شرکت‌های بزرگ دنیا نسبت به نشت اطلاعات کاربران خود جریمه‌های سنگینی پرداخت کردند؛ اتفاقی که در ایران رایج نیست

جریمه‌های میلیون دلاری برای ضعف امنیت سایبری

ندا اظهری
مترجم

حملات سایبری واقعیت ناگواری در تجارت و کسب‌وکارهای امروزی به‌شمار می‌رود که انگیزه عمده این حملات پول است. درواقع، مجرمان سایبری به‌دنبال داده‌هایی هستند که به‌واسطه آنها بتوانند از افراد، کلاهبرداری هویتی کرده یا فرصتی برای نگه‌داشتن اطلاعات سیستم‌های IT در باج‌گیری‌های خود به‌دست آورند. گمانه‌زنی‌ها حکایت از آن دارد که رقم جهانی حملات سایبری تا سال ۲۰۲۵ به مرز ۱۰ هزار و ۵۰۰ میلیارد دلار خواهد رسید. به سرقت رفتن داده‌های کاربران، علاوه‌بر اینکه اطلاعات شخصی آنها را به خطر می‌اندازد، آسیب مالی را نیز به همراه داشته و اعتبار شرکت‌های مورد نظر را نیز زیر سوال می‌برد. در این میان، بسیاری از شرکت‌هایی که مورد حملات سایبری قرار گرفته‌اند، جریمه شده و ملزم به پرداخت جریمه‌هایی شده‌اند که طبق برآوردهایی که در ۲۰۲۳ انجام شده، هزینه درز اطلاعات به حدود ۵ میلیون دلار رسیده است؛ این درحالی است که هزینه درز اطلاعات برای شرکت‌ها در سال ۲۰۲۲ چیزی بالغ بر ۴ میلیون و ۳۵۰ هزار دلار و در سال ۲۰۲۱ حدود ۴ میلیون و ۲۴۰ هزار دلار برآورد شده است. با توجه به فراوانی و افزایش شدت نشت داده‌ها، کسب‌وکارها باید امنیت داده‌ها را در اولویت قرار دهند تا از جریمه‌های سنگینی که ملزم به پرداخت آن هستند، جلوگیری کنند. خطای انسانی، تهدیدات داخلی و حملات سایبری شایع‌ترین دلایل برملا شدن داده‌ها هستند. نهادهای نظارتی مانند دفتر کمیسیون اطلاعات در انگلیس و وزارت بهداشت و خدمات انسانی در آمریکا، جریمه‌ها و مجازات‌های قابل توجهی را برای مشاغلی اعمال می‌کنند که با حملات سایبری مواجه می‌شوند.

این جریمه‌ها در کشورهای دنیا درحالی اتفاق می‌افتد که در ایران از این خبرها نیست و تنها در حد سر و صدای رسانه‌ای باقی می‌ماند و عملا هیچ یک از کاربران کاری از دستش برنمی‌آید تا برای اطلاعات از دست رفته‌اش کاری کند. نمونه آن، همین چند روز پیش خبر هک شدن «اسنپ فود» و لو رفتن بسیاری از اطلاعات کاربران است که سر و صدای زیادی هم به پا کرد. اما درنهایت این مورد لو رفتن داده‌ها نیز بی‌سر و صدا تمام می‌شود و آب از آب هم تکان نمی‌خورد. البته این تنها یک نمونه است و از دیگر موارد نیز می‌توان به حمله سایبری به «تپسی»، شرکت‌های بیمه در ایران و پیام‌رسان‌های داخلی و... اشاره کرد که درنهایت گروه یا گروه‌هایی مسئولیت حملات را عهده‌دار شده و قضیه به همین‌جا ختم شده است و کسی هم یقه شرکت‌ها و سازمان‌ها را برای ضعف امنیت سایبری آنها نگرفته است. اتفاقی که در دنیا این‌گونه رقم نمی‌خورد و شرکت‌ها بعد از هر حمله سایبری که به آنها می‌شود، مورد بازخواست قرار گرفته و ملزم به پرداخت جریمه‌ای بابت ناتوانی در حفاظت از داده‌های کاربران خود می‌پردازند.

