پدافند غیر عامل

- اصول و مبانی پدافند غیر عامل
- بررسی نقش جنگ ها در توسعه فناوری اطلاعات و برعکس
- اصول و مبانی امنیت داده و اطلاعات
- پدافند غیر عامل در سیستم عامل و مسیریاب ها
- پدافند غیر عامل در فناوری اطلاعات

برگرفته از کتاب مهندسی پدافند غیرعامل در فناوری اطلاعات: امنیت به روش پیشگیری الکترونیکی
نویسنده: حمید دوست محمدیان، مریم سادات فاضلی

Dr. Hesamaddin Kamal Zadeh

hesamadin@HUMS.ac.ir

اصول و مبانی پدافند غیر عامل

- پدافند = پد + آفند
- پد = پاد = متقابل یا متضاد
- آفند = جنگ و جدال و دشمنی دفاع

پدافند : دفع، خنثی کردن و یا کاهش تاثیرات اقدامات آفندی دشمن و ممانعت از دستیابی به اهداف خودی است.

پدافند عامل

عبارت است از رویارویی و مقابله مستقیم با دشمن و به کارگیری جنگ افزارهای مناسب و موجود به منظور دفع حمله و خنثی کردن اقدامات آفندی دشمن می‌باشد.

پدافند عامل و استفاده از جنگ افزارها هنگام وقوع جنگ باعث بروز خسارات مالی و جانی برای افراد غیر نظامی می‌شود و همچنین باعث از بین رفتن محیط زیست و آسیب رساندن به زمین می‌شوند.

پدافند غیرعامل

«مجموعه اقدامات غیرمسلحانه‌هایی که موجب کاهش آسیب‌پذیری نیروی انسانی، ساختمان‌ها و تأسیسات، تجهیزات و شریان‌های کشور در مقابل عملیات خصمانه و مخرب دشمن و یا کاهش مخاطرات ناشی از سوانح طبیعی می‌گردد، پدافند غیرعامل نامیده می‌شود.»

پدافند غیرعامل به معنای دفاع بدون به کارگیری تجهیزات نظامی است و در عرصه مدیریت بحران ناشی از جنگ، در تسهیل مدیریت و پایداری زیرساخت‌ها نقش اساسی دارد.

وجه تمایز پدافند عامل و غیرعامل را باید عامل « انسان» دانست. پدافند عامل ابزاری است که نیاز به مدیریت مستقیم و کاربردی انسان دارد و مشتمل بر ابزار و آلات جنگی، سازماندهی، آموزش و مدیریت نیروها می‌باشد و در شرایط عدم حضور انسان، آن ابزار به خودی خود فاقد اعتبار است.

در حالی که پدافند غیرعامل امکانات معماری در زمینه مهندسی جنگ است به گونه‌ای که بدون ابزار و توانمندی، نیروی رزمی و دفاعی را افزایش دهد.

اصول و مبانی پدافند غیر عامل

به کارگیری اقدامات پدافند غیرعامل در کنار پدافند عامل، ضروری و اجتناب ناپذیر بوده و با تأمین پدافند غیرعامل می‌توان با اتخاذ تدابیر و تمهیدات لازم از وارد شدن خسارات سنگین به مراکز حیاتی، حساس و مهم کشور جلوگیری نمود.

به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارایی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

یکی از اصول اساسی دفاع غیرعامل ایجاد استحکامات و سازه‌های امن می‌باشد که نقشی اساسی در حفظ تأسیسات، تجهیزات، نیروی انسانی، مراکز حیاتی، حساس و مهم در زمان بروز تهدید ایفا نموده و می‌تواند تأثیرات بسیار چشمگیری در ارتقا توان رزمی، استمرار عملیات و بالا بردن آستانه مقاومت داشته باشد.

اصول و مبانی پدافند غیر عامل

تاریخچه پدافند غیرعامل

انسان‌های اولیه برای در امان ماندن از تهاجم حیوانات وحشی و دیگر دشمنان خود و همچنین برای کاستن از نگرانی‌های خود به غارها، بالای درختان و دیگر پناهگاه‌های طبیعی پناه بردند.

ایران: وضعیت جغرافیایی و محیط ناامن،ایرانیان را وادار نمود تا به منظور در امان بودن از حمله متجاوزین، خانه‌های مسکونی خودرا به شکل دژ کوچکی بسازند،
به هر گوشه این سرزمین نگاه کنید، قلعه، برج و بارو، ارگ، کهندژ، دربند، خندق و دروازه از ناامنی محیط زندگی و توجه و تدبیر آگاهانه ایرانیان به ملاحظات دفاعی و امنیتی حکایت دارد.

شکل ۲-۱ قلعه بابک خرم‌دین

اصول و مبانی پدافند غیر عامل

تاریخچه پدافند غیرعامل

پس از جنگ جهانی دوم، دولت آلمان توسعه پدافند غیرعامل را در دستور کار خود قرار داد.

در شوروی سابق سازمان دفاع غیرعامل در اواسط سال ۱۹۶۰ میلادی تأسیس گردید و به سرعت توسعه یافت و از سال ۱۹۶۶ با تحولی بزرگ تجدید سازمان گردید و ساخت پناهگاه‌های ضد هسته‌ای و دو منظوره کردن بسیاری از تأسیسات مانند ایستگاه‌ها و معابر مترو و پارکینگ‌های زیر زمینی از همان زمان در دستور کار قرار گرفت.

در آمریکا پس از گذشت بحران‌های برلین و کوبا در سال ۱۹۶۳ موضوع ساخت پناهگاه‌های خانگی و دسته جمعی مطرح شد و توسعه پدافند غیر عامل آمریکا به گونه‌ای بود که دفاع غیر عامل آمریکا به نام یوجین پی ویگر برنده صلح نوبل شد.

در سال‌های ریاست جمهوری کارتر و ریگان پدافند غیرعامل با تأکید بر دلایل سه‌گانه زیر مجدداً در کانون توجه دولتمردان ایالات متحده قرار گرفت.

الف– پدافند غیرعامل جزء مهمی از راهبرد بازدارندگی است.

ب– پدافند غیرعامل ابزار مفیدی برای مدیریت بحران است.

ج– پدافند غیرعامل نقطه کانونی بقای کشور محسوب می‌شود.

در کشور کانادا نیز موضوع پدافند غیرعامل مورد توجه خاصی مبذول گردیده است و دولت مرکزی وظیفه دارد در این مورد به تدوین اصول و سازماندهی تنظیم همکاری دولت و نیروهای مسلح، آموزش مسئولان و مردم، استفاده از همیاری در تدوین برنامه‌های آموزشی محلی، گسترش برنامه‌های تحقیقاتی و نمونه سازی از طرح‌ها اقدام نماید.

اصول و مبانی پدافند غیر عامل

اهداف پدافند غیرعامل

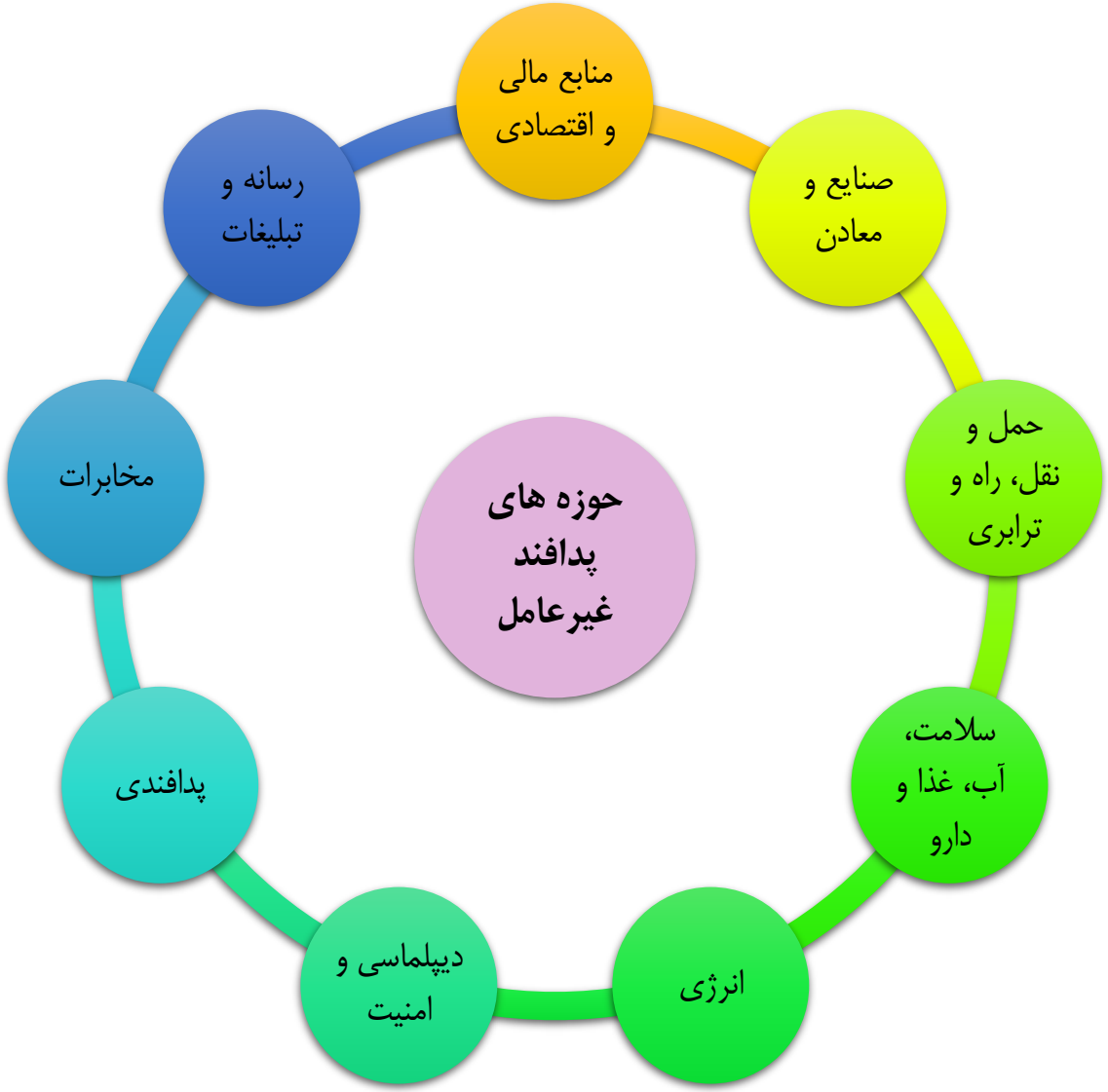
- تقلیل آسیب‌پذیری و کاهش خسارات و صدمات تأسیسات، تجهیزات و نیروی انسانی مراکز حیاتی، حساس و مهم کشور در برابر خطرات طبیعی و حملات دشمن
- حفظ سرمایه‌های کلان ملی کشور
- حفظ توان خودی جهت ادامه فعالیت‌ها و تداوم عملیات تولید و خدمات رسانی
- صرفه‌جویی در هزینه‌های نیروی انسانی
- افزایش آستانه مقاومت مردمی در برابر تهدیدات
- بالا بردن توان دفاعی کشور
- توزیع ثروت، جمعیت و سرمایه‌های ملی در کل فضای سرزمینی کشور از طریق اعمال سیاست تمرکززدایی، آمایش سرزمینی و پراکندگی زیرساخت‌های کلیدی و مراکز حیاتی، حساس و مهم تولیدی محصولات کلیدی (نیروگاهی، پالایشگاهی، صنعتی، نظامی، غذایی، آبرسانی و ...)
- آمادگی‌های لازم جهت مقابله با دشمن در شرایط تهدیدات نامتقارن
- حفظ تمامیت ارضی، امنیت ملی و استقلال کشور
- صرفه‌جویی کلان اقتصادی و ارزی در حفظ تجهیزات و سازه‌های بسیار گران قیمت می‌گردد.
- اقدامات پدافند غیرعامل موجب تحمیل هزینه بیشتر به دشمن می‌گردد.

