PRZEKSZTAŁCANIE KOMUNIKACJI W SEKTORZE BEZPIECZEŃSTWA PUBLICZNEGO W EUROPIE I AFRYCE: CZTERY KLUCZOWE CZYNNIKI

MOTOROLA SOLUTIONS

BADANIE SEKTORA BEZPIECZEŃSTWA PUBLICZNEGO 2015 – EUROPA I AFRYKA

OMÓWIENIE

Komunikacja w sektorze bezpieczeństwa publicznego stale się zmienia. Na skutek dostępu do danych w czasie rzeczywistym, zaangażowania społeczności i interakcji społecznych, migracji do sieci szerokopasmowych oraz wyzwań związanych z wprowadzaniem i zarządzaniem nowymi narzędziami i technologiami.

Badanie pokazuje, w jaki sposób te cztery kluczowe czynniki wpływają na instytucje, niezależnie od ich wielkości. A także na to, w jaki sposób zmiana jest napędzana przez szybkie strumienie danych oraz konieczność komunikacji pomiędzy różnymi sieciami i urządzeniami, m.in. radiotelefonami, smartfonami i tabletami.

CZYNNIK 1. SZYBKIE STRUMIENIE DANYCH W CZASIE RZECZYWISTYM

Możliwość uzyskania dostępu do danych w czasie rzeczywistym ma zasadnicze znaczenie i jest jednym z najważniejszych czynników zidentyfikowanych w badaniu. Aż 77% ankietowanych stwierdziło, że natychmiastowy dostęp do wiarygodnych informacji jest dla nich kluczowy lub bardzo ważny podczas pracy w terenie.

77%

ANKIETOWANYCH STWIERDZIŁO, ŻE DANE W CZASIE RZECZYWISTYM SĄ DLA NICH KLUCZOWE LUB BARDZO WAŻNE

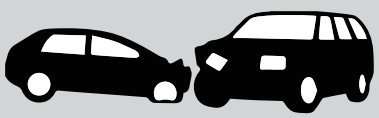
Przy coraz większej ilości danych zalewających dyspozytornie i centra dowodzenia kluczowym wyzwaniem jest zidentyfikowanie istotnych informacji i przekształcenie ich w wiedzę nadającą się do wykorzystania. Ponad 60% oczekuje ukierunkowanych danych w czasie rzeczywistym, dostępnych w trakcie zdarzenia i pomocnych w planowaniu i realizacji skutecznej, bezpiecznej interwencji.

60%

ANKIETOWANYCH OCZEKUJE DANYCH W CZASIE RZECZYWISTYM, DOSTĘPNYCH W TRAKCIE ZDARZENIA

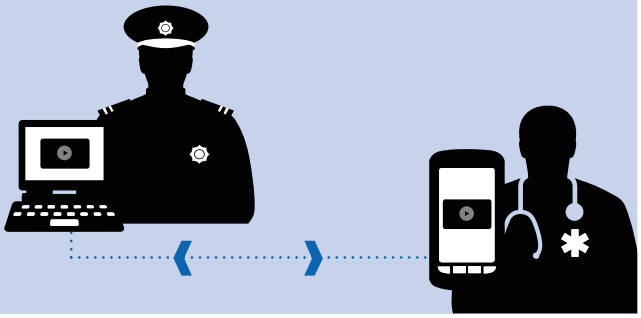
Dlaczego szybkie strumienie danych w czasie rzeczywistym są takie ważne? Ponieważ umożliwiają one ankietowanym szybkie otrzymanie informacji potrzebnych do podzielenia się wymaganą wiedzą ze współpracownikami i lokalnymi placówkami w danej okolicy. Badanie wykazało, jak ważna jest możliwość komunikowania się pomiędzy różnymi sieciami i urządzeniami – od radiotelefonów i laptopów po telefony komórkowe i modemy.

