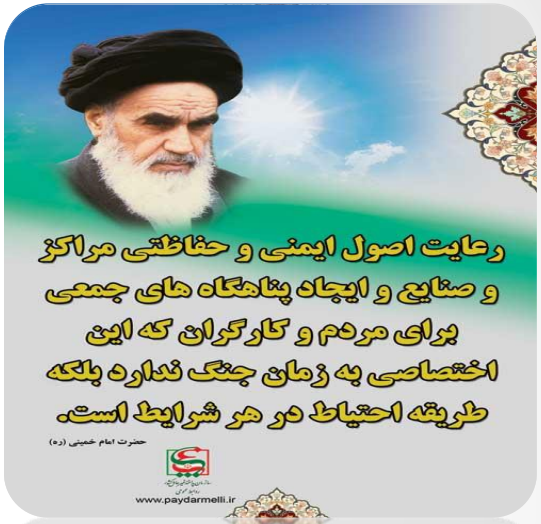

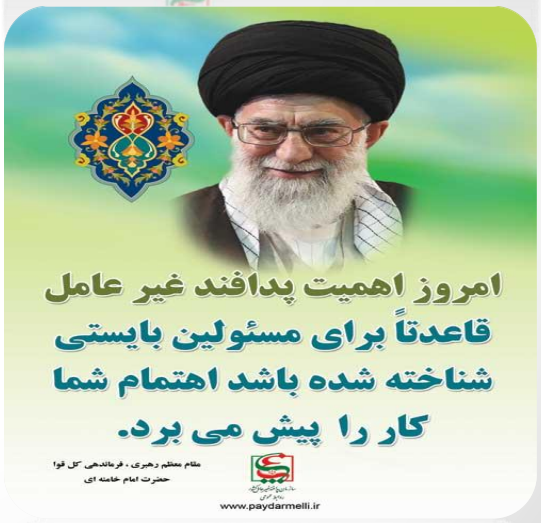

پدافند غیر عامل

پدافند غیر عامل یا دفاع غیر عامل به مجموعه اقداماتی اطلاق می گردد که به استفاده از جنگ افزار فیزیکی نیاز تدارد و با اجرای صحیح آن می توان از وارد شدن خسارت جلوگیری کرد و یا میزان این خسارت را به حداقل ممکن کاهش داد.

پدافند سایبری

به مجموعه اقداماتی گفته می شود که موجب بازدارندگی ، پیشگیری ، ممانعت از انجام ، تشخیص به موقع ، مقابلعه موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه های ملی سایبری ، توسط متخامصین سایبری ، اعم از نیروهای نظامی (ارتش سایبری ، کشورهای متخاصم ، گروه های تحت حمایت پنهان دولت های متخاصم ، جاسوسان سایبری ، تروریست های سایبری) می شود.

راهبرد های نظام پدافند سایبری کشور

- مصون سازی زیر ساخت های حیاتی و حساس کشور در مقابل تهدیدات و حملات سایبری
- ایجاد و توسعه نظام های مورد نیاز پدافند سایبری
- ارتقای کمی و کیفی منبع انسانی حوزه پدافند سایبری
- ارتقای سطح آگاهی ، دانش و مهارت های بومی و فرهنگ سازی در حوزه پدافند سایبری
- تقویت صنعت بومی و توسعه خدمات و محصولات روزآمد پدافند سایبری

سرمایه ملی سایبری

بخشی از سرمایه های های کشور است که در فضای سایبری قابل حفظ ، نگه داری و تحلیل می باشد. سرمایه های سایبری را می توان به سرمایه های سایبری حیاتی ، حساس و مهم طبقه بندی کرد.

نمونه تهدیدات سایبری

- اختلال در شبکه مخابراتی کشور (شبکه ثابت و سیار)
- اختلال و سرقت در شبکه بانکی و مالی کشور
- اختلال در شبکه انرژی کشور (برق ، آب ، گاز و ...)
- اختلال در شبکه حمل و نقل و ترافیک کشور

ویژگی های مشترک حملات ارتش های سایبری

- هدفمندی حملات
- حملات طراحی شده با شناسایی قبلی از هدف
- حملات طراحی شده با دانش فنی بالا و خیلی پیچیده

اهدافی که پدافندهای غیرعامل در حوزهٔ IT و جنگ سایبری دنبال می‌کنند

- استمرار کارکرد صحیح شبکه و سامانه‌های الکترونیکی
- ایجاد محدودیت در دسترسی غیرمجاز به اسرار و اطلاعات شخصی و عمومی
- حصول اطمینان از پایداری و خلل ناپذیری درکنترول فعالیت شبکه‌های الکترونیکی
- توسعه ظرفیت دفاع الکترونیکی در برابر تهاجم فرهنگی و نرم از طریق تقویت و گسترش شبکه‌های ملی اینترنت
- تقویت ضریب امنیت و پایداری در حوزه زیر ساخت‌ها

