسخ به رویداد را توصیف میکند. همچنین این مقاله،توصیفی درباره جزئیات مراحل مختلف ارائه نکرده و فقط یک نمای کلی از موارد نیازمندیها به ما میدهد.

Masurkar مجموعه ای از مقالات [۱۵و۱۶و۱۷و۱۸] را منتشر کرده است که به توصیف فرآیندهای ایجاد و روش اجرای گروه پاسخ به حادثه در یک تشکیلات می پردازد. در مقاله اول [۱۵] متمرکز بر ایجاد تیم پاسخ به حادثه و توسعه سیاستهای پاسخ به حادثه است. مقاله [۱۶] بر روند پاسخ به حادثه و فعالیت های مختلف موثردر پاسخ به حادثه میباشد. مقاله [۱۷] در یک بررسی کلی فعالیتهایی نظیر اقدامات قانونی ، به دست گرفتن منابع و تجربه ها می پردازد. آخرین مقاله [۱۸] بیشتر در عمق نحوه پردازش و تجزیه و تحلیل داده ای حادثه در میان مسائل دیگر پرداخته و بشکل قانونی آن را پوشش میدهد. این مقاله ها یک دید ارزشمند در چگونگی ایجاد و اجرای امنیت کامپیوتر توسط تیم پاسخ به حادثه به ما میدهد. همچنین جزئیات فنی بیشتری، در مورد استفاده از سخت افزار منطبق با سیستم عامل شرکت سان، مایکروسیستم و سولاریس و یا انواع سیستم عاملهای یونیکسی دیگر به ما خواهد داد.

در فریم ورک ارائه شده از دانشگاه DePaul [۱۹] پاسخ به حادثه، متمرکز بر روی استقرار"سطوح امنیتی" است. سطح امنیتی [۱۹] به معنای مقیاسی که توانایی طبقه بندی هر حادثه براساس شدت آن حادثه را بر عهده داردمشخص شده است. علاوه بر این، در این فریم ورک برخی از نقشهای موجود در این فرآیند تعریف شده و چگونگی تقسیم فرآیند پاسخ به حادثه در حالات متفاوت نیز توصیف شده است. اگرچه این اقدامات بشکل خلاصه شرح داده شده اند، اما یک رویکرد مفید را درباره نحوه ارائه یک پاسخ سازمان یافته به حادثه را نشان میدهد.

Payne در [۲۰] روش بدست آوردن معیارهای مناسب را توصیف کرده است. او ادعا میکند که یک معیارخاص و مطلوب، باید هوشمند نیز باشد: یعنی معین، قابل اندازه گیری، دسترس پذیر، قابل تکرار و زمان سنج باشد. سوانسون و همکارانش [۲۱] چگونگی توسعه معیارهای امنیت و روش استفاده بمنظور تسهیل تصمیم گیری و بهبود عملکرد و پاسخگویی برای خدمات امنیتی سازمان را توصیف کرده است. این سند اگرچه بطور کلی پروسه را برای کل سازمان تشریح میکند، اما میتوان از آن به عنوان یک راهنمای ارزشمند در توسعه معیارها برای هر گوهر استفاده نمود. با این حال ، نیاز است جهت استفاده از فرایندهای گوهرتکنیک ها نیز انطباق داده شوند.

Vaughn و همکارانش در [۲۲] پیشنهادی برای طبقه بندی معیارهای امنیت اطلاعات ارائه کرده اند.

Alsaker در [۲۳] لیستی از شاخص ها، برای امنیت اطلاعات منتشر کردند که توسط مرکز تعیین صلاحیت آی تی در خدمات بهداشت و درمان تروندهایم (KITH) استفاده شده است . همه این اسناد اطلاعاتی، یک پس زمینه مناسبی ارائه میکندکه بتوان درجهت توسعه معیارهای فرآیندهای کاری درگوهرهای مختلف استفاده نمود.

