امنیت اطلاعات

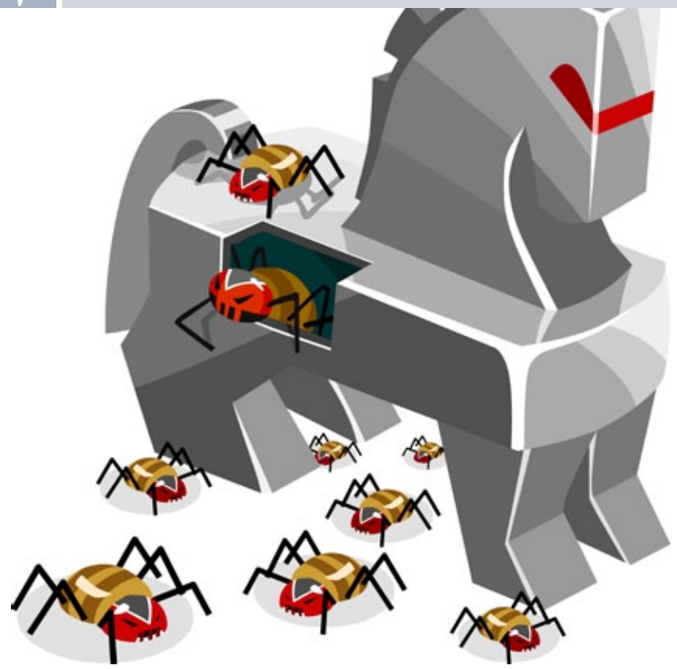
بولتن تحلیلی ■ شماره یک ■ اسفند ۱۳۹۱

شرکت نرم افزاری
امن پرداز

یادداشت

امنیت مفهومی آشنا و کاملا حیاتی برای نوع بشر است. در دوره‌های تاریخی گذشته این موضوع صرفا مفهومی فیزیکی تلقی می شد اما با گذشت زمان و شکل گیری جوامع متمدن، گستره وسیع‌تری یافت بگونه‌ای که حوزه‌های اقتصاد، بازرگانی، سیاست، حکومت، جامعه و بسیاری حوزه های دیگر را در برگرفت. جهان در دهه های اخیر شاهد تحولات چشمگیری در حوزه های فناوری بخصوص فناوری اطلاعات و ارتباطات بوده است و این تحولات عملا زندگی فردی و اجتماعی بشر را دگرگون ساخته و وابستگی کلانی را ایجاد نموده است. شکی نیست که ورود به این حوزه یعنی ورود به فضای مجازی الزامات و تبعات فراوانی به همراه داشته که از مهمترین آنها می‌توان به مفهوم نوین امنیت یعنی امنیت مجازی یا امنیت در فضای سایبری اشاره نمود.امروزه دیگر شکی نیست که اطمینان از ایمن بودن ساختارهای اطلاعاتی و تجهیزات زیرساخت فناوری اطلاعات در سازمان ها، کلید فرصت های پیش رو محسوب می شوند.

برقراری و حفظ امنیت در فضای مجازی نیازمند تحلیل و بررسی بسیار است. رویدادهای اخیر که خبر آنها از اقصی نقاط جهان بگوش می رسد حاکی از گسترش حملات و ناامنی‌های سایبری در مراکز تجاری، صنعتی و یا حتی دولتی است و بی شک نیازمند کسب آگاهی است و برنامه ریزی برای مقابله با انواع تهدیدات و حملات را می طلبد. از این رو تیم تحقیق شرکت نرم‌افزاری امن‌پرداز با رویکرد افزایش آگاهی از مفاهیم امنیت در فضای مجازی اقدام به انتشار این خبرنامه کرده است و امید است با انتشار دانش و آگاهی سهمی هر چند اندک در ارتقا سطح زیرساخت‌های فناوری کشورمان کسب نماییم.



