CoffeeDesk

Oświadczenie Coffeedesk w sprawie ataku hakerskiego

Aktualizacja z dn. 30.11.2020 r.

Dział IT firmy potwierdził, że 28 listopada 2020 roku miał miejsce atak hakerski, w wyniku którego nieuprawniona osoba trzecia uzyskała dostęp do serwera, na którym przechowywane były dane osobowe klientów.

W efekcie działań cyberprzestępczych, strony internetowe www.coffeedesk.pl i www.coffeedesk.com przestały działać, a w konsekwencji nie funkcjonuje również system sklepu internetowego.

Co dokładnie się stało?

Padliśmy ofiarą ataku cyberprzestępczego polegającego na naruszeniu integralności naszej infrastruktury systemowej i włamaniu się na nasz serwer. Do czasu zakończenia śledztwa i weryfikacji nie możemy podawać więcej informacji tym zakresie.

Jakie dane zostały naruszone i w jaki sposób były przechowywane?

Wskutek włamania, osoba trzecia uzyskała dostęp do danych przechowywanych przez nas na serwerze, w tym w szczególności danych związanych z procesami zakupowymi. Dane były przez nas przechowywane w sposób zgodny z wymaganiami prawnymi i obowiązującymi standardami bezpieczeństwa na serwerach jednego z głównych Data Center na terenie Niemiec, będącego pod stałym monitoringiem.

Informujemy, że w wyniku nieuprawnionego dostępu do naszych serwerów, naruszone mogły zostać następujące dane:

- imiona i nazwisko;
- numer telefonu (komórkowego);
- adres e-mail;
- hasło (w formie zaszyfrowanej);
- adres fizyczny (np. zamieszkania, dostawy);
- numer rachunku bankowego - jeśli dokonywali Państwo zwrotu/reklamacji w naszym sklepie, wśród danych rozliczeniowych mógł się znaleźć numer Państwa rachunku bankowego. W takim przypadku prosimy o zachowanie szczególnej ostrożności i monitoring transakcji, a w razie odnotowania podejrzanej aktywności prosimy o kontakt z bankiem. Ważne: nie przetwarzaliśmy danych dotyczących Państwa kart płatniczych - wszystkie dane związane z obsługą płatności przetwarzali dostawcy usług płatniczych. Nie przetwarzaliśmy także Państwa numerów PESEL ani numerów dowodów osobistych, podwyższających ryzyko naruszenia Państwa praw i wolności,
- status klienta;
- historia zamówień (liczby i kwoty zakupów).

Jednocześnie należy podkreślić, że dane osobowe nie zostały utracone. Dzięki zapisaniu ich na aktualizowanej kopii zapasowej, dostęp do nich został niezwłocznie przywrócony.

Jakie działania podjęliśmy jako Coffeedesk na rzecz ochrony danych Klientów i przywrócenia działalności naszych stron internetowych?

Podjęliśmy wielokierunkowe działania zmierzające przede wszystkim do:

- **zatrzymania ataku** - w tym celu odcięliśmy wszelkie nasze zasoby od sieci i ograniczyliśmy do nich jakikolwiek dostęp,
- **weryfikacji skutków ataku** - w tym celu we współpracy ze specjalistycznymi firmami zajmującymi się cyberbezpieczeństwem, rozpoczęliśmy pełen audyt naszej struktury software i hardware,
- **zgłoszenia ataku** - w tym celu wraz z naszym działem prawnym i zewnętrznymi ekspertami przygotowaliśmy zgłoszenie do właściwych organów państwowych zgodnie z ich kompetencjami i obowiązującymi przepisami,
- **ponownego uruchomienia** - w tym celu, na podstawie zaleceń poaudytowych, wprowadzamy wszelkie niezbędne dodatkowe zabezpieczenia i przygotowujemy się do ponownego bezpiecznego uruchomienia naszych stron internetowych.

WAŻNA INFORMACJA: Po ponownym uruchomieniu naszej strony, aby móc się zalogować na swoje konto w Coffeedesk, ze względów bezpieczeństwa nie będą się Państwo mogli zalogować przy użyciu starego hasła - poprosimy o jego zmianę. W innym przypadku nie zostaną Państwo przepuszczeni przez system zabezpieczeń.

Przez cały czas zbieramy wszystkie pytania, które docierają do nas za pośrednictwem maili oraz mediów społecznościowych. Poniżej znajdziecie Państwo aktualne informacje oraz najczęściej powtarzające się pytania dotyczące bezpieczeństwa danych.

Jeżeli dowiecie się o próbie wykorzystania danych przez osobę nieuprawnioną lub jeżeli macie jakiekolwiek pytania albo chcecie przekazać nam dodatkowe informacje w związku z zaistniałym zdarzeniem, prosimy o kontakt pod adresem e-mail: sklep@coffeedesk.pl.

