یادداشتی درباره وضعیت کنونی امنیت فضای مجازی ایران

# چرا این روزها حال اینترنت خوب نیست و پشت‌سرهم هک می‌شویم؟


اگر پیگیر اخبار فناوری و اینترنت بوده باشید، حتما متوجه شدید در دو ماه اخیر خبرهای افشای اطلاعات و رمزعبور و حساب‌های کاربران، هک سایت‌های ایرانی و از سرویس خارج شدن برخی سرورها و هاست‌ها و خبرهای دیگر از این دست مانند هک تلگرام و اپراتورهای تلفن همراه به طرز چشم‌گیری افزایش یافته است.

از سوی دیگر، اینترنت حال خوبی ندارد و یک روز برخی سایت‌های بزرگ با رتبه‌های زیر صد ایران باز نمی‌شوند و مشکل DNS دارند و فردا سرعت اینترنت کاهش ملموسی دارد و اتفاقاتی نظیر این‌ها که هم برای خواننده‌ها و هم برای مدیران سایت‌ها و سرورها دردسرساز هستند. حتا هر هفته شاهدیم که چند سرویس‌دهنده بزرگ و سراسری اینترنت برای چندین ساعت یا چند روز با اختلال همراه هستند و به مشتریان خود اس‌ام‌اس می‌دهند و عذرخواهی می‌کنند.

این روزها خبرهای این چنینی این قدر زیاد شده که برای بسیاری از ما دارد طبیعی و معمولی می‌شود و دیگر مانند گذشته با واکنش‌های هیجانی و آنی همراه با تعجب و کنجکاوی توام نیست. همین دیروز در جمع چندین تن از بچه‌های خبرنگار آی‌تی گفتم فلان سرورها و فلان سایت‌های معروف مورد حمله DDoS قرار گرفتند اما برای هیچ دوستی خبر جدید و با اهمیتی نبود. اما چرا؟ تا حالا فکر کردید چرا یک‌دفعه حجم خبرهای هک و حمله به سایت‌ها و سرویس‌های ایرانی افزایش یافته است؟

شاید شروع داستان به دو ماه قبل برگردد که اعلام شد یک حمله سراسری به وب‌سایت‌های ایرانی دولتی از خارج از کشور صورت گرفته است و پس از آن شاهد هک چندین سایت بزرگ مانند سایت سازمان آمار ایران بودیم. کمی جلوتر آمدیم و خبر افشای اطلاعات کاربران اپراتور ایرانسل روی کانال‌های تلگرام رسانه‌ای شد و چندین هفته در صدر اخبار ایران بود و شاهد اطلاعیه پشت اطلاعیه از ایرنسل در انکار این خبر و قبول مسئولیت و از سوی دیگر وزارت ارتباطات و دیگر متولیان در تایید خبر بودیم. از گوشه و کنار هم خبرهای مختلفی مانند هک سایت بیمارستان میلاد توسط یک بیمار برای گرفتن نوبت پزشکی روی خط خبرگزاری‌ها می‌آمد. خبر بزرگ و تکان‌دهنده دیگر، هک شماره تلفن ۱۵ میلیون کاربر ایرانی روی نرم‌افزار ارتباطی تلگرام بود که باز هم با تایید و انکار مراجع مختلف از جمله خود شرکت تلگرام همراه بود. در چند روز گذشته نیز شرکت‌های کسپرسکی و سیمانتک خبر از یک حمله سراسری سایبری و خطرناک سازمان یافته برعلیه سرورها و IPهای ایرانی و البته کشورهای دیگری مانند چین، روسیه، سوئد، بلژیک و روآندا دادند و گزارش‌های متقن متعددی از وضعیت ترافیک اینترنت این کشورها منتشر شد. در خلال این خبرها، طی دو هفته گذشته بسیاری از سایت‌های علمی و خبری با حملات DDoS مواجه شده که از چند ساعت تا چندین روز از دسترس خارج شدند. همین‌طور برخی سرورهای شرکت‌های ارایه‌دهنده سرویس‌های میزبانی و هاست مورد حمله قرار گرفتند و به طور کامل از دسترس خارج شدند و در برخی موارد کل سرور فرمت

شده و سایت‌های میزبانی شده روی این سرورها به طور کامل از بین رفتند.

در ادامه سعی می‌کنم مهم‌ترین دلایل افزایش حملات و هک‌ها برعلیه سایت‌ها و سرورهای ایرانی را نام ببرم:

- **جنگ سایبری وارد فاز جدیدی شده است:** سال‌ها است داریم درباره جنگ سایبری و لشکرهای سایبری و تقابل دولت‌ها و گروه‌های هکری در دنیای مجازی صحبت می‌کنیم اما بسیاری از مدیران و تصمیم‌گیرندگان این موضوع را یک احتمال یا پیش‌بینی و حتا توهم و تئوری به حساب آورده و هیچ‌گاه به طور جدی دنبال سازوکارها و اقدامات پیش‌گیرانه و محافظتی نبودند تا به امروز که شاهدیم در گزارش‌های کسپرسکی و سیمانتک به طور صریح و واضح از «حملات سازمان‌یافته» و «گروه های هکری» بر علیه کل زیرساخت اینترنت در سراسر جهان صحبت شده است.

- **ضعف مفرط امنیتی سایت‌ها و سرورها:** چندین گروه در این وضعیت اسف‌بار امنیت سایت‌های ایرانی دخیل هستند. مدیرانی که برای امن‌سازی وب‌سایت سازمان و ارگان‌شان بودجه اختصاص ندادند یا بودجه اختصاص دادند و جای دیگری خرج کردند یا بودجه اختصاص دادند اما یک دهم‌اش را به برنامه‌نویس و توسعه‌دهنده سایت دادند و بقیه‌اش را در جاهای دیگری مصرف می‌کنند. همین‌طور کارشناسان فنی که توانایی امن‌سازی یک شبکه و سایت داخلی سازمان یا شرکت را نداشتند و از اطلاعات به‌روزشده‌ای استفاده نمی‌کنند. همین‌طور باید برخی شرکت‌های طراح سایت را مقصر دانست که از فضای به هم ریخته و نابسامان ایران نهایت سودجویی را برده و روزی ده سایت به این شرکت و آن سازمان تحویل داده در حالی که ساده‌ترین نکات امنیتی و پشتیبان‌گیری را رعایت نکرده و اهمیت ندادند. برخی شرکت‌های سرویس‌دهنده اینترنت و میزبانی سایت هم فقط روی کمیت تمرکز کردند و به دنبال مشتری بیشتر و ارایه سرویس بیشتر و افزایش سرورهای خود هستند بدون اینکه ذره‌ای برای فردای روزی که سرورهای‌شان هک شود؛ برنامه و طرحی داشته باشند.

- **ضعف فرهنگی و آموزشی:** متاسفانه بارها شاهدیم که مدیران رده بالای یک سازمان، ساده‌ترین نکات امنیتی برای حفاظت از اطلاعات سازمانی یا سرویس‌های اینترنتی را نمی‌دانند یا رعایت نمی‌کنند. وقتی یک مدیر درک درستی از مقوله امنیت ندارد؛ طبیعی است که در کل آن سازمان و شرکت، امنیت جدی گرفته نشده و شاهدیم یک مشتری با چندین ساعت کار روی یک سایت، می‌تواند آن را از دسترس خارج کند. در حالی که باید هر سازمان یک تیم امنیتی دایمی و مستقر در سازمان خودش داشته باشد تا مرتبا مسایل امنیتی و نکات ضعف را رصد و گزارش‌گیری و رفع نمایند؛ شاهدیم که بسیاری از سایت‌ها و سرویس‌های اینترنتی بعضا پربازدید و درگیر با خدمات روزانه مردم از یک شرکت پشتیبانی هم بهره نمی‌برند.

- **نبود زیرساخت و شبکه ملی اطلاعات بومی:** چندین سال است پرژوه شبکه ملی اطلاعات کلید خورده اما هنوز شاهد خروجی ملموس و عینی کاربردی از آن نیستیم در حالی که چنین زیرساخت و شبکه‌ای اینترانتی باید بتواند بسیاری از سایت‌ها و سرورهای ایرانی را در خود جای داده و از حملات سایبری خارج از کشور محافظت کند. بسیاری از شرکت‌ها و سایت‌ها به علت نبود سرویس‌های خوب در ایران به سراغ سرورهای ارزان‌قیمت خارجی می‌روند و بعد شاهدیم به راحتی هک شده و از دسترس خارج می‌شوند. یکی از اصول مقابله با جنگ‌های سایبری قدرتمندسازی زیرساخت‌های داخلی و ظرفیت‌سازی برای میزبانی سایت‌ها و سرورهای داخلی است.

