امنیت اطلاعات

بولتن تحلیلی ■ شماره دو ■ خرداد ۱۳۹۲

شرکت نرم افزاری

امن‌پرداز

مدیریت امنیت اطلاعات

بخش دوم

پس از بیان مفاهیم اولیه مدیریت امنیت اطلاعات در مقاله شماره ۱، در این مقاله و مقاله های بعدی مراحل پیاده سازی سیستم مدیریت امنیت اطلاعات مطرح خواهد شد.

در استاندارد ISO27001 به منظور ایجاد، پیاده سازی، بهره برداری، پایش، بازنگری، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات یک سازمان از یک رویکرد فرآیندی استفاده شده است.

این رویکرد فرآیندی براساس مدل PDCA (طرح- اجرا- بررسی و اقدام) است. این مدل بیانگر اصول حاکم بر امنیت شبکه ها و سیستم های اطلاعاتی می باشد.

فاز طرح:

• شناخت: سازمان در مرحله شناخت، کلیه فرآیندهای سازمانی و تجاری، شبکه و زیرساخت فناوری اطلاعات شامل سیستم عامل ها، پایگاه داده ها، ارتباطات، برنامه های کاربردی، سرورها، فایروال ها، روترها و سوییچ ها مورد مطالعه قرار می گیرند.

همچنین گردش اطلاعات در سازمان و خارج از آن مورد بررسی قرار می گیرد.

• ارزیابی وضعیت موجود: در این مرحله ارزیابی تکنیکی شامل آزمایش نفوذ و آسیب پذیری سیستم انجام می گیرد. در آزمایش نفوذ سعی می شود همانند نفوذکننده ها از خارج سازمان به سیستم های اطلاعاتی نفوذ کرد و به اطلاعات دست یافت. در ارزیابی آسیب پذیری، امنیت سیستم عامل ها، پایگاه داده ها، برنامه های کاربردی،، برنامه های کاربردی وب، فایروال ها، روترها و... مورد بازیابی و ممیزی قرار می گیرند.

همچنین سیاست ها و روال های امنیتی رسمی و غیررسمی که در سازمان وجود دارند، در این فاز بازبینی می گردد.

• تعیین قلمرو: جهت استقرار سیستم مدیریت امنیت اطلاعات در سازمان، قلمرو ISMS باید به طور شفاف مشخص گردد.

• شناسایی و دسته بندی دارایی های اطلاعاتی: در این مرحله، دارایی های اطلاعاتی شناسایی می گردند. سپس دارایی های شناسایی شده ارزش گذاری و دسته بندی می شوند.

• تدوین طرح ارزیابی ریسک: این مرحله شامل روش شناسی و ابزارهای ارزیابی ریسک، ساختار تیم ارزیابی ریسک، مسئولیت ها و... تدوین می شود.

• ارزیابی ریسک: در این مرحله، کلیه آسیب پذیری ها و سپس تهدیدات به دارایی های اطلاعاتی شناسایی شده در قلمرو سیستم مدیریت امنیت اطلاعات شناسایی می شوند. میزان تأثیر تهدیدات روی سازمان در صورت وقوع تهدیدات تعیین می شود.

• مدیریت ریسک: با توجه به ارزیابی ریسک، ریسک های غیر قابل پذیرش باید مدیریت گردند. کنترل های موجود در استاندارد ISO27001 جهت مدیریت ریسک های غیرقابل پذیرش در سازمان استفاده و انتخاب می شوند.

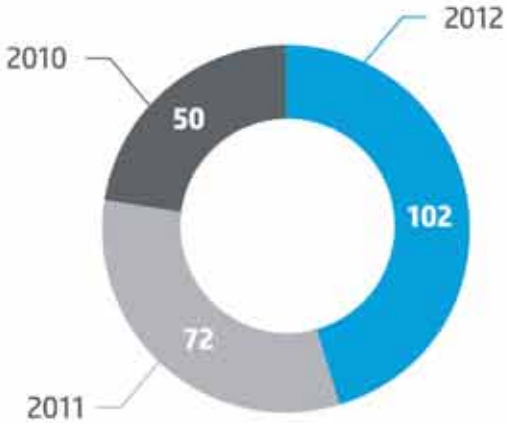
در شماره های بعدی به ادامه مطالب پرداخته خواهد شد.