بدافزارها

یک نرم افزار بر اساس نیت خالق آن به عنوان یک بدافزار شناخته نمی‌شود بلکه بر اساس فعالیت‌ها و کارایی های نرم افزار است که در زمره بد افزارها قرار می‌گیرد.

بدافزارها برنامه‌های رایانه‌ای مخربی هستند که برای اهداف خاصی از جمله سرقت اطلاعات، دسترسی به سیستم های کاربران، از کاراندازی خدمات و ... طراحی و تولید شده و در نتیجه عملکرد آن ها خسارات مادی و معنوی فراوانی برای کاربران و سیستم های رایانه ای به ارمغان می‌آورد. بد افزارها مطابق با دسته بندی زیر از هم تمییز داده می شوند:

- جاسوس‌افزارها (Spyware)
- برنامه‌های تبلیغاتی (Adware)
- جک‌ها (Joke)
- شوخی‌های فریب‌آمیز (Hoax)
- شماره‌گیرها (Dialer)
- بارگیری کننده ها (Downloader)
- کلیک کننده‌ها (Ad clicker)
- درب های پشتی (Backdoor)
- پسورد دزدها (Password-Stealer)
- Exploit
- ثبت کننده وقایع (Key logger)

انواع بدافزار

از انواع بدافزارها می‌توان به ویروس‌ها، کرم‌ها، تروجان ها، روت‌کیت‌ها و.... اشاره نمود.

بد افزارهای مسری: ویروس‌ها و کرم‌ها

- ویروس کامپیوتری: به برنامه‌ای اطلاق می‌شود که نرم افزار قابل اجرایی را آلوده کرده و هنگامی که اجرا می‌گردد سبب شود که ویروس به فایل‌های قابل اجرای دیگر نیز منتقل شود.
- کرم کامپیوتری: برنامه‌ای است که بطور فعالانه خود را روی یک شبکه منتقل می‌کند تا رایانه‌های دیگر را نیز آلوده سازد.

مخفی کارها: تروجان ها، روتکیت‌ها و درهای پشتی ها

- تروجان : برنامه‌ای است که کاربر را تشویق به اجرا می‌کند در حالی که دارای قابلیت خرابکارانه است و این قابلیت را مخفی می‌کند که می‌توانند منجر به آثار نامطلوب فراوانی گردند. از جمله حذف فایل‌های کاربر یا نصب نرم افزارهای خرابکار یا نامطلوب بیشتر

یکی از مرسوم ترین راه‌هایی که جاسوس افزارها توزیع می شوند، از طریق یک تروجان که به عنوان یک قطعه از یک نرم افزار مطلوب که کاربر آن را از اینترنت دانلود می‌کند، است. وقتی که کاربر نرم افزار را نصب می‌کند جاسوس افزار نیز در کنارش نصب می‌شود.

- روتکیت ها : بدافزارهایی هستند که به خودی خود نمی‌توان آنها را مخرب یا خطرناک دانست، بلکه قرار گرفتن آنها در کنار ویروس‌ها یا کرم‌های اینترنتی یا نوع استفاده از آن‌هاست که به آنان ماهیتی خطرناک می‌بخشد. روتکیت نرم‌افزاری است که بوسیله آن این امکان وجود دارد تا فایل، پروسه یا .... را پنهان نمود. روت‌کیت‌ها اغلب در سطح سیستم‌عامل فعالیت کرده و با تغییراتی که در سیستم‌عامل یا منابع آن انجام می‌دهند.

به علت قابلیت پنهان‌سازی قوی اینگونه برنامه‌ها، شناسایی آن‌ها یا برنامه‌هایی که توسط آنها پنهان گردیده اغلب مشکل بوده و این امر می‌تواند مشکلاتی را برای کاربران بوجود آورد

- درهای پشتی: ابزارهایی برای نفوذگران هستند که به وسیله آنها می‌توانند سیستم‌های دیگر را در کنترل خود درآورند.درهای پشتی درون شبکه، پورت‌های TCP یا UDP را باز می‌کنند و شروع به گوش کردن نموده تا دستورات نفوذگرها را اجرا کنند.

