

Rozmowa z Arturem Józefiakiem, Dyrektorem Zespołu Bezpieczeństwa w Accenture w Polsce i Europie środkowowschodniej



Artur Józefiak, Dyrektor Zespołu Bezpieczeństwa w Accenture w Polsce i Europie środkowowschodniej fot. mat. prasowe

Podczas Kongresu 590, który na początku października odbył się w Rzeszowie, wziął Pan udział w panelu dyskusyjnym „Polski wkład w sukces globalnych marek”. Jakie główne wnioski płyną z tej dyskusji w odniesieniu do działań Accenture?

Accenture, jako firma globalna, zapewnia dostęp do rozwiązań i doświadczeń z całego świata, a także transferuje wiedzę w zakresie najnowszych trendów i technologii do polskiej gospodarki. Jednocześnie promujemy rodzime rozwiązania i polskich ekspertów za granicą. Przykładowo zbudowany w Polsce, przy udziale Accenture, system e-bankingu dla mBanku został wdrożony we francuskiej instytucji finansowej. Nie bez znaczenia jest także udział polskich ekspertów Accenture w globalnych projektach. Ich wysokie kompetencje i bardzo dobra praca promują Polskę i sprawiają, że nasz kraj postrzegany jest jako godny zaufania partner

Przedsiębiorcy nierzadko obawiają się wykorzystywania zaawansowanych rozwiązań charakterystycznych dla Przemysłu 4.0. Jak Pan sądzi, dlaczego?

Panuje przekonanie, że niosą one za sobą nierozpoznane jeszcze do końca ryzyka. Jest w tym sporo racji, dlatego tak ważne jest systemowe i uwzględniające kwestie bezpieczeństwa podejście do takich wdrożeń. Realizujemy już takie projekty w Europie Zachodniej, zapewniając bezpieczeństwo na poziomie pojedynczych urządzeń (Industrial IoT) czy całych systemów przemysłowych, które wykorzystują np. automatyzację procesów

czy sztuczną inteligencję. Kluczowe jest, żeby obawy przed nienazwanymi zagrożeniami zastąpić rzetelną analizą zagrożeń i mieć na uwadze bezpieczeństwo rozwiązania od fazy projektowania aż po utrzymanie systemu.

Jednym z elementów tych wdrożeń jest skalowalny system zarządzania tożsamością? Jakie są korzyści dla firmy, która wprowadzi tego rodzaju rozwiązanie?

W skalowalnym systemie zarządzania tożsamością możemy, w sposób scentralizowany, zdecydować, który z pracowników do jakich obszarów działania firmy ma dostęp i jakie ma uprawnienia. Możemy tym również na bieżąco, elastycznie zarządzać. Firmy coraz chętniej wykorzystują te rozwiązania, ponieważ zyskują w ten sposób lepszą kontrolę nad bezpieczeństwem, przyspieszają procesy oraz obniżają koszty. W warunkach Przemysłu 4.0, skalowalne systemy zarządzania tożsamością dotyczą również inteligentnych urządzeń, które uzyskują autonomiczność w procesach produkcyjnych. Trzeba więc być zdolnym do zarządzania tym, gdzie i jakie operacje mogą wykonywać oraz w jaki sposób elastycznie modyfikować te uprawnienia.

Jak dużym wyzwaniem dla przedsiębiorstw, w kontekście Przemysłu 4.0, jest zapewnienie odpowiedniego cyberbezpieczeństwa?

Przemysł 4.0 opiera się na cyfryzacji procesów produkcyjnych poprzez integrację systemów sterowania fabrykami z sieciami i systemami zewnętrznymi, potencjalnie niezaufanymi. Szereg spośród stosowanych dziś systemów zabezpieczeń, kiedy wdrażano te systemy, nie istniało. Wyzwaniem dla firm jest zabezpieczyć systemy, tak aby ryzyko ciągłości biznesowej spadło na tyle, na ile jest to możliwe bez konieczności kosztownej wymiany systemu na nowy. Wysokopoziomowa wiedza, na temat tego jakie zabezpieczenia należy stosować jest publicznie dostępne, jednak warto wspomnieć, że

wybór konkretnych i przede wszystkim adekwatnych rozwiązań oraz samo wdrożenie wymaga doświadczenia i wykwalifikowanego zespołu.

Jakie są najczęstsze bariery we wdrażaniu rozwiązań z zakresu cyberbezpieczeństwa w firmach?

Największą barierą jest świadomość – lub jej brak – dotycząca zagrożeń, jakie niesie za sobą w dzisiejszych czasach świat cyfrowy. Standardowe mechanizmy bezpieczeństwa przestają wystarczać – coraz bardziej wyrafinowane oraz coraz intensywniej wykorzystywane metody ataku, wymagają skomplikowanych i zaawansowanych mechanizmów. Wiele instytucji nie ma świadomości, że stale podlega ryzyku cyberataków, nie zdaje sobie też sprawy z wynikających konsekwencji. Inną kwestią jest brak korelacji potrzeb z potencjalnym ryzykiem – często polskie firmy kupują to, co nowe bez zastanowienia się czy jest im to w ogóle potrzebne. Poważnym problemem jest natomiast brak na polskim rynku wykwalifikowanych kadr, a każde nowe rozwiązanie technologiczne wymaga wsparcia od strony ludzkiej przy odpowiednich umiejętnościach w zakresie bezpieczeństwa IT .

W jaki sposób Accenture Security może pomóc zarówno w podjęciu decyzji, jak i wdrożeniu rozwiązań z zakresu cyberbezpieczeństwa?

Przede wszystkim zaczynamy od zrozumienia jakie zasoby firmy należy chronić, jakie są najważniejsze podatności i wynikających z nich ryzyka dla ciągłości pracy, bezpieczeństwa personelu i w rezultacie biznesu klienta. Proponujemy takie zabezpieczenia, które pozwolą klientowi podjąć świadomie decyzję o tym, na co i ile przeznaczyć środków, aby było to optymalne dla jego biznesu. W nasze analizy włączamy ekspertów z danego sektora, aby umożliwić klientowi jeszcze lepsze zrozumienie procesu zarządzania ryzykiem cyberataku na dany system w kontekście ryzyka biznesowego jego przedsiębiorstwa. Wdrażając

brakujące rozwiązania „pod klucz”, w efekcie zapewniamy pełne dostosowanie organizacji do nowych realiów, przeprowadzając zespoły klienta przez niezbędne procesy transformacyjne.

Co decyduje o tym, że wdrożenie rozwiązań związanych z zapewnieniem bezpieczeństwa jest dla przedsiębiorstwa nie kosztem, ale inwestycją?

Wiele firm nie zastanawia się, jak raz podniesiony poziom bezpieczeństwa utrzymać w przyszłości. Spora część wdrożeń bezpieczeństwa ciągle kończy swój żywot wraz z wyczerpaniem się budżetu CAPEX, a przecież ktoś je potem musi utrzymywać. Potrzebne są aktualizacje procesów pracy z systemami. Mam na myśli testy oraz szkolenia personelu w tym zakresie. Obszar OT, czyli automatyki biznesowej jest szczególnie narażony, ponieważ do tej pory zmieniał się powoli, a przynajmniej wolniej niż obszar biurowego IT. OT nie jest przyzwyczajany do wysokiego tempa zmian. Bez odpowiednio przeprowadzonej transformacji, wdrożone rozwiązania bezpieczeństwa nie dostarczą oczekiwanej od nich wartości. I na ten aspekt położyłbym największy nacisk, ponieważ jako inwestycja zwróci się nam w przyszłości.

Dziękujemy za rozmowę