Aprire la newsletter nel browser

publica

Aggiornamento sull’attacco informatico

Attacco informatico contro un fornitore di software: cosa è noto e cosa resta da chiarire

Buongiorno

vi aggiorniamo di nuovo sull’attacco informatico subito dal nostro fornitore di software PK Softech AG. Abbiamo raccolto nuove informazioni sull’accaduto. Restano tuttavia ancora importanti questioni da chiarire. Desideriamo illustrarvi cosa sappiamo oggi, quali aspetti sono ancora in fase di accertamento e quali sono le implicazioni per voi.

Informazioni attuali sono riportate anche nel nostro sito web. Attacco informatico contro un fornitore di software| PUBLICA

Perché ricevete questo messaggio da uk@publica.ch?
L'indirizzo e-mail uk@publica.ch è gestito dal nostro team Comunicazione aziendale. Attraverso questo indirizzo vi informiamo in merito all’attacco informatico.

I vostri dati personali sono interessati?
Al momento non siamo in grado di rispondere a questa domanda. Attualmente non sappiamo ancora con certezza quali dati siano effettivamente fuoriusciti, a quali persone si riferiscano e quante persone siano coinvolte. Le specialiste e gli specialisti stanno lavorando alla valutazione dei dati acquisiti. È un’operazione complessa che richiede tempo.
È possibile che siano coinvolti i dati di persone assicurate e beneficiarie di rendita di Publica, nonché di ex persone assicurate. Nello specifico si tratta, tra l’altro, di nomi, indirizzi, date di nascita, numeri AVS, numeri di telefono, indirizzi e-mail e informazioni relative alla previdenza professionale. Per le persone beneficiarie di rendita potrebbero essere interessati anche i numeri IBAN.
Le indagini sono in corso. Non appena saremo in grado di identificare le persone coinvolte, le informeremo direttamente.

Il vostro avere di previdenza e la vostra rendita sono al sicuro?
Sì. I sistemi di Publica sono non interessati dall’attacco informatico. L’attività prosegue normalmente. Il vostro avere di previdenza è al sicuro e le rendite vengono versate come di consueto.

Che cos’è successo?
A fine settembre 2026 il nostro fornitore di software è stato vittima di un cosiddetto attacco ransomware. L’attacco è avvenuto presso il fornitore di software e non era diretto contro Publica. L’incidente informatico ha coinvolto anche altre casse pensioni.

Che cos’è un attacco ransomware?
In un attacco ransomware i criminali si introducono in un sistema informatico tramite software dannosi, ad esempio attraverso e-mail contraffatte o sfruttando lacune di

sicurezza. Criptano i dati, rendendoli così inaccessibili. In seguito chiedono il pagamento di un riscatto per ripristinare l'accesso ai dati e minacciano ad esempio di pubblicare i dati sottratti. Anche se il riscatto venisse pagato, non vi è alcuna garanzia che i dati possano essere ripristinati.
Non tutti gli attacchi si svolgono allo stesso modo. In alcuni casi i dati vengono criptati, in altri sottratti e in altri ancora i dati vengono sia criptati che sottratti.
Il gruppo di hacker Akira è stato associato all'attacco. L'Ufficio federale della cibersicurezza (UFCS) fornisce informazioni sulle modalità operative di questo gruppo: Cibercriminalità: Il gruppo AKIRA intensifica le sue attività.

Che cosa è successo al fornitore di software?
Gli accertamenti sono tuttora in corso e per ragioni legate alle indagini Publica non può rendere pubbliche tutte le informazioni. Fondamentalmente dobbiamo, però, partire dal presupposto che vi sia stata una fuoriuscita di dati presso il fornitore del software. Si sta tuttora verificando se e in quale misura siano stati coinvolti dati personali di Publica. È anche possibile che non avremo mai la certezza se siano effettivamente fuoriusciti dati personali di persone assicurate e beneficiarie di rendita.
Pertanto, vi invitiamo a prestare la massima attenzione e a prendere sul serio le misure di protezione.

Perché il fornitore di software conservava dati personali?
PK Softech AG sviluppa il software utilizzato per la gestione della nostra previdenza. Il software viene ulteriormente sviluppato e aggiornato a cadenza regolare.
Prima di introdurre i perfezionamenti pianificati e nuove versioni del software, ovvero le cosiddette release, vengono effettuati test. Questi test servono a verificare che le applicazioni funzionino correttamente nei diversi casi previdenziali nonché nelle situazioni particolari. Per eseguire tali test, il fornitore di software disponeva anche di dati.
La cancellazione dei dati obsoleti nell'ambiente di test è stata confermata dal fornitore del software.
Quali dati possano essere fuoriusciti è oggetto delle indagini in corso.