Wack [۷] پارامترهای مختلفی که میتوان برای اندازه گیری کارایی CSIRT ها بکار برد را تشریح می-کند. در این مقاله مشخص شده است که پیدا کردن یک مقیاس اندازه گیری مستقل جهت پیمایش کارایی یک گوهرمشکل است، اما تجزیه و تحلیل آماری اطلاعات جمع آوری شده از حوادث گوناگون، بدست آوردن یک روش جهت اندازه گیری عملکرد گوهررا قابل انجام دانسته است. بمنظور بهبود عملکرد گوهرباید فرآیندها عملکرد خوبی داشته باشند و بخشهایی که پتانسیل بهتر شدن را دارند شناخته شوند. یک ارزیابی دقیق می‌تواند اطلاعات خوبی درباره سازمان جهت بهبود عملکرد فرآیندها به ما بدهد. این اطلاعات میتواند از طریق مطالعه بر روی فرایندهایی که عملکرد خوبی در روند ارزیابی داشته اند بدست بیاید. در[۷] شناسایی پارامترهایی که می‌تواند برای اندازه گیری عملکردCSIRT مورد استفاده قرارگیرد صورت می‌گیرد ،اما باید پارامترهای بیشتری را جهت اندازه گیری دقیق‌تر و محک زنی انواع مختلف CSIRT ها شناسایی نمود.

Grance و همکارانش در [۲۴] یک راهنمای رسیدگی به رویداد ارائه داده اند که پارامترهایی متفاوتی را برای اندازه گیری داده های رویداد پیشنهاد میکنند و جوانب مثبت و منفی را در پارامترهای متفاوت مورد بحث قرار میدهند. با این حال ، تعداد پارامترهای ارائه شده خیلی کم بوده و پیدا کردن پارامترهای بیشتری که قابلیت اندازه گیری داشته باشند ضروری است.

Brownlee و Guttman در [۲۵] انتظاراتی که کاربران در حوزه کارکردی یک گوهرباید از آن تیم داشته باشند را تشریح می‌کند. می‌توان گفت که این تلاشها برای توصیف انتظارات کاربران از گوهردر نظر گرفته شده است، که خدماتی کاربران ازگوهر انتظار دارند را تعیین می‌کند. کیفیت خدمات انجام شده درهر حوزه نشانه ای از عملکرد تیم خواهد بود. از این امکان میتوان برای اندازه گیری کیفیت خدمات انجام شده توسط گوهر و همچنین یک شاخص مناسب جهت ارزیابی تیمها در برابر یکدیگر و پیدا کردن یک روش با ارزش برای مدیریت بر آنها استفاده نمود.

West-Brownو همکارانش در [۶] به این اشاره میکنند که یک سیستم تضمین کیفیت حتما نیاز بهگوهر داشته و یک چارچوب برای چنین سیستمی تعیین می‌کنند. همچنین نمونه هایی از پارامترهای مختلفی که می‌توانند نشانگرهای حاصل از اندازه گیری کیفیتCSIRT را پیمایش کرده را بررسی می-نمایند. در اغلب موارد نشانگر کیفیت همان شاخص عملکرد خواهد بود و پیشنهادات ذکرشده در این راهنما از آن بعنوان شاخص های عملکرد استفاده میکند. که البته به روز رسانی لیست شاخص‌ها همواره نیاز است.

روش تحقیق

جامعه آماری تحقیق مشتمل بر ۳۳ نفر از افراد شاغل در مرکز ماهر شرکت فناوری اطلاعات و همچنین متخصصین امنیت شرکت ایزایران می‌باشد. روش تحقیق از نوع پیمایشی[۲] و ابزار جمع آوری اطلاعات پرسشنامه بوده است سوالات پرسشنامه در این مقاله از نوع بسته پاسخ است. جدول دموگرافیک تحقیق در ذیل آورده شده است.

[۲] Survey study

جدول شماره ۱- جدول دموگرافیک نمونه آماری

دموگرافیک	دسته بندی	اعداد
تعداد افراد	----------	۳۳ نفر
جنسیت	مونث	63%
	مذکر	37%
تحصیلات	لیسانس	66%
	فوق لیسانس	39.6%
	دکترا	3.3%
میزان تجربه و سابقه کار	زیر ۵ سال	33%
	بین ۵- ۱۰ سال	39.6%
	بالای ۱۰ سال	36.3%

پاسخ سؤالات در پرسشنامه مورد استفاده در این مقاله در مقیاس لیکرت گروه بندی شده است و بدین وسیله به معیار های کمی تبدیل شده است. دو نوع پرسشنامه برای این تحقیق تهیه گردیده است پرسشنامه اول چهت وزندهی هر یک فرآیندهای اجرایی یک مرکز گوهر به روش AHP می باشد و پرسشنامه دوم جهت اخذ شاخصهای برتر هر یک از فرآیند تهیه شده است. جهت بررسی ضریب سازگاری قضاوت ها صورت گرفته نیز از محاسبه ضریب سازگاری استفاده شده است که برای آزمون صورت گرفته میزان این ضریب برابر ۰.۰۲۱ می باشد و کوچک بودن این عدد از ۰.۱ موکد سازگاری قضاوت‌ها می باشد.

جهت سنجش میزان پایایی آزمون از روش بازآزمایی استفاده شده است در این روش دو آزمون طی دو روز از جامعه نمونه (تیم های اعضای مرکز پدافندغیرعامل- ایزایران و تیم ماهر) به عمل آمده است محاسبات این بخش با روش اسپیرمن انجام گرفته است.خروجی محاسبات در SPSS نشان می دهد که با توجه به اینکه مقدار sig از 0.05 کوچکتر است دو آزمون همبستگی دارند و ضریب همبستگی برابرست با ۰.۹۷۱ می باشد .

همچنین جهت سنجش میزان روایی پرسشنامه ها از روش آلفای کرانباخ استفاده شده است. که میزان آلفای به دست آمده برابر با ۰/۸۸ که نشانگر روایی مناسب تحقیق می باشد و خطای حدی در این تحقیق ۰/۶٪ بدست آمده است.

یافته‌ها و نتایج

پرسشنامه ها بین جامعه نمونه که شامل ۳۳ نفر از افراد خبره حوزه تحقیق می باشد توزیع شده است زمان پر نمودن یک ساعت در نظرگرفته شده است و کلیه پرسشنامه ها همزمان به صورت گروهی پر شده اند. به ازای هر شاخص، میانگین نظرات محاسبه شده است .

روش وزن دهی به هر یک از ۵ مرحله با استفاده از روش AHP بوده است و نتایج نهایی در جدول شماره ۱ آمده است.

جدول شماره۲- نتایج بررسی اولویت فرآیندها

نوع فرآیند	آماده سازی	تشخیص	پاسخ	بازیابی	پیگیری
میانگین وزن از روش AHP	۰.۲۰۴	۰.۲۴۴	۰.۲۶۴	۰.۱۵۴	۰.۱۴۴

جدول بالا نشان دهنده این موضوع است که مراحل آماده سازی و تشخیص و پاسخ از دو مرحله انتهایی از اهمیت بیشتری در ارزیابی عملکرد گوهرها برخوردار می‌باشند و مهمترین بخش عملیات امداد و نجات رایانه ای بخش پاسخ با وزن ۰.۲۶۴ می باشد.

پس از محاسبه میانگین های نظرات هر پرسشنامه ، عدد حاصله را در وزن بدست آمده ضرب کرده ایم؛ جداول ذیل میزان هر شاخص (با اعمال وزن) را نشان می دهد.