هزینه‌های رو به افزایش جرایم سایبری

علی‌رغم آگاهی روز افزون مردم در مورد اثرات جرایم سایبری، با این حال جرائم سایبری، فراوانی بیشتری یافته و باعث ایجاد پیامدهای منفی اقتصادی بیشتری می‌شوند. بر اساس تحقیق انجام شده پیرامون هزینه **جرایم سایبری در سال ۲۰۱۲** که توسط شرکت "اچ پی" صورت گرفته است؛ حملات سایبری دو برابر شده‌اند و هزینه‌های اقتصادی ناشی از آن در طول ۳ سال تا ۴۰ درصد افزایش داشته‌اند. بنابر این داشتن اطلاعاتی درست (فهمی روشن) از هزینه‌های جرایم سایبری می‌تواند به سازمان‌ها در برداشت گام‌هایی پیشگیرانه کمک کند تا به دنبال آن بتوانند پیامدهای یک حمله سایبری بالقوه مخرب را تشخیص داده و به موقع با آن به مبارزه برخاسته و نیز از اثرات آن بکاهند

حملات

حملات موفق در هر هفته



هزینه

هزینه سالیانه تحمیل شده برای سازمان‌ها

بدافزار

متداولترین روش هک

زمان

میانگین زمان لازم برای مقابله با یک حمله

منبع: gerdab.ir

کشف تخریبی جدید در بد افزار Trojan.Win32.Narilam.a

به گزارش بخش تحلیل شرکت امن پرداز، در تحلیل های صورت گرفته توسط شرکت های گوناگون تا به حال تصور می شد کار اصلی این بدافزار تغیر تصادفی و در نتیجه تخریب فایل های پایگاه داده نرم‌افزارهای مالی باشدکه پایگاه داده‌های مربوط به نرم افزارهای امین، شهد و مالیران (محصول شرکت طراح سیستم) را مورد حمله قرار می‌دهد؛ اما تحلیل‌های انجام شده در بخش تحلیل شرکت امن پرداز مشخص کرد این بدافزار علاوه بر این به دنبال فایل‌هایی با پسوندهای a، cpp، mnt، vca، prg، frt وCpp می‌گردد و اطلاعات داخل آنها را به صورت تصادفی تغییر می دهد(شکل-۱).

```
mov     [ebp+var_38], 14h
mov     edx, offset a_cpp ; ".cpp"
lea     eax, [ebp+var_8]
call    n23
inc     [ebp+var_2C]
push    dword ptr [eax]
push    [ebp+var_4C]
call    Func8
add     esp, 0Ch
dec     [ebp+var_2C]
lea     eax, [ebp+var_8]
mov     edx, 2
call    n24
mov     ecx, [ebp+var_4C]
push    dword ptr [ecx+318h]
mov     [ebp+var_38], 20h
mov     edx, offset a_a ; ".a"
lea     eax, [ebp+var_C]
call    n23
inc     [ebp+var_2C]
push    dword ptr [eax]
push    [ebp+var_4C]
call    Func8
add     esp, 0Ch
dec     [ebp+var_2C]
lea     eax, [ebp+var_C]
mov     edx, 2
call    n24
mov     ecx, [ebp+var_4C]
push    dword ptr [ecx+31Ch]
mov     [ebp+var_38], 2Ch
mov     edx, offset a_frt_prg_vca_m ; ".frt,.prg,.vca,.mnt"
```

