1 Urządzenia bezpieczeństwa i transmisji danych

1.1 Wymagania ogólne

1.1.1 Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

1.2 Funkcje modułu Firewall

1.2.1 System realizujący funkcję Firewall musi zostać dostarczony w postaci klastra pracującego w trybie Active-Passive składającego się z dwóch urządzeń.
1.2.2 Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
1.2.3 Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
1.2.4 Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
1.2.5 Musi obsługiwać Multicast routing.
1.2.6 Musi obsługiwać Policy Based routing.
1.2.7 Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
1.2.8 Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
1.2.9 Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
1.2.10 Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
1.2.11 Musi obsługiwać Dynamic DNS.
1.2.12 Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
1.2.13 Musi obsługiwać translację portów: PAT.
1.2.14 Musi obsługiwać IPSec NAT traversal.
1.2.15 Musi obsługiwać mechanizm Policy Based NAT.
1.2.16 Musi obsługiwać VLAN 802.1Q.
1.2.17 Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
1.2.18 Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
1.2.19 Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
1.2.20 Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
1.2.21 Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
1.2.22 Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
1.2.23 Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
1.2.24 Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
1.2.25 Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
1.2.26 Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
1.2.27 Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.
1.2.28 Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego agenta na stacjach roboczych użytkowników.
1.2.29 Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
1.2.30 Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.

1.2.31 Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
1.2.32 Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
1.2.33 Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
1.2.34 Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
1.2.35 Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
1.2.36 Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
1.2.37 Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
1.2.38 Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
1.2.39 Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
1.2.40 Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

1.3 Dostarczony system bezpieczeństwa musi zapewniać:

1.3.1 1. Ochronę z wykorzystaniem mechanizmów IPS.
1.3.2 Ochronę antywirusową.
1.3.3 Ochronę przed nieznanymi zagrożeniami.
1.3.4 Ochronę przed phishingiem.
1.3.5 Ochronę przed niechcianą pocztą.
1.3.6 Kontrolę wykorzystywanych aplikacji.
1.3.7 Możliwość filtrowania URL.

1.4 Parametry fizyczne systemu Firewall:

1.4.1 Element systemu pełniący funkcję Firewall musi dysponować :
1.4.1.1 8 portami 1Gb RJ45.
1.4.1.2 Minimum 4 GB pamięci RAM.
1.4.1.3 Minimum 2 porty USB 3.0.
1.4.1.4 Minimum jeden port typu Console.
1.4.1.5 Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza.

1.5 Parametry wydajnościowe systemu:

1.5.1 Przepustowość Firewall minimum: 5.8 Gbps.
1.5.2 Przepustowość IPSec VPN nie mniejsza niż: 2.4 Gbps.
1.5.3 Przepustowość skanowania antywirusowego nie mniejsza niż: 1.47 Gbps.
1.5.4 Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 1.3 Gbps.
1.5.5 Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 1.18 Gbps.
1.5.6 Obsługa nie mniej niż: 50 tuneli IPSec site-to-site.
1.5.7 Obsługa nie mniej niż: 75 tuneli client-to-site.
1.5.8 Obsługa nie mniej niż: 3.500.000 jednoczesnych połączeń.
1.5.9 Obsługa nie mniej niż: 34.000 nowych połączeń na sekundę.
1.5.10 W ramach Firewall system musi obsługiwać minimum: 100 sieci VLAN.

1.6 W ramach ochrony przed atakami system musi zapewniać:

1.6.1 Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 4500 definicji sygnatur.
1.6.2 Automatyczne blokowanie znanych źródeł ataków.
1.6.3 Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
1.6.4 Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
1.6.5 Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.

1.6.6 Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

1.7 W ramach kontroli antywirusowej system musi zapewniać:

1.7.1 Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.

1.7.2 Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.

1.7.3 Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.

1.7.4 Możliwość skanowania plików o rozmiarze co najmniej 20MB.

1.7.5 Możliwość zdefiniowania rozmiaru skanowanego pliku.

1.7.6 Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.

1.7.7 Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.

1.7.8 Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.

1.7.9 Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

1.8 W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać:

1.8.1 Możliwość rozbudowy (np. w oparciu o licencję) o funkcję analizy behawioralnej w oparciu o platformę typu sandbox, w tym co najmniej:

1.8.1.1 W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).

1.8.1.2 Analizę plików pobieranych przez HTTP/HTTPS i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP) oraz plików pobieranych za pomocą protokołu FTP.

1.8.1.3 Ogólne oszacowanie poziomu ryzyka dla analizowanych plików i określanie różnego rodzaju akcji na ich podstawie.

1.8.1.4 Kwarantannę podejrzanych plików co najmniej dla protokołu SMTP.

1.8.1.5 Możliwość blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.

1.8.1.6 Możliwość analizy plików o rozmiarze co najmniej 10MB.

1.8.1.7 Brak ograniczeń co do ilości analizowanych plików.

1.8.2 W ramach ochrony przed phishingiem system musi zapewniać:

1.8.2.1 Możliwość rozbudowy (np. w oparciu o licencję) o funkcję ochrony przed phishingiem, w tym co najmniej:

1.8.2.1.1 Możliwość blokowania dostępu do spreparowanych stron.

1.8.2.1.2 Ochronę przed phishingiem nie zależnie od typu połączenia, protokołu, portu.

1.8.2.1.3 Możliwość tworzenia białych/czarnych list domen, do których połączenia będą filtrowanie.

1.8.2.1.4 Notyfikację użytkownika, którego dotyczy zdarzenie - niezależnie od logów i raportów.

1.8.2.1.5 Kontrolę zapytań DNS.

1.8.3 W ramach kontroli antyspamowej system musi zapewniać:

1.8.3.1 Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.