76%



POTRZEBUJE DOSTĘPU DO SZYBKICH STRUMIENI DANYCH W TERENIE, ABY NATYCHMIAST UZYSKAĆ WYMAGANĄ WIEDZĘ

72% POTRZEBUJE ŁATWEJ KOMUNIKACJI Z **LOKALNYMI PLACÓWKAMI**



81% WYMAGA MOŻLIWOŚCI SWOBODNEGO KOMUNIKOWANIA SIĘ POMIĘDZY **RÓŻNYMI SIECIAMI I URZĄDZENIAMI**

Gdy napływają dane w czasie rzeczywistym, wszystko jest optymalizowane w celu zapewnienia jak najlepszych wyników. Bliższa współpraca i współdzielona łączność są obecnie ważniejsze niż kiedykolwiek przedtem w celu zapewnienia możliwości interoperacyjności i koordynacji różnych pracowników z różnych służb bezpieczeństwa publicznego, którzy korzystają z różnorodnych urządzeń.

CZYNNIK 2. ZAANGAŻOWANIE SPOŁECZNOŚCI I INTERAKCJE SPOŁECZNE

Powszechne wykorzystanie mediów społecznościowych w codziennym życiu otwiera nowe możliwości w dziedzinie bezpieczeństwa publicznego. Coraz więcej postronnych świadków nagrywa zdarzenia przy użyciu urządzeń mobilnych i udostępnia je za pośrednictwem mediów społecznościowych na stronach takich jak Facebook i Twitter. W konsekwencji powstaje bezcenny rejestr zdarzeń, który właściwe służby mogą wykorzystać do zapobiegania przestępstwom, wykrywania sprawców oraz rozwiązywania innych problemów.

Wyniki badania pokazują, że media społecznościowe są powszechnie uznane w sektorze bezpieczeństwa publicznego. Niemal trzy czwarte uczestników badania wykorzystuje je do nadawania wiadomości, a ponad połowa do odbierania informacji i monitorowania zdarzeń w trakcie ich trwania.

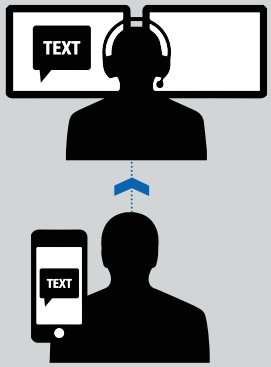
73% ANKIETOWANYCH KORZYSTA Z MEDIÓW **SPOŁECZNOŚCIOWYCH DO UPUBLICZNIANIA INFORMACJI**

54% ANKIETOWANYCH KORZYSTA Z MEDIÓW **SPOŁECZNOŚCIOWYCH DO ODBIERANIA UPUBLICZNIANYCH INFORMACJI**

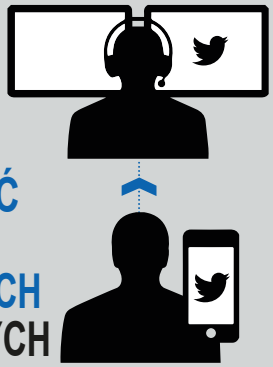
52% ANKIETOWANYCH KORZYSTA Z MEDIÓW **SPOŁECZNOŚCIOWYCH DO MONITOROWANIA ZDARZEŃ**

Media społecznościowe stały się nieodzowną platformą do budowania zaangażowania społeczności i interakcji społecznych. Promują one otwarte rozmowy z osobami prywatnymi i wspomagają właściwe zgłaszanie zdarzeń. Badanie pokazuje, że niemal połowa centrów powiadamiania ratunkowego jest obecnie w stanie przyjmować wiadomości tekstowe, zdjęcia i dane z mediów społecznościowych w takiej czy innej formie od osób prywatnych, a jedna trzecia może przyjmować materiały wideo. Jest to pozytywne zjawisko, podkreślające możliwości, jakimi dysponują centra powiadamiania w zakresie poszerzania sposobów otrzymywania danych od osób prywatnych.

