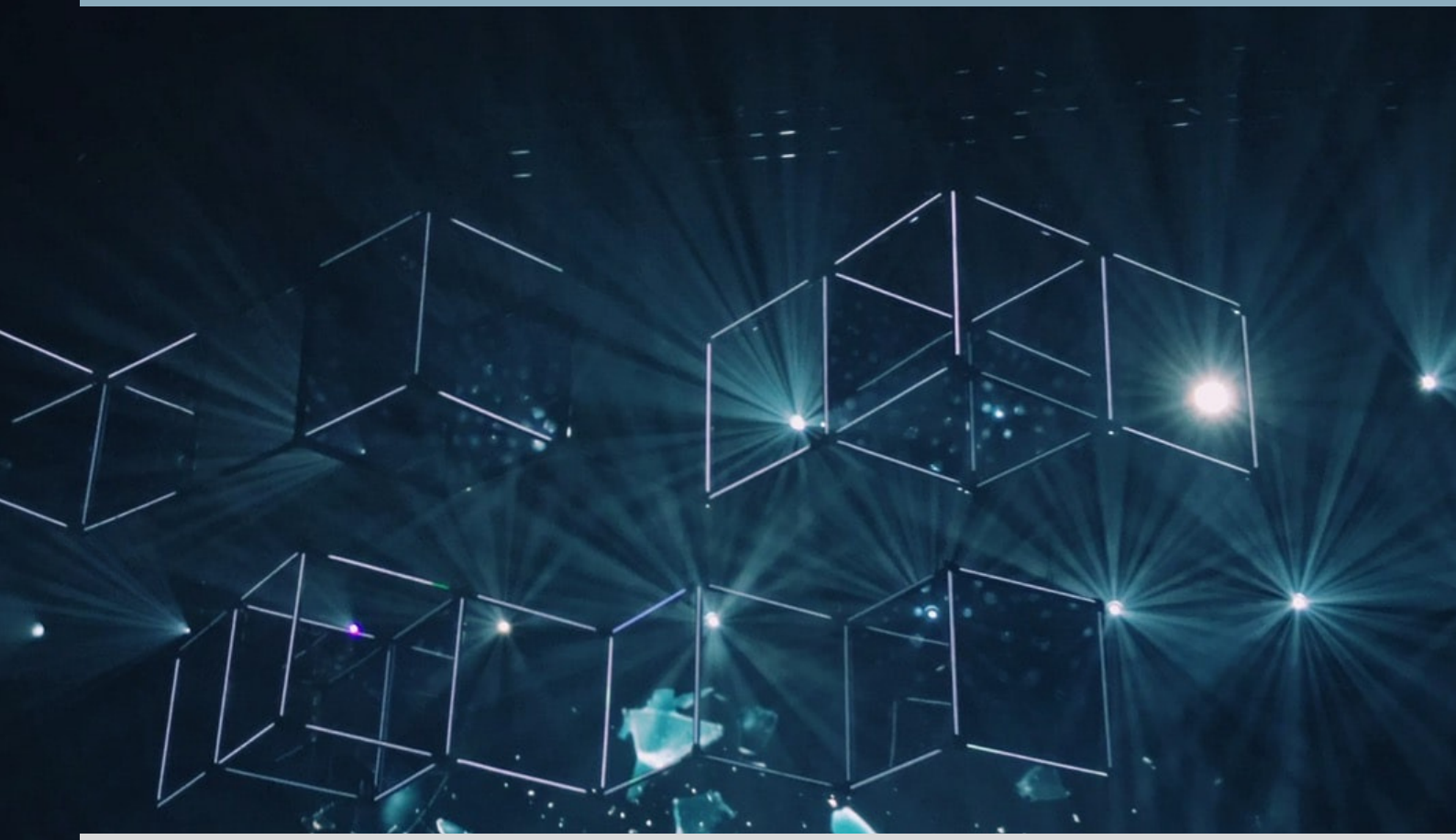
CASE STUDY

IT Solution FACTOR



INNOWACYJNE POMYSŁY SĄ BEZPIECZNE

URZĄD PATENTOWY RZECZYPOSPOLITEJ POLSKIEJ

Rozwiązania FortiGate chronią cenne zasoby Urzędu Patentowego RP, a jednocześnie usprawniają wymianę dokumentów w formie cyfrowej. Dzięki wdrożeniu nowoczesnych rozwiązań, wydajność i dostępność usług sieciowych dla Urzędu wzrosła do niemal 100 procent.

NA STRAŻY INNOWACJI

Urząd Patentowy RP jest centralnym organem administracji rządowej odpowiedzialnym za udzielanie ochrony prawnej na przedmioty własności przemysłowej, tj. wynalazki i wzory użytkowe, znaki towarowe, wzory przemysłowe, oznaczenia geograficzne i topografie układów scalonych.

