باسمه تعالی

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

روش اجرایی

پاسخگویی به رخدادهای رایانه ایی در مرکز ماهر

وزارت ارتباطات و فناوری اطلاعات سازمان فناوری اطلاعات ایران	**روش اجرایی** **مرکز ماهر**	کد: ITC-PR-MAHER-۹۱۰۲۱۶-RW۰۰

فهرست تغییرات ثبت شده در سند				
نسخه	تاریخ	مجوز تغییرات	تغییردهنده	علت انجام تغییرات و بخش های تغییریافته

تأییدیه سند					
	نام و نام خانوادگی	مسئولیت	زیرسیستم	امضا	تاریخ
تهیه کننده	امین گلستانی	کارشناس			
بازنگری کننده					
تأیید کننده اول	اسماعیل رادکانی	معاون گسترش فناوری اطلاعات ایران			
تأیید کننده دوم	مهران شیرازی	مشاور و نماینده رئیس سازمان در سیستم مدیریت کیفیت			
تصویب کننده	علی حکیم جوادی	معاون وزیر و رئیس سازمان فناوری اطلاعات ایران			
این سند در تاریخ ..... به واحدهای ذی ربط ابلاغ و اجرایی شد. گروه نوسازی و تحول اداری مهر و امضاء					

فهرست مطالب

۱ هدف

گرد آوری و تحلیل کدهای مخرب به منظور مقابله با حملات سایبری و همچنین آسیب شناسی و امداد رایانه ایی

۲ دامنه کاربرد

پاسخگویی و هماهنگی عملیات رخدادهای رایانه ایی در سطح کشور برای کلیه زیرشبکه های حساس اعم از دولتی و خصوصی

۳ – اصطلاحات و تعاریف

- کدهای مخرب: بدافزارها و تمامی برنامههای مخربی که می توانند موجب ایجاد اخلال در کاردکرد عادی سیستم شوند
- سنسور و حسگر: منظور تله های نرم افزاری و سخت افزاری است که قابلیت شناسایی و بدام اندازی کدهای مخرب را دارند
- RFP: درخواست ارائه پیشنهاد Request for Proposal
- حمله: هرگونه مراجعه بدون مجوز به بخش خاصی از اطلاعات حمله قلمداد می گردد
- سامانه / پورتال : کانال ارتباطی با سطوح دسترسی متفاوت برای دسترسی به یک پایگاه داده منسجم و طبقه بندی شده.

۴–شناسنامه

تصویر ذیل (کپی پیوست)

شناسنامه خدمت مرکز ماهر

تبصره ۳	صفحه ۱ از ۱

عنوان	شرح
دام دستگاه ارائه خدمت	سازمان فناوری اطلاعات ایران
شرح و تعریف مختصری در راستای معرفی خدمت	مرکز ماهر مسئول در سازمان فناوری اطلاعات ایران ارائه دهنده خدمات به منظور ایجاد ساختار مناسب جهت پاسخگویی، ایجاد هماهنگی‌های لازم و صدور راهنماهای رایانه‌ای و برقراری ارتباط با سایر مراکز و گروه‌های امنیتی در سطح سازمان‌ها، شرکت‌ها و موسسات می‌باشد.
دستگاه یا سایر دستگاههای تعامل	تمام سازمان‌ها، نهادها و شرکت‌های دولتی و اختصاصی
قوانین و مقررات مرتبط با خدمت	ماده واحده اصلاحیه قانون ارتباطات (اقدام چهارم در راهبرد دوم و اساسنامه شرکت فناوری اطلاعات ایران) مصوب خدمات فوریتی مورخ ۸۷/۱۲/۲۷ بند ۱۵ و ۱۹ از ماده ۲
مدت زمان انجام خدمت	زمان پاسخ به رخداد و برطرف سازی به نوع و پیچیدگی رخداد و برطرف سازی متغیر می‌باشد. راه‌اندازی گروهای صدا و زمان نصب و راه‌اندازی یک دستگاه "آلفی نت" ۷ روز از زمان درخواست در نظر گرفته شده است.
هزینه های ارائه خدمت	-
مدارک لازم برای دریافت خدمت	-
نحوه دسترسی برای دریافت خدمت	از طریق ارتباط با مرکز ماهر و تماس با شماره تلفن‌های ۲۳۱۱۵۹۵۰-۲۳۱۱۵۹۵۱ و یا از طریق دسترسی به سایت http://www.certcc.ir

