کد خبر: ۶۸۱۰۷۳
دوشنبه ۵ مهر ۱۳۹۵ ۱۵:۴۶

سوالات بدون پاسخ پیرامون هک شدن یاهو / فاش شدن اطلاعات ۵۰۰ میلیون کاربر حقیقت دارد؟

یاهورسما اعلام کرد که در سال ۲۰۱۴ قربانی‌هک‌گسترده‌ای شده است.اما حدودا بعد از ۲ سال و پس از فروش این اطلاعات در بازار سیاه رسما به این حمله اعتراف کرده است.

به گزارش ایسکانیوز و به نقل از زومیت، اطلاعاتی از جمله نام‌ها،آدرس ایمیل،شماره تلفن و سوالات امنیتی از شبکه شرکت یاهو در سال ۲۰۱۴ دزدیده شده است. رمز عبورها هم البته به صورت مخدوش شده دزدیده شده که باعث می‌شود هکرها نتوانند بلافاصله از آن‌ها استفاده کنند. همچنین شرکت یاهو بر این باور است که اطلاعات مالی دست نخورده باقی مانده است.

این کمپانی، هک را در بیانیه‌ای در پنج‌شنبه شب تایید کرد. اما این بیانیه و اطلاعیه‌ای که در جمعه صبح به مشتریان ارسال شد، سوالات زیادی را ایجاد کردند.

سوالات عمده

مهم‌ترین سوالات درباره این است که چرا این اطلاع‌رسانی اینقدر دیر انجام شده است. چون زمان هک مربوط به ۲ سال پیش بوده و این اطلاعات حدود ۲ ماه پیش در دارک وب ( ) توسط کاربری به نام فروخته شد، کاربری که پیش از این اطلاعاتی از سایت‌های مای‌اسپیس)) و لینکدین () به فروش گذاشته بود. جرمایاه گراسمن مدیر بخش استراتژی امنیت شرکت سنتینل‌وان () می‌گوید: ما در حالی‌که می‌دانیم این اطلاعات در سال ۲۰۱۴ دزدیده شده، اما نمی‌دانیم که یاهو چه زمانی از این هک آگاه شده است. این بخش مهمی از داستان است.

گراسمن که تا سال ۲۰۱۱ مسئول بخش امنیت دپارتمان مهندسی یاهو بوده، می‌گوید این ادعای یاهو که هکرها از پشتیبان دولتی برخوردار بوده‌اند نیازمند تحقیق بیشتری است. او در ادامه گفته است: هکرهای دولتی هیچوقت چنین اطلاعاتی را در بازار سیاه به فروش نمی‌رسانند. کاری که هکر یاهو انجام داده است. این هک به احتمال قریب به یقین فقط با انگیزه‌های مالی انجام شده است، پس احتمال این‌که او از پشتیبانی دولتی برخوردار بوده بسیار کم است. اگر هم چنین باشد پس باید داستان درباره ۲ نفوذ جداگانه توسط ۲ تیم مختلف باشد.

کریس هادسن مدیر بخش اطلاعات امنیت اروپا،آفریقا و خاورمیانه‌ی شرکت امنیتی زسکالر با این گفته‌ها موافق است و در پی آن بیان کرده: بدون هیچگونه اطلاع‌رسانی درباره نحوه این هک،ادعای یاهو مبنی بر دولتی بودن هکرها اصلا قابل اثبات نیست. این ادعای یاهو به نظر بیشتر برای منحرف کردن افکار عمومی به نظر می‌رسد و با توجه به عدم اطلاع رسانی دقیق نمی‌توان به طور قطع نظر داد.

در ضمن معلوم نیست تا چه حد رمزهای عبور از هک نجات یافته‌اند. اما یاهو اذعان کرده رمزها به صورت مخدوش شده به دست هکرها

رسیده است.

این کمپانی تاکید کرده است که قسمت اعظمی از رمزهای عبور توسط الگوریتمی به نام بی‌کریپت () مخدوش شده است. این روش باعث می‌شود حتی رمزهای یکسان به صورت مخلوطی از کاراکترها در دیتابیس ذخیره شوند. این گونه بسیاری از افراد هم که رمزهای بسیار آسانی انتخاب کرده‌اند از هک آسیب‌پذیر نخواهند بود. اما معلوم نیست آن درصد اندک که شامل این رمزنگاری نبوده‌اند چه تضمینی خواهند داشت.

این حمله باعث شده درباره مفید بودن به دست آوردن رمز توسط سوال‌های امنیتی زیر سوال برود، وقتی که به راحتی با چند سوال ساده درباره نام مادر یا شهر تولد هکر می‌تواند رمز قربانی را به دست گیرد. یاهو تمام این سوال‌ها را رمزنگاری نکرده، پس تعدادی از این سوالات به راحتی در دسترس هکرها قرار گرفته است.

سرنوشت ادغام با ورایزون

یک سوال دیگر که بعد از این هک بی‌جواب مانده است: تکلیف ادغام چندین میلیارددلاری یاهو با ورایزون () چه خواهد شد؟ کوین کانینگهام، موسس و رییس شرکت سیل‌پوینت () در این باره می‌گوید: به احتمال زیاد ورایزون با توجه به این قضیه قیمت گذاری کرده است. ادغام شرکت‌ها با روندی بسیار طولانی و دقیق صورت می‌گیرد. شرکت‌ها معمولا با تحقیقی مفصل به چنین پیشنهاداتی دست می‌زنند. ورایزون با توجه به تعداد زیاد کاربران یاهو ریسک چنین ادغامی را از قبل خبر داشته است. این سوال که آیا این خبر بر قیمت‌گذاری تاثیر می‌گذارد یا نه بستگی به بررسی دقیق در زمینه کنترل امنیت یاهو دارد. این هک نه تنها باید نگرانی در زمینه امنیت شبکه را بالا ببرد بلکه دولت را هم باید نگران کند. چون دیده‌ایم در موارد هک‌هایی همچون لینکدین ()، دراپ‌باکس () و بسیاری از موارد دیگر با استفاده از این اطلاعات، اعتبار شهروندان زیادی زیر سوال می‌رود.

توصیه برای کاربران

اما برای کاربران این سوالات اصلا اهمیتی ندارد. تنها توصیه‌ای که در این موقعیت می‌توان به کاربران یاهو کرد این است: پسورد حساب کاربری یاهو و سوالات امنیتی خود را هرچه زودتر تغییر دهند، همچنین پسورد جاهای دیگری که این اطلاعات را در آن استفاده کرده‌اند. در نهایت آن‌ها باید از این پسوردها در هیچ حساب کاربری دیگری استفاده نکنند.

چون یاهو یک سرویس ایمیل بزرگ محسوب می‌شود یک مشکل دیگر هم وجود دارد.هر حساب کاربری که با ایمیل یاهو باز شده است باید هرچه زودتر رمز آن حساب تغییر یابد.

۱۰۱/۱۰۳