Underretning om hackerangreb på KOMiTs softwareløsninger

KOMiT<no-reply@komit.nu>

Underretning om hackerangreb på KOMiTs softwareløsninger
Afsender: KOMiT A.m.b.a. 20.08.2025

Introduktion

Formålet med denne henvendelse er at informere dig/jer om, at en eller flere personer har hacket sig ind på KOMiTs it-systemer. KOMiT er et administrationssystem, som mange i den frie skoleverden anvender. Hackerangrebet kan desværre have berørt dine og/eller dine børns personoplysninger i forbindelse med kontakt til din/jeres skole.
Du har modtaget denne mail fra KOMiT a.m.b.a., fordi du har en relation til en organisation indenfor den frie skoleverden – fx en efterskole, friskole, højskole, fri-fagskole eller privatskole – og har anvendt KOMiTs it-løsninger. Det kan eksempelvis være i forbindelse med tilmelding til en skole.

Hændelsesforløb

Mandag den 11. august 2025 blev der identificeret et hackerangreb mod KOMiTs it-systemer.

De berørte systemer omfatter blandt andet webtilmeldingsservice, multimail og webkarakterer, som administrationen anvender i forbindelse med blandt andet indmeldelse på skolen, udsendelse af mails, mv.

En formodet gerningsperson har tiltvunget sig adgang til en server for at kopiere og stjæle personoplysninger. KOMiT lukkede straks de berørte servere ned for at forhindre yderligere adgang til data og datatab. Vi har involveret vores forsikringsselskab, der har stillet tekniske eksperter til rådighed, og hændelsen er tillige blevet anmeldt til politiet og Datatilsynet.

Berørte oplysninger

De berørte data omfatter:
· Navne på elever/kursist og pårørende samt relationer
· Adresser
· Telefonnummer
· CPR-nummer
· E-mailadresse
· Øvrige oplysninger (fx ønsker til optagelse på særlige linjer på høj- eller efterskoler)

De konkrete data, der er berørt, afhænger af, hvilke oplysninger hver enkelt forældre/kursist/elev har opgivet.

Der er på nuværende tidspunkt ikke konstateret spredning af de stjålne data til tredjepart. Den formodede gerningsperson har øjensynlig ikke intentioner om at sælge eller dele informationerne, men derimod at sætte fokus på eventuelle sikkerhedshuller i de nævnte

systemer. Vi kan dog ikke udelukke, at gerningspersonen efterfølgende vil sælge eller dele informationerne med andre.

Konsekvenser

Hændelsen kan potentielt have konsekvenser for dig og dine personoplysninger i form af misbrug af dine personoplysninger. Misbrug kan bl.a. omfatte identitetstyveri, oprettelse af aftaler, lån eller kreditter i dit navn. Du kan også blive udsat for at blive kontaktet af en potentiel uautoriseret person, der vil forsøge at lokke yderligere oplysninger ud af dig eller presse dig til bestemte handlinger på baggrund af dine personoplysninger.

Nedenfor har vi angivet en række anbefalinger til, hvad du kan gøre for at beskytte dig selv og dine personoplysninger, hvis nogle af de ovenstående konsekvenser opstår.

Anbefalinger – sådan beskytter du dig

KOMiT anbefaler, at du som berørt part er særligt opmærksom og iværksætter følgende:
1. Vælg altid stærke og unikke kodeord og aktiver gerne to-faktor-godkendelse, hvis muligt.
2. Vær opmærksom på uventede e-mails eller SMS'er med links eller anmodninger om personlige oplysninger (phishing-forsøg).
3. Overvej at tilmelde dig en kreditadvarsel hos kreditoplysningsbureauer (fx Experian eller Debitor Registret) for at mindske risikoen for misbrug af dine oplysninger.

KOMiT opfordrer til at følge den rådgivning der findes på www.sikkerdigital.dk.

Foranstaltninger fra KOMiTs side

KOMiT har:
· Sikret de berørte systemer og lukket adgangen
· Påbegyndt en intern undersøgelse og gennemført tekniske opdateringer
· Igangsat yderligere sikkerhedstiltag for at forhindre gentagelser
· Anmeldt hændelsen til Datatilsynet og politiet
· Anmeldt til vores cybersforsikring, der har stillet eksperter i håndtering af sikkerhedshændelser til rådighed

KOMiT er meget kede af situationen og beklager den utryghed, som den kan give anledning til. Vi vil i den kommende tid afdække alle forhold, og om nødvendigt foretage skridt med henblik på at undgå lignende hændelser i fremtiden.

Venlig hilsen

KOMiT a.m.b.a.
Anders Banke, direktør
info@komit.nu

Notification of Cyberattack on KOMiT's Software Solutions
Sender: KOMiT a.m.b.a. – August 20, 2025

Introduction

The purpose of this message is to inform you that one or more individuals have gained unauthorized access to KOMiT's IT systems. KOMiT is an administrative system used by many organizations within the independent school sector. Unfortunately, this cyberattack may have affected your and/or your children's personal data in connection with your school.

You are receiving this email from KOMiT a.m.b.a. because you are affiliated with an organization within the independent school sector – such as a continuation school, free school, folk high school, vocational free school, or private school – and have used KOMiT's IT solutions. This may, for example, have been in connection with school enrollment.

Incident Overview

On Monday, August 11, 2025, a cyberattack targeting KOMiT's IT systems was identified.

The affected systems include the web registration service, multimail, and web-based grading tools, which our administration uses for tasks such as school enrollment and email distribution.

A suspected perpetrator gained access to a server to copy and steal personal data. KOMiT immediately shut down the affected servers to prevent further access and data loss. We have involved our insurance provider, who has made technical experts available, and the incident has been reported to the police and the Danish Data Protection Agency.

Affected Data

The compromised data includes:
· Names of students/participants and relatives, including relationships
· Addresses
· Phone numbers
· CPR numbers (Danish personal ID numbers)
· Email addresses
· Other information (e.g., preferences for enrollment in specific programs at folk high schools or continuation schools)

The specific data affected depends on what each parent/participant/student has submitted.

At this time, there is no evidence that the stolen data has been shared with third parties. The suspected perpetrator does not appear to intend to sell or distribute the information, but rather to highlight potential security vulnerabilities in the mentioned systems. However, we cannot rule out that the perpetrator may subsequently sell or share the information with others.

Potential Consequences

This incident may have consequences for you and your personal data, including the risk of

misuse. Misuse may involve identity theft, unauthorized agreements, loans, or credit taken out in your name. You may also be contacted by unauthorized individuals attempting to extract further information or pressure you into certain actions based on your personal data.

Recommendations – How to Protect Yourself

KOMiT recommends that affected individuals take the following precautions:

Always use strong and unique passwords and enable two-factor authentication where possible.

Be cautious of unexpected emails or SMS messages containing links or requests for personal information (phishing attempts).

Consider registering a credit alert with credit agencies (e.g., Experian or Debitor Registret) to reduce the risk of data misuse.

Follow the guidance available at https://www.sikkerdigital.dk.

Measures Taken by KOMiT

KOMiT has:

· Secured the affected systems and closed access
· Initiated an internal investigation and implemented technical updates
· Launched additional security measures to prevent recurrence
· Reported the incident to the Danish Data Protection Agency and the police
· Activated our cyber insurance, which has provided experts in incident response

KOMiT deeply regrets the situation and the concern it may cause. We will continue to investigate all aspects of the incident and, if necessary, take further steps to prevent similar events in the future.

Kind regards,

KOMiT a.m.b.a.
Anders Banke, Director
info@komit.nu