CoffeeDesk

Podsumowanie zdarzenia dotyczącego naruszenia cyberbezpieczeństwa w Coffeedesk

Aktualizacja: 9 grudnia 2020 r., godz. 10:00

Zgodnie z zapowiedzią dzielimy się naszymi doświadczeniami z ataku cybernetycznego, którego padliśmy ofiarą. Publikując te informacje, mamy na uwadze fakt, że liczba ataków cybernetycznych stale rośnie i zdarzenia, które nas spotkały mogą dotknąć także innych. Ponieważ sami doświadczyliśmy celowego działania osób trzecich, to dziś już wiemy, na które obszary powinniśmy byli zwrócić jeszcze większą uwagę i które zabezpieczenia nie zadziałały. Zawsze dbamy o pełną transparentność tego, co robimy, dlatego też dzielimy się informacjami również i w tym zakresie. Wierzymy, że ta wiedza może pomóc innym. Jednocześnie, raz jeszcze prosimy naszych klientów o zgłaszanie nam wszystkich niepokojących zdarzeń pod adresem: sklep@coffeedesk.pl. Choć dotychczas żaden z otrzymanych sygnałów nie potwierdza udostępnienia danych przez hakerów, to każdy traktujemy bardzo poważnie i szczegółowo weryfikujemy.

Po pozyskaniu informacji o ataku, postępowaliśmy zgodnie z wytycznymi *Computer Security Incident Handling Guide* i zgodnie ze standardem NIST 800-61 przygotowaliśmy raport, który posłużył nam do analiz, sformułowania ustrukturyzowanych wniosków oraz wdrożenia działań naprawczych.

Przebieg zdarzenia

1. W sobotę, 28 listopada 2020 roku ok. godz. 01:00-01:30 w nocy, następującej po tzw. Black Friday doszło do awarii naszego systemu informatycznego, skutkiem czego przestały działać nasze strony internetowe: coffeedesk.pl oraz coffeedesk.com.

2. Pierwszą wiadomość o zdarzeniu powzięliśmy wewnętrznie z raportu usterki systemowej z działu przygotowywania przesyłek (magazynu) już w kilka minut po ataku.

3. Jeszcze w nocy z soboty na niedzielę (nad ranem) odzyskaliśmy dostęp do serwera, na który nastąpił atak. Natychmiast odcięliśmy dostęp do sieci. Na zaatakowanym serwerze znaleźliśmy informację, w której podpisana grupa hakerska zadeklarowała wydanie klucza dostępu do zaszyfrowanych przez złośliwe oprogramowanie danych po zrealizowaniu żądania okupu. Ustaliliśmy, że wszystkie znajdujące się na serwerze

pliki zostały skompresowane i zabezpieczone nieznanym nam hasłem. Potwierdziliśmy zatem, że miał miejsce atak hakerski. Ta inwazyjna zmiana struktury plików była bezpośrednią przyczyną unieruchomienia naszych stron internetowych i systemu sprzedażowego. Do danych na serwerze można było uzyskać dostęp tylko w wyniku działań inwazyjnych określonego typu, angażujących przełamanie zabezpieczeń i oprogramowanie ingerujące w integralność danych. Aby dokonać takiego ataku, należało posiadać wiedzę związaną z hostingiem aplikacji WWW i używaniem repozytoriów kodu.

4. Jeszcze w sobotę przed południem powołaliśmy wewnętrzny zespół kryzysowy oraz zespół ekspertów zewnętrznych, w tym specjalistów z zakresu cyberbezpieczeństwa, komunikacji oraz prawników. Połączone zespoły miały za zadanie przeprowadzić wewnętrzne dochodzenie, ocenić ryzyko związane ze zdarzeniem oraz przedstawić wnioski i rekomendacje w zakresie dalszych działań. Równolegle, nasi pracownicy monitorowali sytuację, odpowiadali na pytania klientów i opracowywali komunikację zgodnie z najlepszą wiedzą posiadaną w danym momencie. Sztab ten pracował non-stop, aż do ponownego, bezpiecznego uruchomienia systemów w poniedziałek 30 listopada.

