# تجربه خدمات آپا در استان خراسان رضوی و کسب مرجعیت استانی در توسعه توان مقابله با حوادث رایانه‌ای

احسان طیرانی راد[1]، محسن کاهانی[2]

۱ مدیر روابط عمومی آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

tayarani@um.ac.ir

۲ دانشیار گروه مهندسی کامپیوتر و مدیر آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

kahani@um.ac.ir

## چکیده

**در این مقاله، ضمن بیان مقدمه‌ای از شکل‌گیری آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد، خدمات و دستاوردهای آن در ۴ سال فعالیت در زمینه امنیت فضای تبادل اطلاعات تشریح شده است. آپای فردوسی با تدبیر مدیریت و اتخاذ سیاست‌های مناسب توانسته است به‌عنوان یکی از آپاهای فعال در کشور شناخته شود که این مهم به مدد خدمات ارزنده آن در استان خراسان رضوی و کسب مرجعیت استانی در زمینه امنیت فضای تبادل اطلاعات به دست‌آمده‌است. از جمله این خدمات آزمون نفوذپذیری سامانه‌ها و شبکه‌های رایانه‌ای، صدور گواهی‌نامه امنیتی برای برنامه‌های کاربردی تحت وب و طرح جامع امنیت شبکه می‌باشد که ضمن معرفی آن‌ها، سیاست‌ها و مزیت‌های آپای فردوسی و دستاوردهای کاری آن نیز تشریح شده است.**

## کلمات کلیدی:

**امنیت فضای تبادل اطلاعات، آپا، دانشگاه فردوسی مشهد، آزمون نفوذپذیری، گواهی‌نامه امنیتی، طرح امنیت شبکه.**

## ۱- مقدمه

امنیت اطلاعات یا امنیت شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری، موضوع جدیدی در حوزه فناوری اطلاعات و ارتباطات نیست؛ اما دغدغه تازه‌ای برای کاربران این حوزه به‌شمار می‌آید. امروزه همگام با پیشرفت فناوری‌های ارتباطی و گسترش شبکه‌های رایانه‌ای، امنیت فضای تبادل اطلاعات به یکی از دغدغه‌های اصلی مدیران، کارشناسان، دانش‌پژوهان و کاربران حوزه فتا[۱] تبدیل شده است. در پاسخ به این دغدغه گروه‌هایی به نام CERT [۲] در دنیا تشکیل شده که در ایران به نام مراکز و آزمایشگاه‌های آپا[۳] فعالیت می‌کنند[۱]. آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد (آپای فردوسی) نمونه‌ای از آن است.

این آزمایشگاه از سال ۱۳۸۷ آغاز به کار نموده است و با توجه به اهداف راه‌اندازی آن و برنامه‌ریزی‌ها و تدابیر و سیاست‌های طرح‌ریزی‌شده توانست در زمینه نهادینه‌سازی موضوع افتا[۴] در حوزه جغرافیایی فعالیت، پیشگام دیگر مراکز مشابه باشد. سیاست‌های آپای فردوسی در زمینه آگاهی‌رسانی، پشتیبانی و امداد و حضور هدف‌مند آن در مراکز تصمیم‌سازی استانی و ملی موجب موفقیت در دست‌یافتن به اهداف آن و ارائه خدمات آپا در استان شده است که در این مقاله به مرور این سیاست‌ها و تدابیر در کسب مرجعیت استانی و ارائه خدمات آپا می‌پردازیم.

## ۲- خدمات آزمایشگاه

خدمات آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد را می‌توان به‌طور کلی و به‌صورت خلاصه در عنوان‌های زیر برشمرد.

### ۲-۱- رسیدگی به حوادث

رسیدگی به حوادث شامل دریافت، اولویت‌بندی، تحلیل و پاسخ به حوادث رایانه‌ای و رخدادهای امنیتی می‌شود.

### ۲-۲- رسیدگی به آسیب‌پذیری‌ها

دریافت گزارش‌ها و اطلاعات لازم در مورد وجود آسیب‌پذیری‌ها در شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری، تحلیل ماهیت و اثرات آن‌ها، اعزام تیم مجرب در صورت لزوم و تهیه گزارش‌های فنی، از جمله اقدام‌هایی است که در ذیل این خدمت ارائه می‌شود.

### ۲-۳- اطلاع‌رسانی

این بخش شامل اطلاع‌رسانی‌های مرتبط با امنیت اطلاعات مانند کشف آسیب پذیری جدید، تولید ابزار یا روش جدیدی برای حمله، اعلام خطر نفوذ، توصیه‌های امنیتی و غیره است. این بخش جزو خدمات بازدارنده است و هدف از آن آگاه‌سازی و اطلاع‌رسانی برای جلوگیری از حوادث در آینده است. حوزه عملکردی این بخش عمومی و محدود به کشور است.

