

प्रेस विज्ञप्ति
PRESS RELEASE

दिनांक / Date: 18.10.2024

हाल ही में दो बीमाकर्ताओं से डेटा प्रकटनों (लीक्स) की सूचनाएँ मिली हैं। प्रारंभ में ही यह स्पष्ट किया जाता है कि आईआरडीएआई डेटा सुरक्षा को बहुत महत्वपूर्ण मानता है तथा डेटा उल्लंघन, बीमा कंपनियों आदि की आईटी प्रणालियों पर साइबर आक्रमणों को अत्यंत गंभीरतापूर्वक लेता है।

बीमा कंपनियों के लिए साइबर सुरक्षा संबंधी दिशानिर्देश विद्यमान हैं जो बीमाकर्ताओं से उनके परिचालन संचालित करने के लिए सुदृढ़ आईटी और साइबर सुरक्षा ढाँचा लागू करने की अपेक्षा करते हैं।

आईआरडीएआई संबंधित बीमाकर्ताओं के विषय में स्थिति की ध्यानपूर्वक निगरानी कर रहा है तथा उनके प्रबंधन के साथ संपर्क में है। नियमित अद्यतन स्थिति की जानकारी यह सुनिश्चित करने के लिए प्राप्त की जा रही है कि पालिसीधारकों के डेटा और हित का पूर्णतः संरक्षण किया जाए और कंपनी इस उल्लंघन के द्वारा उत्पन्न किये गये खतरे को रोकने के लिए सभी आवश्यक कदम उठाये। आईआरडीएआई यह सुनिश्चित करने के लिए बीमा कंपनियों के साथ लगातार संपर्क में रहेगा कि पालिसीधारकों के हितों का पूर्णतः संरक्षण किया जाए। संबंधित बीमाकर्ताओं को अनुदेश दिये गये हैं कि वे इस उद्देश्य के साथ कंपनी के आईटी परिदृश्य का व्यापक संपरीक्षण करने के लिए एक स्वतंत्र संपरीक्षक (आडिटर) की नियुक्ति करें कि कोई असुरक्षित स्थिति न रहे और आईटी प्रणाली उनके परिचालनों के मान और जटिलताओं को पूरा करने के लिए पर्याप्त हो।

संबंधित बीमाकर्ताओं की मानक परिचालन प्रक्रियाओं के भाग के रूप में, उन्होंने साइबर घटना की सूचना सरकार और आईआरडीएआई को दी। संबंधित बीमाकर्ताओं ने प्रभावित आईटी प्रणाली को अलग करने के द्वारा उसे वलयरोधित किया है और साथ ही, मूल कारण का विश्लेषण करने के लिए एक बाह्य आईटी सुरक्षा कंपनी को नियुक्त किया है। उक्त संपरीक्षण फर्म ने कंपनी की आईटी प्रणाली, जिसके अनुसार बीमाकर्ताओं द्वारा कार्य किया जा रहा था, में असुरक्षित स्थितियाँ होने की तथा खतरा उत्पन्न करनेवाले खिलाड़ी द्वारा प्रयुक्त कार्यपद्धति की रिपोर्ट दी जिससे उक्त स्थिति का अनुचित लाभ उठाया गया। उक्त संपरीक्षण फर्म द्वारा सुझाये गये रूप में नियंत्रण, उन्मूलन और पुनःप्रापणीयता योजना बीमाकर्ताओं के द्वारा लागू की जा रही है।

उक्त रिपोर्ट में बताये गये अतिरिक्त निवारक उपाय पालिसीधारकों के डेटा को निरापद और सुरक्षित रखने के लिए कार्यान्वयन की प्रक्रिया में हैं। तत्काल, अल्पावधि और मध्यम समयावधि में प्रणाली का ग्रेड बढ़ाने के लिए बीमाकर्ताओं के द्वारा कार्रवाई की जाएगी। एपीआई असुरक्षितताएँ, अंतराल निर्धारण और वीएपीटी समस्याएँ सुधार के एक उन्नत स्तर पर हैं। उक्त बीमाकर्ताओं ने खतरा उत्पन्न करनेवाले खिलाड़ियों के विरुद्ध विधि प्रवर्तक एजेंसियों के पास एक आपराधिक शिकायत फाइल की है। इसने पालिसीधारकों का डेटा बेचने से खतरा उत्पादक खिलाड़ी को रोकने के लिए सोशल मीडिया प्लेटफार्म पर एक कानूनी नोटिस प्रस्तुत किया है।

इसके अलावा, आईआरडीएआई ने सभी बीमाकर्ताओं को परामर्श जारी किया है कि वे असुरक्षितताओं की पहचान करने के लिए अपनी आईटी प्रणालियों की जाँच करें तथा पालिसीधारकों के डेटा का संरक्षण करने के लिए आवश्यक कदम उठाएँ।

There have been reports of data leaks from two Insurers recently. At the outset, it is stated that the IRDAI considers data security as very important and takes data breach, cyber-attacks on IT systems of insurance companies, etc very seriously.

Cyber security guidelines for insurance companies are in place which require insurers to put in place robust IT and cyber security framework for carrying out their operations.

The IRDAI is closely monitoring the situation in case of the concerned insurers and has been in touch with their management. Regular updates are being obtained to ensure that the policyholders' data and interest are fully protected and the company is taking all steps to arrest the threat posed by this breach. The IRDAI will continue to engage with the insurance companies to ensure that the policyholders' interests are fully protected. The concerned insurers have been instructed to appoint an independent auditor to undertake comprehensive audit of the company's IT landscape with the aim that there are no vulnerabilities and the IT system are adequate to meet the scale and complexities of their operations.

As part of the standard operating procedures of the concerned insurers, they reported the cyber incident to the Government and IRDAI. The concerned insurers have ring fenced the impacted IT system by isolating it and at the same time appointed an external IT security company to undertake root cause analysis. The audit firm reported vulnerabilities in the company's IT system and the methodology used by the threat actor to exploit the same which were acted upon by insurers. The Containment, Eradication and Recoverability plan as suggested by the audit firm are being implemented by the insurers.

Further preventive steps outlined in the report are in the process of implementation to keep the policyholders' data safe and secure. System upgrades over immediate, short and medium time period, will be acted upon by the insurers. The API vulnerabilities, Gap assessment and VAPT Issues are at an advanced stage of rectification. The insurers have filed a criminal complaint with the law enforcement agencies against the threat actors. It served legal notice on the social media platform to prevent the threat actor from selling the policyholders data.

Further, the IRDAI has issued advisory to all insurers to check their IT systems for vulnerabilities and take necessary steps to protect the policyholders' data.