اصول و مبانی پدافند غیر عامل

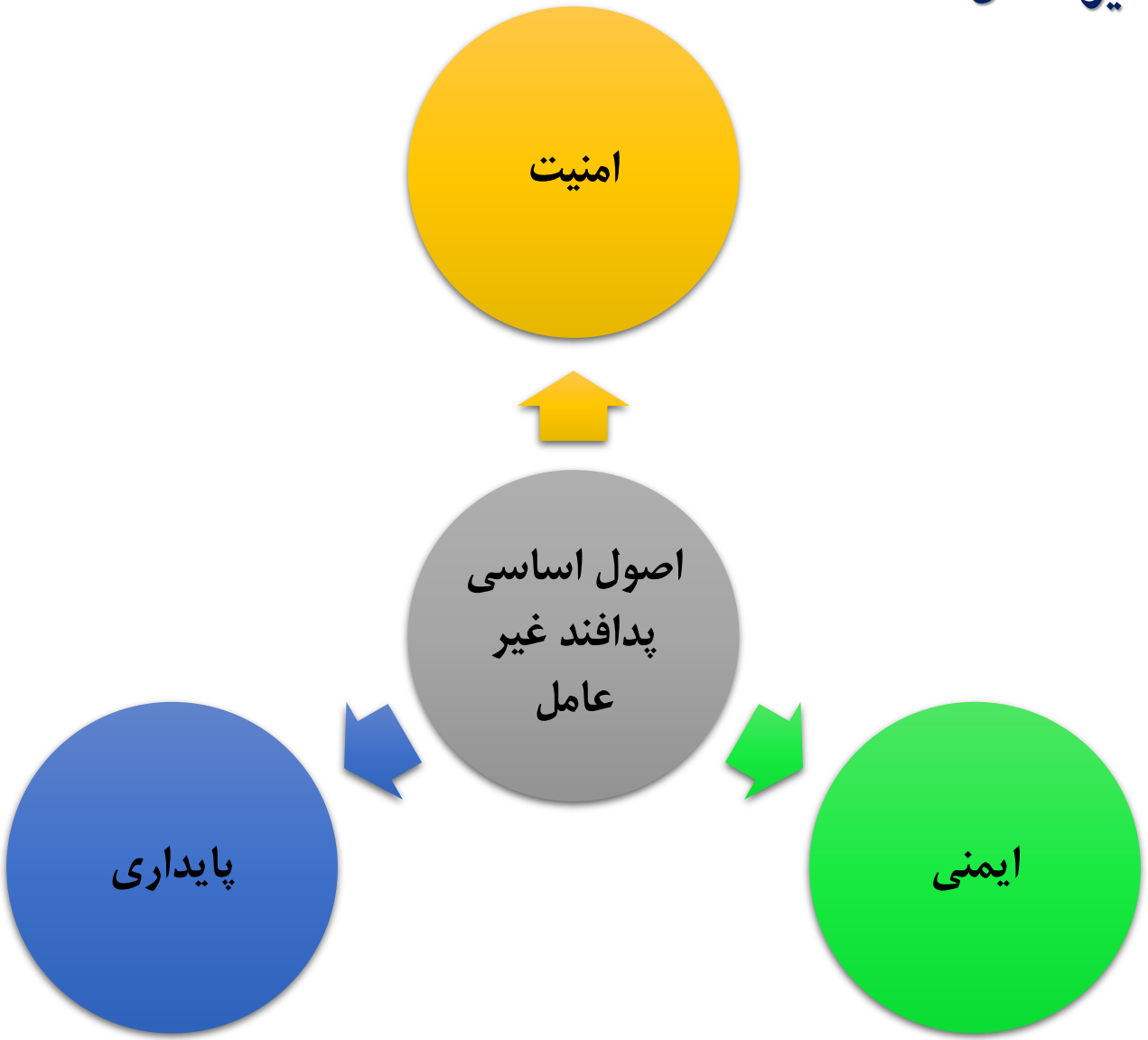
نتیجه به‌کارگیری اقدامات پدافند غیرعامل

اصول و مبانی پدافند غیر عامل

حوزه‌ها و محورهای اساسی پدافند غیرعامل

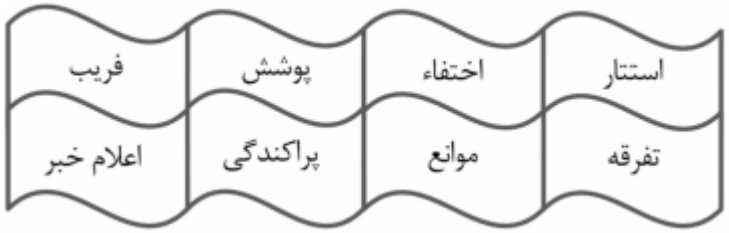


اصول و مبانی پدافند غیر عامل



اصول و مبانی پدافند غیر عامل

اصول پدافند غیرعامل



مجموعه اقدامات بنیادی و زیر بنایی است که در صورت به کارگیری می‌توان به اهداف پدافند غیرعامل از قبیل تقلیل خسارات و صدمات، کاهش قابلیت و توانایی سامانه، شناسایی، هدف یابی و دقت هدف‌گیری تسلیحات آفندی دشمن و تحمل هزینه بیشتر به وی نائل گردد.

استتار

همرنگ و همشکل کردن تأسیسات، تجهیزات و نیروها با محیط اطراف می‌باشد.

استتار دو جنبه دارد:

اول همگون کردن تأسیسات و تجهیزات با محیط اطراف که به وسیله رنگ‌آمیزی یا استفاده از مواد طبیعی و مصنوعی امکان پذیر است،

دوم با تغییر شکل ظاهریشان می‌توان توجه دشمن را از آن‌ها منحرف کرد.

شکل ۴-۱ الف) کارخانه هواپیماسازی قبل از استتار

شکل ۴-۱ ب) همان کارخانه پس از استتار

اصول و مبانی پدافند غیر عامل

اصول پدافند غیرعامل

اختفا

پنهان کردن هدف از حسگرهای دشمن می‌باشد.

اختفا، حفاظت در برابر دید دشمن را تأمین می‌نماید و استتار امکان کشف یا شناسایی نیروها، تجهیزات و تأسیسات و فعالیت‌ها را تقلیل می‌دهد.

فریب

انحراف ذهن دشمن از اهداف حقیقی و مهم به سمت اهداف کاذب و کم اهمیت می‌باشد.

کلیه اقدامات طراحی شده حیله‌گرانه‌ای است که موجب گمراهی و غفلت دشمن در نیل به اطلاعات و محاسبه و برآورد صحیح از توان کمی و کیفی طرف مقابل گردیده و او را در تشخیص هدف و هدف‌گیری با شک و تردیدی مواجه نماید.فریب،

پوشش

به‌طور کلی پوشش به عنوان پنهان‌سازی و حفاظت تأسیسات، تجهیزات، تسلیحات و نیروی انسانی در برابر دید و تیر دشمن، تعریف گردیده است اما باید توجه داشت که پوشش به عنوان بخشی از اقدامات اساسی پدافند غیرعامل مانند استتار، اختفا و فریب محسوب گردیده و قاعدتاً هر یک از این اقدامات مکمل دیگری بوده و مجموعاً می‌توانند ضامن بقای یک واحد در منطقه عملیات باشند.

اصول و مبانی پدافند غیر عامل

اصول پدافند غیرعامل

پراکندگی

گسترش، باز و پخش نمودن و تمرکززدایی نیروها، تجهیزات، تأسیسات یا فعالیت‌های خودی به منظور تقلیل آسیب‌پذیری آن‌ها درمقابل عملیات دشمن به‌طوری که مجموعه‌ای از آن‌ها هدف واحدی را برابردشمن تشکیل ندهند.

تفرقه و جداسازی

جداسازی، گسترش افراد، تجهیزات و فعالیت‌های خودی از محل استقرار اصلی به محلی دیگر به منظور تقلیل آسیب‌پذیری، کاهش خسارات و تلفات می‌باشد، مانند انتقال هواپیماهای مسافربری به فرودگاه‌های دورتر از برد سلاح‌های دشمن یا انتقال تجهیزات حساس قابل حمل از محل اصلی به محل موقت که به علت عدم شناسایی و حساسیت مکانی، دارای امنیت و حفاظت بیشتری می‌باشد.

اعلام خطر

آگاهی و هشدار به نیروهای خودی مبنی بر اینکه عملیات تعرضی قریب الوقوع دشمن، نزدیک می‌باشد، این هشدار که برای آماده شدن است چند دقیقه، چند ساعت یا زمان طولانی‌تر از آغاز مخاصمات اعلام می‌گردد. دستگاه‌های وسائل اعلام خبر شامل رادار، دیده‌بانی، آژیر، بلندگو، پیام‌ها و آگهی‌های هشدار دهنده می‌باشد.

موانع

مانع عبارت است از هر نوع عارضه زمینی، هوایی، دریایی و حالت خاصی از خاک، آب و هوا یا اشیای ساختگی غیر از قدرت آتش و تجهیزات که به منظور به تأخیر انداختن، کانالیزه کردن یا متوقف کردن حرکت دشمن به کار می‌رود.

فناوری اطلاعات

فناوری

فناوری عبارت است ازمجموعه‌ای ازفرایندها، روش‌ها، فنون، ابزار، تجهیزات، ماشین‌آلات و مهارت‌هایی که توسط آن‌ها کالایی ساخته می‌شود یا خدمتی ارائه می‌گردد .

فناوری اطلاعات ؟؟؟

فناوری اطلاعات

پس از در دسترس قرارگرفتن کامپیوتر درسال ۱۹۵۰ میلادی، اولین کاربرد علمی که کامپیوتر درآن استفاده شد انتخابات ریاست جمهوری آمریکا درسال ۱۹۵۱ بود. درسال ۱۹۶۰ با حضور ***کامپیوتر بزرگ*** ایده توسعه پایگاه‌های اطلاعاتی متمرکز اطلاعات و مفهوم انفورماتیک (داده‌پردازی) شکل گرفت و کاربرد آن درحوزه مدیریت اطلاعات طرفداران بیشتری پیدا کرد.

این ایده درسال‌های ۱۹۷۰ تا ۱۹۸۰ به‌صورت استفاده از سیستم‌های هوشمند وکمک به تصمیم‌گیری شکل قوی‌تری به خود گرفت و ایده اصلی اتوماسیون اداری و سیستم‌های بدون کاغذ را تقویت نمود. در کشورهای دیگر مثل ژاپن، آلمان، انگلستان و غیره نیز کاربردهای کامپیوتر در زمینه خدمات بانکداری، هتلداری، مدیریت پروژه‌ها و... رشد نمود.

