



Uznanie odporności i bezpieczeństwa za priorytet

Rozwiązania Alcatel-Lucent Enterprise dla instytucji publicznych

Spis treści

- | Omówienie
- | Dlaczego współpraca IT/OT jest kluczowa
- | Odporne i bezpieczne rozwiązania sieciowe
- | Odporne i bezpieczne rozwiązania komunikacyjne
- | Ochrona ludzi i zasobów
- | Suwerenność i bezpieczeństwo danych



Przegląd

W obliczu rosnących wyzwań globalnych oraz zwiększonego ryzyka cybernetycznego i fizycznego rządy muszą nadać priorytet zarządzaniu ryzykiem, zabezpieczyć infrastrukturę krytyczną i chronić obywateli. Według firmy CloudSEK liczba cyberataków na instytucje rządowe wzrosła w 2022 r. o 95%.¹ Oczekuje się, że działania rządu będą kontynuowane niezależnie od sytuacji, a obywatele będą bezpieczni. W dzisiejszym globalnym klimacie utrzymanie bezpieczeństwa danych, ochrona suwerenności danych i zapewnienie dostępności usług jest ważniejsze niż kiedykolwiek.

Sektor publiczny i dlaczego technologie teleinformatyczne są ważniejsze niż kiedykolwiek

W ostatnich latach transformacja cyfrowa w sektorze publicznym robi szybkie postępy i coraz większa liczba obywateli uzyskuje dostęp do usług cyfrowych. Transformacja cyfrowa umożliwiła także pracownikom rządowym przyjęcie

stylu pracy polegającego na pracy w dowolnym miejscu. Rośnie presja na rządy, by jeszcze bardziej przyspieszyły transformację cyfrową. Według artykułu opublikowanego przez firmę Deloitte 77 procent agencji rządowych twierdzi, że inicjatywy w zakresie transformacji cyfrowej forsowane podczas pandemii już teraz mają pozytywny wpływ na ich organizacje.²

Alcatel-Lucent Enterprise współpracuje z rządami na całym świecie, mając świadomość znaczenia ochrony obywateli, działalności i budynków przed zagrożeniami cybernetycznymi i fizycznymi. Nasze rozwiązania uwzględniają bezpieczeństwo i prywatność danych na każdym etapie projektowania i są wyposażone w niezawodne opcje, które pasują do organizacji każdego typu. Ten e-book zawiera informacje na temat odporności i bezpieczeństwa Twoich rozwiązań komunikacyjnych, chmurowych i sieciowych ALE.

¹ [Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says](#). CSO United States, styczeń 2023 r.

² <https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html>.

Dlaczego współpraca IT/OT jest kluczowa

Zanim zastanowimy się, w jaki sposób można zwiększyć odporność i bezpieczeństwo rozwiązań Alcatel-Lucent Enterprise, należy zwrócić uwagę na zmieniającą się relację między technologiami informacyjnymi i operacyjnymi. W przeszłości zespoły IT i operacyjne nie współpracowały blisko, gdyż każdy miał swoje funkcje i obowiązki. Obecnie te dwa światy zbiegają się i muszą funkcjonować razem. Zespoły IT i operacyjne, które nie są świadome swoich działań lub nie koordynują ich i nie współpracują, narażają całą organizację na ryzyko.

Weźmy na przykład pod uwagę ogromną liczbę urządzeń Internetu przedmiotów (IoT), które są szybko wdrażane w wielu agencjach rządowych i inteligentnych miastach. Gdy dział IT nie wie, że zespół operacyjny wdraża nowe urządzenia IoT, nie może zapewnić zgodności urządzeń z zasadami bezpieczeństwa obowiązującymi w organizacji. Urządzenia IoT charakteryzują się dużym zróżnicowaniem pod względem funkcji cyberbezpieczeństwa i mogą nie być wyposażone w najnowsze mechanizmy ochrony lub ich możliwości mogły nie zostać w pełni wdrożone. Te nieautoryzowane ukryte urządzenia IT mogą mieć uruchomione dowolne oprogramowanie i być zainfekowane wirusami oraz złośliwym oprogramowaniem. Pozostawione bez kontroli mogą łatwo wprowadzać do sieci nowe luki i wektory ataków. Obecnie obserwujemy narodziny współpracy między technologiami IT/OT, niezbędnej do zapewnienia bezpieczeństwa i odporności sieci.



