

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 ریزی و نظارت راهبردی

اسفندماه ۱۳۹۹

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 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 ارایه دهنده محصولات و خدمات امنیتی (سال ۱۳۹۹) 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 ارایه دهنده محصولات و خدمات امنیتی (سال ۱۳۹۸) ۷

معرفی دوره های آموزشی ۷

➤ دوره های آموزش تخصصی و حرفه ای امنیت فضای تبادل اطلاعات ۷

صدور پروانه ها ۸

➤ آمار صدور پروانه فعالیت خدمات ۹۷ تا ۹۹ ۸

➤ آمار صدور پروانه خدمات به تفکیک حوزه امنیت فضای تولید و تبادل اطلاعات (اسفند ماه) ۸

➤ آمار صدور پروانه فعالیت در حوزه خدمات امنیت فضای تولید و تبادل اطلاعات به تفکیک استان ها ۹

➤ عملکرد شاخص ها ۱۱

مجموع آسیب های مهم کشف شده در رصد فضای IP کشور توسط سامانه مرکز ماهر در سال ۹۹ به تفکیک ۱۴

گزارش عملکرد و اقدامات معاونت امنیت فضای تولید و تبادل اطلاعات - اسفند ماه ۹۹ ۱۷

➤ عنوان شاخص های اداره کل نما ۱۷

➤ عنوان شاخص های اداره کل ارم ۱۸

➤ عنوان شاخص های مرکز ماهر ۱۹

فهرست جداول

عنوان

صفحه

جدول ۱: جدول توزیعی پروانه های صادره برای شرکت های فعال در حوزه افتا (سال ۹۹) در یک نگاه.....	۶
جدول ۲: جدول توزیعی پروانه های صادره برای شرکت های فعال در حوزه افتا (سال ۹۹) به تفکیک ماه.....	۶
جدول ۳: شرکت های فعال در حوزه افتا (سال ۹۸) در یک نگاه.....	۷
جدول ۴: آمار صدور پروانه فعالیت خدمات ۹۷ تا ۹۹.....	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.....	۱۱
جدول ۷: شاخص های اداره کل نما.....	۱۷
جدول ۸: شاخص های اداره کل ارم.....	۱۸
جدول ۹: شاخص های مرکز ماهر.....	۲۱

فهرست اشکال

عنوان

صفحه

شکل ۱: مقایسه آسیب پذیر های مهم کشف شده در سال ۹۹.....	۱۴
--	----

گزارش مدیریت و نظارت بر ایجاد سیستم مدیریت امنیت اطلاعات

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

۱. طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS) در سازمان فناوری اطلاعات ایران (۱۳۹۸-ماه ۱۲)
 ۲. همکاری و ارائه مشاوره در زمینه پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS) در شرکت ارتباطات زیر ساخت (۱۳۹۸-ماه ۱۲)
 ۳. فرایند بررسی و صدور گواهینامه های انطباق سیستم مدیریت امنیت اطلاعات (ISMS)
 ۴. تعداد گواهی های صادره:
 - ✓ در سال ۱۳۹۹ ، ۱۰ عدد گواهی
 - ✓ در سال ۱۳۹۸ ، ۱۳ عدد گواهی
 - ✓ در سال ۱۳۹۷ ، ۱۵ عدد گواهی
 - (تدوین دستورالعمل، اخبار و مشارکت های تخصصی در حوزه امنیت فضای تولید و تبادل اطلاعات)
 ۵. مشارکت با سازمان ملی استاندارد ایران در خصوص تدوین استانداردهای حوزه فناوری اطلاعات ۲۰۰ نفر ساعت در سال ۱۳۹۹
 ۶. تهیه و تدوین دستورالعمل های تخصصی حوزه امنیت فضای تولید و تبادل اطلاعات ۶ دستورالعمل در سال ۱۳۹۹
 ۷. 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)
 ۸. سنجش سطح امنیت سایبری کشور و همکاری با نهاد بین المللی GCI رتبه جهانی ۶۰ و رتبه منطقه ای ۱۳
 ۹. رصد، پایش و تحلیل اخبار منتسب به جمهوری اسلامی ایران در حوزه امنیت فضای تولید و تبادل اطلاعات
- رصد ۱۰۰ خبر و تهیه ۱۰ گزارش در سال های ۱۳۹۸ و ۱۳۹۹

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 ۱۳۹۹)

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

جدول ۱: جدول توزیعی پروانه های صادره برای شرکت های فعال در حوزه افتا (سال ۹۹) در یک نگاه

