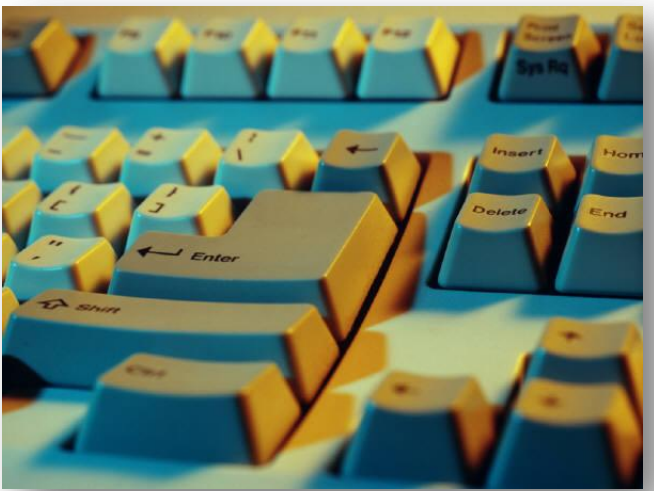
امنیت سخت افزاری

کامپیوترهای شخصی



فهرست

آغاز

هر رایانه از مجموعه ای از سخت افزارها و نرم افزارها تشکیل شده است. در ادامه به بررسی سخت افزارهایی که در امنیت رایانه نقش اساسی دارند می پردازیم.

حافظه‌های سخت افزاری و نقش آن درامنیت رایانه

این قطعات از این نظر دارای اهمیت هستند که کلیه اطلاعات در زمان تولید و بازتولید بر روی این قطعات قرار گرفته و با جابجایی آنها اطلاعات نیز جابجا می شوند و در صورتیکه افراد غیر مجاز به این قطعات دسترسی داشته باشند عملاً به اطلاعات دسترسی پیدا خواهندکرد.

صفحه کلید ونقش آن درامنیت رایانه

کلیه اطلاعاتی که در رایانه تولید می شود به وسیله این قطعه تولید می شود.

اطلاعاتی که در بانک های اطلاعاتی وارد می شوند

اطلاعاتی که تحت عنوان یک نامه تولید می شوند.

اطلاعاتی که تحت عنوان گزارشات و بولتن ها تولید می شوند.

رمزهای عبور و نام کاربرانی که در ایمیل ها استفاده می شود.

شماره ها و رمزهای کارت های اعتباری که در شبکه های بانکی استفاده می شود.
نام کاربری و رمزهای عبوری که برای به روز رسانی سایت ها استفاده می شود.
اطلاعاتی که قرار است رمز شده و نگهداری شوند.
و.....
کمتر اطلاعاتی است که به صورت رقومی تولید شود و با این قطعه سروکار نداشته باشد. به همین خاطر اگر کسی بتواند به اطلاعاتی که از طریق این قطعه تولید می شود دسترسی پیدا کند می تواند ادعا داشته باشد که به تمام اطلاعات رایانه و کاربران مرتبط دسترسی پیداکرده است.
تمام نگهبانان ساختمان ها اسامی افراد و خودرو ها و لوازمی که به ساختمان وارد می شود و یا خارج می شود را یادداشت می کنند تا بتوانند اطلاعات کامل ورودی ها و خروجی های ساختمان را تهیه کنند تا در موارد ضروری بتوان از آن استفاده کرد. این کار بدین خاطر میسر است که نگهبانان در گلوگاه ورودی ساختمان مستقر شده اند.
صفحه کلیدها نیز در گلوگاه ورودی به رایانه ها قرار گرفته اند و می توانند همانند نگهبانان این کار را در فضای مجازی انجام دهند. با هر بار فشردن بر روی دکمه های صفحه کلید، پالسی تولید می شود که همتای کلید وارد شده بوده و در تمام دنیا از یک استاندارد واحد برخوردار است. با ارسال این پالس به داخل رایانه سایر قطعات متوجه نوع اطلاعات وارد شده خواهند شد. حال اگر فردی به صورت غیر مجاز از این پالس های عبوری تصویر تهیه کند می تواند همگام با رایانه در جریان کلیه اطلاعات تولید شده قرار گیرد. این وسیله یا ابزار غیر مجاز چیزی نیست به جز ثبت کننده کلیدها [1]

---

[1] keylogger

انواع ثبت کننده کلیدها

در ادامه به بررسی انواع ثبت کننده کلیدها خواهیم پرداخت.