### ۲-۴- انتشار اطلاعات مربوط به امنیت شبکه

این بخش به ارائه مجموعه‌ای از اطلاعات مفید و جامع در مورد روش‌های برقراری امنیت می پردازد. هدف از این سرویس کمک به افراد و سازمان‌ها برای دستیابی هرچه راحت‌تر به اطلاعات امنیتی است. اطلاعاتی که در این بخش ارائه می‌شود، می‌تواند شامل موارد زیر و حتی بیشتر باشد:

- ارائه رهنمودهای مختلف در ارتقای امنیت سرویس‌های شبکه
- ارائه رهنمودهای مختلف در ارتقای امنیت شبکه‌های بی‌سیم
- ارائه آرشیوی از اطلاع‌رسانی‌های مختلف
- ارائه راهنماهای عمومی و پایگاه دانش در مورد آسیب‌پذیری‌های نرم‌افزارهای شبکه و تجهیزات بی‌سیم
- ارائه مستندات شیوه‌های امن‌سازی نرم‌افزارهای شبکه
- ارائه مستندات شیوه‌های امن‌سازی شبکه‌های بی‌سیم
- ارائه سیاست‌ها، رویه ها و چک‌لیست‌های امنیتی
- ارائه آمارهای مختلف امنیتی مانند آمار حوادث شبکه، آسیب‌پذیری‌های مختلف نرم‌افزاری، انواع نرم‌افزارهای سرویس‌دهنده مورد استفاده، میزان مواجهه سازمان‌های دولتی و خصوصی با انواع حملات، پراکندگی منشا حملات، و غیره

---

[۱] فضای تبادل اطلاعات

[2] Computer Emergency Response Team

[۳] آگاهی‌رسانی، پشتیبانی و امداد در زمینه امنیت فضای تبادل اطلاعات

[۴] امنیت فضای تبادل اطلاعات

- ارائه راهنمایی‌هایی برای کاربران نهایی و ناآگاه از بحث امنیت

## ۲-۵- آموزش

هدف از ارائه این بخش گسترش دانش در زمینه افتا از طریق ارائه مقاله، پوستر، خودآموز و خبرنامه، راه‌اندازی و به‌روزرسانی وب‌گاه، برگزاری سمینار و کارگاه‌های آموزشی، و ارائه دوره‌های آموزشی است.

## ۲-۶- مشاوره امنیتی

هدف این بخش ارائه توصیه‌ها، راهنمایی‌ها و مشاوره‌های امنیتی به سازمان‌های دولتی و شرکت‌های خصوصی است.

## ۲-۷- آزمون نفوذپذیری

از مهمترین و کاربردی‌ترین خدمات آپای فردوسی، ارزیابی امنیتی شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری برای کشف آسیب‌پذیری‌های بالقوه و ارائه راه‌کارهایی برای رفع آن‌ها به متقاضیان است که تحت عنوان آزمون نفوذپذیری[5] مطرح می‌شود. آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد برای این آزمون‌ها مبتنی بر استانداردهای بین‌المللی و بر اساس چارچوب مستندسازی‌شده اقدام می‌کند و گزارش این آزمون‌ها را در قالبی تخصصی و فنی همراه با شرح آسیب‌پذیری‌ها و راه‌حل‌های آن به بالاترین مسئول سازمان یا شرکت متقاضی با طبقه‌بندی «خیلی محرمانه» ارسال می‌کند. استاندارد و چارچوب این آزمون در ادامه می‌آید.

### ۲-۷-۱- آزمون نفوذپذیری برنامه‌های کاربردی تحت وب مبتی بر استاندارد OWASP ASVS در سطح 1A+

استاندارد ASVS[6] مجموعه‌ای از راهبردها و الزامات ایجاد امنیت در برنامه‌های کاربردی تحت وب می‌باشد که بر مبنای نیاز به یک معیار کامل، جامع و در عین حال کاربردی و قابل استفاده برای ارزیابی امنیت این برنامه‌ها ایجاد گردیده است. این استاندارد بخشی از پروژه‌ای جهانی با نام OWASP[7] است که گردانندگان آن با توجه به پیشرفت‌های سریع در عرصه فناوری اطلاعات، هر سال نگارش جدیدی از این استاندارد را ارائه می‌دهند[۲].

در یک نگاه کلی، ویژگی‌های منحصر به‌فرد این استاندارد به شرح زیر است:

۱. قابلیت بسیار بالا برای استفاده به‌عنوان معیاری تعیین کننده سطح امنیت در جزیی‌ترین مؤلفه‌های برنامه‌های کاربردی تحت وب
۲. روشن‌بودن روش پیاده‌سازی و سازگارکردن کنترل‌های امنیتی برنامه‌های کاربردی تحت وب با الزامات استاندارد
۳. قابلیت استفاده از آن در قراردادها برای تعیین خصوصیات امنیتی مورد انتظار کارفرما از محصولات تحت وب

استاندارد ASVS به طور طبیعی بر مبنای مجموعه‌ای از الزامات شکل گرفته است. هر یک از این الزامات مشخص‌کننده یک ویژگی خاص امنیتی در برنامه‌های کاربردی تحت وب و مجموعه آن‌ها لازمه توسعه یک برنامه کاربردی امن است. این الزامات در چهار سطح بیان شده و هریک از این سطوح، شامل مواردی است که بررسی انطباق و سازگاری برنامه کاربردی با آن‌ها دقت عمل و عمق بررسی مشخص و تعیین شده‌ای را می‌طلبد.

الزامات استاندارد ASVS در چهار سطح طبقه‌بندی شده‌اند. در سطوح ۱ و ۲ این استاندارد که هر یک به دو زیرمجموعه A و B تقسیم می‌شود، بخش بزرگی از الزامات امنیتی مهم در برنامه‌های کاربردی تحت وب گنجانده شده است. سطوح ۳ و ۴ این استاندارد شامل بررسی‌هایی است که بایستی در روند توسعه برنامه کاربردی صورت پذیرند. بنابراین، آزمون نفوذپذیری برنامه‌های کاربردی تحت وب به طور طبیعی به سطوح ۱ و ۲ محدود می‌شود.

با این که جداسازی این سطوح بر اساس سطح امنیت مورد انتظار از برنامه کاربردی صورت گرفته است، نوع بررسی‌های متناظر با هر سطح نیز با سطح دیگر کاملاً متفاوت می‌باشد و بر همین اساس، سطح دسترسی به برنامه کاربردی مهم‌ترین عامل تعیین‌کننده ویژگی‌های قابل بررسی است.

آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد، آزمون نفوذپذیری برنامه‌های کاربردی تحت وب را بر اساس استاندارد ASVS در سطح 1A+ انجام می‌دهد. سطح 1A+ دربرگیرنده الزامات سطح 1A و برخی الزامات سطح 2A است که به تشخیص آزمایشگاه برای

[5] Penetration Test
[6] Application Security Verification Standard
[7] Open Web Application Security Project

اطمینان از وجود امنیت کافی در برنامه‌های کاربردی تحت وب حیاتی است.

### ۲-۷-۲- آزمون نفوذپذیری شبکه‌های رایانه‌ای

آزمون نفوذپذیری شبکه‌های رایانه‌ای بر اساس چارچوب OSSTMM [۸] و به صورت آزمون جعبه سیاه[۹] و جعبه سفید[۱۰] انجام می‌شود. در آزمون نفوذپذیری به صورت جعبه سیاه، گروه آزمون نفوذپذیری از یک نقطه دسترسی به شبکه متصل گردیده و بدون آگاهی از جزییات سیستم‌ها، سرویس‌ها و شبکه سازمان مورد نظر و بدون دریافت هیچ‌گونه اطلاعات جانبی در مورد سیاست‌ها، تصمیمات و موارد مشابه، بررسی‌های لازم را در جهت کشف مشکلات امنیتی و نقاط آسیب‌پذیر آغاز می‌نماید. در آزمون جعبه سفید، تیم آزمون نفوذپذیری با آگاهی کامل از ساختار و معماری شبکه و با دسترسی کامل به سیستم‌ها و تجهیزات شبکه اقدام به بررسی مشکلات امنیتی موجود می‌نماید[۳].

### ۲-۸- صدور گواهی‌نامه امنیتی

آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد برای برنامه‌های کاربردی تحت وب، گواهی‌نامه امنیتی مبتنی بر استاندارد OWASP ASVS در سطح 1A+ صادر می‌کند. همان‌گونه که در بخش آزمون نفوذپذیری و در معرفی این استاندارد گفته شد، در هر برنامه کاربردی و در روند آزمون نفوذپذیری و صدور گواهی‌نامه نسبت به ارزیابی آسیب‌پذیری‌ها و تعیین موارد عدم سازگاری با استاندارد اقدام می‌شود و در نهایت و پس از سازگاری با استاندارد، صدور گواهی‌نامه امنیتی صورت می‌گیرد.

