**Cyfrowa tarcza odpowiedzią firm telekomunikacyjnych na zagrożenia dla biznesu**

**Rosnące napięcie geopolityczne, powtarzające się cyberataki, postępy w rozwoju sztucznej inteligencji (AI), oraz hybrydowa architektura chmurowa. Świat wciąż się zmienia, więc systemy bezpieczeństwa również nie mogą stać w miejscu. F5 wyjaśnia jak firmy z branży telekomunikacyjnej mogą wesprzeć swoich partnerów w coraz mniej komfortowym otoczeniu sieciowym.**

Ponieważ cyberprzestępcy coraz częściej wykorzystują sztuczną inteligencję do łamania zabezpieczeń organizacji, agencje sektora publicznego, firmy telekomunikacyjne i inni dostawcy kluczowych elementów infrastruktury stają się głównymi celami ataków. W niektórych przypadkach hakerzy wykorzystują słabości systemu i luki bezpieczeństwa, które pojawiają się podczas transformacji cyfrowej, co może zakłócić istniejące procedury sprawdzania systemów. W miarę rozpowszechniania oprogramowania w różnych chmurach i infrastrukturze wewnętrznej, zbyt łatwo jest naruszyć zabezpieczenia zbudowane dla starszej architektury, która wciąż obecna jest w firmach.

**Geopolityka ma znaczenie**

Razem z transformacją cyfrową, znaczenie mają też uwarunkowania międzynarodowe. Zmienna geopolityka sprawia, że cyberbezpieczeństwo staje się jednym z priorytetów działań instytucji rządowych. Dla przykładu, Unia Europejska przeznaczyła 2 miliardy euro z publicznych pieniędzy na poprawę ochrony cybernetycznej regionu w latach 2021-2027, w ramach strategii bezpieczeństwa cybernetycznego UE. Oznacza to aż czterokrotne zwiększenie inwestycji w porównaniu do poprzedniej strategii.

**Centralizacja jako klucz do ochrony systemu**

*Aby skutecznie utrzymać normy bezpieczeństwa w całej mocno rozproszonej organizacji, potrzebujemy scentralizowanego środowiska zarządzania, które może automatycznie wykrywać pojawiające się zagrożenia w dowolnym miejscu na świecie i łagodzić je tak szybko, jak to możliwe.* – **mówi Alix Leconte, wiceprezes Service Providers (EMEA) F5.**

Dlaczego centralizacja jest ważna? Mówiąc najprościej, w przypadku nowych informacji z zewnątrz lub rzeczywistego ataku potrzebna jest szybka i skoordynowana reakcja całej organizacji. Nie ma czasu na podjęcie działań obronnych przez każdą jednostkę lub agencję z osobna. Potrzebny jest centralny punkt kontroli, który może natychmiast wprowadzić nowe zasady - ogólnofirmowy "kill switch", który automatycznie wyłączy cały ruch przychodzący z podejrzanych źródeł.

Tego rodzaju solidna "cyfrowa tarcza" może natychmiast wykryć złośliwe działania ukierunkowane na aplikacje i dane rozproszone w wielu chmurach oraz środowiskach lokalnych. W tym kontekście szczególnie ważna jest analityka behawioralna - wiele ataków jest tak zakorzenionych w środowisku, że jedynym sposobem ich wykrycia jest identyfikacja wzorców zachowania określonych osób. Cyfrowa osłona oprócz szybkości reakcji, musi być elastyczna i zdolna do szybkiego przełączania się pomiędzy różnymi trybami obrony, w zależności od charakteru nadchodzącego ataku. Jednocześnie musi być też zgodna z lokalnymi zasadami i przepisami. Na przykład, ramy ochrony danych i bezpieczeństwa w USA różnią się znacznie od tych w Europie.

**Rola sektora telekomunikacji w procesie**

Jak pokazują analizy F5, firmy telekomunikacyjne są dobrze przygotowane do wdrażania cyfrowych osłon. Na wielu rynkach spodziewamy się, że coraz większa liczba operatorów będzie włączać tarcze cyfrowe do portfolio swoich rozwiązań. Ponieważ operatorzy telekomunikacyjni są właścicielami dużej części infrastruktury, którą organizacje wykorzystują do łączenia swoich operacji, cyfrowa osłona staje się naturalnym rozszerzeniem ich istniejących propozycji dla przedsiębiorstw. Na swoich rodzimych rynkach, operatorzy telekomunikacyjni cieszą się również zaufaniem władz. W sektorze publicznym, telco może mieć wyższy poziom zgodności z zasadami bezpieczeństwa niż ten dostępny dla innych mniej regulowanych podmiotów.