ثبت کننده کلید سخت افزاری

این وسیله قطعه کوچکی است که بین صفحه کلید و انتهایی ترین قسمت برد اصلی قرار گرفته و کلیه اطلاعات تولید شده به وسیله صفحه کلید را ثبت و از طریق بیسیم به نزدیکترین پایگاه دریافت کننده ارسال می کند. نوع تجاری آن به عنوان قطعه ای به انتهای کابل صفحه کلید وصل شده و براحتی قابل شناسایی است. اما نوع اطلاعاتی آن می تواند به هر شکل قطعه الکترونیکی پوشش داده شده و جایگزین هر کدام از قطعات صفحه کلید و یا برد اصلی شود و به همین خاطر با بازرسی چشمی و یا استفاده از ابزار ابتدایی بازرسی، قابل شناسایی نخواهد بود.

ثبت کننده کلید نرم افزاری

این نرم افزار همانند دیگر انواع نرم افزار های کاربردی یک نرم افزار اجرایی بوده و پس از یک بار اجرا شدن در رایانه در حافظه مقیم شده و با هر بار خاموش و روشن کردن رایانه مجدداً فعال می شود. پس اگر برای یک بار در یک رایانه نصب شود نیاز به نصب مجدد نخواهد داشت و به صورت خودکار وظیفه خود را انجام خواهد داد.

شیوه های نصب ثبت کننده کلید نرم افزاری بر روی یک رایانه

نصب مستقیم

در این شیوه نفوذگر یا عوامل او به صورت مستقیم به رایانه دسترسی پیداکرده و نرم افزار را بر روی رایانه اجرا می کنند. به طور مثال ممکن است رایانه به علت خرابی به نزد یک مغازه و یا شرکت منتقل شود و در این مدت نرم افزار بر روی رایانه نصب می شود و یا ممکن است در طول سفر در داخل و یا خارج از کشور و هنگامی که رایانه در اتاق هتل و یا صندوق امانات هتل گذاشته شده است این

دسترسی صورت گرفته و نرم افزار نصب شود. همچنین ممکن است به صورت صوری سرقت موقت رایانه رخ دهد و پس از زمان اندکی رایانه پیدا شود و این مدت زمان برای نصب نرم افزار ثبت کننده کلید کفایت خواهد کرد!

نصب غیر مستقیم

در این روش ثبت کننده کلید از طریق الواح آلوده که از بازار و از افراد ناشناخته تهیه می شود و یا به صورت برنامه ریزی شده برای یک بار در رایانه (به هر دلیلی) اجرا می شود و به رایانه هدف منتقل می شود.

به طور مثال ممکن است:

گفته شود: «آیا امکان دارد این سی دی را بر روی رایانه خود تست کنید.»

یا در قالب سی دی تبلیغاتی و یا آموزشی از طریق پست و ... ارسال شود.

یا یکی از سی دی هایی که داشته ایم مفقود می شود و وقتی که پیدا می شود این نرم افزار بر روی آن نصب شده است و به مجرد قرار گرفتن در داخل رایانه نرم افزار اجرا می شود.

یا این نرم افزار از طریق یکی از قطعات سخت افزاری که به رایانه اضافه می شود به رایانه منتقل می شود.

یا در زمان اتصال به اینترنت از طریق ایمیل برایمان ارسال شده باشد(خود ایمیل و یا ضمائم ایمیل).

