CNEXT SECURITY SERVICES · FINDINGS REPORT · ONE-OFF

Breach inspection findings report

CUSTOMER
Muster AG, Bern (fictional)

CASE
BI-2026-017, suspected account takeover in accounts

TRIGGER
Customer report of Monday, 2 November 2026, 08:10

RATING
Critical, confirmed by CNEXT

11	4	2	30 d
places inspected	findings with evidence	accounts affected	of logs available

When you receive this document: At the end of the first day of inspection, by email to the people in the alert plan.

Summary

The accounts department's account was signed into on Friday, 30 October 2026, at 14:52 from Lagos with a valid token that had been captured the day before through a fake sign-in page. The attacker created an inbox rule, registered an authenticator app on an unknown device and sent a payment request to three customers on Friday evening. A second account shows the same sign-in page but no further trace. We found no mass downloads or sharing in SharePoint.

Findings

PLACE	FINDING	EVIDENCE	LEVEL
Sign-ins	Sign-in from Lagos with a valid token, device unknown, multifactor check skipped (token replayed)	Sign-in log, export 01	**Critical**
Mailbox	Inbox rule “.”, moves replies containing “invoice” to RSS Feeds and marks them read	Rule export 02	**Critical**
Sign-in methods	Authenticator app registered on an Android device, Friday 14:58	Audit log, export 03	**High**
Outbound mail	Payment request with new bank details to three customers, Friday 17:20	Message trace, export 04	**High**
Apps and roles	No new consent, no role change, no change to conditional access	Exports 05 to 08	**Low**
Files	No mass downloads, no new sharing links in SharePoint and OneDrive	Export 09	**Low**

Timeline

- Thu 29 Oct, 16:41: employee opens the link of a mail “Release invoice” and signs in on a fake page; the token is captured.
- Fri 30 Oct, 14:52: sign-in from Lagos with the token; 14:55 inbox rule; 14:58 authenticator app; 17:20 payment request to three customers.
- Mon 2 Nov, 08:10: customer reports the mail; 09:30 inspection starts; 10:15 logs exported; 10:20 sessions revoked.

Next steps

The containment measures in the log are implemented. Please inform the three customers today with the template in the evidence folder; the handover report follows on Wednesday.

Every name, system and number in this document is invented. Your report contains your environment on the day of the check.