جدول۳-بررسی شاخص ارزیابی فرآیندآماده سازی

فرآیند مربوطه	شاخص‌ها		نمره
آماده سازی[۲۹]	ردیف	شاخصهای ارزیابی	
	۱.	بررسی سیاست های سازمانی [۵]و[۶]	۱.۰۲
	۲.	ایجاد چک لیستهای نیازمندهای زمان بحران پیش از وقوع و بر اساس نیاز سازمان[۵]	۰.۸۸
	۳.	تعریف روالهای مورد نیاز بر اساس نیاز کار مثل تعریف روال گزارش‌دهی [۵]	۰۷۱
	۴.	ارزیابی امنیتی سازمان جهت آشنایی به وضعیت موجود[۶]	۰.۸۲
	۵.	راه اندازی سیکل بهبود امنیت[۲۶]	۰.۷۳
	۶.	استفاده از نرم افزار های trouble ticketing [۲۷]	۰.۵۵
	۷.	انتشار اطلاعات مربوط به امنیت[۲۹]	۰.۶۷
	۸.	آموزش جهت آشنایی کارکنان با نحوه عمل این تیم در سازمان [۲۹]	۰.۶۹

جدول۴-بررسی شاخص ارزیابی فرآیندتشخیص

فرآیند مربوطه	شاخص‌ها		
تشخیص[۲۹]	ردیف	شاخصهای ارزیابی	نمره
	۱.	وجود روال مناسب جهت پاسخ‌گویی[۶]	۱.۰۸
	۲.	زمان پاسخ‌گویی به رخداد [۶]	۰.۹۹
	۳.	روال مناسب ثبت رخداد[۶]	۰.۹۸
	۴.	روال مناسب مستندسازی رخدادهای پیش آمده[۶]	۰.۹۸
	۵.	میزان دانش افراد در تیم [۶]	۱.۱۵
	۶.	تعداد دوره‌های آموزش دیده شده افراد تیم [۶]	۱.۰۱
	۷.	وجود افراد با تخصص‌های خاص[۶]	۱.۱۷
	۸.	میزان سابقه کاری افراد متخصص در هر حوزه [۲۶]	۰.۹۴
	۹.	قابلیت به اشتراک گذاری اطلاعات و تجربیات پیشین [۲۶]	۰.۹۴
	۱۰.	میزان کارایی نرم‌افزارهای Incident Handling در [۲۷]	۰.۷۳
	۱۱.	میزان رسیدگی به رویداد شامل دریافت، مرتب کردن، دسته بندی کردن، اولویت بخشیدن به روخدادها [۲۹]	۰.۹۸
	۱۲.	سرعت طراحی روش ترمیم خرابی و تداوم کار[۲۹]	۰.۸۹

جدول۵-بررسی شاخص ارزیابی فرآیند پاسخ اولیه

فرآیند مربوطه	شاخص‌ها		
پاسخ[۲۹]	ردیف	شاخصهای ارزیابی	نمره
	۱.	تعریف استراتژی های دقیق پاسخ[۶]	۱.۱۷
	۲.	وجود رویه های مکتوبی جهت رسیدگی به اقسام مختلف رخدادها [۶]	۰.۹۴
	۳.	وجود بخش تریاژ [۶]	۰.۹۶
	۴.	وجود روال کاری مناسب برای بخش تریاژ[۶]	۱.۰۰
	۵.	وجود ارتباطات مکانیزه در بخش‌ها مختلف تیم[۶]	۰.۹۱
	۶.	مدیریت حادثه[۵]	۱.۲۳
	۷.	میزان پاسخ به درخواستها و گزارشات و تحلیل حوادث و رویداد ها[۲۹]	۱.۰۶
	۸.	میزان پاسخ به رویداد را از طریق تلفن یا ایمیل [۲۹]	۰.۹۶
	۹.	مدیریت آسیب پذیری[۳] [۲۹]	۱.۱۵

۳ مدیریت آسیب پذیری شامل دریافت اطلاعات و گزارشات در رابطه با آسیب پذیریهای سخت افزار و نرم افزار ، تحلیل ماهیتی، کارکردی و اثرات آسیب پذیریها و توسعه استراتژیهای پاسخ برای کشف و ترمیم آسیب پذیری ها

