**Polskie firmy w wyniku ataków hakerów tracą niemal dwukrotnie więcej niż brytyjskie**

**50 do 250 tys. zł – takie straty ma co trzecia firma (33%) w Wielkiej Brytanii w wyniku ataków hakerów – wynika z najnowszego badania firmy Check Point Software Technologies. W Polsce średnie jednorazowe straty szacuje się na 450 tys. zł!**

Ponad 31% respondentów stwierdziło, że ich firmy padły ofiarą 20 udanych ataków w ciągu ostatniego roku, a 34% z nich nie było w stanie określić liczby udanych ataków na swoją firmową sieć. Było to spowodowane dużą rozbieżnością pomiędzy stopniem zaawansowania ataków a posiadanymi danymi o zagrożeniach.

Według ankiety przeprowadzonej pośród 140 brytyjskich specjalistów z branży IT i bezpieczeństwa internetowego, rosnąca liczba ataków z wykorzystaniem złośliwego oprogramowania ma katastrofalne skutki dla firm, zarówno pod względem kosztów jak i czasu wymaganego do przywrócenia normalnego funkcjonowania zaatakowanych systemów. 28% ankietowanych stwierdziło, że potrzeba średnio 10 dni, aby usunąć skutki pojedynczego ataku. 33% z nich oszacowało koszty naprawy na kwoty w wysokości od 10 000 do 50 000 funtów.

Powyższe wyniki badań potwierdzają wnioski zawarte w raporcie bezpieczeństwa firmy Check Point opublikowanego w maju bieżącego roku, a przede wszystkim zwracają uwagę na narastający problem ochrony przed nowym, nieznanym oprogramowaniem. Raport ten, bazujący na badaniach danych bezpieczeństwa pochodzących z ponad 10 000 organizacji z całego świata i wielu różnych sektorów rynku, pokazuje, że w 33% badanych firm w okresie między czerwcem a grudniem 2013 roku zostało pobrane złośliwe oprogramowanie.

Jakiego rodzaju ataki są najgroźniejsze dla polskich firm

Niepokojącym sygnałem jest wzrost ataków hakerskich w Polsce na małe i średnie firmy w ostatnim czasie. Małe przedsiębiorstwa padają ofiarami ataków na mobilne urządzenia , gdzie przechowywane są informacje o adresach poczty elektronicznej czy numery telefonów osobistych.

Drugim obszarem, stanowiącym zainteresowanie hakerów są strony internetowe firm. Najczęściej dotyczy to stron firmowych i technologicznych oraz sklepów internetowych. W ostatnich latach były one częstym celem ataków służącym do rozpowszechniania fałszywych programów antywirusowych wśród nieświadomych tego faktu użytkowników (banki, sklepy). Obecnie najpopularniejszym typem złośliwego oprogramowania stają się aplikacje umożliwiające przeprowadzanie tzw. „ransomware”. Przestępcy korzystający z zainfekowanych stron internetowych blokują komputery różnych użytkowników, uzyskując dostęp do danych.