

گزارش وضعیت خدمات و سرویسهای ارائه شده در حیطه امنیت فضای تولید و تبادل اطلاعات

تهیه و تدوین:

معاونت امنیت فضای تولید و تبادل اطلاعات

و

مرکز برنامه ریزیک و نظارت راهبردی

مهرماه ۱۴۰۰

بسمه تعالی

مقدمه

در راستای اهداف کلان و انجام وظایف سازمان فناوری اطلاعات ایران در تامین امنیت و فناوری اطلاعات معاونت امنیت این سازمان تشکیل و در سه حوزه نظام مدیریت امنیت اطلاعات (نما)، ارزیابی امنیتی محصولات (ارم)، خدمات مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای (ماهر) فعالیت مینماید.

در این گزارش به اهم اقدامات سازمان در حوزه امنیت فضای تولید و تبادل اطلاعات می پردازیم.

فهرست مطالب

عنوان

صفحه

مقدمه

۲.....

شرکت های فعال در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات و احراز صلاحیت فنی و امنیتی

- شناسایی، ارزیابی و رتبه بندی شرکت های فعال در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات و احراز صلاحیت فنی و امنیتی شرکت های ارائه دهنده محصولات و خدمات امنیتی (سال ۱۴۰۰)..... ۶
- شناسایی، ارزیابی و رتبه بندی شرکت های فعال در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات و احراز صلاحیت فنی و امنیتی شرکت های ارائه دهنده محصولات و خدمات امنیتی (سال ۱۳۹۹)..... ۷

صدور پروانه ها

۷.....

- آمار صدور پروانه فعالیت خدمات ۱۳۹۷ تا ۱۴۰۰..... ۷
- آمار صدور پروانه خدمات به تفکیک حوزه امنیت فضای تولید و تبادل اطلاعات (مهر ۱۴۰۰)..... ۸
- آمار صدور پروانه فعالیت در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات به تفکیک استان ها..... ۹
- عملکرد شاخص ها..... ۱۱
- گزارش خدمات مرکز ماهر مهر ماه ۱۴۰۰..... ۱۳

گزارش عملکرد و اقدامات معاونت امنیت فضای تولید و تبادل اطلاعات -مهرماه ۱۴۰۰

۱۴.....

- عنوان شاخص های اداره کل نما..... ۱۴
- عنوان شاخص های اداره کل ارم..... ۱۶
- عنوان شاخص های مرکز ماهر..... ۱۷

فهرست جداول

عنوان

صفحه

جدول ۱: جدول توزیعی پروانه های صادره برای شرکت های فعال در حوزه افتا (سال ۱۴۰۰) در یک نگاه.....	۶
جدول ۲: جدول توزیعی پروانه های صادره برای شرکت های فعال در حوزه افتا (سال ۱۴۰۰) به تفکیک ماه.....	۶
جدول ۳: شرکت های فعال در حوزه افتا (سال ۹۹) در یک نگاه.....	۷
جدول ۴: آمار صدور پروانه فعالیت خدمات ۱۳۹۷ تا ۱۴۰۰.....	۸
جدول ۵: آمار صدور پروانه فعالیت در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات به تفکیک استان ها.....	۱۰
جدول ۶: عملکرد شاخص.....	۱۲
جدول ۷: شاخص های اداره کل نما.....	۱۵
جدول ۸: شاخص های اداره کل ارم.....	۱۶
جدول ۹: شاخص های مرکز ماهر.....	۱۸

فهرست اشکال

عنوان

صفحه

شکل ۱: گزارشی از خدمات ارائه شده توسط مرکز ماهر.....	۱۳
--	----

گزارش مدیریت و نظارت بر ایجاد سیستم مدیریت امنیت اطلاعات

(حمایت از اجرای سیستم مدیریت امنیت اطلاعات در کلیه دستگاه های اجرایی)

۱. فرایند بررسی و صدور گواهینامه های انطباق سیستم مدیریت امنیت اطلاعات (ISMS)
۲. تعداد گواهی های صادره:
- ✓ در سال ۱۳۹۹ ، ۱۰ عدد گواهی

(تدوین دستورالعمل، اخبار و مشارکت های تخصصی در حوزه امنیت فضای تولید و تبادل اطلاعات)

