ملاحظات پدافند غیر عامل

در حوزه فاوا

فهرست

آغاز

جنگ سایبر

جنگ سایبر، به معنی استفاده از کامپیوترها و فضای تبادل اطلاعات به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت بار جهت ترساندن، تغییر عقیده و یا نابودی یک گروه یا کشور می باشد. جنگ سایبر به قصد کارهای سیاسی انجام می‌گیرد و مکان‌ها و زیرساخت هایی مانند انرژی، حمل‌ونقل، ارتباطات و سرویس‌های خدماتی ضروری را هدف قرار می‌دهد. در جنگ سایبر از شبکه‌های کامپیوتری به عنوان بستر انجام این اعمال خرابکارانه استفاده می‌شود.

- اهداف جنگ های سایبر

اهداف نظامی، خدمات اجتماعی، سامانه های نقل و انتقال، مخابرات، نیرو، انرژی و هر زیرساخت حیاتی می تواند قربانی این جنگ ها بوده و امنیت، ایمنی و پایداری آن به خطر افتد.

نقش پدافندغیرعامل در تأمین امنیت فضای تبادل اطلاعات

لازمه یک دفاع موفق در جنگ سایبر همانا بالا بردن سطح امنیتی عناصر درگیر است و این مهم جز با افزایش دانش در حوزه سایبر میسر نخواهد بود.

بر اساس استانداردهای امنیتی قابل قبول، هر یک از عناصر درگیر در فضای سایبر، باید به اندازه ارزش خود حفاظت گردند. در غیر این صورت، انتخاب مکانیسم‌های دفاعی چندان بهینه نخواهد بود و بدون شک دارای هزینه‌های غیر ضرور است.

بدیهی است آنهایی که قصد حمله داشته باشند تا دندان مسلح می شوند. پس باید ابتدا دارائی‌ها و عناصراصلی و اساسی اطلاعاتی اشیاء مهم در فضای سایبری را تعریف و تعیین نموده و براساس سیاست‌های کلان و با در نظر گرفتن تمامی تهدیدات، تمهیدات دفاعی را پی‌ریزی نمائیم.

مشخصه های یک UTM خوب

با توجه به هدف تهیه UTM، که یکپارچه سازی و مدیریت ابزارهای امنیتی در یک بسته کامل با مدیریت یکپارچه است مهمترین بخش یک UTM سیستم مدیریتی آن می باشد که استفاده از همه ابزارهای امنیتی را ساده تر می کند و همچنین بازدهی را افزایش می دهد. در ادامه تمامی ویژگی های یک UTM که مدیران شبکه با توجه به نیاز سازمان و شبکه مورد نظر مورد بهره برداری قرار می دهند، ارائه شده است.

- Firewall

دیواره آتش امکان برقراری امنیت در لایه‌های ۳ و۴ شبکه را فراهم می‌کند. دیواره آتش با بررسی آدرس IP و شماره پورتهای مبدا و مقصد بسته عبوری و انطباق این موارد با قوانینی که مدیر شبکه مشخص کرده است، اجازه عبور یا عدم عبور بسته را صادر می‌کند.

در واقع فایروال وسیله‌ای است که کنترل دسترسی به یک شبکه را بنابر سیاست امنیتی شبکه تعریف و اعمال می‌کند. علاوه بر این، از آنجا که معمولاً یک فایروال بر سر راه ورودی یک شبکه قرار می گیرد لذا برای ترجمه آدرس شبکه نیز بکار گرفته می شود.

مشخصه‌های مهم یک فایروال قوی و مناسب جهت ایجاد یک شبکه امن عبارتند از:

- توانایی ثبت و اخطار: ثبت وقایع یکی از مشخصه‌های بسیار مهم یک فایروال به شمار می‌رود و به مدیران شبکه این امکان را می دهد که حملات را کنترل کنند. همچنین مدیر شبکه می تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می تواند براحتی به بخشهای مهم از اطلاعات ثبت شده دسترسی پیدا کند. همچنین یک فایروال خوب باید بتواند علاوه بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را از وقایع مطلع کند و برای وی اخطار بفرستد.

- بازدید حجم بالایی از بسته‌های اطلاعات: از جمله تست های یک فایروال، توانایی آن در بازدید حجم بالایی از بسته‌های اطلاعاتی بدون کاهش چشمگیر کارایی شبکه است. حجم داده ای که یک فایروال می‌تواند کنترل کند برای شبکه‌های مختلف متفاوت است اما یک فایروال قطعاً نباید به گلوگاه شبکه تحت حفاظتش تبدیل شود. عوامل مختلفی در سرعت پردازش اطلاعات توسط فایروال نقش دارند. بیشترین محدودیت ها از طرف سرعت پردازنده و بهینه سازی کد نرم افزار بر کارایی فایروال تحمیل می شوند. عامل محدودکننده دیگر می‌تواند کارتهای واسطی باشد که بر روی فایروال نصب می شوند. فایروالی که بعضی کارها مانند صدور اخطار، کنترل دسترسی مبنی بر URL و بررسی وقایع ثبت شده را به نرم افزارهای دیگر می‌سپارد از سرعت و کارایی بیشتر و بهتری برخوردار است.

- سادگی پیکربندی: سادگی پیکربندی شامل امکان راه اندازی سریع فایروال و مشاهده سریع خطاها و مشکلات است. در واقع بسیاری از مشکلات امنیتی که دامنگیر شبکه‌ها می شود به پیکربندی غلط فایروال بر می‌گردد. لذا پیکربندی سریع و ساده یک فایروال، امکان بروز خطا را کم می کند. برای مثال امکان نمایش گرافیکی معماری شبکه و یا ابزاری که بتواند سیاستهای امنیتی را به پیکربندی ترجمه کند، برای یک فایروال بسیار مهم است.

- امنیت و افزونگی فایروال: امنیت سیستم فایروال خود یکی از نکات مهم در یک شبکه امن است. فایروالی که نتواند امنیت خود را تامین کند، قطعاً اجازه ورود هکرها و مهاجمان را به سایر بخش های شبکه نیز خواهد داد. عوامل موثر بر امنیت سیستم های دیوار آتش به شرح زیر می باشد:

- الف- امنیت سیستم عامل فایروال: اگر نرم افزار فایروال بر روی سیستم عامل جداگانه ای کار می‌کند، نقاط ضعف امنیتی سیستم عامل، می تواند نقاط ضعف فایروال نیز به حساب آید. بنابراین امنیت و استحکام

سیستم عامل فایروال و بروزرسانی آن از نکات مهم در امنیت فایروال است.

- ب- دسترسی امن به فایروال جهت مقاصد مدیریتی: یک فایروال باید مکانیزم های امنیتی خاصی را برای دسترسی مدیران شبکه در نظر بگیرد. این روش ها می تواند رمزنگاری را همراه با روش های مناسب تعیین هویت بکار گیرد تا بتواند در مقابل نفوذگران تاب بیاورد.

- Intrusion Detection/Prevention

یک سیستم تشخیص نفوذ عبارتست از ابزاری که منحصراً برای پایش دروازه‌های اطلاعاتی، فعالیت های خصمانه و نفوذهای شناخته شده پیکربندی شده‌است. یک IDS ابزاری تخصصی است که بخوبی قادر است ترافیک شبکه یا فعالیتهای میزبانهای آنرا تجزیه و تحلیل کند. داده‌های تحلیل شده می‌تواند از آنالیز بسته‌های شبکه گرفته تا محتوای فایلهای Log متعلق به فایروالها، روترها و سرویس‌دهنده‌ها و نیز فایلهای Log سیستم‌های محلی و داده‌های جریان شبکه را شامل شود. بعلاوه، یک IDS معمولا دارای یک پایگاه‌داده از الگوها و مشخصه‌های حملات شناخته شده است که می‌تواند این الگوها و مشخصه‌ها را با داده‌های ترافیک شبکه و رفتار شبکه برای یافتن موارد انطباق مقایسه کند. در مواجهه با موارد یافته شده ترافیک خطرناک، سیستم تشخیص نفوذ می‌تواند هشدارهایی را اعلام کرده یا اقدامات خودکار مختلفی را همچون قطع جلسه ارتباطی یا لینک اینترنتی مبدأ حمله، مسدود کردن وی با به‌روز کردن قواعد فایروال یا انجام دادن فعالیتهای بیشتر در جهت شناخت دقیق تر نفوذکننده و جمع‌آوری شواهد بیشتری در مورد فعالیتهای شرورانه انجام دهد. درصورتی که یک سیستم IDS توان پیشگیری از نفوذ را نیز داشته باشند به عنوان IPS معرفی می‌شوند، که در این حالت معمولا سیستم تشخیص نفوذ یا با فایروال در ارتباط بوده و بسته‌ها را از آن دریافت می‌کند و یا اینکه خود در لایه‌های پایینی هم سطح فایروال قرار داشته و فعالیت جلوگیری از نفوذ را نیز انجام می‌دهد.

- شبکه اختصاصی مجازی(VPN)

VPN دو کامپیوتر یا دو شبکه را به کمک یک شبکه دیگر که به عنوان مسیر انتقال به کار می گیرد به هم متصل می کند. برای نمونه می توان به دو کامپیوتر یکی در تهران و دیگری در مشهد که در فضای اینترنت به یک شبکه وصل شده اند اشاره کرد. VPN از نگاه کاربر کاملاً مانند یک شبکه محلی به نظر می رسد. برای پیاده سازی چنین ارتباطی، VPN به هر کاربر یک ارتباط مجازی می دهد.

داده‌هایی که روی این ارتباط رفت و آمد دارند را سرویس گیرنده نخست به رمز در آورده و در قالب بسته‌ها بسته بندی کرده و به سوی سرویس دهنده VPN می فرستد. اگر بستر این انتقال اینترنت باشد بسته‌ها همان بسته‌های IP خواهند بود.

سرویس گیرنده VPN بسته‌ها را پس از دریافت رمز گشایی کرده و پردازش لازم را روی آن انجام می دهد.

- آنتی ویروس

ویروس ها برنامه‌هایی هستند که به شکل پنهانی، موقع اجرا شدن برنامه آلوده، خود را به برنامه‌های اجرایی نظیر فایل‌های COM و EXE می چسبانند و معمولا بدون اینکه تاثیری در کار اصلی برنامه آلوده بگذارند، منتظر زمان فعالیت نهایی یا برقراری شرط خاصی می شوند. حال این فعالیت می تواند بزرگتر کردن فایلهای مختلف DATA یا آلوده کردن فایلهای اجرایی و یا از بین بردن اطلاعات PARTITION TABLE، معدوم کردن اطلاعات با ارزش یا از کار انداختن فایل های اجرایی و ... باشد. ولی در هر حال یک چیز در اکثر ویروس ها مشترک می باشد و آن انتقال ویروس از فایل های آلوده به فایل های سالم است.

آنتی ویروس با بررسی محتوای بسته‌های عبوری از UTM، در صورت وجود ویروس در بسته مورد نظر، اجازه عبور بسته را نمی‌دهد. ویروس‌یاب با جلوگیری از ورود ویروسها از اینترنت و شبکه های دیگر به شبکه داخلی، به میزان زیادی از آلودگی شبکه داخلی در برابر ویروسها محافظت می‌کند. وجود آنتی ویروس به برقراری امنیت در لایه ۷ کمک می‌کند. ویروس‌یاب‌های مسیر Gateway به جای جستجوی فایلها، بسته عبوری را جستجو می‌کنند.

یکی از معیارهای تشخیص قدرت ویروس‌یاب مسیر Gateway، تعداد پروتکل‌های تحت پوشش ویروس‌یاب است. همچنین بهتر است ویروس‌یاب پروتکل های HTTP, FTP, SMTP, POP۳ IMAP, IM VPN را ویروس‌یابی کند. همچنین بهتر است از یک موتور جستجوی ویروس معتبر در ساختار UTM استفاده شود.

نرم‌افزارهای آنتی ویروس تمام فایل‌ها را بطور خودکار بررسی کرده و فایل‌هایی که دارای گونه‌های شناخته شده ویروس‌ها هستند را شناسایی و عکس‌العمل مناسب انجام می‌دهند.

- آنتی اسپم

اسپم در کامپیوتر به ایمیل‌هایی گفته می شود که به طور ناخواسته برای ما فرستاده می شوند و جنبه تبلیغاتی دارند. راه‌های مختلفی برای مقابله با اسپم ها در جاهای مختلف آمده و حتی یاهو هم استفاده از یک آنتی اسپم را برای کاربرانش پیشنهاد کرده است.

- فیلترینگ

فیلتر ابزاری است که به منظور تصفیه اتصالات وب استفاده می‌شود. در کشورهای مختلف دنیا، فیلترینگ به دو روش انجام می‌شود: فیلتر کردن نشانی‌های اینترنتی براساس یک لیست سیاه(در یک پایگاه داده)، و فیلتر کردن براساس محتوای هر صفحه اینترنتی. روش دوم در دنیا به فیلتر محتوا (content filter) معروف است که برای پهنای باند خیلی بالا قابل انجام نیست.

- مدیریت پهنای باند[1]

به منظور تقسیم بهینه پهنای باند اینترنتی بین گروههای مختلف کاربران بر اساس نیاز کاری آنها، می‌توان از این امکان سود برد. همچنین از این امکان می‌توان برای تقسیم پهنای باند خطوط ارتباطی WAN بین نقاط مختلف استفاده کرد.

- Web Caching

به منظور افزایش سرعت دسترسی کاربران به اطلاعات شبکه اینترنت، می‌توان داده‌هایی را که کاربران به آنها مراجعه بیشتری دارند، در دستگاه UTM ذخیره‌سازی کرد. با این کار، کاربران در زمان‌های بعدی در صورت نیاز به این اطلاعات، به جای اینترنت آن‌ها را از دستگاه UTM دریافت می‌کنند. بیشتر UTMها از امکان Caching برخوردار نیستند.

- نوع سیستم عامل مورد استفاده درUTM

نوع سیستم عامل بکار گرفته شده در UTM در حوزه تامین امنیت سیستم بسیار حایز اهمیت می باشد.

ملاحظات پدافند غیر عامل در شبکه هایPAP

به منظور حفاظت از تجهیزات شرکت هایPAP و برقراری امنیت خدمات شبکه های ADSL با رویکرد پدافند غیر عامل و به منظور دست یافتن به اهداف ترسیم شده در اسناد پدافند غیر عامل موارد زیر می تواند تا حدود زیادی مشکلات مهم را در این حوزه برطرف نماید :

- تجهیزاتی که دارای بیشترین نیاز امنیتی هستند، در امن ترین منطقه قرار گیرند و اجازه دسترسی عمومی به آنها و یا از سایر شبکه های دیگر به این منطقه داده نشود. دسترسی ها باید با کمک یک فایروال و

---

[1] Bandwidth Management

یا سایر امکانات امنیتی مانند دسترسی از راه دور[1] به طور امن کنترل شود. همچنین کنترل شناسایی و احراز هویت و مجاز یا غیر مجاز بودن در این منطقه باید با درجه امنیت بالایی انجام شود.

