

حفاظت کامپیوتر قبل از اتصال به اینترنت

تعداد بسیار زیادی از کاربران اینترنت را افرادی تشکیل می‌دهند که

فاقد مهارت‌های خاصی در زمینه فناوری اطلاعات بوده و از امکانات

حمایتی مناسبی نیز برخوردار نمی‌باشند. سیستم‌های اینگونه کاربران

دارای استعداد لازم به منظور انواع تهاجمات بوده و بطور غیر مستقیم

شرایط مناسبی را برای مهاجمان به منظور نیل به اهداف مخرب آنان،

فراهم می‌نمایند.

بر اساس گزارشات متعددی که در چندین ماه اخیر منتشر شده است،

تعداد حملات و آسیب پذیری اینگونه سیستم‌ها، به طرز کاملاً

محسوسی افزایش یافته است. علت این امر را می‌توان در موارد زیر

جستجو نمود:

parsi e-book
WWW.PARSIBOOK.4T.COM

تعداد بسیاری از تنظیمات پیش فرض کامپیوترها، غیر ایمن

می‌باشد. کشف نقاط آسیب پذیر جدید در فاصله بین زمانی که

کامپیوتر تولید و پیکربندی می‌گردد و تنظیماتی که اولین مرتبه توسط

کاربر انجام می‌شود. در مواردی که ارتقای یک نرم افزار از طریق

رسانه‌های ذخیره سازی نظیر CD و یا DVD انجام می‌شود، همواره

این احتمال وجود خواهد داشت که ممکن است نقاط آسیب پذیر

جدیدی نسبت به زمانی که نرم افزار بر روی رسانه مورد نظر مستقر

شده است، کشف شده باشد.

مهاجمان دارای آگاهی لازم در خصوص دامنه‌های آدرس‌های IP از

نوع Dial-up و یا Broadband بوده و آنان را بطور مرتب پویش

می‌نمایند. کرم‌های بسیار زیادی بطور مرتب و پیوسته بر روی اینترنت

در حال فعالیت بوده تا کامپیوترهای آسیب پذیر را شناسایی نمایند. با

توجه به موارد فوق، متوسط زمان لازم به منظور یافتن کامپیوترهای

آسیب پذیر در برخی شبکه‌های کامپیوتر به مرز دقیقه رسیده است .

توصیه‌های استاندارد به کاربران خانگی، Download و نصب Patch

های

نرم افزاری در اسرع وقت و پس از اتصال یک کامپیوتر جدید بر روی

اینترنت است . فرآیند فوق، با توجه به این که مهاجمان به صورت دائم

اقدام به پویش و یافتن قربانیان خود می‌نمایند، ممکن است در موارد

متعددی توام با موفقیت کامل نگردد . به منظور حفاظت کامپیوترها

قبل از اتصال به اینترنت و نصب هر یک از Patch‌های مورد نیاز،

موارد زیر پیشنهاد می‌گردد :

در صورت امکان، کامپیوتر جدید را از طریق یک فایروال شبکه‌ای

(مبتنی بر سخت افزار) و یا روتر فایروال به شبکه متصل نمایید. یک

فایروال شبکه‌ای و یا روتر فایروال، سخت افزاری است که کاربران

می‌توانند آن را بین کامپیوترهای موجود در یک شبکه و دستگاه‌های

Broadband نظیر مودم کابلی و یا DSL نصب نمایند. با بلاک

نمودن امکان دستیابی به کامپیوترهای موجود بر روی یک شبکه محلی

از طریق اینترنت، یک فایروال سخت افزاری قادر به ارائه یک سطح

حفاظتی مناسب برای کاربران در خصوص دریافت و نصب patch های

نرم افزاری ضروری خواهد بود.

در صورتی که قصد اتصال کامپیوتر خود به اینترنت را از طریق یک

فایروال و یا روتری با پتانسیل

NAT:Network Address Translation، داشته باشید و یکی از

موارد زیر درست باشد : الف) ماشین جدید تنها کامپیوتر متصل شده

به شبکه محلی از طریق فایروال است . ب) سایر ماشین های متصل

شده به شبکه محلی پشت فایروال نسبت به نصب patch های مورد

نیاز بهنگام بوده و بر روی آنان گرم ها و یا ویروس هایی وجود نداشته

باشد، ممکن است به وجود یک فایروال نرم افزاری نیاز نباشد. در

صورت امکان، از فایروال نرم افزاری همراه کامپیوتر نیز استفاده

نمایید. در صورتی که سیستم عامل نصب شده بر روی کامپیوتر شما

دارای یک فایروال نرم افزاری از قبل تعبیه شده می باشد، پیشنهاد

می گردد آن را فعال نموده تا امکان اتصال سایرین به شما وجود

نداشته باشد. همانگونه که اشاره گردید، در صورتی که کامپیوتر شما

از طریق یک فایروال به شبکه متصل است و تمامی کامپیوترهای موجود

در شبکه محلی نسبت به نصب هر یک از Patch های مورد نیاز بهنگام

شده می باشند، این مرحله می تواند اختیاری باشد. علیرغم موضوع

فوق، در بخشی از استراتژی «دفاع در عمق» به این موضوع اشاره

شده است که بهتر است فایروال نرم افزاری ارائه شده همراه سیستم

عامل، همواره فعال گردد. در صورتی که سیستم عامل موجود بر روی

کامپیوتر شما دارای یک فایروال نرم افزاری از قبل تعبیه شده

نمی باشد، می توان یک نرم افزار فایروال مناسب را تهیه نمود. پیشنهاد

می‌گردد که اینگونه نرم افزارها از طریق رسانه‌های ذخیره سازی

نظیر CD و یا DVD نصب گردند (در مقابل اتصال به یک شبکه و

دریافت نرم افزار مورد نیاز از یک کامپیوتر حفاظت نشده). در غیر

این صورت همواره این احتمال وجود خواهد داشت که کامپیوتر شما

قبل از اینکه قادر به دریافت و نصب اینچنین نرم افزارهایی گردد،

مورد تهاجم واقع شود.

غیر فعال نمودن سرویس‌های غیرضروری نظیر «اشتراک فایل و

چاپگر»

اکثر سیستم‌های عامل به صورت پیش فرض پتانسیل «اشتراک فایل

و چاپ» را فعال نمی‌نمایند. در صورتی که شما سیستم خود را به یک

سیستم عامل جدید ارتقاء داده اید و کامپیوتر دارای گزینه فعال

«اشتراک فایل و چاپ» می‌باشد، بدیهی است که سیستم عامل جدید

نیز این گزینه را فعال نماید. سیستم عامل جدید ممکن است دارای

نقاط آسیب پذیری باشد که شما آنان را در نسخه قبلی سیستم عامل

مربوطه از طریق نصب تمامی patchهای مورد نیاز، برطرف کرده

باشید و در سیستم عامل جدید این وضعیت وجود ندارد. برای حل

مشکل فوق پیشنهاد می گردد قبل از ارتقای سیستم عامل، پتانسیل

«اشتراک فایل و چاپ» را غیر فعال نموده و در ادامه فرآیند ارتقاء را

انجام دهید. پس از ارتقای سیستم و نصب Patchهای مورد نیاز،

می توان در صورت ضرورت اقدام به فعال نمودن پتانسیل «اشتراک

فایل و چاپ» نمود.

parsi e-book
WWW.PARSIBOOK.4T.COM