Odporne i bezpieczne rozwiązania sieciowe

Infrastruktura sieciowa jest integralną częścią funkcjonowania organizacji rządowych, a także świadczenia usług obywatelom. Ze względu na wrażliwy charakter informacji zawartych w sieciach rządowych i krytyczne znaczenie usług publicznych, przestoje lub zakłócenia w usługach sieciowych mogą mieć poważne konsekwencje, co czyni odporność i bezpieczeństwo priorytetem. Niezawodne i bezpieczne sieci są niezbędne, aby rządy mogły świadczyć skuteczne usługi publiczne, chronić poufne informacje i zapewniać płynność funkcjonowania.

Stworzone przez ALE [Sieci ery cyfrowej](#) są odporne i wykraczają poza to, co oferuje wielu innych dostawców technologii. Już na najwcześniejszych etapach projektowania integrujemy w naszej sieci i rozwiązaniach funkcje bezpieczeństwa, bez dodatkowych kosztów licencyjnych.

6 najlepszych praktyk przy wyborze rozwiązań sieciowych

1. Przyjmij strategię bezpieczeństwa opartą na zasadzie zerowego zaufania. Makro- i mikrosegmentacja sieci ma kluczowe znaczenie dla utrzymania odporności infrastruktury. Etapowe podejście do mikrosegmentacji gwarantuje właściwą implementację i pomaga uniknąć zakłóceń.
2. Rozważ wdrożenie rozwiązania Shortest Path Bridging (SPB) w celu zapewnienia redundancji i bezpieczeństwa, ponieważ takie podejście dynamicznie przekierowuje ruch przez wiele ścieżek w przypadku awarii, tworząc jednocześnie wydajną, skonteneryzowaną sieć. SPB zwiększa bezpieczeństwo dzięki enkapsulacji MAC-in-MAC, eliminując adresy IP i zapobiegając atakom polegającym na podszywaniu się pod IP oraz analizie pakietów.
3. Rozważ wykorzystanie możliwości obudowy wirtualnej w celu zwiększenia niezawodności w krytycznych obszarach, ponieważ zapewnia to redundancję i odporność sieci — wraz z aktualizacjami oprogramowania w trakcie użytkowania (ISSU) i umożliwiając dedykowane połączenia mesh lub pierścieniowe. Obudowa wirtualna stanowi ekonomiczne rozwiązanie upraszczające zarządzanie siecią i jednocześnie zapewnia dużą dostępność.
4. Wdroż protokół Virtual Router Redundancy Protocol (VRRP). VRRP zwiększa odporność sieci, zapewniając zapasowy router wirtualny, który może płynnie przejąć kontrolę w przypadku awarii routera głównego.
5. Wprowadź rozwiązanie, które gwarantuje, że dysponujesz kopiami zapasowymi wszystkich konfiguracji z przełączników sieciowych i możesz je przywrócić w najgorszym przypadku lub gdy zajdzie taka potrzeba.
6. Wyższym stopniem bezpieczeństwa jest posiadanie kodu Secure Diversified Code, który losowo rozmieszcza różne segmenty kodu na przełącznikach, radykalnie zwiększając bezpieczeństwo. Można to zestawzić z niezależnym procesem weryfikacji i walidacji (IVV) przez zewnętrznego eksperta ds. cyberbezpieczeństwa, który analizuje i testuje system operacyjny w celu zidentyfikowania i wyeliminowania wszelkich potencjalnych luk w zabezpieczeniach, backdoorów, złośliwego oprogramowania lub exploitów systemowych.