شکل ۱ - کدخوان فایل های cpp

اگر فایل loginunit.cpp را یافت و در داخل آن کد ;()update_combo وجود داشت، کد آن را تغییر می‌دهد (شکل-۲) .

```
loc_40836A:
mov     dl, 1
mov     eax, ds:off_45E190
call    @TAngles@$bctr$qqrv ; TAngles::TAngles(void)
mov     [ebp+var_C4], eax
mov     ecx, [ebp+arg_0]
push    dword ptr [ecx+330h]
mov     [ebp+var_9C], 0BCh
mov     edx, offset aLoginunit_cpp ; "loginunit.cpp"
lea     eax, [ebp+var_40]
call    n23
inc     [ebp+var_90]
push    dword ptr [eax]
push    [ebp+arg_0]
call    Func8
add     esp, 0Ch
dec     [ebp+var_90]
lea     eax, [ebp+var_40]
mov     edx, 2
call    n24
mov     [ebp+var_9C], 0C8h
lea     eax, [ebp+var_44]
call    unknown_libname_48 ; Borland Visual Component Library & Packages
mov     edx, eax
inc     [ebp+var_90]
mov     ecx, [ebp+arg_0]
mov     eax, [ecx+330h]
mov     ecx, [eax]
call    dword ptr [ecx+1Ch]
lea     edx, [ebp+var_44]
push    edx
```

شکل ۲ - تزریق کد روی فایل LoginUnit.Cpp

کار این کد اجرای فایلی به نام SetSQLCodePage.exe به صورت مخفی و بدون نمایش پنجره برنامه می باشد.
فایل reboot.bat را در کل سیستم جست‌وجو می‌کند و دستور زیر را در آن می نویسد:

sqlmsde\setup\Install.exe

سپس در مسیری که reboot.bat را پیدا کرده به دنبال مسیر sqlmsde\setup می‌گردد و فایل خود را با نام Install.exe در مسیر ذکر شده کپی می‌کند.
همچنین به دنبال فایل SetSQLCodePage.exe در کل سیستم می‌گردد و فایل خود را به جای آن قرار می‌دهد. از جمله فعالیت‌های دیگر این بدافزار می‌توان به مواردی از جمله کپی خود به usbها با نام DATA.exe و قرار دادن رونوشتی از خود با نام lssas.exe (هم نام با یکی از فرآیندهای اصلی ویندوز برای تشخیص داده نشدن) در مسیر C:\Windows\System32 و سپس ساخت value ای به نام LssaShellEx در مسیر HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run در رجیستری برای اجرا در هنگام بالا آمدن ویندوز اشاره کرد .
به دلیل آشنایی دقیق نویسنده بدافزار با کد ها و نام فایل‌های سورس برنامه مالیران و همچنین نام این بدافزار (narilam) می‌توان حدس زد که این بدافزار توسط یک کارمند ناراضی که دسترسی به کد برنامه داشته است و یا با احتمال کمتری توسط شرکتی رقیب، نوشته شده است.