روش‌های کنترل شرایط و محدود کردن خسارات ناشی از حملات

- تعیین آثار نشانه‌ها و هشدارهای امنیتی
- ایمن سازی سیستم‌ها
- خاموشی و بررسی مجدد
- استفاده از خدمات پشتیبانی

روش های پیشگیری

- طراحی امن و ایمن و پایدار سیستم‌ها
- استفاده از شرکت‌های معتبر در پشتیبانی خدمات
- توقف کارکرد در زمان اطلاع از حملات
- کنترل شرایط، کاهش خسارات ناشی از حملات

آسیب پذیری های نرم افزارهای پر کاربرد

آسیب پذیری در Microsoft Office

چندین آسیب پذیری در مایکروسافت آفیس گزارش شده استا که می تواند توسط کاربران خرابکار مورد سوء استفاده قرار بگیرد تا اطلاعات حساس را افشاء نمایند و محدودیت های امنیتی خاص را دور بزنند و حملات اسکریپت بین سایتی را هدایت نمایند و کنترل یک سیستم کاربر را در اختیار بگیرند.

آسیب پذیری در Google Chrome

- یک خطای نامشخص در Blink می تواند برای دور زدن خط مشی های مبدا یکسان مورد سوء استفاده قرار بگیرد.
- یک خطای استفاده پس از آزادسازی در PDFiumمی تواند برای تخریب حافظه مورد سوء استفاده قرار بگیرد.
- یک نوع خطای تداخل در PDFium میتواند برای تخریب حافظه مورد سوء استفاده قرار بگیرد.
- آسیب پذیری در ادوب ریدر و آکروبات

آسیب پذیری در Internet Explorer

- یک خطای استفاده پس از آزادسازی هنگام مدیریت اشیاء CWindow می تواند برای تخریب حافظه مورد سوء استفاده قرار بگیرد.
- یک خطای نامشخص می تواند برای تخریب حافظه مورد سوء استفاده قرار بگیرد.
- یک خطا در موتورهای VBScript و Jscript می تواند برای ایجاد تخریب حافظه مورد سوء استفاده قرار بگیرد.

آسیب پذیری در Adobe Reader و Acrobat

- خطای استفاده پس از آزادسازی دیگری می تواند برای تخریب حافظه مورد سوء استفاده قرار بگیرد.
- یک خطای استفاده پس از آزادسازی هنگام مدیریت اشیاء U3D می تواند برای تخریب حافظه مورد.

وضعیت کمیته پدافند غیر عامل در اداره کل ارتباطات و فناوری اطلاعات استان آذربایجان شرقی

همکاری با کار گروههای تخصصی

- ارائه عملکرد در جلسه شورای برنامه ریزی استان در خصوص تهدیدات فضای سایبری و ارائه راه کار مقابله با آن
- ارائه عملکرد در جلسه شورای هماهنگی بانک ها در خصوص تهدیدات فضای سایبری و ارائه راه کار مقابله با آن
- عضویت و شرکت در جلسات کمیته جرائم سایبری به منظور پیشگیری از وقوع جرائم سایبری
- عضویت و شرکت در جلسات کار گروه انرژی و آب پدافند غیر عامل استان به منظور اتخاذ تصمیمات برای مصون ماندن زیر ساخت ها در مقابل خطرات احتمالی

اقدامات بازدارنده و مقابله با تهدیدات

- **عضو گیری ۱۱۰ نفر از مسئولین و کارشناسان فناوری اطلاعات دستگاه های اجرائی در سامانه تعاملی مرکز ماهر به منظور آگاهی رسانی و نحوه مقابله با تهدیدات سایبری**
- **نصب حسگر های هانی نت در دستگاههای اجرایی مهم و حساس به منظور شناسایی و مقابله با تهدیدات سایبری**
- **راه اندازی مرکز آپا (آگاهی رسانی ، پشتیبانی و امداد فضای سایبری) به منظور انجام پژوهش های مرتبط با امنیت فضای سایبری در دانشکده مهندسی برق و کامپیوتر دانشگاه تبریز**

- **برگزاری دوره های آموزشی برای مسئولین و کارشناسان فناوری اطلاعات استان با موضوعات گروه های واکنش رخداد امداد رایانه ای و سیستم مدیریت امنیت اطلاعات**
- **طراحی وساخت مرکز داده استان بر اساس استانداردهای بین المللی و با نظارت سازمان فناوری اطلاعات ایران**
- **تشکیل گروه های مقابله با رخدادهای رایانه ای**
- **تست نفوذ از پرتال سازمانی**
- **نصب تجهیزات سخت افزاری و نرم افزاری مقابله با حملات سایبری**

- **تعریف پروژه های مرتبط با پدافند سایبری در سند تدبیر و توسعه استان**
- **ارسال هشدارهای امنیتی فضای سایبری به دستگاه های اجرایی استان**
- **حمایت و هدایت بخش خصوصی استان برای اجرا و مشاوره سیستم مدیریت امنیت اطلاعات (ISMS)**

وزارت ارتباطات و فناوری اطلاعات

اداره کل ارتباطات و فناوری اطلاعات استان آذربایجان شرقی

http://tabriz.ict.gov.ir