LIFE IS FOR SHARING.

BADANIE RYNKU BEZPIECZEŃSTWA SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH W POLSCE, 2019

PRZEPROWADZONE PRZEZ PMR

SZANOWNI PAŃSTWO,

WŁODZIMIERZ NOWAK,

Członek Zarządu

Dyrektor ds. Prawnych, Bezpieczeństwa i Zarządzania Zgodnością T-Mobile Polska

jesteśmy dziś świadkami intensywnej cyfryzacji, która stawia przed nami konieczność obserwacji stanu cyberbezpieczeństwa w firmach. Tegoroczne badanie tego obszaru poświęciliśmy kwestii zabezpieczeń służbowych urządzeń mobilnych. Taki wybór był nieprzypadkowy – uważamy, że rzetelna ocena kondycji ICT przedsiębiorstw wymaga przyglądania się różnym aspektom zagrożeń i ochrony. Chciałbym przy tym podkreślić, że obecnie, jak czytamy w raporcie, to segment firmowych urządzeń mobilnych rozwija się najprężniej. Z tym większą uwagą warto przeanalizować sposób korzystania z tych narzędzi w średnich i dużych organizacjach w kontekście bezpieczeństwa danych.

Treści, które znajdą Państwo w tym materiale, przedstawiają intensywną transformację badanego obszaru. Według danych z raportu mimo powszechnego stosowania telefonu komórkowego przez pracowników firm – obok poczty elektronicznej jest on podstawowym narzędziem pracy w dzisiejszych czasach – ponad połowa średnich firm posiada nie więcej niż dwa zabezpieczenia służbowych telefonów komórkowych, z czego 26% tylko jedno.

Wskaźnikiem, który również świadczy o początku rozwoju polityk ochrony urządzeń mobilnych, jest ten związany z kontrolą obszaru wykorzystania telefonu służbowego, jeśli chodzi o Internet. Obecnie przedsiębiorstwa w większości przypadków nie analizują tej aktywności. A przecież już połowa ruchu w sieci odbywa się z poziomu urządzeń mobilnych i ten odsetek w najbliższych latach, zgodnie z prognozami ujętymi w raporcie, wciąż będzie rosnąć. Jako firma technologiczna proponujemy organizacjom rozwiązanie tego problemu m.in. poprzez usługę Cyber Guard, która umożliwia monitorowanie wykonywanych sesji z poziomu smartfonów.

Należy także podkreślić, że ogromny wpływ na krystalizowanie się zasad stosowania sprzętu służbowego miało wprowadzenie RODO w maju 2018 r. Wciąż jednak w przypadku 23% średnich i 10% dużych firm za bezpieczeństwo telefonów służbowych nie odpowiada żaden przypisany do tego zadania dział. W tej sytuacji dobrym pomysłem jest rozważenie outsourcingu usług ICT i takie zadania jako T-Mobile także realizujemy dla różnych podmiotów.

Chciałbym przy okazji zaznaczyć, że T-Mobile, jako firma zaawansowana technologicznie, szczególnie czuje się zobligowana, by przez inicjowanie tematu bezpieczeństwa informatycznego i podejmowanie dyskusji sukcesywnie zwiększać świadomość w tym obszarze. Mam więc nadzieję, że ten raport wpłynie pozytywnie na realizację tego celu. Działania w sferze ICT od lat są priorytetem dla naszej firmy, a nasze doświadczenie i portfolio sukcesywnie rosną, obejmując obecnie usługę całodobowego monitorowania bezpieczeństwa technologicznego, weryfikowania i odpowiadania na incydenty, projektowania i zapewniania bezpiecznej infrastruktury IT czy przetwarzania i przechowywania danych.

Oczywiście obok prowadzenia analiz rynku i inicjowania dyskusji, ważnym obszarem aktywności czołowych przedsiębiorstw technologicznych powinno być proponowanie odpowiednich rozwiązań dostosowanych do warunków i sytuacji panujących w firmach.

Zarysowawszy zaledwie wątki, które kontynuację znajdują w raporcie, zachęcam Państwa do jego lektury i zapoznania się z najnowszym stanem wiedzy na temat cyberbezpieczeństwa smartfonów w polskich firmach. ■

SZANOWNI PAŃSTWO,

wraz z postępującą cyfryzacją przedsiębiorstw obszar cyberbezpieczeństwa nabiera coraz większego znaczenia. Nie tylko reputacja oraz stabilność firm w coraz większym stopniu zależą od umiejętności zabezpieczenia cyfrowych zasobów przedsiębiorstwa, ale równolegle uzyskanie dostępu do danych przynosi coraz większe korzyści. Potencjalne zyski z włamań rosną, a ataki stają się coraz bardziej złożone i zaawansowane. Trendem ostatnich lat jest wykorzystywanie do ataków nie tylko luk w zabezpieczeniach komputerów osobistych, ale coraz szerszej gamy urządzeń: routerów, drukarek, jednak przede wszystkim urządzeń mobilnych. Dlatego kompleksowe podejście do cyberbezpieczeństwa powinno dziś obejmować każde urządzenie umożliwiające połączenie z siecią, znajdujące się w firmie. T-Mobile Polska uważnie śledzi tendencje w tym obszarze i naszymi obserwacjami chcemy podzielić się z Państwem, tworząc publikację, która odpowie na pytania dotyczące bezpieczeństwa informatycznego.

W niniejszym raporcie chcemy Państwu przybliżyć zagadnienie ochrony smartfonów przed cyberatakami. Wśród najistotniejszych tematów, które analizujemy, na pierwszy plan wysuwa się wybór najpowszechniejszych narzędzi stosowanych przez firmy w celu zabezpieczenia sprzętu. Dane te będą wyjątkowo interesujące nie tylko dla dostawców takich rozwiązań. Ważną obserwacją jest także fakt, że wachlarz czynności, do których pracownicy wykorzystują służbowy sprzęt jest bardzo szeroki. Przeglądają oczywiście firmową pocztę – robi to aż 66%. z nich. Dodatkowo – w przypadku średnich firm – chętnie sięgają oni do bazy klientów i danych finansowych. Z kolei osoby zatrudnione w dużych przedsiębiorstwach otrzymują od organizacji funkcjonalności w postaci wglądu do kalendarzy pracowników, a także bardziej zaawansowane, specjalistyczne aplikacje, takie jak CRM czy ERP. Jednocześnie nierzadko zdarza się, że posiadacze służbowych smartfonów aktywnie korzystają za ich pomocą z mediów społecznościowych.

Jako przedsiębiorstwo dostarczające rozwiązania technologiczne zdajemy sobie sprawę, że taka sytuacja stanowi duże wyzwanie dla firm, które jak dotąd nie zbudowały jednolitych standardów w kwestii wykorzystania urządzeń. Rzecz jasna, część organizacji wprowadziła już jednoznaczne zasady, jednak wciąż aż 61% średnich firm oraz 31% dużych podmiotów nie posiada polityki użytkowania firmowych smartfonów. W tym przypadku w przygotowaniu odpowiednich wytycznych istotną rolę odgrywa doradztwo partnerów dysponujących niezbędnymi kompetencjami. Współpracując z zewnętrznym dostawcą usług ICT, można wypracować zbiór rozwiązań dostosowanych do potrzeb danej firmy. Od wielu lat obserwuję rynek biznesowy i w tym czasie miałem okazję niejednokrotnie zaobserwować, że kompleksowe zadbanie o bezpieczeństwo w tym zakresie nie jest dla wielu organizacji łatwe.

JAKUB GÓRNIK,

Dyrektor Departamentu Zarządzania Rozwojem Produktów, Pion B2B
T-Mobile Polska

Nietrudno tu o pewne przeoczenia, które mogą znacząco osłabić konstrukcję ochronną. Również dlatego T-Mobile Polska chce wspierać przedsiębiorstwa w tworzeniu i utrzymaniu spójnych, kompleksowych rozwiązań i od lat sukcesywnie poszerzamy zakres naszych usług w tym obszarze.

Naszą misją pozostaje zagwarantowanie bezpieczeństwa informatycznego we wszystkich wymiarach. Wymaga to nie tylko ciągłego rozwoju kompetencji, wypracowywania nowych rozwiązań oraz produktów. To także, a może przede wszystkim, ciągła obserwacja rynku, wnikliwa analiza trendów i potrzeb. Niniejszy raport stanowi efekt tej aktywności. Liczę, że dostarczy on każdemu czytelnikowi wielu ciekawych, przydatnych i skłaniających do refleksji informacji. ■

SPIS TREŚCI

1. WSTĘP

Oddajemy w Państwa ręce kompendium wiedzy na temat obecnego stanu zabezpieczeń firmowych telefonów komórkowych w polskich przedsiębiorstwach. Ogromnym atutem tego raportu jest prezentacja zagadnienia z różnych punktów widzenia – firm, użytkowników oraz operatora sieci. Podstawowym materiałem wykorzystanym w analizie tematu jest dedykowane badanie B2B – pierwsze tego typu zrealizowane na polskim rynku. Wyniki badania zostały skonfrontowane ze statystykami T-Mobile Polska, dotyczącymi potencjalnych zagrożeń, na które narażone są firmowe telefony komórkowe komunikujące się ze złośliwymi adresami IP. Całość uzupełniają komentarze ekspertów T-Mobile i PMR oraz słownik pojęć z zakresu cyberbezpieczeństwa, w tym również telefonów komórkowych.

2. STRESZCZENIE MENADŻERSKIE

Analiza niniejszego raportu prowadzi do podstawowego wniosku – **firmy w Polsce w sposób zdecydowanie niewystarczający zabezpieczają służbowe telefony komórkowe**. Z jednej strony widać poprawę, jeśli chodzi o bezpieczeństwo rozwiązań stacjonarnych i sieci firmowych. Z drugiej strony zupełnie inaczej traktowany jest obszar „mobile security". Aż 8 na 10 dużych przedsiębiorstw nie posiada oddzielnego budżetu na cyberochronę służbowych telefonów komórkowych. Wśród średnich firm odsetek ten sięga 100%.

Przedsiębiorstwa zdają się nie dostrzegać dynamicznych zmian zachodzących na rynku. Dla rosnącej liczby pracowników smartfon to obecnie drugi komputer i podstawowe narzędzie pracy, z którego 98% zatrudnionych korzysta codziennie. Pomimo tego, firmy nadal w ogromnej większości poprzestają na zabezpieczaniu ekranu (trzy czwarte dużych firm w Polsce). W praktyce ten rodzaj zabezpieczenia może wymuszać producent urządzenia lub dostawca oprogramowania, a nie zawsze jest to świadoma polityka organizacji.

Z badania wynika, że w Polsce aż 23% firm średniej wielkości i 10% dużych nie posiada w swoich strukturach żadnej jednostki oficjalnie odpowiedzialnej za bezpieczeństwo służbowych telefonów komórkowych. W co szóstym średnim przedsiębiorstwie czuwa nad nim dział administracji, co z reguły jest równoznaczne z brakiem kompetencji w tym zakresie.

Brak wiedzy na temat bezpieczeństwa potwierdza również fakt, że w praktyce **firmy nie zdają sobie sprawy z tego, co ich pracownicy robią ze służbowym telefonem**. Wątpliwe wydają się więc ich deklaracje dotyczące faktycznych incydentów. 6 na 10 pracowników działów IT średnich przedsiębiorstw i 8 na 10 w dużych organizacjach otwarcie deklaruje, że nie gromadzi informacji w obszarze wykorzystania przez pracowników służbowych telefonów do celów prywatnych. Może to być związane z zagwarantowaniem prywatności użytkownikom, zwłaszcza że pracodawcy wyrażają zgodę na używanie telefonu do celów prywatnych. Natomiast aż 18% dużych i średnich przedsiębiorstw w kraju przyznaje, że procedury RODO w firmie w ogóle pomijają temat służbowych smartfonów. **Może to w efekcie skutkować karami nałożonymi przez UODO oraz stratami finansowymi i wizerunkowymi.**

W przeprowadzonym badaniu widać duże rozbieżności między wyobrażeniem pracowników działów IT a zachowaniem użytkowników firmowych telefonów. Największe kontrowersje występują w przypadku deklaracji dotyczących dostępu do zasobów i danych przez smartfon służbowy oraz zadań, do których on służy prywatnie. Tutaj często ocena jest diametralnie różna, w zależności od tego, czy pytamy dział IT czy szeregowego użytkownika sprzętu. Co czwarty zatrudniony wykorzystuje służbowy telefon do dostępu do firmowych baz danych klientów. Potwierdzają to przedstawiciele działów IT z zaledwie 14% przedsiębiorstw. Szczególnie wyraźna różnica w ocenie ma miejsce w przypadku dużych firm, gdzie 22% pracowników deklaruje korzystanie z poziomu telefonu z firmowych baz, a potwierdza to tylko 9% przedstawicieli działów IT.

W ocenie jednostek IT tylko co dziesiąty pracownik (dokładnie 11% zatrudnionych) wykorzystuje telefon do obsługi prywatnej poczty, podczas gdy z perspektywy użytkowników sprzętu jest to jeden z głównych obszarów zastosowania firmowego smartfona. W przypadku dużych przedsiębiorstw, blisko co druga osoba (47%) używa telefonu w tym celu. Podobna sytuacja ma miejsce w przypadku hotspotów. Dwie trzecie działów IT deklaruje, że służbowe telefony nie mogą się łączyć w ten sposób z Internetem, ale w praktyce tylko 4% przedsiębiorstw blokuje taką możliwość. W efekcie **trzy czwarte pracowników łączy się z publicznym Wi-Fi przez firmową komórkę**. Jest to jasny sygnał dla organizacji, że należy skuteczniej zabezpieczać telefony służbowe, bo ich ekspozycja na ryzyko i incydenty już teraz jest bardzo częsta i będzie się zwiększała.

3. GŁÓWNE WNIOSKI, PROGNOZY I REKOMENDACJE – OKIEM ANALITYKÓW

3.1. ALARMUJĄCE WYNIKI BADANIA SŁUŻBOWYCH TELEFONÓW

Z badań PMR wynika, że już ponad trzy czwarte dorosłych Polaków w kraju deklaruje korzystanie ze smartfonów. W przypadku sektora przedsiębiorstw zdecydowana większość firm wykorzystuje telefony komórkowe w prowadzonej działalności i trudno obecnie wyobrazić sobie biznes bez komórek. Co więcej, **firmowe smartfony to coraz częściej tak naprawdę przenośne komputery**, naszpikowane już nie tylko preinstalowanymi i konsumenckimi aplikacjami, ale także gwarantujące dostęp do firmowego CRM-u, bazy i historii kontaktów z klientami, wewnętrznego komunikatora czy choćby służbowej poczty. Są to oczywiście tylko przykłady, bo zastosowań telefonu do celów B2B jest coraz więcej.

W tym kontekście wyniki badania w średnich i dużych przedsiębiorstwach, zrealizowanego przez PMR w III kw. 2019 r. na zlecenie T-Mobile Polska, dotyczące bezpieczeństwa firmowych komórek, są zdumiewające i jednocześnie alarmujące. Symptomatyczny jest choćby obserwowany trend, zgodnie z którym, analogicznie do ustaleń z naszych badań sprzed 3 i 5 lat, **firmy praktycznie nie wydzielają osobnego budżetu na zabezpieczanie służbowych telefonów**. Większość z nich poprzestaje na nakazie zabezpieczenia smartfona kodem czy wzorem. Zdaniem decydentów i osób odpowiedzialnych za firmowe bezpieczeństwo IT powinno to skutecznie zamknąć temat. Jednak nawet taki nakaz nie jest egzekwowany przez wszystkie przedsiębiorstwa, mimo że z każdym rokiem komórek jest coraz więcej, a ich możliwości i konsumpcja danych rosną. W rezultacie w 2019 r. **27% średnich firm w Polsce w ogóle nie zabezpieczało swoich firmowych komórek** i taki sprzęt może być używany bez żadnego problemu przez dowolną osobę z zewnątrz. Do zagrożeń z obszaru cyberbezpieczeństwa dochodzi też bezpieczeństwo fizyczne i waga danych, do których potencjalnie może mieć dostęp osoba nieuprawniona. Zdobyta w ten sposób na przykład firmowa książka adresowa to idealne narzędzie do ataku phishingowego. Poza tym w wielu sektorach mamy w następstwie regulacji RODO do czynienia z danymi wymagającymi szczególnej ochrony. Przede wszystkim są to dane osobowe, a w przypadku bankowości również m.in. informacje objęte tajemnicą bankową.

Często bywa, że teoria nie zawsze ma zastosowanie w praktyce i podobnie jest w tym przypadku. Osoby odpowiedzialne za utrzymanie firmowych zasobów i zarządzanie nimi, w tym telefonami komórkowymi, deklarują jedno, a użytkownicy sprzętu postępują zupełnie inaczej. Przykłady można mnożyć. Jednym z najciekawszych, moim zdaniem, są publiczne hotspoty. Według 61% przedstawicieli działów odpowiedzialnych za firmowe komórki w największych firmach w Polsce nie zezwala się na logowanie do publicznych punktów Wi-Fi, podczas gdy ponad trzy czwarte

PAWEŁ OLSZYNKA,
Dyrektor Działu Doradztwa i Analiza Rynku ICT, PMR

(78%) pracowników twierdzi, że przedsiębiorstwo na to pozwala i nic nie stoi na przeszkodzie, aby w taki sposób użyć firmowego telefonu. Można oczywiście udawać, że problemu nie ma, bo przecież skorzystanie z otwartego Wi-Fi to tylko ekspozycja na ryzyko, a nie natychmiastowa utrata danych czy nieautoryzowany dostęp do firmowych zasobów. Mimo wszystko skala nieświadomości i rozbieżności robi ogromne wrażenie, a firmy powinny zwrócić na ten aspekt uwagę i wdrożyć adekwatne rozwiązania, – zablokować dostęp albo zabezpieczyć firmowy sprzęt. Niewątpliwie jest to realne wyzwanie, z którym należy się zmierzyć.

3.2. POSTĘPUJĄCA SMARTFONIZACJA SEKTORA B2C I B2B W POLSCE

W ostatnich latach mamy w Polsce do czynienia z dynamicznym wzrostem sprzedaży smartfonów. W samym 2018 r. rynek wchłonął ich ok. 9,5 mln sztuk, czyli o 9% więcej niż rok wcześniej. Smartfony stanowią już zdecydowaną większość sprzedawanych w kraju telefonów komórkowych ogółem. W związku z tym rośnie także nasycenie tymi urządzeniami. PMR szacuje, że w 2018 r. liczba indywidualnych użytkowników smartfonów w Polsce osiągnęła próg 22,5 mln, przekładając się na 69-procentowy wskaźnik penetracji. Trzeba przy tym zaznaczyć, że wskazane wartości odnoszą się do ludności Polski w wieku 15 lat i więcej, dlatego należy mieć świadomość, że faktyczna liczba Polaków użytkujących smartfony przekracza ten poziom.

Trendy wzrostowe w sprzedaży smartfonów wiążą się przede wszystkim z coraz większą ich funkcjonalnością i zaawansowaniem technicznym, silnie sprzężonym z rozwojem sieci mobilnej oraz rynku produktów cyfrowych (streaming muzyki i wideo, gry, aplikacje mobilne, serwisy społecznościowe) i finansowych (m.in. płatności mobilne). Sprzedażową hossę smartfonów warunkuje również ich popularyzacja przez operatorów komórkowych, którzy aktywnie promują usługi „data" w połączeniu usługami głosowymi w telefonach. Według danych PMR przychody telekomów z mobilnej transmisji danych realizowanej w smartfonach odpowiadają już za przeszło 60% wartości rynku mobilnego internetu w Polsce. Poza tym smartfony są fundamentem mobilności współczesnego społeczeństwa. Ich sprzedaż rośnie zarówno pod względem ilościowym, jak i wartościowym. Wzrostowa dynamika rynku w ujęciu wartościowym to wypadkowa rosnącego wolumenu sprzedaży oraz zwyżkującego popytu na urządzenia droższe, w tym premium.

W samym segmencie przedsiębiorstw telefony komórkowe istotnie wpływają na jego funkcjonowanie, realnie rzutując na jakość, optymalizację (w tym również kosztową) i powodzenie prowadzonego biznesu. PMR szacuje, że w 2018 r. **liczba kart SIM w firmach w Polsce** wzrosła o 6%, osiągając poziom 10 mln sztuk. Okazuje się, że rynek mniej więcej utrzymał skalę zmian z ubiegłego roku. Z kolei **w 2019 r.** wolumen ten **przekroczy 10 mln**. Rosnąca baza kart SIM wykorzystywanych przez klientów biznesowych jest pochodną zwiększającej się liczby podmiotów biznesowych i pracowników oraz rozwoju gospodarki.

Obecnie wykorzystanie smartfonów w biznesie nie ogranicza się wyłącznie do usług tradycyjnych, takich jak połączenia głosowe i wiadomości SMS. W dobie coraz bardziej funkcjonalnych i zaawansowanych technologicznie smartfonów oraz postępującej transformacji cyfrowej biznesu zależność na linii smartfony-biznes jest coraz większa. To sprawia, że inteligentne telefony, oferujące

KATARZYNA SACHA,
Analityk Rynku ICT, PMR

wysoką wydajność, zastępują dziś w wielu zadaniach komputery, stając się pełnoprawnymi narzędziami pracy. Rosnąca mobilność pracowników to dodatkowy czynnik, który wzmacnia ten trend. Co ważne, podstawą zastosowania smartfonów do celów B2B jest dostęp do mobilnej transmisji danych.

A co konkretnie sprawia, że telefony komórkowe to jedne z kluczowych elementów budowania współczesnego biznesu? Tych elementów jest coraz więcej. Na pierwszy plan wysuwa się mocny ekosystem aplikacyjny, który wspomaga pracownika zarówno w wykonywaniu zadań służbowych (dostęp do przeglądarki internetowej, pakietu Office, kalendarza, skrzynki pocztowej, komunikatorów internetowych, aplikacji zadaniowych optymalizujących wszelkie procesy – nawet zakupowe), jak i w kontakcie i podtrzymywaniu relacji z klientami (dostęp do firmowego CRM-u, bazy i historii kontaktów z klientem czy mediów społecznościowych, głównie tych o charakterze ▶

profesjonalnym, rozmowy konferencyjne wideo). Ponadto jest wiele innych aplikacji pozwalających wykonywać wszystkie operacje finansowe, dostarczających narzędzia do pracy projektowej i grupowej, usprawniających zdalną komunikację między zespołami, które pracują w różnych biurach, a także umożliwiających rezerwację lotów, hoteli czy samochodów na całym świecie.

