**18% organizacji z sektora rządowego i obronności celem ataku ukierunkowanego w ciągu 12 miesięcy**

**W badaniu obejmującym niemal 4 000 menadżerów IT z 27 państw Kaspersky Lab stwierdził rosnącą liczbę ataków ukierunkowanych i określił rodzaje działalności, stanowiące najbardziej prawdopodobny cel działań cyberprzestępców – sektor rządowy i obronności, a także branża telekomunikacji.**

W skali globalnej 18% organizacji z sektora rządowego i obronnego odnotowało co najmniej jeden atak ukierunkowany w ciągu minionych 12 miesięcy. Odsetek ataków ukierunkowanych zidentyfikowanych w tym sektorze był najwyższy w tegorocznym badaniu, znacznie przewyższając wynoszącą 12% globalną średnią odnotowaną we wszystkich sektorach biznesowych. Jeśli jednak przyjrzeć się danym dotyczącym wszystkich sektorów biznesowych, wyraźnie widać, że ataki ukierunkowane nie ograniczają się do tej branży. Inne segmenty biznesowe również odnotowały wyższy niż średnia odsetek ataków ukierunkowanych. Przykładem może być branża telekomunikacji, w której 17% firm zostało dotkniętych atakiem ukierunkowanym, jak również sektory usług finansowych oraz transportu i logistyki – oba odnotowały w ciągu minionych 12 miesięcy odsetek ataków ukierunkowanych na poziomie 16%.

Wyniki badania pokazują, że rośnie również łączna liczba ataków ukierunkowanych. W 2013 roku ataki takie odnotowało 12% wszystkich firm. Dla porównania: w 2013 i 2012 roku średnia wynosiła 9%.

Wyniki badania przeprowadzonego we współpracy z B2B International zostały opublikowane w raporcie podsumowującym „Zagrożenia dla bezpieczeństwa IT 2014”, w którym wyszczególniono rodzaje wewnętrznych i zewnętrznych zagrożeń dla bezpieczeństwa, najczęściej napotykanych przez firmy z różnych branż, jak również koszty związane z incydentem naruszenia bezpieczeństwa IT, rodzaje danych, które są najczęściej tracone na skutek takich ataków, i wiele więcej informacji.

W ciągu minionych 12 miesięcy 94% firm zostało dotkniętych przynajmniej jednym pochodzącym z zewnątrz incydentem naruszenia bezpieczeństwa danych, obejmującym ataki phishingowe, ataki DDoS oraz kradzież urządzeń mobilnych. W wielu przypadkach firmy odnotowały utratę poufnych danych biznesowych.

Oprócz coraz większego rozpowszechnienia ataków ukierunkowanych, zarówno pod względem liczby, jak i rodzajów ofiar, coraz częściej ujawniane są również głośne działania cyberprzestępcze ukierunkowane na kluczowe cele. We wrześniu 2013 r. Kaspersky Lab opublikował analizę wieloletniej kampanii ataków ukierunkowanych o nazwie [Icefog](http://www.kaspersky.pl/about.html?s=news_press&amp;amp;cat=1&amp;amp;newsid=2103), której celem były organizacje z branży wojskowej, telekomunikacyjnej, stoczniowej oraz badawczej w Korei Południowej i Japonii. Z kolei w lutym 2014 r. Kaspersky Lab poinformował o wykryciu kampanii cyberszpiegowskiej znanej pod nazwą [The Mask](http://www.kaspersky.pl/about.html?s=news_warnings&amp;amp;cat=4&amp;amp;newsid=2192), której ofiary były zlokalizowane w 31 państwach na całym świecie, łącznie z agencjami rządowymi i organizacjami związanymi z rządem.

Chociaż łączna ilość danych, które zostały ukradzione na skutek ataków ukierunkowanych, jest mniejsza w porównaniu ze stratami na skutek ogólnych ataków z wykorzystaniem szkodliwego oprogramowania, trzeba pamiętać, że te drugie są znacznie bardziej rozpowszechnione (średnio 61% firm odnotowało ataki z udziałem szkodliwego oprogramowania, podczas gdy działania ukierunkowane dotknęły średnio 12% firm). Z drugiej strony, dane skradzione na skutek ataku ukierunkowanego będą prawdopodobnie miały dużą wartość dla cyberprzestępców i utrata tych wysoce poufnych informacji (plany przyszłych produktów, sprawozdania finansowe firm itd.) spowoduje większe szkody długoterminowe dla reputacji firmy.

Atak ukierunkowany zwykle składa się z kilku szkodliwych komponentów, które współdziałają ze sobą w celu obejścia mechanizmów bezpieczeństwa danej organizacji, infekują maszyny i kradną poufne dane. W takich atakach mogą być wykorzystywane unikatowe modyfikacje rozpowszechnionego szkodliwego oprogramowania lub określone luki w zabezpieczeniach atakowanych organizacji. Badania w zakresie bezpieczeństwa prowadzone przez Kaspersky Lab dają firmie unikatową wiedzę dotyczącą strategii ataków ukierunkowanych, co pozwoliło na stworzenie technologii, które mają na celu przeciwdziałanie takim taktykom. Mechanizmy te są wykorzystywane m.in. w rozwiązaniu [Kaspersky Endpoint Security for Business](http://www.kaspersky.pl/biznes).

Pełne wyniki badania „Zagrożenia dla bezpieczeństwa IT 2014” są dostępne w języku angielskim na stronie <http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.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>.