**Check Point Security Report - najnowsze badanie dotyczące bezpieczeństwa w sieci**

**Co 1 minutę użytkownik Internetu wchodzi na zainfekowaną stronę w sieci, co 9 minut korzysta z zagrożonej aplikacji. Co godzinę dochodzi do 2 ataków hakerów na sieci firmowe na świecie, a co 9 minut Internauta pada ofiarą ataku. Ponad połowa (53%) wirusów jest wprowadzanych do sieci firmowych przez nieświadomych pracowników. Skutek – kradzież tajnych informacji o kartach kredytowych i rozprzestrzenianie wirusa w sieciach firmowych.**

To najważniejsze wnioski wynikające z badania Check Point Security Report 2014, przeprowadzonego wśród 10.000 firm na świecie, na podstawie analizy ponad 200 000 godzin obserwacji ruchu sieciowego z ponad 9 000 bram bezpieczeństwa należących do przedsiębiorstw w 122 krajach.

Według najnowszych badań stale wzrasta liczba ataków ze strony hakerów zarówno na osoby prywatne, jak i przedsiębiorstwa. Największym zagrożeniem stają się urządzenia firmowe i mobilne. Jednocześnie 88% firm doświadczyła ataków hakerskich w 2013 roku (wzrost o 50% w stosunku do 2012 r.). Do najbardziej zagrożonych miejsc w sieci należą: Facebook i YouTube.

W 2013 roku ponad połowa - 54% firm całkowicie straciła dane w wyniku niespodziewanych ataków: najwięcej 29% to dane z kart kredytowych, 24% to kody dostępu do danych, 13% to informacje o zarobkach.

W opinii analityków Check Point niepokojącym wydaje się być fakt, iż przedsiębiorstwa nie są świadome skali problemu. Prawie połowa (47%) komputerów firmowych jest zainfekowana niebezpiecznymi wirusami (aż 80% pracowników firm nie zdaje sobie z tego sprawy). Przykładem może być koncern motoryzacyjny Toyota, który udostępniał adresy i dane 95.000 pracowników i filii w ramach ogólnodostępnej sieci korporacyjnej… Do najbardziej zagrożonych plików atakowanych przez hakerów należą dokumenty Microsoft ( 67%).

Ponad połowa (53%) wirusów wprowadzana jest do sieci firmowych drogą połączenia z zainfekowanymi stronami przez pracowników nieświadomych skali zagrożenia – przyznaje Krzysztof Wójtowicz, dyrektor zarządzający Check Point Software Technologies Polska.

W 2013 roku na świecie znacznie zwiększyła się ilość urządzeń mobilnych wykorzystywanych do celów służbowych. Trend popularnie zwany BYOD (Bring Your Own Device) spowodował, że na wielu niezabezpieczonych urządzeniach przenośnych przechowywane są wrażliwe dane firmowe. Nie wszystkie firmy zdają sobie sprawę, że powinny zaktualizować i dostosować swój system przechowywania danych oraz ich zabezpieczenia. Nic dziwnego, że w takiej nowej sytuacji, hakerzy coraz chętniej interesują się urządzeniami mobilnymi i atakami na nie.

Niepokojące było również zjawisko udostępniania i przesyłania przez korporacje plików danych z różnymi informacjami. Na świecie co 49 minut wysyłane są poza sieć firmy tajne dane, tym samym narażając się na niebezpieczeństwo ataku hakerów. Z badań Check Point wynika, że w 2013 roku 36% banków wysyłało dane zawierające informacje o kartach kredytowych swoich klientów na zewnątrz.

W opinii specjalistów Check Point najczęściej atakowanymi instytucjami w 2013 roku były banki, wydawnictwa, instytucje finansowe oraz ubezpieczeniowe. Ciekawostką są coraz częstsze ataki na instytucje edukacyjne – np. Uniwersytet we Włoszech, gdzie celem hakerów były dane osobowe studentów. Tymczasem głównym celem hakerów były dane instytucji finansowych, kody zdalnego dostępu do danych finansowych, reklamy znanych produktów.

Aby skutecznie bronić się przed atakami hakerów należy wprowadzić systemy zabezpieczeń na wielu płaszczyznach. Równie ważny jest czynnik ludzki – nasze badania wykazały, że 80 % pracowników nie jest świadomych skali zagrożenia ze strony hakerów – uważa Krzysztof Wójtowicz z CHP.