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

سال ۹۹	پروانه آزمون	cert/soc	امن سازی	امنیت فیزیکی	مسابقات	مشاوره	ممیزی	فنی	آموزشی
فروردین	6	1	0	3	1	0	0	1	0
اردیبهشت	10	1	0	0	1	0	0	6	1
خرداد	8	2	0	3	0	1	0	1	1
تیر	31	1	1	4	4	3	0	17	1
مرداد	25	2	2	4	3	3	1	8	2
شهریور	20	2	0	8	3	1	1	4	1
مهر	21	4	3	4	2	0	0	5	1
آبان	2	1	0	0	0	0	0	1	0
آذر	42	4	2	12	3	3	1	14	3
دی	23	3	1	7	3	2		5	
بهمن	28	5	3	4	5	1	0	7	3
اسفند	26	4	0	7	3	0	3	8	1
جمع	242	30	12	56	28	2	3	77	14

جدول ۲: جدول توزیعی پروانه های صادره برای شرکت های فعال در حوزه افتا (سال ۹۹) 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 ۱۳۹۸)

سال ۹۸	مدیریتی		عملیاتی				آموزشی	
	مشاوره	ممیزی	ارزیابی امنیتی	پیاده سازی Cert/Soc	امن سازی سامانه ها	امنیت فیزیکی	فنی	آموزشی
	۱۰	۲	۱۵	۸	۲۲	۲۲	۵۸	۱۱
جمع کل	۱۲			۶۷			۵۸	۱۱
۱۴۸								

جدول 3: شرکت‌های فعال در حوزه افتا (سال ۹۸) در یک نگاه

تعداد کل پروانه سال ۱۳۹۸ : ۱۴۸ عدد

معرفی دوره‌های آموزشی

➤ دوره‌های آموزش تخصصی و حرفه‌ای امنیت فضای تبادل اطلاعات

• تامین محتوای آموزشی تخصصی امنیت فضای تولید و تبادل اطلاعات ۲۴۰ ساعت
• برگزاری کارگاه و کلاسهای برخط و مجازی حوزه امنیت فضای تولید و تبادل اطلاعات ۲۴۰۰ نفر ساعت
• برنامه ریزی و برگزاری دوره های آموزشی سیستم مدیریت امنیت اطلاعات در ۱۲ استان کشور ۹۶۰۰ نفر ساعت

صدور پروانه‌ها

➤ آمار صدور پروانه فعالیت خدمات ۹۷ تا ۹۹

ماه			صدور پروانه
سال ۹۷	سال ۹۸	سال ۹۹	
۳	۱۴	۶	فروردین
۱۳	۱۵	۱۰	اردیبهشت
۱۵	۹	۸	خرداد
۱۴	۱۵	۳۱	تیر
۲۸	۳	۲۵	مرداد
۱۳	۱۲	۲۰	شهریور
۲۱	۱۱	۲۱	مهر
۱۸	۸	۲	آبان
۱۰	۱۴	۴۲	آذر
۳۸	۱۷	۲۳	دی
۱۲	۵	۲۸	بهمن
۱۴	۲۵	۲۶	اسفند
۱۹۹	۱۴۸	۲۴۲	جمع کل

جدول ۴: آمار صدور پروانه فعالیت خدمات ۹۷ تا ۹۹

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

صدور پروانه در حوزه مدیریتی امنیت فضای تولید و تبادل اطلاعات : ۳

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

صدور پروانه در حوزه فنی امنیت فضای تولید و تبادل اطلاعات : ۸

صدور پروانه در حوزه آموزشی امنیت فضای تولید و تبادل اطلاعات : ۱

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

استان‌ها

استان	سال		
	۹۷	۹۸	۹۹
البرز	۱	۲	۲
اردبیل	۰	۰	۲
ایلام	۰	۰	۱
اصفهان	۴	۳	۱۰
آذ- شرقی	۲	۷	۱۱
آذ- غربی	۰	۳	۰
بوشهر	۳	۱	۳
چهار محال بختیاری	۰	۰	۱
خراسان شمالی	۰	۰	۴
خراسان جنوبی	۰	۲	۳
خراسان رضوی	۳	۸	۷
خوزستان	۴	۳	۱۲
زنجان	۱	۰	۱
سیستان	۰	۱	۰
فارس	۵	۷	۱۱
قزوین	۰	۱	۰
کهگیلویه و بویر احمد	۰	۱	۰
کرمان	۱	۲	۳
کرمانشاه	۰	۳	۱
گلستان	۱	۱	۱
گیلان	۱	۱	۳
مازندران	۰	۲	۴

