مرکز تخصصی آپا دانشگاه رازی

پیشرو در ارائه خدمات امنیت فناوری و اطلاعات

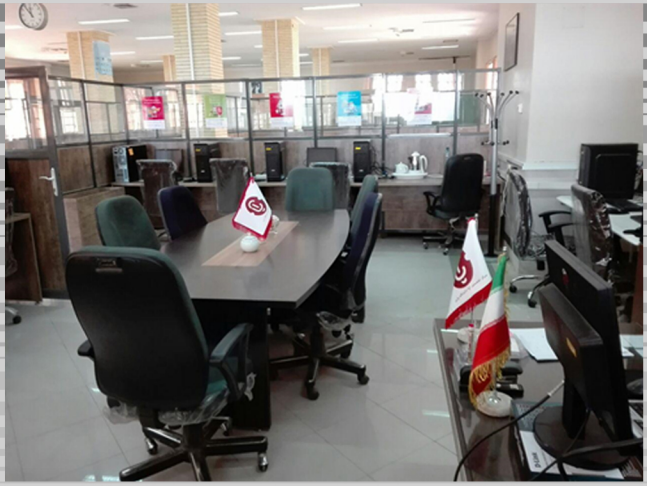
گزارش سالانه مرکز آپا دانشگاه رازی

به نام خدا

اهم فعالیت های انجام شده مرکز آپا دانشگاه رازی

از ۲۷ تیرماه ۱۳۹۵ تا پایان سال ۱۳۹۶

مرکز آگاهی رسانی، پشتیبانی و امداد دانشگاه رازی، همزمان با سفر ریاست محترم جمهور در ۲۷ تیرماه ۱۳۹۵ افتتاح گردید. این مرکز خدمات خود را در قالب شناسایی تهدیدات رایانه ای، کشف و گزارش آسیب پذیری ها، رسیدگی و امداد به سازمان‌ها در هنگام بروز حوادث ناشی از حملات و رخدادهای امنیتی، ارزیابی امنیتی و آزمون نفوذپذیری، پژوهش های کاربردی و توسعه ای، آموزش عمومی و تخصصی در زمینه امنیت سایبری ارائه می دهد. در این مرکز ۱۵ نفر از فارغ التحصیلان و دانشجویان بومی استان در فضایی به مساحت حدودا ۷۰ متر مربع مشغول به فعالیت می باشند. در ادامه گزارش مختصری از اهم دستاوردها و فعالیت های انجام شده در این مرکز از بدو تاسیس تا پایان سال ۱۳۹۶ ارائه شده است.



۱. کشف تهدیدات و آسیب پذیریها

تعداد ۳۰ گزارش مربوط به هک و deface سایتها و پرتالهای دانشگاهی و سازمانی گزارش گردید.

ردیف	عنوان	تاریخ	
۱	موسسه خیریه محک	۲۰۱۷/۱۵/۲	۲۰:۴۴
۲	دانشگاه آزاد اسلامی واحد خسرو شاه	۲۰۱۷/۱۹/۲	۱:۰۲
۳	سایت مرکز سلول درمانی رویال	۲۰۱۷/۲۰/۲	۲۱:۴۹
٤	پژوهشگاه مواد و انرژی	۲۰۱۷/۱۷/۲	۸:۱۱
۵	دانشگاه کاشان	۲۰۱۷/۲۱/۲	۲۰:۰۲
٦	سایت اساتید دانشگاه آزاد تهران شمال	۲۰۱۷/۱/۳	۲۳:۳۰
۷	دانشگاه علوم پزشکی کرمانشاه	۲۰۱۷/۲۸/٦	۲۲:۰۵
۸	دانشگاه علوم پزشکی همدان	۲۰۱۷/۲۸/٦	۲۲:۱۰
۹	دانشگاه علوم پزشکی اصفهان	۲۰۱۷/۲۸/٦	۲۲:۲۰

۲. پاسخگویی به رخدادهای امنیتی

در قالب مشاوره و ارائه روش های امن سازی ۵ سازمان امداد رسانده شد و گزارش های تحلیلی به مراجع زیربط ارائه شد. در این میان ٤ سازمان به باج افزار مبتلا شده بودند و پرتال سازمانی یکی از ادارات استان نیز دچار تغییر چهره (deface) شده بود.