جهانی شدن

- جهانی‌شدن یا Globalization پدیده‌ای که در آن ارتباطات، تجارت، فرهنگ و تکنولوژی به طور گسترده‌تری در سراسر جهان تاثیر می‌گذارند.
- این پدیده باعث اتصال بیشتر کشورها و مردمان به یکدیگر شده است و تأثیرات زیادی در اقتصاد، سیاست، فرهنگ و جوامع دارد.
- یکی از عوامل اصلی جهانی‌شدن، پیشرفت تکنولوژی ارتباطات است.

بررسی نقش جنگ ها در توسعه فناوری اطلاعات و برعکس

جنگ ها

جنگ یک پدیده و واقعیت اجتماعی فوق العاده پیچیده، اجتناب ناپذیر و خسارت آفرین است و از عناصر پایدار تاریخ بشری است.

نسل	سال	هدف	تسلیحات
اول (جنگ‌های اولیه)	پیش از تاریخ تا قرن ۱۵ میلادی	نیازهای فیزیولوژیکی	اعضای بدن، تیروکمان، سنگ، منجنیق و پرتابه
دوم (باروت و سلاح گرم)	سال ۱۴۵۰ الی۱۷۷۵	دلایل مذهبی یا جنگ بین حکومت‌ها	باروت و سلاح گرم
سوم (جنگ‌های صنعتی)	سال ۱۷۷۵ الی ۱۹۱۴	انگیزه‌های صنعتی و اقتصادی (حاصل فناوری)	تسلیحات صنعتی و ادوات نظامی
چهارم (جنگ‌های مکانیزه)	سال ۱۹۱۴ الی ۱۹۴۵	محصول فناوری‌های توان آور	موشک‌های هدایت شونده، رادار، هواپیما، کاربرد کشنده تانک
پنجم (جنگ‌های اتمی)	سال ۱۹۴۵ الی ۱۹۹۱	رقابت اتمی و تلاش در کسب توازن نظامی بین ابر قدرت‌ها	سلاح اتمی

جنگ ها نسل ششم

مشخصه جنگ‌های این دوره

- تأکید بر جنگ نرم (شامل جنگ‌های اطلاعاتی، جنگ روانی و تبلیغاتی، جنگ سایری)
- به کارگیری موضعی و مقطعی جنگ سخت برای تقویت و پشتیبانی جنگ نرم
- تأکید بر جنگ الکترونیک پیشرفته
- تکیه بر سلاح و تجهیزات هوشمند و پیشرفته و دقیق
- توسعه توانمندی‌ها و کسب برتری کامل در هوا
- گسترش عرصه جنگ به فضا
- پرهیز از درگیری قطعی در جنگ سخت، قبل از اطمینان از پیروزی در جنگ نرم
- شروع همزمان به نبرد در خط عمیق نزدیک و عمیق دور (گسترش عرصه نبرد به تمام سطوح جغرافیای کشور هدف)
- تأکید بر انهدام زیر ساخت‌های ملی و مراکز حیاتی، حساس و مهم در کشور در اولویت نخست اهداف تهاجم
- در تلاش مؤکد و مستمر بر قطع ارتباط رهبری و مدیریت دفاعی و عمومی کشور با مردم و نیز با نیروهای دفاعی
- کوتاه شدن مدت زمان جنگ (طراحی جنگ برق آسا)
- خطر پذیری پایین

جنگ ها نسل ششم

نقش اطلاعات در جنگ

۱- کنترل انتقال اطلاعات به طرف مقابل توسط روش‌هایی مانند فریب و پوشش که باعث ایجاد اشـتباه او گردد.

۲- استفاده از قدرت اطلاعات در جهت پیش بینی آینده

۳- استفاده از اطلاعات به منظور تأثیر در نگرش و استنباط دشمن در جهت جلوگیری از ایجـاد درگیـری فیزیکی و مهار اقدامات او

جنگ ها نسل ششم

مراکز تحت پوشش

۱- ***مراکز حیاتی*** : مراکزی هستند که در صورت انهدام کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری در سراسر کشور گردد.

۲- ***مراکز حساس*** : مراکزی هستند که در صورت انهدام کل یا قسمتی از آن ها، موجب بروز بحران، آسیب و صدمات قابل توجهی در نظام سیاسی، هدایت، کنترل و فرماندهی تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیر گذاری منطقه‌ای در بخشی از کشور گردد.

۳- ***مراکز مهم*** : مراکزی هستند که در صورت انهدام کل یا قسمتی از آن‌ها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی، دفاعی با سطح تأثیرگذاری محلی در کشور وارد می‌گردد.

جنگ ها نسل ششم

جنگ ها نسل ششم

جنگ الکترونیک

در جنگ الکترونیک از انرژی الکترومغناطیس،جهت کنترل طیف الکترومغناطیسی و تهاجم به دشمن، استفاده می‌گردد.کنترل طیف الکترومغناطیسی از طریق حفاظت از سامانه‌های خودی و مقابله با سامانه‌های دشمن حاصل می‌شود. جنگ الکترونیک صرفاً محدود به فرکانس‌های رادیویی نمی‌شود و شامل طیف اپتیکی و مادون قرمز نیز می‌گردد.

بمب‌های الکترومغناطیس

یکی از روش‌های نوین تهاجم به اطلاعات، استفاده ازبمب‌های الکترومغناطیس است که در نبردهای یوگسلاوی و نیز عراق به دفعات مورد استفاده قرار گرفت.

بمب الکترومغناطیس نور شدیدی ساطع می‌کند، در یک لحظه همه چیز در خاموشی فرو می‌رود.

جنگ ها نسل ششم

جنگ الکترونیک

آسیب پذیری در اثر بحران الکترومغناطیسی

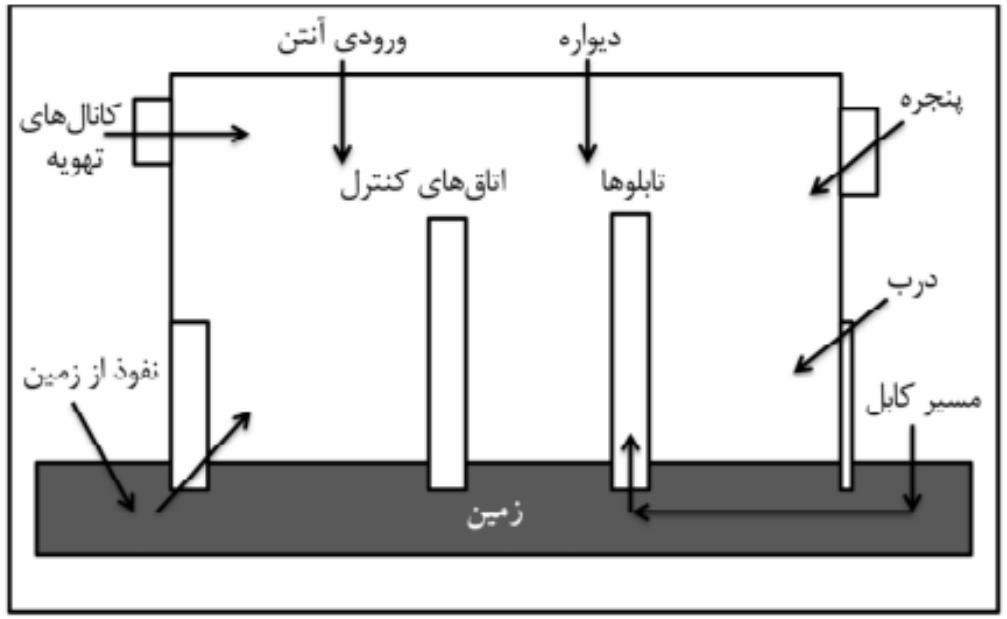
به‌طور کلی تجهیزات الکتریکی و الکترونیکی در اثر بحران الکترومغناطیسی دچار دو نوع آسیب می‌شوند:

۱- **آسیب گذرا:** این آسیب در سیستم‌های دیجیتال رخ می‌دهد و خطای بیت در هنگام ارسال یا پردازش اطلاعات نامیده می‌شود. آسیب گذرا موجب اعلام پیام خطا، عملکرد اشتباه و در بدترین شرایط راه‌اندازی مجدد سیستم‌ها می‌گردد.

۲- **آسیب دائمی:** این آسیب شامل از کار افتادن و سوختن المان‌ها و قطعات پردازشی و کنترلی (آنالوگ و دیجیتال) می‌باشد.

عدم حفاظت الکترومغناطیسی یا عدم کفایت حفاظت تجهیزات مرتبط، آن‌ها را به نقاط آسیب پذیر سیستم تبدیل می‌کند. این تجهیزات عبارت است از:

- تجهیزات الکترونیکی، مخابراتی و ارتباطی
- تجهیزات کنترلی، اعلام خطر و هشدار
- انواع پردازنده‌ها، رایانه‌ها و سرورها
- منابع تغذیه مستقیم و متناوب

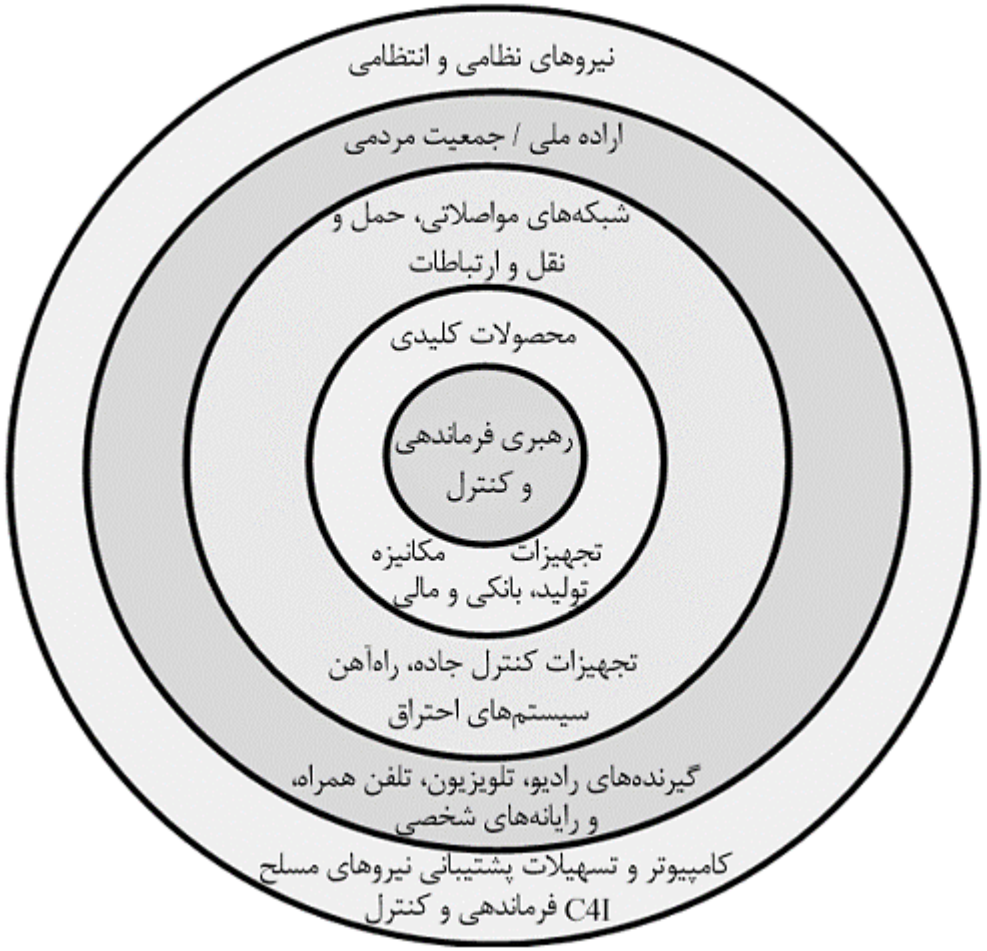


شکل ۱۰-۳ مدل کلی نفوذ پالس الکترومغناطیسی (محیط داخل)

جنگ ها نسل ششم

جنگ الکترونیک

تجهیزات آسیب‌پذیر در یک حمله الکترومغناطیسی از دیدگاه حلقه‌های واردن



جنگ ها نسل ششم

جنگ اطلاعات

Department of Defense

تعریف رسمی *DOD* از جنگ اطلاعات: شامل اقدامات لازم جهت حفظ یکپارچگی سامانه‌های اطلاعاتی خودی در مقابل بهره برداری،آلودگی و تخریب (حفاظت از اطلاعات) و از طرف دیگر تلاش برای بهره برداری،آلوده سازی و تخریب سامانه‌های اطلاعاتی دشمن(حمله اطلاعاتی) و انجام پردازش‌های لازم جهت به دست آوردن برتری اطلاعاتی در مواقع اعمال فشار (حاکمیت اطلاعات).

