

informace o incidentu

Informace o bezpečnostním incidentu a doporučení k obezřetnosti

V tomto dokumentu naleznete základní informace o bezpečnostním incidentu souvisejícím s kybernetickým útokem na IT infrastrukturu Rentea penzijní společnosti, a.s. a doporučení ke zvýšené obezřetnosti.

Co se stalo

Dne 23. 8. 2026 zaznamenal náš dodavatel části technické infrastruktury kybernetický útok typu ransomware, který zasáhl i část IT infrastruktury naší společnosti **Rentea penzijní společnost, a.s.** Ihned po zjištění útoku jsme společně s dodavatelem a s pomocí externích bezpečnostních odborníků začali intenzivně pracovat na omezení dopadů incidentu a zabezpečení dotčeného prostředí. Věc jsme také oznámili Úřadu pro ochranu osobních údajů, České národní bance a prostřednictvím dodavatele Národnímu úřadu pro kybernetickou a informační bezpečnost. Dodavatel také podal trestní oznámení na neznámého pachatele.

Provoz společnosti Rentea penzijní společnost nebyl přerušen, jen v části činností omezen. V souvislosti s incidentem však bohužel došlo také k neoprávněnému přístupu k osobním údajům.

To nejdůležitější chceme říct hned na začátku: **kybernetický incident neznamená ztrátu Vašich úspor u Rentea. Vaše finanční prostředky jsou v bezpečí.**

Incident se týká IT infrastruktury a možného zpřístupnění některých osobních údajů. **Neznamená to, že by útočník získal Vaše prostředky na penzijním spoření nebo s nimi mohl volně nakládat.**

Není proto důvod v souvislosti s tímto incidentem své penzijní spoření rušit, vybírat prostředky nebo kvůli incidentu provádět změny smlouvy.

Jaké údaje mohly být dotčeny

V tuto chvíli stále probíhá podrobné vyhodnocování incidentu a nemáme s jistotou potvrzený přesný rozsah osobních údajů, které mohly být útočníkem získány. Z tohoto důvodu Vás preventivně informujeme o maximálním možném rozsahu údajů, které mohly být incidentem dotčeny:

- identifikační a kontaktní údaje Vás jako našeho klienta,
- identifikační a případně další osobní údaje jiných osob uvedených v souvislosti s Vaší smlouvou, například určených osob, zákonných zástupců či opatrovníků.
- údaje související se smlouvou a penzijním spořením,
- údaje a dokumentace poskytnuté při sjednání nebo v průběhu trvání smlouvy,
- případně další údaje, které byly součástí související klientské dokumentace.

Co to pro Vás prakticky znamená

Samotná znalost Vašich osobních nebo smluvních údajů **neumožňuje automaticky získat přístup k Vaším penězům, bankovnímu účtu nebo jiným zabezpečeným službám**. K takovému přístupu jsou standardně potřeba další přístupové či autorizační údaje.

Osobní údaje však mohou být zneužity například k tomu, aby podvodná komunikace působila věrohodněji. Někdo může znát Vaše jméno, kontaktní údaje nebo informace o smlouvě a vydávat se například za pracovníka Rentea, Vašeho finančního poradce, banku nebo jinou důvěryhodnou instituci.

Proto Vás prosíme především o **zvýšenou obezřetnost vůči neobvyklým telefonátům, emailům a SMS zprávám**.

Na co si nyní dát pozor

Doporučujeme dodržovat několik jednoduchých pravidel:

- **Nesdělujte nikomu hesla, PIN kódy ani jednorázové autorizační kódy.** Pokud Vás někdo o takový údaj požádá, komunikaci ukončete.
- **Nenechte se tlačit k rychlému rozhodnutí.** Typickým znakem podvodu bývá naléhání, že musíte okamžitě něco potvrdit, zaplatit nebo převést peníze.
- **Bud'te obezřetní i tehdy, když volající zná Vaše osobní údaje.** Znalost jména, data narození, smlouvy nebo jiných údajů sama o sobě nepotvrzuje, že skutečně komunikujete s Rentea, poradcem nebo bankou.
- **Neklikejte na neočekávané odkazy a neotevírejte podezřelé přílohy.** Přihlášení do klientského portálu Moje Rentea provádějte pouze přímo přes oficiální stránky Rentea.
- **Nepřevádějte peníze na základě telefonické, e-mailové nebo SMS výzvy,** kterou jste si nezávisle neověřili.
- Pokud se Vám cokoli nezdá, **ukončete komunikaci a kontaktujte nás znovu prostřednictvím oficiálních kontaktů Rentea nebo svého finančního poradce.**

Nejčastěji kladené otázky

1. Přišel/a jsem v důsledku útoku o peníze?

Ne. Vaše finanční prostředky u Rentea jsou v bezpečí. Kybernetický incident neznamená, že by došlo k odcizení Vašich úspor na penzijním spoření.