تا اینجا مفاهیمی کلی از مهمترین بدافزارها ذکر گردید.

در شماره های بعدی جدیدترین بدافزارها معرفی گردیده و اثرات ناشی از آنها ، تحلیلی اجمالی هر یک از آنها و راههای مقابله بیان می‌گردد.

مدیریت امنیت اطلاعات

نیاز روزافزون به استفاده از فناوریهای نوین در عرصه فناوری اطلاعات و ارتباطات، ضرورت استقرار یك نظام مدیریتی را بیش از پیش آشکار می‌نماید . در این گفتار توضیحی اجمالی بر موضوع مدیریت امنیت اطلاعات و ارتباطات و مفاهیم اولیه آن داده خواهد شد.
امنیت اطلاعات به حفاظت از اطلاعات و سیستم‌های اطلاعاتی در مقابل فعالیت‌های غیرمجاز اطلاق می‌شود. این فعالیت‌ها عبارتند از: دسترسی و استفاده غیرمجاز، افشای اطلاعات بدون مجوز، تخریب، تغییر و یا جعل اطلاعات.
در بسیاری از مواقع امنیت اطلاعات در سامانه های رایانه ای تضمین کننده امنیت ملی یك کشور نیز می باشد. حفاظت از اطلاعات محرمانه یک نیاز تجاری و قانونی است که تاثیر معناداری بر حریم خصوصی دارد. در این نوشتار با مفاهیم امنیت اطلاعات آشنا خواهیم شد.

فراهم نمودن امنیت یک فرآیند همیشگی است

مفاهیم پایه

امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها اشاره دارد. در ادامه با مفاهیم سه گانه «محرمانگی»، «یکپارچگی» و «قابل دسترس بودن» آشنا خواهیم شد.

محرمانگی

محرمانگی به معنای جلوگیری از دسترسی افراد غیر مجاز به اطلاعات طبقه بندی شده و افشای اطلاعات توسط افراد غیر مجاز است. به عنوان مثال، برای خرید از بستر اینترنت، کاربر می بایست اطلاعاتی از قبیل شماره کارت، رمزدوم، تاریخ انقضا و عدد تایید کارت (CVV) را از طریق سامانه فروشنده در اختیار بانك عامل جهت پردازش قرار دهد. در این مورد شماره کارت و دیگر اطلاعات مربوط به کارت اعتباری خریدار می بایست محرمانه باقی بماند. حال، اگر فردی به صورت غیر مجاز به این اطلاعات دست یابد، منجر به نقض محرمانگی شده است که می‌تواند منجر به سرقت های مالی از طریق سیستم های بانکداری گردد.

یکپارچگی

یکپارچه بودن به معنای جلوگیری از تغییر در داده‌ها بصورت غیرمجاز و تشخیص به هنگام تغییر در صورت دستکاری غیر مجاز می باشد. یکپارچگی زمانی نقض می‌شود که اطلاعات در حین انتقال بصورت غیرمجاز تغییر داده شود، مانند حملات مرد میانی . سیستم‌های امنیت اطلاعات به طور معمول علاوه بر محرمانه بودن اطلاعات، یکپارچگی آنرا نیز تضمین می‌کنند.

قابل دسترس بودن

قابل دسترس بودن به معنای امکان دسترسی به اطلاعات توسط افراد مجاز می باشد بدین معنی که می بایست از درست کارکردن و جلوگیری از اخلال در سیستم‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات، اطمینان حاصل نمود. یک از راههای از دسترس خارج کردن اطلاعات و سیستم اطلاعاتی درخواست بیش از حد معمول خدمات از سیستم اطلاعاتی است که در این حالت چون سیستم توانایی و ظرفیت چنین حجم انبوده خدمات دهی را ندارد از سرویس دادن بطور کامل یا جزیی عاجز می‌ماند. به این سبك از حملات، حملات تکذیب سرویس گفته می شود.
در این نوشتار به مفهوم امنیت اشاره گردید. در شماره های بعدی به بررسی امنیت اطلاعات از دیدگاه مدیران ارشد و همچنین مسائل مرتبط با سیستم مدیریت امنیت اطلاعات مانند آشنایی با انواع استانداردهای موجود در این زمینه، لازمه ی پیاده سازی آنها و ..... صحبت خواهد شد.