Firmowe smartfony o znacznie większej mocy obliczeniowej oraz z dostępem do platform chmurowych czy plików i sieci firmowych dają możliwość wykorzystania danych w każdym cyklu biznesowej aktywności, np. opcję drukowania materiałów/dokumentów, wygodnej pracy z plikami lub wyświetlania prezentacji u klienta na dużym ekranie z poziomu mobile device.

Smartfony w firmach przejmują również zadania innych urządzeń i rozwiązań. Jeden z głównych przykładów to płatności mobilne i online za pomocą telefonu. Coraz częściej też, wykorzystując technologię Bluetooth Smart i NFC, smartfony pozwalają na mobilne otwieranie drzwi do biura, ale także na kontrolowanie wykorzystania komputerów służbowych, logowanie do firmowych aplikacji oraz obsługę szlabanów i drzwi automatycznych.

Wykorzystanie telefonów komórkowych w firmach na coraz większą skalę pozwala również na wprowadzenie mobilnych rozwiązań w zakresie zarządzania przedsiębiorstwem i pracownikami. Na pewno do tego obszaru klasyfikuje się wszelkie aplikacje typu ERP, stworzone do prowadzenia księgowości, wystawiania faktur czy wsparcia i zdalnego serwisu IT. Specyficznymi usługami dodanymi tego rodzaju w telefonii komórkowej w segmencie biznesowym są również rozwiązania monitorujące oraz przeznaczone do zarządzania flotą samochodową. Pierwsze z nich sprowadzają się do zdalnego lokalizowania telefonów komórkowych używanych przez pracowników firmy. Drugie natomiast pozwalają na inteligentne kontrolowanie firmowych pojazdów, co umożliwia optymalizację wykorzystania floty samochodów w przedsiębiorstwie.

Prognozy dalszego zastosowania smartfonów do celów B2B oraz przeznaczonej dla nich transmisji danych są optymistyczne. W kolejnych latach kluczowe pod tym względem będzie wdrożenie oraz rozwój sieci 5G i w związku z tym podniesienie jakości mobilnych połączeń internetowych. Równolegle zyskująca na znaczeniu komunikacja M2M oraz rozwiązania bazujące na technologii IoT zwiększą zakres biznesowych funkcjonalności inteligentnych telefonów. W dłuższej perspektywie potencjał dostrzega się również w rozwoju wirtualnej rzeczywistości – smartfony, które przechwytują i zmieniają obrazy oraz wyświetlają je w realnym świecie będą kolejnym punktem zwrotnym w cyfrowej transformacji biznesu. Przewiduje się, że największe korzyści z tego będą miały: handel detaliczny, branża wsparcia technicznego i opieka zdrowotna.

W kontekście powyższych trendów zabezpieczenie firmowych komórek powinno być dla przedsiębiorstw działaniem absolutnie priorytetowym. ■

4. BEZPIECZEŃSTWO FIRMOWYCH TELEFONÓW KOMÓRKOWYCH

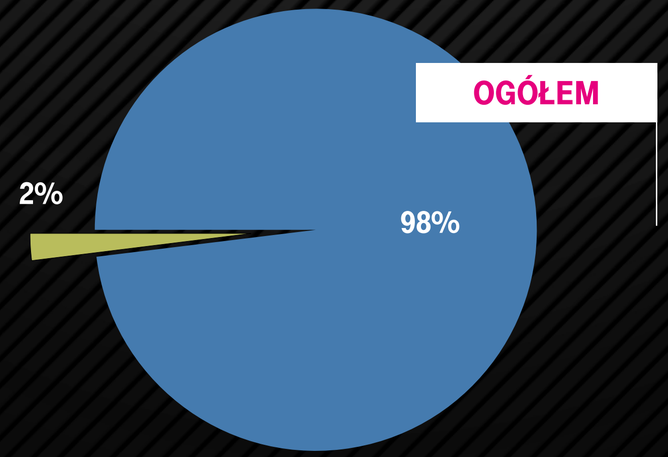
TEORIA VS. RZECZYWISTOŚĆ

Liczba telefonów komórkowych, korzystających z usług innych niż podstawowe, będzie nadal rosła. **Według najnowszych prognoz PMR w perspektywie 5 lat na potrzeby dostępu do Internetu będzie w Polsce używanych 32 mln telefonów**[1]. Już teraz blisko połowa ruchu w sieci Internet odbywa się z poziomu tych urządzeń, a udział ten będzie się zwiększał. Dla dużej liczby pracowników smartfon – ze względu na swoją moc obliczeniową i możliwość dostępu do danych firmowych – już jest drugim komputerem i podstawowym narzędziem pracy.

Faktem jest, że w Polsce liczba komputerów, zarówno w gospodarstwach domowych, jak i w firmach praktycznie się nie zwiększyła. Wzrosty poziomów penetracji z roku na rok są minimalne, a w niektórych segmentach widać nawet odejście od „ciężkiego" sprzętu na rzecz „lżejszych" urządzeń przenośnych. Z badań PMR wynika, że rosnące znaczenie smartfonów w biznesie wpłynęło na politykę zakupową firmowego sprzętu. W przypadku części stanowisk i realizowanych zadań smartfony wypierają tradycyjny hardware, powodując wydłużanie cyklu jego wymian.

Jest to pochodną przenoszenia coraz większej części firmowej działalności na telefon. Z tegorocznego badania wynika, że niemal wszyscy pracownicy średnich i dużych przedsiębiorstw korzystają ze służbowego telefonu komórkowego każdego dnia. Tylko 2% zatrudnionych sięga po niego najwyżej kilka razy w tygodniu. Badanie to potwierdza też, że obecnie smartfon to podstawowe narzędzie pracy i dla niemal 100% firm urządzenie absolutnie niezbędne.

CZĘSTOTLIWOŚĆ KORZYSTANIA ZE SŁUŻBOWEGO TELEFONU KOMÓRKOWEGO WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Codziennie	96%	100%
Kilka razy w tygodniu	4%	0%

Źródło: PMR, 2019 r.

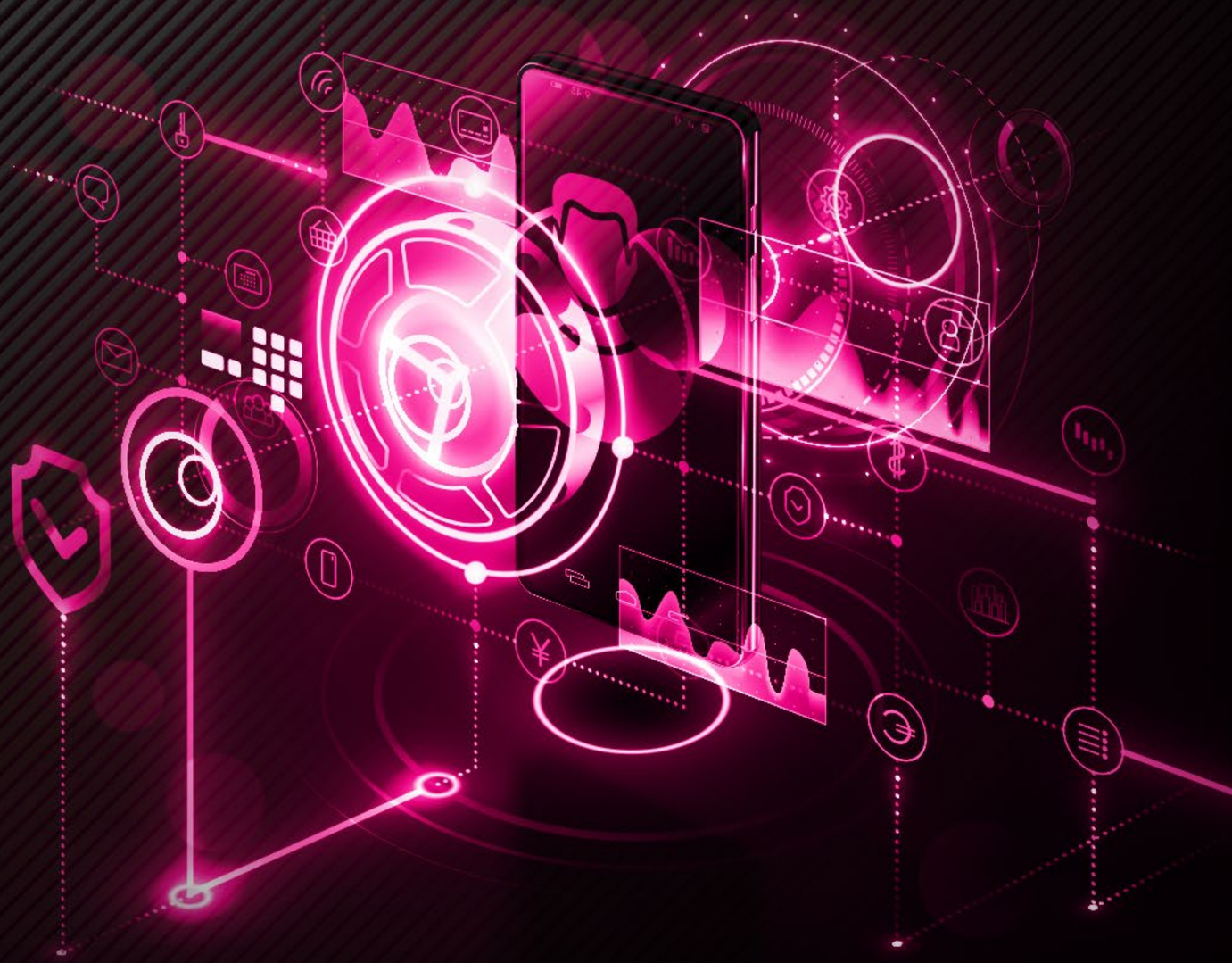
1 Raport PMR „Rynek mobilnego Internetu i usług dodanych w Polsce 2019. Analiza rynku i prognozy rozwoju na lata 2019–2024"

4.1. ZABEZPIECZENIA SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH

Najpopularniejszą metodą zapewniania bezpieczeństwa na służbowych telefonach komórkowych jest stosowanie narzędzi blokowania ekranu, którego wykorzystanie deklaruje 63% pracowników działu IT. Są one popularniejsze wśród firm zatrudniających co najmniej 250 osób – tam odsetek ten wynosi 76%.

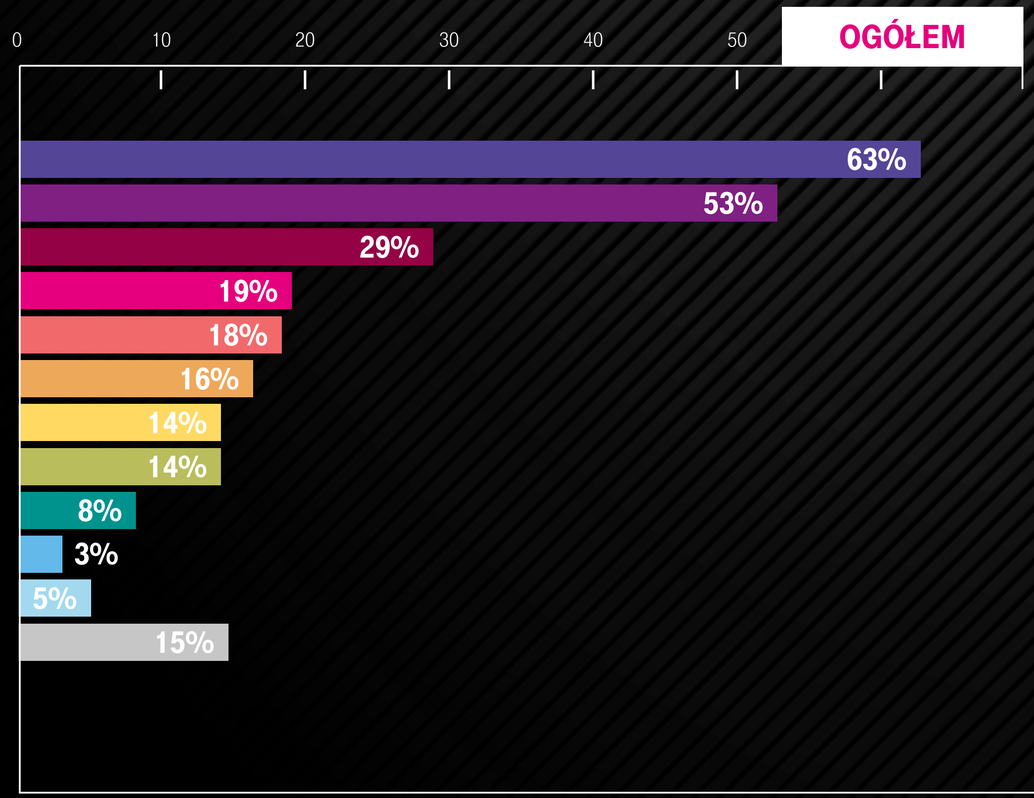
Ponad połowa średnich i dużych przedsiębiorstw posiada nie więcej niż dwa zabezpieczenia służbowych telefonów komórkowych, w tym 26% dysponuje tylko jednym. Najczęściej stosowane zabezpieczenia służbowych smartfonów to blokada ekranu i oprogramowanie antywirusowe. Obie metody często wprowadzane są również razem z procedurami postępowania w przypadku cyberataku lub kradzieży urządzenia.

Generalnie zabezpieczenia służbowych telefonów komórkowych stosowane są częściej przez duże firmy, gdzie odsetek dla każdego typu zabezpieczenia urządzeń jest średnio o 14% wyższy niż w przypadku firm średnich. Nie powinno to dziwić, biorąc pod uwagę skalę działalności i budżety, a także większą świadomość zagrożeń. W średnich przedsiębiorstwach sytuacja jest mniej optymistyczna. Warto wziąć pod uwagę fakt, że **jedna na pięć średnich firm w Polsce oficjalnie nie stosuje żadnych zabezpieczeń w służbowych telefonach komórkowych**, nie licząc się zupełnie z konsekwencjami.



SPOSOBY ZAPEWNIANIA BEZPIECZEŃSTWA SŁUŻBOWYCH TELEFONÓW

KOMÓRKOWYCH **WG DZIAŁÓW IT** W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



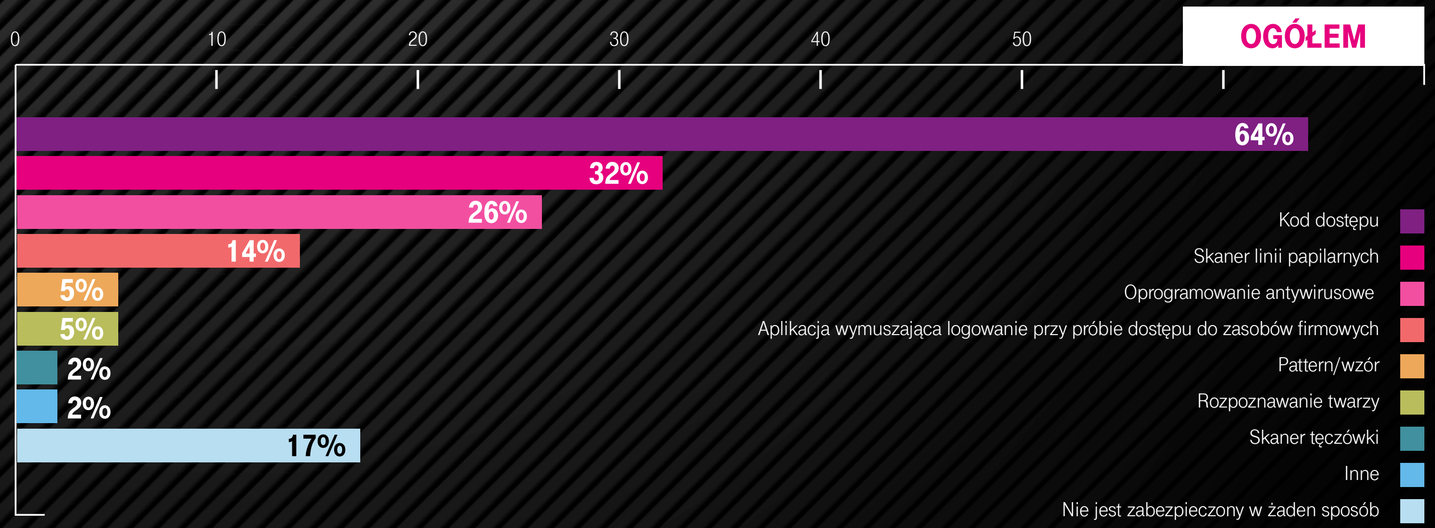
LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Wymuszanie stosowania narzędzi blokady ekranu	52%	76%
Oprogramowanie antywirusowe instalowane na urządzeniu końcowym	40%	67%
Regulamin postępowania w przypadku zagrożenia atakiem/kradzieży/zgubienia telefonu	23%	36%
Ochrona ruchu internetowego w sieci mobilnej zapewniona przez dostawcę usług	17%	22%
Narzędzia do zarządzania urządzeniami mobilnymi, typu MDM/EMM	8%	29%
Szyfrowanie komunikacji, np. VPN	8%	24%
Wymuszanie tworzenia kopii zapasowych	8%	20%
Narzędzia do szyfrowania danych	10%	18%
Narzędzia silnego uwierzytelniania (np. tokeny softwareowe, sprzętowe U2F)	4%	11%
Przekierowywanie ruchu firmowego na prywatny APN	0%	7%
Inne	6%	4%
Nie mamy żadnych narzędzi	21%	9%

Wyjaśnienie: wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

Przedstawione przez działy IT sposoby zabezpieczeń telefonów firmowych korespondują z deklaracjami samych użytkowników. Również ich zdaniem najpopularniejszym zabezpieczeniem służbowych smartfonów jest kod dostępu – posiada go 60% pracowników średnich i 68% pracowników dużych firm. Mniej popularne zabezpieczenia, aczkolwiek wykorzystywane odpowiednio przez 32% i 26% pracowników przedsiębiorstw, to: skaner linii papilarnych i oprogramowanie antywirusowe. Częściej stosowane są one w dużych organizacjach – ok. 35%. Wymienione wyżej najpopularniejsze zabezpieczenia służbowych telefonów komórkowych zazwyczaj występują razem. Trzeba przy tym podkreślić, że nawet rozpoznawanie linii papilarnych czy skaner twarzy to zabezpieczenia, które mogą zostać złamane przez potencjalnego przestępcę. Potwierdzają to choćby testy przeprowadzone przez holenderską organizację Consumentenbond – w 42 na 110 testowanych smartfonów rozpoznawanie twarzy nie działało właściwie[1].

Najistotniejszy jest jednak fakt, że w Polsce aż **27% pracowników średnich firm nie posiada żadnych zabezpieczeń na służbowym telefonie komórkowym** – to odsetek wyższy niż deklarowany przez firmowe działy IT. Co prawda tylko 6% osób badanych, zatrudnionych w dużych firmach, deklaruje całkowity brak zabezpieczeń, ale nawet taki odsetek jest zastanawiający, kiedy zdamy sobie sprawę, że chodzi o naprawdę bardzo poważne przedsiębiorstwa o dużej skali działalności i liczbie pracowników powyżej 250.

SPOSÓB ZABEZPIECZENIA SŁUŻBOWEGO TELEFONU KOMÓRKOWEGO WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Kod dostępu	60%	68%
Skaner linii papilarnych	27%	36%
Oprogramowanie antywirusowe	19%	34%
Aplikacja wymuszająca logowanie przy próbie dostępu do zasobów firmowych	6%	21%
Pattern/wzór	0%	11%
Rozpoznawanie twarzy	4%	6%
Skaner tęczówki	0%	4%
Inne	2%	2%
Nie jest zabezpieczony w żaden sposób	27%	6%

Wyjaśnienie: wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

[1] *https://www.consumentenbond.nl/veilig-internetten/gezichtsherkenning-te-hacken*

Za bezpieczeństwo służbowych telefonów komórkowych w firmach najczęściej odpowiada dział IT. Jednak nie dzieje się tak zawsze. W dużych przedsiębiorstwach taka sytuacja dotyczy 7 na 10 organizacji, w segmencie średnich podmiotów będzie to z kolei stosunek 4 do 10. **W części przedsiębiorstw obowiązek nadzoru nad bezpieczeństwem firmowych komórek spoczywa na dziale administracji** – takie podejście ma aż co szósta średnia organizacja w naszym kraju. W praktyce oznacza to zmarginalizowanie problemu. Trudno przecież oczekiwać od działu administracji, żeby posiadał wiedzę w obszarze bezpieczeństwa teleinformatycznego.

Najbardziej kontrowersyjne i jednocześnie nieco szokujące jest to, **że w Polsce aż 23% średnich i 10% dużych firm nie posiada w swoich strukturach żadnego podmiotu oficjalnie odpowiedzialnego za bezpieczeństwo służbowych telefonów komórkowych**. W 8% firm za bezpieczeństwo telefonów komórkowych nie odpowiada żaden z wymienionych w badaniu podmiotów, zaś 4% wskazało szefa/dyrektora organizacji lub zarząd.

Tegoroczne badania PMR, zrealizowane w 2019 r. potwierdzają, że odbiorcy IT nadal są mocno skoncentrowani na utrzymaniu własnych zasobów i jest to jeden z priorytetów firm. Na drugim miejscu znajduje się – przynajmniej teoretycznie – zapewnienie bezpieczeństwa. W przypadku tej dość szerokiej kategorii przedsiębiorcy wskazywali na chęć inwestowania zarówno w rozwiązania sprzętowe oraz aplikacyjne utrzymywane we własnym zakresie, jak i zakup usług z obszaru cyberbezpieczeństwa od zewnętrznego dostawcy. W przeprowadzonym badaniu ponad połowa dużych firm deklaruje, że korzysta z rozwiązań partnerów zewnętrznych obejmujących ICT, jednak dotyczy to przede wszystkim infrastruktury IT. Generalnie polskie przedsiębiorstwa są przede wszystkim skupione na bezpieczeństwie zasobów stacjonarnych. Zabezpiecza się firmowe sieci LAN/WAN i punkty styku z Internetem. W tym aspekcie w ostatnich latach widać postęp i rosnącą świadomość zagrożeń. Zupełnie inaczej wygląda analiza kategorii „mobile security", relatywnie mniej istotnego dla firm i pochopnie marginalizowanego. W rezultacie stanowi więc „back door" dla potencjalnych przestępców.

PODMIOTY ODPOWIEDZIALNE ZA BEZPIECZEŃSTWO SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)

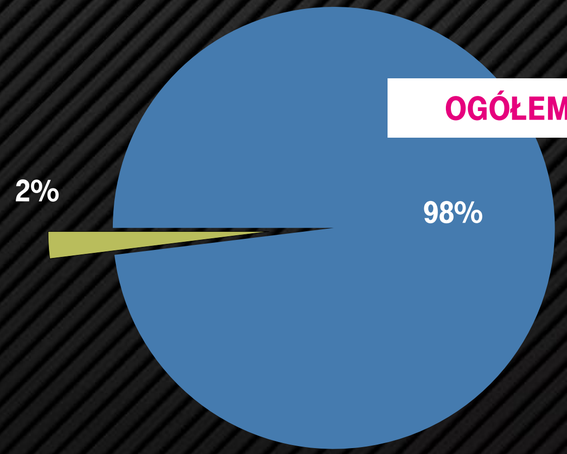
LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Dział IT	42%	74%
Dział administracji	17%	8%
Dział bezpieczeństwa IT/SOC	0%	4%
Nasz dział IT we współpracy z firmą zewnętrzną	2%	2%
Firm zewn./outsourcing	2%	0%
Inne	15%	2%
Nikt	23%	10%

Źródło: PMR, 2019 r.

Z reguły firmy zarządzają telefonami i zapewniają ich bezpieczeństwo we własnym zakresie, nie wykazując zainteresowania outsourcingiem. **Pokutuje myślenie, że nie jest to obszar specjalnie wrażliwy na incydenty. Wiele przedsiębiorstw nadal twierdzi, że przecież to tylko telefony, nie przyjmując jeszcze do wiadomości faktu, że dla coraz większej liczby pracowników smartfon jest pełnoprawnym narzędziem pracy.** Nie chodzi przy tym o usługi podstawowe, takie jak odbieranie połączeń i SMS-ów. Zdarza się nawet, że do tego celu pracownik firmy ma osobne urządzenie, natomiast smartfon pełni rolę przenośnego komputera. Mimo to telefon nie jest na ogół zabezpieczony w takim stopniu, jak firmowy desktop czy laptop. Co ciekawe, z wywiadów pogłębionych w dużych organizacjach wynika, że zdają sobie sprawę z powyższych zmian i trendów rynkowych. Przyznają, że wiedzą, jak wartościowym narzędziem w rękach potencjalnego przestępcy jest firmowa komórka. Tym bardziej dziwi więc takie podejście do zagadnienia bezpieczeństwa.

Jest także pozytywny aspekt, który należy tutaj podkreślić. Praktycznie wszyscy pracownicy średnich i dużych firm, którzy użytkują służbowy telefon komórkowy, wiedzą, komu powinni zgłosić przypadek cyberataku lub zgubienie/kradzież tego sprzętu. Brak takiej informacji deklaruje tylko 4% pracowników średnich przedsiębiorstw.

WIEDZA O OSOBIE ODPOWIEDZIALNEJ ZA PRZYJĘCIE ZGŁOSZENIA CYBERATAKU LUB FIZYCZNEGO ZGUBIENIA SŁUŻBOWEGO TELEFONU WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	96%	100%
Nie	4%	0%

Wyjaśnienie: pytanie zadano użytkownikom telefonów służbowych.
Źródło: PMR, 2019 r.

Na bezpieczeństwo telefonów należy patrzeć przez pryzmat świadomości użytkowników i sposobu korzystania z urządzeń. Kluczowe znaczenie ma np. obszar dostępu do firmowych danych z komórki. Zdaniem reprezentantów IT średnich i dużych organizacji pracownicy z poziomu służbowych smartfonów mają głównie możliwość korzystania z serwera firmowej poczty (69% badanych firm). W przypadku przedsiębiorstw zatrudniających co najmniej 250 pracowników, odsetek ten wynosi aż 77%. Pracownicy średnich firm częściej mają dostęp do książek adresowych i baz klientów niż osoby zatrudnione w dużych organizacjach. Ta druga grupa częściej z kolei może zajrzeć do kalendarzy innych pracowników. 9% specjalistów działu IT deklaruje, że pracownicy firmy nie mają dostępu do żadnych danych firmowych z poziomu telefonu komórkowego. W przypadku tych treści sprawa jest na tyle poważna, że ewentualny wyciek może mieć bardzo poważne konsekwencje dla przedsiębiorstwa. Jeśli np. dane dotyczyłyby klientów firmy, w praktyce oznaczałoby to naruszenie regulacji RODO. Ostatnie **przypadki kar nakładanych przez UODO – właśnie z tytułu wycieku danych i niewystarczających zabezpieczeń – to kwoty liczone już w milionach złotych**[1].

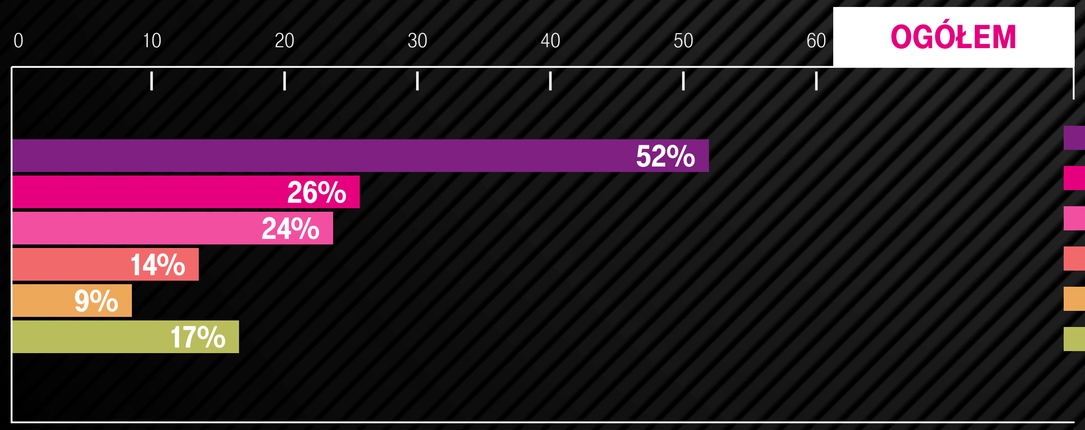
Deklaracje użytkowników telefonów różnią się od deklaracji kadry IT. W dużych firmach połowa osób zatrudnionych mówi o dostępie do książek adresowych pracowników (52% w porównaniu do 24% deklaracji działów IT). Interesujący jest także fakt, że zdaniem specjalistów z IT do danych finansowych ma dostęp 4% pracowników, natomiast użytkownicy służbowych telefonów komórkowych deklarują, że odsetek ten jest wyraźnie wyższy: w przypadku średnich firm wynosi 12%, natomiast dużych – 6%.

W naszej ocenie jest to raczej typowa sytuacja, że formalnie zakres ochrony czy dostęp do zasobów jest określany dość restrykcyjnie, natomiast rzeczywistość pokazuje mniej optymistyczny obraz. Znacznie więcej pracowników ma dostęp do różnego typu danych firmowych z poziomu telefonu niż się działom IT wydaje. Jest to o tyle niebezpieczne, że usypia czujność firmy i sztucznie zaniża poziom ekspozycji na ryzyko. Gdyby przedsiębiorstwa realnie oceniły skalę zjawiska, z pewnością zmieniłoby się ich podejście do inwestycji w profesjonalne zabezpieczenie firmowych telefonów i kompleksową politykę w tym zakresie.

[1] *https://uodo.gov.pl/pl/138/1189*

4.2. DOSTĘP PRACOWNIKÓW DO DANYCH I ZASOBÓW FIRMY

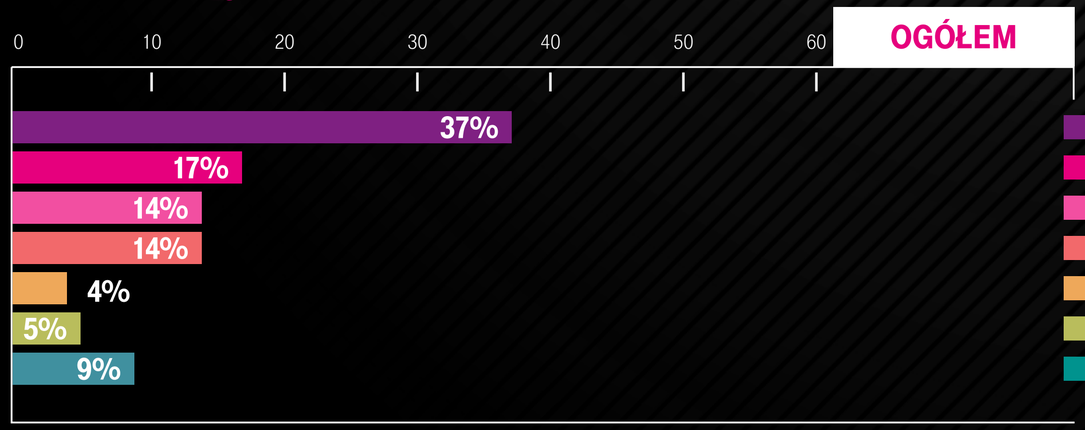
DOSTĘP DO DANYCH FIRMOWYCH Z POZIOMU SŁUŻBOWEGO TELEFONU KOMÓRKOWEGO
WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Książka adresowa pracowników	52%	52%
Bazy klientów	30%	22%
Kalendarze pracowników	12%	36%
Dokumenty (np. arkusze kalkulacyjne/oferty/wyceny/projekty techniczne, itp.)	12%	16%
Dane finansowe	12%	6%
Inne	14%	20%

Wyjaśnienie: wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

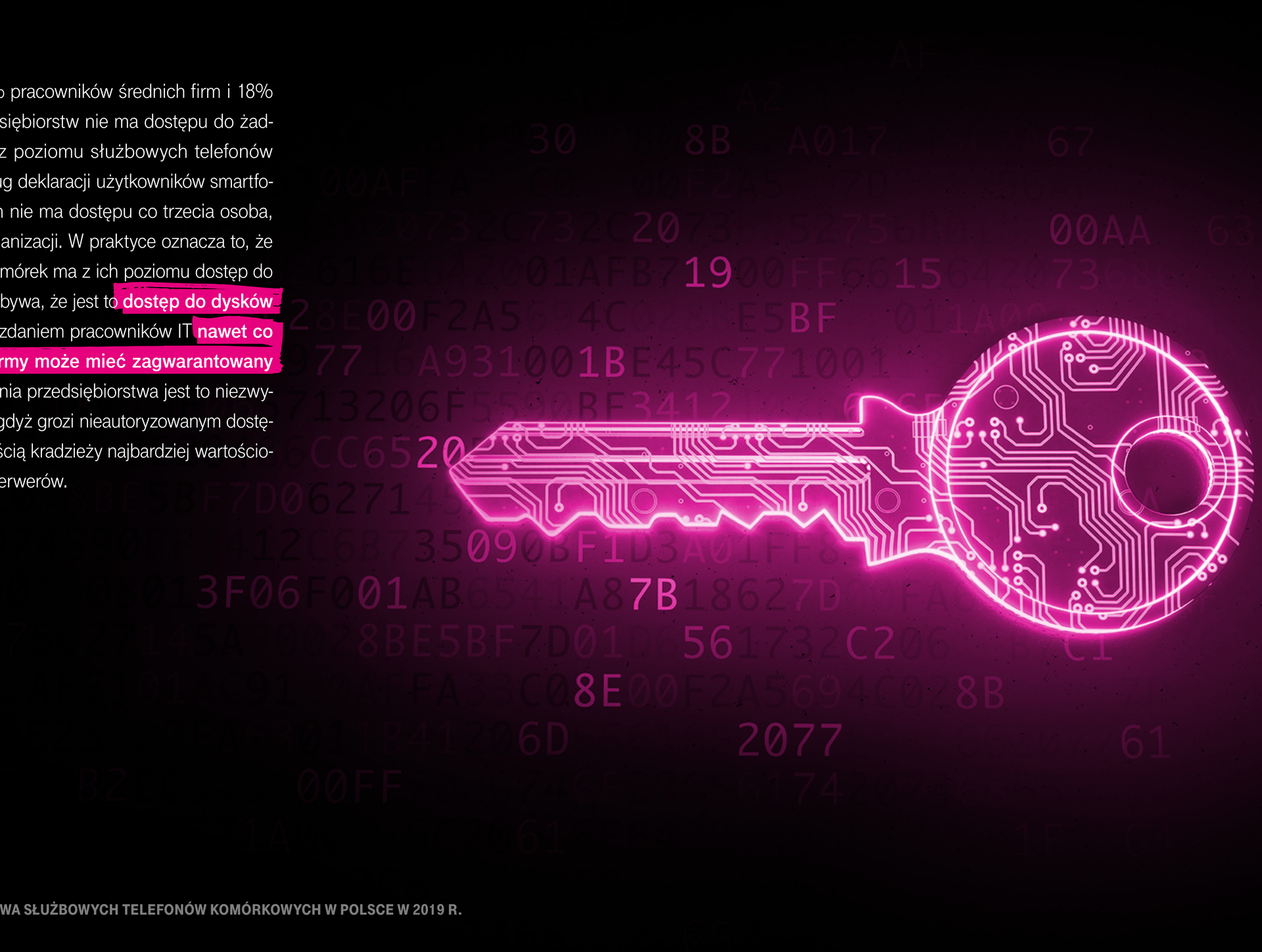
DOSTĘP PRACOWNIKÓW DO DANYCH FIRMOWYCH Z POZIOMU SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



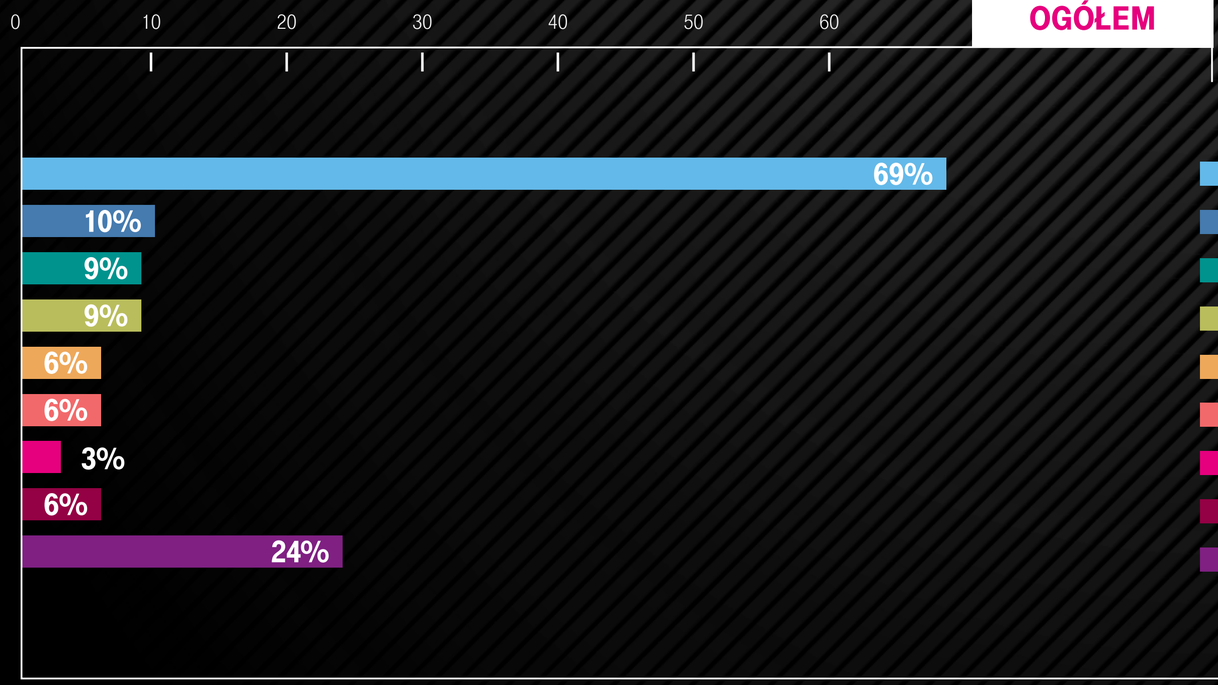
LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Książka adresowa pracowników	49%	24%
Kalendarze pracowników	9%	26%
Bazy klientów	19%	9%
Dokumenty (np. arkusze kalkulacyjne/oferty/wyceny/projekty techniczne itp.)	13%	15%
Dane finansowe	6%	2%
Inne	9%	2%
Pracownicy nie mają dostępu do żadnych danych	9%	9%

Wyjaśnienie: wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

Zdaniem kadry IT tylko 29% pracowników średnich firm i 18% pracowników dużych przedsiębiorstw nie ma dostępu do żadnych zasobów firmowych z poziomu służbowych telefonów komórkowych. Z kolei według deklaracji użytkowników smartfonów do zasobów firmowych nie ma dostępu co trzecia osoba, niezależnie od wielkości organizacji. W praktyce oznacza to, że większość użytkowników komórek ma z ich poziomu dostęp do firmowych zasobów. Często bywa, że jest to **dostęp do dysków sieciowych czy chmury** – zdaniem pracowników IT **nawet co szósty pracownik dużej firmy może mieć zagwarantowany taki wgląd.** Z punktu widzenia przedsiębiorstwa jest to niezwykle niebezpieczna sytuacja, gdyż grozi nieautoryzowanym dostępem, a tym samym możliwością kradzieży najbardziej wartościowych danych z firmowych serwerów.



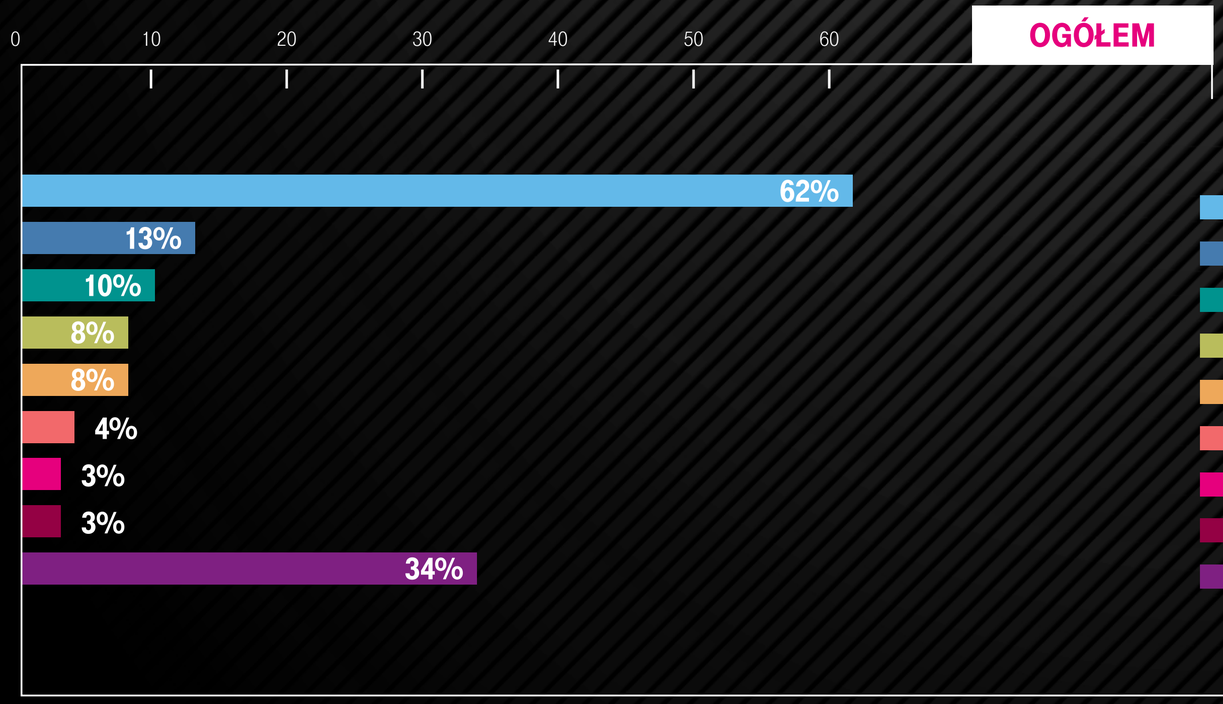
DOSTĘP PRACOWNIKÓW DO ZASOBÓW FIRMOWYCH Z POZIOMU SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Dostęp do serwera firmowej poczty elektronicznej	60%	77%
Dostęp do aplikacji firmowych, np. CRM, ERP, workflow	4%	16%
Dostęp do dysków sieciowych	4%	14%
Dostęp do rozwiązań chmurowych innych dostawców, np. dropbox	2%	16%
Dostęp do narzędzi zdalnej współpracy (komunikatory, sharepoint)	4%	7%
Intranet	2%	9%
Dostęp do firmowych kont bankowych	2%	5%
Inne	9%	2%
Pracownicy nie mają dostępu do żadnych zasobów	29%	18%

Wyjaśnienie: wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

DOSTĘP DO ZASOBÓW FIRMOWYCH Z POZIOMU SŁUŻBOWEGO TELEFONU KOMÓRKOWEGO
WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Dostęp do serwera firmowej poczty	63%	61%
Dostęp do aplikacji firmowych, np. CRM, ERP, workflow	13%	14%
Dostęp do narzędzi zdalnej współpracy (komunikatory, sharepoint)	8%	11%
Dostęp do dysków sieciowych	6%	9%
Dostęp do rozwiązań chmurowych innych dostawców, np. dropbox	8%	7%
Intranet	4%	5%
Dostęp do firmowych kont bankowych	4%	2%
Inne	2%	5%
Nie mam dostępu do żadnych zasobów firmowych	33%	34%

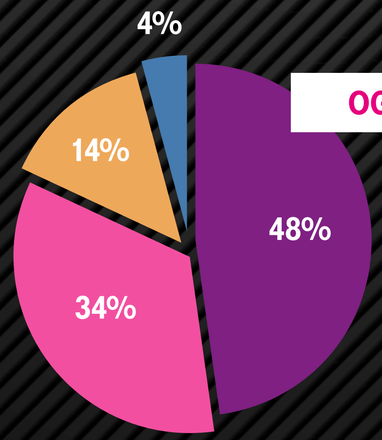
Wyjaśnienie: wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

4.3. UŻYTKOWANIE SŁUŻBOWYCH TELEFONÓW, W TYM DO CELÓW PRYWATNYCH, ORAZ POLITYKA BYOD

Niezwykle ciekawy jest temat hotspotów. 48% pracowników działu IT deklaruje, że pracownicy nie mogą łączyć się z otwartymi sieciami Wi-Fi, ale nie jest to technicznie blokowane. Wśród dużych firm odsetek ten jest nawet wyższy (57%). **Tylko 4% przedsiębiorstw blokuje połączenia z publicznymi sieciami Wi-Fi na służbowych telefonach pracowników**. Co trzecia firma natomiast wprost deklaruje, że pracownicy mogą łączyć się z otwartymi sieciami Wi-Fi za pomocą swojego urządzenia. Ponadto 14% organizacji nie ma w swojej polityce zapisu zakazującego łączenia się z otwartymi sieciami Wi-Fi z komórek.