### ۲-۹- ارائه طرح جامع امنیت شبکه

یکی از اساسی‌ترین و مهم ترین مراحل ایجاد امنیت در بستر فناوری اطلاعات هر سازمان شناسایی و تعیین تمهیدات امنیتی است که در طراحی، پیاده‌سازی و نگهداری از شبکه آن سازمان باید مورد توجه قرار گیرد. این تمهیدات در شبکه‌های رایانه‌ای در قالب طراحی زیرساخت شبکه[۱۱]، توزیع[۱۲] سرویس‌ها[۱۳]، پیکربندی[۱۴] سرویس‌دهنده‌ها[۱۵] و تجهیزات شبکه و در نهایت تدوین سیاست‌های[۱۶] مشخص در نگهداری از آن‌ها قابل بیان است. بدیهی است که این موارد ارتباط تنگاتنگی با نیازمندی‌های غیرامنیتی شبکه داشته و تحت تأثیر پارامترهایی چون گستردگی شبکه، حساسیت اطلاعات مبادله شده و عملیات انجام گرفته در بستر فناوری اطلاعات سازمان، محدودیت‌های ناظر بر منابع مالی و انسانی و موارد مشابه هستند. از این رو تمهیدات بیان شده نمی‌توانند صرفاً بر اساس نیازمندیهای و اهداف امنیتی تعیین گردند. این موضوع باعث تبدیل و تکامل یک مجموعه تمهیدات امنیتی از پیش تعیین‌شده به طرح امنیتی جامعی می‌شود که بر اساس تمامی شرایط شبکه هدف مهندسی و طراحی شده و ناظر بر تمامی محدودیت‌ها است. ارائه چنین طرحی در مرحله نخست نیازمند برخورداری از دانش فنی و مهارت کافی در زمینه شناخت کاستی‌های امنیتی شبکه‌ها و سیستم‌های رایانه‌ای و روش‌های اصولی رفع آن‌ها است. در مرحله دوم، کسب اطلاعات کافی از تمامی پارامترهای تأثیرگذار در شبکه برای رسیدن به نگرشی درست و جامع از بستر هدف الزامی است.

بر این اساس آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد نیز بنا به رسالت خود در زمینه افتا نسبت به تهیه و تدوین طرح امنیت شبکه برای سازمان‌های متقاضی اقدام می‌نماید. این طرح بر اساس نیازمندی‌ها و شرایط فعلی شبکه سازمان موردنظر تدوین گردیده و اولویت‌های زیر در تمامی مراحل مهندسی و طراحی آن مد نظر قرار می‌گیرد.

۱. برخورداری از شالوده امنیتی قوی و کافی برای جلوگیری از حملات متداول در شبکه‌های رایانه‌ای
۲. رفع مشکلات و نواقص امنیتی فعلی شبکه سازمان موردنظر بر اساس نتایج آزمون نفوذپذیری
۳. هماهنگی با استانداردها، روش‌های اصولی و پایه‌ای طراحی شبکه‌ها و پیاده‌سازی تمهیدات امنیتی در آن‌ها
۴. ایجاد بستر مناسب برای گسترش شبکه و همچنین افزودن ویژگی‌ها، قابلیت‌ها و تمهیدات امنیتی بیش‌تر در آینده
۵. همخوانی هر چه بیشتر با شرایط فعلی شبکه سازمان

[8] Open-Source Security Testing Methodology Manual
[9] Black Box
[10] White Box
[11] Infrastructure
[12] Distribution
[13] Services
[14] Configuration
[15] Servers
[16] Policies

۶. کاهش هر چه بیشتر هزینه لازم برای پیاده‌سازی طرح و استفاده بهینه از تجهیزات و امکانات فعلی شبکه

## ۳- گزارش عملکرد

هم‌اکنون آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد در سال چهارم فعالیت‌های خود است و با وجود عمر کمی که از تاسیس، آماده‌سازی و بهره‌برداری آن می‌گذرد، به یاری خدا و تلاش مدیران و مجموعه کارشناسان آزمایشگاه توانسته است دستاوردهای چشمگیری در حوزه افتا داشته باشد که در ادامه به تفصیل به برخی از آنان خواهیم پرداخت.

فعالیت‌های آپای فردوسی را باید در ۲ مرحله بررسی نمود.

۱. خرداد ۱۳۸۷ الی آذر ۱۳۸۸

در این مرحله که با حمایت موسسه تحقیقات ارتباطات و فناوری اطلاعات[۱۷] همراه بود ضمن نهادینه‌سازی موضوع افتا در ساختار حاکمیتی، اجرایی و آموزشی استان خراسان رضوی و استان‌های همجوار و همچنین شرکت‌های خصوصی فعال فاوا[۱۸]، اقداماتی مانند آماده‌سازی و تجهیز آزمایشگاه و فعالیت‌هایی از قبیل انتشار دانش در قالب مقاله‌های علمی و آموزشی، انتشار آسیب‌پذیری‌ها، انتشار اخبار، و برگزاری دوره‌های آموزشی انجام پذیرفت.

۲. آذر ۱۳۸۸ تاکنون

با توجه به ایجاد امکانات و تامین نیروی انسانی آموزش دیده در مرحله قبل ، فعالیت‌های آپای فردوسی وارد مرحله جدیدی شد. در این مرحله ارتقای امنیت سامانه‌ها و شبکه‌های رایانه‌ای سازمان‌های دولتی و اجرایی مورد توجه قرار گرفت و طرح‌هایی با استانداری خراسان رضوی در این زمینه اجرایی شد. همچنین آزمون نفوذپذیری سامانه‌ها و شبکه‌های رایانه‌ای، صدور گواهی‌نامه امنیتی برای برنامه‌های کاربردی تحت وب و ارائه طرح جامع امنیت شبکه رایانه‌ای بر مبنای تقاضای متقاضیان در دستور کار قرار گرفت. برگزاری سمینارها، کارگاه‌ها و دوره‌های آموزشی و شرکت در نمایشگاه‌های تخصصی و معرفی فعالیت‌ها و دستاوردهای آپای فردوسی از دیگر برنامه‌های این مرحله است.

