محموله کیت تشخیص کرونا برای تست ۴۰ هزار نفر به آلمان صادر شد

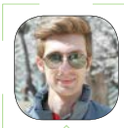
محموله کیت تشخیص ویروس کووید-۱۹ شامل ۴۰ هزار تست ساخته شرکت دانش‌بنیان پیشتاز طب زمان، سه‌شنبه هفته گذشته از فرودگاه امام خمینی (ره) تهران به مقصد آلمان صادر شد. به گفته مدیرعامل این شرکت، این محصول ایران‌ساخت از نظر دقت، عملکرد و زمان تشخیص تمام استانداردهای روز را داشته و مشابه نمونه‌های خارجی است./ معاونت علمی و فناوری

مراقبت بهتر از نوزادان نارس با محصول آنتی‌باکتریال

محققان یک مجموعه دانش‌بنیان با استفاده از پارچه‌های حاوی مواد نانو اقدام به تولید آشیانه نوزاد برای نوزادان نارس کرده است. به گفته مهدی زندی، مدیرعامل این شرکت، نوزادان در رحم مادر با لگد زدن، به تقویت عضلات خود کمک می‌کنند که در نوزادان نارس این کار به دلیل تولد زودهنگام انجام نمی‌شود و در نتیجه عضلات ضعیفی دارند. این آشیانه به نوزاد فرصت می‌دهد تا با لگد زدن در آن عضلات خود را تقویت کند./ ستاد توسعه فناوری نانو

رمزگشایی از علت ریشه‌ای موارد متعدد لو رفتن اطلاعات هویتی مردم از چند پایگاه داده مهم در کشور

فروش اطلاعات به قیمت امنیت مردم



محمدصالح تیمار

دانش

تا همین چند سال پیش وقتی در رویدادهایی نادر خبر لو رفتن اطلاعات مشتریان بانک یا مرکزی منتشر می‌شد تا مدت‌ها آن خبر نقل محافل گوناگون بود، علتش بررسی می‌شد، افراد خاطی و سازمان مقصر مورد بازخواست قرار می‌گرفتند و مکلف به ارائه توضیح بودند... اما اخیرا چند ماهی است با انبوهی از اخبار و شایعات درست و نادرست در مورد لو رفتن اطلاعات هویتی مردم ایران مواجه شدیم. آن قدر که گویی کم‌کم باید جزو خبرهای روزمره و عادی تلقی‌شان کنیم. اطلاعات هویتی مردم از سامانه‌ها و وبگاه‌های مختلف، به دلیل ضعف سیستم امنیتی به بیرون درز کرده و در فضای وب خرید و فروش می‌شود. بدیهی است حفاظت از داده‌ها در برابر هکرها در فضای وب هزینه‌های کلانی دارد. اما سوال مهم این است که نهادهای مختلف دولتی و خصوصی تا چه حد مکلف به پرداخت این هزینه‌ها به منظور به‌کارگیری قوی‌ترین سامانه‌های امنیتی در شبکه هستند و اگر این امنیت بالاست چرا اخبار مربوط به لو رفتن این اطلاعات این قدر مکرر شده است.

اکنون پرسش افکار عمومی این است که نشتی داده‌ها از سامانه‌های گوناگون داخلی دقیقا چرا و چطور اتفاق می‌افتد؟ واکنش مسؤولان به این مسأله چیست؟ آیا لو رفتن اطلاعات خطری برای صاحبان آن دارد؟ مجازات سازمان‌هایی که نتوانسته‌اند از اطلاعات مردم حفاظت کنند چه بوده و ضمانت اجرای آن چیست؟

لو رفتن اطلاعات هویتی کاربران سامانه‌ها، نرم‌افزارها و وبگاه‌ها در سراسر جهان چیز عجیبی نیست. این اتفاقات اغلب با هک شدن بانک‌های اطلاعاتی مرتبط با یک سازمان رخ می‌دهد. بانک‌های اطلاعاتی‌ای که در برخی موارد، اصول امنیتی مربوط به حفاظت اطلاعات کاربران را به‌خوبی انجام داده‌اند و با این حال بازهم در مقابل هکرها شکننده بوده‌اند.

اما به نظر می‌رسد در ایران شرایط متفاوت است و رعایت نشدن پروتکل‌های امنیتی بانک داده‌ها از سوی مالکان آنها منجر به نشتی‌های متعدد و قابل توجه شده است؛ نشتی‌هایی که اطلاعات هویتی مردم را به هدفی در دسترس و آسان برای هکرها تبدیل کرده است.