استان	سال		
	۹۷	۹۸	۹۹
مرکزی	۱	۳	۲
هرمزگان	۲	۰	۴
همدان	۱	۱	۲
یزد	۲	۶	۱۰

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

عملکرد شاخص‌ها

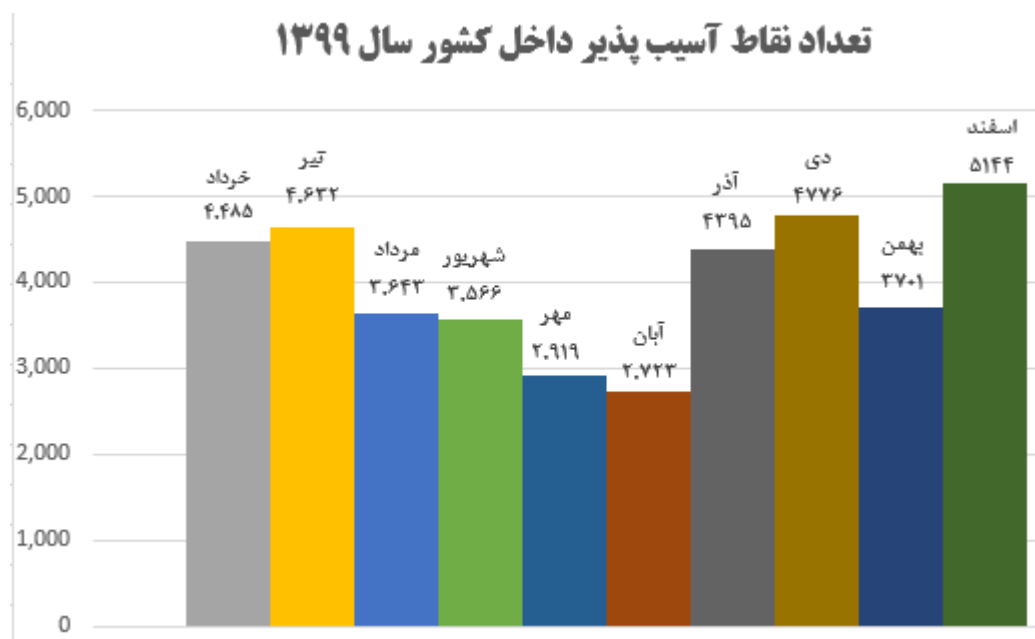
ردیف	عنوان شاخص	واحد	اردیبهشت ۹۹	خرداد ۹۹	تیر ۹۹	مرداد ۹۹	شهریور ۹۹	مهر ۹۹	آبان ۹۹	آذر ۹۹	دی ۹۹	بهمن ۹۹	اسفند ۹۹	جمع کل
۱	تعداد حملات شناسایی شده توسط شبکه ملی تله بدافزار	تعداد	-	۲۸۰۹۸۵۴۴	۵۳۷۸۸۹۶۰	۳۱۹۴۷۰۳۸	۹۴۷۱۳۹۹۷	۵۵۲۹۳۰۴۵	۲۱۲۸۸۸۰۳	۱۷۸۹۶۹۷۰	۱۶۸۹۶۵۴۴	۱۵۷۲۴۹۱۵	۱۶۴۱۷۵۹۵	۴۰۵۹۵۶۶۳۰
۲	تعداد آدرس‌های آلوده به بات‌های شناخته شده	تعداد	۲۵۴۶۴۰	۲۷۲۳۸۹	۳۵۳۷۴۶	۲۵۴۰۳۲	۳۹۳۷۷۶۱	۴۴۳۶۴۷۵	۴۴۹۹۳۲۹	۴۸۷۴۰۴۶	۴۷۸۳۱۱۱	۱۸۱۲۰۷	۴۰۰۴۷۲۷	۲۷۸۵۱۴۶۳
۳	تعداد بدافزار شناسایی شده	تعداد	۱۹۷۸	۴۱۰۰	۲۶۱۴	۲۴۳۲	۱۰۰۰۰۴	۱۶۲۷۶۶	۴۳۹۸۱	۱۸۱۴۴	۲۰۱۰۰	۲۳۷۰۵	۱۶۶۰۹	۳۹۶۴۳۳
۴	تعداد بدافزار تحلیل شده	تعداد	۲۵	۲۲۶	۵۷	۰	۰	۰	۰	۰	۰	۰	۰	۳۰۸
۵	تعداد پیشگیری از حمله در برابر حملات DDOS	تعداد	۱۵۰	۱۵۰	۱۵۰	۱۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۵۰	۱۵۰
۶	تعداد وزارتخانه و سازمان متصل به شبکه ملی اطلاعات که SOC در آنها راه‌اندازی شده	تعداد	۰	۰	۰	۰	۰	۰	۰	یک مورد (در حال راه‌اندازی)	یک مورد (در حال راه‌اندازی)	یک مورد (در حال راه‌اندازی)	یک مورد (در حال راه‌اندازی)	۰

