سرقت اطلاعات و سوابق بهداشت و درمانی در امریکا

نویسنده : علی جعفری 1395-02-08 - 9:30 صبح

در سال 2015، یک نفر از سه آمریکایی قربانی سرقت اطلاعات و سوابق بهداشت و درمانی بودند؛ حملاتی در مقیاس وسیع که هر یک بیش از 10 میلیون تن را متاثر ساختند. بر این اساس به تنهایی در ایالات متحده اطلاعات بیش از 111 میلیون تن بخاطر هک یا حوادث فناوری اطلاعات سرقت یا مفقود شدند.
طبق گزارش قانون شکنی‌ها در حوزه بهداشت درمان (2016) به نقل از Bitglass، 98% از موارد سرقت و انتشار سوابق بخاطر حملات نفوذ در مقیاس وسیع بوده است که صنعت بهداشت و درمان را هدف قرار داده بودند. این حملات جنجالی اصلی‌ترین منبع سرقت و مفقود شدن اطلاعات و سوابق در حوزه بهداشت و درمان بودند، که افزایش توجه هکرها به اطلاعات پزشکی را نشان می‌دهد. برای مثال، حمله هکری Premera Blue Cross که 11 میلیون مشتری بخش بهداشت و درمان را متاثر ساخت و یا حمله هکری Anthem که منجر از سرقت و انتشار سوابق 78.8 میلیون تن گردید.

این یافته‌ها براساس تحلیل داده‌های پایگاه داده «Wall of Shame» وزارت بهداشت و خدمات انسانی ایالات متحده است، که افشا موارد نقض قانون را به عنوان بخشی از قانون انتقال و پاسخگویی الکترونیک بیمه سلامت (HIPAA) شامل می‌گردد.

به گفته نَت کاسیک مدیر اجرایی ارشد Bitglass، «80% افزایش در حملات هکری سرقت اطلاعات در سال 2015 نشان می‌دهد که هکرها بخش بهداشت و درمان را هدف قرار دادند؛ و این در حالی است که این حملات در مقیاس وسیع بوده و تقریبا یکی از هر سه شهروند آمریکایی را متاثر ساخته اند.» «با فرض اینکه هم اکنون با رشد و تکامل فناوری اینترنت اشیا (IoT) اطلاعات بلادرنگ بیماران بصورت آنلاین قابل دسترسی هستند، لذا سازمان‌های بهداشت و درمان باید فناوری‌های امنیت اطلاعات نوآورانه تری را برای برآوردن نیازمندی‌های امنیتی و رعایت مقررات و قوانین اتخاذ نمایند.»
در سال 2015، 56 مورد نقض قانون این چنینی بخاطر هک یا حوادث فناوری اطلاعات وجود داشت، که با 31 مورد در سال 2014 قابل قیاس است. در این میان، فقط 97 مورد بخاطر از دست رفتن یا سرقت اطلاعات بوده اند که در مقایسه با 140 مورد سال 2014 کاهش چشمگیری را نشان می‌دهد.

بر اساس گزارش فوق، «اطلاعات حفاظت شده سلامت (PHI) که اطلاعات حساس مختلف (از قبلی شماره بیمه تامین اجتماعی، سوابق پزشکی و تاریخ تولد) را شامل می‌گردند ارزش قابل ملاحظه ای در بازار سیاه دارند.» «بنا بر گزارش اخیر موسسه Ponemon پیرامون هزینه این موارد نقض، هزینه متوسط به ازای هر سابقه سرقت شده یا از دست رفته بالغ بر 154 دلار است، درحالیکه این رقم بطور متوسط برای سازمان‌های حوزه بهداشت و درمان تا 363 دلار افزایش یافته است.»

Bitglass در گزارش خود هزینه‌هایی را نیز مورد اشاره قرار داده است که مصـرف کننـده‌ها نیز متحمل شده اند: در زمان وقوع موارد نفوذ و سـرقت اطلاعات کارت اعتباری، صادرکننـده‌ها می‌توانند کلیه تراکنشات را فسخ کنند و افراد تحت تاثیر قرار گرفته مشـمول قوانینی می‌شونـد که مسـئولیت‌شان را [در مقابل تراکنشات مشـکوک] محدود خواهد ساخت. با این وجود قربانی‌ها زمانی که اطلاعات هویتی آنها از طریق انتشار اطلاعات حفاظت شده سـلامت سـرقت می‌گردد وسعت عمل زیادی برای جبران ندارنـد و بسـیاری نیز خیلی دیر از سـرقت اطلاعات خود آگاه می‌گردنـد. درحالیکه مجرمین اغلب اطلاعات بهـداشت و درمان حاصل را برای سـرقت اطلاعات هویتی قربانی مورد اسـتفاده قرار می‌دهنـد، این اطلاعات برای اسـتفاده از خـدمات بهداشت و درمان به نام قربانی یا اخاذی از شرکت‌ها نیز قابل استفاده خواهند بود.