به طور اختصار مهم‌ترین ملاحظاتی که به واسطه به‌کارگیری جنگ اطلاعات بر محیط تحمیل می‌گردد عبارتند از :

- حجم انبوه اطلاعات آلوده پراکنده در محیط که موجب سردرگمی ، اغتشاش و بی نظمی نیروها می گردد.
- فشار روانی شدید بر تصمیم‌گیری و اجرا به دلیل حجم وسیع جنگ روانی دشمن
- کاهش شدید اعتماد پذیری به نیروها و امکانات خودی
- مرگ فکری فرماندهان ارشد و میانی

جنگ ها نسل ششم

جنگ اطلاعات

لایه‌های جنگ اطلاعات

- **لایه فیزیکی**

مقوله‌های فیزیکی که به منظور تحت تأثیر قرار دادن اطلاعات به آن‌ها حمله می‌گردد.

- **لایه زیرساخت اطلاعاتی**

فرایندها و محتوای اطلاعاتی که ممکن است مستقیماً و بدون نمود فیزیکی تحت تأثیر قرار گیرند.

- **لایه ادراک**

هدف قراردادن ذهن انسان توسط مطالب الکترونیکی،شفاهی و نوشتاری

جنگ ها نسل ششم

جنگ نرم

در محیط جنگ نرم دشمن تلاش می‌کند به کمک ابزارهای نرم همچون تغییر باور، ارزش، دیدگاه‌ها ، تفکرات، حذف روابط میان اعضا جامعه، حذف وحدت و یکپارچگی استیلای فرهنگی ، ایجاد وابستگی علمی و دانشی و بسیاری راهکارهای دیگر بدون اقدام نظامی، دشمن را نسبت به تغییر رفتار و عمل مطابق خواسته‌هایش متمایل سازد.

جنگ ها نسل ششم

جنگ سایبر

جنگ سایبر به هرگونه عمل خصمانه بر علیه سیستم‌های رایانه‌ای ، شبکه‌های رایانه‌ای یا پایگاه‌های داده رایانه‌ای دشمن اطلاق می‌شود که با هدف کاهش کارایی یا ناتوان سازی صورت پذیرد.

انواع حملات سایبر

- **حملات خاموش**

این حملات شامل فعالیت‌هایی می‌شوند که بدون انجام هرگونه فعالیت ظاهری یا ایجاد تغییرات در سیستم‌های آسیب پذیر، به آن‌ها نفوذ شده و منجر به سوء استفاده از منابع سیستم می‌گردد.

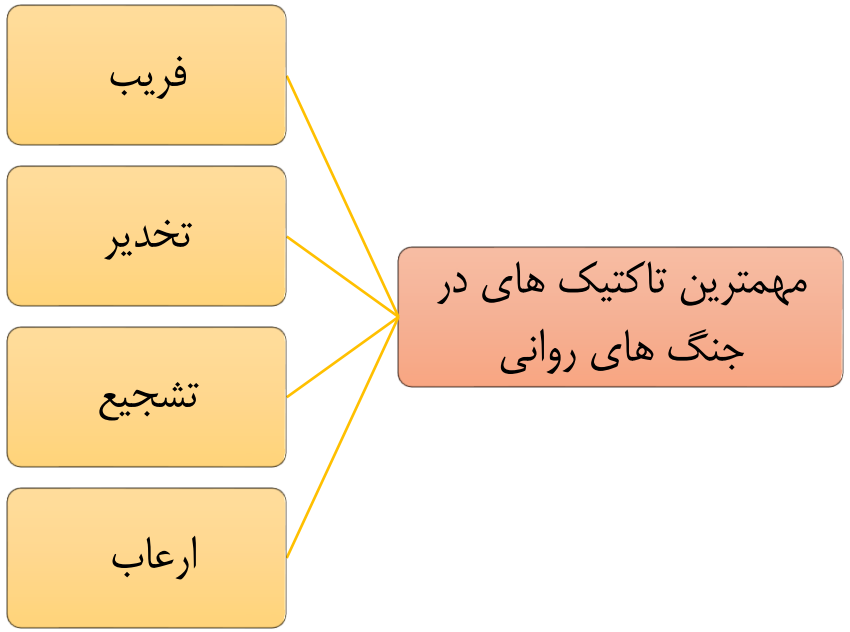
- **حملات فعال**

این حملات، حملاتی هستند که به سیستم‌های کامپیوتری زیرساخت‌های حیاتی نفوذ می‌کنند و می‌توانند اطلاعات حساس را دستکاری کنند و باعث بروز حوادث و فجایع ملی و جبران ناپذیر می‌گردند. از اهداف آن‌ها می‌توان، از کار انداختن شبکه‌های خدماتی عمومی مثل شبکه برق، گاز و ... و همچنین ایجاد وحشت و ترس در جامعه و کاهش میزان اعتماد به دولت و نظام را برشمرد.

جنگ ها نسل ششم

جنگ روانی

جنگ روانی شیوه مؤثری است جهت بهره‌برداری از نقاط ضعف روانی نیروهـای دشـمن بـا هـدف ایجـاد تـرس ، سردرگمی و توانایی در آن‌ها که در نهایت تضعیف روحیه طرف مقابل را در بر خواهد داشت.



جنگ ها نسل ششم

نوع جنگ	نیازهای مسبب	ویژگی‌ها	هدف
جنگ الکترونیک	وابستگی تسلیحات مدرن به اطلاعات	تخریب سخت‌افزاری	اخلال در ارتباطات و شناسایی
جنگ اطلاعات	بی نظم کردن زیر ساخت نظامی	کسب اطلاعات از طرف مقابل	اخلال در توانایی دانشی و تصمیم‌گیری افراد
جنگ نرم	مورد توجه قرار گرفتن نیت و مقاصد طرف مقابل	کسب مشروعیت و جذابیت	متمایل ساختن دشمن نسبت به تغییر رفتار
جنگ سایبر	کاهش کارایی و ناتوان سازی	دانستن همه چیز درباره دشمن	برهم زدن موازنه اطلاعات و دانش به نفع نیروهای خودی
جنگ روانی	برتری اطلاعات	تزریق اطلاعات فاسد	ایجاد جهل مطلق و حذف میل به جنگ

نقش سلاح های اطلاعاتی در میدان جنگ

❑ **سلاح های نرم افزاری اطلاعاتی**

- ویروس های کامپیوتری
- کرم
- تروجان
- اسب تراوا
- بمب های منطقی
- در های پشت قلعه ای

برنامه‌های کاربردی به دو صورت می‌توانند عامل خطر باشند. برنامه‌هایی که به طور عمدی برای ایجاد تهدید ساخته می‌شوند. برنامه‌هایی که به طور غیرعمدی اشکالاتی در آن‌ها وجود دارد. یک اصل در علم کامپیوتر وجود دارد که می‌گوید: هیچ برنامه‌ای بدون اشکال نیست.

تاثیر جنگ در پیشرفت فناوری اطلاعات

با آغاز جنگ جهانی دوم، جنبش و تحرک جدیدی برای ساختن ماشین‌های سریع‌تر و قوی‌تر به وجود آمد و این به خاطر درگیری روزافزون بشر به کارهای اداری و تجاری با حجم زیاد و محاسبات پیچیده و وسیع علمی بود و دولت‌ها به دنبال کامپیوترهایی بودند که بتوانند اطلاعات سری خود را در آن‌ها ذخیره کنند و محاسبات اطلاعاتی خود را هم به سرعت انجام دهند.

در میان کشورهای اروپایی، آلمانی‌ها سرمایه‌گذاری کلان‌تری انجام دادند.

با این حال تلاش آمریکایی‌ها برای ساخت کامپیوترهای پیشرفته‌تر با موفقیت بیشتری همراه بود.

ماشین حساب تمام الکترونیک به نام Marc I انجام محاسبات نیروی دریایی آمریکا روی نقشه‌هایشان بود.

کامپیوتر دیگری که در طول سال‌های جنگ جهانی دوم در سال ۱۹۴۶ ساخته شد « اینـاک » نـام داشـت حل مسایل مربوط به انفجار

آرپانت، شبکه‌ای از رایانه‌ها بود که در سپتامبر ۱۹۶۹ساخته شد هدف از راه‌اندازی این شبکه کنترل تحقیقات علمی در عرصه نظامی و اشتراک‌گذاری نتایج این تحقیقات ، پنتاگون بود.

...

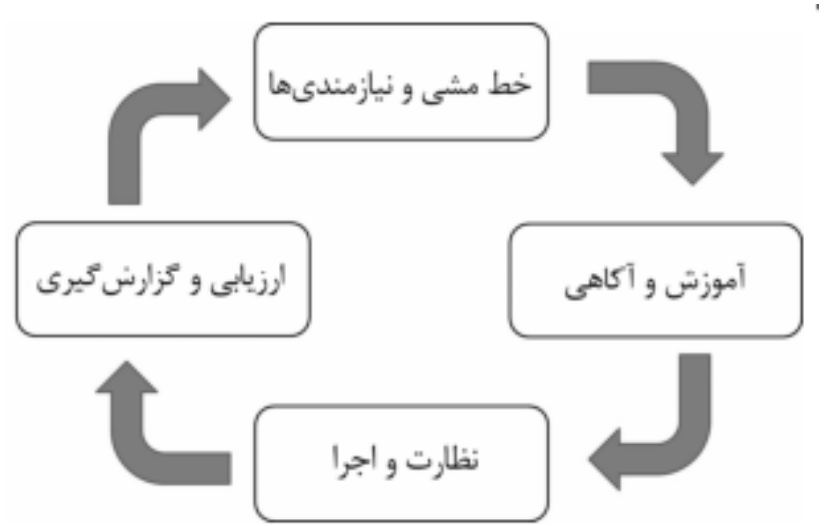
اصول و مبانی امنیت داده و اطلاعات

امنیت اطلاعات

- امنیت اطلاعات به مجموعه‌ای از فرآیندها، سیاست‌ها، تکنیک‌ها، و ابزارهایی گفته می‌شود که برای حفاظت از اطلاعات مهم، حساس و محرمانه در برابر دسترسی غیرمجاز، استفاده غیرمجاز، افشای غیرمجاز، اصلاح غیرمجاز و از دست دادن این اطلاعات به کار می‌روند.
- به طور کلی، هدف امنیت اطلاعات، حفظ محرمانی، یکپارچگی، و دسترسی به اطلاعات است تا سازمان‌ها و افراد بتوانند از اطلاعات خود به بهترین شکل ممکن بهره ببرند و ریسک‌های مرتبط با امنیت اطلاعات را کاهش دهند.
- محرمانی Confidentiality : اطلاعات باید در برابر دسترسی غیرمجاز محافظت شوند، به طوری که فقط افرادی که مجاز به دسترسی هستند بتوانند به آنها دسترسی پیدا کنند.
- یکپارچگی Integrity : اطلاعات باید مورد اعتماد و قابل اعتماد باشند و از هرگونه تغییر غیرمجاز جلوگیری شود. این به معنای حفظ صحت، دقت، و کاملیت اطلاعات است.
- دسترسی Availability : اطلاعات باید در زمان‌های لازم و برای افرادی که به آن نیاز دارند، در دسترس باشند، و از خدشه‌هایی مانند حمله‌های دیده نشده یا خرابی‌های سیستمی جلوگیری شود.