### ۳-۱- ساختار آزمایشگاه

بنا بر اهداف شکل‌گیری آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد در ساختار سازمانی آن و پس از مدیریت آزمایشگاه، ۳ حوزه عملیات، روابط عمومی و اجرایی طراحی شد که ضمن انجام فعالیت‌های تخصصی خود در تعامل با یکدیگر نیر نسبت به اجرای سیاست‌ها اقدام می‌کنند [۴،۵،۶].

فعالیت‌های اصلی آپای فردوسی در حوزه عملیات تعریف شد و بر این اساس گروه‌های رسیدگی به حوادث، بررسی آسیب‌پذیری‌ها، آزمون نفوذپذیری، تحقیق و پژوهش، آموزش و تحریریه فنی در این حوزه تعریف شدند.

از مهم‌ترین فعالیت‌های مراکز آپا، آگاهی‌رسانی و اقدامات ترویجی است. بر این مبنا حوزه روابط عمومی در آپای فردوسی وظیفه آگاهی‌رسانی، اطلاع‌رسانی، تهیه، تدوین و ارائه گزارش‌ها، مدیریت دوره‌های آموزشی، شرکت در نمایشگاه‌های تخصصی مرتبط، به‌روزرسانی وب‌گاه و انتشار خبرنامه را بر عهده دارد.

حوزه اجرایی نیز وظیفه ارتباط و تعامل با سازمان‌های دولتی و خصوصی و پشتیبانی اداری و مالی از فعالیت‌های آزمایشگاه را بر عهده دارد.

### ۳-۲- فعالیت‌های آگاهی‌رسانی، پشتیبانی و امداد

در آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد فعالیت‌هایی از قبیل شناسایی رخدادهای امنیتی، کشف و انتشار آسیب‌پذیری‌ها، انتشار دانش، رسیدگی و کمک به سازمان‌های مختلف در هنگام بروز حوادث ناشی از حملات و رخدادهای امنیتی، ارزیابی امنیتی و انجام آزمون نفوذپذیری بر روی شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری، ارائه طرح امنیت برای امن‌سازی شبکه‌های رایانه‌ای، و خدمات آگاهی‌رسانی و آموزش عمومی و تخصصی مرتبط ارائه می‌شود. همچنین از دستاوردهای مهم فعالیت‌های آپای فردوسی می‌توان به عضویت در کمیسیون‌ها، کمیته‌ها و کارگروه‌های تخصصی در استان و اظهار نظر کارشناسی در پرونده‌های قضایی اشاره نمود. در جدول ۱ برخی فعالیت‌های آپای فردوسی از ابتدای فعالیت تا دی‌ماه ۱۳۹۰ ذکر شده است[۷].

[۱۷] مرکز تحقیقات مخابرات ایران

[۱۸] فناوری اطلاعات و ارتباطات

**شکل (۱) : فعالیت‌های آپای فردوسی**

| نوع فعالیت | تعداد |
|---|---|
| برگزاری سمینارها و دوره‌های آموزشی | ۲۴ |
| برگزاری سمینارهای تخصصی ویژه اعضا | ۴۰ |
| آزمون نفوذپذیری سرویس‌ها | ۸ |
| انتشار مقاله‌های اعتبارسنجی آسیب‌پذیری | ۵ |
| انتشار مقاله‌های علمی و آموزشی | ۷۸ |
| انتشار گزارش آسیب‌پذیری | ۱۸۴ |
| انتشار اخبار و رویدادها | ۸۰۰ |
| انتشار سوال‌های متداول (FAQs) در پورتال | ۹۶ |
| گروه‌های بحث در پورتال | ۵۰ |
| همکاری با پلیس آگاهی استان (پرونده) | ۳۰ |
| عضویت در کمیته‌های تخصصی مرتبط در استان | ۴ |

از فعالیت‌های دیگر آپای فردوسی آزمون نفوذپذیری سامانه‌ها و شبکه‌های رایانه‌ای و صدور گواهی‌نامه امنیتی برای برنامه‌های کاربردی تحت وب است که در جدول ۲ این فعالیت‌ها نیز ذکر شده است.

