



Chroń i daj siłę swojej firmie dzięki Alcatel-Lucent Enterprise

Radzenie sobie z rosnącą złożonością zagrożeń cybernetycznych i zmieniającymi się wymogami regulacyjnymi



Wprowadzenie

W obliczu poważnych zmian zachodzących w działalności organizacji, jednym z kluczowych obszarów, które ulegają zmianom, staje się bezpieczeństwo. Rozwój technologii sztucznej inteligencji zrewolucjonizował tradycyjne modele zabezpieczeń, wymuszając ponowne przemyślenie dotychczasowych, ugruntowanych praktyk.

W odpowiedzi na to nasz zespół ekspertów ds. cyberbezpieczeństwa w obszarach sieci, komunikacji i rozwiązań chmurowych połączył siły, aby podzielić się najważniejszymi spostrzeżeniami na temat nowych zagrożeń, z jakimi mierzą się przedsiębiorstwa, oraz sposobami dodawania niezbędnych warstw ochrony, aby zachować przewagę.

Zmieniający się krajobraz cyberbezpieczeństwa

Na środowisko cyberbezpieczeństwa największy wpływ ma szybki rozwój technologii, coraz bardziej wyrafinowane zagrożenia i zmieniające się przepisy. Eksperti branżowi wskazują na trzy główne trendy kształtujące obecnie cyberbezpieczeństwo przedsiębiorstw:

1. Podwójna rola sztucznej inteligencji
2. Ciągły wzrost liczby ataków ransomware i na łańcuchy dostaw
3. Konieczność solidnego zarządzania tożsamościami w ramach architektur zero trust

Dwustronna rola sztucznej inteligencji w cyberbezpieczeństwie

Sztuczna inteligencja jako broń atakujących

Złośliwe wykorzystanie sztucznej inteligencji stało się jednym z najpoważniejszych zagrożeń dla bezpieczeństwa przedsiębiorstw. Cyberprzestępcy wykorzystują sztuczną inteligencję do automatyzacji rozpoznania, tworzenia hiperspersonalizowanych kampanii phishingowych i opracowywania adaptacyjnego złośliwego oprogramowania, które potrafi omijać tradycyjne systemy wykrywania.

Narzędzia oparte na sztucznej inteligencji analizują publicznie dostępne dane, aby tworzyć profile celów, generować przekonujące materiały audio i wideo typu deepfake oraz wykorzystywać luki w zabezpieczeniach z chirurgiczną precyzją^[1]^[2].

1. <https://gcore.com/blog/10-cybersecurity-trends-2025/>

2. <https://www.pkfod.com/insights/7-cybersecurity-predictions-for-2025/>

3. <https://swisscyberinstitute.com/blog/top-5-cybersecurity-trends-2025/>

Broszura

Chroń i daj siłę swojej firmie dzięki Alcatel-Lucent Enterprise

Charakterystycznym przykładem są wiadomości e-mail phishingowe generowane przez sztuczną inteligencję, które naśladują naturalny styl komunikacji, zwiększając skuteczność o 40% w porównaniu z tradycyjnymi metodami^[3]. Ataki te są dodatkowo wzmacniane przez komodyfikację narzędzi sztucznej inteligencji, co obniża barierę wejścia dla mniej doświadczonych atakujących^[2].

Technologia deepfake to wyjątkowo podstępne zastosowanie sztucznej inteligencji, umożliwiające atakującym podszywanie się pod kadrę kierowniczą lub zaufanych współpracowników podczas rozmów wideo w czasie rzeczywistym w celu autoryzowania fałszywych transakcji lub ujawniania poufnych informacji^[1]^[3]. W jednym udokumentowanym przypadku nagranie typu deepfake przedstawiające dyrektora finansowego zlecającego przelew bankowy spowodowało utratę przez międzynarodową korporację 25 milionów dolarów^[2]. Takie incydenty pokazują, jak ważne jest stosowanie zaawansowanych protokołów uwierzytelniania i szkolenie pracowników w zakresie rozpoznawania syntetycznych komunikatów.

Sztuczna inteligencja jako mechanizm obronny

Paradoksalnie, sztuczna inteligencja stanowi również podstawę nowoczesnych mechanizmów cyberbezpieczeństwa. Algorytmy uczenia maszynowego analizują duże zbiory danych w celu wykrywania anomalii, przewidywania wektorów ataków i automatyzacji reagowania na incydenty. Przykładowo systemy bezpieczeństwa wspomagane sztuczną inteligencją potrafią identyfikować luki typu zero-day, rozpoznając subtelne wzorce zachowań w ruchu sieciowym, co pozwala skrócić średni czas wykrycia z tygodni do godzin^[1]. Według firmy Gartner organizacje inwestujące w platformy do analizy zagrożeń oparte na sztucznej inteligencji odnotowują o 30 procent mniej przypadków udanych naruszeń bezpieczeństwa w porównaniu z organizacjami korzystającymi ze starszych systemów^[4]. Systemy oparte na sztucznej inteligencji są szczególnie skuteczne w identyfikowaniu zagrożeń wewnętrznych poprzez monitorowanie zachowań użytkowników i sygnalizowanie nietypowych wzorców dostępu, co jest coraz ważniejsze w dzisiejszych zdalnych i hybrydowych środowiskach pracy.