Sektor telco może oferować niezbędne oprogramowanie jako usługę dla swoich klientów korporacyjnych. Jednak w niektórych przypadkach, przedsiębiorstwo może potrzebować uruchomić rozwiązanie na miejscu, aby spełnić wymagania dotyczące bezpieczeństwa i ochrony danych.

Tego rodzaju usługa zarządzana musi współpracować z istniejącymi systemami bezpieczeństwa przedsiębiorstwa. Nie zalecamy stosowania podejścia "wyrwij i zastąp". Nacisk powinien być położony na wykorzystanie tego, co już istnieje, przy jednoczesnym zapewnieniu precyzyjnej kontroli nad systemami bezpieczeństwa za pośrednictwem jednej tarczy obronnej.

Cyfrowa osłona musi być również wysoce modułowa i programowalna, z warstwami bezpieczeństwa, które mogą być aktywowane przyrostowo, a nie w modelu wszystko albo nic. Jeśli przedsiębiorstwo zareaguje przesadnie i wyłączy cały ruch, z pewnością nie będzie mogło prowadzić działań w normalnym trybie. W niektórych przypadkach może chcieć jedynie wyłączyć konkretną aplikację lub zablokować przepływ danych z określonej lokalizacji.

Ponadto cyfrowa tarcza powinna uwzględniać DevOps, aby inżynierowie mogli tworzyć niestandardowe schematy zabezpieczeń dla konkretnych przypadków użycia. Mogą na przykład chcieć zapobiec przesyłaniu określonych typów danych do konkretnych krajów.

*Zachęcające jest to, że telekomy zaczynają zdawać sobie sprawę z oferowanych korzyści. F5 współpracuje obecnie z firmami telekomunikacyjnymi, aby zapewnić przedsiębiorstwom cyfrowe tarcze. Dostarczamy technologię bazową do telco, które następnie pakują ją w usługę zarządzaną. W tym miejscu pojawia się F5 Distributed Cloud Web Application and API Protection (WAAP), zawierająca funkcje takie jak F5's Advanced Web Application Firewall, technologię bezpieczeństwa API, obronę przed botami opartą na sztucznej inteligencji oraz ochronę przed rozproszonymi atakami typu DDoS (Distributed Denial-of-Service).* – **mówi Ireneusz Wiśniewski, dyrektor zarządzający F5 Poland.**

Patrząc w przyszłość, zdolność firmy telekomunikacyjnej do dostarczania niestandardowych osłon cyfrowych będzie źródłem zróżnicowania całej branży. W miarę zaspokajania zapotrzebowania na większe bezpieczeństwo cyfrowe, pozycja firm wzrośnie również w oczach decydentów i opinii publicznej.

**Informacje o F5**

F5 (NASDAQ: [FFIV](https://www.nasdaq.com/symbol/ffiv)) to firma zajmująca się bezpieczeństwem i dostarczaniem aplikacji w środowiskach wielochmurowych oraz umożliwia klientom – w tym największym na świecie przedsiębiorstwom, instytucjom finansowym, dostawcom usług i rządom – wprowadzanie w życie niezwykłych doświadczeń cyfrowych. Po więcej informacji przejdź do [strony f5.com](https://www.f5.com/). Śledź [@F5](https://twitter.com/f5) na Twitterze lub odwiedź nasz profil [LinkedIn](https://www.linkedin.com/company/f5/) i [Facebooku](https://www.facebook.com/f5incorporated), aby uzyskać więcej informacji na temat F5, jej partnerów i technologii.

F5 i BIG-IP są znakami towarowymi, znakami usługowymi lub nazwami handlowymi firmy F5, Inc. w Stanach Zjednoczonych i innych krajach. Wszystkie inne nazwy produktów i firm w niniejszym dokumencie mogą być znakami towarowymi ich odpowiednich właścicieli.

**Kontakt:**

Marcin Ołdakowski | Senior Account Executive w Monday Comms | marcin.oldakowski@mondaygroup.pl