Zainwestuj w odporne i bezpieczne rozwiązania sieciowe

Inwestycja w zapewnienie odporności i bezpieczeństwa sieci zawsze ma sens. Jednak zrozumienie, w co najlepiej zainwestować, może być złożone i czasochłonne – planowanie ma kluczowe znaczenie. Zanim zaczniesz, oto kilka kluczowych obszarów, które należy uwzględnić, aby zapewnić bezpieczeństwo i odporność, których wymaga Twoja organizacja:

- Dokonaj przeglądu i aktualizacji projektu sieci, aby upewnić się, że sieć odzwierciedla wymagania Twojej organizacji, w tym odpowiedni poziom odporności wrażliwych i krytycznych obszarów, które mają wpływ na podstawowe usługi publiczne. W obszarach krytycznych rozważ dodanie serwerów zapasowych i wielu połączeń, jeśli jest to możliwe i wykonalne.
- Weźmy pod uwagę rosnące znaczenie czasu reakcji na incydenty. Na przykład w naszym rozwiązaniu Alcatel-Lucent OmniVista Network Advisor wykorzystujemy możliwości sztucznej inteligencji (AI) i uczenia maszynowego (ML), aby szybciej identyfikować i rozwiązywać problemy. To narzędzie poprzez proaktywną identyfikację i rozwiązywanie problemów z siecią lub bezpieczeństwem

rozwiązuje problemy, zanim wpłyną one na użytkowników końcowych. Przyspiesza rozwiązywanie problemów i poprawia bezpieczeństwo sieci poprzez audyty konfiguracji i administrowanie alertami o wszelkich nagłych zmianach w zachowaniu sieci w czasie rzeczywistym.

- Rozważ zastosowanie [przełączników wzmocnionych](#) do pracy w trudnych warunkach. Rodzina wzmocnionych przełączników sieci Ethernet Alcatel-Lucent Enterprise została specjalnie zaprojektowana tak, aby doskonale sprawdzała się w trudnych warunkach i ekstremalnych temperaturach. Przełączniki te są zbudowane z wytrzymałych komponentów i umieszczone w solidnych obudowach, co zapewnia trwałość i niezawodność, oraz mają ten sam system operacyjny, co pozostałe przełączniki ALE. Aby zwiększyć bezpieczeństwo i chronić wrażliwe informacje, niektóre modele przełączników są wyposażone w sygnalizację ingerencji i przekaźniki alarmowe, które umożliwiają podłączenie zewnętrznych systemów alarmowych. Niektóre modele obsługują nawet protokół MACsec w celu bezpiecznej transmisji danych między dwoma urządzeniami końcowymi. Dzięki możliwościom wirtualnej obudowy zastosowanej w wytrzymałych przełącznikach można uzyskać lepszą redundancję, odporność i skalowalność.

Odporne i bezpieczne rozwiązania komunikacyjne

Komunikacja ma kluczowe znaczenie dla interakcji rządów z obywatelami, zainteresowanymi stronami i innymi instytucjami rządowymi, a także dla rozpowszechniania ważnych informacji. Systemy łączności muszą być dostępne w czasach kryzysu, kiedy obywatele najbardziej potrzebują pomocy rządu. Odporność i bezpieczeństwo ewoluują, a regularne przeglądy pomogą zapewnić bezpieczeństwo i dostępność rozwiązania komunikacyjnego Alcatel-Lucent Enterprise.

Rozwiązania komunikacyjne ALE są bezpieczne od samego początku. Oznacza to, że uwzględniamy bezpieczeństwo na każdym etapie definiowania, opracowywania i dostarczania produktu. Cały sprzęt i wszystkie systemy operacyjne są wzmocnione i mają wbudowaną ochronę przed odmową usługi (DoS). Przestrzegamy uznanych certyfikatów i akredytacji w zakresie światowych standardów bezpieczeństwa i prywatności (ISO 27001, ISO 27017 i ISO 27018). Ponadto przestrzegamy specyficznych dla branży standardów bezpieczeństwa i prywatności, takich jak ustawa Health Insurance Portability and Accountability Act (HIPAA) w Stanach Zjednoczonych oraz Hébergeurs de Données de Santé (HDS) dotycząca hostingu danych zdrowotnych we Francji, a także regionalnych standardów bezpieczeństwa i prywatności, takich jak obowiązujące w Unii Europejskiej Ogólne rozporządzenie o ochronie danych (RODO).