1. Card Verification Value (CVV)
2. Man in the Middle
3. Denial Of Service (DOS)

جنگ سایبری

نگاهی به مهمترین حملات سایبری در جهان

نبـــرد مجازی، یا جنگ سایبـــــری،به نوعی از نبرد اطلاق میگردد که طرفین جنگ در آن از رایانه و شبکه های رایانه ای به عنوان ابزار استفاده می کنند جنگ اطلاعاتی با انقلاب اطلاعات ظهور پیدا کرده است. این انقلاب به دلیل دامنه وسیع و تاثیرات گسترده آن می تواند سبک نوینی از جنگ را ارائه بدهد

انواع حملات

شنود یا Interception
در این روش نفوذگر به شکل مخفیانه از اطلاعات نسخه برداری می کند

تغییر اطلاعات یا Modification
در این روش نفوذگر به دستکاری و تغییر اطلاعات می پردازد

افزودن اطلاعات یا Fabrication
در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می کند

وقفه Interruption
در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می شود

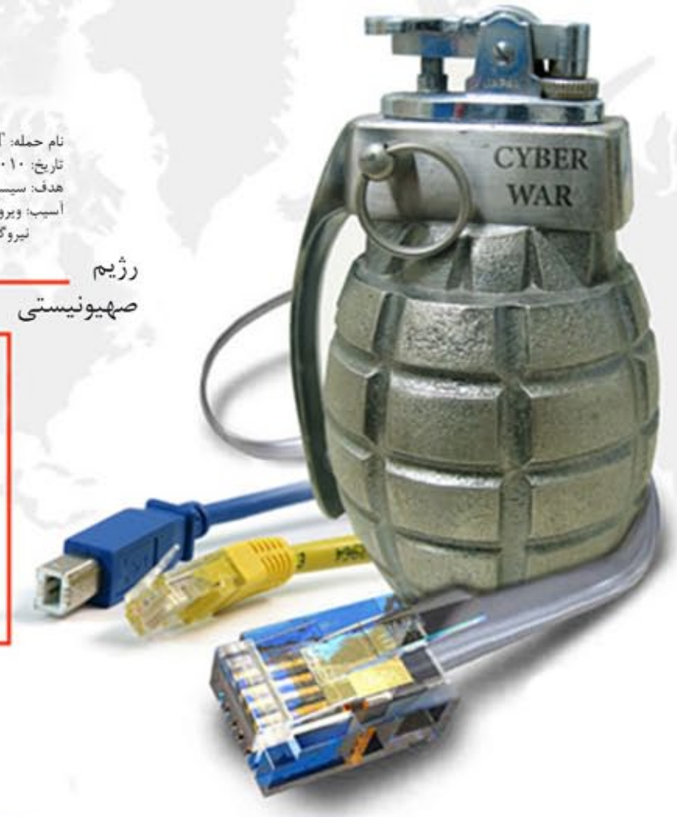
انواع نفوذگران

White hat hackers
هکرهای کلاه سفید یا هکر خوب، متخصصین شبکه هستند که چاله های امنیتی شبکه را پیدا می کنند

Black hat hackers
هکرهای کلاه سیاه اشخاصی هستند که با وارد شدن به شبکه و دستبرد اطلاعات یا جاسوسی کردن، سوء استفاده می کنند

Grey hat hackers
هکرهای کلاه خاکستری حد وسط دو تعریف بالا می باشند

Pink hat hackers
هکرهای کلاه صورتی افراد کم سوادی هستند که با چند نرم افزار خرابکارانه به آزار و اذیت دیگران می پردازند



