Notification of Security Incident

SMS Teknik

Date: 23/08/2024

We are writing to you to inform you of a security incident which involves the text messages sent by Optima, Bankstaff. **There has been no compromise of RLDatix systems, however the backup systems of one of our sub-processors, SMS Teknik has been compromised. There is no ongoing compromise of SMS Teknik systems and no reason to stop using the SMS feature in the application**.

We respect the privacy of your information and value transparency. In order to safeguard you and your personal information, we are letting you know what happened.

Details of the event

These are the details which have been provided by SMS Teknik – translated into English (for Swedish customers the original Swedish should be provided.

****Important Information About Data Breach****
We want to inform you about a security incident that has affected our systems. Between August 12 and 19, 2024, backups of our database were exposed.
On August 19, we discovered that data had been deleted and replaced with a ransom note. We have not been able to confirm that any data has been leaked.

The information that may have been exposed includes communication logs, encrypted passwords, and customers' contact details. The security vulnerability has now been resolved, and we have reported the incident to the Swedish Authority for Privacy Protection and the police.

We regret this and will keep you updated on any developments. Below you will find a personal data incident report for further information.

****Personal Data Incident Report****

****Date and time when the incident was discovered:****
2024-08-19 15:45

****Description of the incident:****
During a disaster recovery exercise of SMS Teknik's operational environment on new hardware, a backup of SMS Teknik's database was exposed. The security flaw, which exposed the backups to outsiders on the Internet without any protection, was open from 2024-08-12 to 2024-08-19 16:20.

The incident was discovered on 2024-08-19 at 15:45 when the restored database during the exercise had its data deleted and replaced with a ransom note. In the message, the perpetrator demands a ransom within 48 hours and claims that the deleted data will be returned if the ransom is paid. The message threatens that the data will be published if the ransom is not paid.

****Description of actions taken, or proposed measures to address or mitigate the effects of the incident:****
As soon as the data breach was discovered, the security flaw was rectified, and the server on which the backup was restored was taken offline from the internet, and forensic work was initiated. Additionally, the breach has been reported to the Swedish Authority for Privacy Protection (IMY), reported to the police, and penetration experts have been hired to search for traces of potential leaks on the darknet.

****Did this involve personal data (Yes/No):****
Yes

****Date and time when the incident came to the attention of the data controller:****
2024-08-19 15:45

****Description of those affected:****
All customers of SMS Teknik.

****Number of data subjects affected:****
All corporate customers of SMS Teknik.

****Categories of personal data affected:****

- Communication logs
- Messages
- Encrypted usernames and passwords
- Contact details of SMS Teknik’s corporate customers
- Invoices of SMS Teknik’s corporate customers

****Number of personal data records affected:****
All SMS messages from SMS Teknik's corporate customers for the past three months, including mobile numbers and text for customers who have not requested anonymized data.

****Description of the likely consequences of the personal data incident:****
There is a risk that personal data in the form of mobile numbers and SMS messages may be exposed on the internet.

****Does the personal data incident pose a risk to the rights and freedoms of natural persons:****
No

****Date and time when the registered data subjects were informed about the incident:****
In conjunction with this information.

****Date and time when the Swedish Authority for Privacy Protection was informed about the incident:****
2024-08-21 12:59

****Internal reference number communicated to the Swedish Authority for Privacy Protection:****
Not provided

****Case number with the Swedish Authority for Privacy Protection:****
IMY-2024-10549

Nature and extent of personal data involved

This could affect all customer employees who have been sent an SMS via one of these products in the last 3 months

- Optima
- Bankstaff

The following information is typically shared with SMS Teknik

- Mobile phone number
- Message content – typically rostering information but could be custom messages

Unauthorized Disclosure

It is possible that the information has been exposed to the internet.

Likely impact of incident

Mobile phone numbers and content of the messages exposed to the internet.
There has been no compromise of RLDatix systems, however the backup systems of one of our sub-processors, SMS Teknik has been compromised. There is no ongoing compromise of their systems and no reason to stop using the SMS feature in the application.

Steps we are taking to address the issue

We are taking this incident seriously; therefore, we have already taken the following steps:

- Commenced an investigation
- Although the SMS Teknik API usernames and passwords stolen were encrypted, we are working with SMS Teknik to take the extra step to reset the account details. **NB. This not the username and password used to access Optima or Bankstaff.**
  We are working hard to get as much information as possible from SMS Teknik to get updates on their investigation.

More information will be provided as we know more, and a report will be provided

Contact person within RLDatix

If would like more information about this incident or the steps we are taking to address it, please contact:

Data protection officer – June Lewis privacy@rldatix.com

Kind Regards
Tom Walker, CISO

Chicago
RLDatix Head Office

311 South Wacker Drive,
Suite 4900
Chicago, Illinois United States
60606
Tel. +1 312 505-9301

Toronto

1 Yonge Street
Suite 2300
Toronto, Ontario, Canada
M5E 1E5
Tel. +1 416 410-8456

Melbourne

Suite 4, Level 4
441 St Kilda Road
Melbourne VIC 3004
Tel. +61 (0)3 9534 4477

Richmond
European Head office

1 Church Road
Richmond, Greater London
TW9 2QE
UK
Tel. +44 (0)20 7355 5555

Stockholm

Box 30077
104 25 Stockholm
Visiting address:
Sankt Eriksgatan 46
112 34 Stockholm
Tel. +46 (0)8 50551800

Frankfurt

Taunusanlage 8
60329 Frankfurt Am Main
Germany
Tel. +49 (0)69 247411440

Riyhad

7487 Khalid Ibn Al Walid
Qurtubah, Riyadh
Riyadh 13245 2218
Kingdom of Saudi Arabia.

For full list of regional offices visit our website