Zespół Coffeedesk

FAQ

1. Dlaczego strona Coffeedesk.pl nie działa?

Padaliśmy ofiarą ataku cyberprzestępczego polegającego na naruszeniu integralności naszej infrastruktury systemowej i włamaniu się na nasz serwer, w efekcie ataku, strony internetowe www.coffeedesk.pl i www.coffeedesk.com przestały działać, a w konsekwencji nie funkcjonuje również system sklepu internetowego.

2. **Kiedy wszystkie funkcjonalności strony www zostaną przywrócone?**

Robimy wszystko, aby jak najszybciej przywrócić funkcjonalności strony. Poinformujemy, jak tylko strona zostanie ponownie uruchomiona.

3. **Czy zamówienia, które zostały dokonane przed wystąpieniem problemów ze stroną zostaną zrealizowane?**

Tak, wszystkie zamówienia dokonane przed zdarzeniem zostaną zrealizowane.

4. **Jakie kroki może podjąć klient, aby zabezpieczyć swoje dane?**

Kluczowym działaniem jest prewencja, dlatego rekomendujemy zmianę haseł dostępu do poczty elektronicznej, bankowości online oraz mediów społecznościowych, jeżeli były identyczne lub podobne do haseł używanych w sklepie coffeedesk.pl. Prosimy o korzystanie z uwierzytelniania dwuetapowego tam, gdzie to możliwe.

Prosimy również o zachowanie ostrożności i nieotwieranie wiadomości od nieznanych i podejrzanych nadawców. Zapewniamy, że jako Coffeedesk nigdy nie poprosimy o podanie dodatkowych danych osobowych czy uzupełnienie opłaty za złożone zamówienie. Jeśli ktokolwiek otrzyma takie wiadomości, prosimy o zgłoszenie ich pod adres sklep@coffeedesk.pl.

5. **Czy znana jest tożsamość osób, które dokonały działania cyberprzestępczego? Do kogo trafiły dane osobowe klientów?**

Wszelkie informacje są przekazywane organom ścigania oraz nadzorczym. Ze względu na dobro postępowania nie możemy na tym etapie upubliczniać żadnych szczegółowych informacji. Jednocześnie zapewniamy, że nad sprawą pracuje zespół ekspertów zabezpieczających ślady włamania oraz audytujących procedury bezpieczeństwa.

6. **W jaki sposób wcześniej przechowywali Państwo dane i jak adresowane były kwestie bezpieczeństwa z tym związane?**

Bezpieczeństwo danych naszych klientów jest dla nas priorytetem. Wdrożyliśmy szereg zabezpieczeń i procedur. Sposób przechowywania danych oraz kwestie dotyczące bezpieczeństwa są realizowane zgodnie ze standardami wymaganymi przez przepisy obowiązującego prawa.

7. **Jakie konkretne działania zostały obecnie podjęte, aby zabezpieczyć dane klientów?**

Natychmiast został uruchomiony sztab kryzysowy, którego celem było m.in. zabezpieczenie danych. Zespół podjął szereg działań programistycznych mających na celu zabezpieczenie zarówno danych jak i serwerów. Na tym etapie, ze względów bezpieczeństwa, to są wszystkie informacje, które możemy przekazać.

8. **Jakie działania zostały obecnie podjęte, aby minimalizować ryzyko?**

Natychmiast został uruchomiony sztab kryzysowy, którego celem było m.in. zabezpieczenie danych. Zespół podjął szereg działań programistycznych mających na

celu zabezpieczenie zarówno danych jak i serwerów. Na tym etapie, ze względów bezpieczeństwa, to są wszystkie informacje, które możemy przekazać.

9. **W przypadku jakichkolwiek obaw, wątpliwości z kim mam się kontaktować? Gdzie mogę uzyskać więcej informacji?**

Wszystkie osoby, które mają obawy lub pytania prosimy o kontakt mailowy: sklep@coffeedesk.pl.

10. **Jakie dane klientów są przez Państwa przechowywane?**

Dane, które przechowujemy obejmują imię i nazwisko, numer telefonu komórkowego, adres e-mail, hasło w formie zaszyfrowanej, adres fizyczny dostawy, numer rachunku bankowego w przypadku osób, które dokonywały zwrotu towarów, status klienta, historia zamówień.

11. **Co z promocjami na Black Weekend? Czy będą przedłużone?**

Promocje Black Weekend będą przedłużone. Poinformujemy o nich już niebawem w oddzielnym komunikacie.

12. **Czy był to pierwszy tego typu atak dokonany na Państwa serwis?**

Jest to pierwsze tego typu zdarzenie.