۳. ارزیابی امنیتی

از مهمترین ارزیابی های انجام شده توسط این مرکز می توان به موارد زیر اشاره کرد:

- پایش وضعیت امنیت سامانه‌های تحت وب و سرورهای عمومی ۵۰ سازمان دولتی در استان کرمانشاه
- بررسی وضعیت گواهی دیجیتال پروتکل SSL در سازمان‌های حوزه انرژی در استان کرمانشاه
- ارزیابی پرتال مرکز ملی پایش محیط کسب و کار
- ارزیابی پرتال سازمان فنی و حرفه ای استان کرمانشاه
- ارزیابی نرم افزار آنتی ویروس پادویش
- شبکه اجتماعی آپانت (کسب مقام چهارم در مسابقه کشف آسیب پذیری شبکه اجتماعی آپانت)

٤. تولید مستندات مرجع

عناوین مهم مستندات مرجع تولید شده در جدول زیر آمده است. بسیاری از این مطالب در پرتال مرکز ماهر نیز منتشر شده است.

	عنوان
۱	بررسی آسیب‌پذیریهای برنامه‌های تحت وب و رفع آنها در سه زبان PHP، ASP و Java
۲	مطالعه و بررسی رویکردها و محصولات همبستگی هشدارهای امنیتی
۳	بدون نوشتن کد نیز می‌توان راهکارهای امنیتی رایج لینوکس را دور زد!
٤	هنگام ارتقاء یا بروزرسانی ویندوز 10 کامپیوتر خود را رها نکنید
٥	یک اکسپلویت ساده جاوااسکریپتی، سیستم حفاظتی ASLR در 22 معماری مختلف cpu را دور می زند!
٦	معرفی Memory Injection و ایده‌هایی برای جلوگیری از این گونه حملات
۷	راهنمای پیکربندی امن IIS در مواجه با حملات DDOS
۸	آشنایی با باج افزار Forgo و روش های مقابله با آن
۹	3 راهکار برای جلوگیری از ورود برنامه‌های مخرب در دستگاه اندرویدی شما
۱۰	راهکارهای مقابله با باج افزار WannaCry

۵. برگزاری کارگاه های آموزشی

در مجموع ۱۱ دوره و کارگاه آموزشی توسط مرکز آپا دانشگاه رازی برگزار شد. حدود ۴۰۰ نفر در این دوره‌ها شرکت نمودند و جمعا ۴۱۸۰ نفر ساعت آموزش داده شد.

کارگاه های آموزشی

ردیف	عنوان	محل برگزاری	زمان	تعداد شرکت کنندگان	ساعت	نفر ساعت
۱	+ Security	دانشگاه رازی	شهریور ۹۵	۲۰	۳۰	۶۰۰
۲	+ Security	دانشگاه کردستان	بهمن ۹۵	۱۲	۳۰	۳۶۰
۳	آزمون نفوذپذیری	دانشگاه رازی	اسفند ۹۵	۱۸	۴۰	۷۲۰
۴	امنیت شبکه سیسکو	دانشگاه رازی	تیر ۹۶	۱۸	۴۰	۷۲۰
۵	امنیت اطلاعات در فضای سایبری، چالش ها و راهکارها	شرکت توزیع برق استان	شهریور ۹۶	۲۰	۴	۸۰
۶	امنیت اطلاعات در فضای سایبری، چالش ها و راهکارها	شرکت برق منطقه ای	شهریور ۹۶	۴۰	۴	۱۶۰
۷	امنیت اطلاعات در فضای سایبری، چالش ها و راهکارها	اداره کل منابع طبیعی و آبخیزداری استان	شهریور ۹۶	۵۰	۴	۲۰۰
۸	امنیت اطلاعات در فضای سایبری، چالش ها و راهکارها	قرارگاه منطقه ای غرب ارتش	شهریور ۹۶	۷۵	۴	۳۰۰
۹	امنیت اطلاعات در فضای سایبری، چالش ها و راهکارها	اداره کل آموزش و پرورش استان	مهر ۹۶	۴۵	۴	۱۸۰
۱۰	کمپ آموزشی مسابقات فتح پرچم	دانشگاه رازی	دی ۹۶	۶۰	۱۲	۷۲۰
۱۱	امنیت اطلاعات در فضای سایبری، چالش ها و راهکارها	اداره کل پست استان	بهمن ۹۶	۳۵	۴	۱۴۰
			جمع	۳۹۳	۱۷۶	۴۱۸۰