1.8.3.2 Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.

1.8.3.3 Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.

1.8.3.4 Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.

1.8.3.5 Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

1.8.4 W ramach filtrowania zawartości URL system musi zapewniać:

1.8.4.1 Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.

1.8.4.2 Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
1.8.4.3 Odpytywanie bazy on-line w czasie rzeczywistym.
1.8.4.4 Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.
1.8.4.5 Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
1.8.4.6 Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
1.8.4.7 Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
1.8.4.8 Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.
1.8.4.9 Możliwość filtrowania treści w oparciu o typy MIME.
1.8.4.10 Możliwość blokowania plików cookies dla określonych domen.
1.8.4.11 Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
1.8.4.12 Analizę treści dla protokołu https.
1.8.4.13 Wyłączenie inspekcji https dla wybranych kategorii stron www.

1.9 W ramach kontroli aplikacyjnej system musi zapewniać:

1.9.1 Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
1.9.2 Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
1.9.3 W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
1.9.4 Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
1.9.5 Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji.

1.10 Wymagane funkcje VPN systemu:

1.10.1 Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
1.10.2 W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
1.10.3 Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
1.10.4 Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
1.10.5 Obsługa Dead Peer Detection (DPD).
1.10.6 Wsparcie dla IKEv1 i IKEv2.
1.10.7 Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
1.10.8 Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
1.10.9 Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
1.10.10 Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
1.10.11 Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
1.10.12 Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
1.10.13 Dla połączeń Client-to-Site możliwość zastosowania dwuskładnikowego uwierzytelnienia w oparciu o tokeny sprzętowe lub programowe.
1.10.14 Musi umożliwiać uruchomienie portalu SSL VPN, który umożliwia autoryzację w oparciu o protokoły RADIUS, LDAP, Active Directory, lokalną bazę użytkowników.
1.10.15 Portal SSL VPN musi zapewniać wsparcie dla protokołów: SSH, RDP, HTTP.
1.10.16 Portal SSL VPN musi wspierać funkcjonalność Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML.

1.11 Zarządzanie

1.11.1 Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
1.11.2 Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
1.11.3 Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
1.11.4 W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
1.11.5 Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
1.11.6 Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
1.11.7 Komunikacja do systemów logowania i raportowania musi być szyfrowana.
1.11.8 W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

1.12 Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

1.12.1 Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
1.12.2 Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
1.12.3 Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
1.12.4 Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
1.12.5 Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
1.12.6 Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
1.12.7 Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
1.12.8 System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
1.12.9 Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
1.12.10 System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
1.12.11 Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
1.12.12 Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
1.12.13 Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
1.12.14 Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
1.12.15 Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
1.12.16 Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
1.12.17 System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
1.12.18 System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
1.12.19 Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
1.12.20 System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
1.12.21 System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
1.12.22 Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
1.12.23 Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

1.13 Licencje i wsparcie techniczne

1.13.1 W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:

1.13.1.1 Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Ochrona przed nieznanymi zagrożeniami, Ochrona przed phishingiem – na okres 5 lat.

1.13.2 System musi być objęty serwisem gwarancyjnym producenta przez okres 5 lat, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 (świadczone telefonicznie lub poprzez portal).

1.13.3 Serwis gwarancyjny/licencyjny/wsparcie musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji.

1.13.4 Zgłaszanie usterek/awarii poprzez pocztę elektroniczną, portal helpdesk lub infolinię (sposób zgłaszania usterek/awarii zostanie uzgodniony z Wykonawcą na etapie zawarcia umowy).

1.13.5 Czas reakcji serwisu od momentu zgłoszenia - 1 godzina, czas na rozwiązanie zgłoszonej usterki/awarii - 24 godziny.

1.14 Wymagania dodatkowe:

1.14.1 Termin dostawy - do 14 tygodnia od dnia podpisania umowy.

1.14.2 Wykonawca w ramach przedmiotu zamówienia zobowiązuje się do instalacji i konfiguracji systemów bezpieczeństwa w miejscu wskazanym przez zamawiającego w terminie 14 dni od dostawy.

1.14.3 Wykonawca powinien posiadać minimum 3 certyfikowanych inżynierów na poziomie Professional (lub odpowiednim) w zakresie instalacji i konfiguracji systemu bezpieczeństwa oferowanego producenta. Certyfikaty inżynierów wykonawca będzie zobowiązany przedstawić na każde żądanie zamawiającego.

1.14.4 Wykonawca w ramach przedmiotu zamówienia zobowiązuje się do zapewnienia dla co najmniej dwóch pracowników zamawiającego, minimum 4 dniowego, certyfikowanego szkolenia (prowadzonego przez autoryzowanego trenera producenta), z zakresu obsługi i konfiguracji systemu bezpieczeństwa dostarczonego w ramach zamówienia– pełne wdrożenie..

……

Data; kwalifikowany podpis elektroniczny
lub podpis zaufany lub podpis osobisty