کشف گروه هکرهای بازی های آنلاین توسط شرکت کسپرسکی

آزمایشگاه شرکت کسپرسکی گروهی از مهاجمان سایبری فعال را که در حدود ۴ سال گذشته به سرورهای توسعه دهندگان و توزیع کنندگان بازی ها به منظور دسترسی به سورس کد بازی ها نفوذ کرده بودند، شناسایی نمود.
شرکت کسپرسکی توانست گروهی با نام " Winnti" را که به ۳۵ سرور مربوط به توسعه دهندگان و توزیع‌کنندگان بازی ها نفوذ نموده بودند، شناسایی نماید. این شرکت اعلام کرده که شواهد کشف شده نشان می‌دهد این گروه به‌منظور توسعه نسخه پولی بازی ها اقدام به سرقت کدهای منبع اختصاصی نموده اند.
اکثر اهداف این گروه در جنوب شرق آسیا و همچنین ژاپن، چین و کره جنوبی بوده است. هرچند که شرکت هایی در آمریکا، آلمان، روسیه، برزیل، پرو و بلاروس نیز مورد حمله قرار گرفته اند.
به گفته شرکت کسپرسکی هنوز میزان مشخصی از آسیب وارد شده توسط این گروه مشخص نشده است. اما این گروه توانسته است گواهینامه های دیجیتالی را که در دیگر حملات به کار می رود، به سرقت ببرد.
آزمایشگاه کسپرسکی برای اولین بار Winnti را در سال ۲۰۱۱، زمانی که بدافزار بر روی کامپیوترهایی که متعلق به بازیکنان یک بازی آنلاین بود، کشف نمودند و این بدافزارها از روی سرور ناشر بازی به روز رسانی می شد.
مهاجمان، بدافزار تروجان را به منظور اعطای دسترسی پنهانی بر روی سرورهای شرکت ها استفاده می‌کردند. پس از بررسی دقیق تر، مشخص شد این گروه از روش های مشابهی علیه ناشران دیگر بازی ها به کار می‌گرفتند.

هک کاربران فیسبوک از طریق چت

حمله Stored Cross-Site Scripting (XSS) یکی از خطرناک ترین حملات Cross-Site Scripting می باشد. در این حمله، کدهای تزریق شده به برنامه کاربردی وب در سرورهای هدف، همچون پایگاه داده، فروم، فیلدهای یادداشت گذاری و.. ذخیره می‌گردد.
۱- Stored XSS در چت فیسبوک: این آسیب پذیری می‌تواند به منظور حملاتی بر روی مرورگر، همچون ربودن اطلاعات مرورگر کاربر، ضبط اطلاعات حساس مشاهده شده توسط کاربران، کدهای مخرب اجرا شده توسط مرورگر کاربر و... استفاده گردد.
زمانی که کاربر پیغام جدیدی در فیسبوک اجرا می‌نماید ، رابط کاربری گرافیکی برای آن پست نشان داده می‌شود. این رابط کاربری به منظور نمایش لینک پست با استفاده از پارامتر [attachment[params][urlInfo][final]، attachment[params][title] ، که توسط فیسبوک فیلتر نشده است استفاده می‌گردد.
۲- Stored XSS در قسمت check-in فیسبوک: آسیب پذیری دیگری که گزارش شده است در صفحه check-in فیسبوک می باشد. به منظور استفاده از این آسیب پذیری مهاجم ابتدا باید مکانی جدید در داخل صفحات فیسبوک ایجاد نماید و سپس، تنظیمات این محل جدید را تغییر دهد. زمانیکه قربانی به مکانی که مهاجم در آنجا قرار دارد می رود، Stored XSS در طرف کاربر اجرا خواهد شد.
۳- Stored XSS در مسنجر فیسبوک: ضعف دیگری که در فیسبوک وجود دارد، تزریق payloadهای Stored XSS در مسنجر فیسبوک می باشد. زمانی‌که که قربانی به حساب کاربری خود در مسنجر وارد شود، کد Stored XSS اجرا می‌گردد.

دانلود بیش از ۹میلیون بار بدافزار "BadNews" اندروید

شرکت امنیتی Lookout ، بدافزار جدیدی در Google play به نام BadNews کشف نموده که تاکنون بیش از ۹میلیون بار دانلود شده است.
این بدافزار در ۳۲ برنامه کاربردی که مربوط به ۴ شرکت مختلف می باشد در Google play کشف گردیده است که به شرکت گوگل اطلاع رسانی شده و این شرکت این برنامه ها را حذف نموده است.
این بدافزار قادر به ارسال پیام های خبری جعلی، و تشویق کاربران به نصب برنامه های کاربردی و ارسال اطلاعات حساس همچون شماره تلفن و شناسه کاربری دستگاه به سرور کنترل (C&C) می باشد. نام یکی از برنامه های کاربردی که دارای این بدافزار می باشد AlphaSMS است.
شرکت Lookout تلاش نموده است سرورهای C&C که در سه کشور مختلف شناسایی شده اند از کار بیاندازد.