پیاده سازی امنیت اطلاعات

سازمان باید سیاست‌ها، استانداردها و رویه‌های مربوط به امنیت اطلاعات خود را تعیین و اعمال کند. این شامل سیاست‌های دسترسی، رمزنگاری، مدیریت رمزها و سایر موارد می‌شود.



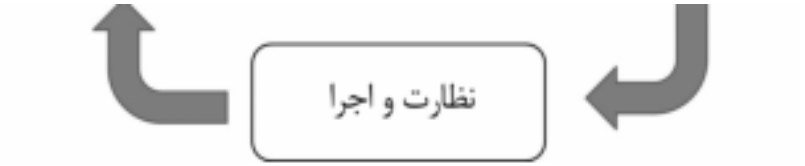
چرخه پیاده‌سازی امنیت اطلاعات

دو عنصر کلیدی در پیاده‌سازی امنیت اطلاعات هستند که به طور مداوم باید اجرا شوند تا امنیت اطلاعات سازمان تضمین شود.

کارکنان باید به مواردی مانند خطرات امنیتی، روش‌های حفاظت اطلاعاتی و گزارش دهی در صورت مشاهده هرگونه تخلف آگاهی داده شوند.

سیستم امنیت اطلاعات باید به صورت دوره‌ای ارزیابی و بازبینی شود تا اطمینان حاصل شود که همچنان موثر و به‌روز است و تطابق با الزامات قانونی و استانداردهای امنیتی را دارد.

پیاده سازی امنیت اطلاعات



نظارت

- نظارت بر فعالیت‌های سیستمی : شامل نظارت بر دسترسی به سیستم، فعالیت‌های شبکه، و سایر فعالیت‌های سیستمی است.
- نظارت بر وقایع امنیتی Security Event Monitoring : به منظور شناسایی و پاسخگویی به حوادث امنیتی مانند تهدیدات نفوذی، نفوذهای موفق، و رفتارهای مشکوک صورت می‌گیرد.
- تجزیه و تحلیل لاگ‌ها Log Analysis : برای شناسایی الگوها و ترکیب‌های غیرمعمول در فعالیت‌های سیستمی انجام می‌شود.

اجرا

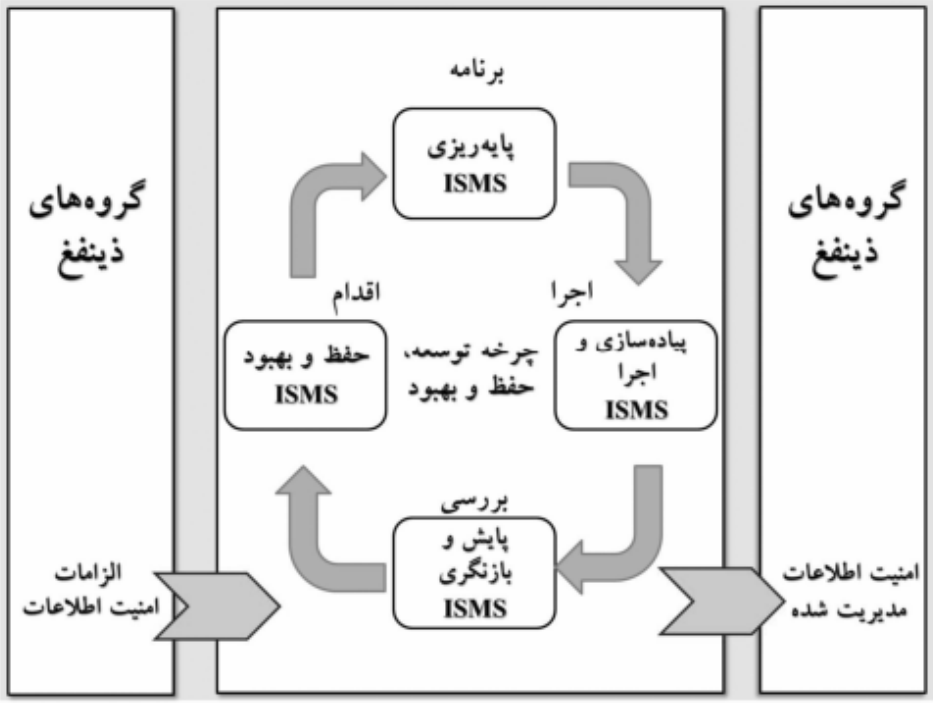
- اجرای سیاست‌ها و استانداردها: سیاست‌ها و استانداردهای امنیتی باید به دقت اجرا شوند تا امنیت اطلاعات تضمین شود.
- مدیریت دسترسی: اجرای سیاست‌های مدیریت دسترسی به منظور اطمینان از اینکه فقط افراد مجاز به دسترسی به اطلاعات هستند و دسترسی غیرمجاز ممنوع است.
- پیکربندی و مدیریت فنی: اجرای فناوری‌های مورد نیاز برای حفاظت از اطلاعات مهم، از جمله نصب و پیکربندی فایروال‌ها، ضدویروس‌ها و سایر ابزارهای امنیتی.

سیستم مدیریت امنیت اطلاعات Information Security Management System (ISMS)

- یک چارچوب است که برای مدیریت و کنترل امنیت اطلاعات در یک سازمان استفاده می‌شود.
- هدف اصلی ISMS، حفاظت از اطلاعات حساس و مهم سازمان در برابر تهدیدها و ریسک‌های مختلف است.
- این سیستم مدیریتی شامل یک سری استانداردها، رویه‌ها، فرآیندها و سیاست‌ها است که اجرای آن‌ها باعث ارتقای سطح امنیت اطلاعات در سازمان می‌شود.
- ISMSمعمولاً بر اساس استانداردهای بین‌المللی مانند ISO/IEC 27001ساخته می‌شود. این استاندارد شامل مجموعه ای از الزامات و رویه‌های مورد نیاز برای ایجاد، پیاده‌سازی، نظارت و بهبود مداوم سیستم مدیریت امنیت اطلاعات در یک سازمان است.
- مزایای استفاده از ISMSشامل حفظ اعتبار و اعتماد مشتریان، کاهش ریسک‌های امنیتی، تضمین تطابق با مقررات و استانداردهای قانونی، و بهبود عملکرد سازمان در برابر تهدیدات امنیتی می‌شود.

این سیستم همچنین به سازمان‌ها کمک می‌کند تا منابع خود را بهینه‌سازی کنند و با هزینه‌های امنیتی موثرتری روبه‌رو شوند.

طراحی، پیاده سازی نگهداری و بهبود سیستم مدیریت امنیت اطلاعات (ISMS)



فاز برنامه

- تعریف محدوده اولیه سیستم مدیریت امنیت اطلاعات
- تعریف سیاست و خط مشی کلی در سیستم مدیریت امنیت اطلاعات
- شناسایی دارایی‌ها
- شناسایی تهدیدها
- ارزیابی ریسک
- تنظیم برنامه برخورد با ریسک‌ها
- انتخاب کنترل‌های امنیتی
- تنظیم بیانیه قابلیت اجرا

فاز اجرا

- بازبینی به منظور بهبود و نهایی‌سازی برنامه برخورد با ریسک
- پیاده‌سازی برنامه برخورد با ریسک و کنترل‌های مربوطه

فاز بررسی

- نظارت بر اجرا
- بازبینی‌های منظم بر کارایی و کارامدی سیستم مدیریت امنیت اطلاعات
- نظارت بر ریسک‌های مورد قبول
- هدایت منظم ممیزی‌های سیستم مدیریت امنیت اطلاعات

فاز اقدام

- پیاده‌سازی موارد بهبود
- انتخاب اعمال اصلاحی مناسب
- اطمینان از رسیدن به اهداف بهبود و توسعه

نحوه پیاده سازی نگهداری مدیریت امنیت اطلاعات در سازمان ها

سازمان‌ها وقتی می‌خواهند گواهینامه بگیرند، اقدام به دریافت آن کرده و به شرکت‌هایی که این خدمات را ارائه می‌دهند مراجعه می‌کنند. شرکت‌های ارائه دهنده این خدمات با شرکت‌های خارجی که در زمینه مدیریت امنیت اطلاعات در ایران شعبه دارند، مشاوره کرده و در نهایت مشاوری از سوی شرکت برای آن سازمان می‌فرستند.

پیاده‌سازی به‌طور اساسی در دو سطح صورت می‌گیرد. در سطح اول که سطح کلی می‌باشد تمرکز روی پروسه‌های تجاری و امنیتی می‌باشد، به‌طوریکه فرهنگ امنیت اطلاعات به عنوان مفاهیم اصلی این سطح مورد بررسی قرار می‌گیرد و سعی می‌گردد رفتار و عملکرد کارکنان در سازمان‌ها اصلاح شده و معیارهای امنیتی در تمامی سطوح سازمانی تفهیم گردد. در سطح دوم، پیاده‌سازی فنی و با جامعیت بیشتر صورت می‌گیرد که با استفاده از استانداردهای بین‌المللی و سیستم‌ها و ابزارهای لازم صورت می‌گیرد. بعد از پیاده‌سازی پروسه‌های مدیریتی و تجاری و نیز پیاده‌سازی فنی و عملیاتی امنیت، سازمان تا حد قابل قبولی می‌تواند از پوشش مناسب مدیریت امنیت اطلاعات اطمینان پیدا نماید.

پدافند غیر عامل در سیستم عامل و مسیریاب ها

پدافند غیر عامل در طراحی سیستم عامل

پدافند غیر عامل در طراحی سیستم عامل

از فایل‌های اصلی حاوی اطلاعات مهم کاربری، مانند کلمه عبور باید حفاظت به عمل آورد و تنها کاربر ریشه به آن‌ها دسترسی داشته باشد.

باید مکانیزم‌های کنترلی خاص در طراحی سامانه مدیریت فرایند، ایجاد و پیاده سازی گردد؛ به‌طوریکه فرایندهای مخاطره‌آمیز مسدود و اطلاعات آن‌ها و کاربران اجرا کننده ثبت و گزارش شود.

