GSD. Security - Suspected data breach

Article ID: KB0040802
Created: 2025-01-29 09:40:25
Updated: 2025-01-29 09:40:25
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/e26fbaa71bf90a5470dacaa3604bcb11', 'value': 'e26fbaa71bf90a5470dacaa3604bcb11'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/b4bec1bac3d716940acd3300150131f7', 'value': 'b4bec1bac3d716940acd3300150131f7'}

General Information:

Possible symptoms/errors:

User calls to reportRansomware with proper backup and without exfiltrationRansomware without proper backupRansomware with backup and without exfiltration in a hospitalRansomware without backup and with exfiltrationData Exfiltration ATTACK of job application data from a websiteExfiltration of hashed password from a websiteCredential stuffing attack on a banking websiteExfiltration of business data by an employee - INTERNAL HUMAN RISK SOURCEAccidental transmission of data to a trusted third partyStolen device storing encrypted personal dataStolen device storing non-encrypted personal dataPostal mail mistake - Highly confidential personal data sent by mail by mistakePersonal data sent by mail by mistakeIdentity theftEmail exfiltration

Alternative names of the system:

N/A

IMPORTANT NOTICE:

Priority of incidents related to scams can be no lower than P3Always begin handling scam attempts by resetting user's Active Directory password

Solution:

1. Reset the user's Active Directory password. Follow GSD. Windows - AD User Account Password Reset (KB0016151)

2. Create an incident containing all available information regarding the scam attempt:

What were the details of the attempt? What was the user told/presented with?Has the user provided any data/downloaded or installed any software/clicked on any links?Any related e-mails or phone numbersContact information of the userTime of the attempt

Assign the incident to Int_WW_CyberThreatDetection_SecaaS_SLS_FDT and send an email to CERT@Fresenius.com containing the ticket number and all relevant information.

3. Since this is a case of a suspected IT Security or Data Protection Incident affecting Capgemini as data processor, GSD must report the incident over a separate portal to inform Capgemini CISO & DPO organization of the potential occurrence of a security incident or personal data incident.

Further instruction can be found here: https://capgemini.sharepoint.com/sites/fresenius_account/SitePages/GSD.-Security---Suspected-data-breach.aspx

Assignment Group:

Int_WW_CyberThreatDetection_SecaaS_SLS_FDTCERT@Fresenius.comDE, CIS Security Incidents

Ticket Creation:

Template: N/ACategorization:

Configuration Item: N/ACategory: N/ASubcategory: N/A

Important Links:

https://capgemini.sharepoint.com/sites/DE_CIS_ISMS/SitePages/Report-an-Incident.aspxhttps://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_enhttps://capgemini.sharepoint.com/sites/fresenius_account/SitePages/GSD.-Security---Suspected-data-breach.aspx