**1 na 8 firm posiada politykę bezpieczeństwa urządzeń mobilnych**

**Tylko około 14% firm posiada w pełni rozwiniętą politykę bezpieczeństwa urządzeń mobilnych dla sieci korporacyjnych.**

Z drugiej strony wzrasta liczba incydentów naruszenia bezpieczeństwa IT wycelowanych w telefony komórkowe i tablety, a większość firm nie posiada żadnych planów ograniczenia wykorzystywania prywatnych urządzeń mobilnych do celów związanych z pracą. Tak wynika z badania [Global Corporate IT Security Risks 2013](http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf) przeprowadzonego tej wiosny przez Kaspersky Lab oraz B2B International wśród firm zlokalizowanych na całym świecie.

Incydenty naruszenia bezpieczeństwa IT dotyczące urządzeń mobilnych już teraz przyjmują wiele różnych postaci, a z czasem mogą stać się tylko bardziej zróżnicowane i rozpowszechnione. 6% respondentów badania B2B International wskazało urządzenia mobilne jako źródło przynajmniej jednego wycieku poufnych danych w ciągu ostatnich 12 miesięcy. Mimo że jest to tylko o 1 proc. więcej w stosunku do 2012 r., urządzenia mobilne spowodowały więcej wycieków krytycznych danych niż ataki phishingowe (5% firm), oszustwa pracowników (4%) czy szpiegostwo korporacyjne (3%).

Przyczyna jest oczywista; każdego dnia w pracy wykorzystywanych jest wiele urządzeń mobilnych – smartfonów i tabletów. Urządzenia te często stanowią własność samych pracowników, dlatego są wykorzystywane zarówno do celów biznesowych, jak i prywatnych. Posiadanie ważnych informacji prywatnych i korporacyjnych (kontakty, aplikacje itd.) pod ręką na jednym urządzeniu bez wątpienia jest wygodne – z drugiej strony stanowi znaczne ryzyko dla bezpieczeństwa firmy. Prawie 65% uczestników badania przyznało, że środowisko BYOD (ang. Bring Your Own Device), w którym pracownicy wykorzystują swoje prywatne urządzenia do pracy, stanowi coraz większe zagrożenie dla bezpieczeństwa korporacyjnej infrastruktury IT. Jednocześnie prawie 64% firm nie planuje wprowadzenia żadnych zakazów dotyczących urządzeń mobilnych, a około połowa zbadanych firm uważa, że restrykcje byłyby bezużyteczne.

Stosowanie polityk bezpieczeństwa IT dla urządzeń mobilnych – wewnętrznych reguł korporacyjnych zarządzających ich użytkowaniem – może w znacznym stopniu zmniejszyć zagrożenia biznesowe związane ze smartfonami i tabletami. Mimo to dobrze opracowana polityka bezpieczeństwa urządzeń mobilnych stanowi częściej wyjątek niż regułę. Około 41% uczestników badania stwierdziło, że ich firma posiada wprawdzie politykę, jednak nie jest ona w pełni rozwinięta, 32% respondentów planuje wprowadzić politykę bezpieczeństwa urządzeń mobilnych w przyszłości, a 13% przyznało, że nie posiada żadnej polityki i nie planuje jej ustanowić.

Jednym z powodów, dla których polityki te nie są w pełni zaimplementowane, może być niewystarczająca ilość zasobów w postaci czasu i pieniędzy. Prawie połowa (48%) respondentów, którzy wskazali na posiadanie polityki bezpieczeństwa urządzeń mobilnych, powiedziała, że zostały przeznaczone na to niewystarczające środki, a kolejne 16% stwierdziło, że nie przyznano na ten cel żadnych pieniędzy.

**Co zrobić, aby polityki były skuteczne**

Skuteczne rozwiązania MDM (zarządzanie urządzeniami mobilnymi), oferowane w [Kaspersky Endpoint Security for Business](http://kaspersky.pl/biznes), zintegrowanej platformie bezpieczeństwa dla firm, umożliwiają zdalne wdrożenie i egzekwowanie polityk korporacyjnych, nawet na prywatnych urządzeniach przynoszonych do firmy. Na przykład, firmy mogą ograniczać listę aplikacji, które można uruchomić na urządzeniu mobilnym, lub zablokować próby przekierowywania użytkowników na szkodliwą stronę za pośrednictwem przeglądarki działającej na smartfonie lub tablecie. Konteneryzacja pozwala na wyizolowanie i zaszyfrowanie danych korporacyjnych i aplikacji, a w przypadku zgubienia lub kradzieży urządzenia kontener może zostać zdalnie wyczyszczony.

Pełny raport z badania przeprowadzonego przez Kaspersky Lab oraz B2B International jest dostępny na stronie <http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf>.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.