۳. مشارکت با سازمان ملی استاندارد ایران در خصوص تدوین استانداردهای حوزه فناوری اطلاعات ۲۰۰ نفر ساعت در سال ۱۳۹۹
۴. تهیه و تدوین دستورالعمل های تخصصی حوزه امنیت فضای تولید و تبادل اطلاعات ۶ دستورالعمل در سال ۱۳۹۹
۵. برگزاری گروه های مطالعاتی تخصصی و مشارکت با مجامع جهانی امنیت فضای تولید و تبادل اطلاعات نظیر اتحادیه بین المللی مخابرات (ITU) برگزاری تعداد ۱۰ جلسه درون سازمانی و مشارکت در ۲ رویداد بین المللی (مجازی)
۶. سنجش سطح امنیت سایبری کشور و همکاری با نهاد بین المللی GCI رتبه جهانی ۶۰ و رتبه منطقه ای ۱۳

شرکت های فعال در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات و احراز صلاحیت فنی و امنیتی

➤ شناسایی، ارزیابی و رتبه بندی شرکت های فعال در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات و احراز صلاحیت فنی و امنیتی شرکت های ارائه دهنده محصولات و خدمات امنیتی (سال ۱۴۰۰)

ردیف	سال ۱۴۰۰								
	مدیریتی			عملیاتی			فنی		آموزشی
	مشاوره	ممیزی	ارزیابی امنیتی	پیاده سازی Cert/Soc	امن سازی سامانه ها	امنیت فیزیکی	مسابقات کشف نقص امنیتی	فنی	آموزشی
	۱۰	۴	۱۷	۹	۳۰	۲۵	۲	۸۲	۱۰
۱۹۹	۱۴			۹۳			۸۲		۱۰

جدول ۱: جدول توزیعی پروانه های صادره برای شرکت های فعال در حوزه افتا (سال ۱۴۰۰) در یک نگاه

تعداد کل پروانه سال ۱۴۰۰ تا پایان مهرماه : ۱۹۹ عدد

سال ۱۴۰۰	پروانه	آزمون	cert/soc	امن سازی	امنیت فیزیکی	مسابقات	مشاوره	ممیزی	فنی	آموزشی
فروردین	۲۹	۱	۳	۳	۵	۰	۴	۰	۱۰	۳
اردیبهشت	۲۲	۳	۰	۱۱	۰	۰	۱	۰	۶	۱
خرداد	۵۱	۲	۲	۶	۱۳	۰	۲	۳	۲۳	۰
تیر	۲۰	۱	۲	۳	۰	۰	۲	۰	۱۰	۲
مرداد	۲۷	۶	۱	۵	۱	۰	۰	۰	۱۴	۰
شهریور	۱۷	۳	۱	۰	۵	۰	۰	۰	۶	۲
مهر	۳۳	۱	۰	۲	۱۱	۲	۱	۱	۱۳	۲
جمع	۱۹۹	۱۷	۹	۳۰	۳۵	۲	۱۰	۴	۸۲	۱۰

جدول ۲: جدول توزیعی پروانه های صادره برای شرکت های فعال در حوزه افتا (سال ۱۴۰۰) به تفکیک ماه

➤ شناسایی، ارزیابی و رتبه‌بندی شرکت‌های فعال در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات و احراز صلاحیت فنی و امنیتی شرکت‌های ارائه‌دهنده محصولات و خدمات امنیتی (سال ۱۳۹۹)

جمع کل	مدیریتی								سال ۹۹		
	عملیاتی						فنی			آموزشی	
	مشاوره	ممیزی	ارزیابی امنیتی	پیاده سازی Cert/Soc	امن سازی سامانه ها	امنیت فیزیکی	مسابقات کشف نقص امنیتی	فنی		آموزشی	
	۲۰	۳	۳۰	۱۲	۵۶	۲۸	۲	۷۷	۱۴		
۲۴۲	۲۳		۱۲۸						۷۷	۱۴	

جدول ۳: شرکت‌های فعال در حوزه افتا (سال ۹۹) در یک نگاه

تعداد کل پروانه سال ۱۳۹۹ تا پایان اسفند ماه : ۲۴۲ عدد

صدور پروانه‌ها

➤ آمار صدور پروانه فعالیت خدمات ۱۳۹۷ تا ۱۴۰۰

صدور پروانه		
ماه	سال ۹۹	سال ۱۴۰۰
فروردین	۶	۲۹
اردیبهشت	۱۰	۲۲
خرداد	۸	۵۱
تیر	۳۱	۲۰
مرداد	۲۵	۲۷
شهریور	۲۰	۱۷