پیوستن گوگل به نهضت FIDO به منظور جایگزینی کلمه های عبور

به منظور جلوگیری از انتخاب رمزهای عبور ضعیف، گروه FIDO قصد دارد که از روش های جایگزینی جهت احراز هویت در زمان وارد شدن به وب سایت ها و حساب های کاربری آنلاین استفاده نماید.
کنسرسیوم FIDO در حال توسعه استانداردی به منظور شناسایی کاربر در زمان اتصال به وب سایت ها و حساب های کاربری آنلاین می باشد. این گروه مشخصاتی را که از تکنولوژی های احراز هویت بسیاری همچون اسکن اثر انگشت، صدا و شناسایی بر اساس صورت پشتیبانی می نماید، پیشنهاد نموده است.
مدیر تیم امنیت گوگل بیان نموده است که پیوستن به اتحاد FIDO روشی مناسب به منظور افزایش احراز هویت می باشد.
لازم به ذکر است که امروزه آسیب پذیری های زیادی به دلیل استفاده از رمزهای عبور ضعیف وجود دارد که با کنار گذاشتن این روش و استفاده از روش های احراز هویت مناسب تر این آسیب پذیری ها کاهش می یابد.

دستگیری فرد مظنون به انجام بزرگترین حمله سایبری

فرد هلندی که مظنون به انجام بزرگترین حمله DDOS است توسط پلیس اسپانیا دستگیر شد. طی گزارش های منتشر شده این فرد با استفاده از یک ماشین وَن که مجهز به آنتن های مختلف به منظور اسکن فرکانس ها بوده، موفق به نفوذ به شبکه کشور و انجام این حمله شده است.
این مهاجم در گذشته ارائه دهنده خدمات اینترنت CB۳ROB و شرکت میزبانی وب CyberBunker بوده است. وی به دست داشتن در راه اندازی حمله DDos، ۳۰۰Gbps، برعلیه آنتی اسپم شرکت Spamhaus که منجر به کند شدن و از کار افتادن وب سایت این شرکت شده ، متهم گردیده است. براساس گزارش های مطرح شده، این حمله به صورت تکنیکی به نام DNS reflection صورت گرفته است. هرچند که این مهاجم، ادعاهای مطرح شده را رد نموده است اما پلیس شواهدی کافی علیه وی در اختیار دارد.

باقی ماندن حملات بر روی برنامه کاربردی جاوا

طبق گزارش های منتشر شده از سوی شرکت Websense در حدود ۹۴درصد از برنامه هایی که جاوا را اجرا می نمایند دارای حداقل یک آسیب پذیری قابل بهره برداری می باشند.
بر اساس تحقیقات صورت گرفته در Websense، اینها فقط حملات 0-day (روز صفر) نیستند که به عنوانی تهدیدی مداوم و همیشگی باقی مانده اند؛ بلکه آسیب پذیری های قابل بهره برداری جاوا تبدیل به ابزاری برای مجرمان سایبری گردیده است.
با وجود آسیب پذیری هایی موجود، به روز نگه داشتن مرورگرها می تواند مسئله ای اساسی باشد- به خصوص این که جاوا مستقل از مرورگر به روز رسانی می گردد و مدیریت آن نیز دشوار می باشد.
لازم به ذکر است که تیم امنیت شرکت Websense، از موتورهای طبقه بندی پیشرفته (ACE) و شبکه جستجوگر تهدید به منظور شناسایی و تجزیه و تحلیل اینکه کدام یک از نسخه های جاوا در حال حاضر در حال استفاده می باشد، استفاده نموده اند.
محققان دریافتند که آخرین نسخه جاوا، ورژن ۱،۷،۱۷، فقط توسط ۵٪ از کاربران استفاده می گردد و اکثر نسخه های دیگر ماهها و یا سالها بروز رسانی نشده است- که این امر اولین گام در بهره برداری می باشد.
نسخه ای که اکنون به طور گسترده استفاده می گردد نسخه ۱،۶،۱۶ می باشد که در حدود بالای ۷۵٪ از مرورگرهایی که از نسخه های جاوا استفاده می کنند حداقل ۶ماه است که استفاده می گردد، در حالی که در حدود ۲/۳ از آنها بیشتر از ۱سال به روز رسانی نشده اند.
با این حال، محققان اعلام کرده اند که میزان آسیب پذیری مرورگرها در حدود ۹۳،۷۷٪ می باشد.