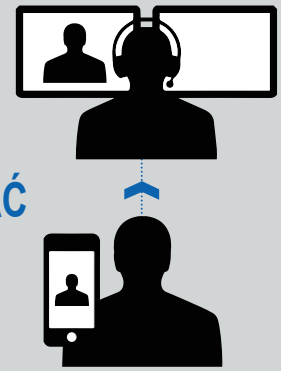
49%
CENTRÓW POWIADAMIANIA RATUNKOWEGO MOŻE PRZYJMOWAĆ
WIADOMOŚCI TEKSTOWE OD OSÓB PRYWATNYCH



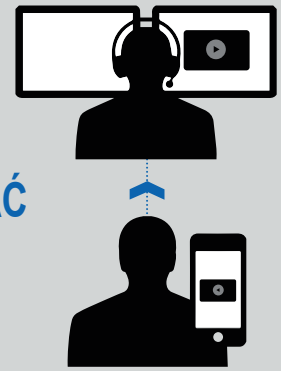
46%
CENTRÓW POWIADAMIANIA RATUNKOWEGO
MOŻE PRZYJMOWAĆ POSTY Z MEDIÓW SPOŁECZNOŚCIOWYCH OD OSÓB PRYWATNYCH



42%
CENTRÓW POWIADAMIANIA RATUNKOWEGO
MOŻE PRZYJMOWAĆ ZDJĘCIA OD OSÓB PRYWATNYCH



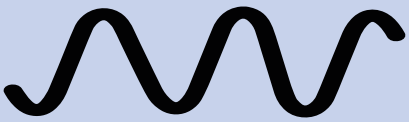
32%
CENTRÓW POWIADAMIANIA RATUNKOWEGO
MOŻE PRZYJMOWAĆ MATERIAŁY WIDEO OD OSÓB PRYWATNYCH



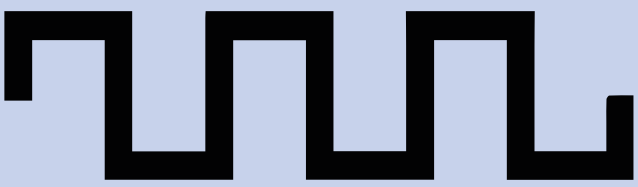
CZYNNIK 3. ROZWÓJ RADIOTELEFONÓW CYFROWYCH I SIECI SZEROKOPASMOWYCH

Ankietowani z sektora bezpieczeństwa publicznego polegają na komunikacji, a przejście na sieci szerokopasmowe jest postrzegane jako kluczowy cel. Badanie pokazuje, że ponad 60% ankietowanych już korzysta z cyfrowej sieci LMR (TETRA, P25, DMR) lub rozważa przejście na technologię cyfrową w ciągu najbliższych trzech lat.

33% ANKIETOWANYCH
JUŻ KORZYSTA Z SIECI CYFROWEJ



28% ANKIETOWANYCH
ROZWAŻA MIGRACJĘ W CIĄGU TRZECH LAT



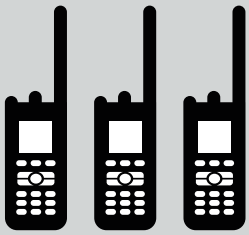
Niektóre instytucje przechodzą z analogowych systemów radiowych na cyfrowe naziemne systemy mobilne, np. TETRA, i wprowadzają systemy szerokopasmowe, jak np. LTE. Większość korzysta z połączenia obu technologii, instalując paralelne systemy LTE, które pracują równolegle do istniejących, nowych lub modernizowanych rozwiązań LMR.

39%
ANKIETOWANYCH
CZEKĄ NA ROZWÓJ FUNKCJI GŁOSOWYCH LTE

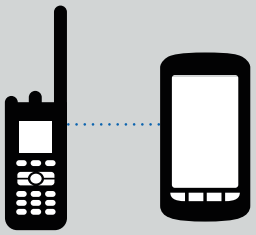
47%
ANKIETOWANYCH
CHCE KORZYSTAĆ Z LTE RÓWNOLEGLE DO ISTNIEJACEGO SYSTEMU LMR

Aby jak najlepiej wykorzystać coraz bardziej dostępne, bogate informacje cyfrowe, niektóre służby bezpieczeństwa publicznego będą korzystać z kilku sieci. Badanie pokazuje kontynuację inwestycji w LMR, często w połączeniu z planami w zakresie LTE. Tylko niewielka liczba organizacji zaprzestała inwestowania lub zredukowała inwestycje w LMR.