صدور پروانه		ماه
سال ۱۴۰۰	سال ۹۹	
۳۳	۲۱	مهر
—	۲	آبان
—	۴۲	آذر
—	۲۳	دی
—	۲۸	بهمن
—	۲۶	اسفند
۱۹۹	۲۴۲	جمع کل

جدول ۴: آمار صدور پروانه فعالیت خدمات ۱۳۹۷ تا ۱۴۰۰

➤ آمار صدور پروانه خدمات به تفکیک حوزه امنیت فضای تولید و تبادل اطلاعات (مهر ۱۴۰۰)

صدور پروانه در حوزه مدیریتی امنیت فضای تولید و تبادل اطلاعات : ۱۴

صدور پروانه در حوزه عملیاتی امنیت فضای تولید و تبادل اطلاعات : ۹۳

صدور پروانه در حوزه فنی امنیت فضای تولید و تبادل اطلاعات : ۸۲

صدور پروانه در حوزه آموزشی امنیت فضای تولید و تبادل اطلاعات : ۱۰

➤ آمار صدور پروانه فعالیت در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات به تفکیک

استان‌ها

استان	سال	
	۱۳۹۹	۱۴۰۰
البرز	۲	۲
اردبیل	۲	۰
ایلام	۱	۲
اصفهان	۱۰	۱۳
آذ- شرقی	۱۱	۸
آذ- غربی	۰	۱
بوشهر	۳	۵
چهار محال بختیاری	۱	۰
خراسان شمالی	۴	۲
خراسان جنوبی	۳	۲
خراسان رضوی	۷	۷
خوزستان	۱۲	۴
سمنان	۰	۱
زنجان	۱	۲
سیستان	۰	۰
فارس	۱۱	۵
قزوین	۰	۰
کهگیلویه و بویر احمد	۰	۱
کرمان	۳	۵

سال		استان
۱۴۰۰	۱۳۹۹	
۳	۱	کرمانشاه
۲	۱	گلستان
۶	۳	گیلان
۴	۴	مازندران
۲	۲	مرکزی
۸	۴	هرمزگان
۲	۲	همدان
۷	۱۰	یزد

جدول ۵: آمار صدور پروانه فعالیت در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات به تفکیک استان ها

عملکرد شاخص‌ها

ردیف	عنوان شاخص	واحد	فروردین ۱۴۰۰	اردیبهشت ۱۴۰۰	خرداد ۱۴۰۰	تیر ۱۴۰۰	مرداد ۱۴۰۰	شهریور ۱۴۰۰	مهر ۱۴۰۰	جمع کل
۱	حملات شناسایی شده توسط شبکه ملی تله بدافزار	تعداد	۹۵۶۷۰۲۸	۹۸۴۷۹۲۳	۵۲۶۹۹۷۰	۶۴۶۳۲۳۱	۵۱۳۵۶۹۴	۶۰۷۱۵۱۹	۱۸۷۳۰۵۸	۴۴۲۲۸۴۲۳
۲	بدافزار شناسایی شده	تعداد	۸۳۶۳	۸۷۲۸	۴۷۰۷	۱۳۹۴۲	۱۲۹۹	۶۰۵۳	۱۲۲۵	۴۴۳۱۶
۳	آدرس‌های آلوده به بات	تعداد	۴۱۰۲۸۱۳	۴۱۴۲۸۶۲	۳۶۶۹۳۱۹	۴۲۴۷۹۲۲	۴۰۱۲۶۴۵	۲۲۳۹۰۳۳	۲۰۵۷۰۴۹	۲۴۴۷۱۶۴۳
۴	نقاط آسیب پذیر داخل کشور	تعداد	۳۵۸۷	۳۸۴۹	۱۲۳۶	۱۱۲۲	۱۶۲۶	۶۰۸	۱۰۴۰	۱۲۸۶۶
۵	پیشگیری از حملات DDOS	تعداد	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰
۶	حملات نفی خدمت شناسایی شده	تعداد	۰	۰	۱	۲	۰	۲	۲	۷
۷	ابزارها و یا سامانه‌های رصد، ارزیابی و پویشگر وبی و غیر وبی بومی	تعداد	۱۵	۱۵	۱۵	۱۶	۱۶	۱۶	۱۶	۱۶

