CySecurity News - Latest Information Security and Hacking Incidents: Missile Supplier MBDA Breach Disclosed by CloudSEK

By CySecurity News, twitter.com/ehackernews

In July, a threat actor operating by the online alias Adrastea claimed to have breached MBDA. The threat actor describes itself as a team of independent cybersecurity experts and researchers.

According to Adrastea, they have taken 60 GB of sensitive data and discovered significant flaws in the organization's infrastructure. As per attackers, the stolen material includes details about the remaining workforce participating in military programs, business ventures, contract agreements, and correspondence with other businesses.

A new advisory about the suspected hacking campaign against MBDA has been published by security researchers at CloudSEK. The blog site, posted on Sunday, claimed that CloudSEK's researchers were successful in locating and decrypting the password-protected ZIP file holding the evidence for the data breach.

The hackers uploaded a post in which the password to unlock the file was mentioned. Two folders with the names 'MBDA' and 'NATO Diefsa' were included in the ZIP file.

The folder, according to the security professionals, contained files outlining the private personally identifiable information (PII) of MBDA's employees as well as numerous standard operating procedures (SOPs) supporting the need for NATO's Counter Intelligence to prevent threats related to terrorism, espionage, sabotage, and subversion (TESS).

The SOPs define NATO collection and plan functions, roles, and practices utilized in support of NATO operations and exercises. According to CloudSEK, "the SOPs also contain all IRM & CM (Intelligence Requirement Management and Collection Management) process activities that result in the successful and efficient execution of the intelligence cycle."

Internal drawings of missile system wiring diagrams, electrical schematic diagrams, and records of actions connecting the MBDA to the European Union's Ministry of Defence were also apparently included in the retrieved papers.

The cybersecurity firm made it clear that Adrastea's reputation as a threat actor is currently poor due to the numerous objections and concerns noted in the dark web forums where hackers purportedly posted the MBDA material.

Furthermore, as this is the group's first known activity, it is challenging to determine whether the material posted is accurate.