ورودی های فرایند خدمت	خروجی های فرایند خدمت
• اعلام رخدادهای امنیتی در فضای اینترنت توسط سازمان‌ها و شرکت‌ها • همکاری با مرکز ماهر از طریق نصب دستگاه "آلفی نت"	○ هماهنگی و اطلاع‌رسانی به منظور رفع یا جلوگیری از انتشار و تکرار رخداد و یا راه‌اندازی سامانه ○ آشنایی با مرکز ماهر ○ توسعه شبکه "آلفی نت" (همکاری) ○ راه‌اندازی و ایجاد ارتباط با سایر گروه‌های یا آلفی نت‌های هماهنگ رخدادگریز

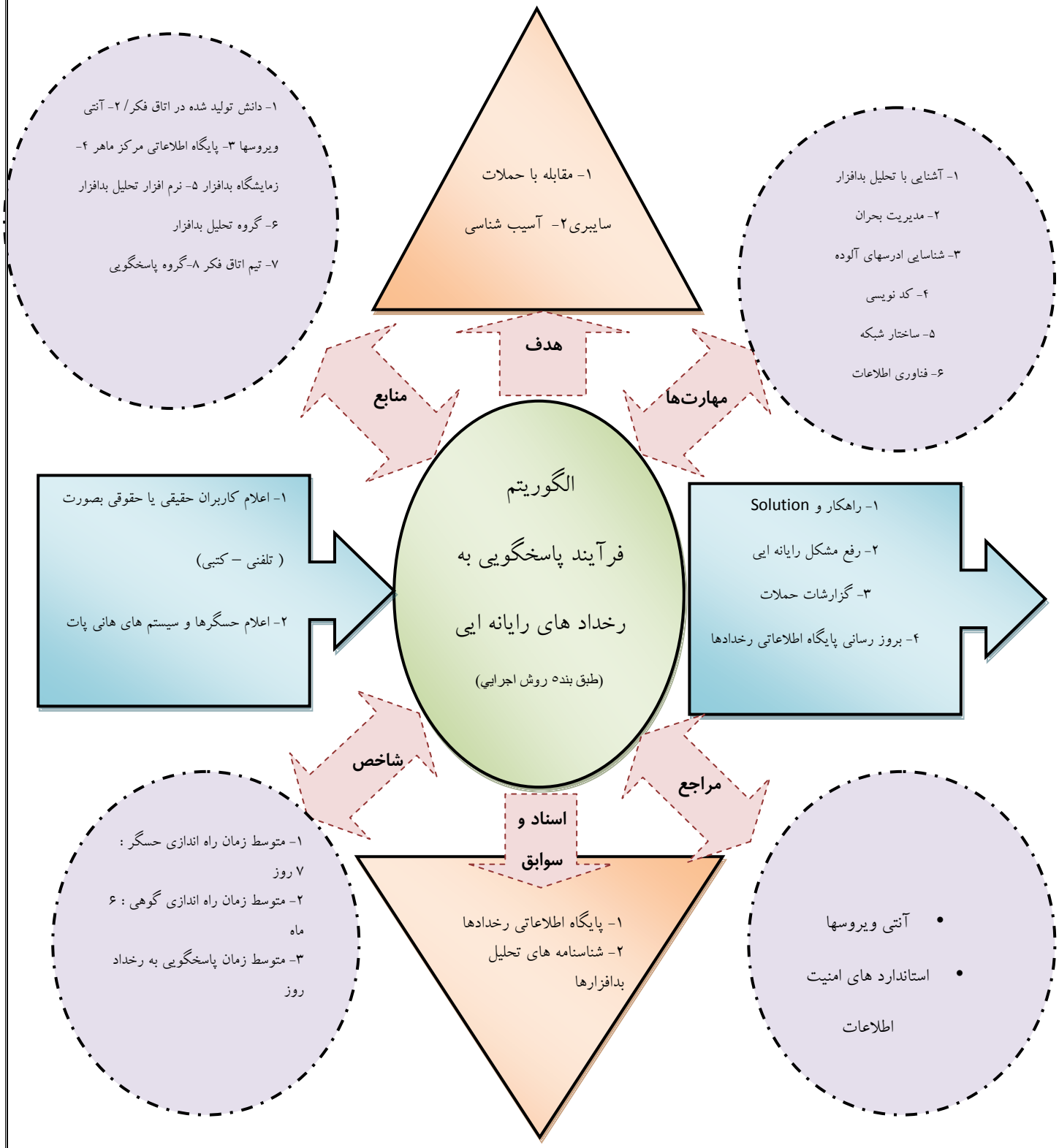
ردیف	شاخص‌های ارزیابی فرایند	ضرایب اهمیت	نحوه سنجش	امتیاز دارد	زمان سنجش
۱	برطرف‌های واصله	۲	تعداد	-	ماهانه
۲	پاسخ به رخداد	۴	تعداد	-	ماهانه
۳	راه‌اندازی همکارها	۳	تعداد	-	ماهانه
۴	عملکرد راه‌اندازی مراکز کوچک	۱	تعداد	-	ماهانه
۵	متوسط زمان راه‌اندازی همکارها	۳	روز	۷	ماهانه
۶	متوسط زمان راه‌اندازی مرکز کوچک	۱	ماه	۶	ماهانه