Deklaracje użytkowników telefonów służbowych różnią się od deklaracji specjalistów IT. Szczególnie widać to w przypadku dużych firm. Jest to typowa sytuacja. Samo stwierdzenie, że nie powinno się czegoś robić, nie jest w stanie zniechęcić wszystkich użytkowników, tym bardziej, gdy jest to technicznie możliwe, a wiele przedsiębiorstw nie monitoruje tak naprawdę aktywności swoich pracowników na telefonach. W efekcie wysyłają im jasny sygnał, że w zasadzie „wszystko jest dozwolone", jeśli tylko pracownik da sobie z tym radę sam.

MOŻLIWOŚĆ ŁĄCZENIA SIĘ ZE SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH Z OTWARTYMI SIECIAMI WI-FI
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)

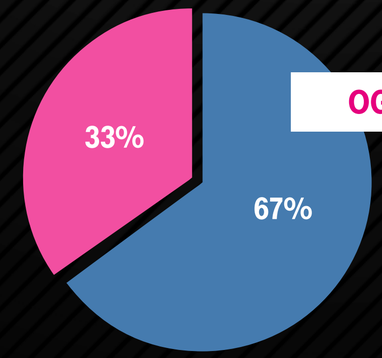


OGÓŁEM

LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Nie, ale nie jest to technicznie blokowane	40%	57%
Tak	40%	28%
Nie zostało to określone w polityce	16%	11%
Nie i jest to technicznie blokowane	4%	4%

Źródło: PMR, 2019 r.

MOŻLIWOŚĆ ŁĄCZENIA SIĘ ZE SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH Z OTWARTYMI SIECIAMI WI-FI
WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



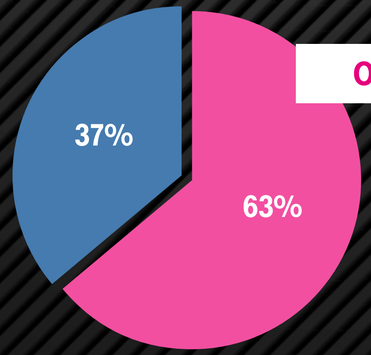
OGÓŁEM

LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	56%	78%
Nie	44%	22%

Źródło: PMR, 2019 r.

Ponad połowa pracowników dużych firm deklaruje, że może korzystać ze służbowej karty SIM na prywatnym telefonie. Co więcej, **dwie trzecie pracowników może korzystać z prywatnej karty SIM na służbowym** sprzęcie. Rodzi to szereg dodatkowych zagrożeń, choćby na styku prywatnych danych i aplikacji z danymi firmowymi w ramach tego samego urządzenia. Synchronizacja może oczywiście opierać się na loginach niepowiązanych z kartą SIM, jednak prywatna karta SIM powoduje, że pracownik traktuje telefon jak własne urządzenie. Ponadto sprawdzenie takiego smartfona przez pracodawcę jest dużo trudniejsze. Powstają kontrowersje w zakresie ewentualnego naruszenia prawa prywatności pracownika. Może on nie chcieć udostępniać danych zawartych w swoim telefonie pracodawcy, na przykład ze względu na tajemnicę osobistej korespondencji.

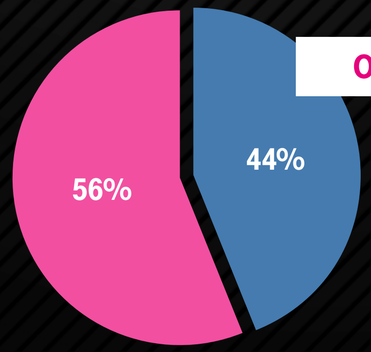
MOŻLIWOŚĆ KORZYSTANIA ZE SŁUŻBOWEJ KARTY SIM NA PRYWATNYM TELEFONIE WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDŹ	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	21%	53%
Nie	79%	48%

Źródło: PMR, 2019 r.

MOŻLIWOŚĆ KORZYSTANIA Z PRYWATNEJ KARTY SIM NA SŁUŻBOWYM TELEFONIE WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



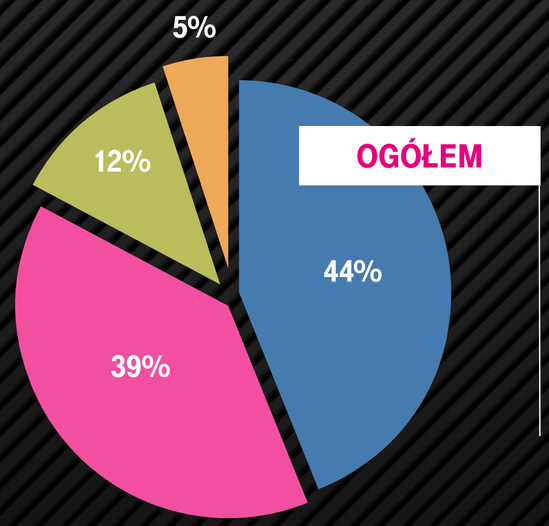
ODPOWIEDŹ	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	23%	64%
Nie	77%	36%

Źródło: PMR, 2019 r.

Jeszcze kilka lat temu popularność zdobywała kontorwersyjna pod względem bezpieczeństwa polityka BYOD. Badanie wykazało, że od stosowania tej polityki odstąpiło już 5% firm, a 12% (zarówno średnich, jak i dużych firm) kontynuuje te praktyki. Zaledwie 44% średnich i dużych przedsiębiorstw nie pozwala pracownikom na korzystanie z prywatnych telefonów komórkowych do celów służbowych. **Podobny odsetek (ok. 40%) nie ma zapisu na ten temat w obowiązującej polityce firmy.** Jest to kontrowersyjna kwestia, bo zarówno z punktu widzenia biznesowego, jak i samego bezpieczeństwa może się wiązać z dużym ryzykiem dla firmy. Do tego dochodzą jeszcze aspekty podatkowe, gdyż BYOD w miejscu pracy to użyczenie prywatnego sprzętu.

STOSOWANIE POLITYKI BYOD (BRING YOUR OWN DEVICE)

WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%), WRZESIEŃ 2019

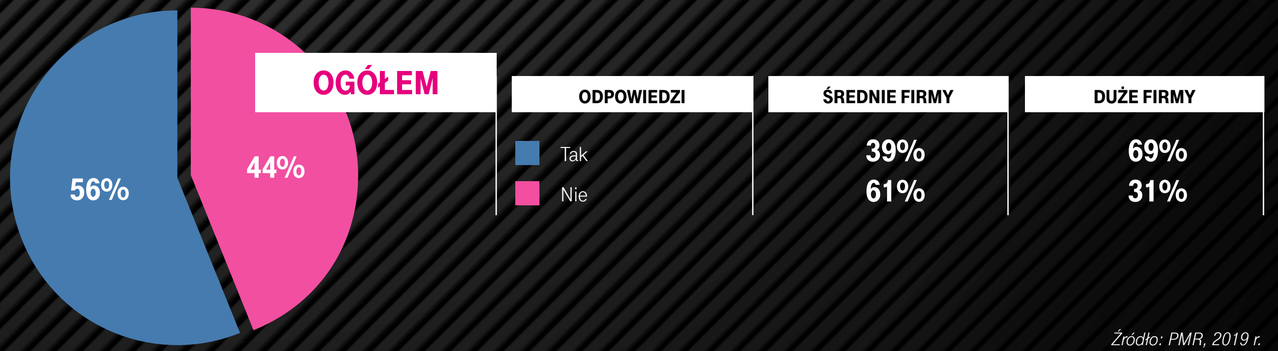


OGÓŁEM	LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
44%	Nigdy nie była i nie jest dozwolona w firmie	41%	48%
39%	Nie zostało to określone w polityce	41%	37%
12%	Była i dalej jest dozwolona w firmie	12%	11%
5%	Była, ale już nie jest dozwolona w firmie	6%	4%

Źródło: PMR, 2019 r.

To zaskakujące, że aż tyle polskich firm pozwala na służbowe kontakty ze sprzętu prywatnego albo co gorsza udaje, że problem ten nie istnieje. Z badań PMR zrealizowanych w ubiegłym roku w regionie środkowoeuropejskim w dużych przedsiębiorstwach (o przychodach powyżej 150 mln € w skali roku) wynika, że są one wielokrotnie bardziej czułe i restrykcyjne w tym zakresie. Z mechanizmów, które są w użyciu w przypadku wdrożenia BYOD przez duże firmy, wymieniane były głównie kilkustopniowe, adekwatne blokady urządzenia, w tym również osobne zabezpieczenia aplikacji firmowych, kontrola instalacji aplikacji, możliwość lokalizacji urządzenia i wdrożone kompleksowe systemy Mobile Device Management (MDM).

POSIADANIE PRZEZ FIRMY POLITYKI UŻYTKOWANIA SŁUŻBOWYCH TELEFONÓW DO CELÓW PRYWATNYCH
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	39%	69%
Nie	61%	31%

Źródło: PMR, 2019 r.

POSIADANIE PRZEZ FIRMY ZAPISU O ZAKAZIE UŻYWANIA SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH PRZEZ OSOBY TRZECIE W POLITYCE UŻYTKOWANIA SŁUŻBOWYCH TELEFONÓW DO CELÓW PRYWATNYCH
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)

ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	64%	58%
Nie	36%	42%

Źródło: PMR, 2019 r.

Aby skutecznie wdrożyć **politykę BYOD,** konieczne jest wypracowanie i ścisłe przestrzeganie praktyk związanych ze zgubieniem czy kradzieżą urządzenia. Nieodzowne jest między innymi zapewnienie separacji danych prywatnych od danych firmowych, z możliwością zdalnego usunięcia tych ostatnich. W rzeczywistości aż 44% polskich firm, w tym ponad **60% średnich przedsiębiorstw, w ogóle nie określiło polityki w zakresie użytkowania służbowych telefonów komórkowych**. Z punktu widzenia bezpieczeństwa i wspomnianej wyżej masowej skali wykorzystania firmowego telefonu jako drugiego komputera jest to bardzo ryzykowne podejście i znowu zupełnie niepotrzebne narażanie się na ewentualne ryzyko, które należy przecież minimalizować.

UŻYWANIE PRZEZ PRACOWNIKÓW SŁUŻBOWYCH TELEFONÓW DO CELÓW PRYWATNYCH WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)

Źródło: PMR, 2019 r.

KORZYSTANIE ZE SŁUŻBOWEGO TELEFONU KOMÓRKOWEGO W CELACH PRYWATNYCH WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)

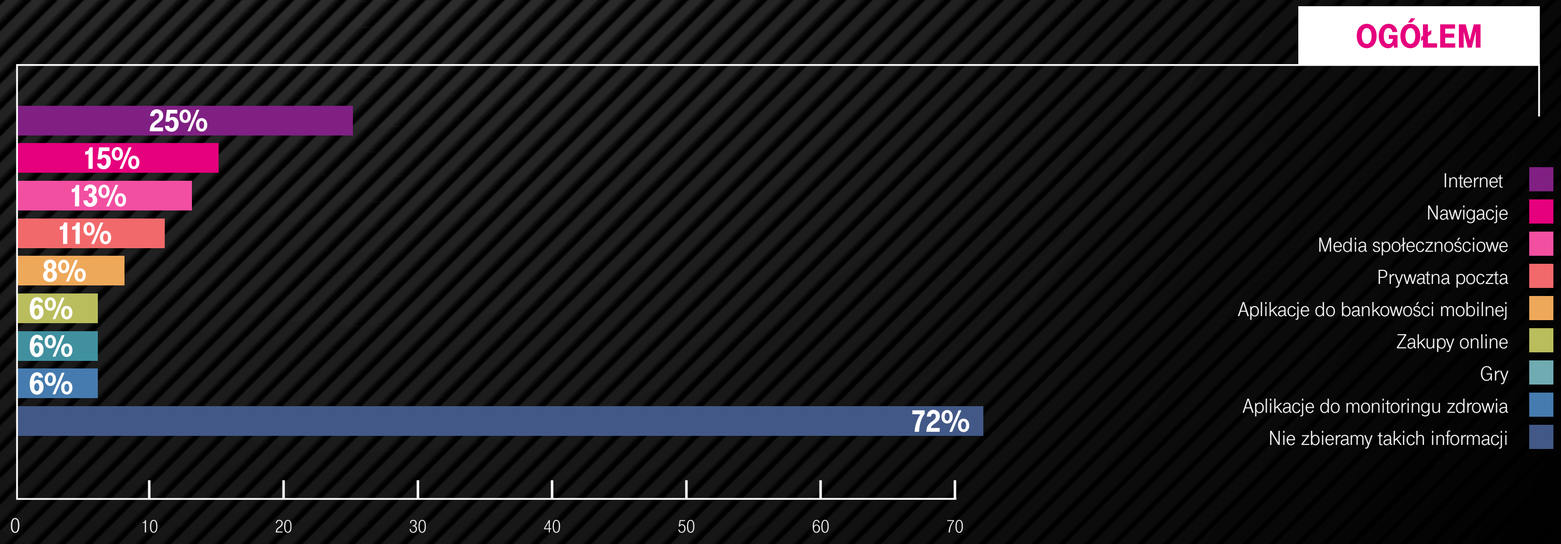
Źródło: PMR, 2019 r.

63% pracowników z działów IT deklaruje, że zatrudnieni w ich organizacjach używają służbowych telefonów komórkowych do celów prywatnych. Odsetek jest wyższy w przypadku dużych firm. Z kolei w przypadku deklaracji samych użytkowników firmowych smartfonów odsetek ten jest znacznie niższy i wynosi 40%. Różnica może wynikać z obawy przed przyznaniem się do korzystania ze służbowego sprzętu poza obowiązkami zawodowymi i ewentualnymi konsekwencjami, które się z tym wiążą.

Polskie firmy w zasadzie nie wiedzą, co ich pracownicy robią ze służbowym telefonem. **6 na 10 specjalistów z działów IT w średnich przedsiębiorstwach i 8 na 10 w dużych firmach otwarcie deklaruje, że nie zbiera informacji na temat wykorzystania służbowych telefonów do prywatnych celów.**

ZAKRES KORZYSTANIA PRZEZ PRACOWNIKÓW ZE SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH DO CELÓW PRYWATNYCH

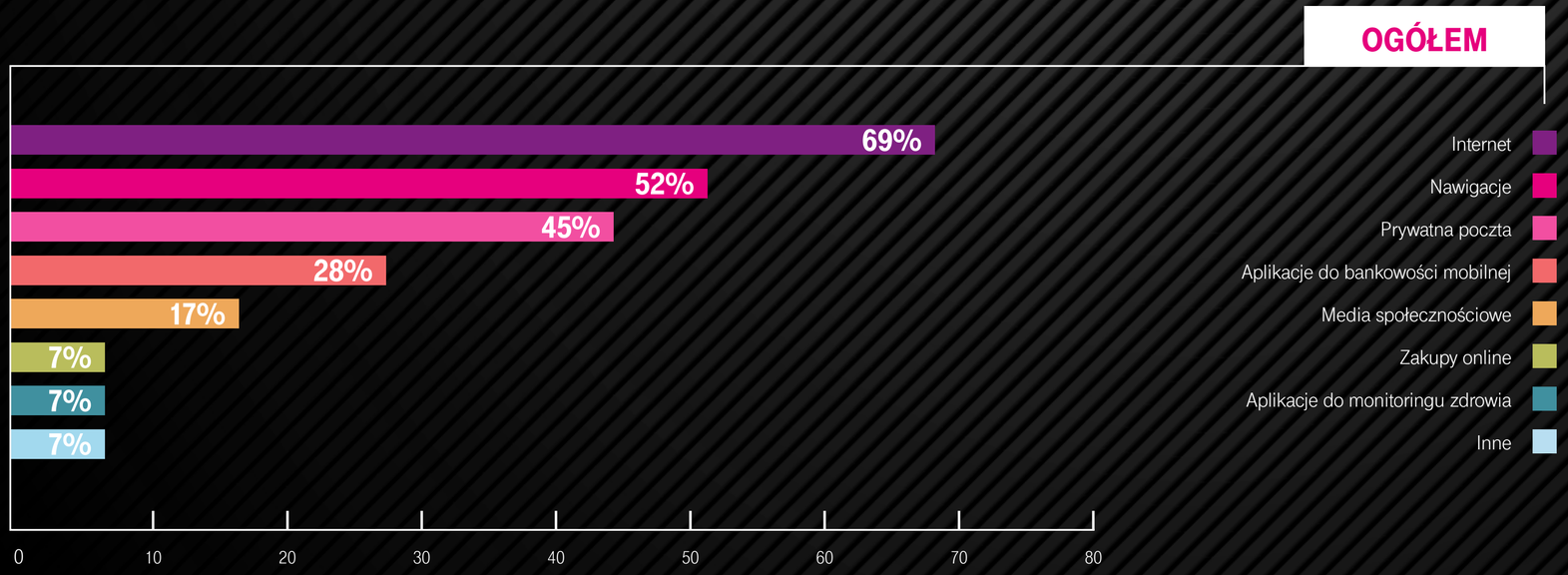
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Internet	35%	18%
Nawigacja	30%	6%
Media społecznościowe	5%	18%
Prywatna poczta	10%	12%
Aplikacje do bankowości mobilnej	10%	6%
Zakupy online	5%	6%
Gry	5%	6%
Aplikacje do monitoringu zdrowia	10%	3%
Nie zbieramy takich informacji	60%	79%

Wyjaśnienie: wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź.
Źródło: PMR, 2019 r.

ZAKRES KORZYSTANIA ZE SŁUŻBOWEGO TELEFONU KOMÓRKOWEGO W CELACH PRYWATNYCH WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%), WRZESIEŃ 2019 R.



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Internet	50%	82%
Nawigacja	42%	59%
Prywatna poczta	42%	47%
Aplikacje do bankowości mobilnej	25%	29%
Media społecznościowe	8%	24%
Zakupy online	0%	12%
Aplikacje do monitoringu zdrowia	8%	6%
Inne	17%	0%

Uwaga! Mała liczebność próby. Zalecana ostrożność przy interpretacji wyników i formułowaniu wniosków.
Pytanie zadano tylko tym respondentom, którzy wykorzystują służbowy telefon komórkowy do celów prywatnych.
Wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

Jak to wygląda w przypadku podmiotów, które zbierają takie informacje? Zdaniem osób z działów IT w średnich firmach pracownicy najczęściej wykorzystują służbowe telefony komórkowe do surfowania po Internecie i nawigacji. W dużych przedsiębiorstwach najczęściej w celach prywatnych pracownicy korzystają z nich do przeglądania Internetu, mediów społecznościowych i prywatnej poczty.

Połowa użytkowników telefonów służbowych w średnich firmach deklaruje, że za ich pomocą wykonuje działania w Internecie. 4 na 10 korzysta z nawigacji oraz sprawdza prywatną pocztę. Co czwarty pracownik na służbowym telefonie korzysta z bankowości mobilnej. Pracownicy dużych firm, podobnie jak średnich, wykorzystują telefony służbowe do surfowania po Internecie, nawigacji i prywatnej poczty, ale odsetek używających tych opcji jest znacznie wyższy – o 5% w przypadku korzystania z poczty i do 32% w przypadku korzystania z Internetu.

Inne sposoby wykorzystania telefonów służbowych do celów prywatnych to rozmowy telefoniczne i wysyłanie SMS-ów.

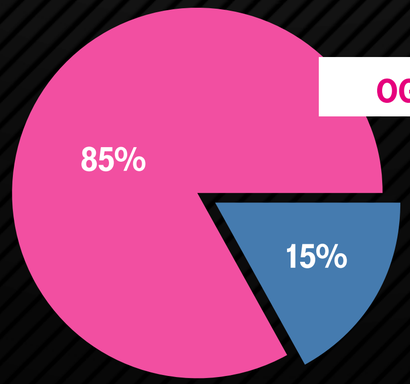
Użytkownicy służbowych telefonów deklarują, że na swoich urządzeniach mają zainstalowane komunikatory typu Messenger, WhatsApp i inne. Częściej zdarza się to wśród pracowników dużych firm, gdzie odsetek sięga 32%. Rzadziej aplikacje instalują pracownicy średnich przedsiębiorstw.

Niezależnie od powyższych rozbieżności i sposobu wykorzystania firmowego sprzętu, podstawowy wniosek jest taki, że **znaczący odsetek pracowników polskich przedsiębiorstw korzysta ze służbowego telefonu do celów prywatnych.** Problem w tym, że za świadomością i przyzwoleniem na to nie idą żadne konkretne działania, mające na celu zabezpieczenie firmowego sprzętu, a tym samym danych, do których mają dostęp. Praktyka pokazuje, że służbowe telefony nie są wystarczająco zabezpieczane. Ponadto firmy otwarcie przyznają, że w ogóle nie monitorują tego, co pracownicy robią na swoich urządzeniach. Swój brak działań w tym zakresie uzasadniają przepisami RODO i ochroną prywatności. Jest to podejście asekuracyjne. Należałoby połączyć ochronę prywatności z ochroną zasobów firmowych, wykorzystując odpowiednie zabezpieczenia telefonu i uświadamiając użytkowników w tym zakresie, m.in. przez właściwe procedury i szkolenia.

4.4. OGRANICZENIA W ZAKRESIE UŻYWANIA SŁUŻBOWYCH TELEFONÓW DO CELÓW PRYWATNYCH I POLITYKA RODO

Nie dziwi więc informacja, że **tylko 15% średnich i dużych firm korzysta z narzędzi (typu aplikacje blokujące dostęp do określonych stron) ograniczających używanie służbowych telefonów komórkowych do celów prywatnych.** Nie są to zatem popularne rozwiązania zwiększające cyberbezpieczeństwo służbowych telefonów komórkowych w Polsce. Niepokój budzi nie tylko obserwacja, zgodnie z którą firmy nie chronią telefonów przed incydentami w zakresie bezpieczeństwa. Jak potwierdzają wyniki, przedsiębiorstwa nie są także przygotowane na wypadek wystąpienia takiej sytuacji. Aż co druga firma w Polsce nie posiada żadnych procedur określających postępowanie w takim przypadku. Analizując duże przedsiębiorstwa, procedury bezpieczeństwa najczęściej zaimplementowane są w organizacjach zatrudniających od 300 do 499 pracowników, ale nawet w tej grupie odsetek jest tylko nieznacznie powyżej średniej.