- سرورهایی که در این شبکه ها مورد استفاده و دسترسی هستند، در منطقه ای جداگانه و دارای ضریب امنیتی بالاتر نسبت به سایر بخش ها قرار گیرند تا در صورت مورد حمله قرار گرفتن یکی، سایرین مورد تهدید قرار نگیرند. به این مناطق مناطق خارج از تهدیدات نظامی[2] گفته می‌شود.

- از فایروال ها به صورت لایه ای استفاده شود، استفاده از فایروال ها به شکل لایه ای و به کارگیری فایروال های مختلف سبب می‌شود تا درصورت وجود یک اشکال امنیتی در یک فایروال، کل شبکه به مخاطره نیفتاده و امکان استفاده از کد های جاسوسی و خرابکارانه نیز به حداقل برسد.

- امکان استفاده از تهدیدات مربوط به استراق سمع که طی آن دشمن می تواند بدون اطلاع طرفین، اطلاعات و پیامها را شنود کند، به حداقل برسد. استفاده از فضاهای امن در قسمت های passive و active می تواند به این مساله کمک کند.

- حملات مرتبط با تحلیل ترافیک که طی آن بر اساس یک سری بسته های اطلاعاتی، مهاجم می تواند ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب کند، شناسایی شود. این حملات از نوع غیر فعال است و اکثراً توسط کاربران خارجی صورت می گیرد.

- امکان دستکاری پیامها و داده ها که بر اساس آن مهاجم می تواند جامعیت و صحت اطلاعات را با تغییرات غیر مجاز برهم زند از

---

[1]. RAS: Remote Access Control

[2]. DMZ: Demilitarized Zone

بین برود. این نوع حملات نیز توسط کاربران خارجی صورت می‌گیرد. همچنین امکان جعل هویت که طی آن مهاجم هویت یک فرد مجاز شبکه را جعل می کند به حداقل میزان ممکن برسد.

- امنیت ارتباطات که در آن با استفاده از فایروال ها، سیستمهای ضد ویروس، سرورهای کنترل دسترسی و احراز هویت، نرم افزارهای مانیتورینگ، ثبت و تحلیل رویدادها می توان به تشخیص هویت و کنترل کاربران پرداخت، به وجود می آید.

- امنیت سیستم ها که در آن با بهره گیری از پویشگرهای امنیتی، آنتی ویروسها، IDS[۱] وIPS[۲] به ثبت و کنترل دسترسی کاربران به منابع پرداخته می‌شود، لحاظ شود.

- سطوحی از امنیت کاربردها به وجود آید که طی آن با بهره گیری از سیستمهای IDS، آنتی ویروس، پویشگر امنیتی و فیلترهای محتوا بر دسترسی کاربران نظارت می‌شود.

- از مدل هایی از مسیریاب ها استفاده شود که سیاست های امنیتی در قبال کلاینت ها در آنها کاملا رعایت شده است و همچنین در مسیریابها، سعی شود که تهدیدها شناسایی شده و از دسترسی شبکه های ناشناس جلوگیری گردد.

- از دیواره های آتش[۳] برای رسیدن به امنیت برای کاربران استفاده شود که این امر در بسیاری از مسیریابها تعبیه شده است.

- ایجاد مکانیزم تولید و تغییر کلید رمز کننده اطلاعات[۱] داخل مسیریابها برای بالابردن ضریب ایمنی لحاظ شود و همچنین تشخیص و شناسایی

---

۱ Intrusion Detection System

۲ Intrusion Prevention System

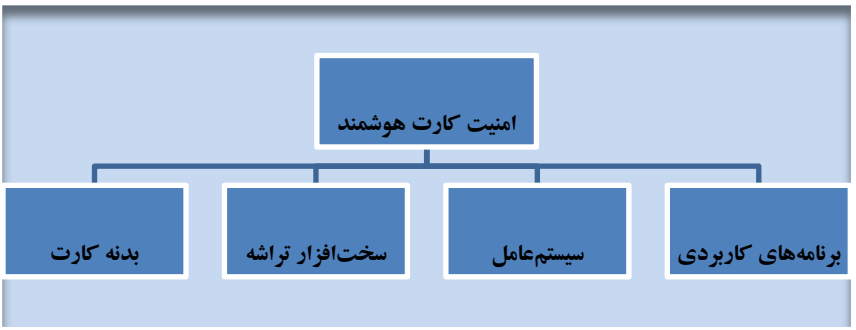
۳. Firewall

حملات خطرناک از طریق پست الکترونیکی و سایر روشها مورد نظر قرار گیرد.

[1] IKE: Internet Key Exchange

ملاحظات پدافند غیرعامل در طراحی کارت هوشمند

موضوع امنیت، ایمنی و پایداری نقطه عطف اصلی در استفاده از این کارت ها است؛ از اینرو در این فصل نگاهی اجمالی به نیازها و ویژگی های امنیتی مورد نیاز در طراحی یک کارت هوشمند در جهت مصونیت از خطرات متصور در فضای جنگ سایبر و مخاصمات بین الملل خواهیم داشت.



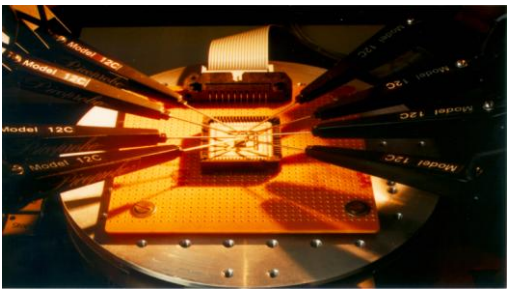
- طراحی کارت هوشمند در هنگام توسعه می بایست شامل یک مکانیزم امنیتی بومی و منتشرنشده باشد که تنها طراح از آن مطلع است و این مکانیزم از دیدگاه طراح به عنوان شرط تضمین کننده برقراری امنیت کارت هوشمند منظور گردد.
- هیچ کدام از باس های درونی تراشه که پردازنده را به حافظه های ROM، RAM و EEPROM متصل می سازند، نباید بیرون از تراشه قرار گیرند و نباید امکان برقراری هیچ گونه اتصال مستقیمی از بیرون به این باس ها وجود داشته باشد.
- از آنجا که در حال حاضر به علت محدودیت های موجود، امکان تولید تراشه در داخل کشور مقدور نمی باشد و با توجه به تهدیدهایی نظیر آنچه که در جنگ های اطلاعاتی روی می دهد و یا دیگر برنامه های تخریبی دشمنان، جهت عدم وابستگی به یک فراهم کننده ماژول کارت

هوشمند، باید حداقل از چند فراهم کننده مختلف که تأمین کننده نیازهای امنیتی ماژول مورد نظر باشند استفاده نمود؛ تا در صورت اعمال تحریم توسط یک فراهم کننده برای کشور، نسبت به آن فراهم کننده وابستگی بوجود نیاید و بتوان ماژول های تهیه شده از فراهم کنندگان دیگر را جایگزین ماژول فعلی نمود؛ هرچند رویکرد بهینه برای مرحله تولید کارت، انتقال فناوری تولید و ساخت تراشه های کارت هوشمند در داخل کشور است.

- یک کارت هوشمند نیاز به مکانیزمی برای تشخیص حمله دارد تا در مواقع لزوم در برابر آن واکنش نشان داده و به طور مثال کلیدهای محرمانه را پاک نماید؛ این مکانیزم می تواند توسط پروسه ای که غیر از شرایط نرمال عملکرد باشد ایجاد شود؛ بطور مثال ولتاژ بالاتر و یا تغییر نرخ کلاک پالس[۱]؛ از آنجایی که این شرایط در زمانی که خطایی در سامانه اتفاق بیافتد نیز ممکن است رخ دهد، معمولاً از مکانیزم اتوماتیکی برای بلوکه و یا پاک کردن کلیدها استفاده نمی شود؛ مگر در کاربردهای خاص استفاده از کارت هوشمند در حوزه های سری و خیلی محرمانه.
- در طراحی یک ماژول کارت هوشمند در سطح ملی، بایستی از ماژول چند لایه استفاده شده و در لایه فوقانی و تحتانی آن نباید اطلاعات ذخیره شود. این عمل در جلوگیری از دسترسی به محتویات داخلی حافظه کارت بخصوصEEPROM تأثیر بسزایی خواهد داشت.

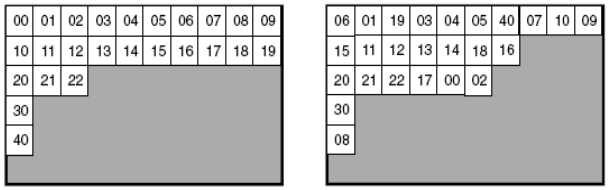
[۱] Clock pulse

- تحلیل ریزتراشه توسط پراب‌گذاری



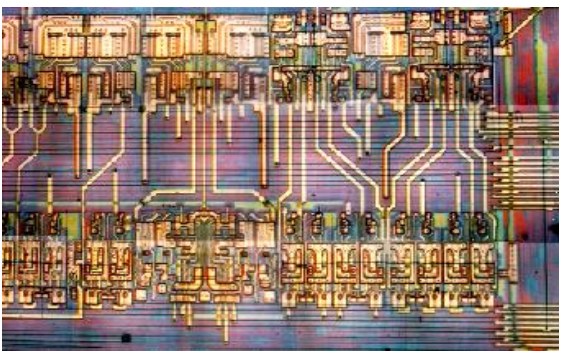
- اندازه های ساختاری فناوری نیمه هادی بکار رفته در سخت افزار تراشه در حدود یک میکرومتر در نظر گرفته شود.
- طراحی مدارهای مجتمع نیمه هادی تراشه شامل پردازنده و حافظه ها باید به گونه ای ویژه و جدا از روال های مرسوم طراحی در نظر گرفته شوند.
- جهت ایجاد مانع برای اسکن تراشه به منظور تعیین جزئیات آن، می بایست از لایه هایی فلزی در طراحی تراشه استفاده نمود.
- در هنگام طراحی بر روی سطح تراشه می بایست لایه های فلزی برای توزیع توان در نظرگرفته شوند.
- می بایست در کنار RAM از حسگری دمایی استفاده شود تا در صورت تغییر ناگهانی یا پایین آمدن بیش از حد مجاز دما، کلیدهای سری پاک شود. همچنین می بایست مکانیزمی برای پاک شدن محتویات، در صورت مقیم شدن طولانی مدت کلیدها یا پارامترهای سری، درون RAM وجود داشته باشد.
- فضای آدرس دهی سلول های حافظه درون تراشه با یک طرح درهم ریختگی منحصر به تراشه می بایست پیچیده سازی شود بنابراین حافظه EEPROM می بایست با یک طرح درهم ریختگی به طور

نرم افزاری آدرس دهی شود. در کنار درهم ریختگی می توان از رمزگذاری حافظه نیز استفاده نمود.



- پیچیده نمودن حافظه
- برای رمزگذاری فضای آدرس دهی سلول های حافظه می بایست از الگوریتم رمز بومی و قدرتمند استفاده نمود.
- ماژول مورد استفاده در کارت هوشمند ملی بایستی دارای حسگر نوری جهت تشخیص نفوذ و حمله فیزیکی به تراشه باشد و در صورت حمله، بایستی اقدامات لازم جهت جلوگیری از دسترسی مهاجم به اطلاعات حساس پیش بینی شده باشد.
- تراشه می بایست مجهز به یک مدار ناظر بر ولتاژ باشد تا در صورتی که ولتاژ تراشه از محدوده تعریف شده تجاوز نمود، آن را خاموش نماید.
- تراشه می بایست مجهز به مداری جهت نظارت بر فرکانس عملکرد تراشه باشد تا اگر فرکانس از نرخ کلاک تعریف شده کمتر یا بیشتر شد، عکس العمل نشان دهد.
- باس های درونی متصل به حافظه می بایست با یک طرح منحصر به تراشه درهم ریخته شوند.

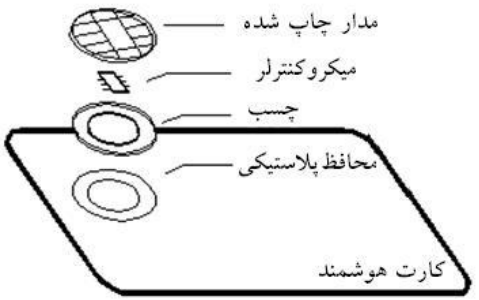
- پیچیده نمودن باس داده
- در برنامه ریزی تراشه می بایست دستورالعمل هایی با مصارف یکسان جریان به کارگیری شود .
- در کد اسمبلی نباید از دستورالعمل هایی که مصرف آنها با سطح میانگین تفاوت معنی داری دارد، استفاده شود.
- در الگوریتم رمز می بایست از چندین پروسه متفاوت برای اجرای محاسبات مشابه استفاده نمود.
- تراشه می بایست مجهز به رگولاتورهای ولتاژ سریع باشد تا جریان های مصرفی درون تراشه را یکسان سازی نماید. در صورت مجهز نبودن تراشه به رگولاتورهای ولتاژ سریع می بایست در درون آن مولدهای نویز مصنوعی تعبیه شده باشد تا توان مصرفی تراشه را یکنواخت نمایند.



لایه درونی تراشه زیرمیکروسکوپ

- وجود مقاومت حسگر برای تنظیم جریان مصرفی به صورت مستقل از دستورالعمل های اجرا شده، موجب جلوگیری از حملات توان مصرفی در صورت اجرای دستورالعمل های مختلف می گردد.

- تمهیدات و مکانیسم های امنیتی در نظر گرفته شده برای برنامه های کاربردی مختلف باید با توجه به ملزومات امنیتی آنها تعریف شود.
- بجز در موارد الزامی و مشخص، دسترسی به منابع و فایل ها در کارت هوشمند، بایستی محدود شود و سطوح دسترسی بایستی بصورت مشخص در مستندات آورده شود.
- بمنظور افزایش سطح امنیت، بایستی ارزیابی کارت در سطوح مختلف امکان پذیر باشد و نباید کلیه کلیدهای مورد نیاز جهت ارزیابی را تنها در یک پایانه نگهداری نمود.

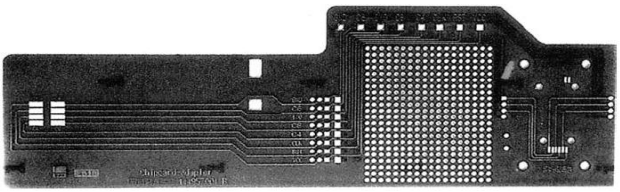


اجزای تشکیل دهنده کارت هوشمند

- می بایست تمهیدات لازم جهت بازگشت خودکار سامانه کارت به حالت اولیه در صورت بروز خطا پیش بینی گردد.
- لازم است برای افزایش ضریب امنیت، تصدیق اصالت دوطرفه صورت گیرد و همچنین اصالت کارت توسط پایانه و هم اصالت پایانه توسط کارت بررسی شود.
- در صورتی که ارتباط برخط برای هر تراکنش در کارت امکان پذیر نباشد بایستی محدودیت هایی برای حداکثر میزان تراکنش های برون خط برای یک پایانه و یک کارت در نظر گرفت.

