محققان خود را برای تهدیدات عصر کامپیوترهای کوانتومی آماده می‌کنند

مهاجمان کوانتومی: امروز ضبط می‌کنند، سال‌ها بعد رمزگشایی می‌کنند!

از هم‌اکنون باید نگران تهدیدات کامپیوترهای کوانتومی باشیم. چنین کامپیوترهایی قادر هستند با کمک خواص کوانتومی، رمز داده‌های محرمانه را در زمان کوتاهی بشکنند. شاید بسیاری از افراد با این استدلال که « فاصله زیادی تا ساخت چنین کامپیوترهایی داریم »، گمان کنند که در حال حاضر داده‌هایمان از شر کامپیوترهای کوانتومی بدخواه مصون هستند. اما باید به این نکته توجه کنیم که شاید کسی در گوشه‌ای از این جهان مشغول ذخیره کردن داده‌های رمزشده امروز ما باشد و برای شکستن رمز آن‌ها، تا زمان ساخت یک کامپیوتر کوانتومی منتظر بماند. با در نظر گرفتن این احتمال، واضح است که همین حالا هم زمان زیادی را در مقابل مهاجمین کوانتومی از دست داده‌ایم.

انتظار می‌رود که کمتر از ده سال آینده، قادر به ساخت کامپیوترهای کوانتومی باشیم. چنین کامپیوترهایی قادرند با سرعتی بسیار بیشتر از کامپیوترهای فعلی مسائل پیچیده‌ای را حل کنند. البته توان و سرعت بالای پردازشی این کامپیوترها همیشه مفید نیست و بر بخشی از جنبه‌های زندگی آینده از جمله امنیت، تأثیرات منفی خواهد گذاشت. در این صورت است که روش‌هایی نظیر RSA وECC که در حفاظت داده‌ها مورد استفاده قرار می‌گیرند در معرض تهدید خواهند بود. شکستن این دیوارهای دفاعی با استفاده از فناوری‌های فعلی، صدها سال زمان نیاز دارد اما یک کامپیوتر کوانتومی قادر است این کار را نهایتاً در چند روز انجام دهد.

Tanja Lange ، استاد رمزنگاری دانشگاه فناوری آیندهوون (Eindhoven) هلند در این زمینه می گوید: « یک مهاجم ممکن است امروز، مکالمات محرمانه ما را ذخیره کند و سال‌ها بعد با استفاده از کامپیوتر کوانتومی رمز آنها را بشکند. در اینصورت همه اسرار امروزمان را از دست خواهیم داد». چنین امکانی نه تنها داده‌های خصوصی مردم، بانک‌ها و پرونده‌های سلامت را در معرض افشا قرار خواهد داد بلکه اسرار دولت‌ها را نیز تهدید خواهد کرد. خانم Lange که مدیریت یک کنسرسیوم تحقیقاتی متشکل از یازده دانشگاه و شرکت را برعهده دارد، بهترین راهکار را استفاده از «رمزنگاری پساکوانتوم» در سازمان‌های امنیتی می‌داند. این کنسرسیوم از سال 2015 با بودجه‌ای 3.9 میلیون یورویی و باهدف توسعه روش‌های جدید رمزنگاری آغاز به کار کرده است. Lange می‌گوید: « شاید این بودجه زیادی به نظر برسد، اما صد برابر کمتر از بودجه‌ای است که صرف ساخت کامپیوترهای کوانتومی می‌شود» او هشدار می‌دهد که باید به پژوهش در حوزه رمزنگاری بهای بیشتری بدهیم: « جا انداختن روش‌های رمزنگاری جدید در بین کاربران نهایی، خود پانزده تا بیست سال زمان لازم دارد و این زمان باید به زمان لازم برای توسعه و استانداردسازی این روش‌ها افزوده شود»

منبع:

دانشگاه آیندهوون (هلند)
منبع عکس (وب‌سایت پی‌سی‌وُرلد)
تاریخ انتشار:
04 مهر 1396

نشانی منبع:
https://www.shabakeh-mag.com/news/9883/%D9%85%D9%87%D8%A7%D8%AC%D9%85%D8%A7%D9%86-%DA%A9%D9%88%D8%A7%D9%86%D8%AA%D9%88%D9%85%DB%8C-%D8%A7%D9%85%D8%B1%D9%88%D8%B2-%D8%B6%D8%A8%D8%B7-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF%D8%8C-%D8%B3%D8%A7%D9%84%E2%80%8C%D9%87%D8%A7-%D8%A8%D8%B9%D8%AF-%D8%B1%D9%85%D8%B2%DA%AF%D8%B4%D8%A7%DB%8C%DB%8C-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF