# دمپایی ابری!

سوسک‌ها موجودات عجیبی هستند، همه چیز می‌خورند! اگر برای مدت زیادی چیزی نخورند، همچنان زنده می‌مانند. به‌سرعت به هر دارو و سمی مقاوم می‌شوند و آن سم نسبت به آن‌ها بی‌اثر می‌شود. وقتی از تمام راه‌کارهای پیش‌رفته و نوین مقابله ناامید می‌شویم، راه حل نهایی که به ذهن می‌رسد بازگشت به راه‌کار سنتی یعنی دمپایی ابری است!

پیش از این، ویروس‌های کامپیوتری عمده‌ترین خطر برای اطلاعات یک فرد یا سازمان به شمار می‌رفتند. از آن‌جا که به نسبت امروز دستگاه‌های کم‌تری به اینترنت متصل بودند، ویروس‌ها با اهداف خراب‌کاری طراحی و تکثیر می‌شدند. امروزه با گسترش ارتباطات اینترنتی و افزایش پهنای باند ارتباطی، بدافزارها بیش‌تر به سمت اهداف تبلیغاتی، جاسوسی و جمع‌آوری داده متمایل شده‌اند. با پیدایش مفهومی تحت عنوان رایانش ابری، مسائل دیگری نیز در زمینه امنیت اطلاعات و حریم شخصی به موارد قبل اضافه شده است. صرف نظر از امنیت فیزیکی اطلاعات، یکی از مباحثی که در امنیت دسترسی و محرمانگی اطلاعات مطرح است، مکان فیزیکی سرویس‌دهنده‌ای است که اطلاعات یک سازمان در آن ذخیره شده است. ممکن است شرکتی که سرویس ابری را در اختیار ما می‌گذارد، کشوری بی‌طرف یا دوست باشد. از آن‌جا که در زیرساخت‌های ابری ممکن است مکان فیزیکی سرویس‌دهنده‌ها در سراسر دنیا پراکنده باشند، ملیت آن شرکت امنیت اطلاعات را تضمین نخواهد کرد.

به عنوان نمونه، در هر کشور مثل امریکا، حکم قضایی می‌تواند اجازه دسترسی و بررسی اطلاعات را صادر کند و این ممکن است مطلوب یک سازمان ایرانی نباشد. حتی اگر شرکت سرویس‌دهنده وعده رمزنگاری اطلاعات با الگوریتم‌های پیش‌رفته را داده باشد، چیزی که ما در این راستا با آن مواجه هستیم تنها یک توافق‌نامه است که باید به آن اطمینان کنیم و آن را بپذیریم. چه تضمینی وجود دارد که اطلاعات واقعاً رمز می‌شوند یا یک نسخه از اطلاعات رمز نشده در جایی ذخیره نمی‌شود؟

زمانی که نگران دسترسی کاربران دیگر به اطلاعات خود هستیم، راحت‌تر می‌توانیم به ادعای شرکت‌های سرویس‌دهنده اطمینان کنیم. اما زمانی که دسترسی خود شرکت سرویس‌دهنده نیز برای ما اهمیت داشته باشد، دیگر هیچ دلیلی برای استفاده از سرویس‌های خارجی وجود نخواهد داشت و تنها راه‌کار استفاده از سرویس‌های داخلی است. اگر این سرویس‌ها روی سرویس‌دهنده‌هایی باشند که به شبکه ملی اطلاعات متصل هستند و هیچ راهی به بیرون نداشته باشند، خیال ما اندکی راحت‌تر می‌شود. اگر این شبکه به شبکه جهانی اینترنت متصل باشد یا حتی همان شبکه ملی اطلاعات نیز آسیب‌پذیری داشته باشد، دسترسی یک نفوذگر می‌تواند امنیت اطلاعات را به مخاطره بیاندازد. بیایید فرض کنیم امنیت نفوذ در این سرویس‌دهنده‌های داخلی برقرار است و هیچ فرد خارجی توان نفوذ به این سیستم‌ها را ندارد، اما آیا سیستم‌عامل نصب شده روی این سرویس‌دهنده‌ها کاملاً مطمئن است؟ برای نگهداری

عکس‌های خصوصی خانوادگی می‌توان به سیستم‌عامل اطمینان کرد، اما آیا برای اطلاعات استراتژیک یک کشور نیز می‌توان به سیستم‌عامل متن‌بسته‌ای مثل ویندوز اطمینان کرد؟