جریمه ۸۸۶ میلیون دلاری آمازون

آمازون جزء آن دسته از شرکت‌هایی است که بارها مورد هدف حملات سایبری قرار گرفته است. حمله‌ای که در جولای ۲۰۲۱ به این شرکت وارد شد، این شرکت را متهم به پردازش داده‌های شخصی در جریان نقض GDPR (مقررات عمومی حفاظت از داده اتحادیه اروپا) به‌ویژه در مورد شیوه‌های تبلیغاتی هدفمند خود کرد. در بررسی‌هایی که روی این حمله سایبری انجام شد، مشخص کرد که آمازون درحال جمع‌آوری داده‌های مربوط به فعالیت‌های آنلاین کاربران از جمله جست‌وجوها و خریدها و استفاده از آن داده‌ها برای نمایش تبلیغات هدفمند بدون رضایت کاربران است. این شرکت از سوی اتحادیه اروپا مجرم شناخته شد و کمیسیون ملی حفاظت از داده که در لوکزامبورگ واقع شده، به‌دلیل نقض مقررات مربوط به نقض مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، ۸۸۶ میلیون دلار جریمه شد که دومین جریمه سنگین تاریخ حملات سایبری را به خود اختصاص داده است. در سطح جهانی، بررسی‌های نظارتی غول‌های فناوری به‌دنبال مجموعه‌ای از رسوایی‌ها در مورد حریم خصوصی و اطلاعات نادرست و نیز شکایت برخی کسب‌وکارها مبنی بر سوءاستفاده از قدرت بازار افزایش یافته است. این جریمه پس از افزایش نظارت بر شرکت‌های بزرگ فناوری اعمال شد که دلیل آن نگرانی در مورد حفظ حریم خصوصی کاربران و مشتریان اعلام شده است.

جریمه یک میلیارد و ۲۰۰ میلیون دلاری یک شرکت چینی

شرکت چینی «دی دی گلوبال» که به‌عنوان یک شرکت ترابری فعالیت می‌کند و بیش از ۵۵۰ میلیون کاربر و ده‌ها میلیون راننده دارد، به پرداخت یکی از بالاترین جریمه‌ها به‌دنبال حملات سایبری محکوم شده است. این شرکت عملکردی مشابه «اوبر» دارد و در سال ۲۰۲۲ به‌دلیل حمله سایبری وسیعی که به آن شد، به‌دلیل نقض حریم خصوصی داده‌های کاربران به یک میلیارد و ۲۰۰ میلیون دلار جریمه محکوم شد. این شرکت سه قانون امنیت سایبری، امنیت داده‌ها و حفاظت از اطلاعات شخصی کاربران خود را نقض کرده و اطلاعات شخصی میلیون‌ها کاربر را در معرض خطر قرار داده است. حمله سایبری که به این شرکت وارد شد، با ایجاد اختلالاتی، باعث شد تا اپ استور، ۲۵ نرم‌افزار تحت عملکرد این شرکت را حذف کند و کاربران جدید قادر به ثبت‌نام نباشند و علاوه‌بر آن، امنیت ملی و منافع عمومی کاربران را در معرض خطر قرار گرفت. علاوه‌بر اعمال جریمه، دولت چین، این شرکت را ملزم به بهبود مدیریت داده‌ها کرده است. همچنین بررسی‌ها نشان داده که این شرکت طی ۷ سال یعنی از ۲۰۱۵ به جمع‌آوری غیرقانونی اطلاعات میلیون‌ها کاربر کرده و پردازش داده‌ها را انجام داده که به‌طور جدی امنیت ملی این کشور را تحت تاثیر قرار داده است.