5. Niezwłocznie po zweryfikowaniu zakresu zdarzenia poinformowaliśmy o nim osoby, których dane były dostępne w bazie Spółki. Wysyłkę wiadomości o zdarzeniu rozpoczęliśmy 29 listopada o godz. 3:00 w nocy. Następnie, w ciągu kolejnych 24 h wystosowaliśmy drugi, rozszerzony komunikat z zakresem danych, do których atakujący mógł uzyskać dostęp.

6. Dostępność danych przywróciliśmy po odtworzeniu z kopii zapasowej, co zrealizowaliśmy jeszcze w dniu 28 listopada 2020 roku, tj. w ciągu ok. 3 godzin od stwierdzenia naruszenia. Spółka nie zapłaciła okupu.

7. Nasze zabezpieczone już strony internetowe oraz system sprzedażowy uruchomiliśmy ponownie 30 listopada ok. godz. 13:00. Atak ransomware (zaszyfrowanie plików i żądanie okupu) polegał zatem przede wszystkim na naruszeniu dostępności danych. Odzyskaliśmy dostęp do danych. Choć hasła były przechowywane w postaci zahaszowanej, to ze względów bezpieczeństwa zresetowaliśmy hasła wszystkich użytkowników, którzy posiadają konto w naszym sklepie internetowym i wymusiliśmy zmianę haseł wszystkich użytkowników, którzy będą ponownie logować się do swojego konta.

8. Zgodnie z procedurami złożyliśmy zawiadomienie o popełnieniu przestępstwa oraz poinformowaliśmy Zespół CERT Polska (zespół reagowania na incydenty) przy instytucie badawczym NASK oraz Prezesa Urzędu Ochrony Danych Osobowych.

Co poszło nie tak?

Przeprowadzona przez nas analiza przyczyn źródłowych incydentu wskazała na to, że przełamanie zabezpieczeń było możliwe na skutek niewystarczających rozwiązań, z których wyciągamy wnioski. Zidentyfikowaliśmy następujące słabości systemu bezpieczeństwa:

- luki bezpieczeństwa w aplikacji webowej,
- usługi sieciowe działające z nadmiarowymi uprawnieniami,
- nieaktualne niektóre komponenty systemu,
- błędy konfiguracji systemu.

Analiza wpływu zdarzenia

Na skutek incydentu doszło do naruszenia poufności, integralności i dostępności systemu informatycznego i przetwarzanych przez nas danych, w tym danych osobowych naszych klientów. Zakres danych osobowych, które przetwarzaliśmy, był ograniczony. Nie przetwarzaliśmy danych dotyczących kart płatniczych i innych metod płatności klientów. W przypadku ograniczonej liczby klientów posiadaliśmy numery rachunków bankowych do zwrotu środków. Hasła przechowywane były w formie niejawnej, przy użyciu algorytmów maskujących treść (tzw. haszowanie) i nie były łatwo dostępne. Niemniej jednak z uwagi na ewentualność przeprowadzenia skutecznego ataku na zahashowane hasła, która techniczne jest możliwa oraz rekomendacje zespołu ekspertów, postanowiliśmy natychmiast zresetować hasła do kont wszystkich naszych klientów.

Co zrobiliśmy i co planujemy zrobić, żeby podnieść poziom bezpieczeństwa?

Natychmiast po stwierdzeniu naruszenia podjęliśmy wielokierunkowe działania zmierzające przede wszystkim do:

- **zatrzymania ataku** - odcięliśmy od sieci wszelkie zasoby Spółki i ograniczyliśmy do nich jakikolwiek dostęp,
- **weryfikacji skutków ataku** - we współpracy ze specjalistycznymi firmami zajmującymi się cyberbezpieczeństwem przeprowadziliśmy pełny audyt struktury software i hardware,
- **zgłoszenia ataku** - niezwłocznie zgłosiliśmy zdarzenie do organów ścigania, do CERT NASK i Prezesa Urzędu Ochrony Danych Osobowych,
- **ponownego uruchomienia** - na podstawie zaleceń poaudytowych, wprowadziliśmy wszelkie niezbędne dodatkowe zabezpieczenia i dopiero na tej podstawie ponownie uruchomiliśmy jej systemy informatyczne.

