CNEXT SECURITY SERVICES · HANDOVER REPORT · ONE-OFF

Handover report

CUSTOMER
Muster AG, Bern (fictional)

CASE
BI-2026-017, account takeover in accounts

DURATION
29 October 2026, 16:41 to 2 November 2026, 16:10

OUTCOME
Attacker locked out, no data exfiltration found

4	3	0	5
days of access	customers informed	reports to authorities needed	measures for the coming weeks

When you receive this document: Within a week of completing the inspection.

Summary

The attacker came through a fake sign-in page that captured the accounts department's token and bypassed multifactor authentication. They had four days of access to one mailbox, sent a payment request and prepared a return through an authenticator app. No customer paid. According to our check no personal data left the system; a report to the FDPIC was not indicated, and Muster AG does not fall under the reporting duty for critical infrastructures.

Gaps used and doors closed

GAP	WHAT THE ATTACKER DID	CLOSED BY
Token phishing	Sign-in through a fake page, token replayed	Sign-in only from compliant devices, shorter sign-in frequency
Sign-in method	Registered an authenticator app of their own	Registration of new methods only from a trusted location
Inbox rule	Hid the replies	Alert on new rules, external forwarding blocked
Phishing mail	Link “Release invoice” to accounts	Safe Links and Safe Attachments for everyone, domain blocked

Measures for the coming weeks

- Introduce passkeys for accounts, purchasing and management, then for everyone; owner: Muster AG IT with CNEXT.
- Payment approvals with the four-eyes principle outside mail, with a call-back on new bank details; owner: finance.
- Route sign-in and audit logs continuously to a storage account so the traces reach further than 30 days; owner: CNEXT.
- Run the checklist of this inspection monthly against the previous month; owner: CNEXT, if the continuous inspection is booked.
- Short training for everyone with the real example of this mail; owner: Muster AG with a template from CNEXT.

Next steps

This report goes to management and the IT lead. The evidence folder stays with you; we delete our copy after the agreed period.

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