**شکل (۲) : خدمات ارزیابی و آزمون آپای فردوسی**

| نوع فعالیت | تعداد |
|---|---|
| آزمون نفوذپذیری شبکه‌های رایانه‌ای | ۲۱ |
| آزمون نفوذپذیری سامانه‌های نرم‌افزاری | ۴۰ |
| صدور گواهی‌نامه امنیتی برای برنامه‌های کاربردی تحت وب | ۴ |
| ارائه طرح جامع امنیت شبکه‌های رایانه‌ای | ۳ |

## ۴- دستاوردها آپای فردوسی و کسب مرجعیت استانی

- فعالیت‌های آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد گستره گوناگونی را از ارزیابی امنیتی و آزمون نفوذپذیری شبکه‌ها و سامانه‌ها، صدور گواهی‌نامه امنیتی، ارائه طرح امنیت شبکه و آگاهی‌رسانی و آموزش‌های تخصصی تا عضویت در کمیته‌ها و کارگروه‌های تخصصی در استان و اظهار نظر کارشناسی در پرونده‌های قضایی شامل می‌شود. این گستره فنی و مورد نیاز فعالان دولتی و خصوصی فاوا در استان خراسان رضوی به همراه سابقه درخشان علمی و پژوهشی مدیریت آپای فردوسی موجب رشد سریع فعالیت‌های آن و کسب مرجعیت استانی در زمینه افتا را به همراه داشت که در قالب دستاوردهای زیر قابل طرح است.
- نهادینه‌سازی افتا و نظام آپا در مدیریت کلان استان خراسان رضوی
- آشنایی مدیران کلان و مدیران فناوری اطلاعات سازمان‌های اجرایی استان خراسان رضوی با اهمیت افتا و کارکرد آپا
- افزایش اهمیت امنیت اطلاعات در بین شرکت‌های ارائه‌دهنده خدمات سخت‌افزاری و نرم‌افزاری و خدمات آپا به این شرکت‌ها
- آگاه‌نمودن بخشی از کارشناسان سازمان‌های اجرایی با اهمیت افتا
- ایجاد انگیزه برای دانشجویان مهندسی کامپیوتر برای انتخاب گرایش‌های مرتبط با امنیت و ادامه تحصیل در این گرایش
- دعوت از آپای فردوسی برای حضور در نمایشگاه‌های تخصصی فاوا و ارائه سمینارهای آموزشی مرتبط در آن‌ها

### ۴-۱- نهادینه‌سازی افتا و نظام آپا در مدیریت کلان استان خراسان رضوی

با ایجاد آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد و عضویت مدیریت آزمایشگاه در کمیسیون فناوری اطلاعات استان خراسان رضوی به عنوان نهاد تصمیم‌ساز در حوزه فاوای استان، موضوع افتا به یکی از دغدغه‌های این کمیسیون تبدیل شد و مصوبه‌های گوناگونی در این زمینه مطرح شد که با توجه به استقرار دبیرخانه این کمیسیون در استانداری خراسان رضوی، مصوبه‌های این کمیسیون از اعتبار اجرایی بالایی برخوردار است. بخشی از مصوبات این کمیسیون که مرتبط با افتا است، در ادامه می‌آید.

- ارزیابی و ممیزی امنیتی شبکه، پورتال و نرم‌افزارهای دستگاه‌های اجرایی استان در سال‌های ۱۳۸۹ و ۱۳۹۰

- برگزاری دوره‌های آموزشی برای کارشناسان فناوری اطلاعات دستگاه‌های اجرایی توسط آپای فردوسی
- لزوم اخذ تائیدیه آپا برای کلیه سامانه‌های نرم‌افزاری تحت وب دستگاه‌های دولتی استان
- استقرار ISMS در دستگاه‌های اجرایی استان
- اجرای طرح‌های امنیتی در دستگاه‌های اجرایی (بر اساس ارزیابی‌های انجام شده)
- فرهنگ‌سازی و آگاه‌سازی کاربران در خصوص امنیت اطلاعات
- تهیه ضوابط و آئین‌نامه‌های امنیت داده‌ها و اطلاعات

پیرو مصوبات کمیسیون فناوری اطلاعات استان و سیاست‌های کلان کشور در زمینه افتا، استاندار خراسان رضوی نیز طی بخش‌نامه شماره ۳۸/۱/۴۷۷۸۶ مورخ ۱۳۸۸/۱۱/۵ مجریان و پیمانکاران پروژه‌های نرم‌افزاری دستگاه‌های اجرایی استان را موظف نمود نسبت به انجام ممیزی و دریافت تائیدیه امنیت نرم‌افزار از طریق آپا اقدام نمایند.

این بخش‌نامه نقطه‌عطفی در تصمیم‌سازی‌های مرتبط با افتا در کشور محسوب می‌شود که ضمن ایجاد دغدغه امنیت اطلاعات و لزوم کاربست آن در انجام پروژه‌های نرم‌افزاری، بر نقش آپا نیز در این روند تاکید می‌نماید.

## ۴-۲- آشنایی مدیران کلان و مدیران فناوری اطلاعات سازمان‌های اجرایی استان خراسان رضوی با اهمیت افتا و کارکرد آپا

با توجه به رسالت آپای فردوسی و با هدف آشنایی مدیران و کارشناسان فناوری اطلاعات استان در بخش‌های دولتی و خصوصی با مقوله افتا، گردهم‌آیی فصلی کارشناسان فناوری اطلاعات استان در تاریخ آبان ۱۳۸۸ به میزبانی آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد و با موضوع امنیت اطلاعات و داده‌ها برگزار شد. در این گردهم‌آیی که حدود ۲۰۰ تن از مدیران و کارشناسان فناوری اطلاعات استان حضور داشتند دو سخنرانی توسط آپای فردوسی انجام شد.