28%
ANKIETOWANYCH
KONTYNUUJE INWESTYCJE W LMR



44%
ANKIETOWANYCH KONTYNUUJE INWESTYCJE W LMR
PRZY JEDNOCZESNYM PLANOWANIU PRZYSZŁEJ SIECI LTE



Ma to sens. Sieci LMR są zawsze dostępnym standardem dla łączności głosowej o kluczowym znaczeniu i najważniejszych aplikacji danych. LTE stanowi dopełnienie tych sieci, wzbogacając je o możliwość szybkiego dostępu i transmisji danych szerokopasmowych. Organizacje planują z wyprzedzeniem, aby zapewnić współpracę tych technologii w celu zwiększenia wydajności operacyjnej i bezpieczeństwa.

Rzecz jasna, przy przechodzeniu na szerokopasmową sieć bezpieczeństwa publicznego pojawiają się wyzwania, którym trzeba stawić czoła. Prawie jedna trzecia ankietowanych jest ograniczona budżetem, 27% martwi się o postrzeganie niezawodności lub dostępności sieci, 18% obawia się słabego zasięgu regionalnego, a 16% – braku wspólnych standardów.

CZYNNIK 4. ZARZĄDZANIE NARZĘDZAMI I TECHNOLOGIĄ

Podczas gdy służby bezpieczeństwa publicznego podejmują wyzwanie zarządzania nowymi narzędziami i technologiami, w chwili obecnej nie znają wszystkich odpowiedzi. Badanie pokazuje, jak szerokie rozpowszechnienie smartfonów, ciągłe bariery dla przyjęcia technologii wideo oraz brak zrozumienia cyberbezpieczeństwa grożą ograniczeniem skuteczności rozwiązań w zakresie nowych technologii.

Efekt smartfona jest cały czas aktualną kwestią. Użytkownicy z sektora bezpieczeństwa publicznego oczekują takiej samej funkcjonalności od narzędzi używanych w pracy, jak w przypadku urządzeń, z których korzystają prywatnie. Ponad 40% ankietowanych używa własnych smartfonów na służbie, a tylko 26% instytucji zwraca im koszty. Wiele organizacji nadal zaopatruje swoich pracowników w smartfony, pomimo potencjalnych zagrożeń bezpieczeństwa, problemów z trwałością oraz braku dedykowanych funkcji bezpieczeństwa.

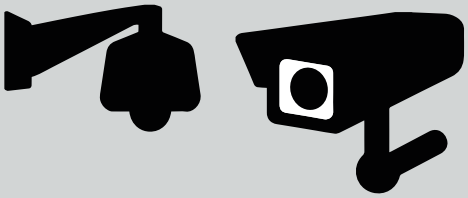
41%
ANKIETOWANYCH
UŻYWA WŁASNYCH SMARTFONÓW

30%
SŁUŻB BEZPIECZEŃSTWA PUBLICZNEGO
ZAOPATRUJE PERSONEL CENTRÓW DOWODZENIA ORAZ CZĘŚĆ ANKIETOWANYCH W SMARTFONY

11%
SŁUŻB BZPIECZEŃSTWA PUBLICZNEGO
ZAOPATRUJE WSZYSTKICH ANKIETOWANYCH W SMARTFONY

Technologia wideo to kolejna niewykorzystana szansa. Pozwala ona śledzić sekwencję zdarzeń, pomaga wykrywać sprawców zdarzeń i chroni ankietowanych przed fałszywymi oskarżeniami. Mniej niż połowa ankietowanych korzysta z rozwiązań wideo; głównie są to stałe systemy nadzoru i kamery w pojazdach. Co jeszcze bardziej zaskakujące, zaledwie 15% organizacji używa oprogramowania do analizy wideo, co sugeruje, że powszechna jest analiza manualna. Ograniczenia budżetowe wydają się być najpoważniejszą barierą dla przyjęcia technologii wideo. 44% ankietowanych wymienia ogólne koszty administracyjne oraz koszty zarządzania dużymi ilościami danych jako główne powody niezainstalowania systemów wideo.