- روتین دستورات و کلاس دستورالعمل های درون نرم افزار کارت نباید آشکار و عمومی یا قابل بازیابی توسط روال های کشف دستورالعمل ها باشد .

- بمنظور جلوگیری از بهره برداری از داده های در حال عملکرد می بایست از ترمینال هایی که توسط دیافراگم هایی اجازه اتصال سیم های اضافی به کارت را نمی دهند و یا مکانیزم پیام رسانی امن استفاده نمود.



آداپتور انتقال داده‌ها

- روتین نرم افزاری مقایسه PIN باید به گونه ای باشد که تمامی ارقام آن را به یکباره مقایسه نماید.

- اجرای مکانیزم های امنیتی نظیر رمزنگاری و احراز هویت می بایست مستقل از زمان پردازش داده ها وکلیدهای مختلف باشد تا حملات زمانی که با تحلیل زمان اجرای داده های مختلف کلید را حدس می زنند، قابل اجرا نباشد.

- الگوریتم های رمزنگاری بکاررفته باید عاری از نویز و مستقل از طول داده ها یا کلید های مختلف باشند.

- فلوچارت برنامه های نرم افزاری باید بسیار قوی طراحی شده باشد . برای این منظور در صورتیکه در بخش هایی از فلوچارت تصمیم گیری مورد نیاز باشد، می بایست برای هر یک از حالات ممکن برای یک شرط دستورالعملی به صورت مجزا وجود داشته باشد.

- حسگرهای آشکارساز پالس های ولتاژ و یا نور ناگهانی می توانند در تشخیص حمله هایی که با ایجاد خطا در عملکرد پردازنده و مشغول

نمودن آن موجب عدم پایداری پردازنده می گردند، نقش موثری داشته باشند.

- بهتر است از یک سیستم عامل بومی جهت استفاده در سامانه کارت هوشمند استفاده شود؛ لیکن در صورت عدم دسترسی به سیستم عامل بومی که دارای قابلیت های مورد نظر باشد،می توان بخشی از سیستم عامل های موجود را بومی سازی و از الگوریتم های اختصاصی برای قسمت های حساس سیستم عامل استفاده نمود.
- لازم است تمامی ارتباطات حساس کارت با ترمینال از جمله روال های احراز هویت توسط برنامه های رمزنگاری و با طول کلید سری مناسب رمز شوند.
- ثبات ها و شمارنده هایی که در برنامه، وظیفه نشان دادن اجرای عملی را دارند باید به گونه ای مخفی سازی شوند تا با بررسی آنها عمل انجام شده مشخص نباشد.
- می بایست طبق استاندارد خاصی ترتیب قرار گرفتن دستورالعمل در EEPROM پشت سر هم و با دقت صورت گیرد تا قطع توان باعث اجرا نشدن بخش امنیتی برنامه نشود.
- کارت هوشمند را باید بتوان در انتهای چرخه حیات به صورت کامل توسط سیستم عامل، غیر فعال نمود؛ اطلاعات غیر ضروری در پایان چرخه حیات کارت بایستی بطور کامل حذف گردند.

ملاحظات پدافند غیر عامل در حوزه سامانه مدیریت پایگاه داده

ملاحظات پدافند غیر عامل که باید در این حوزه رعایت شوند به اختصار در ذیل آورده شده است:

- به دلیل عدم توانایی سامانه مدیریت پایگاه‌داده رابطه ای در تأمین نیاز کاربردهای جدید همچون چندرسانه ای و بلادرنگ و ناتوانی آن در تعریف انواع داده جدید از جانب کاربر، همچنین عدم وجود استاندارد

واحد در سامانه‌های مدیریت پایگاه‌داده شیءگرا و پیچیدگی زبان انحصاری SQL آن، بسیاری از رویکردهای مطالعاتی و تجاری امروز مبتنی بر سامانه مدیریت پایگاه‌داده شیء– رابطه‌ای است. بدین منظور، ساخت سامانه مدیریت پایگاه‌داده مبتنی بر مدل داده ای شیء رابطه ای الزامی است.

- از آنجا که توزیع و تکرار داده ها در سایت‌های مختلف منجر به افزایش دسترس‌پذیری و قابلیت اطمینان سامانه مدیریت پایگاه‌داده می‌شود، لذا سامانه مدیریت پایگاه‌داده ملی باید به صورت نامتمرکز یا توزیع شده پیاده سازی شود.
- کانال ارتباطی مابین سامانه مدیریت پایگاه‌داده و خود پایگاه‌داده می بایست از طریق کانال ارتباطی امن صورت گیرد. مکانیزم امن سازی مناسب همچون رمزگذاری در این بستر ضروری است. می بایست مکانیزم هایی مبنی بر رمزگذاری در فرستنده و گیرنده از جانب سامانه مدیریت پایگاه‌داده تعبیه شود.
- استفاده از یک واسط ارتباطی ایمن به منظور تعامل با سامانه مدیریت پایگاه‌داده ضروری بوده و این سامانه می بایست به صورت بومی طراحی و پیاده سازی شود.
- مدیر ارتباطات مختوم می بایست از مکانیزم های کشف حملات عدم دسترس پذیری استفاده نماید.
- سیستم فایل مورد استفاده سامانه مدیریت پایگاه‌داده ملی لازم است سیستم فایل تعبیه شده ملی باشد.
- به منظور جلوگیری از دسترسی هر کاربر عادی به کاتالوگ سامانه مدیریت پایگاه‌داده که بخش حیاتی هر سامانه است، می بایست مکانیزمی مانند کنترل دسترسی، تمامی تعاملات کاربران با آن را کنترل کند. در بسیاری از سامانه‌ها ثبت وقایع در مورد تعاملات

کاری کاربران و کاتالوگ بکار گرفته می‌شود تا در مواقع اضطراری سامانه به وسیله آن به حالت معمول باز گردد.

- به منظور حفظ امنیت بیشتر در سامانه مدیریت پایگاه‌داده، می توان زیر سامانه مدیریت دیسک را به یک الگوریتم رمزنگاری مجهز نمود. این روش روند کشف اطلاعات توسط اشخاص/سامانه‌های دیگر را غیر ممکن یا حداقل بسیار کند می‌کند.
- به منظور افزایش قابلیت اطمینان سامانه مدیریت پایگاه‌داده، پایداری و دسترس‌پذیری آن از سرویس های انعکاس استفاده می‌شود. در میان روش های انعکاس، روش مبتنی بر ثبت وقایع نسبت به سایر روش ها کارآمدتر است.
- در مکانیزم تهیه نسخه پشتیبان بهتر است که داده ایمن گردد. داده ایمن می تواند توسط عملیات رمزگذاری یا استفاده از امضای دیجیتالی حاصل شود.
- مدیریت امنیت سامانه مدیریت پایگاه‌داده ملی لازم است به صورت نامتمرکز (توزیع شده) باشد.
- بررسی دقیق درخواست های ورودی به سامانه مدیریت پایگاه‌داده برای جلوگیری از تهدیداتی نظیر SQL Injection لازم است.
- سامانه مدیریت پایگاه‌داده ملی بهتر است تحت سیستم عامل‌های مختلف (اعم از ۳۲ بیتی و ۶۴ بیتی) قابل به کارگیری باشد.
- بهتر است سامانه مدیریت پایگاه‌داده دارای امکانات کافی جهت پردازش و جستجو در انواع داده از جمله متن باشد.یر عامل
- زبان پیاده‌سازی سامانه مدیریت پایگاه‌داده ملی بهتر است یک زبان توسعه یافته ملی باشد.
- بهتر است سامانه مدیریت پایگاه‌داده ملی مبتنی بر سیستم عامل توسعه یافته ملی باشد.

- از آنجا که واسط پایگاه‌داده، به عنوان یک backdoor، ضریب امنیتی را پایین می آورد، پیشنهاد می شود از واسط پایگاه‌داده ملی استفاده شود.
- در انتخاب یک سامانه برای ایجاد یک بستر انتخاب صحیح نوع لیسانس بسیار حیاتی است.

ویژگیهای یک IDS مطلوب

مشخصات مطلوب یک IDS بصورت زیر تعریف می شود:

- سیستم باید هر فعالیت مشکوک یا هر رویدادی که بالقوه ممکن است شروع کننده یک حمله باشد، شناسایی کند.
- حملات قبل از آنکه گسترش یابند باید در پائین ترین سطح ممکن تشخیص داده شوند.
- میزبانهای مختلف باید با هم ارتباط داشته و تبادل اطلاعات نمایند.
- باید مکانیسم هایی جهت کنترل و تنظیم سیستم برای مدیران شبکه وجود داشته باشد.
- سیستم باید با تغییر روشهای حمله، قادر به وفق دادن خود با آن حملات باشد و همچنین بتواند چندین حمله همروند را نیز شناسایی نماید.
- سیستم باید مقیاس پذیر بوده و به سادگی قابل توسعه باشد.
- باید غیر قابل انهدام باشد یعنی بتواند از خود محافظت کرده و حملات به خود را شناسایی نماید و همچنین خطای سیستم کم باشد.
- باید کمترین بار اضافی را بر روی سیستمی که در آن در حال اجرا می باشد تحمیل نماید.
- باید پاسخ مناسبی در برابر تغییر سطوح هشدار تولید نماید.

ملاحظات مسیریاب

با توجه به تهدیدات و حملاتی که به طور خلاصه در فصل قبل گفته شد، برای مقابله با آنها باید راهکار و تدابیری اندیشید که در این فصل به بعضی از این ملاحظات به اختصار اشاره می نماییم.

- اتخاذ تدابیر مناسب جهت بکارگیری مسیریاب های ستون فقرات شبکه در اتاق های شیلد با پوشش کلیه باندهای فرکانسی
- برقراری کنترل های دسترسی لازم جهت نظارت بر ترافیک ورودی و خروجی مسیریاب ها
- طراحی توپولوژی شبکه بصورت مقاوم در برابر انواع نفوذ
- بکارگیری قطعات سخت افزاری مطمئن در ساخت داخلی مسیریاب ها
- استفاده از پروتکل های امنیتی در مسیریابی شبکه
- ایجاد نظام کنترل دسترسی با امنیت بالا به منابع شبکه
- غیرفعال کردن سرویس مدیریت از راه دور مسیریاب ها در مواقع غیر ضروری
- ایجاد پروتکل های امنیتی مناسب بر روی سرویس مدیریت از راه دور
- ایجاد موانع مناسب جهت جلوگیری از اعمال نفوذ در سرویس مدیریت از راه دور مسیریاب
- استفاده از مسیریابهای پشتیبان جهت جلوگیری از وقفه در فعالیت شبکه
- نظارت دائم بر روی فعالیت مسیریاب به منظور کشف هرگونه فرآیند غیر عادی
- ایجاد سیستم گزارش گیری از ترافیک شبکه

همچنین برای کاهش تهدیدهای موجود در شبکه، می‌توان از ابزار و روشهای متنوعی استفاده کرد که به سه دسته تقسیم می شوند:

۱. ابزار و روش‌های "تصدیق هویت" کاربران
۲. ابزار و روش‌های پیشگیری[۱]، شناسایی و نشان دادن واکنش در برابر نفوذهای الکترونیکی شامل سیستم های تشخیص نفوذ و رویدادنامه ها، دیواره‌های آتش و تله‌های نرم‌افزاری و سخت افزاری می باشد.
۳. ابزار و روش‌های تامین امنیت ارتباطات نیز شامل شبکه های خصوصی، شبکه های خصوصی مجازی، مودم‌های امن و رمزنگاری داده‌ها می باشد.

و در آخر باید خاطر نشان کرد از منظرهای مختلف عملیاتی، اقتصادی و امنیتی و بطور کل بر اساس ضوابط و معیارهای پدافند غیرعامل در این زمینه، ساخت مسیریاب بومی بهترین راهکار مقابله با تهدیدات می باشد.

ملاحظات پدافند غیرعامل در طراحی سیستم عامل

در این فصل از کتابچه به بیان برخی از مهمترین ملاحظات پدافند غیرعامل در حوزه طراحی سیستم عامل خواهیم پرداخت:

- کد منبع سیستم‌عامل مورد استفاده در کشور بایستی در دسترس متخصصان ذیربط قرار داشته باشد و مورد بررسی قرار گیرد. عدم دسترسی به کد سامانه و عدم امکان بررسی باعث می‌شود تا تولیدکننده سیستم‌عامل بتواند با وارد نمودن برنامه‌های ویژه‌ای در سامانه هدف نفوذ کرده و موجب جاسوسی، شنود هوشمندانه و بوجود آمدن اختلال در عملکرد برنامه‌های کاربردی شود.

---

۱ Prevention

- انجام بررسی‌های لازم بر روی کد منبع سیستم‌عامل از لحاظ امنیت دسترسی به اطلاعات و ثبات عملکرد در آزمایشگاه‌های امنیت سیستم عامل در داخل کشور ضروری است.
- طراحی و استفاده از یک معماری امن برای داشتن یک سیستم‌عامل امن ضروری است.
- در طراحی و پیاده‌سازی سیستم‌عامل باید یک سامانه ثبت وقایع با قابلیت ثبت نوع درخواست، شناسه کاربر و اجرای برنامه وجود داشته باشد.
- در فایل‌سیستم امن می‌بایست قابلیت کنترل مجوز دسترسی در خصوص سطح دسترسی، مالکیت و مجوزهای اعمال تغییرات روی فایل‌ها وجود داشته باشد.
- از فایل‌های اصلی حاوی اطلاعات مهم کاربری مانند کلمه عبور باید حفاظت به عمل آورد و تنها کاربر ریشه به آن‌ها دسترسی داشته باشد.
- می بایست مکانیزم‌های کنترلی خاص در طراحی سامانه مدیریت فرآیند، ایجاد و پیاده‌سازی گردد؛ بطوریکه فرآیندهای مخاطره آمیز مسدود و اطلاعات آنها و کاربران اجرا کننده ثبت و گزارش شود.
- سرویس‌های غیر ضرور، هنگام ارائه محصول به کاربر نهایی می‌بایست غیرفعال باشند.
- در دستگاه‌های ورودی/خروجی برای ایجاد مکانیزم‌های محافظتی باید برای دسترسی هر کاربر، رمز ورود تقاضا شده و متناسب با هر سطح دسترسی، امکانات معینی از سامانه در اختیار کاربر قرار گیرد.
- سیستم عامل ملی می‌بایست 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 سیستم‌عامل ملی می‌بایست امکانات و قابلیت‌های لازم جهت پشتیبانی از استانداردها و پروتکل‌های امن‌سازی سیستم‌عامل پیش بینی شود.
- برای هر سیستم‌عامل مورد استفاده در مراکز کشور باید نمایه حفاظتی متناسب با اهمیت آن مرکز تعریف شود و سیستم‌عامل بکارگیری شده از منظر امنیتی توسط یک نهاد معتبر و مطمئن، ارزیابی و تائید گردد.
- سیستم‌عامل از نظر تداوم اجرا می‌بایست متناسب باشد؛ به بیان دیگر در شرایط از کار افتادن برخی از قسمت‌های سامانه، سیستم‌عامل مورد استفاده باید قادر باشد توابع و عملکردهای اصلی سامانه را همچنان قابل استفاده نگه‌دارد.
- طراحی سیستم‌عامل باید به ترتیبی باشد که بسامد بروز شکست یا خطای ناشی از عیوب سیستم‌عامل تا حد ممکن پایین باشد.
- عواملی همچون توانایی بازگرداندن خدمات سیستم‌عامل به سطح کارایی تعیین شده، توانایی بازگرداندن داده‌هایی که مستقیماً تحت تأثیر خرابی بوده‌اند و زمان لازم و تلاش مورد نیاز برای انجام این کارها؛ تاثیر بسزایی در افزایش زمان برپابودن[۱] سامانه می‌گذارد، مجموعه این نکات همواره می‌بایست جزء اصلی‌ترین مؤلفه‌های طراحی یا انتخاب یک سیستم‌عامل قرار گیرد.
- قابلیت پایداری سیستم‌عامل شامل قابلیت تداوم اجرا[۲]، تحمل در برابر عیب و خطای ناشی از طراحی سامانه[۳]، میزان بلوغ[۴] و قابلیت

---

[۱] Uptime

[۲] Survivability

[۳] Fault Tolerance

[۴] Maturity

بازگرداندن[1] داده‌ها و خدمات به حالت عادی (مورد اشاره در ملاحظات قبل)، عاملی کلیدی محسوب می‌شود که باید مورد توجه قرار گیرد.