جریمه یک میلیارد و ۱۰۶ میلیون دلاری فیسبوک در ۲ سال

در سال ۲۰۲۱، هکرها، اطلاعات شخصی ۵۳۳ میلیون کاربر فیسبوک را شامل شماره تلفن، ایمیل و دیگر داده‌ها را به سرقت بردند. این اطلاعات نه‌تنها حساب‌های کاربری کاربران در شبکه‌های اجتماعی را به خطر می‌اندازد، بلکه هویت و امور مالی آنها را نیز در معرض خطر قرار می‌دهد. علاوه‌بر این، صاحب فیسبوک در سال ۲۰۲۳ به‌دلیل نقض اطلاعات بیش از ۵۰۰ میلیون کاربر و انتشار آنلاین این اطلاعات به مبلغ ۲۹۳ میلیون دلار جریمه شد. در کنار جریمه‌ای که فیسبوک ملزم به پرداخت آن شده، موظف شده است طیفی از اقدامات اصلاحی مشخص را در بازه زمانی تعیین شده‌ای انجام دهد تا بتواند امنیت کاربران خود را بالاتر ببرد. از سپتامبر سال گذشته تاکنون، فیسبوک درمجموع یک میلیارد و ۱۰۶ میلیون دلار جریمه شده است. علاوه‌براین، فیسبوک در سال ۲۰۱۹ نیز از سوی کمیسیون تجارت فدرال به پرداخت ۷۲۵ میلیون دلار جریمه محکوم شد که به دلیل عدم مراقبت لازم از داده‌های کاربران بوده است. در این مورد، شرکت مشاوره سیاسی «کمبریج آنالیتیکا» داده‌های میلیون‌ها کاربر فیسبوک را بدون رضایت آنها به دست آورده بود و این جریمه به دلیل اتهام محافظت نکردن از داده‌های کاربران اعمال شده است. فیسبوک همچنین متهم شده که با گمراه کردن کاربران در مورد میزان کنترلی که بر داده‌هایشان داشتند، درگیر اقداماتی شده است که به اندازه کافی نمی‌تواند امنیت سایبری داده‌ها را برقرار کند.

گوگل و چالش امنیت داده از ۲۰۱۸ تاکنون

اما جنس لو رفتن اطلاعات در گوگل جور دیگری است، به‌طوری که یکی از موارد آن در مارس سال ۲۰۱۸ اتفاق افتاد که طی آن، گوگل پلاس حین برنامه‌نویسی کاربردی، اطلاعات خصوصی بیش از ۵ میلیون کاربر خود را افشا کرد که از دید کاربران دور ماند اما اتفاق مشابهی هم در نوامبر همان سال رخ داد و همین پلتفرم اطلاعات خصوصی ۵۳ میلیون کاربر را در معرض دید عموم قرار داد و گوگل یک سال بعد مجبور شد به دلیل تهمت‌های ناشی از آن، گوگل‌پلاس را تعطیل کند. اما همیشه نقض حریم خصوصی به انتشار غیرقانونی اطلاعات کاربران محدود نمی‌شود، بلکه شرکت‌هایی چون گوگل در طول سال‌های فعالیت خود بارها از اطلاعات کاربران خود سوءاستفاده کرده‌اند که به نوعی نقض حریم خصوصی آنها به شمار می‌رود. گوگل در سال ۲۰۱۹ به اتهام جمع‌آوری اطلاعات شخصی از کودکان بدون کسب رضایت از والدین آنها در پلتفرم یوتیوب و سپس سوءاستفاده از این اطلاعات در تبلیغات هدفمند خود به دلیل نقض قانون حفاظت از حریم خصوصی آنلاین کودکان توسط کمیسیون تجارت فدرال به پرداخت جریمه ۱۷۰ میلیون دلاری متهم شد. علاوه‌بر این، دولت آمریکا در سال ۲۰۲۲ مدعی شد که گوگل به‌طور غیرقانونی مکان کاربران را ردیابی کرده و این اطلاعات را در یک صفحه وب اختصاصی منتشر کرده است. این شرکت به دنبال این اتهام ملزم به پرداخت جریمه ۳۹۱ میلیون و ۵۰۰ هزار دلار شد. این سوءاستفاده از کاربران در حالی اتفاق افتاده که کاربران با اعتماد به یک شرکت، از مکان گوشی‌های خود استفاده می‌کنند. بعد از این پرونده، مورد مشابه دیگری از گوگل نیز افشا شد که طی آن این شرکت به پرداخت ۸۵ میلیون دلار جریمه محکوم شده بود. در این پرونده تنها تعداد انگشت‌شماری از کاربران ایالت‌های تگزاس، واشنگتن، ایندیانا و واشنگتن دی سی از این غول فناوری شکایت کردند.