W 2018 roku Urząd w tzw. trybie krajowym obsłużył ponad 20 tys. zgłoszeń wynalazków, wzorów użytkowych, wzorów przemysłowych i znaków towarowych. Każde zgłoszenie zazwyczaj składała się z kilku dokumentów, które muszą zostać przekierowane do właściwego eksperta, celem weryfikacji formalnej i merytorycznej.

W ramach realizowanych procedur międzynarodowych przesyłane dokumenty wymieniane są również z innymi podmiotami zajmującymi się ochroną własności intelektualnej w Europie i na świecie m.in. Urzędem Unii Europejskiej ds. Własności Intelektualnej, Europejskim Urzędem Patentowym oraz Światową Organizacją ds. Własności Intelektualnej.

Sprawne działanie Urzędu jest ściśle powiązane z wykorzystaniem cyfrowej ścieżki wymiany dokumentów, która może nieść za sobą zagrożenie dla własności przemysłowej zgłaszanej do ochrony. Każda operacja dostępu do materiałów i informacji musi być odpowiednio zabezpieczana. Niedopełnienie należytej ochrony może bowiem nie tylko naruszyć procedury, ale również otworzyć drogę do podważania wydawanych przez Urząd decyzji.

ŚCISŁA KONTROLA SIECI POTRZEBNA OD ZARAZ

Urząd Patentowy RP potrzebował systemowego rozwiązania, które zapewni najwyższej klasy bezpieczeństwo wewnętrznych zasobów sieciowych oraz strefy ograniczonego zaufania (DMZ) przed dostępem osób nieuprawnionych. Liczyło się również precyzyjne zarządzanie dostępem do Internetu i transparentne udostępnianie zasobów Urzędu dla ekspertów pracujących zdalnie.

Zespół IT Urzędu oczekiwał również rozwiązania, które pozwoliłoby nie tylko obserwować ruch sieciowy, ale również powiązać go z konkretnym użytkownikiem, systemem oraz aplikacją. Nie mniej ważna była możliwość centralnego zarządzania oraz przekrojowego raportowania o ruchu sieciowym i zdarzeniach bezpieczeństwa w części infrastruktury objętej systemem.

W odpowiedzi na potrzeby Urzędu, firma IT Solution Factor dostarczyła we współpracy z dystrybutorem Veracomp oraz wdrożyła sprzęt marki Fortinet, znany z wydajności, niezawodności i bogatych możliwości.
W skład ulepszonego ekosystemu sieciowego jednostki weszły dwa modele wielofunkcyjnej platformy zabezpieczeń FortiGate, 1500D oraz 1200D, pracujące w trybie wysokowydajnych klastrów, a także środowisko FortiManager do centralnego zarządzania urządzeniami.

Dla IT Solution Factor to kolejne wdrożenie, bazujące na niezawodnej technologii Fortinet. Dzięki wieloletniemu doświadczeniu naszych inżynierów oraz partnerskiej współpracy z dostawcami projekt został zrealizowany na czas i spełnia wysokie wymagania bezpieczeństwa teleinformatycznego Urzędu – komentuje **Kacper Konopiński, Prezes Zarządu IT Solution Factor.**

FORTIGATE 1200D: BEZPIECZEŃSTWO ZASOBÓW I INTUICYJNE LOGOWANIE

Klaster FortiGate 1200D pracuje jako brama SSL VPN, kontrolując dostęp do zasobów Urzędu oraz zainstalowane na stacjach końcowych systemy antywirusowe. System został skonfigurowany tak, by identyfikować i uwierzytelniać użytkownika na podstawie certyfikatów bezpieczeństwa. Dzięki temu pracownicy zdalni uzyskują dostęp do zasobów od razu po uruchomieniu komputera, bez konieczności dodatkowego logowania, pod warunkiem, że zapewniają zgodność z wymogami bezpieczeństwa (compliance), jak na przykład aktualność baz systemów antywirusowych.

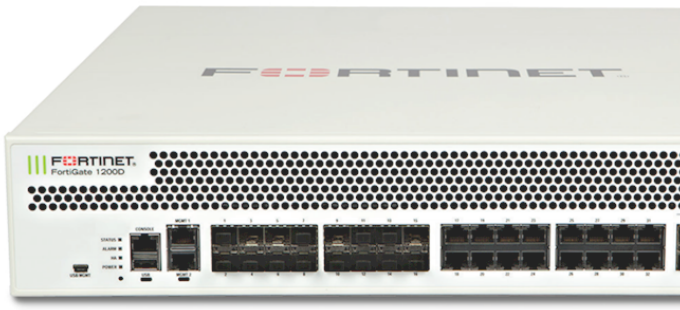
FORTIGATE 1500D: KOMPLEKSOWY FIREWALL

Drugi z zastosowanych klastrów, FortiGate 1500D, pracuje jako system zapory ogniowej do wewnętrznej segmentacji (ISFW). To tutaj zainstalowane na punktach końcowych oprogramowanie FortiClient, wysyła komunikaty telemetrii, umożliwiając nie tylko podgląd adresów IP stacji końcowych na poziomie firewalla, ale również powiązanie ich bezpośrednio z użytkownikami zalogowanymi na tych stacjach.