نه تنها به ویندوز متن‌بسته، بلکه به سیستم‌عامل‌های متن‌باز ساخت خارج نیز نمی‌توان اطمینان کرد. اگر سرویس‌دهنده‌های حساس ما به سیستم‌عامل‌های متن‌باز ساخت داخل مثل لینوکس ملی مجهز باشند و کدهای آن خط به خط از نظر امنیت بررسی شده باشند، خیال ما آسوده‌تر خواهد بود. اما سناریو هنوز به پایان نرسیده است. به این عبارت دقت کنید: «از نظر تئوری هر نرم‌افزار مستقل از میزان پیچیدگی، با استفاده از سخت‌افزار قابل پیاده‌سازی است.» به عنوان نمونه، از نظر تئوری یک نرم‌افزار پیام‌رسان را می‌توان بدون نوشتن حتی یک خط کد برنامه‌نویسی، تنها با استفاده از سیم و ترانزیستور و مدارهای الکترونیکی پیاده‌سازی کرد. اما به دلیل انعطاف‌پذیری کم و هزینه بسیار بالا برای پیاده‌سازی سخت‌افزاری هر برنامه، چنین کاری توجیه ندارد و سخت‌افزارها به شکلی همه‌منظوره طراحی شده‌اند و کاربردهای خاص با استفاده از نرم‌افزار به آن‌ها داده می‌شود. پردازنده اینتل و AMD، کارت گرافیک انویدیا، هارددیسک وسترن‌دیجیتال و بسیاری از برندهای دیگر که قطعات سخت‌افزاری سرویس‌دهنده‌ها را تولید می‌کنند، تحت مدیریت شرکت‌های امریکایی هستند. شاید این شرکت‌ها برای پیاده‌سازی سخت‌افزاری یک برنامه ساده یا حتی پیچیده‌ای که بتواند اطلاعات حساس یک کشور را سرقت کند، انگیزه کافی داشته یا حتی مجاب شده باشند. به دلیل فناوری بالا و پیچیده آن‌ها، هیچ نرم‌افزار یا ابزار عمومی نیز برای سنجش امنیت آن‌ها وجود ندارد.

بنابراین، باید سرویس‌دهنده‌های خود را نیز با سخت‌افزارهایی مجهز کنیم که ابتدا مثل پردازنده‌های ARM معماری باز دارند و دوم ساخت آن‌ها را نیز خود ما در داخل کشور انجام دهیم. برای هارددیسک‌ها و دیگر قطعات سخت‌افزاری نیز به همین ترتیب عمل کنیم. باید توجه داشت یک قطعه سخت‌افزاری مثل هارددیسک با وجود وظیفه معمولی تعریف شده برای آن (ذخیره‌سازی داده)، می‌تواند به خواست شرکت سازنده در پشت صحنه وظایف بی‌ربط به وظیفه اصلی خود (پردازش و ارسال اطلاعات) را نیز انجام دهد. به‌نظر می‌رسد برای رسیدن به فناوری ساخت همه این قطعات با کیفیت مطلوب راه طولانی و پرهزینه‌ای در پیش داریم. پس باید برای مقابله با چنین جاسوس‌های احتمالی، دنبال راه‌کار ساده و سنتی «دمپایی ابری» باشیم! اطلاعات حساس سازمان را در سرویس‌دهنده‌هایی پاکیزه از ویروس قرار دهیم تا از خطر تخریب در امان باشند. سپس هرگونه اتصال آن‌ها به دنیای بیرون را ممنوع کنیم. بعد آن‌ها را در اتاقک‌های سربی با قفل‌های فولادی قرار دهیم! به این ترتیب، هم کسی نمی‌تواند خود دستگاه را سرقت کند، هم احیاناً مدارهای جاسوسی بی‌سیم جاسازی شده در سخت‌افزارهای مختلف نمی‌توانند اطلاعات را به بیرون مخابره کنند. برای اطمینان بیش‌تر نیز در اوقات بیکاری آن را خاموش کنیم و از برق بکشیم!

**تاریخ انتشار:**

25 خرداد 1394

---

**نشانی منبع:** https://www.shabakeh-mag.com/opinion/859