GECOS

doradztwo IT · ERP · cyber

Modernizacja infrastruktury sieciowej i zabezpieczeń w firmie produkcyjnej Panta Plast sp. z o.o działającej w 26 krajach

Klient: Panta Plast sp. z o.o
Partner wdrożeniowy: GECOS Sp. z o.o.
Czas wdrożenia: 2 miesiące
Liczba użytkowników: 32

O Firmie

Panta Plast Spółka z o.o. to polski producent artykułów biurowych, szkolnych i reklamowych, działający nieprzerwanie od 1982 roku na rynku krajowym i europejskim. Firma posiada ugruntowaną pozycję wśród wytwórców wyrobów opartych na foliach PVC i PP, tworzywach sztucznych, sztucznej skórze oraz papierze.

Dzięki rozbudowanemu zapleczu produkcyjnemu, szerokiej gamie wzorniczej oraz dużemu wolumenowi zakupów surowców od światowych producentów, przedsiębiorstwo oferuje wysoką jakość produktów przy zachowaniu konkurencyjnych cen.

Organizacja współpracuje z partnerami handlowymi w 26 krajach oraz rozwija segment dystrybucyjny, oferując produkty renomowanych marek europejskich, takich jak:

- INSTANT – kleje
- NEBULO – kredki i farby
- OPTIMUM – zeszyty i notesy
- PLAYCOLOR – farby
- UNOMAX – artykuły piśmienne
- SPLAT PLANET – artykuły kreatywne
- CENTRUM – artykuły szkolne

Dynamiczny rozwój działalności międzynarodowej wymagał jednak stabilnej, nowoczesnej i bezpiecznej infrastruktury IT.

Wyzwanie biznesowe

Poprawa bezpieczeństwa sieci firmowej -dotychczasowa infrastruktura sieciowa oparta była na przestarzałym rozwiązaniu DrayTek, które:

1. wykorzystywało nieaktualne protokoły VPN,
2. nie posiadało aktualnego wsparcia producenta,
3. generowało niestabilność połączeń między lokalizacjami,
4. nie zapewniało odpowiedniego poziomu ochrony przed współczesnymi zagrożeniami,
5. nie oferowało zaawansowanej analizy i kontroli ruchu sieciowego.

W praktyce oznaczało to zwiększone ryzyko przestojów, potencjalnych incydentów bezpieczeństwa oraz ograniczone możliwości dalszego skalowania infrastruktury.

Rozwiązanie GECOS

W odpowiedzi na te wyzwania firma Gecos Sp. z o.o zaproponowała wdrożenie zapory nowej generacji Stormshield SN330, która stała się centralnym elementem nowej architektury bezpieczeństwa.

Zakres projektu obejmował:

- migrację do nowoczesnych i bezpiecznych protokołów VPN,
- stabilizację komunikacji między lokalizacjami,
- segmentację sieci i kontrolę ruchu między strefami,
- wdrożenie zaawansowanych polityk bezpieczeństwa.
- konfigurację mechanizmu failover dla dwóch niezależnych łączy internetowych, zapewniającego ciągłość działania w przypadku awarii jednego z dostawców.

Dodatkowo uruchomiono kluczowe mechanizmy zwiększające poziom ochrony:
Pełne logowanie i monitoring ruchu sieciowego
Zapewniono pełną widoczność zdarzeń w sieci – rejestrowanie prób połączeń, blokad, anomalii oraz aktywności użytkowników.

Blokowanie ruchu na podstawie geolokalizacji (GeoIP)
Automatyczne odrzucanie połączeń z krajów wysokiego ryzyka znacząco ograniczyło liczbę nieautoryzowanych prób dostępu.
Inspekcja ruchu SSL/TLS
Wdrożono mechanizmy umożliwiające analizę zaszyfrowanego ruchu HTTPS, co pozwala wykrywać zagrożenia ukryte w komunikacji szyfrowanej – bez utraty wydajności sieci.
Całość rozwiązania objęta jest bieżącym wsparciem producenta i regularnymi aktualizacjami bezpieczeństwa.

Rezultaty

Modernizacja infrastruktury przyniosła wymierne korzyści biznesowe:

- wyraźna poprawa stabilności połączeń VPN,
- eliminacja problemów z komunikacją między oddziałami,
- znaczące podniesienie poziomu bezpieczeństwa organizacji,
- redukcja nieautoryzowanych prób połączeń dzięki filtrowaniu geolokalizacyjnemu,
- pełna widoczność i audytowalność ruchu sieciowego,
- możliwość wykrywania zagrożeń w ruchu szyfrowanym,
- infrastruktura gotowa na dalszy rozwój i skalowanie działalności międzynarodowej.

Wdrożenie nowoczesnej zapory nowej generacji nie tylko rozwiązało bieżące problemy techniczne, ale przede wszystkim stworzyło bezpieczne fundamenty pod dalszy rozwój firmy na rynkach europejskich.

