Investigation Findings

Published under Section 48(2) of the Personal Data (Privacy) Ordinance,
Chapter 486 of the Laws of Hong Kong

Ransomware Attack on the Servers of The Hong Kong Ballet Limited

Background

The Office of the Privacy Commissioner for Personal Data (PCPD) completed its investigation in relation to a data breach incident reported by The Hong Kong Ballet Limited (HKB).

The investigation arose from a data breach notification submitted by HKB to the PCPD on 16 October 2023, reporting that HKB suffered from a ransomware attack on 29 September 2023, which affected four physical servers of the information systems of HKB (the Incident).

The investigation revealed that the initial intrusion into HKB's network took place on 15 September 2023. As the operating software of a server (the Server) was outdated at the time of the Incident, the hacker successfully gained access to HKB's network by exploiting the vulnerabilities in the Server. Subsequently, the hacker employed various malicious tools and programmes, including credential dumping tools and remote access tools, to acquire passwords of the information technology (IT) administrator and user accounts and to obtain information about the network and details of computers connected to the network. The information obtained was used by the hacker to carry out lateral movement in HKB's network.

On 17 September 2023, the hacker employed a domain administrator account to deploy "LockBit" ransomware on HKB's information systems, which resulted in the encryption of files and exfiltration of data and files stored therein.

The investigation also found that, HKB was unable to determine the data contained in the encrypted files. Based on HKB's estimation, the number of the affected individuals might be 37,840, which included HKB's staff members, job applicants, ticket subscribers, guest artists, activity participants, donors, sponsors and vendors. The personal data affected included names, HKID Card numbers, passport numbers, photographs, dates of birth, addresses, email addresses, telephone numbers, health information, bank account numbers and/or credit card numbers (without CVV), employment information and academic information.

Investigation Findings

Having considered the circumstances of the Incident and the information obtained during the investigation, the Privacy Commissioner for Personal Data (Privacy Commissioner), Ms Ada CHUNG Lai-ling, found that the following deficiencies of HKB were the contributing factors of the occurrence of the Incident:-

1. **Outdated operating software of the Server**, which was vulnerable to multiple critical remote code execution vulnerabilities. Moreover, HKB did not have any policy or procedures on the patching or update of its servers, which revealed a glaring deficiency in HKB's regular patching and updating practices;

2. **Unnecessary exposure of the Server to the Internet during system migration performed by the service vendor**, thereby significantly increasing the risk of cyberattacks. This led to the Server being exploited by the hacker in the Incident;

3. **Lack of monitoring of the data security measures adopted by the service vendor,** resulting in HKB's failure to ensure that the vendor performed timely updates and implemented adequate security measures to safeguard the personal data stored in the information systems. Further, there was no requirement on safeguarding data security in the relevant service contract signed with the service vendor; and

4. **Absence of security assessments and security audits of the information systems**, which resulted in HKB's inability to identify the vulnerabilities in the Server, and increased the risks of attacks on its information systems.

The Commissioner's Decision

Based on the above, the Privacy Commissioner, Ms Ada CHUNG Lai-ling, found that HKB had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening the requirements concerning security of personal data under Data Protection Principle 4(1) of the Personal Data (Privacy) Ordinance.

The Privacy Commissioner has served an Enforcement Notice on HKB, directing it to take measures to remedy the contravention and prevent similar recurrence of the contravention.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
8 August 2024