پیرو این جلسه، بخش‌نامه استاندار خراسان رضوی و تصویب طرح ارزیابی امنیتی سامانه‌ها و شبکه‌های رایانه‌ای دستگاه‌های اجرایی استان در کمیسیون فناوری اطلاعات، جلسه توجیهی چگونگی انجام این طرح در اسفند ۱۳۸۸ با حضور کارشناسان فناوری اطلاعات دستگاه‌های دولتی برگزار شد و با طی مقدمات و تعیین دستگاه‌های هدف، اجرای طرح برای ۲۵ شبکه رایانه‌ای، ۱۵ پورتال و ۱۰ برنامه کاربردی تحت وب در سال ۱۳۸۹ انجام شد. همچنین در سال ۱۳۹۰ نیز این طرح برای ۱۵ شبکه رایانه‌ای، ۲۰ پورتال و ۲۰ برنامه کاربردی تحت وب نیز تصویب شد که در حال اجرا می‌باشد.

## ۴-۳- افزایش اهمیت امنیت اطلاعات در بین شرکت‌های ارائه‌دهنده خدمات سخت‌افزاری و نرم‌افزاری و خدمات آپا به این شرکت‌ها

در ادامه سیاست‌ها و تدابیر اجرایی آپای فردوسی برای ارتقای سطح امنیت اطلاعات، فعالیت‌هایی نیز برای ارتقای شرکت‌های بخش خصوصی فاوا در زمینه امنیت انجام شد که می‌توان به برخی از آن‌ها اشاره کرد.

- ارتباط و تعامل با سازمان نظام صنفی رایانه‌ای استان خراسان رضوی به عنوان پارلمان بخش خصوصی فاوا در استان
- حضور در نمایشگاه کامپیوتر مشهد در سال‌های ۱۳۸۸، ۱۳۸۹ و ۱۳۹۰ و برگزاری سمینارهای آموزشی با عنوان‌های زیر
  - امنیت نرم‌افزارهای کاربردی تحت وب
  - دیواره آتش
  - جاسوسی در فضای سایبر
  - مدیریت امنیت اطلاعات
  - آگاهی‌های امنیتی سامانه‌ها و شبکه‌های رایانه‌ای
  - تحلیل بدافزارها
- حضور در نمایشگاه شهر الکترونیکی (الهسیت) در سال ۱۳۹۰
- برگزاری کارگاه‌ها و دوره‌های آموزشی در سال‌های ۱۳۸۸، ۱۳۸۹ و ۱۳۹۰ با عنوان‌های زیر
  - امنیت داده‌ها و اطلاعات
  - امنیت در برنامه‌های کاربردی تحت وب
  - پیکربندی امن تجهیزات شبکه
  - لینوکس و پیکربندی امن آن
  - آشنایی با پیکربندی امن تجهیزات سوئیچ و روتر
  - پیکربندی امن MS ISA Serve

- Microsoft Forefront & MikroTik o
- مشاوره به شرکت‌های متقاضی برای امن‌سازی نرم‌افزارها
- صدور گواهی‌نامه امنیتی برای برنامه‌های کاربردی تحت وب

## ۴-۴- آگاه‌نمودن بخشی از کارشناسان سازمان‌های اجرایی با اهمیت افتا

در راستای فعالیت‌های آگاه‌سازی در زمینه مخاطرات امنیتی فتا، دوره آموزش مجازی آگاهی‌های امنیتی سامانه‌ها و شبکه‌های رایانه‌ای به صورت لوح فشرده چندرسانه‌ای تهیه و تدوین شد. این دوره برای کاربران معمولی رایانه‌ها به خصوص کارشناسان دستگاه‌های اجرایی تهیه شد و به غیر از ارائه به صورت لوح فشرده در سامانه آموزش مجازی آپای فردوسی به نشانی http://educert.um.ac.ir نیز قرار گرفته است. این دوره آموزشی با این هدف تدوین شده است که کاربر معمولی فتا با آسیب‌پذیری‌های بالقوه و مخاطرات امنیتی آشنا شود.

## ۴-۵- ایجاد انگیزه برای دانشجویان مهندسی کامپیوتر برای انتخاب گرایش‌های مرتبط با امنیت و ادامه تحصیل در این گرایش

در بستر فعالیت‌های آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد بسیاری از اعضای هیات علمی، دانشجویان دکتری، کارشناسی ارشد و کارشناسی از تمامی دانشگاه‌های شهر مشهد و حتی برخی دانشگاه‌های دیگر همکاری داشتند که موجب گرایش دانشجویان مهندسی کامپیوتر به موضوع امنیت و انتخاب آن به‌عنوان گرایش تخصصی در ادامه تحصیل شد. از طرفی با تاکید فضای مدیریتی و کسب‌وکاری استان بر مقوله افتا و ایجاد فضای کاری مناسب، انگیزه‌های فراوانی برای فعالیت در این زمینه به‌وجود آمد.