Kluczowe usprawnienia bezpieczeństwa i dostępności

W ramach wdrożenia osiągnięto dodatkowe, konkretne wzmocnienia ochrony infrastruktury:

- ✓ skuteczne zablokowanie niepożądanego ruchu przychodzącego z regionów wysokiego ryzyka (m.in. Rosja, wybrane kraje Azji i Afryki),
- ✓ automatyczne blokowanie dostępu do stron internetowych klasyfikowanych jako podejrzane lub niebezpieczne przez CERT Polska oraz inne europejskie instytucje cyberbezpieczeństwa,
- ✓ ograniczenie dostępu VPN wyłącznie do zdefiniowanych użytkowników wraz z precyzyjnym przypisaniem dostępu do wybranych maszyn i zasobów w sieci,
- ✓ automatyczne przełączanie na łącze zapasowe w czasie poniżej 1 sekundy, gwarantujące ciągłość działania nawet w przypadku awarii głównego operatora.

Dzięki tym mechanizmom organizacja znacząco ograniczyła powierzchnię ataku, zwiększyła kontrolę nad dostępem zdalnym oraz zapewniła wysoki poziom dostępności krytycznych usług.

Co mówi klient

„Współpraca z firmą GECOS pozwoliła nam nie tylko poprawić bezpieczeństwo sieci, ale również rozwiązać problemy z ręcznym przepinaniem zapasowego łącza. Doceniamy ich praktyczne podejście, wysokie kompetencje oraz bardzo dobrą współpracę na każdym etapie projektu."

Piotr Stępiński
Panta Plast Sp. z o.o.

„Dzięki współpracy z GECOS zyskaliśmy nowoczesne, bezpieczne środowisko sieciowe, a jednocześnie wspierające dalszy rozwój naszej firmy. Z pełnym przekonaniem rekomendujemy GECOS jako kompetentnego i godnego zaufania partnera w zakresie cyberbezpieczeństwa oraz wdrożeń rozwiązań Stormshield."

Panta Plast Sp. z o.o.

Podsumowanie

Projekt modernizacji infrastruktury sieciowej w Panta Plast Sp. z o.o. miał na celu nie tylko usunięcie problemów technicznych, ale przede wszystkim strategiczne podniesienie poziomu bezpieczeństwa i dostępności środowiska IT.

Wdrożenie zapory nowej generacji Stormshield SN330 pozwoliło:

- ustabilizować komunikację między lokalizacjami,
- zapewnić automatyczne przełączanie łączy internetowych,
- skutecznie ograniczyć nieautoryzowany ruch z regionów wysokiego ryzyka,
- wdrożyć zaawansowaną kontrolę i inspekcję ruchu sieciowego (w tym SSL/TLS),
- precyzyjnie zarządzać dostępem VPN do użytkowników i zasobów,
- uzyskać pełną widoczność oraz audytowalność zdarzeń w sieci.

Efektem jest nowoczesne, skalowalne i odporne na zagrożenia środowisko sieciowe, które wspiera dalszy rozwój organizacji oraz minimalizuje ryzyko operacyjne.
Projekt stanowi przykład kompleksowego podejścia do cyberbezpieczeństwa – łączącego stabilność infrastruktury, ciągłość działania oraz realne wzmocnienie ochrony danych i zasobów firmy.

O GECOS Sp. z o.o.

GECOS to polska firma z ponad 20-letnim doświadczeniem w transformacji cyfrowej przedsiębiorstw. Specjalizujemy się w wdrożeniach systemów IT – głównie systemów ERP oraz rozwiązań cyberbezpieczeństwa.

Jesteśmy certyfikowanym partnerem **Comarch** i Microsoft.

Nasza oferta obejmuje:

- → Wdrożenia systemów ERP (Comarch ERP XL, Comarch ERP Optima)
- → Rozwiązania cyberbezpieczeństwa i zgodności regulacyjnej (TISAX, NIS2, ISO)
- → Urządzenia NFG - Stormshield
- → Środowiska Microsoft 365 i Azure
- → Doradztwo w zakresie transformacji cyfrowej

Naszą filozofią pracy jest hasło: „Najpierw procesy, potem technologia”.

Doświadczenie: **ponad 300 udanych transformacji cyfrowych w polskich firmach produkcyjnych, handlowych i usługowych**. Nasze wdrożenia łączą technologię z praktyką biznesową: zero przestojów, szkolenia w języku procesów, wsparcie po certyfikacji.

GECOS
doradztwo IT · ERP · cyber

GECOS sp. z o.o.

Strategiczny Partner Comarch I
15 lat doświadczenia
w transformacji cyfrowej

+48 502 474 034

cyber@gecos.pl

gecos.pl/cyber

NCC-PL Krajowe Centrum Kompetencji Cyberbezpieczeństwa
Ministerstwo Cyfryzacji
ECCC European Cybersecurity Competence Centre
Co-funded by the European Union