ایران
نام حمله: STUXNET
تاریخ: ۲۰۱۰-۲۰۰۹
هدف: سیستم های صنعتی
آسیب: ویروسی شدن چند رایانه، اختلال در فعالیت نیروگاه هسته ای

رژیم صهیونیستی

گرجستان
علت: جنگ اوستیای جنوبی
تاریخ: ۲۰۰۸
آسیب: وب سایت دولت گرجستان برای چندین ساعت غیر فعال شد

استونی
علت: یادبود جنگ شوروی و انتخاب تالین به عنوان پایتخت
تاریخ: ۲۰۰۷
آسیب: وب سایت دولت، بانک ها و روزنامه ها برای چندین ساعت غیر فعال شد

روسیه

امریکا
نام حمله: AURORA
تاریخ: ۲۰۰۹
هدف: فعالان حقوق بشر چینی، پایگاه فناوری مستقر در آمریکا
آسیب: سرقت رمز عبور کاربران گوگل به خطر افتادن ایمیل فعالان

نام حمله: BYZANTINECANDOR
تاریخ: ۲۰۰۲
هدف: نیروهای نظامی و سازمان های دولتی امریکا
آسیب: سرقت بخش زیادی از اطلاعات حساس

چین

هند
نام حمله: GHOSTNET
تاریخ: ۲۰۰۹-۲۰۰۷
هدف: سفارتخانه های بسیاری از کشورها نظیر امریکا، دفتر تبعیدیان تبت
آسیب: نامعلوم، نفوذ به رایانه کاربران

نام حمله: Shadow in the cloud
تاریخ: ۲۰۰۹-۲۰۱۰
هدف: دفاتر دولتی هند و تبت، دفتر سازمان ملل
آسیب: تبعیدیان تبت و مکاتبات محرمانه دولت هند به خطر افتاد

نام حمله: WIKILEAKS TAKE DOWN
تاریخ: ۲۰۱۰
علت: انتشار اسناد محرمانه
آسیب: قطعی مکرر سایت غیر فعال کردن دامنه سایت

حمایت دولتی: دور از ذهن، بعید، پذیرفتنی، محتمل، قطعی
توانمندی: کم، متوسط، زیاد

منبع : NewScientist

www.infographics.ir

تست نفوذپذیری

با توجه به گسترش فناوری اطلاعات و افزایش روز افزون استفاده از سیستم های رایانه ای و همچنین افزایش مبادلات از طریق بستر شبکه های رایانه ای، لزوم توجه به مسائل امنیتی بیش از پیش احساس می شود. ایجاد بستر امن انتقال اطلاعات در شبکه های داخلی درون سازمانی و سیستم های خارجی و همچنین برای کاربران از موارد قابل اهمیت می باشد که نیازمند توجه بسیار زیاد مدیران در این حوزه می باشد. لذا برای ارزیابی کارآیی سیستم های امنیتی پیاده سازی شده، نیازمند اجرای فرآیندی با عنوان آزمون نفوذ پذیری می باشد. در این مقاله نگاهی اجمالی به مفاهیم تست نفوذ و تعاریف مرتبط با آن خواهیم داشت.

آزمون نفوذ پذیری چیست؟

آزمون نفوذ پذیری یك پروسه مجاز، برنامه ریزی شده و سیستماتیك برای به کارگیری آسیب پذیری ها جهت نفوذ به سرور، شبکه و یا منابع برنامه های کاربردی می باشد. در واقع تست نفوذ روشی برای ارزیابی امنیتی یك سیستم یا شبکه کامپیوتری است که از طریق شبی سازی حمله یك نفوذگر صورت می‌گیرد. در این آزمون تمامی مشکلات امنیتی همراه با ارزیابی میزان اهمیت آنها و همچنین پیشنهاد هایی برای کاهش اثر خطرات و یا راه حل های فنی به صاحب سیستم ارائه می‌گردد.