شرح کلی و مسئولیت‌ها / فرایند اجرایی:

۱) با توجه به اعلام رخداد امنیتی از طرف سازمان‌ها و یا شرکت‌ها به مرکز ماهر پاسخگویی به رخداد آغاز می‌گردد.
۲) شبکه "آلفی نت" به اعضای "آلفی نت"های عرام راه‌اندازی می‌گردد.
۳) پس از جمع‌آوری داده‌های "آلفی نت"ها اقدام به تجزیه و تحلیل داده‌های گردآوری شده و آشنایی برطرف‌ها صورت می‌پذیرد.
۴) راه‌اندازی و برقراری ارتباط با سایر گروهها و طراحانی توان عضویتی مرکز ماهر بعنوان مرکز هماهنگ‌کننده طی انجام می‌گیرد.

- جزء مسئول فعالیت‌ها مرکز ماهر و کارکنان آن مرکز بوده که داده مذکور سازمانی مرکز ماهر در دست تدوین می‌باشد.

وزارت ارتباطات و فناوری اطلاعات سازمان فناوری اطلاعات ایران	**روش اجرایی** **مرکز ماهر**	کد: ITC-PR-MAHER-۹۱۰۲۱۶-RW۰۰



۴ – مسئولیت‌ها

مدیران کلیه واحدهای مرکز در انجام هماهنگی های لارم و اقدامات مقتضی در رفع یک رخداد ، حسب وظایف محوله بطور رسمی مسئول و پاسخگو می باشند.

وزارت ارتباطات و فناوری اطلاعات سازمان فناوری اطلاعات ایران	**روش اجرایی** **مرکز ماهر**	کد: ITC-PR-MAHER-۹۱۰۲۱۶-RW۰۰

روش‌اجرایی

شماره فرایندها

۱

اعلام رخداد توسط کاربران حقیقی یا حقوقی

اعلام حسگرها و سیستم های هانی پات

۲

فیلترینگ

۳

اولویت بندی

۴

جستجو در پایگاه اطلاعاتی و رصد واحدی

۵

تحلیل تخصصی و آزمایشگاهی

۶

مشاوره

۷

تائید

بهنگام سازی آرشیو و توسعه سنسورهای، حسگرها و سامانه گردآوری کننده بدافزار یا سایر ابزارها

پاسخ و رفع رخداد

RFP

مطالعه و مشاوره RFP

تنظیم شرح خدمات

تائید و ارسال شرح خدمات به معاونت مالی اداری

اصلاح و تکمیل و عودت شرح خدمات

ابلاغ قرارداد به پیمانکار

نظارت بر عملکرد

۸ تعریف پروژه

تهیه گزارشات عملکرد

پیمانکار

فرایند ۱:

اعلام رخداد توسط کاربران حقیقی یا حقوقی

اعلام حسگرها و سیستم های هانی پات

جمع آوری و ورود اطلاعات اولیه

از طریق ارسال نامه

از طریق اعلام تلفنی

از طریق اعلام سنسورها و حسگرهای نصب شده در زیرشبکه استانهای کشور

فرایند۲ : فیلترینگ

فیلتر نمودن کلیه ورودی ها و خارج نمودن درخواست های کاذب از طریق اجرای فرایند احراز هویت ، تکمیل نمودن فرم مخصوص پاسخگویی به رخداد و ثبت رخداد.

فرایند۳: اولویت بندی

تعیین اولویت پاسخگویی به رخدادها بر اساس ضریب اهمیت تعیین شده

فرایند ۴: جستجو در پایگاه اطلاعاتی و رصد واحدی

بررسی پایگاه اطلاعاتی به منظور مشخص شدن تکراری بودن درخواست ، در صورت تکراری بودن اطلاعات نهایی موجود در پایگاه اطلاعاتی بعنوان راهکار به متقاضی ارائه می گردد

الف: رصد آسیب پذیریهای حوزه افتا

۱ - دریافت گزارش اولیه جدیدترین آسیب پذیریها و تهدیدات رایانه ای از منابع معتبر امنیتی داخلی یا خارجی

۲ - بررسی میزان ارتباط و صحت اطلاعات رخداد با سازمانهای مخاطب کشور

۳ - انتخاب گزارشات با اهمیت بیشتر (بر حسب شدت آسیب پذیری و سطح حساسیت سازمانهای مخاطب) جهت تحلیل و ارائه راهکار

۴ - تحلیل گزارشات مربوط به اسیب پذیری ها و تهدیدات

۵ - تهیه و ارائه گزارشات تحلیل و ابزار تهیه راهکارها

۶ - صحت سنجی و تکمیل راهکارهای ارائه شده

۷ - تعیین مخاطبین سازمانی رخداد شناسایی شده

۸ - تهیه مکاتبات محرمانه مربوط به رخداد و راهکارهای مربوطه

۹ - تایید محتوای مکاتبات مربوط به رخداد و راهکارهای مربوطه توسط مدیر مرکز

۱۰ پاسخگویی به سوالات و ابهامات ارسال شده از گروه پاسخگویی نسبت به سازمانها در خصوص محتوای گزارشات تکمیلی

۱۱ درج اتمام هشدار

ب: تحلیل تهدیدات

۱ - دریافت گزارش مربوط به رخدادهای به وقوع پیوسته در سطح کشور از گزارش مراجع امنیتی بین المللی و یا مراجع اطلاعاتی داخلی

۲ - دریافت اطلاعات تکمیلی از مراکز یا سازمانهای هدف با هماهنگی مراجع اطلاعاتی کشور

۳ - تحلیل و صحت سنجی وقوع رخداد با استفاده از گردآوری اطلاعات تکمیلی از مراکز همکار، آپا و سازمانهای هدف و ...

۴ - ارجاع رخداد جهت تحلیل دقیق و فنی به مراکز آپا با توجه به حوزه فعالیت و تعیین اولویت زمانی

۵ - بررسی خروجی ها و تایید نتایج

۶ - تعیین احتمال متاثر بودن سازمانها و نهادهای حیاتی و حساس کشور با توجه به نوع رخداد

۷ - آماده سازی زیرساخت ارتباطی سریع با نمایندگان سازمانها

۸ - ارائه نتایج تحلیل اولیه مرکز به سازمانهای هدف و راهکارهای مقابله و کاهش پیامد

۹ - دریافت و جمع آوری خروجی ها و نتایج اعمال راهکارها در سازمانها

۱۰ بررسی و تحلیل مجدد اطلاعات کسب شده به منظور پوشش کامل رخداد و ارائه راهکارهای پاکسازی قطعی با همکاری مراکز اپا

۱۱ پاسخگویی به سوالات و ابهامات مطرح شده در خصوص راهکارها و گزارشات ارائه شده به سازمانهای هدف