جدول۶-بررسی شاخص ارزیابی فرآیند بهبود و بازیابی

فرآیند مربوطه	شاخص‌ها		
بازیابی[۲۹]	ردیف	شاخصهای ارزیابی	نمره
	۱.	وجود استراتژی‌های بهبود و بازیابی[۶]	۰.۶۳
	۲.	وجود ابزارهای خودکار در بهبود وبازیابی(SOCوIDS) [۶]	۰.۶۳
	۳.	بررسی میزان زمان بهبود و ارزیابی[۶]	۰.۵۶
	۴.	درصد میزان رخدادهای مهار نشده [۶]	۰.۵۵
	۵.	مدیریت آثار باقی مانده [۲۹]	۰.۶۲
	۶.	تحلیل اثر باقی مانده حمله[۲۹]	۰.۵۹
	۷.	پاسخ اثر باقی مانده حمله[۲۹]	۰.۵۱
	۸.	مستند سازی در رابطه با بهترین روال های امنیتی رایج[۲۹]	۰.۵۲
	۹.	انتشار اطلاعات حمله یک نفوذگر، آسیب پذیریهای امنیتی، اعلام خطر نفوذ و ویروس کامپیوتری یا شوخی های فریب آمیز از طرق مختلف [۲۹]	۰.۵۵
	۱۰.	آرشیو اعلام خطرها، هشدارها و دیگر اعلان ها[۲۹]	۰.۵۵

جدول۷-بررسی شاخص ارزیابی فرآیند پیگیری

فرآیند مربوطه	شاخص‌ها		
پیگیری[۲۹]	ردیف	شاخصهای ارزیابی	نمره
	۱.	شناسایی آسیب پذیرهایی مورد سوء استفاده [۶]	۰.۶۱
	۲.	شناسایی روش جلوگیری از سوء استفاده [۶]	۰.۵۹
	۳.	میزان شناسایی افراد مهاجم[۶]	۰.۶۲
	۴.	شناسایی انگیزه افراد مهاجم [۶]	۰.۵۵
	۵.	زمان صرف شده از لحظه کشف یک رخداد تا لحظه براندازی آن[۶]	۰.۶۲
	۶.	راه اندازی سیکل بهبود امنیت[۹]	۰.۵۳
	۷.	فراهم کردن راه حل و استراتژی های کاهش خطر از طریق ارائه اصلاحیه یا اعلام خطر[۲۹]	۰.۵۵
	۸.	توسعه استراتژیهای دیگر پاسخ یا راه حل های جایگزین موقت[۲۹]	۰.۴۹

جهت محاسبه شاخص های برتر هر فرآیند میانگین اعداد بدست آمده محاسبه شده است و شاخص هایی که مقدار عددیشان از این مقدار بیشتر بوده است به عنوان شاخص برتر در نظر گرفته شده است .شاخص های برتر هر فرآیند به صورت ذیل می باشد:

جدول شماره۸ - شاخص‌های برتر فرآیندآماده سازی

فرآیند مربوطه	شاخص‌ها		
آماده سازی	ردیف	شاخصهای ارزیابی	نمره
	۱.	بررسی سیاست های سازمانی	۱.۰۲
	۲.	ایجاد چک لیستهای نیازمندهای زمان بحران پیش از وقوع و بر اساس نیاز سازمان	۰.۸۸
	۳.	ارزیابی امنیتی سازمان جهت آشنایی به وضعیت موجود	۰.۸۲

جدول۹- شاخص‌های برتر فرآیندتشخیص

فرآیند مربوطه	شاخص‌ها		
تشخیص	ردیف	شاخصهای ارزیابی	نمره
	۱.	وجود روال مناسب جهت پاسخ‌گویی	۱.۰۸
	۲.	میزان دانش افراد در تیم	۱.۱۵
	۳.	وجود افراد با تخصص‌های خاص	۱.۱۷

جدول شماره ۱۰- شاخص‌های برتر فرآیند پاسخ اولیه

فرآیند مربوطه	شاخص‌ها		
پاسخ	ردیف	شاخصهای ارزیابی	نمره
	۱.	تعریف استراتژی های دقیق پاسخ	۱.۱۷
	۲.	مدیریت حادثه	۱.۲۳
	۳.	میزان پاسخ به درخواستها و گزارشات و تحلیل حوادث و رویداد ها	۱.۰۶
	۴.	مدیریت آسیب پذیری	۱.۱۵