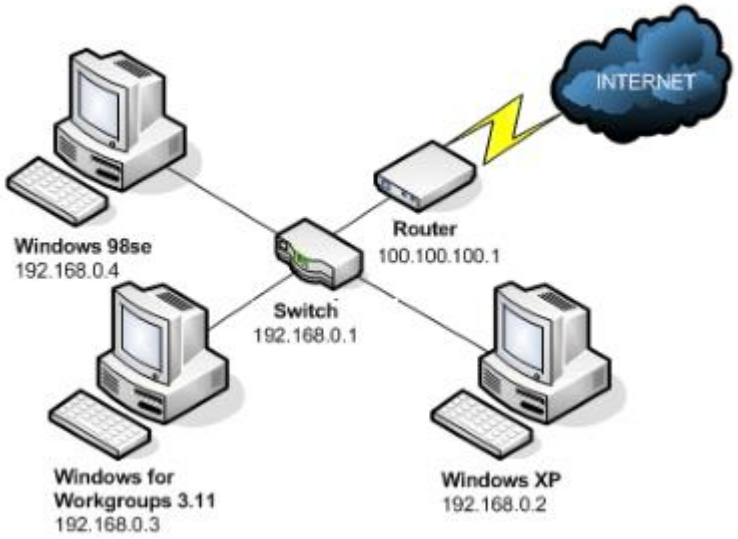
سرویس‌های غیرضروری، هنگام ارائه محصول به کاربر نهایی باید غیرفعال باشند.

در دستگاه‌های ورودی/خروجی برای ایجاد مکانیزم‌های محافظتی باید برای دسترسی هرکاربر، رمز ورود تقاضا شده و متناسب با هر سطح دسترسی، امکانات معینی از سامانه در اختیار کاربر قرار گیرد.

سیستم عامل ملی باید دارای سطح قابل قبولی از امنیت ذاتی در برابر نرم‌افزارهای مخرب باشد، این نوع از امنیت بیشتر در سیستم عامل‌های چند کاربره مطرح است.

در طراحی سیستم عامل ملی باید امکانات و قابلیت‌های لازم جهت پشتیبانی از استانداردها و پروتکل‌های امن‌سازی سیستم عامل پیش بینی شود.

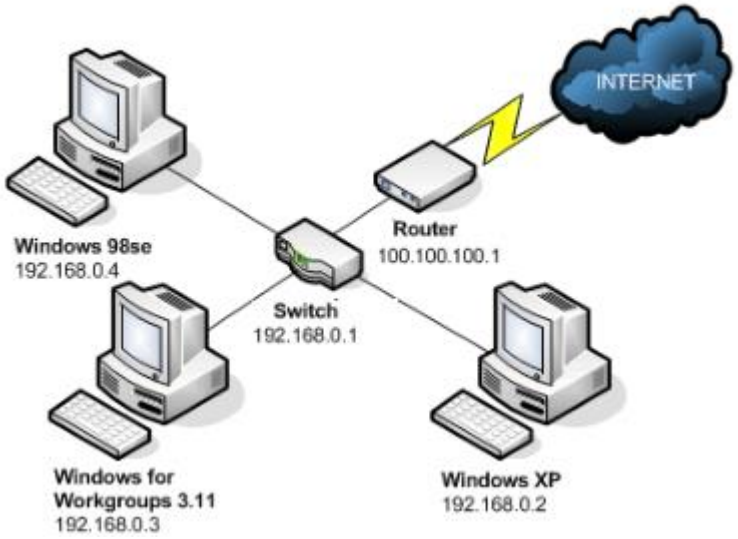
پدافند غیر عامل در حوزه مسیریاب



دامنه تاثیر حملات علیه مسیر یاب ها

- ***ازدحام شبکه*** : میزان بسیار زیاد حجم ترافیک از طریق یک قسمت خاص از شبکه ارسال می‌شود که قابلیت ارسال آن حجم را ندارد.
- ***سیاه چاله*** : میزان زیادی از ترافیک داده به صورت غیرضروری از یک مسیریاب ارسال می‌شود و در نتیجه مسیریاب، بسیاری و گاهی همه بسته‌ها را حذف می‌کند.
- ***دوتکه شدن*** : یک قسمت از شبکه به صورت واقعی یا مجازی از کل شبکه جدا و غیرقابل دسترسی می‌شود.
- ***فعال‌سازی شدید*** : نرخ ارسال ترافیک در شبکه بسیار سریع (و غیرضروری) تغییر پیدا می‌کند که منجر به ایجاد ***اختلاف*** زیاد در نرخ دریافت بسته‌ها می‌گردد. این امر باعث عدم کارکرد صحیح برخی عملیات شبکه نظیر برنامه‌های چندرسانه‌ای می‌شود.
- ***ناپایداری*** : پروتکل مسیریابی ناپایدار می‌شود به نحوی که همگرایی در عملیات مسیریابی صورت نمی‌گیرد.

پدافند غیر عامل در حوزه مسیریاب



برقراری امنیت در حوزه کاری مسیر یاب در چهار لایه زیر باید دنبال شود:

۱- **فیزیکی**: داخلی‌ترین لایه نیازمند مصون‌سازی در یک مسیریاب، لایه فیزیکی است چرا که با داشتن دسترسی فیزیکی، یک نفوذگر می‌تواند کنترل کامل مسیریاب را در دست بگیرد. از این‌رو برای این لایه امنیتی، باید سیاست‌های مشخصی در نظر گرفته شود.

۲- **نرم افزار و پیکربندی ثابت:** مفاهیمی همچون نشانی واسط‌ها، رمزهای عبور و کنترل دسترسی به پورت‌های پیکربندی، در این لایه مطرح می‌شوند و قابل دسترسی هستند

۳- **پیکربندی پویا:** این لایه شامل اطلاعاتی همچون جدول‌های مسیریابی و ***ARP*** و گزارشات است.

۴- **داده‌های عبوری و سرویس‌ها**: سیاست امنیت مربوط به این بخش شاید بزرگ‌ترین بخش از تدوین سیاست امنیتی مسیریاب باشد. در این لایه، تصمیم در خصوص آدرس‌ها و پروتکل‌هایی که مجوز عبور دارند، موضوع اصلی است.

پدافند غیر عامل در حوزه امنیت فیزیکی و کنترل دسترسی

- پدافند غیرعامل در حوزه امنیت فیزیکی و کنترل دسترسی به عواملی اشاره دارد که باعث افزایش امنیت فیزیکی سازمان می‌شوند، اما خود به تنهایی به عنوان یک عامل تهدیدی در نظر گرفته نمی‌شوند.
- این اصطلاح معمولاً برای تجهیزات و سیستم‌هایی مانند درها، قفل‌ها، دیوارهای ضد آتش، دوربین‌های مداربسته، نورپردازی، سیستم‌های اعلام و اطفاء حریق، و دستگاه‌های کنترل دسترسی استفاده می‌شود.

مراحل دفاع در حوزه سایبری

۱- ***جلوگیری*** : عبارت است از شناسایی راه‌های نفوذ و حمله و مقابله با آن‌ها جهت افزایش ضریب امنیت،ایمنی و پایداری.

- ***طراحی امن و ایمن و پایدار سیستم ها***

در صورتی که امنیت جزء معیارها و اصول طراحی سیستم‌ها قرار بگیرد، سیستم‌ها بسیار امن تر و ایمن‌تر و پایدارتر از قبل خواهند بود.

- ***متوقف نمودن حملات***

از دیگر راه‌های جلوگیری از حملات، متوقف نمودن آن‌ها می‌باشد.این روش از طریق استفاده از تجهیزات پیشرفته امنیتی و وضع قوانین لازم، میسر است.

- ***خاموشی و تخصیص مجدد*** :

خاموش کردن و تخصیص‌دهی مجدد باید به صورت ***بلادرنگ*** و به سرعت انجام گیرد.

- **پشتیبانی:** نکته قابل توجه این است که باید همواره از اطلاعات جمع‌آوری شده، قبل از هر حمله‌ای پشتیبانی کنیم.

تعریف مرکز داده

الف- با امنیت فیزیکی و الکترونیکی بالا، برخوردار از پهنای باند ارتباطی وسیع، متصل به شبکه‌های رایانه‌ای ملی و جهانی، با خدمات تمام وقت و در دسترس.

ب- دارای انواع تجهیزات سخت‌افزاری (رایانه‌ها، ***مودم*** ها و مسیریاب‌ها و سایر موارد) و نرم‌افزاری پیشرفته (پایگاه‌های داده، سرورها و سایر موارد) که از پشتیبانی و نگهداری حرفه‌ای و تمام وقت برخوردار است.

ج- با پشتیبانی و ارائه خدمات مرتبط با اطلاعات و داده‌ها از قبیل خدمات ذخیره، نگهداری و بازیابی داده‌ها، ***ERP*** ، ***میزبانی خدمات اینترنتی*** ، ***میزبانی خدمات کاربردی*** ، میزبانی برون سپاری خدمات و غیره برای کلیه اشخاص حقیقی و حقوقی.

مکان مناسب جهت اتاق سرور

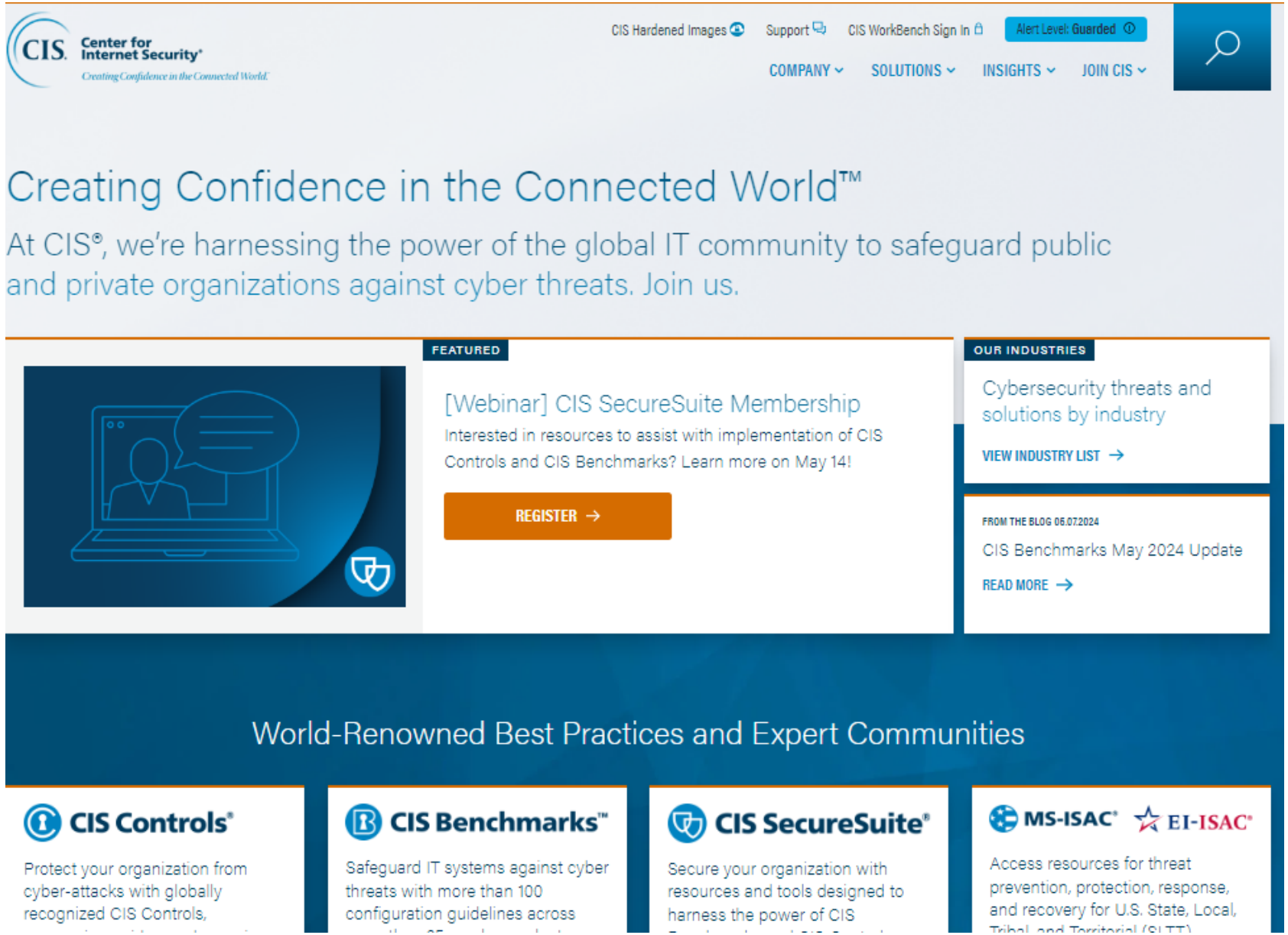
معمولاً اتاق سرور را در پایین‌ترین طبقه درنظر می‌گیرند و این مکان باید با کانال‌ها و رایزرهای ساختمان در ارتباط باشد. در صورتی‌که از این اتاق به اتاق‌های دیگر و همچنین به طبقات دیگر کانالی وجود نداشته باشد باید آن را ایجاد نمود.