جریمه ۴۰۳ میلیون دلاری برای تخلف اینستاگرام

اینستاگرام در سپتامبر ۲۰۲۲ با جریمه‌ای ۴۰۳ میلیون دلاری از سوی کمیسیون حفاظت از داده‌های ایرلند هنگام بررسی داده‌های کودکانی که در پلتفرم اینستاگرام صاحب حساب‌های تجاری هستند، متوجه سوءاستفاده از این حساب‌ها شد و این شرکت را به دلیل نقض قوانین حفاظت از حریم خصوصی کودکان محکوم کرد. این کمیسیون متوجه شد که اینستاگرام، این حساب‌های کاربری را عمومی کرده و اطلاعات کودکان را در معرض سوءاستفاده قرار داده است. این جریمه پس از اتخاذ تصمیم در مورد حریم خصوصی اتحادیه اروپا اعمال شد که برای نقض مقررات عمومی حفاظت از داده‌های اتحادیه اروپاست. مشکلی که در رابطه با این پلتفرم مطرح بود، قرار گرفتن اطلاعات خصوصی کاربران شامل شماره تلفن و ایمیل کاربران و انتشار عمومی آنها و قرار گرفتن این اطلاعات در دسترس عموم هنگام ارتقا به حساب‌های تجاری بوده است. این جریمه ۴۰۳ میلیون دلاری، جزء بزرگ‌ترین جریمه‌های «مقررات عمومی حفاظت از داده اتحادیه اروپا» است که غول‌های رسانه‌های اجتماعی تاکنون با آن مواجه شده‌اند. دیگر موردی که اینستاگرام با آن مواجه شد، به سال ۲۰۱۹ برمی‌گردد که طی آن، این پلتفرم اطلاعات شخصی بیش از ۴۹ میلیون کاربر را از طریق یک سرور محافظت‌نشده حاوی اطلاعات این کاربران، افراد مشهور و حساب‌های برند اینستاگرام به صورت آنلاین منتشر کرد.

لو رفتن اطلاعات ۴۰۰ میلیون کاربر توییتر

توییتر به‌عنوان یکی از محبوب‌ترین شبکه‌های اجتماعی در دنیا در سال ۲۰۲۰ به اتهام نقض قانون حریم خصوصی اطلاعات کاربران به ۱۵۰ میلیون دلار جریمه محکوم شد. این شرکت متهم شد که از شماره تلفن و ایمیل جمع‌آوری‌شده از کاربران برای اهداف امنیتی در تبلیغات هدفمند سوءاستفاده کرده و در محافظت کافی از داده‌ها در برابر دسترسی غیرمجاز ناتوان عمل کرده است. اتفاق دیگری هم در سال ۲۰۲۲ رخ داد و اطلاعات ۴۰۰ میلیون کاربر و ۵ میلیون و ۴۰۰ حساب کاربری توییتر شامل شماره تلفن و ایمیل لو رفت. این مجموعه داده توسط هکری با نام صفحه نمایش Ryushi آپلود شد. این هکر مدعی شد که داده‌ها را با استفاده از تکنیک برداشت از وب به داده‌ها دسترسی پیدا کرده است. او برای فروش داده‌های هک‌شده ۲۰۰ هزار دلار از توییتر درخواست کرده و هشدار داده بود که اگر توییتر، پیش از فروش این داده‌ها، اقدام به خریداری آن نکند، اعتماد خود را بین کاربران از دست خواهد داد. از دیگر مواردی که توییتر با آن مواجه شده به اوایل سال ۲۰۲۳ برمی‌گردد که در آن ایمیل بیش از ۲۰۰ میلیون پروفایل کاربر در انجمن‌های هکرهای زیرزمینی در گردش بود. کارشناسان هشدار داده بودند که لو رفتن این اطلاعات می‌تواند هویت واقعی کاربران ناشناس توییتر را فاش کند و سرقت حساب‌های توییتر را برای مجرمان آسان‌تر کند.

سه‌شنبه ۱۲ دی ۱۴۰۲
شماره ۴۰۴۷
WWW.FDN.IR
FARHIKHTEGANDAILY