13. **Czy poinformowali Państwo klientów o zaistniałej sytuacji?**

Jesteśmy w stałym kontakcie z naszymi klientami zarówno na naszych kanałach w mediach społecznościowych jak i za pomocą komunikatów e-mail. Będziemy na bieżąco aktualizować posiadane informacje.

14. **Czy zdarzenie zostało zgłoszone do odpowiednich służb zajmujących się ochroną danych osobowych?**

Zgodnie z obowiązującymi przepisami poinformowaliśmy Prezesa UODO.

15. **Czy dane mojej karty zostały wykradzione i powinienem ją zablokować?**

Coffedesk.pl nie przechowywał danych dotyczących kart. W bazie znajdowały się numery kont osób, które dokonały zwrotu towaru.

16. **Do jakich moich danych dostęp uzyskała osoba trzecia?**

W wyniku nieuprawnionego dostępu do serwera osoby trzecie potencjalnie mogą mieć dostęp do informacji obejmujących: imię i nazwisko, numer telefonu komórkowego, adres e-mail, hasło w formie zaszyfrowanej, adres fizyczny dostawy, numer rachunku bankowego w przypadku osób, które dokonywały zwrotu towarów, status klienta, historia zamówień.

17. **Co to dla mnie znaczy? Jakie to ma dla mnie konsekwencje?**

Potencjalnie nieuprawniony dostęp do wskazanych danych może ułatwić przeprowadzenie nielegalnych działań tj. uzyskaniu dostępu do innych kont użytkownika czy założenie konta internetowego.

18. Czy dane do mojego nr konta mogły być udostępnione?

W bazie znajdowały się tylko numery kont osób, które dokonywały zwrotu zakupionych towarów i do tych danych mogą mieć dostęp osoby trzecie.

19. Kiedy można spodziewać się wysyłki zamówień opatrzonych komentarzem?

Zamówienia opatrzone komentarzem nie zostały zrealizowane w czasie weekendu, ale są naszym priorytetem. W sprawie szczegółów ich realizacji będziemy kontaktować się indywidualnie.

20. Skąd mają Państwo ten adres e-mail?

Wszelkie dane pozyskaliśmy w sposób zgodny z prawem. W celach bezpieczeństwa prewencyjny komunikat przekazaliśmy do wszystkich osób, do których mieliśmy kontakt w naszej bazie danych. W celu uzyskania szczegółowych informacji prosimy o kontakt sklep@coffeedesk.pl

21. Dlaczego komunikacja pojawiła się w takim terminie?

Komunikaty i kontakt z klientami pojawił się natychmiast po potwierdzeniu zdarzenia i weryfikacji jego zakresu.

22. Czy otrzymaliście żądanie okupu?

Dla dobra prowadzonego śledztwa nie możemy przekazywać szczegółów zdarzenia.

23. Jakiego rodzaju był to atak?

Na tym etapie nie możemy przekazać żadnych szczegółowych informacji dla dobra prowadzonego śledztwa.

24. Co dokładnie się stało?

Padaliśmy ofiarą ataku cyberprzestępczego polegającego na naruszeniu integralności naszej infrastruktury systemowej i włamaniu się na nasz serwer. Do czasu zakończenia śledztwa i weryfikacji nie możemy podawać więcej informacji.

25. Jakie dane zostały naruszone i w jaki sposób były przechowywane?

Wskutek włamania się na serwer, osoba trzecia uzyskała dostęp do wszelkich danych przechowywanych przez nas na serwerze w tym w szczególności danych związanych z procesami zakupowymi. Dane były przez nas przechowywane w sposób zgodny z wymaganiami prawnymi, jak i obowiązującymi standardami bezpieczeństwa na serwerach jednego z głównych Data Center na terenie Niemiec, będącym pod stałym monitoringiem.

26. Jakie działania podjęła firma?

By chronić dane naszych klientów podjęliśmy szereg działań. Aby zatrzymać atak odcięliśmy wszelkie nasze zasoby od sieci i ograniczyliśmy do nich jakikolwiek dostęp. Zweryfikowaliśmy skutki ataku i w tym celu we współpracy ze specjalistycznymi firmami

zajmującymi się ochroną przed cyberprzestępczością, rozpoczęliśmy pełen audyt naszej struktury software i hardware. Nasz dział prawny wraz z zewnętrznymi ekspertami przygotował zgłoszenie ataku do właściwych organów zgodnie z ich kompetencjami i obowiązującymi przepisami. Ponadto na podstawie zaleceń poaudytowych, wprowadzamy wszelkie niezbędne dodatkowe zabezpieczenia i przygotowujemy się do ponownego bezpiecznego uruchomienia naszych stron internetowych.