Ouvrir la newsletter dans le navigateur

publica

Point de situation sur la cyberattaque

Cyberattaque contre un fournisseur de logiciel: ce que nous savons et ce que nous ignorons

Bonjour,

Nous souhaitons vous donner de nouvelles informations sur la cyberattaque dont a été victime notre fournisseur de logiciel PK Softech AG. Nous en savons désormais davantage sur ce qui s'est passé. Toutefois, des questions importantes restent ouvertes. Nous faisons ici le point sur les informations dont nous disposons à ce jour, les éléments qui restent à clarifier et les conséquences possibles pour vous.

Vous trouverez des informations actuelles sur notre page dédiée à cet incident: Cyberattaque contre un fournisseur de logiciel | PUBLICA

Pourquoi recevez-vous ce message depuis l'adresse uk@publica.ch?
L'adresse uk@publica.ch est gérée par notre équipe de la Communication d'entreprise. C'est par cette adresse que nous vous informons au sujet de la cyberattaque.

Vos données personnelles sont-elles concernées?
Nous ne pouvons malheureusement pas encore vous le dire. Nous ne savons pas encore avec certitude quelles données ont effectivement fuité, à quelles personnes elles appartiennent, ni combien de personnes sont concernées. Des spécialistes analysent actuellement ces données. Ce travail est complexe et prend du temps.
Les données susceptibles d'être concernées sont celles des personnes assurées, des bénéficiaires de rente et des anciennes personnes assurées de Publica. Il s'agit notamment des noms, adresses, dates de naissance, numéros AVS, numéros de téléphone et adresses électroniques, ainsi que d'informations relatives à la prévoyance professionnelle. Pour les bénéficiaires de rente, les numéros IBAN peuvent également être concernés.
Les investigations sont en cours. Dès que nous serons en mesure de déterminer quelles personnes sont concernées, nous les informerons directement.

Votre avoir de prévoyance et votre rente sont-ils en sécurité?
Oui. Les systèmes de Publica ne sont pas touchés par la cyberattaque. Les activités se poursuivent normalement. Votre avoir de prévoyance est en sécurité et votre rente est versée comme d'habitude.

Que s'est-il passé?
Fin septembre 2026, notre fournisseur de logiciel a été victime d'une attaque par rançongiciel (ransomware). L'attaque a visé le fournisseur de logiciel et n'était pas dirigée directement contre Publica. D'autres caisses de pensions sont également touchées par cet incident.

Qu'est-ce qu'une attaque par rançongiciel?
Lors d'une attaque par rançongiciel, des cybercriminels s'introduisent dans un système informatique au moyen d'un logiciel malveillant, par exemple par le biais de

faux e-mails ou de failles de sécurité. Ils chiffrent les données et les rendent ainsi inaccessibles. Ils exigent ensuite une rançon pour les débloquer et menacent par exemple de publier les données volées. Même si la rançon est payée, rien ne garantit que les données soient restituées.
Toutes les attaques ne se déroulent pas de la même manière. Parfois les données sont chiffrées, parfois elles sont volées, parfois les deux.
Le groupe de pirates informatiques Akira est associé à cette attaque. L'Office fédéral de la cybersécurité (OFCS) fournit des informations sur le mode opératoire de ce groupe: Cybercriminalité: Le groupe AKIRA intensifie ses activités

Que s'est-il passé chez le fournisseur de logiciel?
Des clarifications sont toujours en cours, et des raisons liées à la stratégie de l'enquête expliquent également pourquoi Publica ne peut pas publier toutes les informations. Toutefois, nous devons partir du principe que des données ont été dérobées chez le fournisseur de logiciel. La question de savoir si des données personnelles de Publica sont concernées, et dans quelle mesure, fait toujours l'objet d'investigations. Il est également possible que nous ne sachions jamais avec certitude si des données personnelles de personnes assurées et de bénéficiaires de rente ont fuité.
C'est pourquoi nous vous invitons à continuer de faire preuve de vigilance et à prendre les mesures de protection au sérieux.

Pourquoi le fournisseur de logiciels disposait-il de données personnelles?
PK Softech AG développe le logiciel utilisé pour la gestion de notre prévoyance. Ce logiciel est régulièrement développé, amélioré et mis à jour.
Avant l'introduction des améliorations prévues et des nouvelles versions du logiciel, appelées releases, des tests sont effectués. Ces tests permettent de vérifier que les applications fonctionnent correctement, y compris pour les différents cas de prévoyance et les situations particulières. Le fournisseur de logiciel disposait de données pour effectuer ces tests.
La suppression des anciennes données dans l'environnement de test nous a été confirmée par le fournisseur de logiciel.
Les vérifications en cours visent notamment à déterminer quelles données ont éventuellement fuité.

