CASE STUDY

ATENDE

W trosce o bezpieczeństwo Narodowego Banku Polskiego

Branża: sektor finansowy

Cel projektu: zakup oraz wsparcie kluczowych urzadzeń sieciowych celem zapewnienia pełnej dostępności z zachowaniem maksymalnego poziomu bezpieczeństwa

Rozwiązanie:

NBP to najważniejsza instytucja finansowa w Polsce. Szczególnie istotne dla niej jest zachowanie ciągłości działania i bezawaryjne świadczenie usług wszystkim klientom. Wraz z rozwojem sieci, dodawaniem nowych procesów biznesowych oraz systemów i usług, konsekwencje oraz koszty ewentualnego przestoju w działaniu infrastruktury sieciowej znacznie rosną. Stąd NBP postawiło na gwarancję pełnej dostępności z zachowaniem maksymalnego poziomu bezpieczeństwa.

Atende dla tego klienta zrealizowało projekt polegający na zakupie oraz wsparciu kluczowych urządzeń sieciowych, a także na świadczeniu usług serwisu SMARTnet dla wszystkich urządzeń sieciowych Cisco będących w posiadaniu klienta.

Cisco SMARTnet to usługa wsparcia technicznego przeznaczona dla klientów, którzy potrzebują pełnego wsparcia technicznego w utrzymaniu oprogramowania Cisco oraz gwarancji wymiany sprzętu w przypadku awarii w czasie określonym przez SLA (ang. Service Level Aggrement).

Efekt:

Dzięki naszemu wsparciu klient zmniejszy ryzyko związane z błędami w oprogramowaniu, problemami z bezpieczeństwem, a także zwiększy ogólną sprawność operacji sieciowych i wydajności sieci. Dodatkowo, dzięki usługom Cisco Advanced Services, NBP będzie mogło lepiej identyfikować zagrożenia sieciowe oraz wykrywać luki bezpieczeństwa w otoczeniu sieciowym, zarządzaniu siecią oraz w procesach operacyjnych.

Od lat gwarantujemy bezpieczeństwo i spokój

Atende posiada wieloletnie doświadczenie w tworzeniu i utrzymaniu rozwiązań zapewniających bezpieczeństwo IT. Razem z naszymi Klientami poszukujemy optymalnego kompromisu pomiędzy minimalizacją ryzyka, wynikającego z korzystania z sieci komputerowych, a maksymalizacją wydajności pracy. Systemy te mogą być dodatkowo wyposażane w oprogramowanie do analizy zagrożeń na podstawie informacji zbieranych z poszczególnych urządzeń. Nasz proces odpowiedniego zabezpieczenia przed cyberatakami często obejmuje: audyt bezpieczeństwa IT, konsultacje w zakresie wyboru rozwiązań (od najlepszych globalnych dostawców po rozwiązania własne z Grupy Atende), wdrożenie przez najlepszych polskich inżynierów, monitoring i serwis w trybie 24/7.

Oferujemy:

- zapory ogniowe (firewall)
- systemy zabezpieczeń przed atakami typu DDoS, w tym autorski system redGuardian, której przeznaczeniem jest ochrona przed ostatnio szczególnie popularnymi atakami typu DDoS (distributed denial of service)
- systemy zabezpieczeń przed intruzami (ang. IPS — Intrusion Prevention Systems)
- systemy antywirusowe i antyspamowe
- systemy ochrony przed dostępem do niepożądanych treści webowych
- specjalistyczne oprogramowanie do analizy zagrożeń
- usługi odtwarzania awaryjnego, w tym kompleksowy audyt bezpieczeństwa IT i budowę od podstaw zapasowego centrum przetwarzania danych (ang. DRC - Diaster Recovery Center) lub disaster recovery “w chmurze” (RaaS)
- modelowanie i nadzorowanie polityk bezpieczeństwa IT

Atende S.A. | **+48 22 29 57 300** | **kontakt@atende.pl** | **atende.pl**