Wyzwania regulacyjne i etyczne

Podwójne zastosowanie sztucznej inteligencji spowodowało wprowadzenie rygorystycznych regulacji. Ustawa UE o sztucznej inteligencji, uchwalona w lutym 2025 r., zabrania wykorzystywania wysoce ryzykownych zastosowań sztucznej inteligencji w takich obszarach, jak nadzór biometryczny i nakazuje przejrzystość w podejmowaniu decyzji algorytmicznych^[3]. Przedsiębiorstwa muszą teraz przeprowadzać niezależne audyty systemów sztucznej inteligencji, dokumentować pochodzenie danych i zapewniać etyczne korzystanie z nich — jest to skomplikowane zadanie, biorąc pod uwagę nieprzejrzystość wielu modeli uczenia maszynowego. Organizacje powołują przekrojowe komisje etyczne ds. sztucznej inteligencji, aby poruszać się po tym obszarze i współpracować z organami regulacyjnymi w celu kształtowania przyszłych ram.

Eskalacja ataków ransomware i na łańcuch dostaw

Celowanie w kluczowych dostawców

Ataki typu ransomware ewoluowały od kampanii oportunistycznych do strategicznych operacji wymierzonych w kluczowych dostawców i usługodawców. Ataki na CDK Global i Change Healthcare w 2024 r. pokazały, jak destabilizacja pojedynczego dostawcy może sparaliżować całe branże, generując miliardy dolarów w postaci zakłóceń operacyjnych i wysiłków naprawczych^[5]. W roku 2025 atakujący coraz częściej skupiają się na dostawcach oprogramowania jako usługi (SaaS) i firmach zajmujących się infrastrukturą chmurową, wykorzystując ich scentralizowaną rolę w ekosystemach przedsiębiorstw. Na przykład atak ransomware na dużego dostawcę pamięci masowej w chmurze może jednocześnie pozbawić tysiące firm dostępu do ich danych, zwiększając tym samym możliwości wymuszenia^[2].

Rozprzestrzenianie się powiązanych ze sobą systemów i niewystarczające zarządzanie ryzykiem w łańcuchu dostaw ułatwiają tego typu ataki. Wiele przedsiębiorstw nie ma wglądu w zabezpieczenia swoich dostawców, co naraża je na lawinowe awarie. Firma Gartner podaje, że do 2026 r. 60% organizacji będzie musiało zmierzyć się ze znacznym naruszeniem łańcucha dostaw spowodowanym lukami w zabezpieczeniach podmiotów zewnętrznych w procesach DevOps i flotach urządzeń IoT^[4].

Ekosystemy ransomware-as-a-service (RaaS)

Rozwój platform typu ransomware-as-a-service sprawił, że dostęp do zaawansowanych narzędzi ataków stał się bardziej powszechny, umożliwiając nawet mało doświadczonym przestępcom przeprowadzanie wyrafinowanych kampanii. Operatorzy RaaS zapewniają konfigurowalne złośliwe oprogramowanie, portale płatnicze i wsparcie negocjacji w zamian za część okupu — zazwyczaj wynoszącą od 20 do 30 procent^[2]. Model ten doprowadził do wzrostu o 150% liczby incydentów z użyciem oprogramowania wymuszającego okup od 2023 r., a średnie żądania okupu przekroczyły 5 milionów dolarów za incydent^[2].

Współczesne oprogramowanie ransomware wykorzystuje techniki zaciemniania oparte na sztucznej inteligencji, takie jak kod polimorficzny i szyfrowanie z opóźnieniem czasowym, aby uniknąć wykrycia. Napastnicy wykradają również dane przed wdrożeniem szyfrowania, grożąc ujawnieniem poufnych informacji, jeśli nie otrzymają zapłaty — taktyka ta jest znana jako podwójne wymuszenie^[1]. Przedsiębiorstwa przeciwdziałają tym zagrożeniom, stosując odizolowane od sieci kopie zapasowe, zdecentralizowane rozwiązania do przechowywania danych i systemy weryfikacji integralności oparte na technologii blockchain^[1].

Organizacje będą potrzebowały bezpiecznych technologii na każdym szczeblu, aby zapobiegać atakom typu ransomware i atakom na łańcuchy dostaw, powstrzymując je i ograniczać ich skutki.