ج: تدوین بولتن

۱ - دریافت اخبار امنیتی به روز در خصوص رخدادهای گزارش شده در سطح بین المللی

۲ - بررسی اخبار مرتبط با دارایی های اطلاعاتی کشور و یا با سطح ریسک بالا

۳ - تحلیل اخبار مرتبط در حوزه افتا

۴ - بررسی تحلیل ها و گزارشات تهیه شده در حوزه اخبار افتا

۵ - تدوین و ویرایش بولتن خبری در خصوص حوزه اخبار افتا

۶ - تایید محتوای بولتن خبری توسط مدیر مرکز

۱۲ تعیین مخاطبین سازمانی رخداد شناسایی شده

۷ - تهیه مکاتبات محرمانه مربوط به رخداد و راهکارهای مربوطه

د: پاسخگویی

۱ - ارسال مورد پاسخگویی از گروه پاسخگویی

۲ - تحلیل و بررسی مشکل ارسال شده با توجه به الویت زمانی آن

۳ - تدوین اطلاعات تکمیلی درخواستی از سازمان جهت تحلیل بیشتر مشکل و ارائه به مسئول گروه پاسخگویی

۴ - تحلیل بیشتر مشکل مورد بحث با توجه به دریافت اطلاعات تکمیلی

۵ - ارجاع مشکل جهت تحلیل دقیق تر به مراکز آپا (در صورت لزوم)

۶ - ارائه راهکارها و پیشنهادات جهت رفع مشکل به گروه پاسخگویی

و: توصیه نامه

۱. بررسی منابع مطالعاتی در حوزه افتا به منظور استخراج موضوعات و مفاهیم کلیدی و پایه این حوزه

۲. انتخاب موضوع دارای اهمیت بالا در حوزه افتا برای مخاطبین عام
۳. بررسی و جستجوی روشها و راهکارهای تکمیلی در خصوص پوشش آسیب پذیریهای امنیتی
۴. بیان و تبدیل راهکارهای فنی و تخصصی در سطح کاربران عام
۵. تهیه و تدوین توصیه نامه امنیتی در خصوص مشکلات کاربران و راهکارهای پوشش آنها
۶. تایید محتوای توصیه نامه امنیتی
۷. ارسال توصیه نامه امنیتی در سطح سازمان، وزارت و زیر ساخت

فرایند ۵: تحلیل رخداد و آزمایشگاهی

درصورت بروز حمله تیم امداد اقدام به بررسی موضوع می نماید این بررسی می تواند از طریق کنترل IP های مهاجم یا رهگیری مهاجم از طریق شرکتهای میزبانی کننده شبکه صورت پذیرد درصورتیکه فایل بدافزار در اختیار باشد تیم تحلیل بدافزار اقدام به کدخوانی یا رمزگشایی می کند و با تهیه شناسنامه فنی بدافزار آنرا مورد پایش و بررسی قرار می دهند

الف: شناسایی تهدیدات جدید ناشی از انتشار بدافزارها و کدهای مخرب

۱۳ دریافت نمونه از شبکه هانی نت ملی
۱۴ دریافت نمونه از طریق وبسایت مرکز
۱۵ نمونه برداری از سطح سازمانها و فضای سایبری کشور
۱۶ دریافت نمونه بدافزارها و کدهای مخرب از طرق ارتباطی مختلف
۱۷ تحلیل نمونه های دریافتی و ارزیابی سطح تهدیدات آنها
۱۸ تهیه گزارش از موارد با اهمیت
۱۹ اطلاع به مراجع بالادست

ب: جمع آوری و ذخیره سازی جدیدترین بدافزارهای گسترش یافته

۱ - جمع آوری نمونه ها از طریق اشتراک در سرویس های بین المللی

۲ - جمع آوری نمونه ها از طریق مراوده با گروه های فعال در زمینه بدافزار در داخل و خارج کشور

۳ - تهیه و توسعه ابزار های شناسایی سریع گونه های تهدید کننده

۴ - ذخیره سازی نمونه ها در بانک اطلاعات بدافزار

۵ - ارسال مدیریت شده نمونه ها به تولید کنندگان آنتی ویروس داخلی و مراکز تحقیقاتی

ج: پیگیری اخبار حوزه بدافزارها از منابع مختلف رسمی و غیر رسمی جهت آگاهی سریع از رویدادها

۸ - پیگیری جدیدترین اخبار منتشر شده توسط شرکت های فعال در حوزه بدافزار

۹ - تماس مستقیم با متخصصین داخلی و خارجی برای دستیابی به اخباری که منتشر نشده و یا هرگز منتشر نخواهند شد.