- پیش از استفاده می‌بایست میزان کارایی سیستم‌عامل هدف از نظر زمان و مدیریت منابع در یک آزمایشگاه مجهز و مطمئن، ارزیابی و تعیین شود.
- بروزرسانی منظم، دقیق و متناسب با اهمیت کارکردی سیستم‌عامل، فرآیندی است که مرتباً باید انجام پذیرد.
- تشکیل تیم‌های متعدد فنی، زبده و مجرب برای ارائه خدمات سریع، صحیح و مطمئن به سیستم‌عامل‌های مستقر در مراکز کشور جهت تضمین پایداری کل سامانه کامپیوتری و تشکیل مراکز پشتیبانی ضروری است.
- ویژگی‌های قابلیت بکارگیری (شامل چگونگی نصب و راه‌اندازی، میزان کاربرپسندی[2]، میزان شناسایی سخت‌افزارهای کامپیوترهای سازمان، میزان یکپارچگی و سازگاری با بستر سخت‌افزاری موجود، امکانات نرم-افزاری همراه و یکپارچه با سیستم‌عامل، تعداد و نوع قالب‌ها و پروتکل‌های استاندارد پشتیبانی شده توسط سیستم‌عامل) در طراحی، پیاده‌سازی و ارزیابی سیستم‌عامل کامپیوترهای شخصی سازمان‌ها و مراکز مهم باید مورد توجه خاص قرار گیرد.
- استفاده از قالب فایل‌ها و پروتکل‌های ارتباطی استاندارد یا استانداردسازی آن‌ها، به منظور کاهش هزینه‌ها، افزایش قابلیت همکاری سامانه‌ها، افزایش کیفیت خدمات و نهایتاً نظارت بر حسن عملکرد سامانه‌ها، لازم است

---

[1] Recoverability

[2] User-Friendly

دستورالعمل های پدافند غیر عامل در حوزه الکترومغناطیس

- دستورالعمل های قبل از بحران

رعایت یک سری از نکات و پیاده سازی آنها در شرایط صلح و قبل از وقوع بحران، به صورت موثری می تواند هزینه های ناشی از آسیب دیدگی تجهیزات در شرایط وقوع بحران را کاهش دهد. نکات مورد نظر شامل موارد ذیل می باشد:

- برنامه ریزی استراتژیک و تدوین دستورالعمل های مدیریتی:

این برنامه ریزی ها به تدوین دستورالعمل های مدیریتی و اجرایی منجر خواهد شد. برخی از نکات مهم که در این دستورالعمل ها باید رعایت شوند عبارتند از:

- توزیع افراد بر اساس تخصص فنی مورد نیاز جهت تعمیر، نگهداری و پشتیبانی برای هر بخش صورت گرفته شود.
- دفترچه های تعمیر و راه اندازی سیستم های آسیب پذیر مربوط به هربخش با استفاده از تیم خبره فنی آماده شود.
- توجه دقیق به دستورالعمل راه اندازی سیستم ها و تجهیزات هر بخش در شرایط وقوع بحران و پس از بحران صورت گیرد.
- در صورتی که توسعه سایت مد نظر باشد، پیاده سازی و اجرای تجهیزات جدید باید منطبق با اصول پدافند غیر عامل در حوزه بحران الکترومغناطیسی باشد.
- ارزیابی آسیب شناسی، مقاوم سازی و دستورالعمل های نگهداری:

این اقدام که با همراهی افراد متخصص در آسیب شناسی و افراد مجری بخش باید انجام شود، منجر به تهیه چک لیست اولیه از لحاظ نوع آسیب، میزان آسیب پذیری، راهکار رفع آسیب(تعمیر، تعویض یا خاموش و

روشن نمودن مجدد)، زمان مورد نیاز جهت راه اندازی و هزینه رفع آسیب خواهد شد.

- مقاوم سازی الکترومغناطیسی ساختار ها و تجهیزات:

این اقدامات به دو گروه عمومی و اختصاصی تقسیم می گردند.

۱. گروه عمومی: اقداماتی که در مورد کلیه سطوح مقاوم سازی لازم الاجرا هستند، که به ترتیب اولویت عبارتند از:

- دیواره های محافظ
- درب های محافظ
- مدارات محافظت کننده
- فیلترهای کانال تهویه
- اتصال زمین مناسب
- دکلها و آنتن ها و ...

۲. گروه اختصاصی: اقدامات خاص که برای رسیدن به سطوح اول، دوم یا سوم مقاوم سازی لازم الاجرا هستند؛ مانند: سطح دوم شیلد دیواره، استفاده از توری و شیشه هادی در پنجره و ...

یک نمونه محفظه طراحی و ساخته شده از جنس آلومینیوم با ضخامت
حدود ۱ تا ۱.۵ میلی متر برای حفاظت تجهیزات حساس

شبکه هشدار دهندگی:

سنسورهای هشدار دهنده پالس های الکترومغناطیسی می توانند هرگونه مخاطره الکترومغناطیسی در باند پایین فرکانسی و مایکروویو را اعلام نمایند. این هشدار برای شروع آماده باش و عملیات پدافندی لازم است.

هشدار دهنده ها می بایست از نظر انتشار امواج الکترومغناطیسی و فضای سیستم های خودی در محل های مناسبی تعبیه شوند.

یک نمونه هشدار دهنده بحران الکترومغناطیسی

- آموزش بصورت توسعه ای و کلاسیک:

مفاهیم بحران الکترومغناطیسی، منابع بحران، آسیب پذیری ها و راهکارهای مقاوم سازی در سطوح کارشناسی و مدیریتی می بایست به کاربران مرتبط آموزش داده شود. این آموزش ها می تواند بصورت کارگاه های آموزشی کوتاه مدت برای مدیران و دوره های میان مدت برای کارشناسان فنی برگزار گردد.

بروشورها و دفترچه های حاوی اطلاعات کلیدی که دارای نکات مفید در خصوص اصول پدافند غیرعامل در حوزه مورد نظر می باشند بایستی تهیه و در اختیار افراد مسئول هر بخش قرار داده شود.

همچنین می بایست تمهیداتی جهت آگاه نمودن تیم های تخصصی و ارائه آموزش های مستمر جهت راه اندازی مجدد بخش های آسیب پذیر با کمترین هزینه در شرایط وقوع بحران و پس از بحران اندیشیده شود.

موضوعات اصلی این آموزش ها شامل موارد زیر می باشد:

- آموزش نصب و قرائت هشدار دهنده ها
- آزمایش دوره ای چاه و اتصال زمین
- آزمایش دوره ای اتصالات
- دستورالعمل های حین وقوع بحران

این دستورالعمل ها می بایست از لحظه وقوع بحران الکترومغناطیسی بکار گرفته شود. فعال شدن سیستم هشداردهنده همراه با وقوع اختلال در عملکرد سیستم ها و تجهیزات الکترونیکی، کنترلی و مخابراتی حساس سایت ها از جمله نشانه های بروز چنین بحران هایی می باشد. اختلال در عملکرد، سبب وقوع حوادث غیر قابل پیش بینی برای سیستم ها و

تجهیزات «مقاوم نشده» می گردد و تا زمانیکه سیستم ها به حالت طبیعی بازنگردند احتمال وقوع هرگونه حادثه وجود دارد.

- در شرایط وقوع تهدید الکترومغناطیسی

موارد اساسی ذیل می بایست در اسرع وقت توسط کارشناسان و مدیران مربوطه انجام گیرد:

- به علائم هشداردهنده ها توجه شود:

در زمان بحران، هنگامی که بخش های فرآیندی و عملکردی تجهیزات الکترونیکی و ... دچار مشکل شده اند، اولین اقدام، بررسی وضعیت سیستم هشداردهنده می باشد. اگر این سیستم، فعال باشد(وجود اعلام خطر)، باید دستورالعمل های مربوط به زمان بحران، اجرا شود. در غیر اینصورت باید به دستورالعمل های معمول مربوط به تعمیر و نگهداری سیستم ها و تجهیزات مراجعه نمود.

- صحت عملکرد گیرنده ها و بخش های مختلف که دارای دریافت کننده های داده می باشند، بررسی شود.
- برنامه های اجرایی و بخش های مختلف الکترونیکی وکامپیوتری بررسی شود.
- دستگاه هایی که قابلیت خاموش شدن دارند، خاموش شوند.
- سیستم های اطفاء حریق و عملکرد آنها بررسی شود.

- دستورالعمل های پس از وقوع بحران
  - توجه به هشدار دهنده ها:

پس از گذر از زمان بحران، می بایست هشدار دهنده ها بررسی شده، راه اندازی مجدد یا در صورت خرابی جایگزین شوند.

- برآورد آسیب های وارده:

در صورت وقوع بحران و ایجاد اختلال در عملکرد سیستم ها و تجهیزات سایت به دلیل آسیب، مراحل ذیل باید به اجرا در آید:

- مراجعه تکنیسین بخش آسیب دیده به همراه کارشناسان فنی
- شناسایی نوع آسیب گذرا یا دائمی بوجود آمده برای بخش
- ارزیابی عملکرد المان، قطعه یا سیستم آسیب دیده با توجه به مشخصات تعریف شده برای سیستم مورد نظر[1]
- ارائه گزارش مربوط به دسته بندی سیستم ها یا قطعات آسیب دیده به همراه بیان نیازمندی ها و ضرورت ها، بمنظور برآورد آسیب جهت راه اندازی مجدد.
- راه اندازی مجدد سیستم ها:

بر اساس گزارش تهیه شده توسط کارشناسان فنی و نوع آسیب ایجاد شده مراحل ذیل باید اجرا شود.

- بخش های آسیب دیده به لحاظ ایجاد توقف در عملکرد کلی سیستم بایستی اولویت بندی شوند .
- با توجه به اولویت بندی صورت گرفته، نسبت به راه اندازی آنها اقدام شود.
- در صورتی که آسیب از نوع گذرا باشد، تغذیه سیستم قطع و وصل گردد. در این شرایط امکان راه اندازی و بازگشت به حالت عادی برای سیستم، محتمل خواهد بود.
- در صورت عدم بازگشت به حالت عادی، متخصصین بخش تعمیر و نگهداری با توجه به دستورالعمل های حفاظتی اقدام نمایند.

---

[1] محتمل ترین بخش آسیب دیده در هر سیستم، قسمت‌های ورودی یا خروجی(تغذیه، دیتا، مخابراتی و کامپیوترها) می باشد. این قسمتها جهت ارزیابی در اولویت اول قراردارند.

- در صورتیکه آسیب از نوع دائمی قابل مشاهده باشد، متخصصین بخش تعمیر و نگهداری با توجه به دستورالعمل های حفاظتی اقدام نمایند.

- استفاده از سیستم های پشتیبان حفاظت شده:

در شرایط وقوع بحران، امکان آسیب دیدگی برای تجهیزات حساس الکترونیکی و مخابراتی که در انبار قطعات نگهداری می شوند نیز وجود دارد. بمنظور نگهداری تجهیزات در انبار می بایست اصول مربوط به مقاوم سازی را اجرا نمود. در صورت نیاز به قطعات و تجهیزات (وجود آسیب دیدگی) جهت تعمیر یا تعویض، می بایست از قطعات و تجهیزات پشتیبان حفاظت شده استفاده نمود.

- راه اندازی مجدد فعالیت ها:

پیش از وقوع بحران، تجهیزات و سیستم های آسیب پذیری که تداوم فعالیت های اصلی وابسته به آنها می باشد، می بایست شناسایی شوند. راه اندازی مجدد فعالیت ها در دو حالت می تواند رخ دهد.

۱. این حالت مربوط به دسته ای از فعالیت ها می باشد که تنها با استفاده از نیروی انسانی و سیستم های ارتباطی[۱] می توانند تحت شرایطی مجدد راه اندازی شوند. جهت راه اندازی این فعالیت ها نیازی به سیستم ها و تجهیزات نبوده و این عمل بصورت معمول در یک زمان کوتاه و با استفاده از نیروی انسانی امکان پذیر است.

[۱] سیستم های ارتباطی باید همانند سیستم های پشتیبان حفاظت شوند.

۲. در این حالت، فعالیت هایی که جهت تداوم تولید، نیاز به استفاده سیستم و تجهیزات موجود دارند، با رعایت اصول فنی سایت مورد نظر، راه اندازی مجدد می شوند.

پدافند غیرعامل و سامانه موتور جستجوی اینترنت

موتورهای جستجو نقش بسزایی در راهنمایی کاربران به محتوای مورد نظر و تکمیل روند ارائه کالا، خدمات و محتوا به صورت اینترنتی ایفا می‌کنند. قطع یا تحریم سرویس موتورهای جستجو عملاً دسترسی کاربران داخلی به سایت‌های داخلی و خارجی و دسترسی سایت‌های داخلی به کاربران داخلی و خارجی را قطع خواهد کرد. از سوی دیگر با توجه به کارکرد این سامانه‌ها روزانه داده‌های فراوانی از نحوه جستجوی افراد، نیازها و تمایلات آنها در اختیار سرویس‌دهندگان قرار می‌گیرد. این موضوع ضرورت طراحی و پیاده سازی موتورهای جستجوی بومی و ملی کارا، مطمئن و پایدار را نشان می‌دهد، در غیر این صورت انباشت ذیقیمتی از اطلاعات مربوط به فضای داخلی، طرز فکر و تلقی مردم در موضوعات مختلف و مواردی از این دست به راحتی در اختیار بیگانگان قرار می‌گیرد.

با توجه به شرایط حاضر، نکات ذیل جهت حفظ حریم شخصی کاربران در هنگام استفاده از موتورهای جستجو ارائه می‌شود:

- عدم استفاده از سرویس‌های حساب کاربری در زمان جستجو
- عدم استفاده از سرویس‌های جستجو ISP
- تغییر IP یا استفاده از برنامه‌های مخفی کننده IP
- جلوگیری از ثبت Cookieها از طرف موتور جستجو
- ملاحظات پدافند غیرعامل در طراحی موتور جستجوی ملی
- نکته مهم در طراحی یک موتور جستجوی داخلی علاوه بر کارایی و پایداری، موفقیت در جذب کاربران است. نمونه‌های مشابه نشان داده است که موتورهای جستجوی منطقه ای تنها زمانی توانسته‌اند با نمونه‌های مطرح جهانی رقابت کنند که از مزیت های خاص منطقه ای

نظیر زبان، کتاب‌ها و خدمات محلی بهره کافی برده باشند. در ادامه برخی از مهمترین ملاحظات پدافند غیر عامل در طراحی موتورهای جستجو در کشور بیان شده است.

- از فناوری‌های غیربومی که کد آن قابل دسترس نیست استفاده نشود. همچنین استفاده از فناوری‌های متن باز به تنهایی کافی نیست بلکه باید از روش‌های بهینه‌سازی کدها و اضافه کردن بسته‌ها و سرویس‌های امنیتی سخت افزاری یا نرم‌افزاری بومی به اجزا، بستر معماری و ارتباطی آن نیز استفاده کرد.

- به منظور حفظ امنیت اطلاعات تبادل شده بین اجزای موتور جستجو باید از استانداردها و پروتکل‌های امنیتی بومی استفاده شود. در غیراین صورت مهاجم بین راه می‌تواند داده‌های مورد جستجو را شنود کرده و به تحلیل جستجوی افراد دست یابد. همچنین می‌تواند در نتایج جستجوی افراد تأثیر گذاشته و داده‌های تبادل شده را تحریف کند. پروتکل استفاده شده می‌تواند از الگوریتم‌های رمزنگاری داخلی و خاص سازمان استفاده کند.

- مکانیزم‌های مناسب برای حفظ الگوریتم‌های استفاده شده و محرمانه ماندن معماری نرم‌افزار اعمال شود. مهاجمان و هرزنگارها با داشتن اطلاعات دقیق از الگوریتم‌ها و معماری موتور جستجو راحت‌تر می‌توانند به آن حمله کرده و آن را از کار بیاندازند. لذا این نکته نه تنها باید در طراحی نرم‌افزار مورد توجه قرار گیرد بلکه تیم طراحی و پشتیبانی آن نیز باید آموزش‌های لازم را دیده باشند و در حفظ مسائل امنیتی آن حداکثر تلاش خود را بکنند.

- ملاحظات پدافند غیرعامل در بسترهای نرم‌افزاری نظیر پایگاه داده، مستندات، سیستم‌عامل و کارگزار وب باید رعایت شود. از آنجاییکه کارکرد موتور جستجو وابسته به سامانه های نرم‌افزاری و سخت‌افزاری بستر آن است، عدم رعایت این ملاحظات امنیت و پایداری موتور جستجو را با خطر مواجه می‌کند.

- موتور جستجو برای ارائه سرویس خود نباید به کارگزارهای خارج کشور و تنها به محتوای خارجی وابسته باشد. بدین منظور ماشین‌های کارگزار موتور جستجو باید در داخل کشور باشند. همچنین با توجه به پیاده‌سازی شبکه اینترانت ملی، خدمت‌دهی موتور جستجو نباید وابسته به شبکه ارتباطی خارج از شبکه داخلی باشد. این خود امکان خروج ترافیک داده از مرزهای کشور را کاهش داده و می‌تواند باعث افزایش امنیت داده‌ها شود.

- معماری موتورجستجو باید قابلیت توزیع شدن و تکرارپذیری در مؤلفه‌هایی مانند وب‌خز، شاخص‌گذار و سامانه ذخیره‌سازی را داشته باشد. تکرارپذیری اجزای معماری جهت افزایش کارایی، جلوگیری از اشباع شدن و افزایش پایداری سامانه است. همچنین با توزیع کردن داده‌ها در کارگزارهای مختلف پایداری سامانه افزایش می‌یابد. آنچه که در هنگام توزیع‌پذیری از دیدگاه امنیتی مهم به نظر می‌رسد حفظ یکپارچگی و جامعیت در هنگام توزیع‌کردن فعالیت‌ها و وظایف است تا بتوان تعادلی بین سرعت و دقت و امنیت ایجاد کرد. موتورهای جستجو حتی با داشتن بخشی از داده‌های خود نیز باید بتوانند به پرسش‌های کاربر پاسخ دهند.

- در هنگام موازی‌سازی و تکرار، مؤلفه‌های موتور جستجو باید در مناطق جغرافیایی مختلف پراکنده شود. این عمل در کنار استقلال مؤلفه‌ها و مقاومت در برابر خرابی یک یا چندین جزء موتور جستجو نقش بسزایی در افزایش پایداری سامانه خصوصاً در جنگ‌های فیزیکی دارد.

- ردگیری و تحلیل پرسش‌ها و رفتار کاربر در موتور جستجو تنها برای افراد مجاز ممکن باشد. اطلاعات آماری و تحلیلی در مورد جستجوهای دسته‌های مختلف کاربران اطلاعات مهمی هستند که ارزش سیاسی، اجتماعی و اقتصادی بالایی دارند. دسترسی افراد بدخواه به این اطلاعات می‌تواند آن‌ها را در برنامه‌ریزی برای ایجاد تنش‌های اجتماعی، سیاسی و اقتصادی در کشور یاری کند. از طرف دیگر این داده‌ها می‌تواند برای دولت‌مردان و برنامه‌ریزان کشور کمک بسزایی باشد. لذا دولت‌ها در کشورهای مختلف محدودیت‌های خاصی روی نحوه انتشار این اطلاعات وضع می‌کنند.

- مکانیزم بازنمایی موتور جستجو باید کاربر را از خطرهای امنیتی موجود در نتایج جستجو مطلع و حفاظت کند. گزارش‌های بسیاری وجود دارد که موتور جستجویی در هنگام نمایش نتایج جستجو با نمایش بخشی از محتوای ناامن سایت موجب به خطر افتادن امنیت کاربران خود شده است. موتور جستجو باید این گونه محتوا را در هنگام نمایش نتایج جستجو حذف کند. همچنین بعضی مهاجمان با استفاده از موتور جستجو و کلیدواژه‌های جذاب، کاربران را به سایت خود می‌کشند. موتور جستجو باید خطر سایت‌های ناامن را به کاربرانی که روی لینک آنها کلیک می‌کنند هشدار دهد. با این کار از حمله فرد مهاجم به وسیله موتور جستجو جلوگیری می‌شود.

- الگوریتم جمع‌آوری و رتبه‌بندی موتور جستجو باید تدابیر لازم برای جلوگیری از هرزنگاری را در نظر گرفته باشد. شخص مهاجم با استفاده از هرزنگاری می‌تواند سایت‌های مورد نظر خود را در صدر نتایج جستجوی کاربران قرار دهد. با این کار عملاً موتور جستجو از ارائه سرویس باز مانده و تبدیل به وسیله‌ای تبلیغاتی برای مهاجمان می‌گردد.

- اعمال درست سیاست‌های وب‌خز در موتور جستجو به منظور بالا بردن پایداری و کارایی موتور جستجو و مقابله با دام‌های وب‌خز. این سیاست‌ها باید با توجه به محتوا و کاربران هدف موتور جستجو به

گونه‌ای انتخاب شود که علاوه بر حفظ کارایی و سودمندی موتور جستجو پایداری آن را خدشه‌دار نکند. مثلاً دام وب‌خز می‌تواند آن را در حلقه‌ای بی‌نهایت به دام انداخته یا منجر به اتلاف فضای زیادی از مخزن ذخیره‌سازی گشته و پایداری سامانه را دچار خدشه کند.

- موتور جستجو باید قابلیت پشتیبانی از زبان فارسی را در واسط کاربری، جستجو و بازنمایی داشته باشد. همچنین واسطهای کاربری غیربومی باعث وابستگی افراد جامعه به کاربری این گونه واسطها شده و آنها را از زبان بومی دور نگه می‌دارد.

- در جمع‌آوری اطلاعات و همچنین ثبت تعامل کاربران با سامانه باید مسائل مربوط به حریم شخصی کاربران رعایت شود. در واقع خود موتور جستجو نباید ناقض حریم امنیتی کاربران خود باشد. این نقض حریم می‌تواند در تحلیل اطلاعات تعامل کاربر با سامانه یا دسته‌بندی و ارائه داده‌ها به شکلی باشد که حمله فرد مهاجم (خصوصاً حملات مربوط به مهندسی اجتماعی) را تسهیل کند. به این ترتیب فرد مهاجم از موتور جستجو برای یافتن سریع‌تر هدف خود و حمله به آن بدون ردپا استفاده می کند. هر سازمان یا ارگانی که اطلاعات خود را در وب قرار می‌دهد باید روالی تکراری برای بررسی محتوای اطلاعاتی که از سازمان در اختیار عموم قرار می‌گیرد داشته باشد و این اطلاعات را قبل از فرد مهاجم یافته و از روی وب حذف کند.

- در جمع‌آوری اطلاعات موتور جستجو و بازنمایی آن‌ها به کاربر باید موارد حقوق مؤلفین در نظر گرفته شود. موتور جستجو باید حقوق مؤلفین را طبق یک پروتکل حقوق محتوای دیجیتال توافقی در مورد ارائه خدماتی مثل جستجوی کتاب‌ها یا محتواهای غیر رایگانی که سایت‌های خبری، کتابخانه‌ها و آرشیوها تنها جهت جستجو شدن در اختیار موتور جستجو قرار داده‌اند رعایت کند.

معیارها و راهکارهای امنیتی در شبکه های ارتباطات سیار

در این فصل به راهکارهای پدافند غیرعامل به منظور امن، ایمن و پایدار نمودن شبکه ارتباطات سیار در دو سطح طراحی– معماری و پیاده‌سازی، پرداخته می‌شود. در این راستا ابتدا معیارها و محورهای پدافند غیرعامل تشریح و سپس راهکارهایی برای مقابله با حملات و مشکلات شبکه ارتباطات سیار، براساس این محورها توصیه می‌گردد.

- محورهای دفاع غیرعامل در شبکه‌های ارتباطات سیار

پدافندغیرعامل بمنظور امن، ایمن و پایدارسازی شبکه‌های ارتباطات سیار محورهای ذیل را دنبال می‌کند:

- استفاده از شبکه‌های جایگزین به صورت منطقه‌ای و یا سراسری
- کاهش امکان حمله به نقاط حیاتی، حساس و مهم شبکه
- کاهش میزان خسارات ناشی از حمله به نقاط مهم، حساس و حیاتی شبکه
- کاهش هزینه و افزایش سرعت و سهولت بمنظور جبران خسارات وارد شده به نقاط مهم، حساس و حیاتی شبکه و بازسازی شبکه با اندیشیدن تمهیدات لازم
- ایجاد امکان شناسایی دشمن و کشف نفوذ به شبکه ارتباطات سیار در صورت هرگونه حمله یا نفوذ
- محدود سازی گستره حملات به شبکه ارتباطات سیار
- راهکارهای پدافند غیرعامل در شبکه‌های ارتباطات سیار

در این بخش به بیان راهکارهای پدافند غیرعامل به منظور تأمین امنیت، ایمنی و پایداری شبکه‌های ارتباطات سیار مبتنی بر محورهای ذکر شده در بخش قبل پرداخته می‌شود. هدف از این راهکارهای امنیتی بالابردن مقاومت شبکه، کاهش میزان خسارات و تسهیل بازسازی شبکه در حملات و شرایط بحران ومخاصمات بین‌الملل است. در یک دسته‌بندی راهکارهای امن، ایمن و پایدارسازی شبکه ارتباطات سیار در برابر حملات و آسیب‌پذیری‌ها را می‌توان به دو بخش تقسیم نمود:

الف) راهکارهای مربوط به طراحی شبکه: راهکارهایی که کلان‌تر و غالباً از جنس معماری و طراحی بوده و لازمه برخی از آنها تغییرات گسترده و زیربنایی در شبکه‌های ارتباطات سیارمی‌باشد.

ب) راهکارهای مربوط به پیاده‌سازی: راهکارهایی که اجرایی‌تر و جزئی‌تر هستند و برخی از آنها روش‌هایی هستند که راهکارهای طراحی را عملی می‌سازند.

- راهکارهای طراحی شبکه

همانطور که اشاره شد، راهکارهای طراحی عموماً کلان‌تر و غالباً از جنس معماری و طراحی می‌باشند. این راهکارها براساس اصول راهبردی و مبتنی بر محورهای دفاعی بیان شده در بخش قبل تدوین شده است. اصول کلی حاکم بر راهکارهای این بخش پیشگیری از حمله و نفوذ، جلوگیری از انتشار و تشدید، شناسایی و بازسازی تا حد ممکن است. این راهکارها شامل موارد ذیل می‌باشد:

- محرمانه و مخفی نگهداشتن اطلاعات ساختار، طراحی و پیاده‌سازی شبکه و نیز اطلاعات مربوط به نقاط مهم، حساس و حیاتی شبکه که تأثیر بسزایی در امنیت شبکه و جلوگیری از نفوذ و دسترسی دشمن دارد. مثالی از آن طبقه‌بندی محرمانه برای اطلاعات جداول مسیریابی صدا در شبکه است.
- مستقل‌سازی حداکثری بخش‌های مختلف شبکه ارتباطات سیار از شبکه‌های دیگر مخابراتی و رایانه‌ای.
- اجرای اصول و راهکارهای امنیتی در طراحی و پیکربندی زیرشبکه‌ها جهت جلوگیری از حمله و نفوذ به شبکه.
- رعایت اصول طراحی منطقه‌ای در شبکه ارتباطات سیار بگونه‌ای که حملات به یک مرکز (یا منطقه) صرفاً منجر به اختلال یا دسترسی غیرمجاز به همان مرکز (منطقه) شود و یا کمترین میزان مشترکین را تحت تاثیر قرار دهد. یکی از اصول مهم در این راهکار، طراحی شبکه بصورت مجموعه‌ای از زیرشبکه‌های نسبتاً مستقل است.
- رعایت اصول طراحی لایه‌ای در شبکه ارتباطات سیار به صورتی که نفوذ یا صدمه به یک لایه وسیله‌ای برای گسترش نفوذ و صدمه به لایه‌های دیگر نشود.