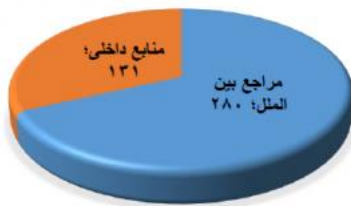
ردیف	عنوان شاخص	واحد	فروردین ۱۴۰۰	اردیبهشت ۱۴۰۰	خرداد ۱۴۰۰	تیر ۱۴۰۰	مرداد ۱۴۰۰	شهریور ۱۴۰۰	مهر ۱۴۰۰	جمع کل
۹	اسامی ابزارها و یا سامانه‌های رصد، ارزیابی و پوشگر وبی و غیر وبی بومی	گزارش				سامانه مودم چک- سامانه SSLچک- سامانه هوشیار- سامانه دانا- سامانه بینا- سامانه کلاه سفید- سامانه تله بدافزار- سامانه شناسا- سامانه ویروس کاو- سامانه تیکتینگ-سامانه DNS check- سامانه آفاق- سامانه واکاو - سامانه ساتا -سامانه هشدار-انجمن مرکز ماهر				
۱۰	سامانه‌های ارزیابی امنیتی شده	تعداد	۳	۱۴	۱۱	۱۲	۱۰	۲۴	۱۹	۹۳
۱۱	اطلاعیه ارایه شده با موضوع امنیت	تعداد	۷	۱۰	۱۲	۲۰	۱۵	۲۰	۹	۹۳
۱۲	هشدار ارایه شده	تعداد	۴۱۷۲	۴۷۶۵	۱۶۸۷	۱۸۱۶	۱۸۷۰	۱۷۴۹	۱۲۹۸	۱۷۳۵۷
۱۳	شناسایی حملات دیفیس	تعداد	۶	۵	۱۹	۱۰	۱۱	۱۲	۱۵	۷۸
۱۴	مراکز آپا	تعداد	۳۴	۳۴	۳۴	۳۴	۳۴	۳۴	۳۴	۳۴
۱۵	رصد اطلاعات (مهم و حیاتی) افشا شده در سطح کشور	تعداد	۷	۷	۱۲	۱۵	۳۱	۲۵	۱۷	۱۱۴
۱۶	نمایندگان سازمان ها و ادارات ، نهادها و بانک‌ها در انجمن مرکز ماهر	تعداد	۵۶	۱۵۶	۱۷۲	۲۱۰	۲۴۵	۲۷۷	۳۱۳	۳۱۳

جدول ۶: عملکرد شاخص

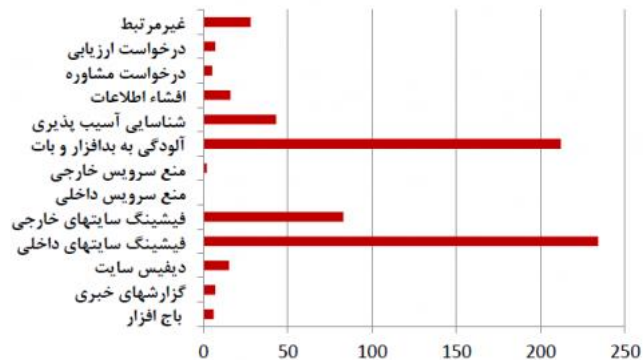
➤ گزارش خدمات مرکز ماهر مهرماه ۱۴۰۰

گزارشی از ۶۵۸ مورد خدمت ارائه شده توسط مرکز ماهر در مهر ماه سال ۱۴۰۰ در گراف‌های زیر قابل مشاهده است. خدمات ارائه شده شامل فراوانی و نوع رخدادهای رسیدگی شده توسط مرکز، بخش‌های دریافت کننده این خدمات و نحوه مطلع شدن مرکز از این رخدادهای است.