Les données ont-elles déjà été publiées sur le darkweb?
À l'heure actuelle, nous ne disposons d'aucun indice selon lequel des données de Publica auraient été publiées sur le darkweb.
Cela ne signifie toutefois pas que nous pouvons exclure une fuite de données. Nous suivons la situation en permanence et nous communiquerons dès que nous disposerons de nouvelles informations.

Une rançon a-t-elle été exigée ou des personnes font-elles l'objet de chantage?
Lors d'attaques par rançongiciel, les criminels tentent souvent d'extorquer une rançon. Nous ne savons pas si des demandes de rançon ont été formulées dans le cadre de cette attaque, ni si des organisations ou des personnes sont victimes de chantage. Ces questions font l'objet de l'enquête en cours menée par le Ministère public de la Confédération.

Les e-mails ou les appels suspects sont-ils liés à la cyberattaque?
Nous recevons des questions concernant un éventuel lien entre la cyberattaque et des e-mails, des SMS ou des appels suspects.
Un tel lien n'est pas nécessairement établi. En effet, les criminels peuvent obtenir des coordonnées par différents moyens. Ils utilisent, par exemple, des informations accessibles au public, des données issues de précédentes fuites de données ou envoient des messages frauduleux à un grand nombre de destinataires.
Ainsi, si vous recevez un message suspect, cela ne signifie pas automatiquement que vos données ont fuité dans le cadre de la cyberattaque actuelle. Inversement, nous ne pouvons pas non plus exclure, à ce stade, l'existence d'un lien.

Comment pouvez-vous vous protéger?
Veuillez continuer de faire preuve de vigilance, en particulier face aux e-mails, aux SMS et aux appels inattendus. Les criminels peuvent utiliser des informations personnelles pour inspirer confiance.

- Ne communiquez jamais vos mots de passe ni vos données d'accès.
- Ne cliquez pas sur des liens suspects et n'ouvrez pas les pièces jointes inattendues.
- Faites preuve de prudence si quelqu'un vous demande des données personnelles ou des informations bancaires.
- Ne vous laissez pas mettre sous pression. En cas de doute, contactez directement l'organisation concernée pour vérifier la situation. Utilisez pour ce faire les coordonnées dont vous disposez déjà. Sensibilisez également les membres de votre famille et vos connaissances à ces risques.
- Vous trouverez de plus amples informations sur les nouvelles formes d'escroquerie et sur la conduite à adopter sur le site de l'Office fédéral de la sécurité.

Que fait Publica?
Nous prenons la fuite de données personnelles très au sérieux. En collaboration avec les services fédéraux compétents, nous faisons tout pour faire la lumière sur cet incident.
Le 15 octobre 2026, nous avons déposé une plainte pénale auprès du Ministère public de la Confédération.
Ces dernières années, nous avons renforcé notre système de gestion de la sécurité de l'information et mis en œuvre différentes mesures visant à mieux protéger les données. Dans le cadre de l'incident actuel, nous réexaminons également les mesures de sécurité existantes.
Notre priorité est de faire toute la lumière sur cet incident, de protéger au mieux les personnes potentiellement concernées et de les tenir informées.

Et ensuite?
Nous comprenons que les questions sans réponse soient source d'inquiétude. Vous trouvez certainement irritant de ne toujours pas savoir si vos données personnelles sont concernées. Nous comprenons tout à fait ce sentiment.
Les vérifications sont approfondies et prennent du temps. Nous souhaitons vous informer de la manière la plus complète possible. En même temps, il nous tient à cœur de ne communiquer que des informations confirmées.
Dès que nous disposerons de nouveaux éléments, nous vous tiendrons informés. Si nous constatons que vos données personnelles sont concernées, nous vous en informerons directement.
Vous trouverez les dernières informations ainsi que les réponses aux questions fréquemment posées sur notre page consacrée à cet incident.

Meilleures salutations
Caisse fédérale de pensions Publica

Caisse fédérale de pensions Publica
Eigerstrasse 57, CH–3007 Berne

Editeur Protection des données
Vous recevez cette newsletter parce que nous avons une obligation légale d'information envers vous. Il n'est pas possible de se désinscrire.
Envoi avec mailXpert