جدول شماره ۱۱- شاخص‌های برتر فرآیند بهبود و بازیابی

فرآیند مربوطه	شاخص‌ها		
بازیابی	ردیف	شاخصهای ارزیابی	نمره
	۱.	وجود استراتژی‌های بهبود و بازیابی	۰.۶۳
	۲.	وجود ابزارهای خودکار در بهبود وبازیابی(SOCوIDS)	۰.۶۳
	۳.	مدیریت آثار باقی مانده	۰.۶۲
	۴.	تحلیل اثر باقی مانده حمله	۰.۵۹

جدول شماره ۱۲- شاخص‌های برتر فرآیند پیگیری

فرآیند مربوطه	شاخص‌ها		
پیگیری	ردیف	شاخصهای ارزیابی	نمره
	۱.	شناسایی آسیب پذیرهایی مورد سوء استفاده	۰.۶۱
	۲.	شناسایی روش جلوگیری از سوء استفاده	۰.۵۹
	۳.	میزان شناسایی افراد مهاجم	۰.۶۲
	۴.	زمان صرف شده از لحظه کشف یک رخداد تا لحظه براندازی آن	۰.۶۲

جمع بندی

موضوع مورد مطالعه در این تحقیق ارائه مدلی جهت ارزیابی مراکز گوهر می‌باشد. با انجام مطالعات کارهای مرتبط با موضوع مقاله، فرآیندهای کاری یک گوهر، به ۵ مرحله تقسیم شده است که این ۵ مرحله عبارتند از :آماده سازی، تشخیص، پاسخ، ارزیابی و پیگیری می باشد که تحلیل‌های آماری نشان داده است مهمترین فرآیند کاری تیم گوهر بخش پاسخگویی به رخداد می‌باشد که مهمترین شاخصهای ارزیابی این فرآیند عبارتست از ۱- تعریف استراتژی های دقیق پاسخ ۲- مدیریت حادثه ۳- میزان پاسخ به درخواستها و گزارشات و تحلیل حوادث و رویداد ها ۴- مدیریت آسیب پذیری می باشد که شاخصهای دیگر هر فرآیند در جدول بخش ۴ شماره ۸و۹و۱۰و۱۱و۱۲ آورده شده است جهت تحلیل روایی و پایایی پرسشنامه های آزمون از آلفای کرونباخ و باز آزمایی استفاده شده است .

میزان آلفای به دست آمده برابر با ۰/۸۸ که نشانگر روایی مناسب تحقیق می باشد و خطای حدی در این تحقیق ۰/۶٪ بدست آمده است و همچنین میزان ضریب همبستگی بین دو آزمون برابرست با ۰.۹۷۱ است که این نمره موکد همبستگی بین دو آزمون و میزان پایایی می باشد.

منابع

[1] “State of the Practice of Computer Security Incident Response Teams (CSIRTs)” (October 2003),Technical Report, Carnegie Mellon Software Engineer Institute,.
[2] “Organizational Models for Computer Security Incident Response Teams (CSIRTs)” (December 2003) Handbook, Carnegie Mellon Software Engineer Institute.
[3] “Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd Edition” (April 2003), Mellon Software Engineer Institute.
[4] “RFC 2350: Expectations for Computer Security Incident Response” , June 1998.
[5] Killcrece et al: State of the Practice of Computer Incident Response Teams (CSIRTs), (2003), Technical Report CMU/SEI-2003-TR-001, Pittsburgh,Pennsylvania, Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University.