۱۰ عضویت در گروه های تخصصی این حوزه جهت دریافت آخرین اخبار و اطلاعات

۱۱ تهیه گزارش از مهمترین اخبار

۱۲ ارائه موارد با اهمیت به مراجع بالادست

د: ارائه گزارش جهت ایجاد آمادگی و مقابله با رویدادها

۷ - ارائه گزارش در خصوص عملکرد بدافزارهای ناشناس جمع آوری شده توسط هانی پات

۸ - ارائه گزارش در خصوص تهدیدات امنیتی با ریسک زیاد

۹ - ارائه گزارش در خصوص مهمترین تهدیدات امنیتی به وجود آمده

ه: ارائه ابزار و راهکار مقابله با تهدیدات واقع شده

۱ - تشخیص و تفکیک رویداد های خاص با اهمیت بالا

۲ - تهیه دستورالعمل مقابله و ارائه گزارش مربوطه

۳ - ارائه ابزار مناسب جهت شناسایی و پاکسازی

۴ - ارسال ابزار و راهنمای استفاده به سازمانها و انتشار عمومی آن در صورت نیاز

فرایند ۶: مشاوره

درصورتیکه از طریق دانش موجود نتوان به ماهیت حمله با بدافزار پی برد از طریق تشکیل اتاق فکر و یا دعوت مشاوران متخصص برای حمله بوجود آمده تدبیری اتخاذ می گردد که البته برای هرنوع حمله تدبیری خاص و منحصر به فرد لازم است.

فرایند ۷: تائید

پس از یافتن راهکار مناسب، اخذ تائید اجرا و مصوب نمودن راهکار جهت اعلام ضروری است

فرایند ۸: بروز رسانی آرشیو و توسعه سنسورهای، حسگرها و سامانه گردآوری کننده بدافزار یا سایرابزارها

پس از اخذ مجوز اعلام نتیجه، خروجی را به اولویت بندی شده و با رعایت اولویت در اختیار گروه پاسخگویی به رخداد قرار می گیرد.

الف: شناسایی زیر شبکه های حساس ملی

۲۰ دریافت اطلاعات اولیه از خارج از تیم

۱ ۱ دریافت وضعیت از سازمانها

۱ ۲ دریافت وضعیت از تیم های داخلی مرکز ماهر

۱ ۳ شناسایی زیرشبکه بصورت تصادفی

۲۱ تعیین اولویت و فیلترینگ درخواست وارده

۲۲ بررسی و امکان سنجی زیرشبکه سازمان اعلام شده بصورت غیرحضوری

ب: اقدام برای ارتقاء سطح امنیتی زیرشبکه

۱۲ هماهنگی با مسئولین شبکه سازمان ها یا حراست‌های IT سازمانها

۱۳ امکان سنجی نصب حسگر و سنسورهای گردآوری کننده بدافزار بصورت حضوری در صورت نیاز

۱۴ مشاوره و راهنمایی به مدیرشبکه سازمان متقاضی جهت رفع موانع نصب حسگر و سنسورها

۱۵ انجام مکاتبه با مدیر فناوری اطلاعات سازمان متقاضی و درخواست مشخصات فنی

۱۶ انجام هماهنگی و مشاوره جهت ارائه توضیحات فنی توجیهی – تشریحی

۱۷ دریافت پاسخ و مشخصات فنی مورد نیاز از سازمان متقاضی

۱۸ تنظیم برنامه زمانبندی با توجه به منابع سخت افزاری و تجهیزات سخت افزاری

۱۹ هماهنگی و درخواست مجوز ورود به سازمان متقاضی

۲۰ ارجاع و صدور دستور کار به نصاب حسگر یا سنسورهای هانی پات

۲۱ تحویل سرور به نصاب

۲۲ پیکربندی نرم افزارها بر سرور

۲۳ هماهنگی نصاب با مسئول شبکه سازمان مربوطه

۲۴ مراجعه حضوری نصاب جهت نصب حسگر و سنسور

۲۵ اجرای فرایند نصب

۲۶ اجرای فرایند لینک به پورتال ملی هانی نت

۲۷ نظارت بر دریافت برخورد توسط کارشناسان ماهر

۲۸ تائید صحت عملکرد سنسور یا حسگر منصوبه

۲۹ تکمیل صورتجلسه تحویل سخت افزار توسط سازمان متقاضی

۳۰ اعلام محل نصب و مشخصات کامل سنسور به سازمان

۳۱ صدور نام کاربری و رمز عبور برای متقاضی بصورت محرمانه

۳۲ تکمیل و تائید فرم های آزمایش و تحویل

ج: پایش و مانیتورینگ سطح کیفی عملکرد سنسورها

۱۳ تهیه گزارش هفتگی ثبت برخورد

۱۴ بررسی علل عدم کاربری برخی ماشین های مجازی

۱۵ انجام فرایند تخصصی رفع مشکل سنسورها بصورت ریموت

۱۶ به مدار بازگرداندن سنسورهای منصوبه و ارائه گزارش اصلاحی

۱۷ تهیه گزارش ثبت برخورد ها بصورت ماهانه

۱۸ رفع مشکلات سنسورها از راه دور

۱۹ ارائه گزارش اقدامات انجام شده در قالب مانیتورینگ

۲۰ برگزاری جلسه هماهنگی در جهت رفع مشکلات تخصصی مانیتورینگ

۲۱ اعلام مشکلات فنی یا ستادی غیر قابل رفع در تیم به مدیرمرکز

۲۲ به روزرسانی سنسور و تست مجدد صحت کارکرد

د: گزارش

۱۰ ارائه گزارش وضعیت کاربری سنسورها و حسگرهای منصوبه به سازمان متقاضی بصورت محرمانه

۱۱ ارائه گزارش وضعیت کاربری سنسورها و حسگرهای مربوطه به مدیر

۱۲ ارائه گزارش ثبت برخورد بصورت هفتگی . ماهانه و سالیانه به مدیر

۱۳ ارائه گزارش اقدامات انجام شده در تیم مانیتورینگ به مدیر

۱۴ ایجاد دسترسی گزارش گیری برای مرکز راهبردی افتا

درصورت نیاز به توسعه یا بکارگیری ابزاردیگر از طریق تعریف پروژه جدید و تهیه و تنظیم RFP اقدام می گردد بدین صورت که حسب RFP ارائه شده طبق نیاز بوجود آمده، اقدام به تهیه شرح خدمات می گردد و پس از قطعیت شرح خدمات آنرا به معاونت مالی اداری و تدارکاتی ارسال می دارند لذا پس از طی

فرایندهای مالی و تامین اعتبار اقدام به انعقاد قرارداد جدید در جهت رفع نیاز می گردد و عملکرد پیمانکار مربوطه طبق مفاد قرارداد بدقت مورد پایش و کنترل قرار می گیرد .

فرایند ۹: پاسخ و رفع رخداد

گروه پاسخگویی به رخداد ها حسب مورد ارجاعی اقدام به پاسخ می نمایند در صورتیکه از طریق حسگرهای هانی پات ، اطلاعات دریافت شده باشد نتایج بررسی ها به اطلاع سازمانها و مسئولین شبکه ها رسیده می شود و در صورتیکه اطلاعات از طریق درخواستهای تلفنی باشد نتایج بررسی ها طی ارسال نامه های محرمانه به اطلاع متقاضی رسیده می شود و یا از طریق انجام مکاتبات محرمانه، نتیجه اقدامات به اطلاع متقاضی رسیده می شود.

۵ – پیوست‌ها:

–فرم صورتجلسه تحویل تجهیزات هانی پات

–فرم اعلام آدرس های آلوده

–فرم راهنمای پاکسازی بدافزارها

–فرم پاسخگویی به رخداد

– گزارش اولیه تحلیل بدافزار