6 najlepszych praktyk do Twoich rozwiązań komunikacyjnych

Poniżej przedstawiamy 6 najlepszych praktyk zapewniających pełną optymalizację odporności i bezpieczeństwa, zintegrowanych w rozwiązaniach komunikacyjnych ALE.

1. Upewnij się, że masz najnowszą wersję oprogramowania lub odpowiednie poprawki, aby zapewnić sobie najnowsze ulepszenia zabezpieczeń i lepszą ochronę.
2. Rozważ rozwiązanie obejmujące monitorowanie alarmów i pamiętaj o regularnych aktualizacjach z uwzględnieniem odpowiednich progów. Sprawdzaj, czy powiadomienia o awariach systemu komunikacji lub alerty jakościowe są wysyłane do odpowiednich osób.
3. Przeanalizuj i wdróż politykę silnych haseł, najlepiej używając zewnętrznego uwierzytelniania z serwerem RADIUS. Wprowadź przypomnienia dla użytkowników, aby pomóc zapobiegać oszustwom związanym z pobieraniem opłat drogowych, które nadal stanowią zagrożenie w wielu krajach.
4. Zapewnij pracownikom szkolenia podnoszące świadomość zagrożeń dla bezpieczeństwa i upewnij się, że zdają sobie sprawę z ryzyka oraz środków zapobiegawczych.
5. Upewnij się, że posiadasz zautomatyzowane zdalne tworzenie kopii zapasowych systemu, co pomoże uniknąć utraty danych konfiguracyjnych.
6. Rozważ zastosowanie konkretnej sieci VLAN dla usług głosowych. Oddzielenie usług głosowych od reszty transmisji zmniejsza ryzyko kontaminacji, która potencjalnie może zakłócić funkcjonowanie a nawet zagrozić dostępności usług publicznych.



Zainwestuj w odporne i bezpieczne rozwiązania komunikacyjne

W ciągu ostatnich kilku lat środowisko globalne uświadomiło nam znaczenie komunikacji między rządem a obywatelami. Poniżej przedstawiono kilka kluczowych obszarów, które agencje rządowe powinny uwzględnić w kontekście inwestycji w rozwiązania komunikacyjne w celu zwiększenia odporności i bezpieczeństwa.

- Redundantna i odporna architektura. Twoja architektura powinna być w pełni redundantna i odporna. Duplikowanie serwerów połączeń w obszarach krytycznych, wdrażanie redundancji w lokalizacjach zdalnych i duplikowanie krytycznych serwerów aplikacji może zapewnić dodatkową ochronę.
- Utwórz przepływ pracy za pomocą aplikacji Rainbow lub narzędzia Alcatel-Lucent Visual Notification Assistant(VNA) z automatycznymi wyzwalaczami (wyzwalaczem jest człowiek, IoT lub system) w celu powiadamiania kluczowych osób o problemach z systemem, aby mogły szybko działać i przyspieszyć proces odzyskiwania
- Wdroż skuteczne szyfrowanie. Podstawą szyfrowania są standardy branżowe zaprojektowane natywnie w rozwiązaniu, bez żadnego wpływu na jakość i wydajność głosu