Sono già emersi dati nel dark web?
Al momento non sussiste alcune indicazione che i dati di Publica siano stati pubblicati nel dark web.
Ciò non significa tuttavia che possiamo escludere una fuoriuscita di dati.
Continuiamo a monitorare la situazione. Non appena disporremo di nuovi elementi, vi informeremo.

È stato richiesto un riscatto o ci sono persone ricattate?
Negli attacchi ransomware, i criminali cercano spesso di estorcere denaro chiedendo il pagamento di un riscatto. Non sappiamo se in relazione a questo attacco siano state avanzate richieste di riscatto o se siano state ricattate organizzazioni o singole persone. Questi aspetti sono oggetto delle indagini tuttora in corso da parte del Ministero pubblico della Confederazione.

Le e-mail o chiamate sospette sono collegate all'attacco informatico?
Attualmente riceviamo domande in merito a possibili collegamenti tra e-mail, SMS o telefonate sospette e l'attacco informatico.
Tuttavia, non è detto che vi sia necessariamente un collegamento. I criminali informatici ottengono i dati di contatto in vari modi. Ad esempio utilizzano informazioni di dominio pubblico, dati provenienti da precedenti fughe di dati oppure inviano messaggi fraudolenti a numerosi destinatari.
Se ricevete un messaggio sospetto, non significa automaticamente che i vostri dati siano stati sottratti nell'ambito dell'attuale attacco informatico. D'altra parte, al momento non possiamo nemmeno escludere un collegamento.

Come potete proteggervi?
Vi preghiamo di prestare la massima attenzione, in particolare a e-mail, chiamate e SMS inaspettati. I criminali possono utilizzare dati personali per ispirare fiducia.

- Non comunicate mai password o dati di accesso.
- Non cliccate su link sospetti e non aprite allegati inattesi.
- Fate attenzione se qualcuno vi chiede dati personali o informazioni bancarie.
- Non lasciatevi mettere sotto pressione. In caso di dubbio, rivolgetevi direttamente all'organizzazione in questione. Avvaletevi dei recapiti già a vostra conoscenza. Sensibilizzate anche i vostri familiari e conoscenti in merito a questi rischi.
- Ulteriori informazioni sulle attuali truffe e sul comportamento corretto da adottare sono disponibili presso l'Ufficio federale della cibersicurezza (UFCS).

Che cosa fa Publica?
Prendiamo molto sul serio la possibile fuoriuscita di dati personali. Stiamo lavorando unitamente ai servizi competenti della Confederazione al fine di fare piena luce sull'accaduto.
Il 15 ottobre 2026 abbiamo presentato una denuncia penale al Ministero pubblico della Confederazione.
Negli ultimi anni abbiamo rafforzato il nostro sistema di gestione della sicurezza delle informazioni e adottato singole misure per migliorare la protezione dei dati. Anche in relazione all'incidente attuale, stiamo riesaminando le misure di sicurezza esistenti.
La nostra priorità è fare chiarezza sull'accaduto e proteggere e informare nel miglior modo possibile le persone potenzialmente coinvolte.

Come si procede ora?
Comprendiamo che le questioni ancora aperte possano generare incertezza. Forse vi infastidisce il fatto di non sapere ancora se i vostri dati personali siano stati coinvolti. Capiamo perfettamente questa preoccupazione.
Gli accertamenti sono complessi e richiedono tempo. Intendiamo fornirvi informazioni il più possibile complete. Al contempo, è però importante per noi comunicare soltanto informazioni verificate.
Non appena ne sapremo di più, provvederemo a informarvi nuovamente. Se dovessimo constatare che i vostri dati personali sono interessati, vi informeremo direttamente.
Trovate gli aggiornamenti e le risposte alle domande frequenti nel nostro sito web.

Cordiali saluti
Cassa pensioni della Confederazione Publica

Cassa pensioni della Confederazione Publica
Eigerstrasse 57, CH–3007 Berna

Impressum Protezione dei dati
Riceve questa newsletter perché abbiamo un obbligo legale d'informazione nei suoi confronti. Pertanto non è possibile disiscriversi.
Inviato con mailXpert