25 PROC. FIRM ZANOTOWAŁO WZROST LICZBY CYBERATAKÓW W 2018 ROKU

Skutki cyberprzestępczości dotknęły 68 proc. ankietowanych przedsiębiorstw, a 25 proc. z nich zanotowało wzrost liczby cyberataków - wynika z raportu KPMG w Polsce „Barometr cyberbezpieczeństwa. W obronie przed cyberatakami". Globalne straty spowodowane działalnością cyberprzestępców wyniosły około 1 % światowego PKB.

Jak wskazuje cytowany w raporcie Michał Kurek z KPMG, cyberprzestępczość rozwija się dziś niezwykle dynamicznie, a jej transgraniczny charakter sprawia, że hakerzy są dziś bezkarni. "Globalne straty z tytułu cyberprzestępczości szacowane są na 1 % światowego PKB. Cyberprzestępcy są coraz lepiej zorganizowani i dysponują ogromnym zapleczem kapitałowym. Część grup wspierana jest przez obce państwa" – ocenił Kurek.

Według raportu, który powstał na podstawie ankiety wśród 100 firm, szeroko rozumiana cyberprzestępczość została uznana za zagrożenie przez 96 proc. z nich, co oznacza wzrost o 12 punktów procentowych wobec zeszłorocznego badania. W ramach cyberprzestępczości organizacje wskazują najczęściej na zagrożenie ze strony pojedynczych hakerów (84 proc.), zorganizowane grupy cyberprzestępcze (58 proc.) oraz cyberterrorystów (54 proc.).

Ponad 9 na 10 osób odpowiedzialnych za bezpieczeństwo IT w firmach, które wzięły udział w badaniu KPMG, wskazało, że największymi cyberzagrożeniami dla ich organizacji są kradzieże danych przez pracowników, złośliwe oprogramowanie szpiegujące lub szyfrujące dane (ang. ransomware), a także ukierunkowane ataki (ang. APT – Advanced Persistent Threat) oraz phishing.

Zdaniem autorów raportu, większość firm "bardzo optymistycznie oceniła poziom swoich zabezpieczeń". Najlepiej oceniona została ochrona przed złośliwym oprogramowaniem (97 proc.) oraz zabezpieczenia styku z siecią internet (94 proc.). Ten sam odsetek firm uważa, że osiągnęły dojrzałość w kwestii monitorowania i reagowania na incydenty związane z naruszeniem bezpieczeństwa. W opinii osób odpowiedzialnych za bezpieczeństwo IT w firmach, najgorzej zabezpieczone są działania związane z zarządzaniem bezpieczeństwem w relacjach z partnerami biznesowymi, zarządzaniem bezpieczeństwem urządzeń mobilnych, a także procesami wytwarzania oprogramowania, które dodatkowo są zagrożone ryzykiem braku wymaganych inwestycji przez ankietowane firmy.

KPMG pytało także o monitorowanie bezpieczeństwa. Z ankiet wynika, że 6 proc. organizacji w ogóle nie prowadzi takiego monitoringu, a większość przedsiębiorstw robi to nieregularnie (61 proc.) lub opiera się wyłącznie na wpisaniu stosownego wymogu w obowiązki administratorów (67 proc.). Co trzecia firma deklaruje proaktywne poszukiwanie śladów cyberataków (ang. Threat Hunting) oraz ma dedykowany zespół SOC (ang. Security Operations Center). Najczęściej stosowanymi przez firmy rozwiązaniami mającymi na celu wykrywanie cyberataków są zewnętrzne źródła informacji, tzw. Threat Intelligence, które wdrożyło 61 proc. organizacji. 4 przedsiębiorstwa na 10 rozwijają wewnętrzne bazy wiedzy o zagrożeniach oraz stosują rozwiązania IDS/IPS (ang. Intrusion

Prevention/Detection Systems).

Ponad połowa ankietowanych firm (57 proc.) opracowała procedury reagowania bądź plany zarządzania kryzysowego na wypadek wystąpienia cyberataku, jednak zaledwie 17 proc. zdecydowało się na organizację dedykowanego zespołu CSIRT (ang. Computer Security Incident Response Team). Co czwarte przedsiębiorstwo korzysta z outsourcingu w tym zakresie. Podobny odsetek zdecydował się na transfer ryzyka cyberataku poprzez wykupienie polisy ubezpieczeniowej. Firmy rzadko testują skuteczność wdrożonych procesów reakcji na cyberatak – co piąta organizacja przeprowadziła w tym celu testy penetracyjne przy podejściu Red Team, a jedynie 8 proc. skorzystało z gier symulacyjnych. Z badania wynika, że aż 16 proc. ankietowanych firm nie jest w żaden sposób przygotowanych na cyberatak.

Jak wskazuje raport, dla 63 proc. firm najważniejszym problemem, który uniemożliwia budowę systemów cyberbezpieczeństwa, jest brak wykwalifikowanych pracowników. Czynnik ten już drugi rok z rzędu jest dla organizacji nieco bardziej istotny niż brak wystarczających budżetów, na które wskazało 61 proc. przedsiębiorców. Oba te obszary odgrywają coraz większą rolę w zapewnieniu odpowiedniego poziomu bezpieczeństwa IT. W 2018 roku wzrosły one aż o 14 punktów procentowych w porównaniu z pierwszą edycją badania.

Raport KPMG w Polsce pt. „Barometr cyberbezpieczeństwa. W obronie przed cyberatakami” powstał na podstawie badania zrealizowanego na próbie 100 firm. Badanie zostało zrealizowane metodą CATI (ang. Computer-Assisted Web Interview) wśród osób odpowiedzialnych za bezpieczeństwo IT (członków zarządu, dyrektorów ds. bezpieczeństwa, prezesów, dyrektorów IT lub innych osób odpowiedzialnych za ten obszar). Badanie przeprowadzono w lutym 2019 roku przez firmę Norstat Polska.

AK/PAP