37%
SŁUŻB BEZPIECZEŃSTWA PUBLICZNEGO
KORZYSTA ZE STAŁEGO SYSTEMU NADZORU WIDEO



25%
SŁUŻB BEZPIECZEŃSTWA PUBLICZNEGO
KORZYSTA Z KAMER W POJAZDACH

18%
SŁUŻB BEZPIECZEŃSTWA PUBLICZNEGO
KORZYSTA Z KAMER NOSZONYCH NA CIELE LUB NA KASKU

Badanie pokazuje, że służby korzystają z całego szeregu narzędzi do walki z zagrożeniami w dziedzinie cyberbezpieczeństwa dotyczącymi posiadanych sieci i urządzeń. Skanery i zapory sieciowe przeciw wirusom i złośliwemu oprogramowaniu są najpopularniejszymi narzędziami, stosowanymi odpowiednio przez 77% i 72% ankietowanych. Jednak – co zaskakujące – 22% ankietowanych nie wiedziało, z jakich narzędzi korzysta, lub nie korzystało z żadnych narzędzi tego typu.

Nie ulega wątpliwości, że nowe narzędzia i technologie wymagają zarządzania. Przejście na nowsze systemy cyfrowe wiąże się z koniecznością dysponowania bardziej zaawansowanymi umiejętnościami IT, odpowiednimi do zarządzania złożonymi sieciami i nieustannymi zagrożeniami w dziedzinie cyberbezpieczeństwa. Badanie pozwoliło zidentyfikować trzy kluczowe obszary wymagające wsparcia.

46%

SŁUŻB BEZPIECZEŃSTWA PUBLICZNEGO

WYMAGA WSPARCIA W ZAKRESIE UTRZYMANIA SIECI, ŁĄCZNIE Z DORADZTWEM TECHNICZNYM I SERWISEM

38%

SŁUŻB BEZPIECZEŃSTWA PUBLICZNEGO

WYMAGA WSPARCIA W ZAKRESIĘ USŁUG BEZPIECZEŃSTWA, ŁĄCZNIE Z AKTUALIZACJĄ BAZY WIRUSÓW I AUDYTAMI

36%

SŁUŻB BEZPIECZEŃSTWA PUBLICZNEGO

WYMAGA WSPARCIA W CAŁYM CYKLU ŻYCIA, ŁĄCZNIE Z MODERNIZACJĄ SPRZĘTU I AKTUALIZACJAMI OPROGRAMOWANIA

Ponadto 31% ankietowanych wskazało na potrzebę wsparcia w szeregu innych dziedzin, m.in. zarządzaniu operacjami sieciowymi, zarządzaniu operacjami radiowymi i konserwacji radiotelefonów.

Przy większej liczbie sieci, platformach nowych technologii oraz konieczności ciągłych aktualizacji organizacje będą w coraz większym stopniu sięgać po zewnętrzne usługi zarządzania świadczone przez ekspertów ds. sieci. Zarządzanie systemem będzie miało zasadnicze znaczenie dla zapobiegania nieprzewidzianym problemom mogącym mieć wpływ na dostępność i funkcjonalność sieci o kluczowym znaczeniu.

UCZESTNICTWO W BADANIU

Coroczne badanie firmy Motorola zapewnia wgląd w trendy w zakresie technologii w sektorze bezpieczeństwa publicznego. Badanie to zostało przeprowadzone pod koniec 2015 roku i odzwierciedla informacje uzyskane od ponad 100 profesjonalistów z branży bezpieczeństwa publicznego w Europie i Afryce w całym przekroju instytucji różnej wielkości. Badanie dla Europy i Afryki zostało przeprowadzone po raz pierwszy. Bazuje ono na podobnym badaniu przeprowadzanym w Ameryce Północnej już po raz piąty.

Spośród ankietowanych 36% instytucji zatrudnia mniej niż 50 pracowników, 17% – od 51 do 100, 6% – od 101 do 250, 9% – od 251 do 750 i 32% – ponad 750.

Uczestników badania stanowili różni funkcjonariusze służb bezpieczeństwa publicznego, w tym policji, straży pożarnej, ratownictwa medycznego, obrony cywilnej oraz wydziałów administracji rządowej.

Uwagi
1 – Wszystkie wartości procentowe zostały zaokrąglone do najbliższego pełnego procentu.

Więcej informacji na temat planowania i wdrożenia zintegrowanego podejścia komunikacyjnego w zgodzie z trendami udzieli lokalny przedstawiciel firmy Motorola. Zapraszamy także na stronę **www.motorolasolutions.com**

MOTOROLA