- Wdroż rozwiązanie [Rainbow™ firmy Alcatel-Lucent Enterprise](#), idealne narzędzie do współpracy, uzupełniające rozwiązania komunikacyjne ALE. Rainbow oferuje kompleksowy zestaw funkcji, w tym komunikację głosową, wideo i komunikatory internetowe, umożliwiając bezproblemową komunikację i efektywną współpracę. Dzięki Rainbow możesz wymieniać obrazy, filmy i nagrania z monitoringu wideo, zwiększając świadomość kontekstową i usprawniając podejmowanie decyzji. Rainbow zapewnia także komunikację hybrydową z bezpieczną łącznością pomiędzy lokalną firmą a chmurą. Zapewnia niezawodną komunikację, utrzymując kontakt ze współpracownikami i klientami korzystającymi z Rainbow oraz gwarantując nieprzerwaną łączność nawet w trudnych sytuacjach. Komunikacja hybrydowa ma również tę zaletę, że operacje w chmurze i lokalnie są uruchamiane z różnych lokalizacji, co zapewnia najwyższą odporność i utrzymanie otwartej komunikacji.
- Dla instytucji o bardziej rygorystycznych wymaganiach dotyczących bezpieczeństwa Rainbow Edge oferuje alternatywę lokalną z instancją w chmurze prywatnej. Instancja może być hostowana w dowolnym centrum danych, zapewniając pełną kontrolę nad serwerami, pamięcią masową i sieciami, co umożliwia instytucjom dostosowywanie i konfigurowanie infrastruktury zgodnie z ich wymaganiami. Można wdrożyć spersonalizowane zasady bezpieczeństwa, a zasobami można zarządzać autonomicznie. Ten poziom kontroli zapewnia pełną widoczność i władzę nad infrastrukturą, umożliwiając instytucjom podejmowanie świadomych decyzji i optymalizację wydajności zgodnie z ich celami.
- Zdefiniuj bezpieczną strategię komunikacji rozproszonego personelu. ALE zapewnia wiele opcji komunikacji i współpracy pracownikom rozproszonym, mobilnym i pracującym z domu, w tym:
 - Rainbow
 - [IP Desktop Softphone](#)
 - [Telefony programowe ALE](#)
 - [Telefon stacjonarny z wbudowaną siecią VPN i możliwością masowego wdrażania z wbudowanymi zabezpieczeniami \(VPN\)](#)

Ochrona ludzi i zasobów

ALE oferuje elastyczne, bezpieczne i wysoce dostępne systemy komunikacji i powiadomień w czasie rzeczywistym oraz [systemy powiadomień](#). Rozwiązania te można zintegrować z działaniami centrum kontroli bezpieczeństwa publicznego lub inteligentnych miast, usprawniając przydzielanie połączeń i ustalanie priorytetów, ułatwiając kontekstową wymianę informacji z danymi IoT oraz wzmacniając współpracę między służbami ratowniczymi i różnymi zainteresowanymi stronami, co umożliwia lepsze podejmowanie decyzji i koordynację.

Możliwość łączenia urządzeń IoT w budynkach, obiektach i miastach, w połączeniu z analityką i sztuczną inteligencją, zasadniczo zmienia krajobraz komunikacyjny. Dzięki integracji czujników, nadzoru wideo, przepływu pracy Rainbow i sztucznej inteligencji możliwe jest przejście od podejścia reaktywnego do proaktywnego, co zwiększa efektywność procedur pod względem czasu i kosztów. Integracja ta ułatwia kompleksowe zrozumienie kontekstu oraz wspiera procesy decyzyjne i tym samym skraca czas reakcji na sytuacje kryzysowe. Dodatkowo takie funkcje, jak śledzenie zasobów oraz kontrola inteligentnych zamków i światel usprawniają funkcjonowanie. Co więcej, możliwość rejestrowania komunikacji i rejestrowania działań upraszcza analizę po zdarzeniu, poprawiając procesy bezpieczeństwa i ograniczając potencjalne zobowiązania. Kluczowe znaczenie dla osiągnięcia tych postępów ma połączone w sieci środowisko z wszechobecnym dostępem do Wi-Fi i łatwym wdrażaniem IoT.

W przypadku działających pod presją czasu, bezpiecznych i wysoce dostępnych platform komunikacji w czasie rzeczywistym solidna infrastruktura jest niezbędna do zapewnienia płynnego działania. Twoja infrastruktura technologiczna powinna obejmować odpowiednie oprogramowanie, protokoły sieciowe o wysokiej dostępności oraz elastyczność umożliwiającą włączenie wytrzymałych przełączników sieciowych, które można bezproblemowo zintegrować z

ekosystemem i wytrzymać trudne warunki środowiskowe, w tym ograniczony przepływ powietrza, wstrząsy i ekstremalne temperatury pogodowe. Wybór wytrzymałego sprzętu zapewnia długą eksploatację w tak trudnych lokalizacjach, gdzie sprzęt mniej wytrzymały działałby krócej.