سه سال پیش بود که خبر در دسترس بودن اطلاعات کاربران یکی از اپراتورهای تلفن همراه همه را شوکه کرد. اطلاعاتی که از طریق یک ربات تلگرامی به آسانی در دسترس همگان قرار گرفته بود. از آن موقع تاکنون این اتفاق بارها تکرار شده است و در ماه‌ها و هفته‌های اخیر خبرهایی از این دست هر روز به گوش‌مان می‌رسد. افشای بانک اطلاعاتی یک شرکت بزرگ حمل‌ونقل ریلی، هک شدن اطلاعات شناسنامه‌ای ۸۰ میلیون ایرانی از بانک‌های اطلاعاتی سازمان ثبت‌احوال و وزارت بهداشت، هک شدن اطلاعات کاربری پنج میلیون کاربر یک اپ‌استور ایرانی آیفون، افشای اطلاعات یک وبگاه فروش بلیت سفر، لو رفتن اطلاعات هویتی مردم از یک صرافی آنلاین و چند مورد دیگر، همه و همه به دلیل نواقص امنیتی بانک‌های اطلاعاتی سازمان‌های دولتی و خصوصی گریبان‌گیر مردم شده است.

مجموعه این اتفاقات، اطلاعاتی نظیر نام و نام خانوادگی، کد ملی، نشانی ایمیل، شماره تلفن، عکس پرسنلی و مواردی دیگر را در اختیار هکرها قرار داده است.

ضعف امنیتی یا بی‌توجهی مسؤولان؟

حال باید ببینیم عامل لورفتن این حجم انبوه اطلاعات چیست؟ میلاد نوری، کارشناس فناوری اطلاعات در پاسخ به این پرسش به جام‌جم می‌گوید: «به نظر من عوامل اصلی لو رفتن اطلاعات به شکل‌های مختلف را می‌توان در چند مورد جست‌وجو کرد، ناآگاهی مردم از مسائل امنیتی و حریم شخصی در فضای آنلاین، ضعف سیستم‌های امنیتی و اجرایی نشدن قانون برای مجازات شرکت‌ها و سازمان‌هایی که نتوانسته‌اند از اطلاعات کاربران محافظت کنند.»

این کارشناس فناوری اطلاعات اجرا نشدن قانون برای مجازات بانیان این مساله را عامل اصلی تعدد این رخدادها می‌داند و معتقد است تا زمانی که افشای اطلاعات کاربری برای مالکان داده مجازات یا جریمه قابل‌توجهی در پی نداشته باشد، تکرار آن جای تعجب ندارد. او می‌گوید: «وقتی لو رفتن اطلاعات کاربران یک وبگاه معتبر فروش بلیت با چند توییت در شرح مختصر مساله و عذرخواهی تمام می‌شود و مالکان داده هیچ بهایی نمی‌پردازند، واضح است سایر موسسات و سازمان‌ها توجه جدی به پیاده‌سازی پروتکل‌های امنیتی برای پایگاه‌های داده خود نمی‌کنند. زیرا تجربه به آنها نشان داده است ماجرا با یک عذرخواهی ساده در فضای مجازی حل می‌شود و کسی پیگیری‌اش نمی‌کند.»

اسماعیل باقری اصل، پژوهشگر در حوزه امنیت زیرساخت‌های حساس و حیاتی، تصریح می‌کند: «در بسیاری از موارد رعایت نشدن حداقل سیاست‌های امنیتی منجر به نشت اطلاعات می‌شود. بسیار پیش می‌آید که در برقراری ارتباط بین دو پایگاه داده یا جابه‌جایی داده‌ها بین دو سازمان، توسعه‌دهندگان که نسبت به سیاست‌ها و راهکارهای امنیتی بیگانه‌اند، امور مربوطه را انجام می‌دهند و باعث ایجاد آسیب‌پذیری امنیتی در سامانه و داده‌های مرتبط به آن می‌شوند. در واقع با اولویت ندادن به راهبردهای تاب‌آوری سایبری که تمام اصول سه‌گانه امنیت را نیز شامل می‌شود، مخاطره بیشتر خواهد شد.»

گفتنی است حفظ محرمانگی، یکپارچه بودن و دسترس‌پذیری، سه مفهوم اصلی امنیت اطلاعات در فضای وب است.

لزوم اجرایی شدن لایحه حریم خصوصی

با این اوصاف درمی‌یابیم یکی از مهم‌ترین عوامل نشتی اطلاعات، نبود رویکرد جدی امنیتی در میان مدیران سازمان‌ها و کسب‌وکارهاست که می‌تواند به ضرر کاربران تمام شود و فراگیر نبودن این رویکرد از آنجا می‌آید که قانون مدونی برای مجازات مالکان داده‌هایی که نتوانسته‌اند از آنها محافظت کنند وجود ندارد.

