وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

توصیه نامه ایمن سازی ساختارها و سامانه های فناوری اطلاعات

توصیه نامه شماره ۶ :حفاظت در مقابل کدهای سیار

نوع سند	توصیه نامه
سطح دستیابی سند	عمومی
سطح امنیتی سند	عادی
اولویت سند	خیلی فوری
تاریخ ارائه سند	خرداد ۹۰
نگارش سند	۱
تعداد صفحات	۸
مؤلف/مؤلفین سند	سازمان فناوری اطلاعات
کد سند	R900310-6

هدف:

هدف از تدوین این توصیه نامه محافظت از اطلاعات سازمانی در مقابل تهدیدهای ناشی از بکارگیری کدهای سیار[1] می باشد.

ضرورت:

کدهای سیار، نرم افزارهای کم حجم و معمولاً پرقدرتی هستند که به صورت گسترده ای در اینترنت و سایر شبکه های رایانه ای به کار گرفته می شوند و امکانات بسیاری را در اختیار استفاده کنندگان قرار می دهند.

تهدید ناشی از این نرم افزارها از آنجا سرچشمه می گیرد که این گونه ابزار معمولاً حین تماس کاربر با یک وب سایت و بدون آگاهی وی، از رایانه راه دور به رایانه او منتقل شده و به صورت خودکار نصب می شوند و امکانات کنترلی بسیاری را در اختیار رایانه راه دور قرار می دهند. این امکانات با هدف تسهیل بهره برداری کاربر از امکانات رایانه (سایت) راه دور ایجاد می شوند ولی به آسانی می توانند مورد سوءاستفاده قرارگرفته و باعث افشاء یا تخریب اطلاعات شوند.

[1] - Mobile Code

الزامات:

- لازم است روش های استفاده از کدهای سیار در شبکه ارتباطی مطالعه شده و بر اساس نیازهای موجود یا آینده، سیاست ها و پیکربندی های ضروری برای امن سازی بهره برداری از کدهای سیار تدوین شده و بر روی ماشین های میزبانی که نیاز به استفاده از آن دارند اعمال شود. به عنوان مثال اگر از زبان برنامه نویسی جاوا استفاده می شود لازم است تحلیل ریسک امنیتی بکارگیری ماشین مجازی جاوا روی ایستگاه های کاری انجام پذیرد.
- هنگام حفاظت از میزبان در مقابل کد سیار باید از مکانیزم های بهبود یافته تصدیق هویت، روشهای کنترل صحت داده ها و کنترل دسترسی کدهای سیار و همچنین بررسی صحت معنایی کد استفاده نمود.
- از آنجا که روش های حفاظت از میزبان ها در مقابل تهدیدات ناشی از کدهای سیار و یا حفاظت از کدهای سیار در مقابل عملکرد میزبان های آلوده نیاز به سطح بالایی از دانش تخصصی برنامه نویسی (در سطح سیستم) دارد، استفاده از مشاوره فنی نهادهای تخصصی در این زمینه ضروری است.
- در بخش سیاست گذاری لازم است در خصوص صدور مجوز استفاده از قابلیت های جاوا ، جاوا اسکریپت ، Activex و مانند آن در هر یک از مرورگرهای وب نصب شده بر روی ایستگاه‌های کاری تصمیم گیری شود. نتیجه تصمیم باید اعمال یکی از سیاست های زیر باشد:
  - قابلیت های فوق غیرفعال[1] شوند.

[1] - Disable

- قابلیت های فوق فقط هنگام ارتباط با سرورهای داخلی فعال باشند.
- قابلیت های فوق فقط هنگام ارتباط با سرورهای معتمد[1] فعال باشند.
- قابلیت های فوق هنگام ارتباط با هر نوع سروری فعال باشد.

- محصولاتی که برای حفاظت در مقابل تهدیدات ناشی از کدهای سیار به کار گرفته می شوند لازم است خود دارای گواهینامه های امنیتی مربوط که بر اساس استانداردهای مرتبط صادر شده اند باشند. (به عنوان مثال بر اساس معیارهای معرفی شده در CC[2] یا NIST Sp800-23 ارزیابی و سطح بندی شده باشند). البته لازم است توجه شود رعایت الزامات این استانداردها به معنی امن بودن کامل محصول نیست، زیرا برخی از محصولاتی که در کشورهای غربی (بخصوص ایالات متحده) تولید و یا عرضه می شوند ملزم به رعایت شرط هایی هستند که ممکن است ناقض اصل محرمانگی در سایر کشورها باشند. بنابراین در مراکز حساس و حیاتی لازم است قبل از استفاده از این گونه ابزار امنیتی، ارزیابی داخلی در خصوص آنها به عمل آید.

- ممیزی پیکربندی مرورگرهای وب به منظور اطمینان از رعایت سیاست پذیرش کدهای سیار باید به طور مرتب انجام شود.

- کنترل نسخه[3] و مدیریت وصله های نرم افزاری[4] باید به عنوان بخشی از برنامه کنترل کدهای سیار محسوب شده و به اجراء گذاشته شود.

[1] - Trusted
[2] -Common Criteria for Information Technology Security Evaluation
[3]- Version Control
[4]- Patch Management

- در شرایطی که اصولاً نیازی به دریافت کد سیار نیست (مثل کامپیوترهایی که خطوط تولید را کنترل می نمایند و یا به فرآیند خاصی تخصیص داده شده اند) لازم است از روش جداسازی (منطقی یا فیزیکی) استفاده شود تا ریسک ناشی از تهدیدات کد سیار به طور کامل حذف گردد.

