SOC-as-a-Service - bezpieczeństwo organizacji jako usługa

Dawid Jankowski

Security Operations Center

Każda firma, bez względu na swoją wielkość, powinna zadbać o bezpieczeństwo danych i systemów. Klienci zawsze liczą na poufność wrażliwych danych, kontraktów oraz wszelkich innych informacji, które mogą być szkodliwe w przypadku ich ujawnienia. Wyciek takich danych może być katastrofalny w skutkach wizerunkowych jak i finansowych. Do tego dochodzi również utrata wiarygodności, kontraktów, przerwa w produkcji oraz potencjalne bankructwo.

Od momentu wybuchu pandemii COVID-19, kiedy to większość firm przeszła na tryb pracy zdalnej, cyberataki znacząco się nasiliły. Według danych purplesec.us wzrost ten szacuje się na poziomie 600%, a roczne straty wynikające z cyberataków wynoszą 6 bilionów USD. Co więcej, trend ten nieustannie przyśpiesza. Szacuje się, że w roku 2025 liczby te się podwoją. Same ataki typu Ransomware (szyfrowanie komputera i wymuszenie okupu w celu odzyskania danych) są około 57-krotnie bardziej szkodliwe niż w roku 2015. Najczęstszym celem są małe i średnie przedsiębiorstwa z uwagi na brak lub niewystarczające zabezpieczenia.

Skuteczna obrona firmy przed atakami, wymaga utworzenia jednostki Security Operations Center. Składa się ona z ekspertów w dziedzinie cyberbezpieczeństwa, którzy nieustannie monitorują środowisko IT organizacji, aktualizują sygnatury ataków, systemy obronne oraz są świadomi nowych możliwości ataków i trendów.

Czym jest SOC-as-a-Service?

Tworzenie własnego zespołu SOC - jest nie tylko czasochłonne, ale i kosztowne. Ciągła rywalizacja o najlepszych specjalistów IT i nieustanne szkolenia wymagają dużych nakładów. Dzięki nowoczesnym rozwiązaniom chmurowym na rynku pojawiło się doskonałe rozwiązanie tego problemu.

SOC-as-a-Service to usługa, która działa jako wsparcie w wykrywaniu oraz reagowaniu na zagrożenia skierowane w przedsiębiorstwo. Systemy klienta są zabezpieczone przez ekspertów, którzy stale aktualizują wiedzę z zakresu cyberbezpieczeństwa.

Dlaczego wybrać SOC-as-a-Service zamiast własnego zespołu SOC

SOC-as-a-Service to naturalna ewolucja w sferze cyberbezpieczeństwa firmy. Jest odpowiedzią na narastające ryzyko związane z atakami na małe i średnie przedsiębiorstwa.

Zidentyfikować można cztery główne obszary związane z korzyściami rozwiązań SOCaaS:

1. **Istotnie zmniejszone ryzyko ataku.** W naszym narożniku są eksperci z dziedziny cyberbezpieczeństwa. Nieustannie monitorują systemy bezpieczeństwa, dzięki czemu ryzyko wycieku danych lub przerwy w produkcji jest znacznie mniejsze.

2. **Szybsza detekcja oraz czynności zapobiegawcze.** Podczas ataku czas gra kluczową rolę. Przykładowo, kiedy maszyna jest zainfekowana, trzeba ją natychmiast odizolować od reszty, a kiedy konto użytkownika zostało przechwycone, trzeba natychmiast zresetować hasło. Profesjonalne zespoły SOC posiadają sprawdzone predefiniowane automatyzacje w celu szybkiej i precyzyjnej reakcji na cyberzagrożenia. Przywrócenie produkcji potrafi być tak szybkie, że użytkownicy nie zauważą przerwy w dostawie.

3. **Skalowanie.** Kiedy firma rośnie, SOCaaS rośnie wraz z nią. Dla doświadczonego partnera i dostawcy SOCaaS podwojenie zasobów SOC nie stanowi żadnego problemu. Firmy te dysponują bowiem ogromną liczbą ekspertów gotowych do pracy 24/7.

4. **Mniejszy koszt.** SOCaaS eliminuje potrzeby utrzymania własnej jednostki, w tym: personelu, jego ciągłych szkoleń, biura, sprzętu czy licencji. Przykładowo do zapewnienia monitoringu 24/7 potrzebny jest kilkuosobowy zespół. Realnej pracy może być natomiast znacznie mniej. Dostawcy SOCaaS dysponują specjalistami efektywniej, dzieląc ich czas pomiędzy różnymi projektami. Szacuje się, że SOCaaS może kosztować nawet 90% mniej od tradycyjnej jednostki SOC w firmie.

Należy zatem zadać sobie pytanie czy wraz z nasilaniem się liczby ataków rok do roku nasze systemy obronne idą z nimi w parze, a nawet je wyprzedzają.