آزمون نفوذپذیری

بخش دوم

در نسخه قبل مقدمه‌ای از آزمون نفوذپذیری، روش‌های اجرای این آزمون و فازهای این فرآیند بیان گردید. در این مقاله به توضیح اولین فاز یعنی برنامه ریزی پرداخته خواهد شد.

فاز برنامه ریزی:

به منظور اجرای آزمون نفوذپذیری موفق، آماده‌سازی جهت انجام این فرآیند ضروری می‌باشد. بدین منظور جلسه ای باید مابین سازمان و آزمون کنندگان برقرار گردد. در این جلسه در مورد مواردی همچون دامنه و مواردی که سازمان خواستار اجرای تست بر روی آن‌ها می‌باشد بحث می‌گردد. این جلسه بدین منظور می‌باشد که یک هدف مشخص برای آزمون کننده مشخص گردد. در اکثر موارد هدف از اجرای آزمون نفوذپذیری مشخص نمودن آسیب پذیری‌های قابل بهره‌برداری موجود در شبکه کامپیوتری و یا وب سایت سازمان می‌باشد. دامنه آزمون نفوذ شامل شناسایی ساختار شبکه کامپیوتری و یا وب سایت سازمان، میزان نفوذ به هدف می‌باشد.

این فاز معمولا شامل تمامی فعالیت هایی است که می‌بایست پیش از آغاز آزمون واقعی صورت پذیرد.