در این باره، ابوالقاسم صادقی، معاون امنیت سازمان فناوری اطلاعات ایران در مصاحبه با خبرگزاری مهر گفته است از طریق مرکز ماهر (مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای) مسائل امنیتی که سازمان‌ها باید رعایت کنند به آنها ابلاغ شده است؛ با این حال، سازمان‌های مذکور این ابلاغ‌ها را جدی نمی‌گیرند و با سهل‌انگاری آنها هم هیچ برخوردی قضایی نمی‌شود. او در ادامه می‌گوید: «به دلیل نبود قوانین و قاعده برای حفظ حریم خصوصی در فضای سایبری، نهادهایی مانند مرکز ماهر نمی‌توانند به‌راحتی فعالیت مؤثر داشته باشند.»

صادقی در مورد خلأ قانونی و نبود مجازات برای بانیان لو رفتن داده‌ها تصریح می‌کند: «لایحه حریم خصوصی در فضای سایبری که مدت‌هاست از سوی سازمان فناوری اطلاعات تهیه شده، در انتظار تصویب در کمیسیون تخصصی دولت است.»

انتظار می‌رود با تصویب این لایحه و تدوین قوانین سختگیرانه در مورد حفاظت از اطلاعات کاربران، افشای اطلاعات به‌آسانی اتفاق نیفتد.

اوضاع در آن سوی آب‌ها چگونه است؟

هک شدن بانک‌های اطلاعاتی و لو رفتن اطلاعات کاربران برای بعضی از بزرگ‌ترین شرکت‌های حوزه‌های وب، انرژی، اقتصاد و غیره در سراسر جهان رخ داده است. شرکت‌هایی که با صرف بودجه‌های قابل توجه سعی در ایمن‌سازی بانک‌های داده خود داشته‌اند. تفاوت افشای اطلاعات در چنین مواردی با آنچه در ایران شاهد آن بوده‌ایم، رویکرد امنیتی مالکان داده در حفاظت هرچه بهتر این داده‌ها است.

عرف رایج در جهان این است که وقتی اطلاعات بانک داده‌ای لو می‌رود، مالکان داده سریعا جوانب امر به کاربران خود اطلاع می‌دهند، از آنها می‌خواهند در اسرع وقت نسبت به ایمن‌سازی حریم شخصی خود اقدام کرده و نسبت به زوایای مختلف سوءاستفاده از داده‌ها با احتیاط بیشتری عمل کنند.

میلاد نوری با ذکر مثالی ابعاد واکنش‌های مدیران برخی شرکت‌های بزرگ جهان در این موارد را این‌طور توضیح می‌دهد: مثلا اگر آدرس ایمیل و شماره تلفن و رمز ورود به یک سامانه هک شود، مدیران آن سامانه با صدور بیانیه‌ای ضمن عذرخواهی از کاربران، از آنها می‌خواهند نسبت به تغییر رمز ورود به آدرس ایمیل، رمز کارت‌های بانکی و موارد دیگر اقدام کنند تا اگر رمز ورود آنها به این سامانه با جاهای دیگری بود، دچار مشکل نشوند. اما این همه ماجرا نیست و مسؤولان آن سازمان شفاف‌سازی می‌کنند که علت این نقص امنیتی دقیقا چه بوده است؟ مثلا توضیح می‌دهند که کدگذاری یکی از پایگاه‌ها به خوبی صورت نگرفته بود یا یک عضو خرابکار داخل مجموعه عامل لو رفتن اطلاعات بوده است.

با این شفاف‌سازی، این اطمینان به مخاطب داده می‌شود که چنین مسأله‌ای دیگر تکرار نمی‌شود و همچنین شرکت‌ها و سازمان‌های دیگر سعی در بررسی نواقص مشابه احتمالی خواهند داشت.

نوری تصریح می‌کند رعایت نشدن سلسله مراتب در دسترسی به اطلاعات از عوامل مهم آسیب‌پذیری امنیتی بانک‌های اطلاعاتی است که بارها مشکل آفریده است.