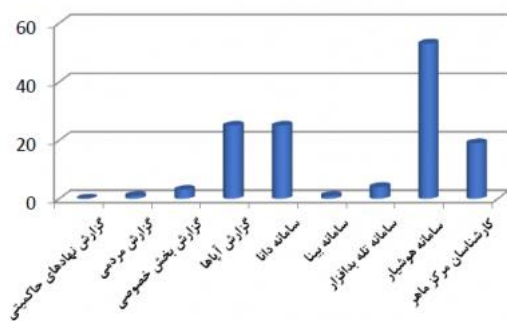
نحوه مطلع شدن مرکز ماهر از رخداد



فراوانی نوع رخداد



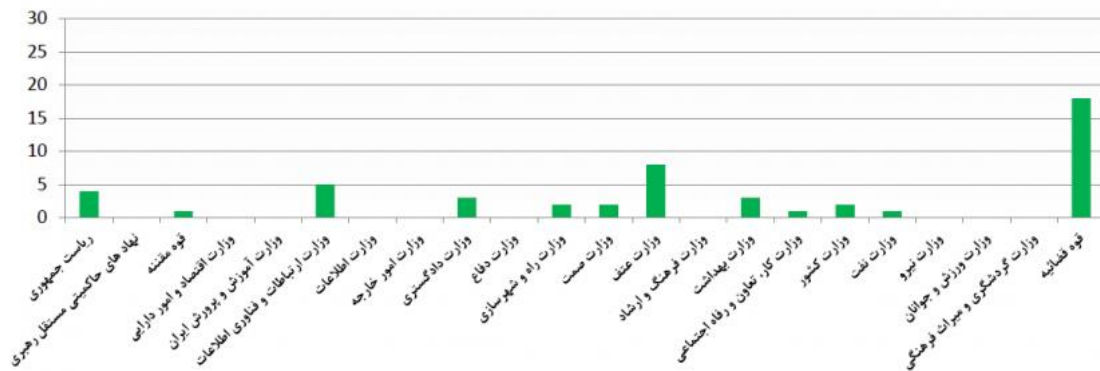
نحوه مطلع شدن مرکز ماهر از منابع داخلی



بخش‌های دریافت کننده خدمت



بخش‌های حاکمیتی دریافت کننده خدمت



شکل ۱: گزارشی از خدمات ارائه شده توسط مرکز ماهر

گزارش عملکرد و اقدامات معاونت امنیت فضای تولید و تبادل اطلاعات - مهرماه ۱۴۰۰

➤ عنوان شاخص های اداره کل نما

تعداد به تفکیک استانها																عنوان شاخص های اداره کل نما- (مهرماه ۱۴۰۰)	واحد/تعداد	زیر شاخص
تهران	بوشهر	آذربایجان شرقی	خراسان شمالی	خراسان رضوی	زنجان	کرمان	کرمانشاه	گیلان	گلستان	مرکزی	هرمزگان	یزد	خوزستان					
۱		خدمات امنیت فضای تولید و تبادل اطلاعات		پروانه/گواهی														
		۱	خدمات مدیریتی امنیت فضای تولید و تبادل اطلاعات	۲	۱	۰	۰	۰	۰	۰	۰	۰	۰	۰				
		۲	خدمات عملیاتی امنیت فضای تولید و تبادل اطلاعات	۱۶	۸	۱	۳	۰	۰	۱	۱	۱	۰	۱				
		۳	خدمات آموزشی امنیت فضای تولید و تبادل اطلاعات	۲	۱	۰	۰	۱	۰	۰	۰	۰	۰	۰				
		۴	خدمات فنی امنیت فضای تولید و تبادل اطلاعات	۱۳	۶	۰	۲	۱	۰	۱	۰	۰	۱	۱	۰			

تعداد به تفکیک استانها														واحد/تعداد	عنوان شاخص های اداره کل نما- (مهر ماه ۱۴۰۰)	
تهران	بو شهر	آذربایجان	خراسان شمالی	خراسان رضوی	زنجان	کرمان	کرمانشاه	گیلان	گلستان	مرکزی	هرمزگان	یزد	خوزستان			
														ساعت جلسه	مشارکت با سازمان ملی استاندارد ایران جهت تدوین استانداردهای ملی فناوری اطلاعات	۲
۶		۲											۲	۱۰	کمیسیون های فنی	۶
۷														۲	کمیته های ملی	۷
۸														۰	کمیته برنامه ریزی	۸
														سند	دستورالعمل های تدوین شده امنیت فضای تولید و تبادل اطلاعات	۳
۹														۰	دستورالعمل های تدوین شده	۹

جدول ۷: شاخص های اداره کل نما

➤ عنوان شاخص های اداره کل ارم

شاخص	زیر شاخص	عنوان شاخص های اداره کل ارم (مهر ۱۴۰۰)	واحد	تعداد کل تأییدیه/گواهی (معتبر/تمدید/منقضی)	تعداد کل محصولات
۱	ارزیابی امنیتی محصولات فضای تولید و تبادل اطلاعات		تأییدیه/گواهی	واحد (تأییدیه/گواهی)	واحد (عدد)
	۱	درخواست صدور گواهی محصولات داخلی	۱۸	۸۸	۸۸
	۲	صدور گواهی محصول داخلی	۲	۸۸	۸۸
	۳	درخواست تمدید گواهی محصولات داخلی	۰	۰	۰
	۴	محصولات داخلی در حال تمدید	۰	۱۳	۱۳
	۵	گواهی های منقضی شده محصولات داخلی	۰	۲۱	۲۱
	۶	درخواست و صدور تأییدیه محصولات خارجی	۲۷	۴۸۰	۹۹۲۹۵
	۷	انتشار پرو فایل های حفاظتی	۰	۴۰	۴۰
	وضعیت آزمایشگاه های ارزیابی امنیتی				
	۱	فعال	۷	۷	-
۲	۲	در حال تمدید	۰	۰	-
	۳	در حال اعتبارسنجی	۱	۱	-