[6]"Handbook for Computer Security Incident Response Teams (CSIRTs) 2nd edition" (2003), Handbook CMU/SEI-2003-HB-002, Pittsburgh Pennsylvania, Networked Systems Survivability Program,Software Engineering Institute, Carnegie Mellon University.
[7] Wack : Establishing a Computer Security Incident Response Capability (CSIRC) (1991) , NIST Special Publication 800-3, Computer Systems Laboratory, National Institute of Standards and Technology (NIST).
[8] Schultz & Shumway (2002), Incident Response, A strategic guide to handling system and network security breaches, New Riders, Boston, Indiana, USA, ISBN 1578702569.
[9] Schultz (2004), Incident response teams need to change, Computers &Security, 23(2) s87-88.
[10] Alberts (2004), Defining Incident Management Processes for CSIRTs: A work in progress, Technical Report CMU/SEI-2004-TR-015,Pittsburgh Pennsylvania, Networked Systems Survivability Program,Software Engineering Institute, Carnegie Mellon University.
[11] Lucas & Moeller (2004), The Effective Incident Response Team, Addison-Wesley, ISBN 0201761750.
[12] Mandia & Prosise (2003), Incident Response & Computer Forensics 2nd ed., McGraw-Hill/Osborne, ISBN 007222696X.
[13] Peikari & Chuvakin(2004), Security Warrior, O'Reilly & Associates, ISBN 0596005458.
[14] Wright : How to Design a Useful Incident Response Policy, http://www.securityfocus.com/printable/infocus/1247,
[15] Marsukar (2003), Responding to a Customer's Security Incidents – Part 1: Establishing Teams and a Policy, Sun Microsystems, Sun BluePrints OnLine, www.sun.com/blueprints/0303/817-1795.pdf.
[16] Marsukar(2003),Responding to a Customer's Security Incidents – Part 2: Executing a Policy, Sun Microsystems, Sun BluePrints OnLine, http://www.sun.com/blueprints/0403/817-1796.pdf,
[17] Marsukar(2003), Responding to a Customer's Security Incidents – Part 3: Executing a Policy, Sun Microsystems, Sun BluePrints OnLine, http://www.sun.com/blueprints/0903/817-3733.pdf, last updated Sept 2003
[18] Marsukar(2003), Responding to a Customer's Security Incidents – Part 4: Executing a Policy, Sun Microsystems, Sun BluePrints OnLine, http://www.sun.com/blueprints/1003/817-4002.pdf, last updated Oct 2003
[19] DePaul University (2002), A Framework for Incident Response, Information Security Team, DePaul University, Chicago, Illinois.
[20] Payne (2001), A Guide to Security Metrics, SANS Security Essentials GSEC Practical Assignment.
[21] Swanson (2003), Security Metrics Guide for Information Technology Systems, NIST Special Publication 800-55, Computer Security Division, National Institute of Standards and Technology (NIST).
[22] Vaughn et al : Information Assurance Measures and Metrics, State of practice and proposed taxonomy, Mississippi State University,2001.
[23] Alsaker (2004), Indikatorer for informasjonssikkerhet, Trondheim, Kompetansesenter for IT i helsesektoren (KITH), KITH rapport 08/04,ISBN 82-7824-225-9, http://www.kith.no/vedlegg/19224/R08-04_Indikatorer_ informasjonssikkerhet.pdf.
[24] Grance (2004), Computer Security Incident Handling Guide, NIST Special Publication 800-61, Computer Security Division, National Institute of Standards and Technology (NIST).

[25] Brownlee, Guttman (1998), Request For Comments 2350, Expectations for Computer Security Incident Response, http://www.ietf.org/rfc/rfc2350.txt.
[26] Pethia & van Wyk (1999), Computer Emergency Response – An international problem, Austin, Texas, Proceedings of the 13th international conference on Software engineering.
[27] Fogle (2003), The Benchmarking Process; One Team's Experience,IEEE Software, September/October, pp. 40-47.
[28] Hansman (2003), A Taxonomy of Network and Computer Attack methodologies, Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, New Zealand.
[29] Marie & Büyüközkan (1997), Methods and Tools for First Five Steps of Benchmarking Process, Innovation in Technology Management - The Key to Global Leadership, Portland International Conference on Management and Technology (PICMET '97), Portland, Oregon, USA.