- طراحی شبکه بگونه‌ای که تا حد ممکن اختلال و یا دسترسی به یک کاربرد یا سرویس، به سایر خدمات صدمه‌ای وارد ننماید.
- معماری و طراحی شبکه ارتباطات سیار به گونه‌ای که در صورت گسترش خسارت به مراکز، لایه‌ها و کاربردهای دیگر، خسارت مستهلک و میرا شود، نه اینکه تشدید گردد.
- طراحی و معماری بگونه‌ای که در حوادث و حملات، بصورت نظام مند و به سرعت مکان، نوع، عامل و سطح تأثیر شناسایی شود.
- طراحی دفاع در شبکه ارتباطات سیار بگونه‌ای که دشمن برای حمله، به دانش سطح بالا و متنوع، هزینه زیاد، ابزار و تجهیزات متعدد، پیشرفته و پیچیده نیاز داشته باشد.
- استفاده از راهکارهای بومی و نوآورانه امن، ایمن و پایدارسازی شبکه و عدم استفاده از پیشنهادات، روش‌ها و الگوریتم‌های امنیتی شناخته‌شده می‌تواند منجر به چنین نتایجی شود.

- راهکارهای پیاده‌سازی شبکه

راهکارهای پیاده‌سازی، اجرایی‌تر و جزئی‌تر بوده و برخی از آنها در واقع روش‌هایی برای عملیاتی کردن راهکارهای طراحی ارائه شده در بخش قبل هستند. این راهکارها به دو گروه قابل تقسیم هستند. که در ادامه فصل به آنها می پردازیم.

۱. راهکارهای امنیتی فناورانه: در این بخش مجموعه‌ای از راهکارهای ایمن‌سازی شبکه ارتباطات سیار که بیشتر در حوزه پیاده‌سازی است، بیان شده است.

- اعمال اصول امنیتی در نصب تجهیزات و راه‌اندازی شبکه: راه‌اندازی مراکز و نصب تجهیزات شبکه (NE[۱]) باید در مناطقی که احتمال وقوع حمله یا حوادث غیر مترقبه کمتر و یا شرایط برای جبران خسارات احتمالی مناسب‌تر باشد، انجام پذیرد.
- اجرای اصول اختفا[۱]، استتار[۲] و فریب[۳] در نصب تجهیزات و ایجاد و راه‌اندازی مراکز. اختفا به‌معنی مخفی‌سازی از دید دشمن، استتار به معنای مشابه‌سازی اهداف (تجهیزات،

[۱] Network Elements

کابل‌ها و مراکز) با زمینه قرارگیری و فریب به معنی به اشتباه انداختن دشمن در مورد اهداف واقعی است که این سه راهکار به عنوان سه اصل مهم پدافندغیرعامل باید در پیاده‌سازی شبکه‌های ارتباط سیار در نظر گرفته شود.

- پراکندگی حداکثری مراکز و تجهیزات: یکی دیگر از روش‌های دفاعی در پدافند غیرعامل، پراکنده سازی مکانی حداکثری تجهیزات مهم، حساس و حیاتی شبکه ارتباطات سیار است. البته ماهیت شبکه ارتباطات سیار پراکنده بوده که این خود یک حسن به حساب می‌آید ولی بخش‌های مهم متمرکز شبکه همچون نظارت و مدیریت از مراکز آسیب پذیر شبکه ارتباطات سیار محسوب می‌شود.
- مقاوم سازی مراکز و ارتباطات: با امن‌سازی شبکه‌های ارتباطات سیار می‌توان از برخی از حملات نرم پیشگیری نمود. به همین خاطر الزام اپراتورهای تلفن همراه به مقاوم‌سازی امنیتی و پیاده‌سازی استانداردها، رویه‌ها و راهکارهای فنی امنیتی برای حفظ امنیت شبکه ارتباطات سیار تحت مدیریت خود نقش به‌سزایی در بالا بردن مقاومت شبکه‌های تلفن‌همراه در هنگام حملات دشمن و حوادث غیر مترقبه خواهد داشت.
- راه‌اندازی مراکز پاسخگویی به حوادث امنیتی: در کنار ایجاد مؤسسات ملی امداد و نجات برای شبکه‌ها سامانه‌های رایانه‌ایCERT ملی، بطور خاص برای شبکه‌های ارتباطات سیار نیز باید گروه‌ها و مراکز پاسخگو به حوادث امنیتی (IRT[۴]) راه‌اندازی شود.
- تدارک تجهیزات و اجزای جبرانی در شبکه ارتباطات سیار: به منظور بازسازی سریع شبکه ارتباطات سیار، باید به میزان قابل قبولی اجزای شبکه و قطعات جانبی برای جایگزینی وجود داشته باشد.

---

[۱] Concealment

[۲] Camouflage

[۳] Deception

[۴] Incident Response Team

- رعایت اصول راه‌اندازی سریع: جهت بازسازی، ترمیم و راه‌اندازی مجدد شبکه آسیب دیده، باید اصول و مواردی رعایت شود تا محل و نحوه ذخیره‌سازی تجهیزات و لینک‌های جایگزین، شیوه‌های حمل و نقل آنها، روش نصب و تعمیر آنها، سریع و آسان باشد.

- توسعه توان تولید و پشتیبانی داخلی در تجهیزات شبکه: تا حد امکان قابلیت ساخت و تعمیرات اساسی تجهیزات در داخل کشور و توسط شرکت‌ها و نیروهای داخلی فراهم آید.

- بالابردن کیفیت و قابلیت اعتماد[1] تجهیزات شبکه: استفاده از اجزای با طول عمر بالا و با کیفیتی که در شرایط آب و هوایی و سایر شرایط نامساعد نیز بخوبی کار خود را انجام دهند و بکارگیری شیوه‌هایی که باعث طولانی شدن زمان تعمیرات اساسی تجهیزات شود لازم به نظر می‌رسد. همچنین، قابلیت اعتماد به تجهیزات و اتصالات کابلی یا رادیویی در شرایط عادی در برابر خطای اپراتور انسانی، حرارت محیط، شرایط جوی غیر حاد و ... نیز باید وجود داشته باشد.

- نکته دیگری که در اینجا لازم به ذکر است، تلاش برای کاهش هزینه تولید، تعمیر و نصب تجهیزات شبکه به منظور بالا بردن صرفه و امکان مالی برای بازسازی خسارت محتمل زمان حادثه است. شاید یکی از روش‌ها نیز استفاده از توان داخلی برای تولید و پشتیبانی تجهیزات شبکه باشد.

- راهکارهای امنیتی مربوط به فرایندها و روال‌ها

در این بخش راهکارهای امنیتی که در مباحث پیاده‌سازی شبکه‌های ارتباطات سیار و در حوزه مرتبط با فرایندها و روال‌های سازمانی است، بیان می‌گردد. این موارد به طور مستقیم قابل تست و پیاده‌سازی نیستند، بلکه به منظور تدوین دستورالعمل‌ها، رویه‌ها، قوانین و دوره‌های آموزشی مورد بررسی قرار می‌گیرند.

---

[1] Reliability

- بالا بردن اولویت امنیت نزد اپراتورهای تلفن همراه: اپراتورهای تلفن همراه باید روال‌های درون و برون سازمانی را که امنیت شرکت و شبکه تلفن همراه را تقویت می‌کنند، اجرا نمایند.
- رعایت روال‌های امنیتی مرتبط با مشترکان: در روال‌های مربوط به خرید، صدور و تخصیص SIM به مشترک، باید اصول امنیتی جهت فاش نشدن این اطلاعات مراعات گردد.
- معتمد و آگاه بودن مجریان و مدیران شبکه: یکی از مسائلی که تاثیر بسزایی در امنیت شبکه ارتباطات سیار دارد، معتمد بودن و داشتن آگاهی و دانش امنیتی کافی مجریان و مدیران شرکت‌های اپراتور تلفن همراه است، بگونه‌ای که ایشان در مواجهه با برخی معضلات امنیتی و یا مشکلات پیش‌بینی نشده در شرایط عادی و یا بحرانی بتوانند به خوبی عکس‌العمل نشان دهند. همچنین وضعیتی اتفاق نیفتد که خودشان خواسته یا ناخواسته، عامل و یا تشدید کننده حملات دشمن شوند. طبق آمارهای بین‌المللی اکثر حملات و نفوذها به شبکه‌ها با واسطه یا بی واسطه از طریق کارکنان داخل سازمان است و نه هکرهای خارجی. از جمله مسائلی که باید رعایت شود، اینست که تا حد ممکن، نصب، راه‌اندازی و نگهداری تجهیزات مراکز مهم و بطور خاص، حساس و حیاتی توسط افراد مورد اعتماد و تایید شده صورت پذیرد. در صورتی که چاره‌ای جز بکارگیری افراد خارجی و یا ناشناخته نیست، این افراد باید تحت نظارت و کنترل کامل افراد معتمد باشد. همچنین مدیران و متولیان آگاه شبکه‌های ارتباطات سیار باید نظارت، بازدید و تست‌های دوره‌ای و مرتب در مراکز و لایه‌های شبکه بر روی طراحی‌ها، سخت‌افزار و نرم‌افزار شبکه داشته باشند.
- مراعات کنترل دسترسی و امنیت فیزیکی : رفت و آمدها به مراکز و اماکن مهم، حساس و حیاتی شبکه ارتباطات سیار، همچنین دسترسی‌های فیزیکی و غیر فیزیکی به سخت‌افزارها و نرم‌افزارها باید طبق اصول امنیتی از پیش تعریف شده و کاملاً مطابق با آن باشد. همچنین کلیه دسترسی‌ها نیز به طرق مختلف باید تحت کنترل و نظارت و قابل بررسی باشد.
- ایجاد روال‌های امن در مورد اطلاعات شبکه: اطلاعات ساختاری، طراحی و عملیاتی شبکه ارتباطات سیار، تعداد و نوع تجهیزات و سیستم‌ها، جداول مسیریابی، ظرفیت

اجزای شبکه، نسخه نرم‌افزار و سخت‌افزار، وضعیت حال حاضر و برنامه آینده توسعه شبکه، ایرادات و مشکلات فعلی شبکه ارتباطات سیار باید تحت طبقه‌بندی صحیح و منطبق با اصول پدافند غیرعامل قرار گیرد.

- ایجاد ساختار اطلاع‌رسانی عمومی: بسیاری از نفوذها به شبکه‌ها، ویروس‌های مخرب در شبکه، حملات از کار انداختن تجهیزات، مشکلات ناشی از شبکه اینترنت در GPRS، از ورودی گوشی و SIM مشترک حاصل می‌شود. با گسترش قابلیت‌های حافظه‌ای و پردازشی گوشی‌های تلفن همراه، روز به روز بر این تهدیدات افزوده می‌شود. به عنوان مثال غالب ویروس‌های شناخته شده موبایل که می‌تواند ترافیک و سیگنالینگ شبکه را تحت تاثیر قرار دهد، از طریق بلوتوث منتقل می‌شود که ارتباطی با شبکه ارتباطات سیار ندارد. آموزش عمومی کاربران تلفن همراه، گسترش و بالا بردن سطح اطلاعات عمومی مشترکین از تهدیدات و مشکلات و عوارض امنیتی ممکن در مورد تلفن همراه، تدوین دوره‌های آموزشی و اطلاع‌رسانی و تبلیغاتی از جمله راهکارهایی هستند که می توانند نقش مؤثری در کاهش این مشکلات داشته باشند.

ملاحظات پدافند غیرعامل در حوزه امنیت فیزیکی و کنترل دسترسی

امنیت فیزیکی در محیط فناوری اطلاعات و ارتباطات در سه بعد «داده‌ها و اطلاعات»، «شبکه و ارتباطات» و «سخت‌افزارها و تجهیزات» قابل بررسی است. در ادامه توضیحات مختصری در خصوص هرکدام از این ابعاد به همراه ملاحظات مربوطه بیان خواهد گردید.

امنیت فیزیکی داده‌ها و اطلاعات

ارتباط مستقیمی بین میزان امنیت فیزیکی و امنیت داده‌ها و اطلاعات وجود دارد. در حقیقت، هدف بسیاری از حملات و خرابکاری‌های فیزیکی در سامانه‌ها، کارگزارها و شبکه‌ها، نفوذ و دسترسی به اطلاعات و داده‌های حساس سازمان ها است. اهم حوزه‌های امنیت فیزیکی داده‌ها و اطلاعات به شرح ذیل است:

۱. محفظه‌ها / مخازن داده

- اطلاعات طبقه‌بندی شده و محرمانه و نیز سامانه‌های اطلاعاتی حساس باید در محفظه‌ها و اتاق‌هایی نگهداری شوند که دسترسی به آن‌ها محدود بوده و محیط پیرامون آن‌ها نیز دارای حفاظ‌های امنیتی مناسبی باشد.
- ورود به اتاق‌های کارگزارها و مخازن داده‌ها و اطلاعات منوط به اخذ مجوزهای مشخص باشد.
    - تا حد ممکن نباید اطلاعات مهم در رایانه‌های شخصی نگهداری شوند. این اطلاعات حتی‌الامکان در رسانه‌های فقط خواندنی ذخیره گردند.
- محفظه‌ها/ مخازن اطلاعات از نزدیکی به مواد و تجهیزات پرخطر در امان باشند.
- اعمالی چون خوردن، نوشیدن، سیگار کشیدن و نظایر آن در مجاورت و درون محفظه‌ها و اتاق‌هایی که حاوی اطلاعات و تجهیزات اطلاعاتی هستند، ممنوع گردد.

۲. کلیدهای محفظه‌ها/مخازن امنیتی

در این بخش منظور از کلید انواع کلیدهای مکانیکی، شماره شناسایی خصوصی، کارت‌های دسترسی و یا ترکیبی از دو یا چند مورد فوق است.

- کلیدهای محفظه‌ها/ مخازن امنیتی با توجه به بالاترین درجه حساسیت اطلاعات و یا تجهیزاتی که توسط آن قابل دسترسی هستند، محافظت شوند. کلیدهای محفظه‌ها/ مخازن امنیتی باید زمانی که یکی از موارد زیر محقق شد، تغییر کنند:
    ۱. شواهدی از حمله و یا نفوذ رؤیت شود.
    ۲. تهدیدات و خطرات غیرقابل قبولی مشاهده شود.

۳. فردی که به این مکان‌ها دسترسی داشته است، تغییر کند.

۳. داده‌های در حال تبادل

شنود و یا استراق سمع الکترونیکی یکی از هوشمندانه‌ترین راه‌های سرقت داده‌های در حال تبادل محسوب می‌شود. امروزه مهاجمین با کمترین تجهیزات ممکن نیز قادر به شنود و رونوشت تمامی فعالیت‌های انجام شده روی رایانه قربانی هستند؛ نظیر ثبت تمامی کلیدهایی که بر روی صفحه کلید فشار داده می‌شوند، تمامی اطلاعاتی که روی یک مانیتور نمایش داده می‌شوند و تمامی فایل‌هایی که برای چاپگر[۱] ارسال می‌شوند. انواع روش‌های شنود و محافظت در مقابل آن‌ها به شرح ذیل ارائه می شود:

۴. شنود از طریق کابل‌ها و سیم‌ها

سیم‌ها و کابل‌های الکتریکی، به خاطر نوع عملکردشان، جزء اولین گزینه‌های انتخابی مهاجمین برای شنود هستند. مهاجم به راحتی می‌تواند مکالمه‌ای را که بین یک جفت سیم در حال انجام است با یک پیوند ساده دنبال کند.

