Jin Takeichi

From: [redacted]
Sent: Monday, January 26, 2026 2:45 PM
To: [redacted]
Subject: Take One Systems Ransomware Event

Hello.

We are writing to inform you of a security incident involving our internal server environment and to provide a transparent account of the actions we have taken to secure your data.

1. Event Overview

On 2025-01-25 approximately 6:00am, we identified a ransomware attack that impacted a segment of our local server infrastructure in our Gardena office. An internal server at the Take One Systems office in Gardena was encrypted by ransomware and rendered inaccessible. These servers are used primarily for our internal business operations. Immediately upon detection, we disconnected the network to prevent the further spread of the infection.

2. Actions Taken & Status

Upon discovery, we took the following immediate steps:

- We had blocked any external access to our Gardena office network, and then internally, physically disconnected all devices. And then, we had successfully restored all impacted systems using our nightly backup from 2025-01-24, by 2025-01-25 13:00. Our internal system's and our cloud account passwords had been changed by 17:00, and any external access remains blocked for now. Services have been returned to normal operation, but we continue to monitor and investigate.

- Our cloud environment, including our Microsoft 365 Tenant, Azure, Google Workspace, and our Data Centers that hosts webservers, application servers, and email server, were not afffected. We had thouroughly investigated for unauthorized access and outage, but no apparent affect identified. We had changed passwords for all admin passwords and verified that MFA is active. We'll continue to monitor and investigate.

3. Regarding the impact on AKC

The files stored on our servers included documents necessary for us to provide IT support to your company. The files related to AKC we had stored, were mostly estimates and invoices, and PC setup records, admin passwords, and some of Microsoft 365 account passwords. While we cannot confirm whether the files were stolen and retained by hacker, or if they will be made public, but we will implement all possible measures to prevent any harm.

Below, is what we recognized as critical , and the actions taken.

a) Microsoft 365 Admin account password
Microsoft 365 Admin account was recorded in our file server, but the account is protected with MFA.
We had already changed password. We will assume this is contained.

b) Domain registration Admin password
We had domain admin password for koyucorp.com , on our file server.
We had already changed password last night, and activated MFA.

c) Microsoft 365 user login passwords
We normally don't store user's password, as they should primarily be maintained by end-users,
but we found some notes that we kept when we created new accounts, which was saved on our server.
Those passwords may have potentially been leaked and hacker may attempt to use it.
Therefore, we must suggest you (everyone at Koyu , excluding EagleVines) to change their Microsoft 365 password.
Can you ask each one, to https://myaccount.microsoft.com/ , and change password ? `

d) PC Setup Notes
When we configure and setup PCs for Koyu, we keep the records, including the password created.
Recently, Chiaki's PC, Guest PCs for Hotels, were recorded in such manner and was kept in our file server that had been hacked.
However, hacker can't access someone's PC just by obtaining PC login password, unless he/she have physical access, therefore risk level is low.

e) Trendmicro and Avanan Security
Trendmicro (PC security) and Avanan (Email Phishing filter) were both maintained by our Login account, which was unaffected by ransomware incident.
We had already changed our passwords and verified MFA is active.

f) Intuit Quickbooks Login
We had a Intuit Account (admin@koyucorp.com) which can be used to access Quickbooks Online, saved in our file server.

We had changed password and verified that MFA is active.

At this moment, above concludes my report for now.
At this time, there is no further action required on your part regarding the administrative password that we used.

Please instruct users to change passwords, and if possible, setup MFA by SMS or Smartphone App.

We will provide as much support as possible, so please let us know.   Should you have any questions, please contact us and we will respond as promptly as possible.

Over the next few days, while addressing this matter, responses to non-urgent inquiries may be delayed. However, we are constantly monitoring emails and phone calls.

We take this situation very seriously and are committed to further strengthening our management systems. We sincerely appreciate your understanding and cooperation.

Jin Takeichi
竹市 仁
Take One Systems, Inc.
Email: jin@takeone.net
[redacted]