1. <https://gcore.com/blog/10-cybersecurity-trends-2025/>

2. <https://www.pkfod.com/insights/7-cybersecurity-predictions-for-2025/>

3. <https://swisscyberinstitute.com/blog/top-5-cybersecurity-trends-2025/>

4. <https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025>

5. <https://www.staysafeonline.org/articles/cybersecurity-predictions-for-2025-challenges-and-opportunities>

Zarządzanie tożsamością i nakaz zerowego zaufania

Kryzys tożsamości maszyn

Wraz z wdrażaniem przez przedsiębiorstwa generatywnej sztucznej inteligencji, Internetu rzeczy i architektur chmurowych, liczba danych identyfikacyjnych maszyn — dane uwierzytelniające urządzenia, interfejsy API i zautomatyzowane ciągi — przewyższyła liczbę ludzkich danych osobowych, a co za tym idzie również ich poziom ryzyka. Firma Gartner wskazuje, że niezarządzane dane identyfikacyjne maszyn będą głównym wektorem ataków w 2025 r., a zagrożone klucze API i konta usług będą przyczyną 45% naruszeń bezpieczeństwa chmury^[4]. Aby temu zaradzić, firmy coraz częściej wdrażają narzędzia do zarządzania certyfikatami, które automatyzują częstszą rotację danych identyfikacyjnych, wzmacniając w ten sposób zasady dotyczące najmniejszych uprawnień w celu wykrywania nieprawidłowego zachowania maszyn w czasie rzeczywistym^[1].

Architektura Zero Trust w praktyce

Ramy podejścia oparte na zasadzie zerowego zaufania, które zakładają, że żaden człowiek ani maszyna nie jest z natury godny zaufania, przesunęły się z celów ambitnych na potrzeby operacyjne. Wdrażanie koncentruje się na ciągłym uwierzytelnianiu, mikrosegmentacji i szyfrowanej komunikacji. Na przykład sieć o zerowym zaufaniu może wymagać weryfikacji biometrycznej w celu zapewnienia dostępu do poufnych danych, odizolowania środowisk programistycznych od systemów produkcyjnych i szyfrowania całego ruchu wschód-zachód w centrach danych^{[1][3]}.

Narodowy Instytut Norm i Technologii Stanów Zjednoczonych (NIST) podaje, że organizacje, które wdrażają zasadę zerowego zaufania, zmniejszają średnio o 70 procent skutki naruszeń^[1]. Sukces zależy od zintegrowania zasad zerowego zaufania z istniejącą infrastrukturą, co stanowi wyzwanie dla przedsiębiorstw korzystających ze starszych systemów. Coraz większą popularność zyskują podejścia hybrydowe, takie jak programowo definiowane kręgi dla zasobów lokalnych i rozwiązania zero trust oparte na chmurze^[3].

Czynnik ludzkie i zagrożenia wewnętrzne

Według Światowego Forum Ekonomicznego 95 procent incydentów związanych z bezpieczeństwem cybernetycznym ma miejsce z powodu błędu ludzkiego. Ataki phishingowe wykorzystujące treści generowane przez sztuczną inteligencję omijają filtry poczty e-mail o 30 procent skuteczniej niż tradycyjne metody, a nieumyślne ujawnienie przez pracowników danych uwierzytelniających w narzędziach do współpracy stanowi przyczynę 25 procent naruszeń^[5] [2]. Zagrożenia wewnętrzne nasilają się w wyniku błędów w ręcznej konfiguracji dostępu do sieci i pracy zdalnej, w której urządzenia osobiste i niezabezpieczone sieci stanowią punkty wejścia dla atakujących.

Konieczne stało się umożliwienie użytkownikom lepszej ochrony siebie, przy jednoczesnym łagodzeniu obciążeń wynikających z coraz bardziej restrykcyjnych zasad bezpieczeństwa. Administratorzy sieci i aplikacji muszą zadbać o automatyzację operacji oraz aktywne wsparcie za pomocą sztucznej inteligencji, aby zapewnić narzędzia niezbędne do ochrony przed skutkami potencjalnych błędnych konfiguracji.

Broszura

Chroń i daj siłę swojej firmie dzięki Alcatel-Lucent Enterprise

Podejście ALE do zabezpieczania komunikacji i produktów sieciowych

Podejście Alcatel-Lucent Enterprise do kwestii bezpieczeństwa ma na celu zapewnienie skuteczności interakcji cyfrowych i zgodności ich ze standardowymi przepisami branżowymi. Technologia cyfrowa jest powszechna, a coraz częściej stosuje się sztuczną inteligencję (SI) i urządzenia IoT, zbierające dane w celu obsługi alertów w czasie rzeczywistym i planowania przyszłości. Zabezpieczenie i wzmocnienie sieci oraz komunikacji, na których opiera się dzisiejsze przedsiębiorstwo, ma kluczowe znaczenie dla uniknięcia przerw w świadczeniu usług. Rozwiązania ALE przeznaczone do komunikacji biznesowej i infrastruktury sieciowej wdrażają kompleksowe zabezpieczenia cybernetyczne, ponieważ jest to jedyny sposób na zagwarantowanie kompleksowego stosowania zabezpieczeń. Takie podejście do cyberbezpieczeństwa pomaga przedsiębiorstwom i instytucjom publicznym:

- Zapobiegać cyberatakam, wdrażając zabezpieczenia cybernetyczne w każdym aspekcie konstrukcji produktu, aby zmniejszyć obszar podatny na atak
- Zapewnić ochronę przed cyberatakami, wdrażając we wszystkich elementach rozwiązania najnowsze standardy bezpieczeństwa i najlepsze praktyki w celu zwiększenia odporności
- Reagować na cyberataki, podejmując w przypadku wystąpienia ataku szybkie i adekwatne działania w celu ograniczenia skutków i zwiększenia odporności

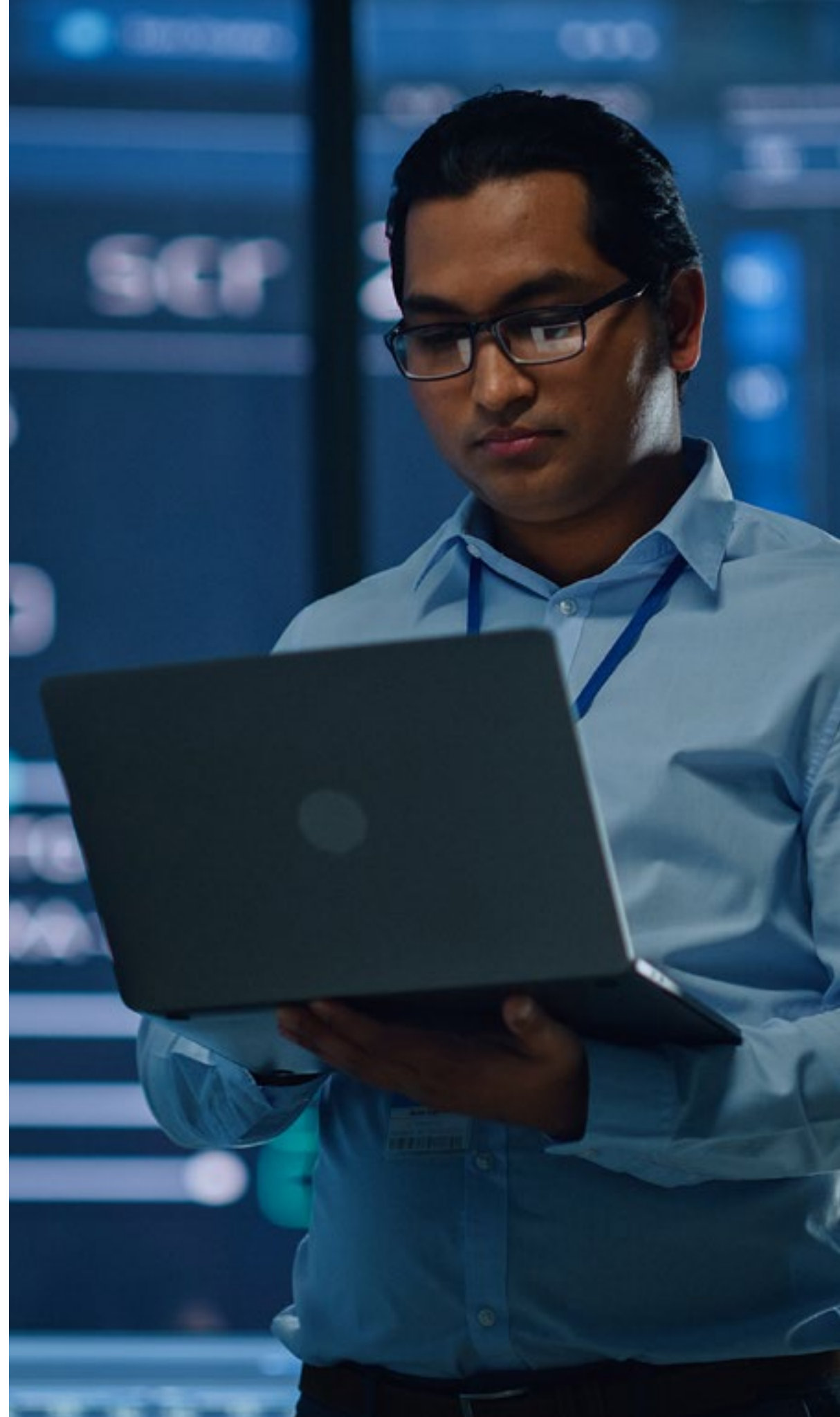
Podejście firmy ALE, producenta sprzętu i oprogramowania, do kwestii cyberbezpieczeństwa koncentruje się na obszarach opisanych poniżej, aby wykryć potencjalne luki w zabezpieczeniach przeciwko cyberzagrożeniom.

1. Projektowanie z myślą o bezpieczeństwie

W przeszłości większość projektów rozwiązań wynikała z potrzeby wprowadzenia nowych funkcji, a bezpieczeństwo było kwestią ważną, ale drugorzędną. W bieżącej sytuacji tradycyjne priorytety projektowe uległy odwróceniu. Wymagania dotyczące cyberbezpieczeństwa muszą obecnie determinować projektowanie rozwiązań. Rozwiązania sprzętowe i programowe, które z założenia są bezpieczne, uwzględniają bezpieczeństwo na każdym etapie od koncepcji, przez opracowanie po dostarczenie produktu. Cały sprzęt i systemy operacyjne są wzmacniane, zabezpieczenia typu „odmowa usługi” (DoS) są zintegrowane, a w rozwiązaniach wdrażane są najlepsze praktyki w zakresie cyberbezpieczeństwa, które są dla branży najważniejsze.

Broszura

Chroń i daj siłę swojej firmie dzięki Alcatel-Lucent Enterprise





2. Bezpieczeństwo dostępu do sieci dzięki zasadzie zerowego zaufania

Strategie bezpieczeństwa zapewniające zaufanie na podstawie lokalizacji użytkowników w firmowej zaporze ogniowej, wprowadzanych przez nich danych uwierzytelniających lub używanej aplikacji bądź urządzenia już nie wystarczają – nawet w przypadku połączenia wielu mechanizmów bezpieczeństwa. Obecnie żaden użytkownik, urządzenie ani aplikacja nie powinny być darzone zaufaniem dorozumianym. Model bezpieczeństwa dostępu do sieci dzięki zasadzie zerowego zaufania (ZTNA) pomaga organizacjom skutecznie przeciwdziałać stale ewoluującym zagrożeniom. ZTNA nie ufa żadnemu użytkownikowi, urządzeniu ani aplikacji, bez względu na lokalizację. Firma ALE stosuje zasady ZTNA, umożliwiając egzekwowanie zasad opartych na rolach, kontrolę dostępu uwzględniającą lokalizację i dynamiczną segmentację użytkowników, urządzeń i aplikacji — niezależnie od tego, czy są zarządzane, czy nie.

3. Makro- i mikrosegmentacja

Makro- i mikrosegmentacja umożliwia szczegółowe i wysoce kontrolowane podejście do cyberbezpieczeństwa wszystkich zróżnicowanych użytkowników, urządzeń i aplikacji uzyskujących dostęp do sieci. Makrosegmentacja polega na segregowaniu użytkowników, urządzeń i aplikacji zgodnie z ich domeną funkcjonalną, aby nie mogli komunikować się z elementami w innych makrosegmentach. Na przykład aplikacje do zunifikowanej komunikacji i współpracy w jednym makrosegmencie nie mogą komunikować się z technologiami bezpieczeństwa, takimi jak kamery CCTV i systemy zamków do drzwi, w drugim makrosegmencie lub z czujnikami i elementami sterującymi oświetleniem, ogrzewaniem i klimatyzacją w trzecim makrosegmencie.

Mikrosegmentacja określa, w jaki sposób użytkownicy, urządzenia i aplikacje w ramach makrosegmentu mogą wchodzić ze sobą w interakcje i zwykle podlega bardzo szczegółowym zasadom bezpieczeństwa. Na przykład kamera monitorująca nie powinna łączyć się z blokadą w drzwiach, mimo że znajdują się one w tym samym makrosegmencie związanym z bezpieczeństwem.

4. Szyfrowanie na całej drodze przesyłu danych

W nowoczesnych organizacjach pracownicy, klienci, partnerzy i dostawcy mogą znajdować się w dowolnym miejscu na świecie. Z kolei rozwiązania, których używają do komunikacji i współpracy, mogą być zainstalowane w budynku, w którym pracują, po drugiej stronie miasta lub w centrum danych na drugiej półkuli. W każdym przypadku ludzie muszą mieć możliwość bezpiecznej i poufnej wymiany informacji za pomocą głosu, wideo i tekstu. Aby mieć pewność, że tylko uczestnicy rozmowy mają dostęp do wymienianych informacji, każda rozmowa musi być w pełni zaszyfrowana od źródła do miejsca docelowego. Oznacza to, że każdy element sprzętu i oprogramowania biorący udział w komunikacji typu „end to end” musi mieć wbudowane mechanizmy szyfrowania zatwierdzone przez agencje bezpieczeństwa.

5. Certyfikaty bezpieczeństwa i prywatności oraz zgodność z przepisami

Kilka lat temu najbardziej rygorystyczne certyfikaty i akredytacje bezpieczeństwa były wymagane tylko w przypadku produktów zabezpieczających, takich jak zapory ogniowe, lub w określonych branżach, takich jak wojskowość. Obecnie standardy bezpieczeństwa muszą być stosowane do wszystkich produktów technologicznych we wszystkich sektorach. Kluczowe jest sprawdzenie, czy uznane certyfikaty i akredytacje potwierdzają twierdzenia dotyczące cyberbezpieczeństwa.