روش های تست- جعبه سیاه در مقابل جعبه سفید

تست نفوذ و یا ارزیابی آسیب پذیری ها از دیدگاه مدیریتی به دو روش اساسی می‌تواند انجام شود. در واقع تست نفوذ می‌تواند به صورت محرمانه (تست جعبه سیاه) و یا به صورت عمومی (تست جعبه سفید) انجام پذیرد.

تفاوت اصلی در این روشها میزان دانش تیم آزمونگر از جزئیات پیاده سازی سیستم های مورد بررسی می باشد. در تست نفوذ به روش جعبه سیاه فرض می شود اعضای تیم تست هیچگونه اطلاعاتی از زیرساخت های سیستم ها ندارند و لذا ابتدا باید گستردگی و توزیع سیستم را یافته و سپس شروع به تحلیل کنند. این مرحله به عنوان مرحله جمع آوری اطلاعات شناخته می‌شود. در نقطه مقابل و در انتهای دیگر طیف، روش جعبه سفید وجود دارد که در آن اطلاعات کامل زیر ساخت، در اختیار تیم تست قرار می‌گیرد. این اطلاعات معمولاً شامل نمودارهای شبکه، کدهای منبع و اطلاعات آدرس دهی IP است. در میان این دو طیف گسترده ای وجود دارد که آن را به عنوان روش جعبه خاکستری می شناسند. آزمون جعبه خاکستری روشی از انجام آزمون نفوذ است که بعضی از موارد را از روش جعبه سیاه و بعضی دیگر را از روش جعبه سفید به ارث برده است.

فرآیند تست نفوذ شامل بخش های زیر می باشد:

- برنامه ریزی
- جمع آوری اطلاعات
- شناسایی آسیب پذیری ها
- ارزیابی آسیب پذیری ها
- کسب دسترسی
- افزایش دسترسی های کسب شده
- بررسی مجدد و عمیق تر سیستم
- انجام حملات خاص
- تهیه گزارش

در شماره های بعدی به بررسی هریک از بخش های فرآیند تست نفوذ به صورت جزئی پرداخته خواهد شد.

آسیب پذیری دسترسی از راه دور root در روترهایی با چیپست های Broadcom

محققان شرکت DefenseCodeآسیب پذیری امنیتی مهمی را کشف نموده اند که به مهاجم غیر مجاز اجازه می دهد که از راه دور کدهای دلخواهی را با دسترسی root در محصولاتی که (UPnP (Universal Plug and Play توسط Broadcom در آنها پیاده سازی گشته است و توسط روترهایی که دارای چیپست Broadcom هستند استفاده گشته است، اجرا نماید.
روترها با آسیب پذیری پشته Broadcom UPnP غالبا بر اساس چیپست Broadcom می باشند. محققان اعلام نمودند که «در حقیقت اجزای میان افزار (firmware) آسیب پذیر یکسانی در حداقل دو محصول Linksys سیسکو استفاده می شود. این محصولات عبارتند از WRT54G3G و WRT310N.
این آسیب پذیری در ماژول های wanipc و wanppp پشته Broadcom UPnP قرار دارد. هرچند سرویس UPnP جهت استفاده در شبکه های محلی در نظر گرفته شده است، اما محققان Rapid7 طی تحقیقاتی متوجه شده اند که در حدود بالای ۸۰ میلیون دستگاه در شبکه اینترنت وجود دارد که به درخواست UPnP پاسخ می دهند که آنها را به حملات از راه دور آسیب پذیر نموده است.
گروه تحقیقاتی DefenseCode لیست کامل روترهایی که دارای این آسیب پذیری می باشند ارائه ننموده است، اما احتمالا محصولات شرکت هایی همچون USRobotic، Netgear، D-Link، Zyxel، TP-Link، Cisco، Asus، Broadcom و ... دارای این آسیب پذیری می باشند.