- برای کاهش ریسک تهدیدات ناشی از کدهای سیار تا حدی که امکان دارد باید از نصب نرم‌افزارهای متعدد روی یک ایستگاه کاری جلوگیری شود. هر چه تعداد نرم افزارهای نصب شده روی یک ایستگاه بیشتر باشد احتمال پیکربندی نادرست افزایش می یابد.

- به هر نرم افزار فقط باید حق دسترسی در حد مورد نیاز آن اعطاء شود. به عنوان مثال در سیستم عامل یونیکس نرم افزارهایی که با حقوق دسترسی ممتاز (مثل کاربر Root) اجراء می شوند می‌توانند بسیار خطرناک باشند.

- برای حفاظت از کد سیار در مقابل میزبان آلوده نیز (که به تازگی به آن توجه شده است و دارای پیچیدگی های خاص خود است) باید از طریق حفاظت از داده های انتقالی (در مقابل حفاظت از کد) و روش های مبتنی بر صحت یا محرمانگی اقدام نمود.

- لازم است نرم افزارهای کاربردی قابل استفاده در سیستم های مدیریت اطلاعات، بر اساس مدل «دفاع عمقی[1]» طراحی شده باشند تا در صورت ضعف عملکرد سیستم عامل در مقابل حملات، بتوانند از داده های خود حفاظت نمایند.

[1]- Defense in Depth

- لازم است رویه های پاسخگویی به حوادث حاوی دستورالعمل های مقابله با حوادث ناشی از عملکرد کدهای سیار و چگونگی محدودسازی اثرات آن باشد.

فرآیند:

مراحل پیاده سازی این توصیه نامه به شرح زیر می باشد:

- در ابتدا مطالعه ای بر روی انواع مختلف کد های سیار و بخصوص انواع جدید آن صورت گرفته و فهرستی از گونه های کد سیار تهیه می شود.

- در صورتی که نیاز به دریافت کد سیار نباشد ممنوعیت دریافت آن به اطلاع کاربران رسیده و مکانیزم اطمینان از آن تدوین و پیاده سازی شود.

- در صورت نیاز به دریافت کد سیار بایستی ریسک امنیتی استفاده از این کدها مورد ارزیابی قرار گرفته و مخاطرات آن برآورد شود.

- پس از تحلیل ریسک، الزامات امنیتی و سیاست های امن سازی بهره برداری از کدهای سیار در راستای حذف، کاهش یا مدیریت مخاطرات تدوین شود.

- مکانیزم ها و ابزار مورد نیاز جهت برآورده ساختن الزامات و سیاست ها تامین شود.

- پس از تامین مکانیزم ها و ابزار، مکانیزم ها پیاده سازی شده و کلیه الزامات و سیاست های تدوین شده اجرا شود.

- در صورتی که کلیه الزامات کنترل کدهای سیار تدوین شده (بیان شده در این توصیه نامه و الزامات اختصاصی سازمان) برآورده شده باشد دریافت کدهای سیار بلامانع خواهد بود.

به طور کلی روش های حفاظت در مقابل آسیب های ناشی از عملکرد کدهای سیار را می توان به صورت شکل زیر فهرست نمود:

- اجرای کد سیار در محدودهٔ تحت کنترلی از ماشین میزبان بعد از چک کردن خواص مختلف از جمله خواص زبان برنامه نویسی یا ترکیب دستورالعمل های موجود در آن
- تعیین شرایط (سیاست های) ثابت برای جلوگیری از اجرای کد سیار
- استفاده از امضای دیجیتال برای تصدیق هویت و تضمین محتوی کد ارسال شده
- استفاده از روش های کنترل دسترسی برای محدود ساختن حوزه های حمله احتمالی
- کنترل ساختار کد با در نظر گرفتن هدف ارسال یا اجرای آن
- استفاده از روش های رمزنگاری برای تضمین صحت داده های ارسالی
- کنترل صحت پردازش انجام شده توسط میزبان بر روی کد سیار
- کنترل محرمانگی روش پردازش کد و یکتایی آن در ماشین میزبان
- انجام ممیزی های دوره ای بر اساس چک لیست های درون سازمانی

توضیحات:

کد سیار نرم افزاری است که هنگام تماس با سیستم های راه دور (معمولاً در اینترنت) به ایستگاه کاری تماس گیرنده منتقل[1] شده و بدون آگاهی کاربر روی ایستگاه کاری نصب و اجراء می شود. مثالهایی از کدهای سیار عبارتند از:

- اسکریپت های جاوا[2]
- اسکریپت های ویژوال بیسیک[3]
- اپلت های جاوا[4]
- کنترل های اکتیواکس[5]
- پویانمایی های فلش[6]
- تصویرهای متحرک Shock Wave[7]

همچنین کدهای سیار می توانند از طریق فایل های ضمیمه پست الکترونیک (مثل ماکروهای موجود در یک فایل متنی) و یا کدهای HTML موجود در بدنه پست الکترونیک به ماشین کاربر منتقل و بدون آگاهی وی نصب شوند. هرچند کدهای سیار برای انجام عملیات ضروری یا افزودن کارآیی برنامه های تحت وب و با اهداف مثبت، طراحی و بکار گرفته شده اند اما می توانند به عنوان دریچه ای آسان برای

[1]- Download
[2]- Java Script
[3]- VB Script
[4]- Java Applet
[5] -Activex control
[6]- Flash Animations
[7]- Shock Wave Movies

نفوذ به رایانه های هدف به کار گرفته شوند. در حالت عادی کدهای سیار به دلایل زیر به کار گرفته می شوند:

الف- جمع آوری داده از مکان های مختلف و متعدد

ب- جستجو و غربال گری

ج- دیده بانی و آشکارسازی

د- انتشار اطلاعات مورد نظر

هـ- بحث و گفتگو

و- تجارت الکترونیکی

ز- پردازش موازی

ح- سرگرمی