Oto kilka przykładów zgodności, których należy szukać:

- Globalne standardy bezpieczeństwa i prywatności, takie jak ISO 27001
- Specyficzne dla branży standardy bezpieczeństwa i prywatności, takie 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
- Regionalne standardy bezpieczeństwa i prywatności, takie jak rozporządzenie o ochronie danych osobowych (RODO) oraz dyrektywa NIS 2 w Unii Europejskiej

6. Ciągłe, specjalistyczne testy bezpieczeństwa

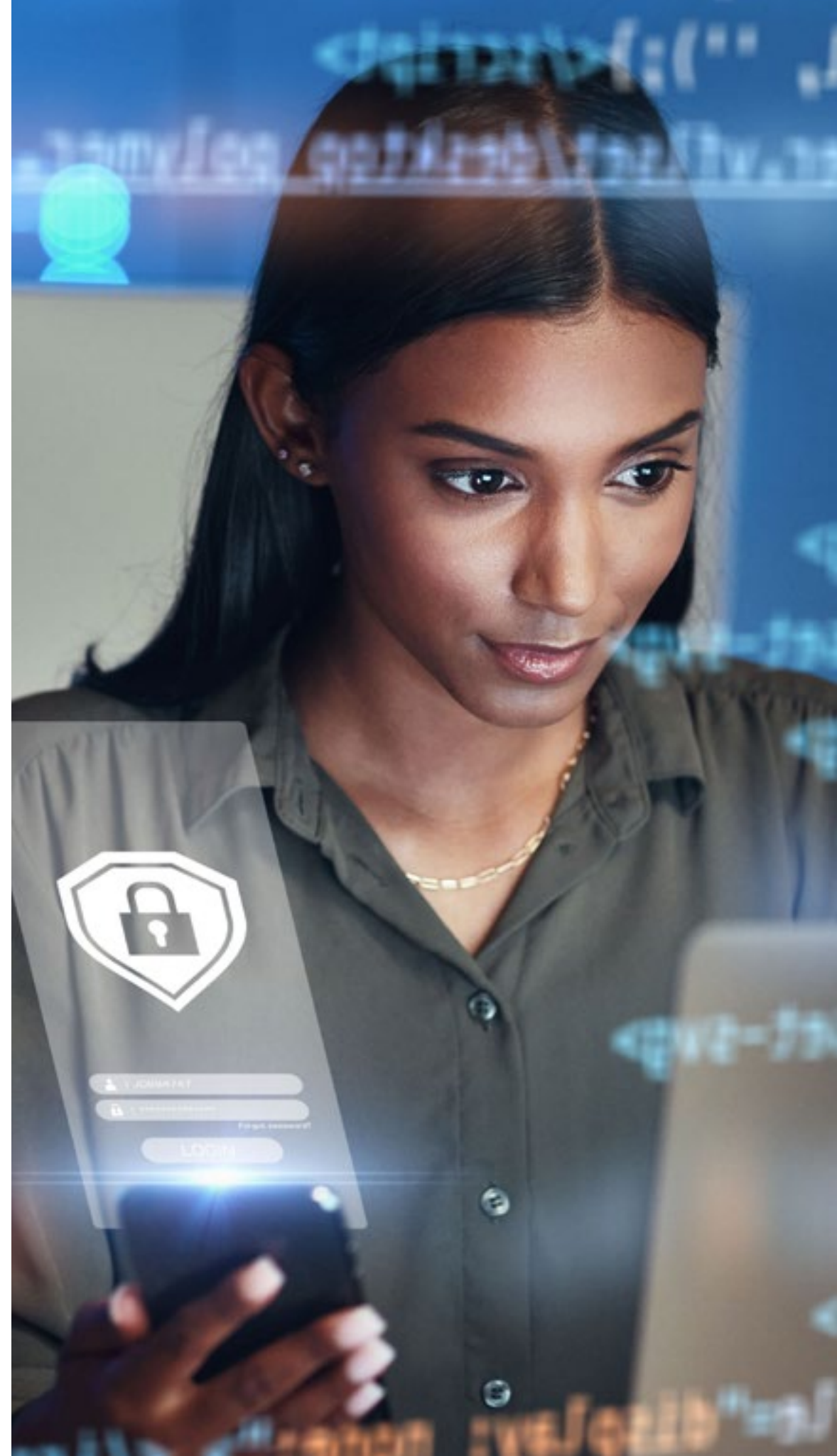
Podobnie jak standardy bezpieczeństwa, wyspecjalizowane procesy testowania zabezpieczeń, które kiedyś były zarezerwowane dla produktów zabezpieczających, są teraz obowiązkowe w rozwiązaniach do zunifikowanej komunikacji i współpracy. Doskonałym przykładem są testy penetracyjne. Testy te symulują cyberataki w celu ujawnienia luk w zabezpieczeniach, dzięki czemu można je proaktywnie usunąć, zanim pojawią się problemy. Aby być o krok przed cyberzagrożeniami w ciągle zmieniającym się środowisku, testy penetracyjne, które są oparte wyłącznie na wymaganiach bezpieczeństwa cybernetycznego, muszą być prowadzone na bieżąco. Dostawcy technologii pomagający swoim klientom w utrzymaniu maksymalnego bezpieczeństwa cybernetycznego muszą zapewnić zasoby, narzędzia i wiedzę niezbędne do prowadzenia ciągłych testów penetracyjnych.