باقری‌اصل: در بسیاری از موارد رعایت نشدن حداقل سیاست‌های امنیتی منجر به نشت اطلاعات می‌شود. در واقع با اولویت ندادن به راهبردهای تاب‌آوری سایبری که تمام اصول سه‌گانه امنیت را نیز شامل می‌شود، مخاطره بیشتر خواهد شد

خطرات افشای اطلاعات مردم

نکته

شاید در نگاه اول اطلاعات هویتی و شماره تلفن و نشانی ایمیل کاربران یک سامانه یا تعداد زیادی از مردم، مهم به نظر نرسد و خطرات آن از دید ما پنهان بماند. اما در دسترس بودن این اطلاعات چقدر مشکل‌آفرین است؟ اهمیت این اطلاعات کجاست که اشخاصی در داخل و خارج از ایران برای خریدن آنها مبالغی را هزینه می‌کنند؟

میلاد نوری معتقد است اطلاعات موجود در هر پایگاه به تنهایی، احتمالا، خطر چندانی نخواهد داشت و اگر اطلاعات چند بانک داده در کنار هم قرار بگیرند باید گوش به زنگ بود. او می‌گوید: «این اطلاعات دستمایه مناسبی برای هک اجتماعی است. یعنی هکر می‌تواند با استفاده از این اطلاعات، اعتماد افراد را برای کلاهبرداری‌ها فراهم کند. یا حتی ممکن است در یک شبکه پیام‌رسان به کاربر پیام بدهد و با ارائه این اطلاعات بگوید من تلفن همراه تو را هک کرده‌ام و به متن پیام‌هایت دسترسی دارم، اگر می‌خواهی پیام‌ها را افشا نکنم، پنج میلیون تومان پرداخت کن! اغلب کاربران هم از روی سادگی و بی‌اطلاعی گول می‌خورند.»

در چنین مواردی لو رفتن اطلاعات و آگاه نبودن مردم در کنار هم بستر آسانی را برای کلاهبردارها فراهم می‌کنند. البته اینها فقط مثال‌هایی ساده هستند و خطرات بزرگ‌تری هم می‌تواند در انتظار کاربران باشد. این کارشناس فناوری اطلاعات می‌افزاید: «برخی موسسات خصوصی برای احراز هویت کاربران‌شان از آنها می‌خواهند کارت ملی خود را در دست بگیرند و برای آنها عکسی واضح از کارت ملی و چهره‌شان بفرستند! اگر اطلاعات چنین موسسه‌ای افشا شود (که در مواردی چنین شده است) خرابکارها می‌توانند از عکس و اطلاعات هویتی اشخاص برای سودجویی‌های بزرگ‌تر استفاده کنند. مثلا با اطلاعات آنها یک وبگاه شرط‌بندی راه بیندازند یا فعالیت‌های سایبری خرابکارانه انجام دهند.»

نوری: وقتی لو رفتن اطلاعات کاربران یک وبگاه معتبر فروش بلیت با چند توییت در شرح مختصر مساله و عذرخواهی تمام می‌شود واضح است سایر موسسات و سازمان‌ها توجه جدی به پیاده‌سازی دستورالعمل امنیتی برای پایگاه‌های داده خود نمی‌کنند

این داستان ادامه دارد؟!

مکث

باتوجه به آنچه گفته شد، مشخص نیست سازمان‌ها و شرکت‌های خصوصی و دولتی چه زمانی برای امنیت پایگاه‌های داده خود چاره‌ای دقیق و محکم خواهند اندیشید. اگر جلوی این وضع گرفته نشود بعید نیست به‌زودی این ماجرا از نشت اطلاعات هویتی مردم جدی‌تر شود و شاهد لو رفتن اطلاعات مهم‌تری باشیم.

باقری‌اصل در این باره به جام‌جم می‌گوید: «در انقلاب صنعتی چهارم، تمامی زیرساخت‌ها، سامانه‌ها، ارتباطات به سمت یک‌پارچه شدن خواهند رفت. این یعنی امکان وقوع تهدیداتی که منجر به نقض سه اصل امنیت می‌شوند، بیشتر می‌شود. در نتیجه بهتر است سازمان‌ها و زیرساخت‌های حساس و حیاتی، تدوین استراتژی‌های ارزیابی، بهبود و بلوغ تاب‌آوری سایبری را در دستور کار خود قرار دهند که بتوانند با بهره‌گیری از آن، در صورت بروز مخاطرات، اعم از سایبری و غیرسایبری، در کوتاه‌ترین زمان ممکن نسبت به پاسخگویی به رخدادها اقدام نمایند.»

نوری در پایان صحبت‌هایش اوضاع فعلی کشور را بهشتی برای هکرها می‌داند و می‌گوید: «از آنجا که این کارها برای هکرها درآمدزا است، وقتی کشوری را با چنین اشکالات گسترده‌ای در تامین امنیت بانک‌های داده پیدا می‌کنند، روی آن متمرکز شده و دست از سرش برنمی‌دارند.»