جدول ۶: عملکرد شاخص

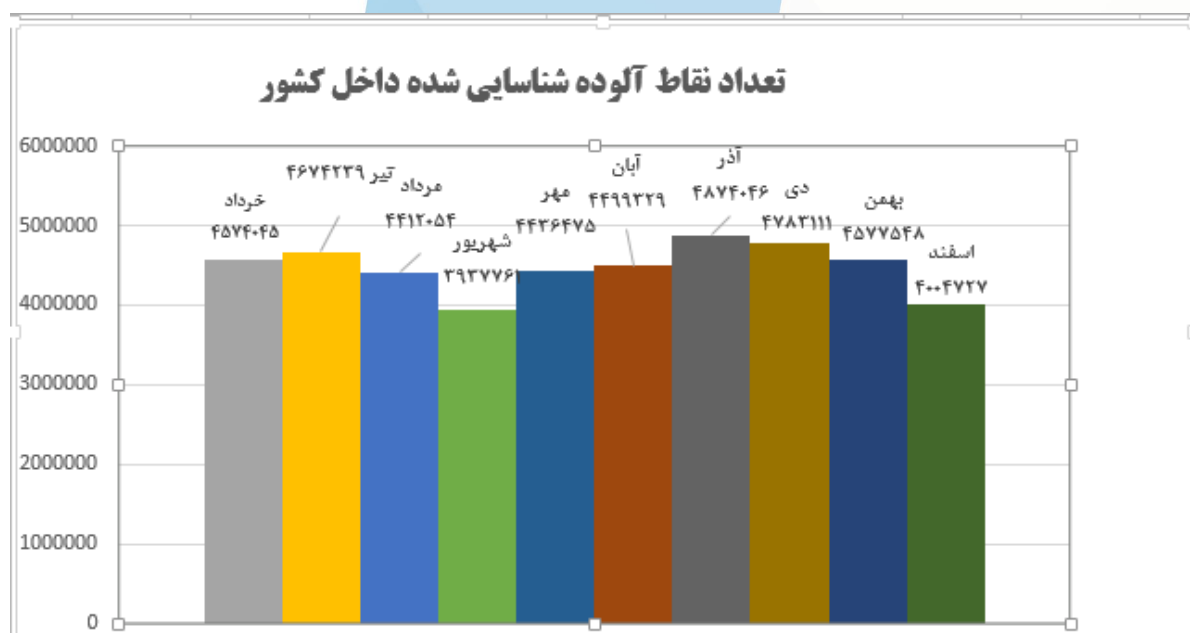
[illegible]

مجموع آسیب‌های مهم کشف شده در درصد فضای IP کشور توسط سامانه مرکز ماهر در سال ۹۹ به تفکیک

بر اساس امکانات سپر دفاعی دژفا، فضای IP کشور نسبت به آسیب‌پذیری‌های دارای درجه خطر بالا و خطرناک به صورت مستمر رصد می‌شود. در نه ماه اخیر حدود ۴۰۰۰۰ نقاط آسیب‌پذیر شناسایی شده و در سه ماهه اخیر با افزایش تقریبی حملات مواجهه بوده ایم.