یا از طریق بیسیم و بلوتوث به داخل رایانه منتقل شود.

به مجرد نصب این نرم افزار بر روی رایانه اولین وظیفه آن که پنهان سازی خود است انجام می پذیرد و این پنهان سازی به روش های مختلف صورت می پذیرد. بطوریکه در جستجوی های عادی مانند لیست برنامه های نصب شده و جستجو در رایانه و ... نمی توان پی به وجود این نرم افزار برد.

انواع ثبت کننده های کلید نرم افزاری

آماتور

اینگونه از ثبت کننده ها معمولاً بـا اسـتفاده از انـواع ضـدبدافزارها قابـل پیگیـری، ردیابی و از بین بردن است و اطلاعات آنها معمولاً در بانـک اطلاعـاتی ایـن ابـزار یافت می شود.

حرفه ای

اینگونه از ثبت کننده ها تا زمانی که در یک نقطه از دنیا کشف نشوند، در بانـک اطلاعاتی ضدبدافزارها قرار ندارند و به همین خاطر نبایـد انتظـار داشـت بتـوان بـا استفاده از ضدبدافزارها آنها را پیداکرد.

چه اطلاعاتی توسط ثبت کننده ها ثبت می شوند؟

همانگونه که قبلا نیز گفته شد تقریباً تمـام اطلاعـات تولیـد شـده توسـط کـاربران توسط این نرم افزارها ثبت می شود. به غیر از اطلاعات انتقالی توسط ابزار ذخیـره ساز، تمام اطلاعات تولید شده اعم از رمز یا غیر رمـز توسـط ایـن نـرم افـزار ثبـت می شود.

پس از ثبت چه اتفاقی برای اطلاعات ثبت شده می افتد؟

این نرم افزارها پس از انجام مأموریت خود در کسب اطلاعات، معمولاً به صورت ذیل عمل می کنند:

باقی ماندن در داخل رایانه به صورت فایل رمز شده و در مکانی پنهان که نفوذگر بتواند در نفود بعدی به آن دسترسی داشته وکپی کرده و از رایانه خارج کند.

انتقال از شبکه داخلی به یکی از رایانه های متصـل بـه شـبکه (بسـتگی بـه وسـعت شبکه در داخل یا خارج از کشور) و دسترسی نفوذ گر به اطلاعات از آن طریق.

ارسال از طریق اینترنت

به مجرد اتصال رایانه آلوده به شبکه اینترنت، فایل رمز شده به ایمیل و یا آدرس FTP ویا هر آدرسی که در اینترنت مشخص شده است ارسال می شود. این آدرس ها از قبل توسط برنامه نویس برای نرم افزار، مشخص شده است و ارسال اطلاعات معمولاً به بصورت پنهان و بدون برانگیختن حساسیت کاربر انجام می پذیرد.

به چه شکل در مقابل این نرم افزار ثبت کننده امنیت داشته باشیم؟

موارد ذیل از جمله اقدامات محافظتی است که می تواند کاربران را در مقابل این قبیل نرم افزارها مصون نماید.

عدم در اختیار گذاشتن رایانه به صورت فیزیکی در اختیار فرد نفوذگر به صورت مستقیم یا غیر مستقیم

عدم گرفتن ابزار ذخیره ساز از دیگران به منظور تست و ....

عدم اتصال ابزار ذخیره ساز ناشناس به رایانه

عدم اتصال رایانه دارای اطلاعات طبقه بندی شده به شبکه های ناشناس و مخصوصا اینترنت

نصب نرم افزارهای معتبر ضدبدافزار و به روزکردن بانک اطلاعاتی آن (البته نه از طریق اتصال به اینترنت!!)