- به طور منظم تمامی سیم‌هایی که داده‌ها را حمل می‌کنند جهت یافتن آسیب‌های فیزیکی، بازرسی شوند.
- با استفاده از کابل‌های حفاظ‌دار، از امکان نظارت غیرمجاز سیم‌ها کاسته شود.

۵. شنود از طریق اترنت[۲]

---

[۱] Printer

[۲] Ethernet

- از آنجاکه مهاجمین به طور گسترده از اترنت و سایر شبکه‌های محلی، برای شنود استفاده می‌کنند، اطمینان حاصل شود که سامانه‌ها، زیرشبکه‌ها و شبکه‌هایی که استفاده نمی‌شوند، دارای پورت‌های کابل‌های دوسویه فعال و یا اترنت در درونشان نیستند.
- تمامی آدرس‌های IP که در شبکه‌ها مشخص شده‌اند به صورت دوره‌ای بررسی شوند تا اطمینان حاصل گردد میزبان غیرمجازی از طریق اینترنت در شبکه فعالیت نداشته است.
- از نرم‌افزارهای رصد LAN استفاده شود، تا به محض تشخیص یک بسته که از یک آدرس ناشناخته استفاده می‌کند، هشدارها فعال شود.

۶. شنود از طریق پورت‌های کمکی روی پایانه‌ها

بسیاری از ترمینال‌های کامپیوتری مجهز به یک پورت پرینتر جهت استفاده و یک پورت برای پرینتر کمکی هستند. اگر مهاجمی بتواند یک ارتباط[۱] با پورت‌های چاپگر برقرار کند، می‌تواند از این پورت‌ها برای شنود استفاده کند.

- اگر از چاچگر کمکی استفاده می‌شود اطمینان حاصل شود که کابل‌های دیگری به پورت چاپگر پایانه متصل نیستند.

۷. پشتیبان داده‌ها

حفاظت فیزیکی یک پشتیبان، به اندازه حفاظت فیزیکی یک کارگزار و یا سامانه اطلاعاتی اهمیت دارد؛ زیرا در صورت خرابی، یا به سرقت رفتن پشتیبان، بخش اعظمی از اطلاعات، نابود یا به سرقت می‌رود.

---

[۱] Link

- پشتیبان‌ها در مکان‌هایی که توسط عموم قابل دسترسی هستند، قرار داده نشوند.
- پشتیبان‌ها ونسخه‌های اصلی در مکان های جداگانه نگهداری شوند.
- تمامی رسانه‌های ذخیره‌سازی به صورت «غیرقابل نوشتن[1]» ذخیره شوند.
- بمنظور حفاظت از اطلاعات نسخه‌های پشتیبان، از قفل‌های سخت‌افزاری و نرم‌افزاری استفاده شود.
- قبل از دور انداختن رسانه‌های ذخیره‌سازی، اطمینان حاصل شود که داده‌های موجود بر روی آن‌ها کاملاً پاک شده‌اند. از مطمئن‌ترین راه‌های امحاء رسانه‌های ذخیره‌سازی تخریب فیزیکی است.

۸. رسانه‌های غیرالکترونیکی

رسانه‌های دیجیتالی، تنها منابع ذخیره‌سازی داده‌ها نیستند که باید قبل از دور انداختن پاکسازی کامل شوند، بلکه رسانه‌های دیگری نیز وجود دارند که ممکن است حاوی اطلاعات مهمی برای مهاجمین و قفل‌شکن‌ها باشند؛ از جمله این رسانه‌ها می‌توان به نتیجه چاپی نرم‌افزارها، یادداشت‌ها، مستندات طراحی، کدهای مقدماتی، مستندات برنامه‌ریزی، خبرنامه‌های داخلی، دفترچه‌های تلفن و یادداشت شرکت، راهنمای کاربر و نظایر آن اشاره نمود. برای نمونه اگر مستند چاپ شده طراحی و معماری شبکه در دسترس باشد یک مهاجم می‌تواند با دسترسی به آن از کارگزارها، لینک‌ها و سامانه‌های مختلف مطلع شده، نقاط ضعف توپولوژی را یافته و از آن استفاده نماید.

[1] Write Protected

- رسانه‌ها می‌بایست در مکان‌های امن نگهداری شوند.
- می بایست به کاربران آموزش داده شودکه اطلاعات حساس را بدون رعایت موارد امنیتی به هیچ عنوان در معرض نمایش نگذارند و یا دور نیندازند.

امنیت فیزیکی شبکه و ارتباطات

شبکه، دارای منابعی فیزیکی همچون سامانه‌ها، دستگاه‌های شبکه (مسیریاب[۱]، سوئیچ[۲]، دیوارآتش[۳]، هاب[۴] و...)، اتاق کارگزار و تجهیزات آن، تجهیزات ذخیره‌سازی و نظایر آن می باشد. شبکه، نحوه ارتباط منابع را با یکدیگر مشخص می‌کند. به عبارت دیگر لینک‌های جریان داده را بین این عناصر مشخص می‌کند.

بنابراین امنیت فیزیکی یک شبکه در بردارنده امنیت موارد زیر است:

۹. منابع فیزیکی موجود در شبکه

۱۰. نحوه ارتباط‌دهی منابع فیزیکی (توپولوژی فیزیکی شبکه)

۱۱. لینک‌های موجود بین منابع فیزیکی (کابل‌کشی)

۱۲. محیط شبکه (مرز شبکه با بیرون نظیر ارتباطات اینترنت، شبکه محلی، شبکه مجازی خصوصی[۵]، برنامه‌های کاربردی و ...)

۱۳. دستگاه‌های ایمنی شبکه (مسیریاب، دیوار آتش)

---

[۱] Router
[۲] Switch
[۳] Firewall
[٤] Hub
[٥] VPN

مهمترین اصل در امن‌سازی منابع فیزیکی موجود در شبکه آن است که دسترسی فیزیکی به این منابع محدود و کنترل شود. بسیاری از روش‌های حفاظتی که روی یک شبکه و یا سامانه اعمال می‌شود، توسط نرم‌افزارها فراهم می‌گردد، ولی اگر یک مهاجم (داخلی یا خارجی) موفق شود به صورت فیزیکی به یک کامپیوتر و یا شبکه دسترسی پیدا کند، امکان محدود کردن فعالیت‌ها و نفوذهای بعدی وی به شبکه داخلی و محرمانه سازمان، بسیار مشکل خواهد شد. برخی از خطراتی که از جانب مهاجمین، سازمان را تهدید می‌کنند عبارتند از:

۱۴. ورود و خروج غیرمجاز

۱۵. نظارت و کنترل از راه دور

۱۶. دسترسی غیرمجاز به کامپیوترها و سرورها و منابع اطلاعاتی حساس

۱۷. سرقت داده‌ها، اطلاعات و تجهیزات

۱۸. نصب سخت‌افزارها و یا نرم‌افزارهای شنود

۱۹. تخریب و یا دستکاری ساختارها و کابل‌های ارتباطی

۲۰. سرقت کامپیوترها، کارگزارها و سایر عناصر شبکه

۲۱. نصب برنامه‌های مخرب، ویروس‌ها و کرم‌ها

پس از دسترسی به اطلاعات و منابع اطلاعاتی وضعیت به مراتب دشوارتر خواهد شد. مهاجمین قادرند اطلاعات را تغییر دهند، پاک کنند، یا اینکه اطلاعات بدست آمده را به رقبا و یا دشمنان بفروشند، آنها را در اینترنت پخش کنند و سازمان ها را از این ناحیه متحمل خسارات فراوانی نمایند.

- دسترسی به شبکه داخلی از نواحی پذیرش عمومی و سایر نواحی محدود شود.
- جهت ورود به اتاق کارگزار و به طور کلی مکان‌های امن از کارت‌های شناسایی استفاده گردد.
- اتاق کارگزار به تجهیزات نظارت ویدئویی و همچنین UPS مجهز گردد.
- حتی الامکان از پنجره ها در مراکز داده استفاده نشود.
- در اطراف سامانه‌های مهم نظیر کارگزارها، حفاظ‌های مناسب تعبیه گردد.
- کابل‌ها در زیر زمین جاسازی شده و با پوشش‌های حفاظتی مقاوم شوند.
- مانیتورها و صفحه کلیدها در فواصل دوری از پنجره‌ها و درب‌ها و دریچه‌ها قرار داده شوند.
- کابل‌های شبکه در مقابل سامانه‌های شنود حفاظت شوند.
- صفحه نمایش، میزکار و حتی تابلوهای اتاق کنفرانس پس از اتمام کار پاک گردند.
- درایوهای فلاپی دیسک و CD-ROM و پورت های USB از روی سامانه‌های مهم حذف گردند.
- سطح امنیتی مطلوب برای Rack انتخاب گردد.

امنیت فیزیکی تجهیزات/سخت‌افزارها

در این بخش سعی شده است محدوده دید، کوچکتر شده و امنیت سامانه‌های رایانه‌ای و سخت‌افزارهای مربوط به آن‌ها مورد توجه قرار گیرد. نکته مهم اینست

که تجهیزات و سامانه‌های اطلاعاتی مهم و با ارزش (نظیر کارگزارها، تجهیزات اطلاعاتی دارای طبقه‌بندی، نمونه‌ها و مدل‌های مهندسی، اطلاعات مالی، سیاسی، نظامی و ...) باید در مکان‌های ایمن نسبت به مخاطرات ذیل نگهداری شوند.

۲۲. بمب الکترومغناطیسی

این بمب در اصل یک موج ضربه‌ای الکترومغناطیس است که یک میدان مغناطیسی بسیار قوی ایجاد می‌کند، این میدان مغناطیسی به نوبه خود، میدان الکتریکی با قدرت هزاران ولت بر متر به صورت ناپایدار در هادی‌های الکترونیک ایجاد کرده و با وارد شدن به یک دستگاه هادی جریان برق، این دستگاه را با توجه به میزان مقاومت آن بدون هیچ‌گونه سروصدا یا بر جای ماندن نشانه‌ای منهدم کرده و یا به آن آسیب می‌رساند. شناسایی عوامل حملات الکترومغناطیس بسیار دشوار است. از این روش می‌توان برای نابودکردن و ایجاد اختلال در تجهیزات الکتریکی و الکترونیکی بویژه رایانه‌ها، تجهیزات ارتباطی، رادیو یا گیرنده‌های رادار استفاده کرد.

اقدامات حفاظتی در برابر موج الکترومغناطیسی بر پایه جلوگیری از ورود، انتشار و انعکاس انرژی استوار است. بر این اساس، انرژی از قطعات، تجهیزات و ادوات، دور نگه داشته می شود.

- از پوشش و موانع فلزی کافی در اطراف ادوات و تجهیزات (شیلد الکترومغناطیسی) استفاده شود.
- جلوگیری کننده‌های سریع جریان[۱] در خطوط تغذیه، سیگنال و خطوط کنترلی نصب گردد؛ اتصال بین دیواره و جلوگیری کننده‌های سریع

[۱] Surge arresters

جریان و ارتباط این دو به زمین با امپدانس پایین ایجاد گردد و علاوه بر آن نقاط ورودی و محل اتصالات کنترل شود.

- هیچگاه برای شبکه از کابل‌های مسی بر روی زمین (بخصوص در بیرون ساختمان) استفاده نشود مگر اینکه با یک عایق پوشانده شده باشند.
- در سازه‌ها از فیلترهای الکتریکی و کف‌پوش‌های ضدالکتریسیته استفاده شود.

۲۳. عوامل محیطی مخرب

عملکرد صحیح سامانه‌های رایانه‌ای و سخت‌افزارهای مرتبط با آن‌ها، شرایط محیطی و فیزیکی خاصی را می‌طلبد. عواملی همچون انفجار، آتش، دود، رطوبت، ضربه، پارازیت الکتریکی، سیل و زلزله می‌تواند تأثیرات مخرب فراوانی در عملکرد و صحت تجهیزات، سامانه‌ها و اطلاعات داشته باشد.

- از پوشش‌های مستحکم جهت استفاده از تجهیزات و سامانه‌های مهم در نواحی پر خطر استفاده گردد.
- در نزدیکی سامانه‌های مهم، تجهیزات اطفاء حریق نصب و به پرسنل آموزش‌های کاربری لازم ارائه شود.
- علاوه بر رایانه‌ها، کابل‌کشی ساختمان نیز در برابر آتش‌سوزی ایمن باشد.
- با توجه به مضرات دود برای سامانه‌های رایانه‌ای و این موضوع که در برخی مواقع دود علامت خطر آتش‌سوزی است، سامانه‌های تشخیص دود در اتاق‌های حاوی تجهیزات پراهمیت، نصب و راه‌اندازی گردد.

- هرگز در اطراف مکان‌هایی که حاوی اطلاعات و سخت‌افزارهای حساس هستند، از درب‌ها و دیوارهای شیشه‌ای استفاده نشود.
- رایانه‌ها در مجاورت پنجره‌ها و یا در سطوح فوقانی اتاق‌ها قرارداده نشوند.
- از جاسازی تجهیزات سنگین در مجاورت سامانه‌های رایانه‌ای جلوگیری شود.
- حسگرهای تشخیص رطوبت در کف اتاق کارگزار و سایت‌های رایانه استفاده شود. حسگرها طوری تنظیم شوند که هنگام وجود رطوبت آسیب‌زننده به صورت خودکار جریان برق را قطع نمایند.
- برای کارگزارها و سایر سامانه‌های اطلاعاتی مدار الکتریکی جداگانه‌ای به همراه یک محافظ الکتریکی در نظر گرفته شود تا از ایجاد پارازیت جلوگیری شود.

مشخصه‌های متمایز کننده سامانه های مدیریت تهدید یکپارچه

یکی از دغدغه‌های مدیران امنیت شبکه انتخاب یک سامانه مدیریت تهدید یکپارچه مناسب برای شبکه تحت مدیریت خود است. در زیر به بررسی برخی از ویژگی‌هایی که باعث ایجاد تمایز بین سامانه‌های مدیریت تهدید یکپارچه هنگام استفاده در شرایط متفاوت می شوند، می‌پردازیم.

نحوه ارائه امکانات

از آنجا که نحوه و کیفیت ارائه امکانات در UTMهای مختلف متفاوت است، بهتر است قبل از خرید سامانه مدیریت تهدید یکپارچه نسبت به نصب آزمایشی و

بررسی امکانات آن اقدام گردد. بعنوان مثال ممکن است تعداد شناسه‌های ضدبدافزار یک UTM بسیار کمتر از UTM دیگر باشد، همچنین ممکن است فعال کردن یکی از سرویس‌های امنیتی UTM، تاخیر زیادی در پردازش بسته‌ها توسط UTM ایجاد کند و یا سرویس کنترل برنامه‌های کاربردی در یک UTM امکان انتخاب و جلوگیری از اجرای برنامه‌های بیشتری را نسبت به UTM دیگر داشته باشد. تنها راه پی بردن به این تفاوت‌ها، آزمایش و بررسی عملی UTM است.