بیانیه مأموریت پدافند غیرعامل در حوزه فناوری‌اطلاعات و ارتباطات

- پدافند غیرعامل در حوزه فناوری اطلاعات، یکی از زیرمجموعه‌های پدافند غیرعامل کشور بوده و سهم عمده‌ای در راهبرد دفاعی کشور دارد.
- پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات، پیشگیری و کاهش آسیب‌پذیری و پایداری زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات کشور در برابر تهدیدات را به دنبال خواهد داشت.
- پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات ضمن توسعه و ارتقای ظرفیت‌های دفاعی، با کاهش جدی آسیب‌پذیری‌های اساسی و افزایش توان بازدارندگی، ارتقای ظرفیت مدیریت کشور در شرایط بحران را دنبال نموده و تردید اساسی در اراده و میل تهاجمی دشمن ایجاد می‌نماید.

Center for Internet Security (CIS)

یک سازمان غیرانتفاعی که هدف آن کمک به مردم، مشاغل و دولت‌ها برای محافظت از خود در برابر تهدیدات سایبری است.


CIS Center for Internet Security
Creating Confidence in the Connected World
CIS Hardened Images
Support
CIS WorkBench Sign In
Alert Level: Guarded
COMPANY
SOLUTIONS
INSIGHTS
JOIN CIS
Creating Confidence in the Connected World™
At CIS®, we're harnessing the power of the global IT community to safeguard public and private organizations against cyber threats. Join us.
FEATURED
[Webinar] CIS SecureSuite Membership
Interested in resources to assist with implementation of CIS Controls and CIS Benchmarks? Learn more on May 14!
REGISTER
OUR INDUSTRIES
Cybersecurity threats and solutions by industry
VIEW INDUSTRY LIST
FROM THE BLOG 06.07.2024
CIS Benchmarks May 2024 Update
READ MORE
World-Renowned Best Practices and Expert Communities
CIS Controls®
Protect your organization from cyber-attacks with globally recognized CIS Controls,
CIS Benchmarks™
Safeguard IT systems against cyber threats with more than 100 configuration guidelines across
CIS SecureSuite®
Secure your organization with resources and tools designed to harness the power of CIS
MS-ISAC®
EI-ISAC®
Access resources for threat prevention, protection, response, and recovery for U.S. State, Local,

کنترل های Basic (کنترل ۶-۱)

کنترل های Foundational (کنترل ۱۶-۷)

کنترل های Organizational (کنترل ۲۰-۱۷)

کنترل های Basic

- ۱.موجودی دارایی های سخت افزار
- ۲.موجودی دارایی های نرم افزار
- ۳.مدیریت پیوسته آسیب پذیری ها
- ۴. استفاده کنترل شده از مجوزهای دسترسی مدیریتی
- ۵.پیکربندی امن برای سخت افزارها و نرم افزارها
- ۶.تحلیل لاگ های سیستم

کنترل ۱: موجودی و کنترل دارایی های سخت افزار

استفاده از DHCP

استفاده از ابزار Passive Discovery

استفاده از ابزار Active Discovery

آدرس دهی دارایی های غیرمجاز

ثبت آدرس شبکه، آدرس سخت افزار و .. توسط سخت افزار

موجودی دقیق از دارایی های سخت افزار سازمان

استفاده از گواهینامه های امنیتی

استفاده از پورت کنترل سطح دسترسی

کنترل ۲: موجودی و کنترل دارایی های نرم افزار

استفاده از ابزار لیست موجودی نرم افزارها	پشتیبانی نرم افزار توسط فروشنده	لیستی به روز از نرم افزار های مجاز سازمان
آدرس دهی نرم افزارهای غیرمجاز	ادغام دارایی های سخت افزار و نرم افزار	ردیابی نام، نسخه، تاریخ نصب همه نرم افزارهای مهم
تفکیک سیستم ها از نظر فیزیکی یا منطقی	استفاده از لیست سفید	

کنترل ۳: مدیریت پیوسته آسیب پذیری ها

- استفاده از ابزارهای به روز رسانی خودکار
- استفاده از یک حساب اختصاصی برای اسکن آسیب پذیری ها
- استفاده از ابزار اسکن آسیب پذیری خودکار
- استفاده از فرایند رتبه بندی ریسک
- مقایسه نتایج حاصل از اسکن های متوالی آسیب پذیری ها

کنترل ۴:استفاده کنترل شده از مجوزهای دسترسی مدیریتی

استفاده از یک حساب اختصاصی برای فعالیت های سطح بالاتر	تغییر رمزهای عبور پیش فرض	فقط افراد مجاز دارای دسترسی های بالا باشند
استفاده از ایستگاه های کاری اختصاصی برای کارهای اداری	استفاده از احراز هویت برای دسترسی های اداری	استفاده از رمزهای عبور منحصربه فرد
هشدار هنگام ورود ناموفق به حساب اداری	هشدار هنگام تغییر عضویت در گروه اداری	دسترسی به ابزارهای اسکریپت نویسی فقط به کاربرانی نیاز به این قابلیت ها دارند

کنترل ۵:پیکربندی امن برای سخت افزارها، نرم افزارها بر روی دستگاه های موبایل، لپ تاپ ها و ایستگاه های کاری

استفاده از تصاویر و الگوهای ایمن برای همه سیستم های سازمان

پیکربندی ایمن برای همه سیستم عامل ها و نرم افزارهای مجاز

استفاده ازابزارهای مدیریت پیکربندی سیستم

ذخیره تصاویرو الگوهای اصلی بر روی سرورهای پیکربندی شده

تنظیم هشدارهنگام وقوع تغییرات غیرمجاز

کنترل 6: جمع آوری، پایش و تحلیل لاگ های سیستم

- داشتن فضای کافی برای ذخیره سازی لاگ ها
- فعال کردن لاگ های سیستم در همه دستگاه های شبکه
- استفاده از سه منبع زمان هماهنگ برای سرورها و دستگاه های شبکه
- مرور لاگ ها به طور منظم
- استفاده از ابزارهای تحلیلی log یا SIEM
- مدیریت ورود (log) در سیستم مرکزی
- تنظیم SIEM به طور منظم


کنترل های Foundational
۷. محافظت از ایمیل و مرورگرهای وب
۸. دفاع در برابر بد افزارها
۹.محدود کردن و کنترل پورت های شبکه، پروتکل ها و سرویس ها
۱۰. قابلیت بازیابی اطلاعات
۱۱. پیکربندی امن برای ابزارهای شبکه ای
۱۲. دفاع مرزی
۱۳. حفاظت از اطلاعات
۱۴. دسترسی کنترل شده براساس نیاز به دانستن
۱۵. کاهش دسترسی بی سیم
۱۶. کنترل و نظارت بر حساب های کاربری

کنترل ۷:محافظت از ایمیل و مرورگرهای وب

- فقط زبان های مجاز اسکریپت نویسی در مرورگر اجرا شوند
- حذف یا غیرفعال کردن افزونه های غیرمجاز
- استفاده از مرورگرهای دارای پشتیبانی
- وارد کردن کلیه درخواست های URL ازهریک از سیستم های سازمان
- مشترک شدن در سرویس دسته بندی URL
- استفاده از فیلترهای URL مبتنی بر شبکه
- بلاک کردن پیوست های ایمیل غیرضروری برای سازمان
- استفاده از DMARC
- استفاده از DNS
- استفاده از Sandbox

کنترل ۸: دفاع در برابر بدافزارها

فعال کردن DEP و ASLR سیستم عامل

به روز بودن Anti-malware

استفاده از Anti-malware

ارسال رویدادهای شناسایی بدافزار به ابزارهای مدیریت ضد بدافزار

اجرانشدن خودکار محتوای Removable Media در دستگاه ها

اسکن ضد بدافزار از Removable Media

فعال کردن DNS

کنترل ۹: محدود کردن و کنترل پورت های شبکه، پروتکل ها و سرویس ها

اسکن خودکار پورت ها برای شناسایی پورت غیرمجاز

فقط سرویس های تایید شده اجرا شوند

مرتبط کردن پورت های فعال و پروتکل ها به دارایی سخت افزار

مسدودکردن ترافیک های غیرمجازی که به سمت سرور می روند

استفاده از فایروال های مبتنی بر شبکه

کنترل ۱۰: قابلیت بازیابی اطلاعات

آزمایش داده ها در Backup Media

بکاپ کامل از سیستم

تهیه بکاپ به طور منظم از داده ها

دارابودن نسخه های بکاپ از یک قسمت آفلاین

رمزگذاری نسخه های بکاپ

کنترل ۱۱: پیکربندی امن برای ابزارهای شبکه ای مانند فایروال ها، روتر ها و سوییچ ها

مقایسه پیکربندی امنیتی شبکه با پیکربندی های تایید شده	مستند کردن قوانین پیکربندی در یک سیستم مدیریت پیکربندی	اعمال استانداردهای پیکربندی امنیتی برای همه دستگاه های مجاز شبکه
استفاده از یک دستگاه اختصاصی برای وظایفی که نیاز به دسترسی بالا دارند	مدیریت دستگاه های شبکه با احراز هویت و رمزگذاری	نصب آخرین نسخه از بروزرسانی مربوط به امنیت
	مدیریت زیرساخت شبکه از طریق یک شبکه اختصاصی	

کنترل ۱۲: دفاع مرزی

رد کردن ارتباطات از طریق درگاه های غیرمجاز

محدود کردن دسترسی فقط به Ipهای مورد اعتماد و لازم

شناسایی اتصالات غیرمجاز به شبکه

تهیه فهرست موجودی به روز از تمام مرزهای شبکه

استقرار مجموعه NetFlow در دستگاه های مرزی شبکه

استقرار سیستم های پیشگیری از نفوذ مبتنی بر شبکه (IPS)

استقرار سیستم های تشخیص نفوذ مبتنی بر شبکه (IDS)

پیکربندی سیستم های مانیتورینگ

اسکن تمام دستگاه های سازمانی که از راه دور به شبکه وصل می شوند.

رمزگشایی ترافیک شبکه در پروکسی

فیلتر اتصالات غیرمجاز

کنترل ۱۳: حفاظت از اطلاعات

مسدود کردن ترافیک غیرمجاز شبکه	حذف داده یا سیستم هایی که مورد نیاز سازمان نیستند	موجودی تمام اطلاعات حساس
استفاده از مکانیزم های رمزگذاری تایید شده	نظارت و ردیابی هرگونه استفاده غیرمجاز از رمزگذاری	اجازه دسترسی فقط به فضای ذخیره سازی ابری مجاز(cloud storage)
رمزگذاری داده ها در دستگاه های ذخیره سازی USB	ننوشتن داده ها در رسانه قابل جابجایی خارجی (external removable media)	مدیریت دستگاه های USB

کنترل ۱۴: دسترسی کنترل شده برمبنای نیاز(ضرورت) به دانستن

- غیرفعال کردن ارتبطات ایستگاه کاری به ایستگاه کاری دیگر
- فعال کردن فایروال بین VLANها
- قرار دادن اطلاعات حساس در شبکه های محلی مجزا
- محافظت از اطلاعات ذخیره شده بر روی سیستم ها
- استفاده از ابزار Active Discovery
- رمزگذاری تمام اطلاعات حساس
- ثبت جزئیات دقیق برای دسترسی به داده های حساس یا تغییرات آن ها
- استفاده از DLP برای کنترل دسترسی به داده ها

کنترل ۱۵: کاهش دسترسی بیسیم

محدود کردن دسترسی بیسیم در دستگاه هایی که هدف تجاری آن ها برای دسترسی بیسیم نیست

استفاده از سیستم تشخیص نفوذ بیسیم (WIDS)

پیکربندی ابزار اسکن آسیب پذیری شبکه

تهیه فهرست از نقاط دسترسی بیسیم متصل به شبکه

استفاده از پروتکل های احراز هویت

استفاد از استاندارد رمزگذاری پیشرفته (AES)

غیرفعال کردن شبکه بیسیم peer to peer در کلاینت های بیسیم

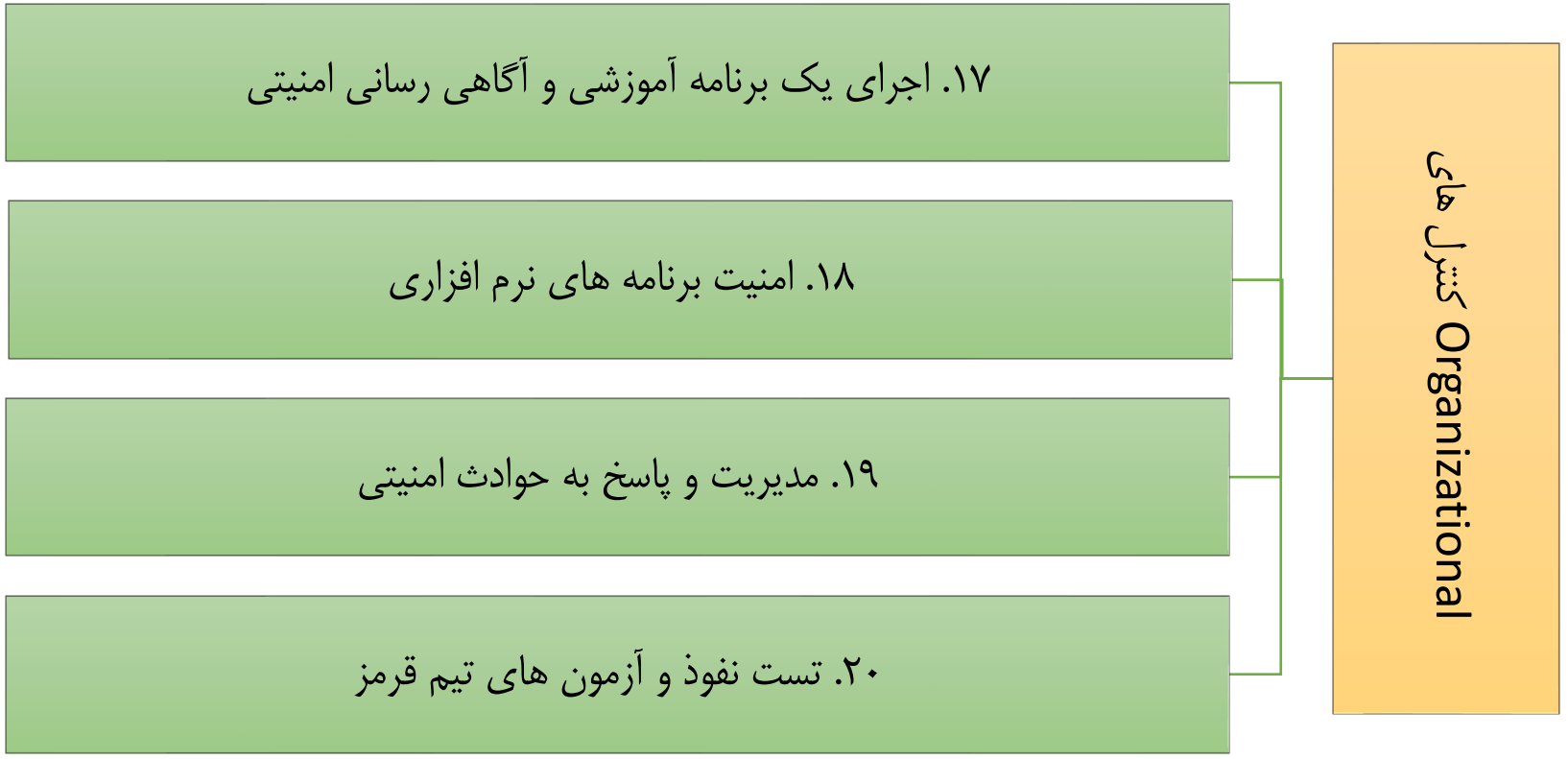
فعال کردن دسترسی بیسیم برروی کلاینت هایی که دارای یک هدف اساسی تجاری بیسیم هستند

ایجاد یک شبکه بیسیم جداگانه برای دستگاه های شخصی و غیر قابل اعتماد

غیرفعال کردن دسترسی بیسیم دستگاه هایی مانند بلوتوث و NFC

کنترل ۱۶: کنترل و نظارت بر حساب های کاربری

انتقال نام های کاربری ازطریق کانال های رمزگذاری شده بین شبکه ها	رمزگذاری اطلاعات احراز هویت	مدیریت احراز هویت چندعاملی برای همه حساب های کاربری	پیکربندی دسترسی برای همه حساب ها	تهیه موجودی از سیستم های احراز هویت
نظارت بر تاریخ انقضاء همه حساب ها	غیرفعال شدن خودکار حساب های کاربری در صورت عدم فعالیت	غیرفعال کردن حساب های کاربری غیرمرتبط با مشاغل سازمان	ایجاد یک فرایند خودکار برای لغو دسترسی به سیستم	تهیه موجودی از حساب های سازمان یافته توسط سیستم احراز هویت
	هشدار در صورت انحراف از لاگین نرمال در ورود به سیستم	نظارت تلاش برای دسترسی به حساب های کاربری مسدود شده	قفل شدن خودکار workstation sessions در صورت عدم فعالیت	


کنترل های Organizational
۱۷. اجرای یک برنامه آموزشی و آگاهی رسانی امنیتی
۱۸. امنیت برنامه های نرم افزاری
۱۹. مدیریت و پاسخ به حوادث امنیتی
۲۰. تست نفوذ و آزمون های تیم قرمز

کنترل ۱۷: اجرای یک برنامه آموزشی و آگاهی رسانی امنیتی

ایجاد یک برنامه آگاهی از امنیت برای همه کارکنان	ارائه آموزش برای رفع شکاف مهارت های مشخص شده	ایجاد یک نقشه راه آموزش با استفاده از تجزیه و تحلیل شکاف مهارت ها
آموزش به کارکنان در مورد چگونگی شناسایی اشکال مختلف مهندسی اجتماعی	آموزش به کارکنان درمورد احراز هویت ایمن	به روز کردن برنامه آگاهی از امنیت
آموزش به کارکنان در خصوص شناسایی و گزارش حوادث	آموزش به کارکنان در زمینه علل غیرعمدی افشای داده	آموزش به کارکنان در خصوص ذخیره، انتقال و ازبین بردن اطلاعات حساس

کنترل ۱۸: امنیت برنامه های نرم افزاری

استفاده از مولفه های به روز و قابل اعتماد برای نرم افزار توسعه یافته توسط سازمان	اطمینان از پشتیبانی نرم افزارهای خریداری شده برای سازمان توسط توسعه دهنده	بررسی های صریح خطا برای همه نرم افزارهای توسعه یافته داخلی	ایجاد روش های کدنویسی ایمن و متناسب با زبان های برنامه نویسی
ایجاد محیط های جداگانه برای سیستم های تولیدی و غیرتولیدی	استفاده از ابزارهای تحلیل ایستا و پویا برای بررسی کدهای امن	آموزش پرسنل توسعه دهنده نرم افزار برای نوشتن کد امن	استفاده از الگوریتم های رمزگذاری استاندارد
	استفاده از الگوهای پیکربندی برای برنامه هایی که به پایگاه داده متصل اند	نصب فایروال های برنامه وب	

کنترل ۱۹: مدیریت و پاسخ به حوادث امنیتی

تعیین پرسنل مدیریتی برای پشتیبانی و رسیدگی به حوادث

اختصاص یک سری وظایف برای پاسخگویی به حوادث

مشخص شدن نقش پرسنل و مراحل مدیریت حوادث توسط برنامه های نوشته شده برای پاسخگویی به حوادث

برنامه ریزی و انجام سناریو هایی برای نیروی کار درگیر در واکنش به حادثه

انتشار اطلاعات مربوط به گزارش ناهنجاری برای اعضای تیم رسیدگی به حوادث

تدوین استانداردهایی برای گزارش حوادث

اولیت بندی حوادث براساس تاثیری که روی سازمان می گذارند

کنترل ۲۰: تست نفوذ و آزمون های تیم قرمز

انجام تمرینات دوره ای تیم قرمز برای آزمایش آمادگی سازمان

شناسایی آسیب پذیری ها با تست های نفوذ داخلی و خارجی

ایجاد برنامه ای برای تست نفوذ که شامل حملات ترکیبی باشد

استفاده از ابزارهای اسکن آسیب پذیری و تست نفوذ

ایجاد بستر آزمایش برای عناصری که در هنگام تولید آزمایش نمی شوند

تست های نفوذ شامل اطلاعات و مصنوعات محافظت نشده سیستم باشد

کنترل هر حساب کاربری یا سیستمی که برای انجام تست نفوذ استفاده می شود

مستند کردن نتایج تست نفوذ با استفاده از استانداردها