نصب نرم افزار های آشکارکننده ارسال و دریافت اطلاعات مانند انواع فایروال

دقت در هنگام تحویل رایانه برای تعمیر و یا تنظیم و یا نصب نرم افزار و سخت افزار جدید

کنترل مجدد ابزار ذخیره سازی که روی رایانه های دیگری نصب شده است، قبل از نصب مجدد بر روی رایانه خود

Setup و نقش آن در امنیت رایانه

این مرحله را می توان اولین مرحله ایمن سازی رایانه (در صورت فعال شدن) برای کاربر در نظر گرفت. اطلاعات اولیه موجود در اینقطعه (بایوس یا سیموس) را می توان به دو گروه متمایز از یکدیگر تقسیم بندی کرد:

- اطلاعات مربوط به کارخانه سازنده
- اطلاعات مربوط به کاربر

اطلاعات اولیه مربوط به کارخانه سازنده در بر گیرنده اطلاعات اولیه مربوط به سخت افزار و راه اندازی ابتدایی رایانه و شناسایی سخت افزار ها و صحت کارکرد آن ها بوده و قسمت دیگر مربوط به کاربر و اطلاعات اولیه ای که توسط کاربر تنظیم می شود و یکی از این اطلاعات مربوط به رمز اولیه است که توسط کاربر در این رابطه تنظیم می شود. این رمز قابل تغییر بوده وتوسط هر کاربر می تواند به صورت دلخواه تنظیم شده و یا غیر فعال گردد.

این رمز کارکردهای مختلفی می تواند داشته باشد:

- ممانعتازدسترسیبهتنظیماترایانه
- ممانعتازدسترسیبه هاردرایانه
- ممانعتازدسترسیبهاطلاعاترایانهبهصورتبدون رمز (اطلاعات هارد را به رمز تبدیل می کند.)
- ترکیبی از حالات فوق

در زمان فعال سازی این رمز به مجرد روشن کردن رایانه توسط هر فردی پس از چک کردن صحت عملکرد سخت افزار رایانه پیغامی به شکل زیر مشاهده و بدون داشتن رمز مربوطه امکان ادامه کار با رایانه وجود نخواهد داشت:

Enter your password

بسیاری از کاربران با اطمینان از اینکه این رمز می تواند مانع از دسترسی افراد غیر مجاز به اطلاعات رایانه آن ها شود، رایانه را در موقعیت های مختلف به شکل خواسته و یا نا خواسته در اختیار افراد غیر مجاز قرار می دهند.

با توجه به اینکه اطلاعات در این قسمت به صورت سخت افزاری ذخیره می شود احتمال اینکه با جابجایی رایانه و قطع برق، اطلاعات این قسمت (ازجمله رمز) پاک شود وجود دارد. کارخانه های سازنده رایانه برای اینکه این نقیصه را برطرف کنند معمولاً در کنار این قطعه یک عدد باطری قابل شارژ[1] قرار می دهند تا به صورت خودکار توسط برق، شارژ شده و برای زمان های کوتاه چند ساعته که برق قطع می شود برق مورد نیاز این قطعه را تأمین کند. روش های گذر از این رمز توسط افراد غیر مجاز در ادامه بیان می شود.

- قطع برق رایانه همزمان با برداشتن باطری بک آپ

در این حالت نفوذگر پس از باز کردن کیس رایانه ابتدا جریان برق رایانه را با قطع اتصال برق قطع کرده و پس از آن باطری را از محل خود خارج می سازد و بدینوسیله باعث می شود که اطلاعات مربوط به کاربر (از جمله رمز اولیه) برداشته شود. با برداشتن رمز به راحتی نفوذگر می تواند از این مرحله عبور نماید.

عیب این کار برای نفوذگر این است که به مجرد اینکه کاربر اصلی بخواهد رایانه را روشن کند متوجه فاقد رمز بودن رایانه شده و مشخص می شود که فردی به این رایانه نفوذکرده است. نفوذگران برای حل این مسأله با توجه به اینکه رمز اولیه را نمی دانند، با گذاشتن یک رمز دیگر تلاش دارند تا به کاربر این نکته را القاء کنند که به علت نوسانات برق یا رعد و برق و یا

---

[1] Backup battery

فراموشی یا .....!! این رمز به صورت خودکار تغییر پیداکرده است؛ و حال شما می دانید که به هیچ عنوان با نوسانات برق و رعد و برق و.... این رمز تغییر نخواهد کرد و تنها علت آن می تواند تحرکات یک نفوذگر باشد.