سمینارها و رویدادهای تخصصی

ردیف	عنوان	زمان	مکان	شرکت کنندگان
۱	سمینار اهمیت امنیت سایبری در پدافند غیر عامل	۳ آبان ۹۵	دانشگاه رازی	۱۵۰ نفر
۲	سمینار اهمیت امنیت سایبری در پدافند غیر عامل	۸ آبان ۹۶	دانشگاه رازی	۱۸۰ نفر
۳	رویداد معارفه مسابقه فتح پرچم غرب کشور	۲۰ آذر ۹۶	دانشگاه رازی	۳۰ نفر
۴	مسابقه فتح پرچم غرب کشور	۱۴ دی ۹۶	دانشگاه رازی	۸۰ نفر

٦. برگزاری اولین مسابقه فتح پرچم غرب کشور

این مسابقه با هدف ترغیب دانشجویان به مطالعه و تحقیق بر موضوعات امنیت سایبری در قالب سه رویـداد به شرح زیر برگزار شد و به برگزیدگان جوایز نفیسی اهدا گردید.

- رویداد معارفه: ۲۰ آذر ۹۶ - دانشکده فنی دانشگاه رازی - تعداد شرکت کنندگان: ۳۰ نفر
- کمپ آموزشی: ۵ الی ۷ دی ۹۶ - کتابخانه مرکزی دانشگاه رازی - تعداد شرکت کنندگان: ٦۰ نفر
- مسابقه اصلی: ١٤ دی ۹٦ - کتابخانه مرکزی دانشگاه رازی - تعداد شرکت کنندگان: ۱۳ تیم از دانشـگاه هـای سطح استان و شهرستانهای همجوار

۷. طراحی و تولید ابزارهای مقابله با حوادث

از جمله ابزارهای تولید شده در مرکز آپا می توان به موارد زیر اشاره کرد.

ردیف	عنوان	خروجی
۱	سایمان: ابزاری برای آموزش تست نفوذ روی برنامه‌های تحت وب	این ابزار یک سامانه عمدا آسیب پذیر می باشد که به منظور آموزش حملات رایج بر روی سامانه های تحت وب تولید شده است. راهکارهای مقابله و امن سازی نیز در این ابزار شرح داده شده است. این پروژه به صورت یک پروژه متن باز در اختیار مرکز ماهر و مراکز آپا و سایر علاقمندان قرار گرفت.
۲	ابزار مسدود کردن و فیلترینگ پورت یو اس بی	این ابزار همه تجهیزات متصل به سیستم را مسدود می‌کند به جزء آنهایی‌که درفیلترینگ توسط مدیر سیستم مشخص شده‌اند. امکان ارائه گزارش های مختلف از دسترسی ها و اتصالات از جمله ویژگی های این ابزار می باشد.
۳	سایتبان: سامانه پایش پایگاههای اینترنتی	این سامانه قابلیت تشخیص مبتلا شدن به حملات DDOS و نفوذهایی که منجر به deface شدن صفحات یک سایت می شوند را دارد. علاوه به ارائه هشدار از طریق ایمیل و پیامک امکان ارائه عکس العمل مناسب در مواجه به این حملات را دارد.
٤	سایمان 2: ابزاری برای برگزاری مسابقات فتح پرچم	پلفترمی جامع است که شامل تعدادی سایت آسیب پذیر می باشد که برای مسابقات فتح پرچم می توان از آنها استفاده نمود.
۵	ابزار یو اس بی هانی پات	یک حافظه فلش را شبیه سازی می کند که برای تشخیص سیستم های آلوده وبه دام انداختن ویروس هایی که از طریق حافظه فلش منتقل می شوند به کار می رود.

۸. مشارکت موثر در همایش های سالانه آپا

در دوره گذشته همایش آپا که در سالهای ۹۵ و ۹۶ به ترتیب در شهرهای مشـهد و زاهدان برگـزار گـردید، مرکز آپای دانشگاه رازی حضوری پررنگ داشت. در همایش آپا ۲ با ارائه مقاله و در همایش آپا ۳ کارگاه تست نفوذ روي سامانه های تحت وب را برگزار نمود.