در شرایط فعلی ورود مقامات قضایی به این مسأله و تدوین نظام قانونی سخت‌گیرانه و اجرای آن، برای تامین امنیت اطلاعات در فضای وب، می‌تواند راه‌حلی سریع و ثمربخش برای بهبود اوضاع باشد.

دنیای ذهن

کشف سرچشمه شادی در مغز

فاطمه نقدی

دانش

«جست‌وجوی سرچشمه‌های شادی» شاید پرطرفدارترین گزاره در ذهن ما باشد! وقتی که بارها و بارها به آن فکر کرده‌ایم، گاهی به سرچشمه‌های بیرونی سفر کرده‌ایم، برای به دست آوردن ثروت تلاش کرده‌ایم و گاهی اوقات هم هنگام مراقبه، به سرچشمه‌ای درونی رسیده‌ایم و شادی را همچون رودی خنک و گوارا در سراسر روانمان حس کرده‌ایم. بشر همواره به دنبال این سرچشمه‌ها بوده است. از افلاطون و ارسطو گرفته تا روان‌شناسان مثبت‌گرا و اقتصاددانان.

بعد از سال‌ها تحقیق و گمانه‌زنی، اکنون خبر جذاب این است: «سرچشمه شادی کشف شد!» این کشف، را محققان دانشگاه زوریخ سوئیس با همکاری مراکز تحقیقاتی دیگر، انجام داده‌اند. آنها به ما می‌گویند برای برداشتن جرعه‌ای شادی از این چشمه، لازم است ظرفی به همراه داشته باشید! ظرفی درون مغز خودتان، ظرفی که با آن سخاوتمندانه به دیگران می‌بخشید! آن وقت است که این سرچشمه فعالانه می‌جوشد و جریان شادی، در تمام روان شما به‌راه می‌افتد.

اما این کشف، چگونه صورت گرفت؟ آنها ۵۰ نفر شرکت‌کننده را به دو گروه تقسیم کردند. به شرکت‌کنندگان گفته شد که در طی چند هفته آینده مبلغی پول در اختیارشان قرار می‌گیرد و آنها باید تصمیم بگیرند آن را برای خود یا دیگران هزینه کنند. نیمی از آنها متعهد شدند پول را برای کسی که می‌شناسند صرف کنند (گروه آزمایش، وعده سخاوت) و نیم دیگر متعهد بودند پول را صرف خود کنند (گروه کنترل). در حالی که شرکت‌کنندگان تصمیم خود را برای انجام دادن یا ندادن رفتار سخاوتمندانه می‌گرفتند، محققان فعالیت را در سه بخش از مغز شرکت‌کنندگان بررسی کردند. این سه ناحیه مناطق زیر بودند:

۱. در محل اتصال تمپوپریتال جایی که رفتارهای خیرخواهانه و سخاوتمندانه پردازش می‌شود.

۲. جسم مخطط شکمی، جایی که با احساس شادی ارتباط دارد.

۳. قشر اوربیتوفرونتال، جایی که هنگام تصمیم‌گیری، جوانب مثبت و منفی تصمیم را درنظر می‌گیریم.

این سه ناحیه مغز، با توجه به این‌که شرکت‌کنندگان رفتار سخاوتمندانه را انتخاب کرده بودند یا جزو گروه کنترل بودند، تعامل متفاوتی را نشان دادند. همچنین گروه اول بعد از انجام یا تصمیم به کار خیرخواهانه، احساس شادمانی بیشتری نسبت به گروه کنترل داشتند.

محققان، میزان شادی شرکت‌کنندگان هردو گروه کنترل و آزمایش را قبل و بعد از تصمیم‌گیری اندازه‌گیری کردند. نتایج این مطالعه نشان داد شادی و سخاوتمندی روی یکدیگر تاثیر می‌گذارند.

نکته قابل توجه این است که حتی وعده سخاوتمندی، مناطق شادی را در مغز فعال می‌کند. ارتباط این ناحیه با ناحیه شادی می‌تواند احساس خوشبختی را تشدید کند.

این کشف بزرگ راه بشر را برای رسیدن به سرچشمه‌های دیگر شادی هموارتر می‌کند. همچنین به نظر می‌رسد ادامه این راه به مغز خود ما بستگی دارد! این‌که ظرف‌های بزرگ‌تری برای برداشتن شادی از سرچشمه‌های سخاوت برداریم و شادی را فعالانه تولید کنیم یا ظرف‌هایمان را بشکنیم و چشمه شادی خشک شود!

مبنع: Science Daily