Open newsletter in browser

publica

Update on the cyber attack

Cyber attack on software supplier: what we know, and what we don’t

Dear

We are writing again to update you on the cyber attack on our software supplier PK Softech AG. We now know more about what happened. At the same time, some important questions remain unanswered. Here, we explain what we know today, what is still under investigation, and what it all means for you.

You can find the latest information on our dedicated page. Cyber attack on software supplier | PUBLICA

Why are you receiving this communication from uk@publica.ch?
The uk@publica.ch e-mail address is managed by our Corporate Communications team. We are using this address to inform you about the cyber attack.

Are your personal data affected?
Unfortunately, we are not yet in a position to say. We do not currently have confirmed information about which data were actually leaked, whose data they are, and how many people are affected. Right now, the specialists are evaluating these data sets. This is complex and takes time.
Data relating to active members, pension recipients and former active members of Publica may be affected. These include names, addresses, dates of birth, OASI numbers, telephone numbers, e-mail addresses and information about occupational pensions. In the case of pension recipients, the IBAN may also be affected.
This is currently being investigated. As soon as we have established which individuals are affected, we will notify them directly.

Are your pension assets and pension safe?
Yes. Publica’s systems are not affected by the cyber attack. Operations are running as normal. Your pension assets are safe and pensions are being paid as usual.

What happened?
At the end of September 2026, our software supplier fell victim to what is known as a ransomware attack. The attack was aimed at the supplier, and not directly at Publica. Other pension funds are also affected by the cyber incident.

What is a ransomware attack?
In a ransomware attack, cyber criminals use malware to penetrate a computer system, for example by sending fake e-mails or exploiting security vulnerabilities.

They encrypt data and make it impossible to access them. They then demand a ransom to release the data, and may for example threaten to publish stolen data. Even if the ransom is paid, there is no guarantee that the data will be restored.
Not every attack is carried out in the same way. Sometimes data are encrypted, sometimes they are stolen, and sometimes both.
The hacker group Akira is being linked to the attack. The National Cyber Security Centre (NCSC) has information about how this group operates: Cybercrime: The AKIRA group steps up its activities

What happened at the software supplier?
Investigations are still ongoing, and for reasons connected to this, Publica is not able to publish all information. Essentially, however, we must assume that data were leaked from the software supplier. Efforts are continuing, to establish whether and to what extent personal data from Publica were among them. It is also possible that we will never know with certainty whether the personal data of active members and pension recipients have been leaked.
Please therefore remain on your guard, and take the protective measures seriously.

Why did the software supplier have personal data?
PK Softech AG develops the software we use to manage our pensions. This is regularly refined and updated.
Tests are carried out before planned updates and new software releases, to check whether the applications and the various pension cases as well as special situations operate correctly. Data are also present at the software supplier for the purpose of these tests.
The software provider has confirmed that the old data in the test environment have been deleted.
The investigations are looking into which data may have been leaked.

Have data already turned up on the dark web?
As things stand, we have no indications that data from Publica have been published on the dark web.
That does not, however, mean that we can rule out data leakage. The situation is still being monitored. As soon as we have new information about this, we will let you know.

Was a ransom demand made, or is anybody being blackmailed?
In a ransomware attack, criminals often attempt to blackmail the victim into paying a ransom. We do not know whether ransom demands were made in connection with this attack, or whether organisations or individuals are being blackmailed. These questions are part of the ongoing investigations by the Office of the Attorney General.

Are suspicious e-mails or telephone calls linked to the cyber attack?
We are currently being asked about whether suspicious e-mails, text messages and telephone calls are linked to the cyber attack.
This is not necessarily the case. Criminals obtain contact details in a variety of ways. For example, they may exploit publicly accessible information or data from earlier leaks, or they may send fraudulent messages to multiple recipients.
Therefore, if you receive a suspicious message, this does not automatically mean that your data have been leaked during the current cyber attack. Conversely, we are not at present able to rule out a connection.

How can you protect yourself?
Please be on your guard, especially if you receive unexpected e-mails, text messages and telephone calls. Criminals may use personal information in order to appear trustworthy.

- Do not share any passwords or login details.
- Do not click on any suspicious links or open unexpected attachments.
- Exercise caution if anyone asks for personal details or bank information.
- Do not allow yourself to be pressured. If in doubt, ask the organisation concerned directly, using the contact details you already know. Make your family and friends aware of these risks.
- You can find more information about current scams and how to protect yourself on the website of the National Cyber Security Centre.

What is Publica doing?
We take the potential leaking of personal data extremely seriously, and we are working with the federal offices responsible to resolve the incident.
We filed a criminal complaint with the Office of the Attorney General on 15 October 2026.
Over recent years, we have strengthened our information security management system and implemented a number of measures to improve data protection. We are also reviewing our existing security measures in connection with the current incident.
Our priority is to resolve the incident and to provide the best possible protection and information to those who may be affected.

What happens next?
We understand that the unanswered questions are causing concern. You may also be angry that you still do not know whether your personal data are affected. We fully appreciate this.
The investigations are extensive and will take time. We want to provide you with as much information as we can. At the same time, we believe it is important to share only information that has been confirmed.
As soon as we know more, we will contact you again. If we find out that your personal data are affected, we will notify you directly.
You can always find the latest updates and answers to frequently asked questions on our dedicated page.

Kind regards,
Swiss Federal Pension Fund Publica

Swiss Federal Pension Fund Publica
Eigerstrasse 57, CH–3007 Bern

Publisher information Privacy policy
You are receiving this newsletter because we have a statutory duty to inform you. It is therefore not possible to unsubscribe.
Sent using mailXpert