سرقت ۳۰۰۰ سند محرمانه از سفارت ژاپن توسط بدافزار

وزارت خانه کشور ژاپن آخرین قربانی یک حمله سایبری از طریق یک بدافزار که مظنون به ارسال بیش از ۳۰۰۰ سند محرمانه از وزارت خانه این کشور می باشد، است.
در طی تحقیقات فراوان صورت گرفته، کارشناسان دریافتند که هکرها برای حمله از آسیب پذیری APT در "HTran" استفاده می نمایند. کامپیوترها در وزارت خانه های کشاورزی، جنگلداری و شیلات کشور ژاپن نیز مشکوک به آلوده شدن به این بدافزار می باشند.
HTran یک بازگداننده اتصال ابتدایی است که جهت تغییر ترافیک TCP از یک میزبان به میزبان دیگر طراحی گشته است. لازم به ذکر است که HTran توسط یک هکر مشهور چینی ایجاد گردیده است.
HTran توسط بسیاری از هکرها جهت پنهان نمودن مکان فرماندهیشان و سرورهای کنترل استفاده می‌گردد. دبیرخانه کابینه مرکز امنیت اطلاعات ملی کشور ژاپن یک سال پیش به انتقال مشکوک HTran که در این وزارتخانه رخ داده بود، پی برده بود.
پلیس این کشور مطرح نموده است که: هیچ گروه یا شخصی به عنوان مجرم در این حمله سایبری جدید توسط پلیس شناسایی نشده است. اما پلیس سوالاتی در مورد اینکه چگونه این حمله سایبری شناسایی گشته است و این که آیا اطلاعات حساسی به سرقت رفته است یا خیر از این وزارتخانه مطرح خواهد نمود .

آسیب پذیری جدید در محصول " رمزنگاری دیسک کامل PGP " شرکت سیمانتک

شرکت سیمانتک جهت رمزنگاری تمامی محتواهای موجود در دیسک " رمزنگاری دیسک کامل PGP" را تولید نموده است؛ که این محصول دارای آسیب پذیری می باشد.
براساس گزارش های مطرح شده در ۲۵ دسامبر ۲۰۱۲، درایور کرنل pgpwded.sys که با محصول PGP Desktop سیمانتک توزیع گشته است دارای آسیب پذیری بازنویسی حافظه بوده است که این نسخه از نرم افزار به روز رسانی گردیده است.
هرچند شرکت سیمانتک تایید نموده است که این آسیب پذیری مسئله ای مهم و بالقوه‌ای می باشد، اما در ادامه گفته شده که سوء استفاده از این آسیب پذیری به راحتی امکان پذیر نمی باشد. این آسیب پذیری فقط در سیستم هایی که دارای ویندوز XP و یا ویندوز ۲۰۰۳ هستند وجود دارد. و مهاجم جهت سوء استفاده از این آسیب پذیری نیازمند دسترسی محلی به کامپیوتر آسیب پذیر می باشد.
لازم به ذکر است که مهندسین رمزنگاری شرکت سیمانتک با استفاده از مطالبی که فردی با نام Nikita در وبلاگ خود مطرح نموده بود توانستند این موضوع را متوجه گردند. شرکت سیمانتک همچنین اعلام نموده است که :"این آسیب پذیری به مهاجم با سطح دسترسی پایین اجازه می دهد که وی بتواند کدهای دلخواهی را با سطح دسترسی بالا اجرا نماید."