جدول ۸: شاخص های اداره کل ارم

➤ عنوان شاخص های مرکز ماهر

شاخص	عناوین شاخص های مرکز ماهر (مهرماه ۱۴۰۰)		واحد	عملکرد
۱	میزان پوشش نظارتی در فضای سایبری کشور			
	۱	ترافیک در حال پایش از کل ترافیک بین الملل کشور در مرکز عملیات امنیت	درصد	۷/۵
	۲	رصد اطلاعات (مهم و حیاتی) افشا شده در سطح کشور	تعداد	۱۷
	۳	درصد پوشش سازمان های غیر زیر ساختی تحت نظارت مرکز ماهر	درصد	۷۹
	۴	پایش منابع خبری در حوزه امنیت سایبری	تعداد	۱۷۸
	۵	خبرهای وارده به سامانه هوشیار جهت رصد اخبار امنیت سایبری	تعداد	۵۵۰۰۰
	۶	رصد فیشینگ سایت های داخلی کشور	تعداد	۲۳۴
	۷	تعاملات بین المللی	تعداد	۲۸۰
۲	خدمات امداد و عملیاتی مرکز ماهر			
	۱	حملات نفی خدمت گزارش شده به ماهر	تعداد	۲
	۲	هشدار در خصوص نقاط آلوده در سطح کشور	تعداد	۲۰۴۸۴
	۳	هشدار در خصوص نقاط آسیب پذیر در سطح کشور	تعداد	۱۰۴۰
	۴	هشدارهای ناشی از حملات تله بدافزار	تعداد	۱۷۸

عناوین شاخص های مرکز ماهر (مهر ماه ۱۴۰۰)					شاخص	واحد	عملکرد
		۵	گزارشات دریافتی از کلاه سفید	تعداد	۱		
		۶	باج افزارهای رسیدگی شده	تعداد	۶		
		۷	هشدارهای منتشر شده از سایت ماهر	تعداد	۷		
۳	وضعیت امنیت سایبری کشور						
		۱	تعداد نقاط آلوده داخل کشور	تعداد	۲,۰۵۷,۰۴۹		
		۲	میانگین سهم آلودگی به ازاء هر آی پی در سه اپراتور اول آلوده کشور (شرکت مخابرات ایران، شرکت ارتباطات سیار ایران و شرکت خدمات ارتباطی ایرانسل)	مقدار	۰/۲۶		
		۳	تعداد نقاط آسیب پذیر داخل کشور	تعداد	۱۰۴۰		

جدول ۹: شاخص های مرکز ماهر

ITO.GOV.IR

Information Technology Organization of Iran began its services as a subset of Ministry of ICT in 1998 considering the ever-increasing need of the country to construct and develop the computer networks and their connections and ultimately, to connect these networks to the international networks, and in order to establish necessary communication infrastructures for realizing these goals, and also in order to get access to information sources. In the fall of 2010, on the basis of joint proposal by the Vice-president of Management and Development and Human Resources and the Ministry of Communication and Information Technology, in order to abstract the policy-making and sovereignty-related activities from the government companies, Iranian IT Company was changed from a government company into a government institution named Iranian Information Technology Organization. This change was based on the sovereignty-related duties mentioned in the company's articles of association.

ITO manages the support functions and organizes the security of the space of information exchange, hardware and software. It also improves the electronic capabilities, develops the internet service and information technology and their applications in the country. It also manages and monitors the integration of activities in the field of information technology and electronic applications. Moreover, ITO directs the IT section as an agent for the Ministry of Communication and Information Technology and recommends policies for the private sector in order to promote the IT applications in the country.

© 2019 Information Technology Organization of Iran All Rights Reserved

Information Technology Organization of Iran began its services as a subset of Ministry of ICT in 1998 considering the ever-increasing need of the country to construct and develop the computer networks and their connections and ultimately, to connect these networks to the international networks, and in order to establish necessary communication infrastructures for realizing these goals, and also in order to get access to information sources. In the fall of 2010, on the basis of joint proposal by the Vice-president of Management and Development and Human Resources and the Ministry of