## ۴-۶- دعوت از آپای فردوسی برای حضور در نمایشگاه‌های تخصصی فاوا و ارائه سمینارهای آموزشی مرتبط در آن‌ها

مرجعیت آپای فردوسی در زمینه افتا موجب دعوت مسئولان نمایشگاه‌های تخصصی کامپیوتر از این آزمایشگاه برای حضور در نمایشگاه‌ها و ارائه سمینارهای آموزشی مرتبط در آن‌ها شد. این دعوت با هدف ارائه فعالیت‌های تخصصی فاوا و ارائه موضوع‌های مرتبط با افتا در نمایشگاه‌ها و جذب بازدیدکننده تخصصی صورت می‌گرفت و آزمایشگاه آپا دانشگاه فردوسی نیز در راستای فعالیت‌های ترویجی خود در نمایشگاه‌های زیر شرکت نمود.

- نمایشگاه کامپیوتر، اینترنت، تجارت الکترونیک و ماشین‌های اداری مشهد (COMEX) در سال‌های ۱۳۸۸، ۱۳۸۹ و ۱۳۹۰
- نمایشگاه IT و شهر الکترونیکی (elecit) در سال ۱۳۹۰
- نمایشگاه پژوهش و فناوری در سال‌های ۱۳۸۸، ۱۳۸۹ و ۱۳۹۰

## ۵- نتیجه‌گیری

همان‌گونه که در این مقاله اشاره شد آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد از سال ۱۳۸۷ با هدف فعالیت در زمینه افتا آغاز به کار نموده است و فعالیت‌هایی از جمله شناسایی رخدادهای امنیتی، کشف و انتشار آسیب‌پذیری‌ها، انتشار دانش، رسیدگی و کمک به سازمان‌های مختلف در هنگام بروز حوادث ناشی از حملات و رخدادهای امنیتی، ارزیابی امنیتی و انجام آزمون نفوذپذیری بر روی شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری، صدور گواهی‌نامه امنیتی برای برنامه‌های کاربردی تحت وب، ارائه طرح امنیت برای امن‌سازی شبکه‌های رایانه‌ای، و خدمات آگاهی‌رسانی و آموزش عمومی و تخصصی مرتبط توسط آن انجام می‌شود.

آپای فردوسی در راستای اهداف کلان و بخشی خود و با اتخاذ سیاست‌های کاری و تعامل مناسب با مجموعه تصمیم‌سازان فاوا در استان خراسان رضوی توانست نقش محوری در این استان ایفا نموده و به عنوان مرجع اقدام‌های مرتبط با افتا شناخته شود. بخشی از این اقدام‌ها و فعالیت‌ها در این مقاله ارائه گردید که به سبب آن دستاوردهای زیر حاصل شده است.

- نهادینه‌سازی افتا و نظام آپا در مدیریت کلان استان
- آشنایی مدیران کلان و مدیران فناوری اطلاعات سازمان‌های اجرایی استان خراسان رضوی با اهمیت افتا و کارکرد آپا
- افزایش اهمیت امنیت اطلاعات در بین شرکت‌های ارائه‌دهنده خدمات سخت‌افزاری و نرم‌افزاری و خدمات آپا به این شرکت‌ها

- آگاه‌نمودن بخشی از کارشناسان سازمان‌های اجرایی با اهمیت افتا
- ایجاد انگیزه برای دانشجویان مهندسی کامپیوتر برای انتخاب گرایش‌های مرتبط با امنیت و ادامه تحصیل در این گرایش
- دعوت از آپای فردوسی برای حضور در نمایشگاه‌های تخصصی فاوا و ارائه سمینارهای آموزشی مرتبط در آن‌ها

## مراجع

[۱] مرکز تحقیقات مخابرات ایران، اولین کنفرانس حوادث و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات، تهران، مرکز تحقیقات مخابرات ایران، ۱۳۸۸.

[2] OWASP, Application Security Verification Standard 2009 – Web Application Standard, www.owasp.org.

[3] ISECOM, Open-Source Security Testing Methodology Manual, 2006.

[4] Chris Alberts, Audrey Dorofee, Georgia Killcrece, Robin Ruefle, Mark Zajicek, Defining Incident Management Processes for CSIRTs: A Work in Progress, TECHNICAL REPORT CMU/SEI-2004-TR-015 ESC-TR-2004-015, October 2004.

[5] Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek, State of the Practice of Computer Security Incident Response Teams (CSIRTs), TECHNICAL REPORT CMU/SEI-2003-TR-001 ESC-TR-2003-001, October 2003.

[6] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek, Handbook for Computer Security Incident Response Teams (CSIRTs), HANDBOOK CMU/SEI-2003-HB-002, First release: December 1998, 2nd Edition: April 2003.

[7] http://cert.um.ac.ir

This page is intentionally left blank