Dodatkowo, podjęliśmy obszerne działania komunikacyjne i techniczne zmierzające do zminimalizowania negatywnych skutków naruszeń, przede wszystkim poprzez bezpośrednie poinformowanie o zaistniałej sytuacji wszystkich podmiotów z bazy danych. Dla zwiększenia zasięgu komunikatów oraz pełnej transparentności, poinformowaliśmy także o zdarzeniu w naszych kanałach w mediach społecznościowych oraz udzieliliśmy informacji zainteresowanym mediom.

Zamierzamy kontynuować otwartość w komunikacji oraz reagować na wszelkie zgłoszone sytuacje, które niepokoją osoby, których dane dotyczą.

Od momentu zidentyfikowania incydentu i zrozumienia jego przyczyny, natychmiast uruchomiliśmy szereg działań w zakresie poprawy bezpieczeństwa systemu informatycznego i danych naszych klientów. Kluczowe działania, które już zrealizowaliśmy oraz które planujemy wdrożyć w kolejnych krokach, to:

- przegląd konfiguracji i skany bezpieczeństwa systemu oraz serwerów,
- ponowna instalacja i konfiguracja elementów architektury systemów informatycznych,
- wykonanie hardeningu konfiguracji pakietów oprogramowania wspomagającego aplikację oraz serwera, tj. wprowadzenie dalszych rygorystycznych zasad, kryteriów i warunków realizowania procesów informatycznych,
- wprowadzenie najnowocześniejszych metod szyfrowania danych i silniejszych metod hashowania haseł,
- przegląd kodu źródłowego aplikacji webowej oraz naprawa wykrytych podatności aplikacji systemu sprzedażowego,
- wzmocnienie mechanizmów kontroli dostępu do systemu informatycznego oraz wprowadzenie nowych środków technicznych i organizacyjnych w tym zakresie,
- rozszerzenie mechanizmów monitorowania dostępu do systemu informatycznego oraz zmian wprowadzanych konfiguracji z uwzględnieniem systemu automatycznych powiadomień,
- uruchomienie dodatkowych zabezpieczeń aplikacji webowej poprzez uruchomienie zapory aplikacyjnej oraz innych dodatkowych warstw zabezpieczeń.

Jednocześnie zastrzegamy, że ze względów bezpieczeństwa zdecydowaliśmy się nie udzielać szczegółowych informacji o technologiach stosowanych zabezpieczeń.

Jakie wyciągnęliśmy z tego wnioski?

Zdarzenie, które nas dotknęło, może dotknąć każdego. Bazując na dobrych praktykach oraz mając na uwadze wnioski z przeprowadzonej analizy i nasze własne doświadczenia, zdecydowaliśmy się podzielić rozwiązaniami, o których naszym zdaniem warto sobie co jakiś czas przypominać, jeśli chcemy ograniczyć ryzyko przeprowadzenia skutecznych ataków.

Chcesz wzmocnić ochronę przed atakiem?

1. Regularnie poddawaj testom bezpieczeństwa swoje systemy informatyczne i aplikacje webowe.
2. Natychmiast usuwaj luki bezpieczeństwa, które mogą ułatwić przeprowadzenie ataku.
3. Uruchamiaj usługi sieciowe z najniższym możliwym poziomem uprawnień.
4. Regularnie przeglądaj konta użytkowników i ich uprawnienia.
5. Regularnie instaluj aktualizacje systemów informatycznych.
6. Używaj silnych mechanizmów uwierzytelnienia i mocnych algorytmów hashujących do przechowywania haseł.
7. Przeglądaj konfigurację systemów informatycznych i dostosowuj ją do aktualnych trendów zagrożeń.
8. Wykonuj regularne kopie zapasowe systemów informatycznych i danych.
9. Zadbaj o skuteczny system monitorowania i ostrzegania o atakach.
10. Zadbaj o bezpieczeństwo swoje i swoich klientów, wyciągając wnioski z popełnionych błędów.