Justice Department contains ransomware attack

The Department of Justice and Constitutional Development says it has made strides in recovery after its IT systems experienced a ransomware attack last month.

Source: © Maksim Kabakou – 123RF.com

During the attack, the department's IT systems were encrypted and unavailable to officials and the public and affecting all of the department's electronic systems.

The department now says the spread of the malware – or malicious software – has been contained and some online services have been restored.

According to the department, a team comprising of departmental officials, industry specialists and advisors from organs of State is working to ensure as little disruption as possible to child maintenance payments in particular.

Personal information potentially compromised in ransomware attack, says Justice dept

6 Oct 2021

"Another critical area that has been given high priority is the electronic recording of court proceedings to ensure that courts are able to operate as normal. Most of the recordings are intact, and able to sync back to the central repository.

“Where courts are still experiencing challenges, a special capacity has been deployed to attend to queries on a case-by-case basis. The web portal that is used by transcribers to download court recordings for transcription purposes was successfully restored,” the department said in a statement.

Progress has also been made in the restoration on its Integrated Case Management System – an administration system used in the courts.

“Parts of the system are already accessible, such as curatorship, and the online portals used for historic searches. More work will be done in the next few days to complete the process of bringing back online functionality in respect of Trusts, Deceased Estates and Insolvencies, among others,” the Justice department said.

No ransom paid to alleged hackers - Department of Justice

21 Sep 2021

The department added that a high-level assessment on the 1,200 files containing personal information that may have been compromised during the attack has been finalised.

“The department has strengthened security measures to protect sensitive personal information under its custodianship. Measures include upgrading our ICT security infrastructure and ensuring more stringent access control electronic and physical,” it said.