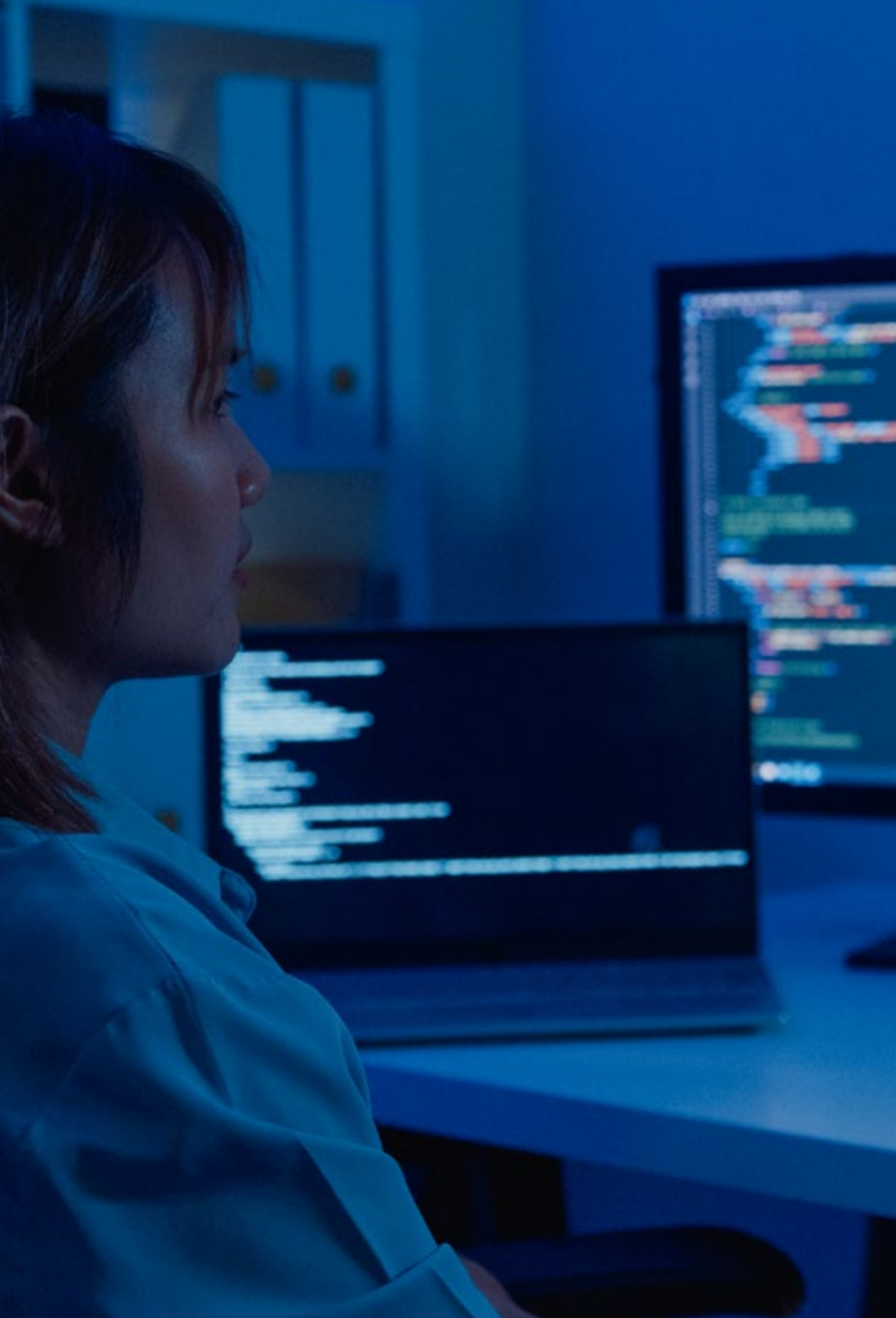
7. Suwerenność danych

Suwerenność danych stała się istotną kwestią dla większości przedsiębiorstw, które muszą chronić swoją własność intelektualną, dbać o zaufanie klientów i zapewniać sobie przewagę konkurencyjną. Dzięki wdrażaniu nowych technologii, takich jak chmura obliczeniowa, a ostatnio także sztuczna inteligencja, otwartość systemów komunikacyjnych organizacji na świat zewnętrzny stała się ważniejsza niż kiedykolwiek wcześniej, a bezpieczeństwo dostępu do sieci stało się równie istotne. Niektóre firmy decydują się na rozwiązanie chmury publicznej, które spełnia ich potrzeby, a jednocześnie ogranicza wewnętrzną powierzchnię ataku ich systemu informatycznego. Inni zdecydują się na bardziej tradycyjne podejście, wykorzystując aplikacje do komunikacji ujednoliconej hostowane w sieci prywatnej, na miejscu lub w dedykowanej chmurze prywatnej. Bez względu na wybór klienta, firma ALE jest w stanie dostarczyć swoje produkty i usługi we wszystkich kontekstach wdrożenia, aby zapewnić suwerenność nad krytycznymi danymi.