- رمز از پیش تعریف شده [۱]

تمام رایانه ها برای این قسمت دارای رمز از پیش تعریف شده (مانند شاه کلید) بوده و اگر کسی دارای این رمز باشد بدون نیاز به رمز تعریف شده توسط کاربر می تواند به سهولت وارد رایانه شده و این دسترسی هیچ تأثیری بر روی عملکرد رمز کاربر نخواهد داشت و کاربر در مراجعه به رایانه با هیچ تغییری در رایانه خود مواجه نخواهد شد.

این رمز معمولاً در اختیار نمایندگی های مجاز شرکت های سازنده رایانه بوده و از آن برای رفع عیب و ... در زمان ارجاع رایانه برای تعمیر استفاده می کنند.

بسیاری از کاربران در این اندیشه هستند چون این رمز در اختیار نمایندگی های مربوطه است پس هیچ خطری آنها را تهدید نمی کند و با کوچکترین اتفاقی که در این رابطه بیفتد می توانند با مراجعه به عوامل انتظامی و طرح شکایت از نمایندگی های مربوطه دایره مظنونین را تنگ ترکرده و به فرد نفوذگر دسترسی داشته باشند. اما شما نیک می دانید که با مراجعه به سایت های اینترنتی از جمله www.passware.com می توان این نکته را متوجه شد که فقط نمایندگی ها و تمام افراد عالم دسترسی به این رمز ها را دارند! زیرا تقریباً ۲۴ ساعت پس از ارائه این رمز به نمایندگی ها، افراد سودجو این رمزها را کشف شده و در این سایت ها قرار می دهند.

---

[۱] Default password

- حمله به رمز

در این حالت نفوذگران با استفاده از نرم افزارهایی که می توان آن ها را به راحتی در اینترنت پیدا و در یک فلاپی و یا لوح راه انداز کپی کرد، سامانه را به صورت مستقل راه اندازی کرده و سپس با استفاده از این نرم افزارها به رمز حمله می کنند این نوع از حمله دو کارکرد می تواند داشته باشد:

۱. از کار انداختن رمز
۲. پیدا کردن و نشان دادن رمز

در هر دو حالت نفوذگر می تواند با فاقد رمزکردن و یا دانستن رمز به سامانه دسترسی داشته باشد. به نظر می رسد راه مقابله با این حمله گرفتن امکان دسترسی نفوذگر به لوح و یا فلاپی به منظور ممانعت از بوت کردن سامانه باشد. این کار به دور روش صورت می پذیرد:

۱. سخت افزاری

در این روش ابزار مربوطه به صورت سخت افزاری از رایانه جدا می شود و اشکال برای کاربر اصلی این خواهد بود که دسترسی کار بر را نیز به این ابزار قطع کرده و چون کاربران اصلی با این ابزار زیاد کار دارند باعث سختی در استفاده از رایانه خواهد شد.

۲. نرم افزاری

در این روش با استفاده از روش های مختلف نرم افزاری که رایج ترین آن استفاده از قسمت setup است دسترسی به این ابزار قطع می شود. اشکال این روش در این است که نفوذگران می توانند با دسترسی به setup و دسترسی و یا از کار انداختن رمز آن مجدد سامانه را به حالت اولیه برگردانند و نیت خود را عملی سازند.

- استفاده از روش های از کار انداختن رمز از روی مادر برد

معمولاً بر روی مادربرد ها در قسمت هایی علامات کوچکی که بر روی آن clrp۱ نوشته شده است وجود دارد و نفوذگران با دسترسی به این قسمت و با استفاده از ابزار رسانه برق و ایجاد اتصال کوتاه می توانند رمز موجود setup را پاک کرده و از این مرحله عبور کنند.