KORZYSTANIE Z NARZĘDZI TECHNOLOGICZNYCH OGRANICZAJĄCYCH UŻYWANIE SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH DO CELÓW PRYWATNYCH
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)

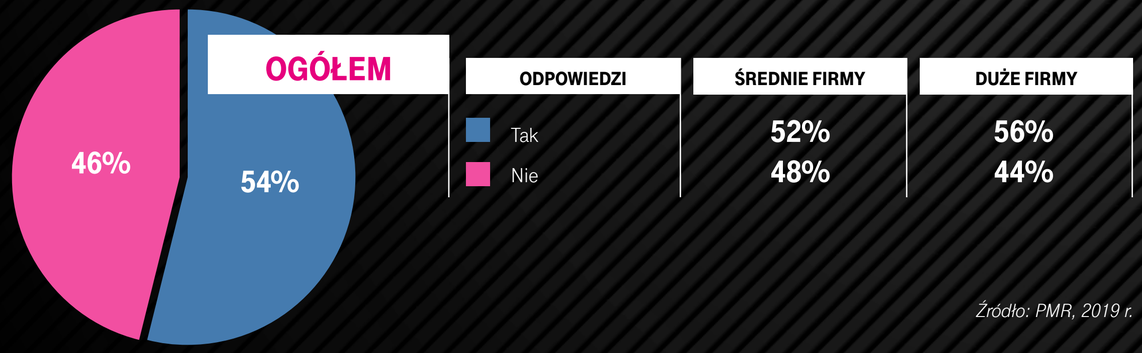


OGÓŁEM

ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	13%	17%
Nie	88%	83%

Źródło: PMR, 2019 r.

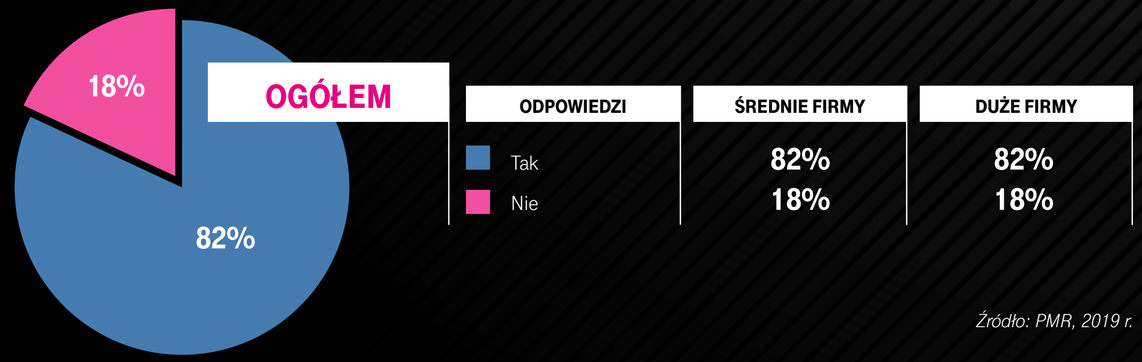
POSIADANIE PRZEZ FIRMĘ SZCZEGÓŁOWYCH PROCEDUR POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA INCYDENTÓW BEZPIECZEŃSTWA NA SŁUŻBOWYCH TELEFONACH KOMÓRKOWYCH WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	52%	56%
Nie	48%	44%

Źródło: PMR, 2019 r.

OBJĘCIE PROCEDURĄ RODO SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	82%	82%
Nie	18%	18%

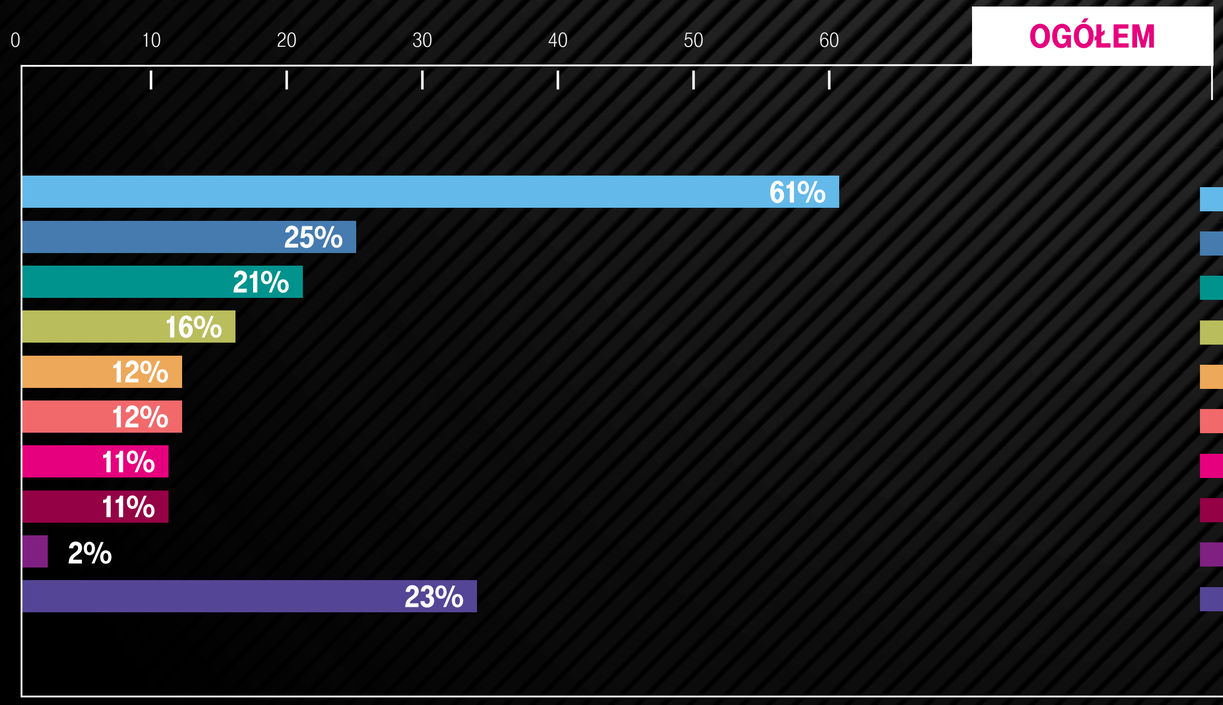
Źródło: PMR, 2019 r.

Trochę lepiej wygląda sytuacja, jeśli chodzi o wdrożenie przepisów RODO. Procedurą RODO w firmach objętych jest 82% komórek, co oznacza, że aż **18% telefonów służbowych w Polsce się RODO wymyka.** Daje to do myślenia, biorąc pod uwagę kary i inne konsekwencje dla przedsiębiorców. Najbardziej na wyobraźnię firm mogą zadziałać kolejne kary UODO, których wprowadzenie jest tylko kwestią czasu, jeśli w niemal co piątej średniej i dużej firmie w kraju ochrona danych osobowych nie dotyczy kanału „mobile". Najpopularniejszym sposobem na implementację przepisów RODO jest zainstalowanie oprogramowania antywirusowego praktykowane przez 66% podmiotów średnich i 57% dużych. 1 na 5 średnich i dużych firm instaluje ponadto na służbowych telefonach pracowników narzędzia do autoryzacji.

Pozostałe sposoby na uwzględnienie RODO na telefonach komórkowych stosowane są głównie przez organizacje zatrudniające co najmniej 250 pracowników. 36% dużych firm wprowadziło szyfrowaną komunikację (np. przez połączenie VPN), a 29% wdraża kompleksowe rozwiązania typu MDM/EMM w zakresie zarządzania urządzeniami mobilnymi. Najczęciej używane narzędzia do egzekwowania RODO w firmach to oprogramowanie antywirusowe wraz z narzędziami autoryzacji i szyfrowanym połączniem VPN.

28% średnich firm oraz 18% dużych oświadcza, że wdrożyło RODO za pomocą innych, niewymienionych w ankiecie sposobów. Wśród odrębnych procedur zaimplementowania RODO wskazywano głównie: regulaminy, procedury bezpieczeństwa oraz pisemne oświadczenia pracowników o braku danych poufnych/wrażliwych na służbowych telefonach komórkowych. Takie podejście oznacza de facto brak kontroli. Użytkownicy sprzętu mogą nawet nie zdawać sobie sprawy, że mają dostęp do danych wrażliwych, np. w firmowych mailach. Podpisanie oświadczenia nic w tym przypadku nie zmieni.

SPOSÓB UWZGLĘDNIENIA RODO NA SŁUŻBOWYCH TELEFONACH KOMÓRKOWYCH WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Zainstalowano oprogramowanie antywirusowe	66%	57%
Zainstalowano narzędzia do autoryzacji	24%	25%
Rozpoczęto szyfrowanie komunikacji, np. VPN	7%	36%
Wdrożono kompleksowe rozwiązania typu MDM/EMM	3%	29%
Zainstalowano narzędzia do autentykacji	7%	18%
Zainstalowano narzędzia do szyfrowania danych	3%	21%
Zamówiono ochronę ruchu internetowego w sieci mobilnej	7%	14%
Wdrożono narzędzia do zdalnego czyszczenia urządzeń mobilnych	7%	14%
Przekierowywano ruch firmowy na prywatny APN	0%	4%
Inne	28%	18%

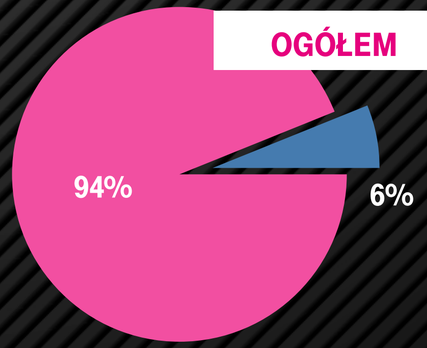
Wyjaśnienie: pytanie zadano tylko tym respondentom, których pracodawcy objęli RODO służbowe telefony komórkowe.
Wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

4.5. CYBERATAKI NA FIRMOWE TELEFONY KOMÓRKOWE

6% pracowników działu IT w średnich i dużych przedsiębiorstwach podejrzewa, że w ich organizacji w ciągu ostatniego roku co najmniej jeden pracownik padł ofiarą cyberataku na służbowy telefon komórkowy. Podejrzenia te są większe w przypadku średnich firm, gdzie do takiego ataku mogło dojść na co dziesiątej komórce. Warto podkreślić, że dane te są spójne ze statystykami T-Mobile Polska w ramach monitoringu potencjalnych zagrożeń firmowych telefonów (więcej informacji na ten temat w dalszej części raportu). Jeśli chodzi o deklaracje użytkowników, zdecydowana większość z nich nie przypomina sobie wystąpienia sytuacji związanej z naruszeniem cyberbezpieczeństwa służbowego telefonu. Oczywiście do tej oceny należy podchodzić z dużym dystansem.

Ogólnie rzecz biorąc, wyraźnie większy odsetek pracowników działów IT podejrzewa wystąpienie cyberataku na firmowe telefony niż wynikałoby to z deklaracji ich użytkowników. Różnica ta może może być spowodowana obawą pracowników przed przyznaniem się do naruszenia cyberbezpieczeństwa na ich służbowych telefonach. Niepokój ten prawdopodobnie wynika z podejrzeń ze strony osób zarządzających bezpieczeństwem służbowych telefonów o niewłaściwe użytkowanie lub ryzykowne aktywności w Internecie (np. odwiedzanie potencjalnie niebezpiecznych stron) na służbowych telefonach komórkowych. Dane z systemu Cyber Guard T-Mobile Polska pokazują jednak, że takie incydenty mają faktycznie miejsce. **Co 14. telefon służbowy użytkowany w średnich i dużych firmach w Polsce komunikuje się ze złośliwymi adresami IP, narażając tym samym firmę na ryzyko.**

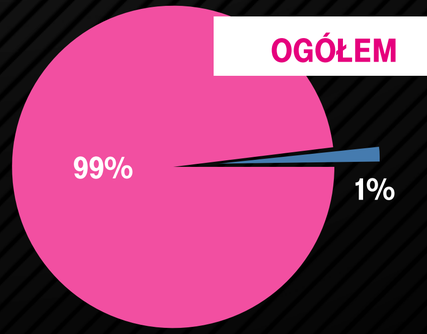
PODEJRZENIA PRACOWNIKÓW Z DZIAŁU IT ODNOŚNIE CYBERATAKÓW NA SŁUŻBOWE TELEFONY PRACOWNIKÓW W CIĄGU OSTATNIEGO ROKU (%)



OGÓŁEM	ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
	Tak	10%	2%
	Nie	90%	98%

Źródło: PMR, 2019 r.

ATAK LUB NARUSZENIE CYBERBEZPIECZEŃSTWA W SŁUŻBOWYM TELEFONIE KOMÓRKOWYM W CIĄGU OSTATNIEGO ROKU WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



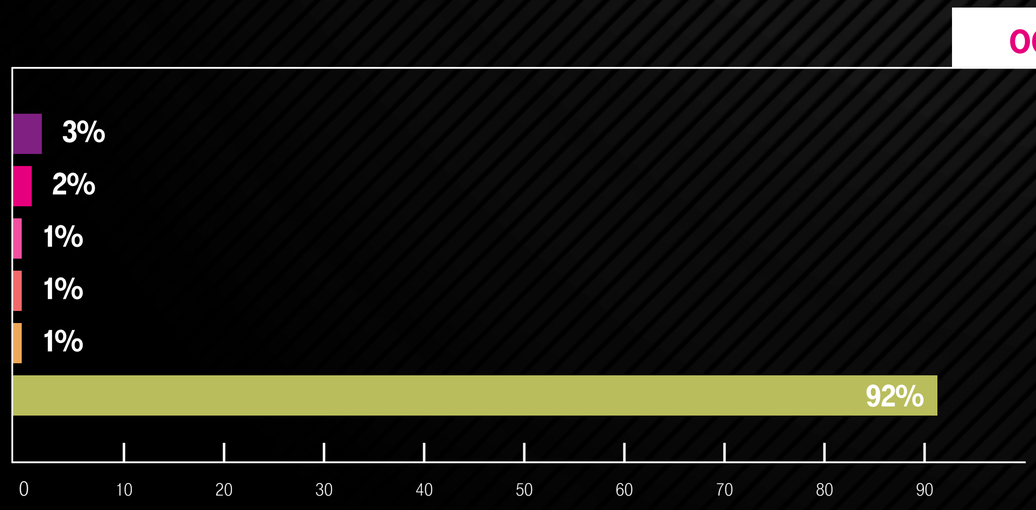
OGÓŁEM	ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
	Tak	2%	0%
	Nie	98%	100%

Źródło: PMR, 2019 r.

Wśród incydentów w zakresie bezpieczeństwa, mających miejsce na służbowych telefonach komórkowych, specjaliści z działu IT wymieniają phishing, czyli przekierowywanie na fałszywą stronę, oraz smishing, czyli otrzymywanie SMS-ów premium. Użytkownicy służbowych telefonów najczęściej nie są w stanie jednoznacznie ocenić, czy miał miejsce cyberatak na smartfonie, dlatego zapytaliśmy ich o najpopularniejsze symptomy ataku, które mogli zaobserwować. Okazuje się, że grupa ta rzadko deklaruje ich występowanie. **9 na 10 badanych pracowników nie zauważa żadnych oznak sugerujących atak na służbowy telefon.** Respondenci, którzy zauważyli na swoich urządzeniach oznaki naruszenia cyberbezpieczeństwa, najczęściej wymieniają spowolnienie pracy telefonu (3%).

Pracownicy w firmach zatrudniających od 50 do 250 osób częściej doświadczają spowolnienia funkcjonowania służbowych telefonów komórkowych lub samoczynnego otwierania się „dziwnych", podejrzanych stron lub aplikacji. Z kolei zatrudnieni w dużych przedsiębiorstwach częściej zgłaszają podejrzane zachowanie niektórych aplikacji i samoczynne wybieranie numerów (znaków na klawiaturze). Dane z systemu Cyber Guard T-Mobile Polska, które prezentujemy w dalszej części raportu, potwierdzają powyższe wskazania – aż 95% incydentów związane jest z zagrożeniami typu malware/trojan, których symptomy są m.in. właśnie takie, o jakich mówią użytkownicy służbowych telefonów.

OZNAKI NARUSZENIA CYBERBEZPIECZEŃSTWA NA SŁUŻBOWYM TELEFONIE KOMÓRKOWYM WG UŻYTKOWNIKÓW W W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Spowolnienie pracy telefonu	4%	2%
Przegrzewanie się telefonu	2%	2%
Samoczynne otwieranie się dziwnych stron	2%	0%
Dziwne/podejrzane zachowanie niektórych aplikacji	0%	2%
Samoczynne wybieranie numerów/znaków na klawiaturze	0%	2%
Nie zauważyłem nic takiego	92%	92%

Wyjaśnienie: wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

Podsumowując, najczęstsza droga cyberataku w firmach średniej i dużej wielkości to sieć firmowa (19%) oraz zabiegi socjotechniczne typu phishing (16%). 47% badanych specjalistów IT deklaruje, że w ciągu ostatnich 12 miesięcy incydenty cyberbezpieczeństwa nie pojawiły się w żadnym kanale.

Teoretycznie telefony nie są w czołówce, jeśli chodzi o cel cyberprzestępców. **W praktyce 43% polskich firm nie monitoruje nawet liczby incydentów w zakresie bezpieczeństwa telefonów komórkowych**, więc trudno poprawnie zweryfikować tę tezę. Przedsiębiorstwa, które prowadzą takie statystyki, w ciągu ostatniego miesiąca odnotowały poniżej dziesięciu tego typu incydentów. Faktem jest, że liczba zagrożeń w kanale mobile stale rośnie. Izraelska spółka Check Point Software poinformowała w tym roku[1] o nowym rodzaju ataków na smartfony.

Polega on na wysyłaniu niestandardowych wiadomości SMS w celu modyfikacji ustawień sieciowych i internetowych w urządzeniu. Wykorzystywana w tym przypadku sprytna technika inżynierii społecznej jest przypomnieniem, że ataki phishingowe to poważne zagrożenie dla firmowych telefonów.

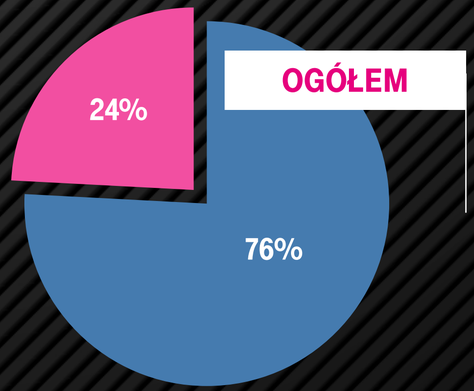
1 https://research.checkpoint.com/advanced-sms-phishing-attacks-against-modern-android-based-smartphones/.

4.6. SZKOLENIA W OBSZARZE „MOBILE SECURITY”

6 na 10 firm przeprowadza dla pracowników szkolenia tak, aby mieli świadomość cyberataków na telefony komórkowe. Potwierdzają to również sami pracownicy. Bardziej popularne są one jednak w dużych organizacjach, gdzie odsetek ten wynosi 66% (w porównaniu z 54% w średnich firmach). Firmy, które przeprowadzają takie szkolenia, częściej kierują na nie wybranych pracowników (55%), zwykle kadrę menadżerską, która i tak jest bardziej świadoma zagrożeń.

W praktyce **szkolenia**, na temat procedur korzystania z firmowego telefonu, a szczególnie możliwych zagrożeń, **zarezerwowane są dla wybranych grup pracowników** – zwykle menedżerów i kadry kierowniczej. Reszta zatrudnionych (blisko 40%) jest pomijana, więc na ogół nie jest świadoma potencjalnego narażenia przedsiębiorstwa na straty w przypadku niepoprawnego zabezpieczenia urządzeń firmowych. W rzeczywistości to właśnie szeregowi pracownicy powinni być lepiej uświadomieni w kwestii użytkowania firmowego telefonu i ewentualnych zagrożeń, ponieważ są najsłabszym ogniwem, a ich poziom wiedzy jest zwykle relatywnie najniższy.

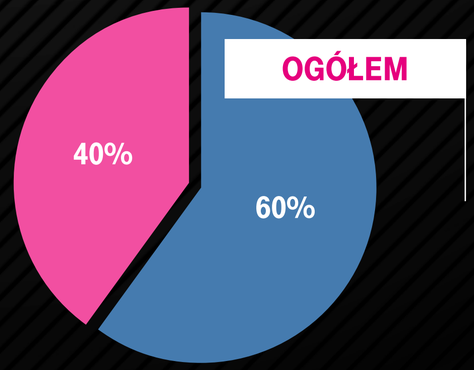
ODBYCIE SZKOLENIA W ZAKRESIE PROCEDUR KORZYSTANIA ZE SŁUŻBOWEGO TELEFONU KOMÓRKOWEGO WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	78%	73%
Nie	22%	27%

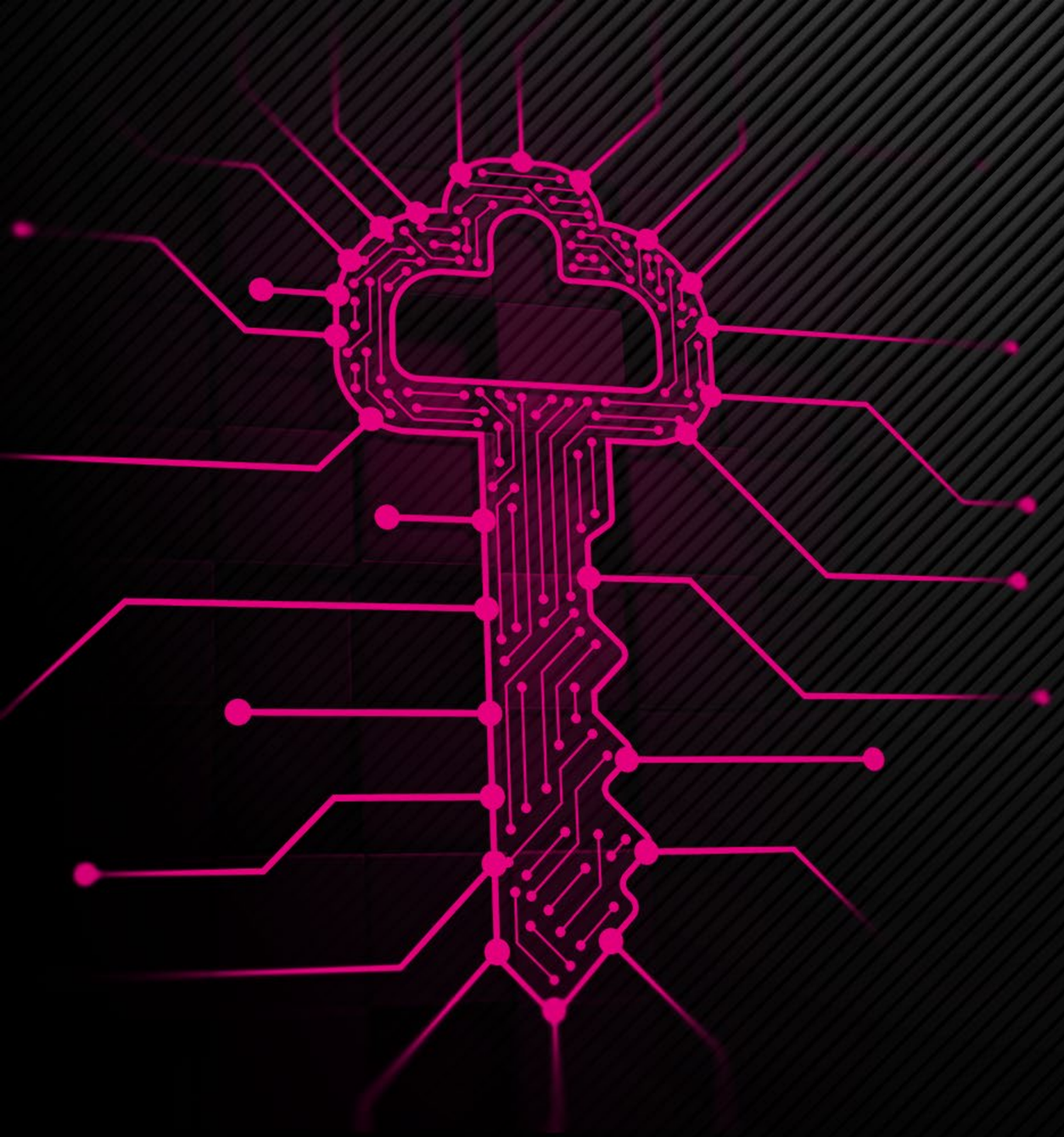
Źródło: PMR, 2019 r.

PRZEPROWADZANIE SZKOLEŃ DLA PRACOWNIKÓW Z ZAKRESU ŚWIADOMOŚCI O CYBERATAKACH NA TELEFONY KOMÓRKOWE WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)

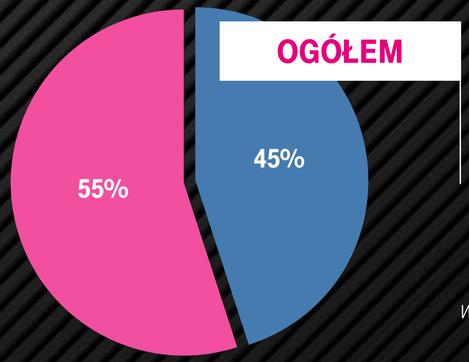


ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	54%	66%
Nie	46%	34%

Źródło: PMR, 2019 r.



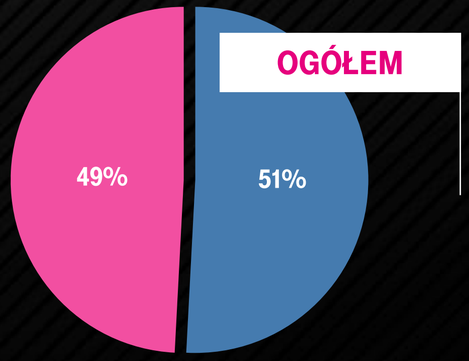
BENEFICJENCI SZKOLEŃ Z ZAKRESU ŚWIADOMOŚCI O CYBERATAKACH NA TELEFONY KOMÓRKOWE (%) WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE.



MOŻLIWOŚĆ	ŚREDNIE FIRMY	DUŻE FIRMY
Wszyscy pracownicy	59%	32%
Wybrane grupy pracowników	41%	68%

Wyjaśnienie: pytanie zadano tylko tym respondentom, których pracodawcy przeprowadzają szkolenia z zakresu świadomości o cyberatakach. Źródło: PMR, 2019 r.

PRZEPROWADZANIE PRZEZ FIRMY SZKOLEŃ DLA PRACOWNIKÓW, MAJĄCYCH NA CELU ZWIĘKSZENIE ŚWIADOMOŚCI CYBERATAKÓW NA SŁUŻBOWE TELEFONY KOMÓRKOWE WG UŻYTKOWNIKÓW W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



MOŻLIWOŚĆ	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	46%	55%
Nie	54%	45%

Źródło: PMR, 2019 r.

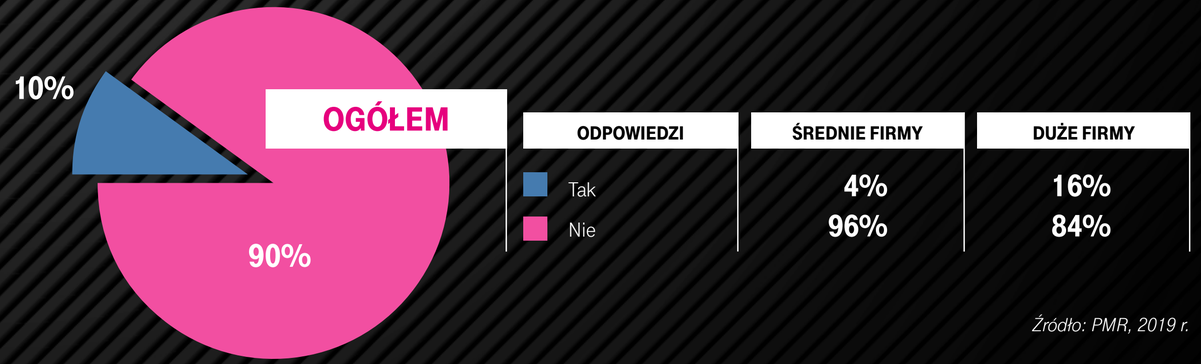
4.7. BUDŻETY NA „MOBILE SECURITY” I UBEZPIECZENIA FIRMOWYCH TELEFONÓW

Brak odpowiednich działań w zakresie zabezpieczenia telefonów komórkowych ma odzwierciedlenie w budżetach. **Aż 8 na 10 dużych firm nie ma oddzielnego budżetu na cyberochronę służbowych telefonów komórkowych. Wśród średnich przedsiębiorstw odsetek ten sięga 96%.** Wśród dużych podmiotów środki przeznaczone na cyberochronę smartfonów oraz plany ich zgromadzenia mają najczęściej firmy zatrudniające powyżej 1000 pracowników oraz te liczące od 300 do 499 osób.

W przypadku cyberataków na służbowe telefony, częściej ich ofiarami padały firmy średniej wielkości niż duże. 4% przedsiębiorstw zatrudniających od 50 do 250 pracowników otwarcie przyznaje, że poniosło straty lub nałożono na nie kary finansowe, a 2% doświadczyło tzw. czarnego PR-u ze strony konkurencji. Z kolei w przypadku 2% dużych firm cyberatak na służbowe telefony doprowadził do wycieku danych klientów, danych finansowych itp. W praktyce liczby te mogą być nawet wyższe. Trzeba zwrócić uwagę na fakt, że ponad połowa podmiotów w ogóle nie monitoruje telefonów. Dodatkowo część z nich odmawia odpowiedzi na pytania o konsekwencje cyberataków, zasłaniając się swoją polityką bezpieczeństwa.

Ubezpieczenie służbowych telefonów komórkowych posiada 4 na 10 przedsiębiorstw. Najczęściej jest to ubezpieczenie od zniszczenia (83%) i kradzieży (72%). **Ubezpieczenie firmowych telefonów komórkowych od cyberataku deklaruje 17% firm w naszym kraju. Z badań PMR wynika, że jest to odsetek ponad dwukrotnie mniejszy niż ubezpieczenia od cyberataków w ogóle.** To kolejny dowód, że firmy spychają „mobile security” na margines, co może okazać się bardzo kosztowne, bo w przypadku ewentualnych strat przedsiębiorstwo zmuszone będzie w całości pokryć koszty z własnych środków.

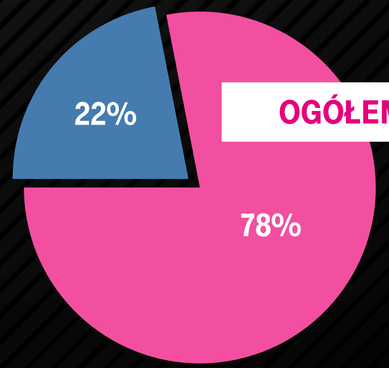
POSIADANIE ODDZIELNEGO BUDŻETU NA CYBEROCHRONĘ SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	4%	16%
Nie	96%	84%

Źródło: PMR, 2019 r.

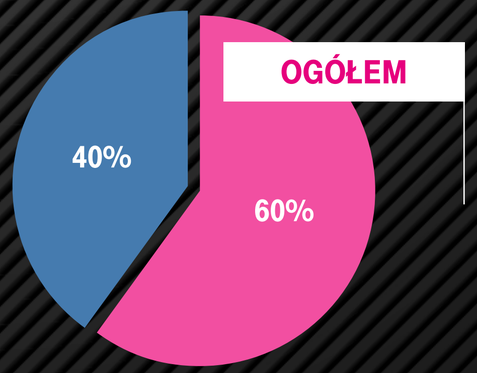
PLANY PRZEZNACZENIA DEDYKOWANEGO BUDŻETU NA CYBEROCHRONĘ SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	13%	33%
Nie	87%	67%

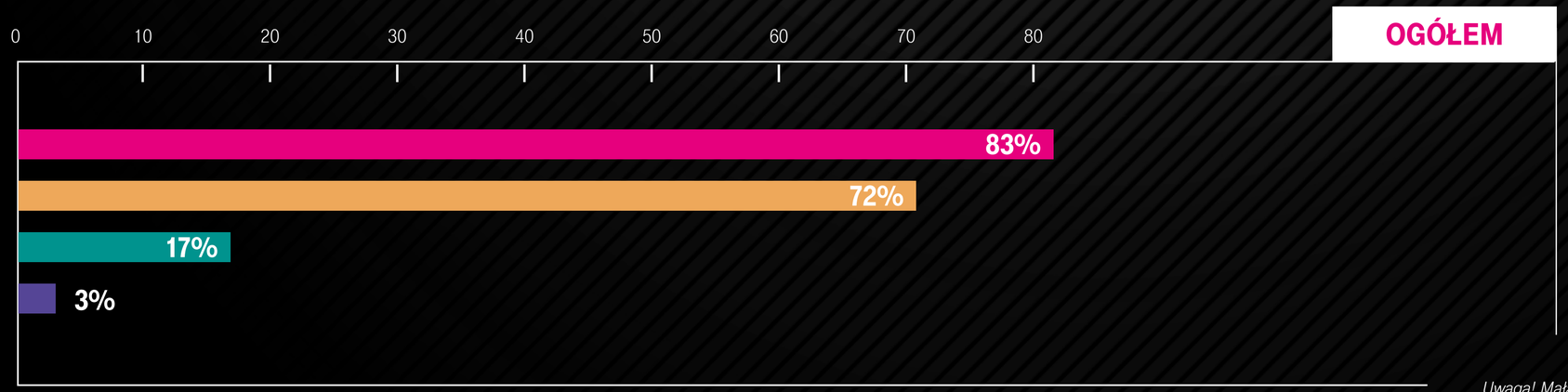
Źródło: PMR, 2019 r.

UBEZPIECZENIE SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



ODPOWIEDZI	ŚREDNIE FIRMY	DUŻE FIRMY
Tak	37%	43%
Nie	63%	57%

ZAKRES UBEZPIECZENIA SŁUŻBOWYCH TELEFONÓW KOMÓRKOWYCH
WG DZIAŁÓW IT W ŚREDNICH I DUŻYCH FIRMACH W POLSCE (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Od zniszczenia	80%	86%
Od kradzieży	73%	71%
Od cyberataków	13%	21%
Inne	7%	0%

Uwaga! Mała liczebność próby. Zalecana ostrożność przy interpretacji wyników i formułowaniu wniosków.
Pytanie zadano tylko tym respondentom, którzy posiadają ubezpieczenie telefonów komórkowych.
Wartości nie sumują się do 100%, ponieważ respondenci mogli wskazać więcej niż jedną odpowiedź. Źródło: PMR, 2019 r.

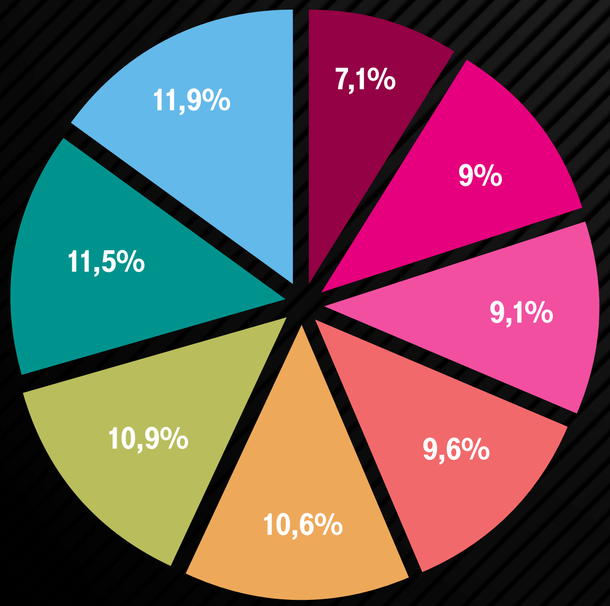
5. ZAGROŻENIA I ATAKI NA TELEFONY KOMÓRKOWE – CO WIDAĆ W SIECI OPERATORSKIEJ?

Atrakcyjność przestępczości internetowej sukcesywnie rośnie. Tak samo jest w przypadku zagrożenia atakami na urządzenia mobilne. Według różnych szacunków liczba ataków na smartfony podwaja się z roku na rok. Nic nie wskazuje na to, że ta tendencja się zmieni. W przypadku przedsiębiorstw poziom ochrony i inwestycji w bardziej zaawansowane rozwiązania zabezpieczające również rośnie. Dotyczy to jednak przede wszystkim serwerów i komputerów. Nie jest w tej sytuacji zaskoczeniem, że przestępcy szukają najsłabszych elementów firmowego systemu. Za takie uznaje się obecnie telefony, które są na szczycie listy najgorzej zabezpieczonych składowych firmowej infrastruktury. **Zainteresowanie tematem hackowania smartfonów potwierdzają choćby pierwsze doniesienia o szukaniu podatności bezpośrednio na kartach SIM, aby w ten sposób przejąć kontrolę nad urządzeniem użytkownika. Dodatkowym atutem komórek jest fakt, że w odróżnieniu od komputerów, często są aktywne praktycznie przez całą dobę. Do tego dochodzi efekt skali – telefonów jest obecnie wielokrotnie więcej niż wszystkich komputerów w firmach.** Dlatego nie dziwi fakt, że większość zagrożeń w zakresie bezpieczeństwa IT dotyczy urządzeń mobilnych. To tylko kilka powodów, dlaczego coraz częściej zachodzi konieczność uwzględnienia w firmowych politykach bezpieczeństwa IT zarządzania flotą urządzeń mobilnych. W tej części raportu zaprezentujemy najważniejsze dane liczbowe z systemu Cyber Guard T-Mobile Polska, który monitoruje transmisję danych w sieci operatora pod kątem występowania zagrożeń. Jest to rozwiązanie obserwujące nie tylko ruch przeglądarkowy, ale całość ruchu internetowego na wszystkich 65 tys. portów. Cyber Guard korzysta z wielu aktualizowanych codziennie źródeł feedów dotyczących złośliwych adresów IP w danym dniu, co umożliwia bardzo precyzyjną identyfikację zainfekowanych urządzeń mobilnych.

Są to dane w 100% zanonimizowane i prezentowane na poziomie agregatów. Statystyki opatrzone są komentarzami na temat najważniejszych trendów i zależności. Całość uzupełnia opis najciekawszych zagrożeń i podatności.

Najważniejszy wskaźnik ze statystyk generowanych przez T-Mobile Polska pokazuje, że aż 7,25% telefonów działających w Polsce w segmencie biznesowym (średnie i duże przedsiębiorstwa) komunikuje się ze złośliwymi adresami IP na całym świecie, przy czym dla średnich firm jest to ok. 8%, a dla dużych firm ok. 5%. Warto podkreślić, że większość organizacji w ogóle nie ma świadomości, że tak się dzieje, co widać na przykładzie badania PMR. Wynika z niego, że 43% podmiotów w żaden sposób nie monitoruje służbowych telefonów, więc ich wiedza na temat możliwych cyberataków jest mocno ograniczona.

UDZIAŁ (%) KART SIM W ŚREDNICH I DUŻYCH FIRMACH W POLSCE, KTÓRE PRZYNAJMNIEJ RAZ W MIESIĄCU KOMUNIKOWAŁY SIĘ Z POTENCJALNIE ZŁOŚLIWYMI ADRESAMI IP NA ŚWIECIE W PODZIALE NA PRODUCENTÓW TELEFONÓW: APPLE, HTC, HUAWEI, LG, MOTOROLA, SAMSUNG, SONY, XIAOMI



Wyjaśnienie: tylko karty używane w telefonach wybranych producentów. Dane na wykresie nie odwzorowują podanej kolejności.
Źródło: T-Mobile Polska, 2019 r.

Dwa najbardziej popularne mobilne systemy operacyjne w kraju, jeśli chodzi o smartfony, charakteryzuje podobny poziom bezpieczeństwa, rozumiany jako ekspozycja na ryzyko komunikacji z potencjalnie złośliwymi adresami IP.

Można zaryzykować tezę, że poziom bezpieczeństwa urządzeń zależy od dostępności aktualizacji systemu operacyjnego. Częstotliwość aktualizacji jest większa w przypadku modeli tzw. flagowych, dla których poprawki dostępne są częściej niż dla telefonów mniej popularnych.

Podział zagrożeń z uwzględnieniem producentów telefonów jest mocno skorelowany z popularnością smartfonów, z jakich korzystają użytkownicy w Polsce. W efekcie pozycja poszczególnych dostawców jest rezultatem umasowienia ich rozwiązań. Ma natomiast niewiele wspólnego z faktem, że jeden smartfon jest bardziej bezpieczny niż inny. Owszem, różnice istnieją, jednak i tak **kluczowe znaczenie ma zachowanie użytkownika**. Bez bardziej wnikliwych badań trudno natomiast zakładać, że konsumencka ekspozycja na ryzyko w sieci może być różna w przypadku różnych producentów sprzętu.

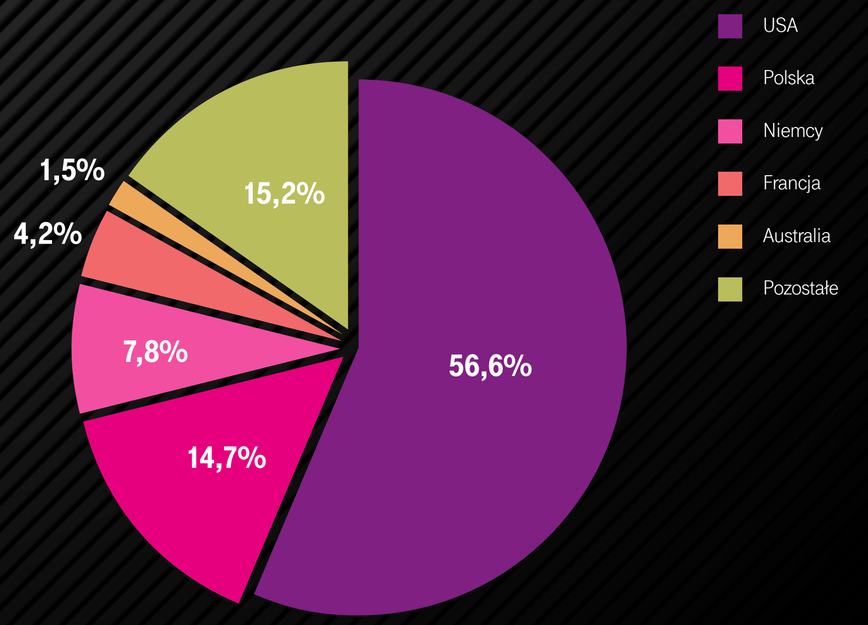
Specjaliści od cyberbezpieczeństwa podkreślają, że przeciętny użytkownik telefonu, nawet biznesowy, nie musi się znać na szczegółowej mechanice ataków w sieci. Kluczowa jest jednak sama świadomość istnienia zagrożeń. Każda osoba powinna zdawać sobie sprawę, że codziennie należy liczyć się z wieloma zagrożeniami – począwszy od phishingu, przez szkodliwe aplikacje, po strony zainfekowane celowo i niecelowo.

Każdy odnośnik, który możemy kliknąć na portalu, warto traktować z odrobiną podejrzliwości. Innymi słowy, najważniejsze jest krytyczne podejście do odbieranych treści (np. nietypowych reklam, nieznanych linków itp.).

Potencjalnie złośliwe sesje to takie, w których uczestniczą serwery o adresach IP występujących na listach. Listy tworzone są w oparciu o informacje na temat kampanii różnych grup hakerskich, aktywności szkodliwego oprogramowania, automatów skanujących sieć w poszukiwaniu podatnych urządzeń. Musimy pamiętać, że jeden adres IP może obsługiwać wiele serwisów i w zależności od liczby zgłoszeń niekorzystnej aktywności rośnie poziom „pewności" szkodliwości. Jednak nigdy nie możemy powiedzieć, że jakikolwiek adres jest w 100% szkodliwy. Mimo wszystko, ekspozycja na ryzyko w przypadku kontaktu z takim adresem jest ponadprzeciętna i rośnie prawdopodobieństwo szkody dla użytkownika.