Broszura

Chroń i daj siłę swojej firmie dzięki Alcatel-Lucent Enterprise





8. Inteligentne operacje i automatyzacja bezpieczeństwa

Pakiet OmniVista i Network Advisor firmy ALE zapewniają zaawansowane bezpieczeństwo operacyjne dzięki monitorowaniu w czasie rzeczywistym, audytom konfiguracji i automatyzacji reagowania na zagrożenia. Dzięki wbudowanemu AIOps anomalie sieciowe są wykrywane proaktywnie, a następnie dostarczane są wskazówki dotyczące ich rozwiązania. Często do rozwiązania problemów z jakością doświadczenia (QoE) lub zgodnością wystarczy jedno kliknięcie. Zmniejsza to ryzyko wystąpienia błędu ludzkiego, przyspiesza reakcję na incydenty i zapewnia zgodność z polityką w złożonych środowiskach.

9. Bezpieczna łączność wszędzie

Firma ALE obsługuje bezpieczną sieć SD-WAN dla przedsiębiorstw rozproszonych i pracy zdalnej, łącząc widoczność sieci, bezpieczeństwo i optymalizację wydajności, dostosowując się do nowoczesnych modeli pracy z dowolnego miejsca. Szyfrowanie MACsec pozwala zachować integralność i poufność danych w środowiskach WAN obejmujących wiele lokalizacji.

10. Bezpieczny łańcuch dostaw oprogramowania

Firma ALE stosuje rygorystyczne środki bezpieczeństwa w celu zabezpieczenia swojego łańcucha dostaw oprogramowania, obejmujące sygnowane obrazy oprogramowania sprzętowego, bezpieczne procesy rozruchu, wzmocnione systemy operacyjne i niezależną walidację kodu źródłowego. Praktyki te ograniczają narażenie na zagrożenia ze strony oprogramowania i zapewniają zaufane środowiska wdrożeniowe.



Dlaczego firma ALE jest Twoim zaufanym dostawcą zabezpieczeń infrastruktury sieciowej i platformy komunikacji biznesowej

Chociaż wielu dostawców technologii kładzie nacisk na bezpieczeństwo cybernetyczne, nie wszyscy mają wszechstronną wiedzę specjalistyczną w zakresie wdrażania kompleksowych zabezpieczeń. Firma Alcatel-Lucent Enterprise znacznie wyprzedza innych dostawców, wdrażając wszystkie najlepsze praktyki wymagane dla kompleksowego bezpieczeństwa cybernetycznego. Zobowiązujemy się:

- Postępować 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
- Stosować normę ISO 27001 do wszystkich naszych rozwiązań opartych na chmurze
- Stosować ZTNA, szczegółową segmentację sieci i bardzo szczegółowe zasady bezpieczeństwa, aby zmniejszyć ryzyko nieautoryzowanych działań
- Przeprowadzać wysoce specjalistyczne testy bezpieczeństwa, takie jak testy penetracyjne, na wszystkich naszych produktach

- Dbać o to, by nasze produkty posiadały kluczowe certyfikaty branżowe, takie jak HDS, HIPAA oraz ustawa Family Educational Rights and Privacy Act (FERPA) oraz FIPS 140-2 dla sektora administracji publicznej i wojskowego
- W przypadku naszych produktów brać pod uwagę certyfikaty regionalne, takie jak CSPN firmy ANSSI we Francji, ENS w Hiszpanii, C5 w Niemczech i ANATEL w Brazylii
- Przestrzegać regionalnych przepisów dotyczących bezpieczeństwa i prywatności, takich jak RODO i dyrektywa NIS 2 w Unii Europejskiej

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

Broszura

Chroń i daj siłę swojej firmie dzięki Alcatel-Lucent Enterprise



Zakończenie

Trendy w dziedzinie cyberbezpieczeństwa w 2025 r. wymagają zmiany paradygmatu w strategii przedsiębiorstw. Organizacje muszą pogodzić podwójną rolę sztucznej inteligencji, która może być jednocześnie zagrożeniem i obrońcą, inwestować w odporne łańcuchy dostaw, aby przeciwstawić się atakom ransomware, oraz przeprojektować systemy zarządzania tożsamościami, aby sprostać wyzwaniom świata zerowego zaufania. Przestrzeganie przepisów, etyczne wykorzystanie sztucznej inteligencji i współpraca międzybranżowa będą miały kluczowe znaczenie dla ograniczania ryzyka. Wraz ze zwiększaniem się powierzchni ataków związanych z przetwarzaniem brzegowym i wdrażaniem Internetu rzeczy, przedsiębiorstwa, które postawią na adaptacyjne mechanizmy obronne, edukację pracowników i proaktywne wykrywanie zagrożeń, będą miały największe szanse na rozwój w tym niestabilnym otoczeniu. Aby pójść naprzód, potrzebne są innowacje technologiczne oraz wsparcie i wiedza fachowa zaufanego wykonawcy, takiego jak ALE.

Dowiedz się więcej

Aby dowiedzieć się więcej, odwiedź stronę [ALE Security Solutions](#). Jeśli chcesz porozmawiać z jednym z naszych ekspertów ds. bezpieczeństwa, [skontaktuj się z nami](#).