کشف آسیب پذیری در دهها وب سایت نظامی آمریکا از جمله وب سایت پنتاگون توسط مهاجمان

مهاجمی با نام مستعار " ~!White!~" توانست آسیب پذیری های مربوط به حمله تزریق دستورات sql را در دامنه های وب سایتهای پنتاگون، وب سایتهای نظامی و سازمان ملل متحد شناسایی نماید. حمله تزریق Sql یکی از مکانیزم های حمله به وب سایتها می باشد که توسط مهاجمان جهت سرقت اطلاعات از سازمان ها استفاده می گردد.
این مهاجم جزییات بیشتری در مورد یافته های خود در چندین وب سایت مهم، همچون وب سایت دفتر پست پنتاگون، دفتر معاون برنامه های علمی، انجمن نظامی Wiesbaden، NMCI Legacy Applications، انجمن نظامی Darby، وزارت امور اقتصادی و اجتماعی در سازمان ملل متحد و ... را بیان نموده است.
حمله تزریق دستورات sql در مواردی به مهاجم اجازه می‌دهد که اطلاعات مربوط به پایگاه داده مرتبط با وب سایت را مشاهده نماید و یا آنها را از بین برد.
این هکر همچنین بیان نموده است که توانسته پایگاه داده Pentagon.mil و چندین وب سایت ذکر شده را هک نماید.

نقاط ضعف جدی در پروتکل امنیتی مورد استفاده در بانکداری های آنلاین و فیسبوک

بر اساس تحقیقات محققان در دانشگاه رویال، پروتکلی که در بانکداری آنلاین و فیس بوک جهت ایجاد امنیت استفاده می‌گردد دارای ضعف های امنیتی جدی می باشد.
پروتکل (TLS (Transport Layer Security توسط میلیون ها نفر روزانه در سراسر دنیا استفاده می‌گردد. این پروتکل برای بانکداری آنلاین مانند داده های مربوط به کارت های عابر بانک که در هنگام خرید های آنلاین استفاده می‌گردد، امنیت ایجاد می نماید. همچنین، بسیاری از شرکت هایی که خدمات پست الکترونیک ارائه می دهند مانند گوگل و شرکت های دیگر همانند فیس بوک از این پروتکل استفاده می نمایند.
محققان دانشگاه رویال متوجه شدند که می توان حمله "مرد میانی" را بر علیه این پروتکل به کار برد و اطلاعات حساس شخصی را تغییر داد. آنها همچنین ضعفی مرتبط با Sessio های این پروتکل را پیدا نمودند.
این محققان همچنین اذعان نمودند که آنها هم اکنون با چندین شرکت بزرگ مانند Oracle، Google و OpenSSL جهت تست و آزمایش این حمله و پیاده سازی روش هایی جهت مقابله با آن در حال همکاری می باشند.

معرفی ابزار

یکی از حوزه هایی که در انواع صنایع غیر قابل چشم پوشی است، حوزه ابزارها و نرم افزارهای موجود در آن صنعت خاص است. با پیشرفت تکنولوژی، نرم افزارها وابزارهای گوناگونی جهت تسهیل انجام امور، ایجاد گردیده است. حوزه ی امنیت اطلاعات مانند دیگر حوزه ها دارای ابزارهای مختلفی است که هریک برای رفع نیاز خاصی بوجود آمده است.
در زیر تقسیم بندی نرم افزارهای موجود در حوزه امنیت اطلاعات مطرح گردیده است:

ابزارهای مورد استفاده در حوزه تست نفوذپذیری
- پویشگر
  - o پویشگر شبکه داخلی
  - o پویشگر برنامه های کاربردی تحت وب
- نفوذکننده
  - o نفوذ کننده برنامه های کاربردی تحت وب
  - o نفوذ کننده برنامه های رومیزی
  - o نفوذ کننده سرویس های تحت شبکه

ابزارهای مورد استفاده در حوزه محافظت
- محافظت کننده
  - o فایروال
  - o سیستم های تشخیص نفوذ
- ضد ویروس
- ضد بدافزارها

ابزارهای مورد استفاده در حوزه بدافزار
- تروجان
- روتکیت
- ویروس رایانه‌ای
- کرم رایانه‌ای
- درهای پشتی

در شماره های بعد به بررسی اجمالی هر یک از این ابزارها و انواع مختلف آن ها پرداخته خواهد شد.

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
w w w . a m n p a r d a z . c o m