میزان گذردهی[1] و کارایی[2]

تولیدکنندگان UTM، معمولاً دستگاه‌های خود را در مدل‌های مختلف برای شبکه با ترافیک متفاوت عرضه می‌کنند. برای هر یک از مدل‌ها میزان کارایی سرویس‌های مختلف (بعنوان مثال دیواره آتش، ضدبدافزار، IPS و...) براساس مقادیر Mbps یا Gbps عنوان می‌گردد. ضروری است در هنگام انتخاب مدل UTM، ترافیک شبکه براساس این مقادیر ارزیابی گردد و با در نظر گرفتن گسترش‌های آینده اقدام به خرید UTM کرد. همچنین در برخی موارد ممکن است مقادیر اعلام شده توسط شرکت سازنده با واقعیت تطابق نداشته باشد بنابراین ضروری است قبل از خرید دستگاه، اقدام به تست عملی آن دستگاه در شبکه مقصد گردد.

---

[1] Throughput

[2] Performance

نوع پردازش بسته‌ها

برخی از UTMها به‌صورت نرم‌افزاری و برخی دیگر به‌صورت سخت‌افزاری بسته‌ها را پردازش می‌کنند. UTMهایی که بسته‌ها را به‌صورت سخت‌افزاری پردازش می‌کنند میزان گذردهی و کارایی بهتری دارند و در ضمن قیمت آن‌ها بالاتر از نمونه‌هایی با پردازشگر نرم‌افزاری است. استفاده از این نوع UTMها نسبت به مدل‌هایی با پردازش نرم‌افزاری ارجحیت دارد.

نوع سیستم عامل مورد استفاده در UTM

توصیه می‌گردد UTMی برای استفاده انتخاب گردد که سیستم‌عامل مخصوص به خود را داشته باشد. زیرا در این حالت، امکان حدس زدن نقاط ضعف امنیتی سیستم‌عامل آن توسط نفوذگران وجود نخواهد داشت.

وجود مستندات کامل، پشتیبانی مناسب و امکان بروزرسانی

لازم است تا سازنده برای کار با دستگاه، مستندات کاملی فراهم کرده باشد. در این صورت استفاده از امکانات دستگاه راحت‌تر خواهد شد.

از آنجا که دستگاه UTM معمولاً در گلوگاه شبکه قرار می گیرد، اگر شرکت سازنده از تیم پشتیبانی قوی و سریعی برخوردار نباشد، ممکن است در صورت بروز اشکال برای دستگاه باعث از کار افتادن و قطع سرویس‌های موجود در شبکه گردد. بنابراین می‌بایست دستگاه UTM از پشتیبانی مناسبی برخوردار باشد.

همچنین بهتر است دستگاهی جهت نصب در شبکه انتخاب گردد که احتمال بسیار ضعیفی در اختلال بروزرسانی پایگاه داده ضد بدافزار، IPS ، سامانه پالایش وب و ... آن وجود داشته باشد.

بومی بودن محصول

از زمانیکه برخی از نگرانی‌ها در خصوص تعرض به حریم خصوصی افراد و سازمان‌ها و قطع سرویس‌های ضروری ظاهر گردید، متخصصان فناوری اطلاعات جهت مقابله با این تهدیدات و تأمین پایداری خدمات تحت شبکه بنگاه‌ها، افراد و دستگاه‌های مختلف تلاش‌های ارزشمندی را ساماندهی نمودند تا فضای اعتماد به تبادلات الکترونیکی دچار آسیب کمتری شود. در همین راستا تولید محصولات مختلف امنیتی اعم از تجهیزات سخت‌افزاری و نرم‌افزاری در حوزه‌های گوناگون، ارائه راهکارها و تدوین سیاست‌های خرد و کلان جهت صیانت از امنیت و پایداری فضای تبادل اطلاعات، تربیت نیروهای متخصص به منظور حفاظت از شبکه‌های تبادل اطلاعات، همچنین ایجاد آمادگی در برابر حوادث ناشی از تهدیدات الکترونیکی، همگام با پیشرفت دانش IT در صحنه دنیای دیجیتال نمود بیشتری پیدا کرده است.

نخستین قدم در مسیر تحقق امنیت و پایداری در فضای تبادل اطلاعات کشور، تأمین و تولید خدمات و محصولات امنیتی مورد نیاز بصورت بومی و با استفاده از دانش پایه این فناوری بمنظور کاهش و قطع وابستگی به محصولات امنیتی دیگر کشورها است. در این راستا لازم است به طور جد نسبت به بومی سازی، افزایش توان داخلی و استفاده از این محصولات در محیط شبکه ملی اقدام شود. از اینرو با توجه به شرایط بین المللی از یک سو و همچنین تحریم‌های مطرح، بومی بودن سامانه‌ها و اتکا به توان داخلی از مهمترین شاخصه‌های انتخاب در این حوزه است. از طریق استفاده از سامانه‌های بومی از طرفی از انتقال اطلاعات داخل سازمانی و بعضاً دارای طبقه‌بندی به خارج از کشور توسط دستگاه‌های تولید بیگانگان تا حد زیادی جلوگیری بعمل می‌آید و از سمت دیگر محدودیت‌های پشتیبانی و ارائه خدمات با جایگزینی توان داخلی مرتفع می‌گردد.

روش‌های مقابله با مخاطرات امنیتی و ایمنی در مسیریاب

با توجه به نقاط آسیب‌پذیر و همچنین بررسی تهدیدات و حملات صورت گرفته علیه مسیریاب‌ها، برقراری امنیت در حوزه کاری مسیریاب باید در چهار لایه مختلف به شرح ذیل دنبال شود.

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

۲. نرم‌افزار و پیکربندی ثابت: مفاهیمی همچون نشانی واسط‌ها، رمزهای عبور و کنترل دسترسی به درگاه‌های پیکربندی، در این لایه مطرح می‌شوند و قابل دسترسی هستند، از سوی دیگر با توجه به اینکه در صورت نفوذ به این لایه، کنترل لایه‌های بالاتر نیز به دست نفوذگر خواهد افتاد، مصون نگاه داشتن این لایه از آسیب‌ها، حملات و نفوذهای احتمالی اهمیت خاصی خواهد داشت از این‌رو باید سیاست امنیتی مربوط به آن به دقت و بصورت جامع تدوین و اعمال شود.

۳. پیکربندی پویا: این لایه شامل اطلاعاتی همچون جدول‌های مسیریابی و ARP[۱] و گزارشات است. سیاست‌های امنیتی، باید نحوه دسترسی به این لایه را مورد توجه قرار دهند.

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.

---

[۱] Address Resolution Protocol

بررسی نکات و دستورالعمل های امنیتی دسترسی به مسیریاب

در این قسمت از کتابچه نگاهی مختصر به مهمترین روش ها و موارد مؤثر در دسترسی به یک مسیریاب خواهیم داشت و در هر بخش به راهکارهای لازم جهت ارتقای ضریب امنیتی مربوطه اشاره ای خواهیم کرد.

۱. دسترسی فیزیکی

مهمترین و اولین نکته‌ای که باید مورد توجه مدیر امنیتی یک مسیریاب قرار گیرد، امنیت دسترسی فیزیکی و ایمنی آن است. اگر امنیت فیزیکی مسیریاب تأمین نشود، تدابیر امنیتی دیگر نیز، اثرات مورد انتظار را نخواهند داشت. اگر مهاجم به یک مسیریاب دسترسی فیزیکی داشته باشد، در صورت داشتن تجهیزات لازم ودانش کافی، قادر خواهد بود کنترل کامل مسیریاب را در دست بگیرد. از راهکارهای تأمین امنیت فیزیکی می‌توان به نگهداری مسیریاب در یک محوطه در بسته امن و ایمن و اعمال سیاست های کنترل تردد و احراز هویت مناسب اشاره کرد.

۲. پیکربندی مسیریاب

اعمال هر تغییر در پیکربندی مسیریاب ممکن است باعث ایجاد یک آسیب‌پذیری جدید و یا اختلال در عملکرد مسیریاب گردد. از این‌رو دقت در پیکربندی این سامانه و اعطای مجوزهای لازم تنها به افراد صاحب صلاحیت از اهمیت فراوانی برخوردار است. باید دقت شود هرگونه پیکربندی و یا تغییر در آن پس از طی مراحل لازم و تنها هنگامی صورت پذیرد که اطمینان کافی از سلامت پیکربندی وجود داشته باشد. بعنوان نمونه یکی از موارد عمومی مهم، هنگام پیکربندی مسیریاب غیرفعال کردن واسط‌های بدون استفاده است.

۳. فهرست دسترسی[۱]

فهرست‌های دسترسی، از ابزارهای معمول مورد استفاده جهت اعمال سیاست‌های امنیتی سازمان‌ها و متولیان شبکه در خصوص تعیین اجازه عبور انواع بسته‌های ورودی به مسیریاب است. درصورتی که پس از انطباق یک بسته ورودی با فهرست دسترسی، این بسته اجازه عبور پیدا نکند، عملیات مسیریابی روی آن انجام نمی‌گیرد.

ساده‌ترین نوع فهرست دسترسی، فهرست دسترسی استاندارد است. در این نوع فهرست دسترسی می‌توان عبور داده از یک واسط را برحسب نشانی مبدأ بسته، کنترل کرد. بعد از تعریف فهرست دسترسی، هیچ بسته‌ای عبور نخواهد کرد مگر اینکه در فهرست دسترسی، به آن اجازه عبور داده شده باشد. فهرست دسترسی استاندارد فقط بر حسب نشانی IP مبدأ می‌تواند به بسته‌ها اجازه عبور و بسته های عبور داده نشده را گزارش دهد. با توجه به محدودیت‌های این نوع فهرست دسترسی، امروزه نوع دیگری از فهرست دسترسی مورد توجه قراردارد که فهرست دسترسی گسترش‌یافته[۲] نامیده می‌شود. در فهرست دسترسی گسترش‌یافته، می‌توان برحسب نشانی مبدأ، نشانی مقصد، پورت مبدأ، پورت مقصد، پروتکل و حتی اینکه ارتباط قبلاً برقرار شده است یا نه، اجازه عبور بسته‌ها را داد و یا از عبورآن‌ها جلوگیری کرد. باتوجه به توانمندی‌ها و پیچیدگی‌های این امکان، نحوه ساختن این فهرست‌ها از اهمیت فراوانی برخوردار است. چراکه تعریف صحیح فهرست‌های دسترسی و وجود سیاست‌های مناسب

---

[۱] Access list

[۲] این نوع فهرست دسترسی به عنوان پایه‌ای برای فهرست‌های دسترسی پیشرفته‌تر نظیر فهرست‌های Context-Based و Reflex محسوب می‌شود.

در این حوزه باعث می‌شود تا همه بسته‌هایی که مجاز هستند، بتوانند عبور کنند و هیچ بسته غیرمجازی، اجازه عبور نیابد.

۴. رمز عبور[۱]

رمز عبور، کلید اصلی و از پایه‌ای‌ترین مفاهیم در جلوگیری از دسترسی بدون مجوز به تجهیزات شبکه‌ای است. اولین قدم در مدیریت رمز عبور، انتخاب رمز عبور مناسب و محافظت از آن است. از جمله سیاست های لازم در انتخاب رمز عبور، می توان به موارد ذیل اشاره کرد:

۲۴. رمز عبور نباید از نام سازمان مربوطه منتج شده باشد.
۲۵. رمز عبور نباید کوتاه باشد.
۲۶. تغییر رمز عبور، نباید بر یک قاعده ثابت باشد.
۲۷. مدیران غیرتکنیکی نباید رمز عبور را بدانند.
۲۸. رمز عبور نباید در جایی نوشته یا دخیره شود.

۵. خطوط کنترل[۲]

دسترسی به خطوط کنترل، شامل پورت کنسول، درگاه کمکی[۳] و درگاه telnet باید محدود شود. اولین روش برای پیکربندی و مدیریت مسیریاب، پورت کنسول است، لذا تأمین امنیت و پایداری آن بسیار ضروری است. از جمله روش های عمومی اعمال محدودیت در دسترسی به خطوط کنترل می‌توان به استفاده از رمز عبور و یا جلوگیری از اتصال از راه دور اشاره نمود.

---

[۱] Password

[۲] Line Access Router

[۳] Auxiliary ports

بررسی نکات و دستورالعمل های امنیتی پروتکل های مسیریابی

قسمت مهمی از امنیت مسیریاب، امنیت مسیریابی آن است. بعنوان مثال، یک مهاجم می تواند با فرستادن پیام های مسیریابی غلط، باعث تغییر در جدول های مسیریابی شود و بدین ترتیب در کل عملیات مسیریابی اختلال ایجاد کند. مهاجم همچنین می تواند داده های عبوری شبکه را به سمتی که مایل است هدایت کرده و از این طریق باعث به خطر افتادن امنیت شود. برای جلوگیری از این تغییرات غیرمجاز و نادرست در جدول های مسیریابی، چند راه وجود دارد:

۶. استفاده از مسیریاب ثابت: این روش در شبکه های کوچک، قابل اجراست ولی برای شبکه های بزرگ، مناسب نمی باشد.

۷. استفاده از فهرست دسترسی بعنوان صافی: در بسیاری از مواقع برای جلوگیری از عبور داده‌های خاص، از فهرست‌های دسترسی استفاده می‌کنند. فهرست دسترسی دارای توانایی های متعددی است.

۸. احراز هویت[۱]: با استفاده از این روش، منابع اطلاعاتی که اطلاعات مسیریابی را می فرستند، احراز هویت می شوند و از دسترسی و تغییرات غیرمجاز به صورت خودکار جلوگیری به عمل می آید.

۹. غیرفعال کردن مسیریابی RIP[۲] و استفاده از پروتکل OSPF[۱] به جای آن: علی‌رغم مزیت سرعت در پروتکل RIP، این پروتکل در انتقال پیام‌ها

---

[۱] Dynamic Routing Authentication

[۲] Routing Information Protocol

غیر قابل اطمینان است لذا اگر استفاده از آن برای رفع نیاز خاصی لازم نیست، بهتر است به جای آن از پروتکل OSPF استفاده شود.

۱۰. پنهان کردن اطلاعات مسیریابی: یکی دیگر از راهکارهای جلوگیری از تغییرات غیرمجاز در جداول مسیریابی جلوگیری از دسترسی مهاجمین یا نفوذگران به اطلاعات مربوط به مسیریابی از طریق دستورات و امکانات تعبیه شده در مسیریاب‌ها است. بدین ترتیب باعث می‌شویم که مسیریاب های دیگر، نتوانند اطلاعات مسیریابی پروتکل مورد استفاده را برای مسیریابی خود به دست آورند.

همچنین ممکن است بر روی پروتکل‌های مسیریابی حملات DoS نیز صورت گیرد. بعنوان یکی از نتایج این حملات می توان به جلوگیری از فرستادن و یا دریافت اطلاعات مسیریابی و یا از کار افتادن بخش‌هایی از شبکه اشاره کرد. برای مقابله با این حملات باید نسخه های پشتیبان از اطلاعات مسیریابی موجود باشد تا به سرعت بتوان خسارت وارده را جبران کرد.

---

[۱] Open Shortest Path First