W przypadku niedostępności ścieżki podstawowej istnieje możliwość automatycznego przełączenia na alternatywną ścieżkę między klastrami urządzeń FortiGate 1500D oraz FortiGate 1200D, a także automatyczne, powrotne przełączenie, kiedy ścieżka podstawowa staje się dostępna. To zapewnia nieprzerwaną ochronę zarówno przychodzącego, jak i wychodzącego ruchu sieciowego Urzędu.

RUCH SIECIOWY WIDOCZNY JAK NA DŁONI

Oba klastry - FortiGate 1200D oraz FortiGate 1500D - są zarządzane z poziomu jednej maszyny wirtualnej: FortiManager. Funkcjonalność zarządzania zdarzeniami (FortiAnalyzer) pozwala na centralne składowanie logów z obu grup urządzeń FortiGate Urzędu.



Dzięki powiązaniu urządzeń FortiGate z FortiAnalyzer, możliwe jest śledzenie skompromitowanych hostów oraz wykonywanie działań automatycznych, takich jak blokowanie czy kwarantanna. System został skonfigurowany tak, by powiadamiać administratora o zdarzeniach nie tylko standardowych, ale również o niestandardowych możliwych do wystąpienia w infrastrukturze Urzędu. Na poziomie FortiAnalyzer skonfigurowano również moduł raportujący, który automatycznie generuje raporty okresowe oraz, w razie potrzeby, na żądanie.

URZĄD PATENTOWY 4.0

Dzięki dostarczonym przez Veracomp i wdrożonym przez IT Solution Factor urządzeniom FortiGate, Urząd Patentowy RP ma zapewnioną wysoką wydajność i dostępność usług sieciowych, na poziomie ponad 99,9 proc. Zespół IT może weryfikować na bieżąco ruch przechodzący przez urządzenie, bazując nie tylko na adresach IP, ale także na ID użytkowników, działających aplikacjach czy odwiedzanych stronach. Kontroli podlega również stan bezpieczeństwa urządzeń końcowych, wewnętrznych oraz zdalnych.

System automatycznych powiadomień o nietypowych zdarzeniach w sieci oraz intuicyjny i przejrzysty system FortiClient znacznie skracają czas rozwiązywania incydentów. Administratorów wspiera automatyzacja krytycznych działań, np. zmiana na alternatywną ścieżkę sieciową jest całkowicie zautomatyzowana i zajmuje kilka sekund, a nie jak wcześniej kilka godzin. System generuje pogłębione raporty, przedstawiając informacje zbiorcze w sposób pozwalający na zrozumienie istniejącego wolumenu ruchu w sieci oraz przewidywanie pewnych trendów. Dzięki temu administratorzy mogą zoptymalizować planowanie rozwoju sieci i całości infrastruktury Urzędu.

veracomp inspirujemy IT

FORTINET

Bezpieczeństwo teleinformatyczne zasobów i danych przetwarzanych w Urzędzie jest zawsze traktowane priorytetowo. Jesteśmy bardzo zadowoleni z wdrożonego rozwiązania, które pozwala nam sprawniej i efektywniej wykonywać naszą pracę. Kompleksowy monitoring ruchu sieciowego wspiera nas w wykrywaniu anomalii i w podejmowaniu stosownych działań korygujących - podsumowuje **Justyn Łojko, Dyrektor Departamentu Informatyki Urzędu Patentowego RP.**

KORZYŚCI Z WDROŻENIA ROZWIĄZAŃ FORTINET

- Zabezpieczenie dostępu do wewnętrznych zasobów sieciowych;
- Ścisła kontrola dostępu do Internetu i do udostępnianych zasobów, szczególnie dla pracowników zdalnych;
- Podgląd ruchu sieciowego i możliwość powiązania go z konkretnym użytkownikiem systemem oraz aplikacją;
- Możliwość centralnego zarządzania systemem oraz przekrojowego raportowania o ruchu sieciowym i incydentach bezpieczeństwa;
- Możliwość zastosowania DLP w przyszłości po dostosowaniu systemów dziedzinowych;
- Łatwa integracja z rozwiązaniami Sandbox w celu wykrywania zagrożeń nieznanych w ramach Security Fabric;

- Możliwość wykrywania i blokowania najnowszych zagrożeń w ramach FortiGuard Virus Outbreak Service;
- Bezpieczeństwo uruchamiania nieznanych plików MS Office, PDF dzięki funkcji Content Disarm and Reconstruction;
- Proste w realizacji wdrożenie 2FA w oparciu o token fizyczny lub aplikacyjny;
- Radykalne obniżenie przestojów w dostępie do zasobów w razie awarii;
- Prostsze badanie źródeł cyberzagrożeń oraz raportowanie skuteczności środków bezpieczeństwa.