- **هزینه‌های بالا:** این مورد یکی از دردناک‌ترین غصه‌های فضای کنونی آی‌تی ایرانی است. سازمان‌های دولتی، شرکت‌های سرویس‌دهنده خدمات هاست و اینترنت، شرکت‌های خدماتی و خصوصی؛ همه و همه یک درد مشترک دارند و آن نبود بودجه و پول برای توسعه زیرساخت آی‌تی است. در نتیجه، از سرورهای پشتیبان‌گیری خبری نیست، فایروال‌ها قدیمی هستند و از کار افتاده‌اند، برای امنیت یک سایت هیچ بودجه‌ای تخصیص داده نمی‌شود و سخت‌افزارها و پلتفرم‌ها همه قدیمی و به‌روزنشده هستند. در حالی که مقوله امنیت یکی از سریع‌ترین حوزه‌های در دنیا شناخته شده که روزانه دارد توسعه پیدا می‌کند؛ باور کنید برخی سایت‌ها و سرورها دارند با نرم‌افزارها و وب‌سرویس‌های ده سال پیش کار می‌کنند و چون هیچ‌وقت کسی به سراغ هک آن‌ها نرفته، تصور می‌کنند امن هستند و نیازی به امن‌سازی و به‌روزرسانی ندارند.

وضعیت اینترنت در ایران نسبت به ده سال گذشته بسیار متفاوت شده است. امروز بخشی عظیمی از تراکنش‌های مالی روی بسترهای شبکه و اینترنت انجام می‌شود و همه بانک‌ها سرویس‌های آنلاین دارند که هریک میلیون‌ها کاربر دارد. سازمان‌های بزرگ دولتی نظیر بیمارستان‌ها، تامین اجتماعی، پلیس، اداره راهنمایی و رانندگی، بیمه‌ها، دانشگاه‌ها و غیره سرویس‌های حضوری خود را روی بستر اینترنت عرضه می‌کنند و میلیون‌ها بازدیدکننده دارند. یک روز و یک ساعت از دسترس خارج شدن یکی از این سرویس‌ها می‌تواند زیان‌های فراوانی به همراه داشته باشد و به همین دلیل است که امنیت هم باید بیشتر مورد توجه قرار گیرد.

امنیت فضای مجازی در ایران همانند یک کلاف درهم‌پیچیده و چند سر است که همه هم در جایگاه مقصر هستند و هم در جایگاه قربانی و برای غفلت از مقوله امنیت ده‌ها دلیل محدودیت‌های مالی، نیروی انسانی و ساختاری را پیش می‌اندازند. آن‌چه که مسلم است، این حملات و فضای تازه به وجود آمده تدام خواهد یافت و شاید هم بیشتر و بیشتر شود، به طوری که آسیب‌های جدی به کل زیرساخت‌های ایران وارد کند. این اتفاق‌های اخیر می‌تواند یک هشدار و تلنگر خوب برای مدیران سایت‌ها، سرورها، شرکت‌های ارایه‌دهنده اینترنت و خدمات هاست باشد.

==========

**شاید به این مقالات هم علاقمند باشید:**


**نکات امنیتی مهم برای کاربران سازمان‌ها**

**راهنمای حذف بدافزارها**

**چگونه ساعت‌های هوشمند را امن کنیم؟**

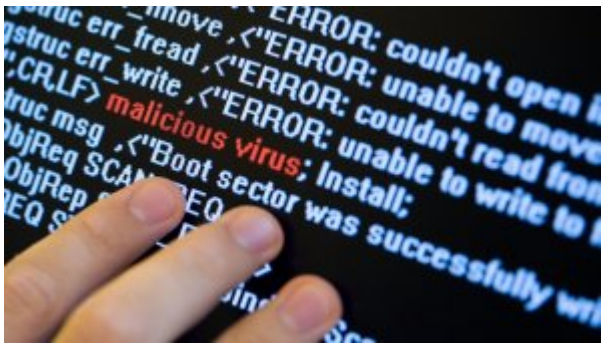

**آموزش ورود به ویندوز 10 با تغییر رمز عبور مدیر سیستم (Admin)**

**9 ترفند برای کنترل فرزندان در ویندوز 10**


**ده اشتباه مرگ‌بار در مدیریت امنیت اطلاعات**

**رمزنگاری اطلاعات بیهوده است؛ شما باز هم هک می‌شوید**

**به این چهار نکته توجه کنید تا هک نشوید!**




**10 علامت آلودگی کامپیوتر به یک بدافزار**

**5 علامت هشداردهنده هک شدن یک برنامه وب**

**تاریخ انتشار:**
20 مرداد 1395

**نشانی منبع:** https://www.shabakeh-mag.com/opinion/4115