شکل ۱: مقایسه آسیب‌پذیری‌های مهم کشف شده در سال ۹۹



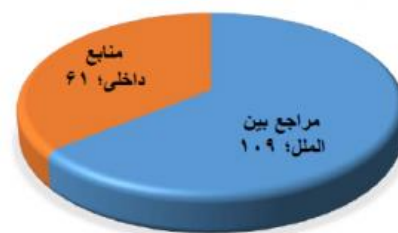
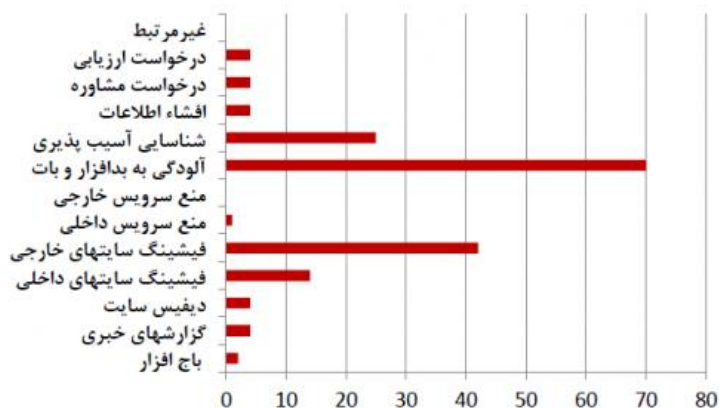
گزارش خدمات مرکز ماهر در بازه زمانی اول لغایت ۱۵م فروردین (۲۵۴ مورد خدمت)

گزارشی از ۲۵۴ مورد خدمت ارائه شده توسط مرکز ماهر در دو هفته اول فروردین ماه سال ۱۴۰۰ (۱۱ الی ۱۵ فروردین 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 رخدادهاست.

