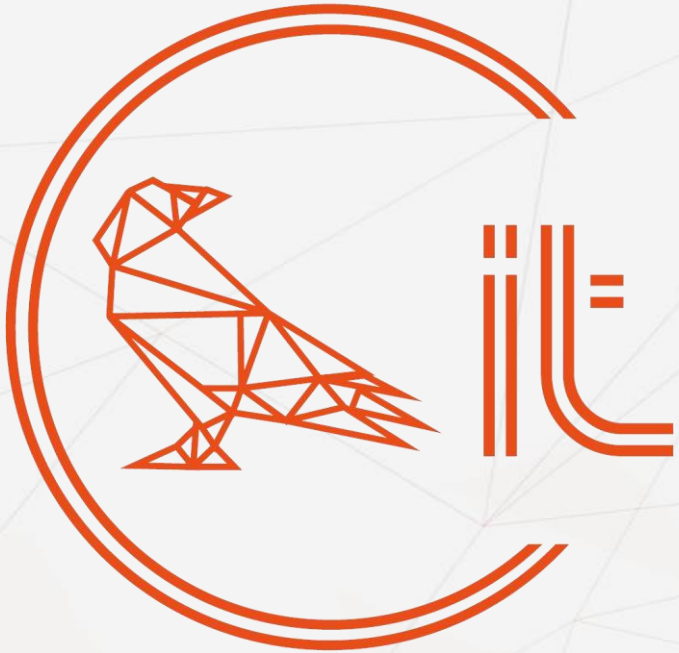

Consult it!

Edycja 2022

Wprowadzenie

Firma“Eklamot” - e-commerce ubrań.

Obecnie spółka posiada w swojej ofercie blisko 150 marek. Dodatkowo, Eklamot zapewnia bezpłatną dostawę i zwroty na terenie całej Polski oraz nie wymaga minimalnej kwoty zamówienia. Dzięki wysokim inwestycjom i systematycznemu rozwojowi, spółka jest obecnie jednym z liderów branży odzieżowej na rynku.

Miesiąc temu spółka mierzyła się z atakiem hakerskim wykorzystującym podatność systemu Magento (CVE-2022-24086). Dzięki wsparciu doradców z firmy konsultingowej, udało się zażegnać kryzys.

Obecnie firma przygotowuje się do wprowadzania zmian na każdym polu security. Mając na uwadze efektywność i szybkość pracy konsultantów, Zarząd Eklamot postanowił ponownie zwrócić się o pomoc.

Wprowadzenie

Jednym z zaniedbanych obszarów w spółce Eklamot jest architektura IT, która od lat była rozbudowywana bez stosowania odpowiednych praktyk bezpieczeństwa.

Obecna architektura składa się z dwóch środowisk: on-prem i cloud, na których działają aplikacje. Dodatkowo, firma pobiera dane z zewnętrznych firm, które wykorzystuje do działania aplikacji. W związku z postępującą pandemią, technicy z firmy Eklamot musieli udostępnić pracownikom możliwość pracy zdalnej, co również wymagało ingerowania w architekturę IT.

Dostępne dane (załączony plik)

Pracownicy firmy z działu IT przekazali do wglądu zestaw danych o głównych systemach w E-klamot, architekturze IT oraz instrukcjach procesów związanych z bezpieczeństwem (w tym nowa polityka haseł, która została zaktualizowana na początku kwietnia).

Dodatkowo, w ramach wstępnego audytu bezpieczeństwa jako jeden z głównych problemów pracownicy wszystkich działów Eklamot zgłosili spam oraz maile phishingowe. Jeden z takich maili dotarł również do księgowości i niestety, przelew do “klienta-przestępcy” został zrealizowany. Choć nie była to duża kwota - Zarząd wyznaczył 2 główne cele dla zespołu konsultantów:

Zadania dla konsultantów

1. Zaproponować zmiany w obecnych systemach, procesach i architekturze bezpieczeństwa, na podstawie dostarczonych przez dział IT materiałów.

2. Zaprojektować lub zaprogramować od zera nowy system, który zaadresuje problem Phishingu.

Terminy

08.05.2022 -> do godziny 23:59 należy przesłać raport przedstawiający analizę obecnego stanu bezpieczeństwa firmy Eklamot wraz z propozycją zmian. Dyrektor działu IT wraz ze swoim zespołem wybierze najlepsze ich zdaniem propozycje, kładąc nacisk na adekwatność i wdrażalność.

21.05.2022 -> 10 najlepszych zespołów będzie miało okazję zaprezentować swoje propozycje zmian w formie prezentacji przed Zarządem firmy Eklamot. Ostateczną decyzję w kwestii wyboru najlepszej oferty podejmie Zarząd. (Uwaga: Część prezentacyjna skierowana będzie do całego Zarządu – dlatego należy podsumować zmiany w sposób zrozumiały dla osób, które nie zajmują się bezpośrednio obszarem IT)