***

البته روش های فنی دیگری نیز وجود دارد که نفوذگران می توانند با استفاده از آن ها و یا با استفاده از روش های ترکیبی از رمز اولیه رایانه عبور کنند. کاربران ممکن است پس از ترک فیزیکی و مراجعه مجدد به رایانه با حالات زیر روبرو شوند:

- رایانه فاقد رمز اولیه شده است:
  - این حالت نشان دهنده این است که نفوذ گر با استفاده از روش اول رمز سامانه را ازکار انداخته است.
- رمز اولیه رایانه عوض شده است:
  - این حالت نشان دهنده این است که نفوذ گر پس از از کار انداختن رمز کامپیوتر رمز دیگری را بر روی سامانه قرار داده است.
- رمز اولیه رایانه عوض نشده است:
  - این حالت می تواند نشان دهنده این باشد که نفوذ گر با استفاده از رمز های از پیش تعریف شده به سامانه نفوذ کرده است و هیچ رد پایی به جا نگذاشته است.

---

[۱] Clear password

نتیجه این خواهد شد که با هر بار دور شدن فیزیکی از رایانه، این احتمال باید داده شود که به رایانه نفوذی صورت گرفته است. (مخصوصاً در سفرهای خارج از کشور)

Rom[1] ونقش آن درامنیت رایانه

یکی دیگر از قطعات رایانه «رام» است. اطلاعات اولیه رایانه برای راه اندازی در این قطعه قرار داده شده است. تا سال ۲۰۰۰ میلادی این قطعه جزو قطعاتی بود که به حافظه فقط خواندنی معروف بودند یعنی اینکه این اطلاعات را می توان فقط خواند و نمی شود از آن ها کاست و یا اینکه به آنها اضافه کرد. در سال ۲۰۰۰ به علت به وجود آمدن مشکل تغییر تاریخ برای رایانه ها سازندگان به فکر افتادند که اطلاعات این قطعه را قابل ارتقاء و قابل تغییر سازند. به موازات، نویسندگان برنامه های مخرب که به دنبال این بودند تا از کوچک ترین حافظه که با تغییر هارد در آن اختلالی ایجاد نشود برای برنامه های خود استفاده کنند به فکر نوشتن برنامه های مخرب مقیم در این حافظه افتادند و امروزه استفاده از این فضا برای آلوده کردن سامانه ها به امری رایج در بین نفوذگران تبدیل شده است. پس اگر کسی احساس کرد بر روی هارد رایانه او برنامه مخرب وجود دارد و در نظر داشته باشد به عنوان آخرین راه حل برای نجات از دست این نرم افزار مزاحم هارد خود را فرمت نماید ممکن است با این ذکاوت نفوذگر روبرو شود که نرم افزار مخرب را در رام پنهان کرده باشد و عملاً موفق به فرار از دست این نرم افزار نشود.

---

[1] Read only memory

نقش سخت افزارهای دیگر در امنیت رایانه

سایر سخت افزار های یک رایانه که به عنوان اجزا ورودی و خروجی مورد استفاده واقع می شوند جزو ابزارهایی هستند که نفوذگران، نرم افزار های مخرب خود را از آن طریق در رایانه وارد می کنند. این مجموعه قطعات می توانند از درایوهای انواع الواح فشرده گرفته تا انواع کارت هایی که به رایانه اضافه می شود و انواع پورت های رایانه را شامل شود. کاربران عادی، امروزه فکر می کنند که تنها راه استفاده از فلاش ممووری در رایانه، استفاده از پورت های USB است اما کاربران حرفه ای تر می دانند کابل های رابط برای تبدیل هر پورتی به پورت دیگر به قیمت های ارزان در بازار فروخته می شود.