Średnio komunikacja między złośliwymi serwerami a urządzeniami klientów to 76 kb. Nie są to teoretycznie duże pliki, ale odnosząc je do znaków (tekstu), to znaczące liczby (60 tys. znaków). Ze statystyk T-Mobile Polska wynika, że zdarzają się zdecydowanie większe wycieki, w rozumieniu danych przetransferowanych na potencjalnie złośliwe adresy IP. **Największe sesje to skala rzędu 4,3 GB. Zakładając, że w wyniku nawiązania złośliwej sesji doszło do rzeczywistego wycieku, z pewnością taka ilość danych oznaczałaby przesłanie wszystkich informacji tekstowych z urządzenia, ewentualnie ok. 1000 średniej jakości zdjęć lub ponad 40 filmików 30 sekundowych (FHD 30 k/s) nagranych smartfonową kamerą.**

UDZIAŁ (%) POSZCZEGÓLNYCH KRAJÓW W LICZBIE POTENCJALNYCH INCYDENTÓW (ZŁOŚLIWYCH SESJI) Z WYKORZYSTANIEM KART SIM W ŚREDNICH I DUŻYCH FIRMACH W POLSCE



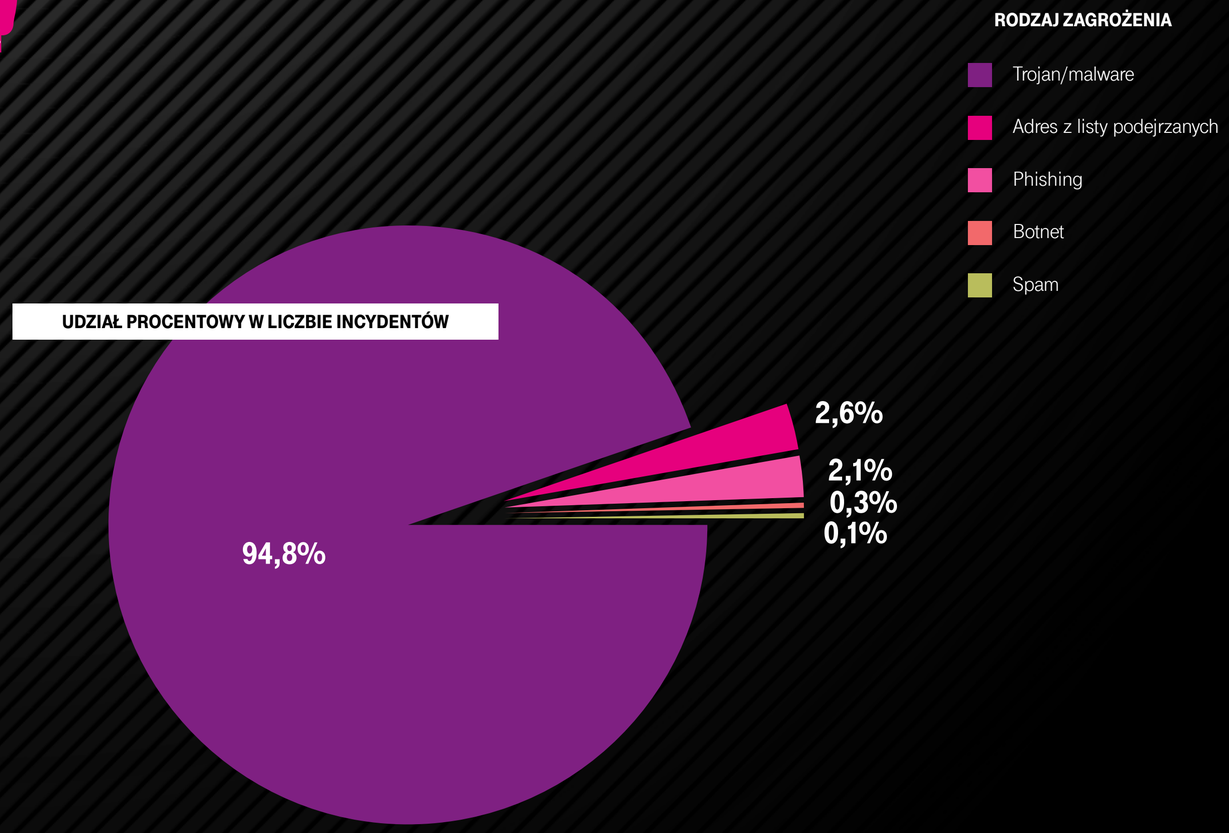
Źródło: T-Mobile Polska, 2019 r.

Geografia złośliwych sesji jest zbieżna z lokalizacją największych farm serwerowych na świecie. Powodem nawiązywania złośliwych sesji z krajami takimi jak USA, Niemcy i Francja jest lokalizacja największych serwerowni, centrów danych i punktów wymiany ruchu światowych gigantów w obszarze chmury publicznej, takich jak Amazon, Microsoft i Google. W przypadku Francji chodzi o największe serwerownie OVH – również jednego z liderów w obszarze chmury i usług hostingowych.

Drugie miejsce Polski wynika z faktu, iż prezentujemy wyniki monitoringu kart SIM i telefonów zalogowanych w sieci T-Mobile Polska. Siłą rzeczy Polacy korzystają z lokalnych zasobów hostingowych. Do tego dochodzi natężenie zarówno ruchu lokalnego, jak i krajowych punktów wymiany ruchu.

Średni czas trwania jednej złośliwej sesji to przeciętnie 19,5 sekundy. Teoretycznie to tyle, co wczytanie strony z całą jej zawartością – obrazki, tekst, skrypty itp. W praktyce jest to też czas absolutnie wystarczający do skutecznego spenetrowania urządzenia klienta.

NAJPOPULARNIEJSZE TYPY ZAGROŻEŃ WEDŁUG UDZIAŁU PROCENTOWEGO W LICZBIE INCYDENTÓW (ZŁOŚLIWYCH SESJI) W CIĄGU JEDNEGO MIESIĄCA Z WYKORZYSTANIEM KART SIM W ŚREDNICH I DUŻYCH FIRMACH W POLSCE



Źródło: T-Mobile Polska, 2019 r.

Ze statystyk T-Mobile Polska wynika ponadto, że **zdecydowanie najczęstszymi zagrożeniami są te typu malware/trojan. Odpowiadają za 95% incydentów**, do których dochodzi w ciągu miesiąca. Poniżej prezentujemy najciekawsze przykłady tego rodzaju zagrożeń, zestawione przez specjalistów z zakresu cyberbezpieczeństwa T-Mobile Polska. Pokazują one bieżące trendy w tym obszarze.

Malware (złośliwe oprogramowanie)

Przykłady:

Murofet (zwany także LICAT) – do rodziny Zeus. Wykorzystuje algorytm generowania domeny (DGA) do określenia bieżących nazw domen C2. Istnieją co najmniej trzy różne wersje DGA Murofeta.

Nymaim – od 2013 r. wykorzystywany głównie jako dropper dla ransomware TorrentLockera, a od pierwszego kwartału 2016 r. poznany przede wszystkim jako banker – czyli trojan Nymaim, który powstał w oparciu o kod źródłowy innego szkodliwego programu (Gozi). Początkowo zapewniał cyberprzestępcom zdalny dostęp do komputerów PC. Później jako trojan bankowy został sklasyfikowany przez badaczy bezpieczeństwa w rankingu TOP 10 najpopularniejszych szkodliwych programów finansowych.

P2pgoz – GameOver Zeus (GOZ), wersja peer-to-peer (P2P) z rodziny złośliwego oprogramowania bankowego Zeus, wykrytego we wrześniu 2011 r., wykorzystuje zdecentralizowaną infrastrukturę sieciową skompromitowanych komputerów osobistych i serwerów internetowych do wykonania polecenia i kontroli GOZ. Często rozpowszechniany za pośrednictwem spamu i wiadomości phishingowych, używany jest głównie przez cyberprzestępców do zbierania informacji bankowych z komputera ofiary, takich jak dane logowania.

Banjori – wykrada dane osobiste, takie jak nazwy użytkowników oraz hasła, przesyła je do serwera zarządzania i dystrybucji, należy do grupy określanej mianem „Banking malware".

Bedep – to trojan, który otwiera backdoora na zainfekowanym systemie i może zapewnić złośliwemu aktorowi pełną kontrolę nad systemem, a także pobrać dodatkowe złośliwe oprogramowanie. Po wykonaniu Bedep jest w stanie ułatwić kradzież informacji. Da się go ponadto wykorzystać do oszustwa polegającego na tym, aby kliknąć i odwiedzić określone strony internetowe w celu uzyskania korzyści finansowych.

Beebone – jest to zaawansowany wirus (istnieje pewna symbioza z wirusem Vobfus). Wykryto warianty, w których wirus CVobfus pobiera części kodu Beebona, po czym Beebone pobiera kolejne części kodu Vobfusa i tak naprzemiennie. Symbiotyczna relacja między robakiem Vobfus a trojanem Beebone z pewnością jest dla ataku korzystna. Ponieważ obie rodziny szkodliwego oprogramowania nie są jednolicie wykrywane, tylko jeden szkodliwy program początkowo zainfekuje system docelowy. Po pobraniu zostanie zainstalowany nowy wariant złośliwego intruza z działającego złośliwego oprogramowania, który może jeszcze bardziej utrudnić ustalenie przyczyny problemu.

Trojan (koń trojański)

Przykłady wraz z funkcjonalnościami:

Trojan-Banker – jego celem jest kradzież danych konta dla systemów bankowości internetowej, systemów płatności elektronicznych oraz kart kredytowych lub debetowych.

Trojan-DDoS – może uruchamiać ataki typu „odmowa usługi" (DoS) i nierzadko wpływa nie tylko na punkty końcowe, ale także na strony internetowe. Wysyła wiele żądań – z komputera i kilku innych zainfekowanych urządzeń – atak może więc przeciążać adres docelowy, co prowadzi do odmowy usługi.

Trojan-Downloader – może pobierać i instalować na komputerze nowe wersje szkodliwych programów, w tym trojany i adware.

Trojan-FakeAV – kopiuje aktywność oprogramowania antywirusowego i żąda okupu za usunięcie zagrożeń, które w praktyce są fabrykowane.

Trojan-GameThief – kradnie informacje o kontach użytkowników gier online.

Trojan-Ransom – może zmieniać dane w punkcie końcowym, co prowadzi do nieprawidłowego działania urządzenia. Cyberprzestępca może żądać okupu w celu odblokowania właściwych ustawień lub umożliwienia odzyskania danych.

Trojan-SMS – atakuje smartfony i tablety z systemem operacyjnym Android i może przechwycić SMS-y z banków, w których wysyłane są hasła do autoryzacji transakcji na rachunkach rozliczeniowych. Trojan rozprzestrzenia się jako aplikacja podszywająca się pod Flash Player. Po pobraniu jej z zainfekowanej strony instaluje się na smartfonie lub tablecie. Przy tym trudno ją usunąć, ponieważ posiada uprawnienia administratora. Później złośliwa aplikacja skanuje urządzenie w poszukiwaniu aplikacji bankowych. Jeśli znajdzie jedną z nich, generuje podrobioną stronę logowania i blokuje ekran do czasu wpisania danych. Informacje te trafiają do przestępców.

Trojan-Spy – może szpiegować sposób korzystania z urządzenia np. przez śledzenie danych wprowadzanych za pomocą klawiatury, robienie zrzutów ekranu lub uzyskiwanie listy uruchomionych aplikacji.

Trojan-Mailfinder – wykrada adresy e-mail z urządzenia.

Adres z listy podejrzanych

Pod tą kategorią kryją się adresy zaklasyfikowane jako potencjalnie niebezpieczne. System Cyber Guard T-Mobile Polska zasilany jest listami, na których znajdują się złośliwe domeny. T-Mobile Polska ma listy zdefiniowane według własnych opisów, ale korzysta również z list zewnętrznych w tym obszarze. Najważniejszym źródłem jest lista firehol_level1, zawierająca ponad 621 mln potencjalnie złośliwych adresów IP z całego świata (w tym ok. 6 tys. adresów z Polski). Lista jest automatycznie aktualizowana i regularnie uzupełniania o nowe adresy.

Phishing

Przykłady:

Spear phising – nakierowany na określonego użytkownika. Otrzymana wiadomość jest wysłana rzekomo przez kogoś, kogo znamy, np. e-mail od bliskiej osoby zatytułowany „zaproszenie na spotkanie klasowe". Po jego otwarciu proszeni jesteśmy o zalogowanie się swoimi danymi.

Clone phising – ataki, podczas których oryginalna wiadomość e-mail zostaje przechwycona i podmieniona na kopię zawierającą groźne wirusy i programy. Cyberprzestępca zastępuje wcześniejsze linki i załączniki szkodliwym oprogramowaniem, a następnie przesyła wiadomość dalej, posługując się przy tym fałszywą nazwą konta e-mail (która jest podobna do pierwowzoru).

Whaling – phising ukierunkowany przede wszystkim na kadrę kierowniczą przedsiębiorstw, VIP-ów lub osoby bardzo dobrze sytuowane (stąd nazwa – whaling: z ang. wielorybnictwo – oszuści liczą na „duży połów").

Botnet

- Przestępcy mogą używać botnetów do:
- rozsyłania spamu,
- rozprzestrzeniania wirusów,
- atakowania komputerów i serwerów,
- popełniania innych rodzajów przestępstw i oszustw.

Botnety są ważnym i bardzo eksploatowanym narzędziem w rękach cyberprzestępców, które głównie rozsyła ogromne ilości spamu. Hakerzy często ze sobą współpracują, właściciele botów wynajmują je innym osobom tak, aby te również mogły rozsyłać tego typu wiadomości. Przykładem niechcianej informacji

e-mail, wysyłanej przez takie botnety, są np. takie, które reklamują podróbki leków lub zachęcają do kliknięcia jakiegoś łącza, a to grozi pobraniem programu do kradzieży danych albo programu szpiegującego. W efekcie dochodzi do powiększenia sieci botów, ponieważ spam zawierający szkodliwe załączniki i łącza jest wyposażony w programy, które atakują kolejne komputery i tworzą nowe boty.

Spam

Większość spamu można przyporządkować do jednej z następujących kategorii:

- zawartość dla dorosłych,
- zdrowie,
- IT,
- finanse,
- edukacja/szkolenia.

Patrząc szerzej, już dzisiaj połączenie z Internetem mają nie tylko urządzenia powszechnie utożsamiane z pracą w sieci, takie jak komputery czy urządzenia mobilne. Połączone są z nim inteligentne systemy zarządzania monitoringiem, oświetleniem i temperaturą w firmie czy w domu, Smart TV oraz sprzęty typu lodówka, pralka czy kuchenka. Do wielu domowych sieci podłączone są bezprzewodowe urządzenia medyczne czy przedmioty monitorujące dzieci. Domowe sieci i urządzenia IoT są podatne na zagrożenia, ponieważ ich zabezpieczenie jest często zaniedbywane przez producentów. Do grona przedmiotów codziennego użytku narażonych na cyberataki zaliczyć też trzeba samochody. Dwa lata temu mieliśmy już do czynienia z udanymi atakami na systemy komputerowe w autach. Firma Chrysler musiała wycofać 1,5 mln sztuk modeli Chrysler Jeep po tym, jak hakerzy włamali się do nich z odległości ponad 10 mil i przejęli kontrolę nad systemem klimatyzacji, radiem czy wycieraczkami.

Czy kilka lat temu komuś przyszłoby do głowy, że jego telewizor czy kamera internetowa posłuży do zmasowanego ataku DDoS?

Dzisiaj jest to możliwe, ponieważ wiele urządzeń powszechnego użytku zawiera interfejs sieciowy i komunikuje się z Internetem, tworząc infrastrukturę znaną pod nazwą IoT (Internet Rzeczy). Infrastruktura tego typu może być narzędziem służącym hakerom do przeprowadzenia ataku DDoS. Skala tego rodzaju zdarzeń jest coraz większa. Jeden z ostatnich przykładów to atak, który w pewnym momencie generował ruch wielkości prawie 1 Tb/s (1000 Gb/s). Celem ataku był system informatyczny należący do francuskiego dostawcy usług sieciowych OVH. Ocenia się, że tak duży ruch – największy jak dotąd odnotowany na świecie – generowało 152 tys. zhakowanych wcześniej urządzeń IoT, takich jak kamery CCTV i urządzenia wideo.

Z powyższych danych i wniosków wynika bardzo istotny trend w obszarze zagrożeń, który w kolejnych latach będzie się na pewno umacniał. Podatności poszukuje się i nadal będzie się ich poszukiwać, dyskontując zależność dwóch głównych zmiennych:

- skali zjawiska, czyli najczęściej liczby urządzeń (im większa, tym bardziej atrakcyjny cel),
- stopnia ochrony (im mniejszy, tym bardziej atrakcyjny cel).

W przypadku urządzeń ekosystemu IoT widać jak na dłoni, że spełniają one niemal w 100% oba powyższe warunki. Problemem jest to, że z reguły nikt nie czuwa nad aktualizowaniem oprogramowania zarządzającego takimi urządzeniami IoT. W efekcie po pewnym czasie jest ono pełne luk pozwalających instalować malware służący do przeprowadzania ataków DDoS. To poważne ostrzeżenie, że ataków takich może być wkrótce dużo więcej.

Czy powyższy przykład można odnieść przez analogię do telefonów komórkowych? Nie ulega wątpliwości, że również w tym obszarze wpasowuje się w trend. Skala zjawiska jest znacząca – liczba urządzeń rośnie, a poziom ich zabezpieczenia nadal pozostawia wiele do życzenia. Do tego dochodzi jeszcze aspekt danych, do których można mieć dostęp. Jeśli chodzi o komórki, to tworzą one znacznie większe możliwości niż urządzenia IoT. Jest to jasny sygnał, szczególnie dla sektora B2B, że lekceważenie zagrożeń może być naprawdę kosztowne.

Faktem jest, że telefony komórkowe, bez których większość z nas nigdy nie opuszcza domu, są podatne na cyberataki. Jeden z najbardziej spektakularnych i działających na wyobraźnię cyberataków w 2019 r. dotyczył WhatsAppa – komunikatora instalowanego powszechnie na smartfonach. 13 maja świat obiegła informacja, że atakujący wykorzystali lukę w WhatsAppie – aplikacji zainstalowanej na 1,5 mld urządzeń na całym świecie – i z powodzeniem zainstalowali oprogramowanie szpiegujące u 1400 ofiar[1]. Napastnicy uzyskali pełny dostęp do wszystkiego, co znajduje się na zhakowanych urządzeniach mobilnych: informacji osobistych, ale przede wszystkim również danych firmowych, poczty elektronicznej, kontaktów, kamery, mikrofonu i lokalizacji. Należy zwrócić uwagę, że atakujący wykorzystywali podatność do wprowadzania złośliwego kodu i kradzieży danych ze smartfonów z systemem Android i iOS przez umieszczenie połączenia WhatsApp, nawet jeśli ofiara nie odebrała połączenia. Oprogramowanie szpiegujące kasowało też wszystkie dzienniki rozmowy tak, aby ofiary nie wiedziały, że ich urządzenie zostało zhakowane.

Przypadek ten pokazuje, że mimo wszelkich starań producenci urządzeń i systemów operacyjnych nie są w stanie zabezpieczyć użytkowników smartfonów. Aby zapewnić im odpowiednią ochronę, konieczne są dedykowane rozwiązania zabezpieczające telefony, a zwłaszcza uniemożliwienie oprogramowaniu szpiegującemu rozpoczęcia procesu gromadzenia informacji na temat użytkownika. Zdaniem specjalistów, jeśli oprogramowanie szpiegujące zostanie wykryte po zainfekowaniu urządzenia, jest już najczęściej za późno i proces szpiegujący uruchamia się automatycznie. Najważniejsze jest powstrzymanie ataku, zanim faktycznie zainfekuje telefon. Jeśli jednak urządzenie zostanie zainfekowane, wówczas priorytetem jest zakłócenie komunikacji tak, aby ograniczyć do minimum eksport wrażliwych danych ze smartfona.

1 https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab.

5.1. OKIEM EKSPERTA T-MOBILE

SZANOWNI PAŃSTWO,

jak możemy zaobserwować w niniejszym raporcie, firmy w dalszym ciągu zbyt mało uwagi poświęcają zagadnieniu cyberbezpieczeństwa telefonów służbowych. Ma to swoje konsekwencje na różnych płaszczyznach. W mojej opinii pierwszym krokiem jest przydzielenie odpowiedzialności za bezpieczeństwo smartfonów konkretnej jednostce.

Drugim jest stworzenie kompleksowej polityki użytkowania takiego sprzętu. Do trzeciego filaru należy dobór odpowiednich narzędzi oraz skuteczne nimi zarządzanie. Wyodrębnić możemy też czwarty – obejmujący monitoring urządzeń. Różnego rodzaju luki występują na wszystkich tych polach. Obrazują to choćby takie wskaźniki jak ten związany z 16-procentową grupą przedsiębiorstw, którzy nie posiadają w swoich strukturach żadnego działu zajmującego się bezpieczeństwem służbowych telefonów komórkowych. Sądzę, że na szczególną uwagę zasługują również dane świadczące o słabej kontroli firm nad użytkowaniem sprzętu służbowego, włączając w to korzystanie z Internetu, hotspotów czy kontrolę dostępu do danych.

Jednocześnie, jak czytamy, mimo tych luk firmy niechętnie decydują się na wsparcie partnerów zewnętrznych – taki krok podejmuje zaledwie kilka procent z nich. Tymczasem często to właśnie ono umożliwia optymalizację zarządzania urządzeniami oraz kosztów przeznaczanych na ten cel. Jako T-Mobile Polska od lat konsekwentnie włączamy się w budowanie świadomości przedsiębiorstw w tym zakresie. Te działania skutkują oczywiście również ciągłym tworzeniem i doskonaleniem adekwatnych produktów.

Do takich rozwiązań należy nasza usługa Cyber Guard, która analizuje cały ruch w sieci (kilkanaście miliardów sesji internetowych dziennie) – bazując na szerszych danych niż tylko DNS – pod kątem zdefiniowanych zagrożeń, dopasowanych profilem do potrzeb firmy. Oprogramowanie, które udostępniamy naszym Klientom pozwala na zdefiniowanie indywidualnych blokad bezpieczeństwa, wybranych pod kątem organizacji. Umożliwia to sprawne zarządzanie bezpieczeństwem wszystkich firmowych mobilnych urządzeń, dzięki czemu wychwytywanie incydentów jest dużo łatwiejsze. Warto podkreślić, że technologia ta pozwala nie tylko ochronić się przed cyberzagrożeniami, w tym wyciekami danych, ale również przed nadużyciami, co pozostaje równie istotną kwestią dla bezpieczeństwa całej firmy.