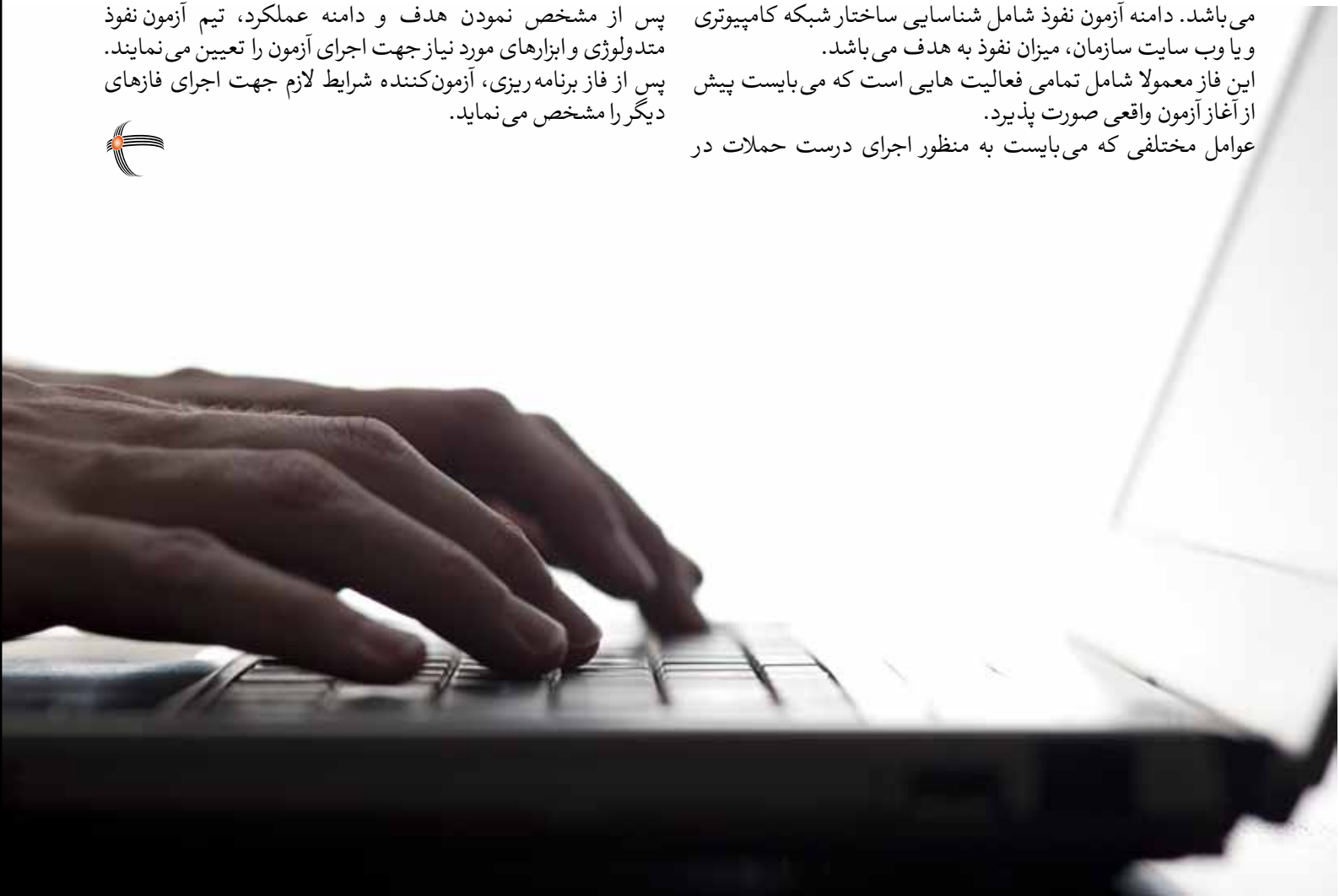
عوامل مختلفی که می‌بایست به منظور اجرای درست حملات در نظر گرفته شود، وجود دارد. بر خلاف هکرها، آزمون‌کننده دارای محدودیت‌های بسیاری در زمان اجرای آزمون نفوذ می‌باشد. بنابراین وجود برنامه‌ای مناسب به منظور اجرای آزمون نفوذی موفق نیازمند است.

محدودیت هایی که وجود دارد به شرح زیر می‌باشد:

- زمان: در شرایط واقعی، یک هکر دارای زمان کافی جهت طرح حمله خود می‌باشد. اما برای یک آزمون کننده محدودیت زمانی وجود دارد. وی می‌بایست در مدت زمان تعیین شده آزمون را انجام دهد و همچنین باید به عواملی مانند ساعات کاری سازمان هدف توجه نماید.
- محدودیت‌های قانونی: آزمون کننده توسط یک قرارداد قانونی، که در آن تمامی موارد قابل قبول و غیرقابل قبول که ممکن است بر روی کسب و کار سازمان هدف تأثیرگذار باشد، محدود گردیده است.

پس از مشخص نمودن هدف و دامنه عملکرد، تیم آزمون نفوذ متدولوژی و ابزارهای مورد نیاز جهت اجرای آزمون را تعیین می‌نمایند.

پس از فاز برنامه ریزی، آزمون‌کننده شرایط لازم جهت اجرای فازهای دیگر را مشخص می‌نماید.



شرکت نرم افزاری

امن پرداز

آدرس: تهران، میدان ونک، خیابان شهید خدامی، پلاک ۳۰ ، طبقه ٤، واحد ۷
تلفن: ۸۸۷۷۳۷٦۸ و ۵-۸۸٦٦۳٦۱۳ فکس: ۸۸۷۹۷۱۷۰
www.amnpardaz.com
info@amnpardaz.com