2. Může se útočník dostat k mým penězům jen díky získaným osobním údajům?

Samotná znalost osobních či smluvních údajů automatický přístup k Vaším prostředkům neumožňuje. Přístup k zabezpečeným službám standardně vyžaduje další autentizaci nebo autorizaci.

Přesto doporučujeme zvýšenou obezřetnost, protože získané údaje mohou být použity k vytvoření věrohodnějšího podvodného telefonátu, e-mailu nebo SMS.

3. Musím kvůli incidentu rušit nebo měnit své penzijní spoření?

Ne. V souvislosti se samotným incidentem není důvod penzijní spoření rušit, vybírat prostředky ani provádět změny smlouvy.

4. Musím si změnit heslo?

Pokud používáte stejné heslo i pro více různých služeb, doporučujeme z obecného bezpečnostního hlediska používat pro každou důležitou službu unikátní heslo a tam, kde je to možné, vícefaktorové ověření.

Nikdy však neměňte heslo prostřednictvím odkazu, který Vám nečekaně přijde e-mailem nebo SMS. Do portálu Rentea vstupujte přímo prostřednictvím oficiálních stránek a přihlásíte se pomocí bankovní identity.

5. Jak poznám, že mi skutečně volá Rentea?

Pokud máte jakoukoli pochybnost, **nemusíte pokračovat v hovoru**. Hovor ukončete a kontaktujte Rentea sami prostřednictvím oficiálního telefonního čísla nebo svého finančního poradce.

Buďte obezřetní zejména tehdy, pokud po Vás někdo požaduje heslo, PIN, autorizační kód, okamžitou platbu nebo převod peněz.

6. Volající o mně zná osobní údaje. Znamená to, že je opravdu z Rentea?

Ne nutně. Právě znalost skutečných údajů může být použita k tomu, aby podvodná komunikace působila důvěryhodně. Pokud máte pochybnost, komunikaci ukončete a ověřte si ji nezávisle přes oficiální kontakty.

7. Přišel mi e-mail nebo SMS od Rentea. Co mám dělat?

Pokud zprávu neočekáváte nebo Vás vyzývá k přihlášení, zadání údajů, platbě či rychlému jednání, doporučujeme na odkazy neklikat a zprávu si nejprve ověřit.

Bezpečnější je otevřít si stránky Rentea samostatně a přihlásit se do portálu přímo.

8. Musím si kvůli incidentu měnit občanský průkaz?

Samotný kybernetický incident automaticky neznamená, že je nutné měnit osobní doklady. Pokud bychom na základě dalšího šetření zjistili skutečnosti vyžadující další konkrétní opatření z Vaší strany, budeme Vás o nich informovat.

9. Co mám dělat, pokud zaznamenám podezřelý telefonát nebo zprávu?

Nic nepotvrzujte, nesdělujte přístupové ani autorizační údaje, neposílejte peníze a komunikaci ukončete. Následně si požadavek ověřte prostřednictvím oficiálních kontaktů Rentea nebo svého poradce.

Pokud jste již přístupové údaje nebo autorizační kód někomu poskytli, případně jste na základě podezřelé komunikace provedli platbu, kontaktujte bezodkladně příslušnou banku či poskytovatele dané služby.

10. Co pro ochranu klientů dělá Rentea?

Klienty, jejichž osobní údaje mohly být tímto incidentem dotčeny, průběžně informujeme individuální e-mailovou komunikací rozesílanou prostřednictvím skupiny Partners. Vzhledem k rozsahu incidentu může doručení oznámení probíhat i v následujících dnech. Situaci nadále aktivně řešíme a spolupracujeme s bezpečnostními odborníky, dohledovými orgány i orgány činnými v trestním řízení.

Jsme Vám k dispozici

Pokud máte jakékoli pochybnosti nebo jste zaznamenali podezřelou komunikaci související s Rentea, obraťte se na nás:

- **E-mail:** info@rentea.cz
- **Telefon:** +420 800 99 77 33

Ještě jednou se Vám za komplikace a nejistotu spojenou s touto situací omlouváme. Děkujeme za Vaši důvěru.

Rentea penzijní společnost, a.s.

Informace ke kybernetickému incidentu

Stav informací k 31. 8. 2026