PAWEŁ DOBRZAŃSKI,

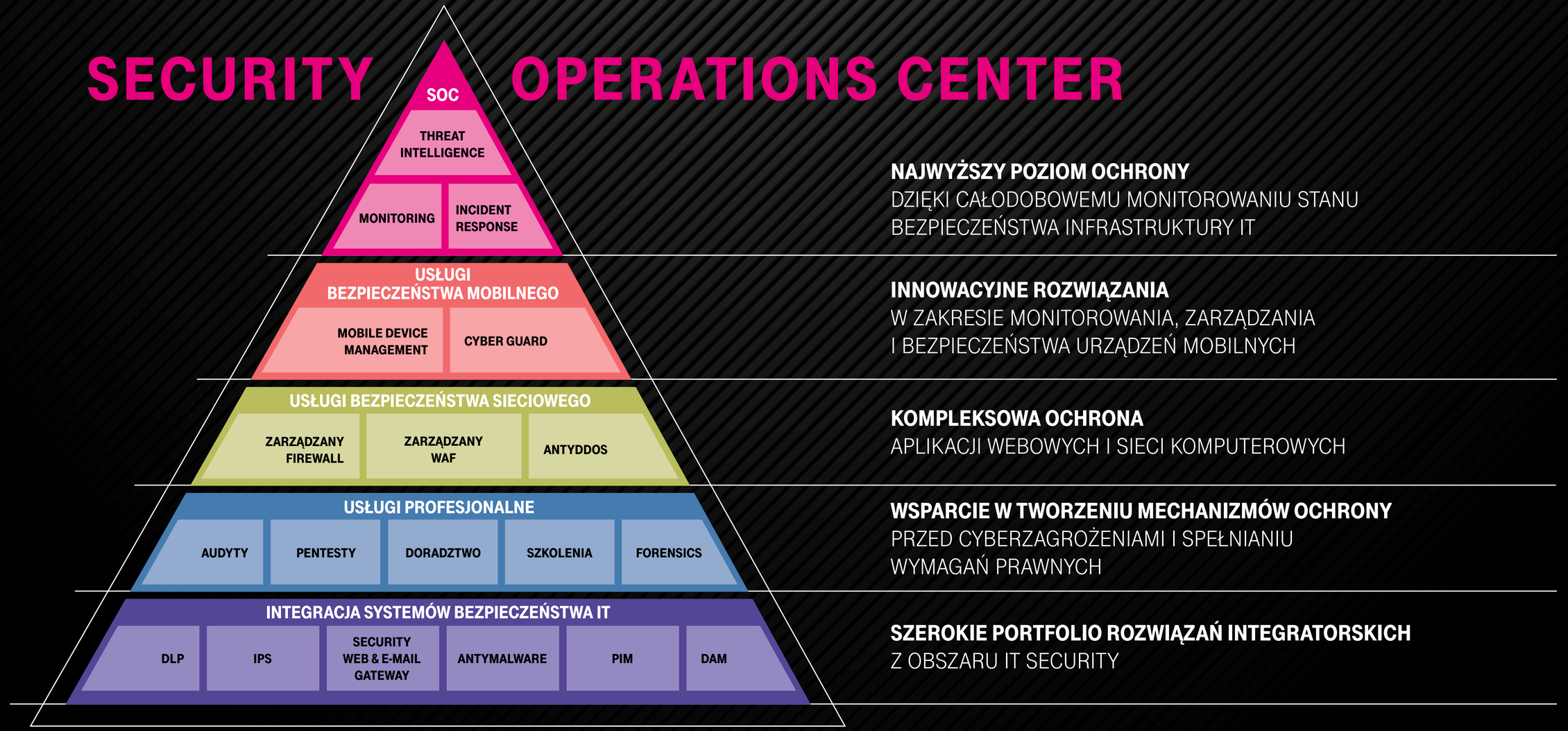
Dyrektor Departamentu
Bezpieczeństwa
T-Mobile Polska

Niewątpliwą przewagą jest tu ponadto wygoda rozwiązania – zarówno w aspekcie jego swobodnej skalowalności, jak i braku konieczności instalacji aplikacji. Usługi tego typu znacząco mogą podwyższyć poziom kontroli przedsiębiorstwa nad posiadanymi przez niego urządzeniami mobilnymi, a tych, jak wynika z prognoz, w najbliższych latach wciąż będzie w świecie biznesu przybywać. ■

6. OFERTA USŁUG BEZPIECZEŃSTWA T-MOBILE

6.1. USŁUGI BEZPIECZEŃSTWA W OFERCIE T-MOBILE

T-Mobile jest dostawcą usług zarządzanego bezpieczeństwa (tzw. Managed Security Services), obejmujących poniższe rozwiązania.



NAJWYŻSZY POZIOM OCHRONY
DZIĘKI CAŁODOBOWEMU MONITOROWANIU STANU BEZPIECZEŃSTWA INFRASTRUKTURY IT

INNOWACYJNE ROZWIĄZANIA
W ZAKRESIE MONITOROWANIA, ZARZĄDZANIA I BEZPIECZEŃSTWA URZĄDZEŃ MOBILNYCH

KOMPLEKSOWA OCHRONA
APLIKACJI WEBOWYCH I SIECI KOMPUTEROWYCH

WSPARCIE W TWORZENIU MECHANIZMÓW OCHRONY
PRZED CYBERZAGROŻENIAMI I SPEŁNIANIU WYMAGAŃ PRAWNYCH

SZEROKIE PORTFOLIO ROZWIĄZAŃ INTEGRATORSKICH
Z OBSZARU IT SECURITY

6.2. OKIEM EKSPERTA T-MOBILE

SZANOWNI PAŃSTWO,

TOMASZ ŁUŻAK,
Product Manager
odpowiedzialny za rozwój
oferty usług bezpieczeństwa IT

smartfony to urządzenia, z którymi praktycznie się nie rozstajemy i które stały się nieodłącznym elementem naszego życia. Obecne smartfony mają odpowiednią moc obliczeniową, żeby zastąpić komputer w większości podstawowych zadań. Ponadto nie ustępują standardowym komputerom w zakresie dostępu do różnego rodzaju aplikacji czy danych.

Dlatego sięgamy po nie i pracujemy z nimi znacznie częściej niż z tradycyjnymi komputerami, choć mało kto zdaje sobie z tego sprawę. Warto przytoczyć w tym miejscu chociażby niektóre wyniki badania Smart(fonowe) relacje, przeprowadzonego w 2018 r. przez Ipsos na zlecenie Huawei. Ponad połowa Polaków przyznaje w nim, że ma telefon komórkowy pod ręką przez ponad 13 godzin w ciągu doby, prawie trzy czwarte z nich kładzie przed snem telefon w pobliżu łóżka, a ponad 50% sięga po niego zaraz po przebudzeniu. Dla ponad 53% Polaków telefon komórkowy jest ważniejszy niż komputer. Ludzie uzależnieni od swoich smartfonów, z wiecznie pochylonymi głowami, doczekali się nawet swojego określenia: smombies (od smartphone zombies). Jedno jest pewne – smartfony na stałe już zmieniły nasze życie, sposoby komunikacji czy spędzania wolnego czasu, ale także znacząco ułatwiły naszą pracę i zwiększyły jej wydajność.

W tym miejscu powinniśmy sobie jednak zadać kilka pytań. Czy kiedykolwiek zastanawialiśmy się, jakiego rodzaju dane znajdują się na naszym smartfonie i co mogłoby się z nimi stać w przypadku zgubienia/kradzieży urządzenia lub ich wycieku? Nie chodzi tu tylko o zdjęcia czy SMS-y, ale także nasze kontakty, załączniki mailowe czy inne dane, do których mamy dostęp przez różnego rodzaju aplikacje mobilne. Problem ten dotyczy zarówno naszych prywatnych, jak i firmowych telefonów. Czy mamy świadomość, że smartfony są również podatne na cyberataki? Głównym problemem nie są w tym przypadku złośliwe strony WWW czy zainfekowane załączniki, przesyłane drogą mailową, ale przede wszystkim typowo mobilne aplikacje, zawierające złośliwy kod i często podszywające się pod inne, oryginalne produkty. Czy wiemy, dlaczego cyberprzestępcy atakują nasze urządzenia mobilne? Przede wszystkim jest to zazwyczaj znacznie łatwiejsze niż ataki na coraz lepiej zabezpieczone komputery czy sieci. Po drugie – aby kraść (np. przez przechwytywanie kodów jednorazowych, wysyłanych przez banki, kradzież portfeli mobilnych czy kryptowalut) lub zarabiać (np. przez dołączenie naszego smartfona do botnetu, generującego ataki DDoS lub wysyłającego spam, instalację mobilnego ransomware lub adware czy kopanie kryptowalut). Po trzecie – aby nas szpiegować przez kamerę wideo, mikrofon, śledzenie lokalizacji czy analizę historii połączeń i wiadomości. Finalnie – aby wykraść naszą tożsamość internetową w celu dostępu do kont online, zdalnego czytania e-maili czy SMS-ów, kradzieży zdjęć czy dokumentów oraz podszywania się pod nas np. w mediach społecznościowych. Ostatnia kwestia, którą powinniśmy rozważyć, brzmi: czy w jakikolwiek sposób chronimy nasze urządzenia mobilne przed cyberzagrożeniami? Na to pytanie pada niestety z reguły odpowiedź jednoznacznie negatywna...

Z przeprowadzonego przez PMR badania na zlecenie T-Mobile Polska wyłania się niezbyt optymistyczny obraz. Z jednej strony na telefonach służbowych przechowujemy ogromne ilości danych, które wykorzystujemy w najważniejszych procesach biznesowych, a z drugiej strony urządzeń tych praktycznie nie zabezpieczamy przed zagrożeniami, przez co stają się one coraz częściej łakomym kąskiem dla cyberprzestępców.

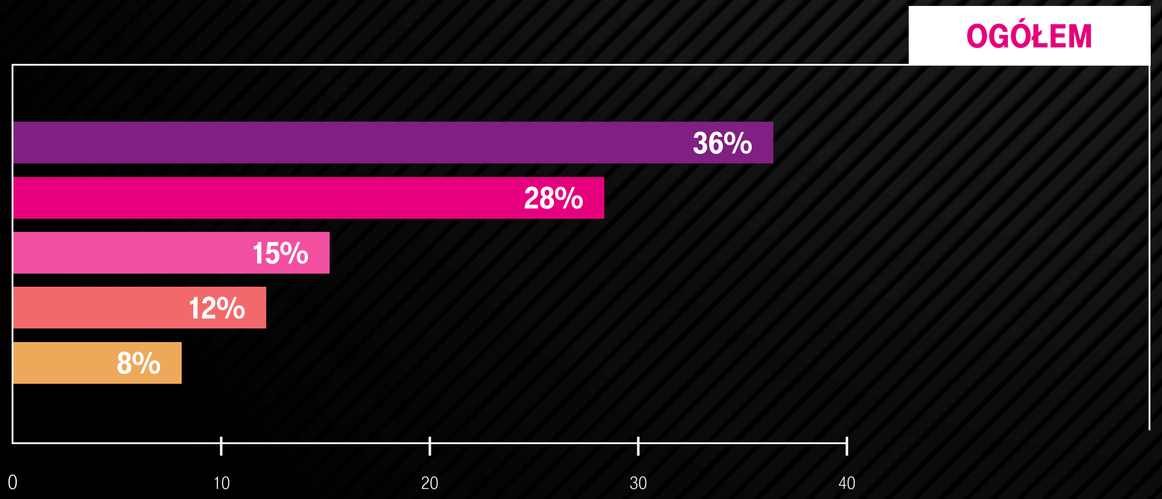
Warto jednak podkreślić, że nasze smartfony nie są bezbronne – istnieją proste i skuteczne metody ochrony przez atakami cybernetycznymi. W przypadku naszych prywatnych urządzeń w zupełności wystarczy instalacja oprogramowania antywirusowego. Firmy natomiast powinny podejść do tematu cyberochrony w sposób bardziej kompleksowy. Przede wszystkim warto zacząć od wdrożenia rozwiązań w zakresie zarządzania flotą urządzeń mobilnych typu MDM/EMM (Mobile Device Management/Enterprise Mobility Management), dzięki którym będziemy mieć możliwość m.in. separacji danych prywatnych i firmowych na telefonie, ich szyfrowania, przeprowadzenia zdalnej aktualizacji czy blokowania wybranych aplikacji, a w przypadku kradzieży lub zgubienia telefonu – zdalnego usunięcia danych, wyłączenia urządzenia czy ustalenia jego lokalizacji. Samo rozwiązanie MDM/EMM, choć podnosi „higienę" pracy z mobilnymi urządzeniami firmowymi, nie zapewnia jednak pełnej ochrony przed zagrożeniami. Dlatego coraz więcej przedsiębiorstw, chcąc kompleksowo chronić flotę swoich urządzeń mobilnych, decyduje się na wprowadzenie rozwiązań bazujących na firewallach aplikacyjnych, dzięki czemu możliwe jest szczegółowe analizowanie całego ruchu wychodzącego i przychodzącego na komórkach służbowych oraz blokowanie zidentyfikowanych ataków. Całość zabezpieczeń mogą dopełnić narzędzia sieciowe, monitorujące na bieżąco sesje nawiązywane przez nasze smartfony, identyfikujące złośliwe oprogramowanie i reagujące automatycznie w przypadku wykrycia zainfekowania. Rozwiązania tego typu posiadają kilka istotnych zalet: nie wymagają jakiegokolwiek ingerowania w urządzenia końcowe (np. instalację), są łatwo skalowane, bardzo wydaje i efektywne.

T-Mobile Polska oferuje całą gamę usług z zakresu bezpieczeństwa dla średnich i dużych przedsiębiorstw. Jesteśmy w stanie kompleksowo i skutecznie zabezpieczyć również flotę urządzeń mobilnych w Państwa firmie. Zachęcam do zapoznania się z naszą szczegółową ofertą.

7. METODOLOGIA

Na przełomie września i października 2019 r. firma badawczo-analityczna PMR na zlecenie T-Mobile Polska, przeprowadziła badanie w średnich (50-249 pracowników) i dużych (250 i więcej pracowników) firmach działających na terenie Polski. Przedsiębiorstwa, które wzięły udział w badaniu, działają w branżach: produkcyjnej i przetwórstwa przemysłowego, handlu hurtowego i B2B, budownictwa, edukacji oraz IT/telekomunikacji i mediów.

BRANŻE, W KTÓRYCH DZIAŁAJĄ BADANE FIRMY (%)



LEGENDA	ŚREDNIE FIRMY	DUŻE FIRMY
Działalność produkcyjna i przetwórstwo przemysłowe	34%	39%
Handel hurtowy, handel B2B i handel pojazdami	32%	25%
Budownictwo (firmy budowlane i wykończeniowe)	17%	14%
Edukacja	10%	14%
Informatyka/telekomunikacja/media	7%	9%

Źródło: PMR, 2019 r.

Koncepcja i główne cele badania zakładały konfrontację opinii osób odpowiedzialnych za zarządzanie, utrzymanie i zabezpieczenie firmowej infrastruktury IT oraz służbowych telefonów komórkowych z opiniami użytkowników końcowych firmowych komórek. Próba badawcza wyniosła 200 wywiadów. W każdej z ankietowanych firm przeprowadzono dwie osobne rozmowy. Jedną z pracownikiem działu IT – menadżerem, specjalistą, kierownikiem, specjalistą ds. bezpieczeństwa IT lub innym, czyli osobą posiadającą wiedzę na temat rozwiązań wykorzystywanych w obszarze IT (uwzględniając bezpieczeństwo IT i telekomunikację), drugą z pracownikiem firmy niezwiązanym z IT lub bezpieczeństwem teleinformatycznym, ale korzystającym ze służbowego telefonu komórkowego co najmniej kilka razy w tygodniu.

Badanie przeprowadzono z zastosowaniem podejścia ilościowego, wykorzystując technikę CATI (ankiety telefonicznej) na losowej próbie średnich i dużych firm. Zastosowana metodologia pozwoliła na uzyskanie standaryzowanych i rzetelnych danych ilościowych, dzięki którym można przedstawić wyniki uogólniające na całą populację średnich i dużych przedsiębiorstw w Polsce. Średni czas trwania wywiadu wynosił ok. 15 min, a pytania różniły się w zależności od typu respondenta – do pracowników działu IT w firmach skierowane były pytania specjalistyczne, związane m.in. ze stosowanymi rozwiązaniami z zakresu cyberbezpieczeństwa, RODO czy incydentami bezpieczeństwa cyfrowego na służbowych telefonach komórkowych. Z kolei pracownikom niezwiązanym z działem IT lub bezpieczeństwa cyfrowego zadano pytania głównie o kwestie użytkowania służbowych telefonów komórkowych i występowania symptomów cyberataku.

W przypadku danych z systemu Cyber Guard T-Mobile Polska referencyjnym okresem badawczym jest marzec 2019 r., przy czym rozkład jest porównywalny w kolejnych miesiącach. Analizą zostały objęte wyłącznie służbowe telefony komórkowe w dużych i średnich firmach. Baza nie zawierała kart SIM instalowanych w urządzeniach innych niż telefony. Obserwacja uwzględnia kilkadziesiąt tysięcy klientów. Analiza była prowadzona na danych zanonimizowanych.

8. WAŻNE POJĘCIA I DEFINICJE

Poniżej prezentujemy słownik ważnych pojęć z zakresu cyberbezpieczeństwa, w tym z obszaru zagrożeń i zabezpieczeń telefonów komórkowych.

Botnet – to grupa komputerów zainfekowanych szkodliwym oprogramowaniem (np. robakiem), pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu.

BYOD – używanie własnych urządzeń w miejscu pracy.

DDoS – rozproszony atak odmowy usługi, atak sieciowy, polegający na wysłaniu do atakowanego systemu takiej ilości danych, których system ten nie będzie w stanie obsłużyć. Celem ataku jest blokada dostępności zasobów sieciowych. W przypadku DDoS do ataku wykorzystywanych jest wiele urządzeń i połączeń sieciowych, co odróżnia go od ataku DoS, który korzysta z jednego urządzenia i jednego połączenia internetowego.

Incydent – zdarzenie zagrażające lub naruszające bezpieczeństwo w sieci Internet. Do incydentów zalicza się m.in. włamania lub próby włamań do systemów komputerowych, ataki typu DDoS, spam, rozsyłanie malware'u i inne przypadki naruszania zasad, które obowiązują w sieci.

Malware (złośliwe oprogramowanie) – to szeroki termin, obejmujący fragmenty kodu i programy, które szkodzą systemom. Wrogie, inwazyjne i celowo dokuczliwe złośliwe oprogramowanie ma na celu inwazję, uszkodzenie lub dezaktywację komputerów, systemów komputerowych, sieci, tabletów i urządzeń przenośnych, często przez częściowe przejęcie kontroli nad działaniem urządzenia.

Złośliwe oprogramowanie ma na celu nielegalne zarabianie pieniędzy. Nie może uszkodzić fizycznie sprzętu systemu lub sprzętu sieciowego, jednak może ukraść, zaszyfrować lub usunąć dane, zmienić lub przechwycić podstawowe funkcje komputera i szpiegować działania na komputerze bez wiedzy i akceptacji użytkownika.

MDM – oprogramowanie do zarządzania bezpieczeństwem urządzeń mobilnych.

Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) albo nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.

Podatność – błąd, luka, cecha sprzętu lub oprogramowania komputerowego stanowiąca zagrożenie dla bezpieczeństwa. Może zostać wykorzystana przez atakującego, jeżeli nie zostanie zainstalowana odpowiednia poprawka.

Polityka bezpieczeństwa/cyberbezpieczeństwa – to dokument, który warunkuje możliwość efektywnego i całościowego zarządzania w danej firmie bezpieczeństwem IT. Zawarte są w nim cele i działania, określające warunki zarządzania, ochrony i rozpowszechniania w organizacji aktywów systemu informatycznego. Tekst umożliwia pracownikom lepsze zrozumienie, czemu służą procedury bezpieczeństwa, a tym samym podnosi ich świadomość w zakresie zagrożeń i związanego z nimi ryzyka. W ramach polityki cyberbezpieczeństwa każdy realizowany projekt IT powinien zawierać procedury i instrukcje postępowania. Powstanie tego dokumentu może być wynikiem zewnętrznych regulacji prawnych albo reguł panujących w samej firmie.

Ransomware – rodzaj złośliwego oprogramowania, które po wprowadzeniu do systemu użytkownika szyfruje pliki na dysku. Odszyfrowanie wymaga zapłacenia okupu cyberprzestępcom.

RODO/GDPR – Regulacja o Ochronie Danych Osobowych.

SOC – Operacyjne Centrum Bezpieczeństwa, łączące zarówno funkcje techniczne, jak i organizacyjne, w którym systemy typu SIEM, systemy antywirusowe, IDS/IPS i firewalle dostarczają informacji do centralnego systemu zarządzania incydentami.

Spam – niepożądana przez odbiorców wiadomość tekstowa. Wysyłana jest najczęściej masowo (do wielu odbiorców) w formie reklamy przez rozmaite firmy (z reguły zagraniczne, które trudno zidentyfikować) lub hakerów (spamerów), mających na celu wyłudzenie danych osobowych lub dostępu do komputera. Najczęściej wiąże się z zapychaniem serwerów i blokowaniem skrzynek adresowych. Spam jest rozpowszechniany za pośrednictwem poczty elektronicznej, choć występują również jego odmiany krążące jako wiadomości wysyłane z poziomu komunikatorów internetowych, a także SMS-ów.

Spyware – program szpiegujący, którego zadaniem jest śledzenie działań użytkownika komputera. Monitorowanie aktywności odbywa się bez zgody i wiedzy użytkownika. Zbierane informacje dotyczą m.in. adresów odwiedzanych stron internetowych, adresów e-mail, haseł czy numerów kart kredytowych. Do programów typu spyware należą m.in. adware, trojany i keyloggery.

Trojan (koń trojański) – złośliwy program, który umożliwia cyberprzestępcy zdalne przejęcie pełnej kontroli nad systemem komputerowym. Instalacja konia trojańskiego najczęściej odbywa się przez uruchomienie złośliwych aplikacji pochodzących z niezaufanych stron internetowych lub załączników mailowych. Poza zdalnym wykonywaniem komend, trojan jest w stanie umożliwić podsłuchanie komunikacji i przechwycić hasła użytkownika.

UODO – Urząd Ochrony Danych Osobowych.

VPN – wirtualna sieć prywatna.

T-Mobile Polska S.A.
ul. Marynarska 12
02-674 Warszawa

Więcej informacji o usługach:
www.t-mobile.pl/biznes

LIFE IS FOR SHARING.