أ ب: أرامكو السعودية تقر بتعرضها لابتزاز بـ50 مليون دولار



التغيير

أقرت شركة "أرامكو" النفطية العملاقة، الأربعاء، بتعرضها لعملية "ابتزاز" عقب تسريب بيانات خاصة بها، مشيرة إلى أن "خاطفي البيانات" يطالبون بفدية قدرها 50 مليون دولار.

وقالت الشركة في تصريح لوكالة "أسوشييتد برس"، إن "البيانات المسربة من الشركة - وهي ملفات باتت تستخدم فيما يبدو في محاولة ابتزاز إلكتروني تنطوي على طلب فدية بقيمة 50 مليون دولار - جاءت على الأرجح من أحد المتعاقدين معها.

وأضافت أنه "نما لعلمنا مؤخرا نشر غير مباشر لعدد محدود من بيانات الشركة تحتفظ بها أطراف ثالثة متعاقدة معها".

ولم تذكر الشركة اسم المتعاقد الذي أصابه الضرر، ولا ما إذا كان هذا المتعاقد قد تعرض للاختراق أو ما إذا كانت المعلومات قد تسربت بطريقة أخرى.

وأضافت: "نؤكد أن نشر البيانات لم يكن بسبب خرق لأنظمتنا، وليس له تأثير على عملياتنا، والشركة مستمرة في الحفاظ على أمن سيبراني قوي".

وزعم أحد مواقع شبكة الإنترنت العميقة "دارك ويب" أن جهة الابتزاز تمتلك ما حجمه 1 تيرابايت من بيانات "أرامكو".

ومنحت الصفحة أرامكو مهلة لحذف البيانات مقابل 50 مليون دولار من العملات المشفرة، ولم يتضح بعد من يقف وراء مؤامرة الفدية.

وتم استهداف أرامكو من قبل بهجوم إلكتروني عام 2012، حين تأثرت الشركة بما يسمى "فيروس شمعون"، الذي حذف محركات الأقراص الصلبة ثم عرض صورة لعلم أمريكي محترق على شاشات الحاسبات.

وأجبر الهجوم أرامكو على إغلاق شبكتها وتدمير أكثر من 30 ألف جهاز حاسب آلي.

لاحقا، ألقى مسؤولون أمريكيون باللوم في هذا الهجوم على إيران، التي تعرضت بدورها لاستهداف برنامجها التخصيب النووي بفيروس "ستكس نت"، ومن المرجح أنه صناعة أمريكية وإسرائيلية.

وفي عام 2017، انتشر فيروس آخر في أنحاء المملكة وعطل أجهزة حاسبات في مشروع "صدارة"، المشترك بين أرامكو وشركة داو للكيماويات ومقرها ميشيجان، وصدرت تحذيرات حينها من أنه قد يكون نسخة أخرى من فيروس "شمعون".

وتعرض مجموعة التهديد، التي تعرف باسم "زيرو إكس"، للبيع على الشبكة المظلمة البيانات التي تزعم أنها اكتسبتها من خلال اختراق "شبكة وخوادم" أرامكو في مرحلة ما من العام الماضي.

وتشمل البيانات المعروضة للبيع، بحسب الموقع، وثائق تتعلق بمصافي أرامكو، ومعلومات شخصية عن أكثر من 14 ألف موظف، ومواصفات مشاريع للأنظمة، وصحائف تسعير وتحليلات داخلية، بالإضافة إلى معلومات متعلقة بالأمن بما في ذلك عناوين بروتوكول الإنترنت، ونقاط الوصول إلى " Fi-Wi".

وتدعي المجموعة أنها كانت تتفاوض على بيع البيانات مع خمسة مشترين محتملين مهتمين.