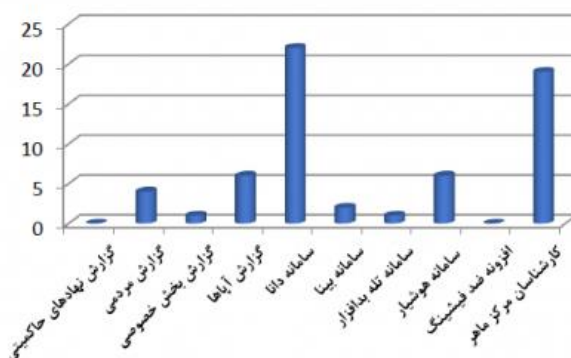
فراوانی نوع رخداد



نحوه مطلع شدن مرکز ماهر از رخداد

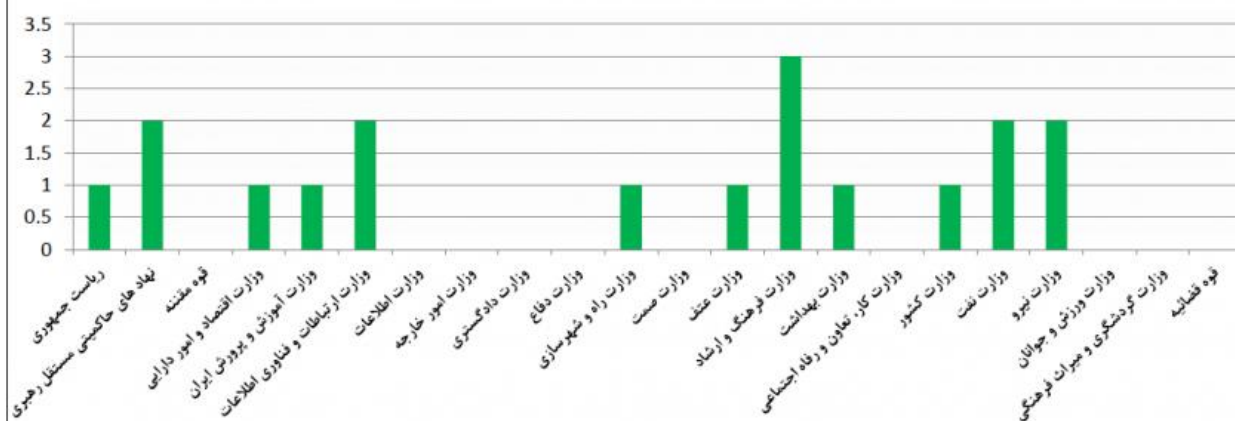


بخش های دریافت کننده خدمت



نحوه مطلع شدن مرکز ماهر از منابع داخلی

بخش های حاکمیتی دریافت کننده خدمت



گزارش عملکرد و اقدامات معاونت امنیت فضای تولید و تبادل اطلاعات - اسفند ماه ۹۹

➤ عنوان شاخص های اداره کل نما

تعداد به تفکیک استانها									واحد/تعداد	عنوان شاخص های اداره کل نما - (اسفند ماه ۹۹)	زیر شاخص	شاخص
تهران	البرز	خوزستان	فارس	خراسان شمالی	خراسان جنوبی	خراسان رضوی	کرمان	یزد				
									پروانه / گواهی	خدمات امنیت فضای تولید و تبادل اطلاعات	1	1
1	1	0	0	0	0	0	0	1	3	خدمات مدیریتی امنیت فضای تولید و تبادل اطلاعات	1	
8	0	2	2	0	1	1	0	0	14	خدمات عملیاتی امنیت فضای تولید و تبادل اطلاعات	2	
0	0	0	1	0	0	0	0	0	1	خدمات آموزشی امنیت فضای تولید و تبادل اطلاعات	3	
4	0	1	0	1	0	1	1	0	8	خدمات فنی امنیت فضای تولید و تبادل اطلاعات	4	
0		0	0	0	0	0	0	0	1	گواهی انطباق سیستم مدیریت امنیت اطلاعات (ISMS) پوشهر	5	

جدول ۷: شاخص های اداره کل نما

➤ عنوان شاخص های اداره کل ارم

شاخص	زیر شاخص	عنوان شاخص های اداره کل ارم (اسفند ماه ۹۹)	واحد	تعداد کل تأییدیه / گواهی (معتبر / تمدید / منقضی)	تعداد کل محصولات
1	ارزیابی امنیتی محصولات فضای تولید و تبادل اطلاعات				
	۱	درخواست صدور گواهی محصولات داخلی	تأییدیه / گواهی	۶۷	واحد (عدد)
	۲	صدور گواهی محصول داخلی	۲۲	۶۷	۶۷
	۳	درخواست تمدید گواهی محصولات داخلی	۹	۶۹	۶۹
	۴	محصولات داخلی در حال تمدید	۰	۲	۲
	۵	گواهی های منقضی شده محصولات داخلی	۰	۹	۹
	۶	درخواست و صدور تأییدیه محصولات خارجی	۰	۲۱	۲۱
	۷	انتشار پرو فایل های حفاظتی	۰	۳۴۶	۵۷۳۱۶
	وضعیت آزمایشگاه های ارزیابی امنیتی				
2	1	فعال	۷	۷	—
	2	در حال تمدید	—	—	—

جدول ۸: شاخص های اداره کل ارم

➤ عنوان شاخص های مرکز ماهر

شاخص	عناوین شاخص های مرکز ماهر (اسفند ماه ۱۳۹۹)		واحد	عملکرد
۱	میزان پوشش نظارتی در فضای سایبری کشور			
	۱	سامانه های دولت الکترونیک تحت نظارت مرکز عملیات امنیت	درصد	۰
	۲	ترافیک در حال پایش از کل ترافیک بین الملل کشور در مرکز عملیات امنیت	درصد	۷/۵
	۳	رصد اطلاعات (مهم و حیاتی) افشا شده در سطح کشور	تعداد	۳
	۴	درصد پوشش سازمان های غیر زیر ساختی تحت نظارت مرکز ماهر	درصد	۴۶
	۵	پایش منابع خبری در حوزه امنیت سایبری	تعداد	۱۸۰
	۶	خبرهای وارده به سامانه هوشیار جهت رصد اخبار امنیت سایبری	تعداد	۶۰۰۰۰
	۷	رصد فیشینگ سایت های داخلی کشور	تعداد	۲۵
۱۹	۸	تعاملات بین المللی	تعداد	۲۲۵

شاخص	عناوین شاخص های مرکز ماهر (اسفند ماه ۱۳۹۹)			واحد	عملکرد
۲	خدمات امداد و عملیاتی مرکز ماهر				
	زیر شاخص	۱	حملات نفی خدمت گزارش شده به ماهر	تعداد	۰
		۲	هشدار در خصوص نقاط آلوده در سطح کشور	تعداد	۳۲۵۲۲۰
		۳	هشدار در خصوص نقاط آسیب پذیر در سطح کشور	تعداد	۵۱۴۴
		۴	هشدارهای ناشی از حملات تله بدافزار	تعداد	۹۰
		۵	گزارشات دریافتی از کلاه سفید	تعداد	۱۸
		۶	باج افزارهای رسیدگی شده	تعداد	۳
		۷	هشدارهای منتشر شده از سایت ماهر	تعداد	۹
	وضعیت امنیت سایبری کشور				
۳	زیر شاخص	۱	تعداد نقاط آلوده داخل کشور	تعداد	۴۰۰۴۷۲۷
		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	۰/۴۸۷

عناوین شاخص های مرکز ماهر (اسفند ماه ۱۳۹۹)			شاخص		واحد	عملکرد
	۳	تعداد نقاط آسیب پذیر داخل کشور	تعداد	۵۱۴۴		

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