W dziedzinie systemów bezpieczeństwa fizycznego stawka jest wysoka. Każda minuta i każdy fragment materiału wideo może mieć dla władz kluczowe znaczenie w identyfikowaniu nieprawidłowości, ustalaniu źródła incydentu lub zrozumieniu przyczyny katastrofy. Niezbędna jest solidna [infrastruktura nadzoru wideo](#). Infrastruktura sieciowa powinna nie tylko zapewniać wystarczającą przepustowość i technologię Power over Ethernet (PoE) dla kamer monitorujących, ale także bezproblemowo integrować się z systemami zarządzania monitoringiem wideo. Integracja ta zapewnia wydajną i niezawodną sieć nadzoru, płynną pracę i łatwe rozwiązywanie problemów. Zespół operacyjny powinien być w stanie szybko rozwiązać wszelkie problemy z urządzeniami wideo, szczególnie w środowiskach, w których każda klatka wideo ma krytyczne znaczenie. Integracja [Alcatel-Lucent OmniSwitch®](#) rozwiązania, realizowana za pomocą wtyczek z głównymi systemami zarządzania wideo, umożliwia osiągnięcie tego istotnego celu.

Co więcej, zdarzają się sytuacje, w których konieczne staje się śledzenie zasobów lub lokalizowanie osób lub sprzętu w organizacji. Skuteczne rozwiązanie do śledzenia zasobów opiera się na możliwości łatwego i dokładnego lokalizowania ludzi i majątku. System taki podnosi również poziom bezpieczeństwa i ochrony, umożliwiając szybkie wysłanie pomocy, gdy znane jest miejsce pobytu poszczególnych osób. Dzięki rozwiązaniu [Alcatel-Lucent OmniAccess® Asset Tracking](#) można szybko zlokalizować i pokazać na mapie planu piętra. Śledzenie zasobów informuje także o wzorcach użytkowania, a wiedza o tym, czy zasoby są wykorzystywane nadmiernie, czy niedostatecznie, może dostarczyć cennych informacji.



Suwerenność i bezpieczeństwo danych

Alcatel-Lucent Enterprise znacznie przewyższa innych dostawców technologii, wdrażając wszystkie najlepsze praktyki wymagane dla kompleksowego bezpieczeństwa cybernetycznego. W ALE:

- Postępujemy zgodnie z najlepszymi praktykami i zaleceniami Narodowego Instytutu Nauki i Technologii (NIST) podczas przeprowadzania w naszych rozwiązaniach oceny ryzyka nowych funkcji i wdrażania funkcji cyberbezpieczeństwa, takich jak natywne szyfrowanie
- Posiadamy certyfikat Common Criteria EAL2
- Stosujemy normy ISO 27001 do wszystkich naszych rozwiązań opartych na chmurze
- Stosujemy ZTNA, szczegółową segmentację sieci i bardzo szczegółowe zasady bezpieczeństwa, aby zmniejszyć ryzyko nieautoryzowanych działań
- Przeprowadzamy na naszych produktach wysoce specjalistyczne testy bezpieczeństwa, takie jak testy penetracyjne

- Dbamy o to, by nasze produkty posiadały kluczowe certyfikaty branżowe, takie jak HDS, HIPAA oraz ustawa Family Educational Rights and Privacy Act (FERPA)
- ALE International działa zgodnie z dyrektywą Unii Europejskiej w sprawie bezpieczeństwa sieci i informacji (NIS 2).

Jako uznani eksperci ds. cyberbezpieczeństwa mamy wkład w propozycje Unii Europejskiej dotyczące dyrektyw w sprawie cyberbezpieczeństwa. Wykorzystujemy również naszą wiedzę z zakresu cyberbezpieczeństwa, aby pomóc naszym klientom wybrać i wdrożyć odpowiednią kombinację bezpiecznych rozwiązań do zunifikowanej komunikacji i współpracy, a także szkolić ich pracowników w zakresie najlepszych praktyk w dziedzinie bezpieczeństwa cybernetycznego.