**Firmy ponoszą gigantyczne koszty spowodowane lekceważeniem przez pracowników zasad bezpieczeństwa sieciowego**

**Wyniki przeprowadzonej przez SailPoint Technologies – amerykańskiego dostawcę oprogramowania do zarządzania cyfrową tożsamością przedsiębiorstwa – ankiety wskazują na niepokojący trend. Pracownicy w coraz większym stopniu lekceważą zasady bezpieczeństwa, co często prowadzi do gigantycznych strat finansowych.**

Według przeprowadzonej w tym roku ankiety, aż 75% respondentów potwierdziło, że korzysta z tych samych haseł do różnych usług, zarówno prywatnych jak i służbowych. Jest to znaczący wzrost w stosunku do 2014 roku, w którym problem ten dotyczył 56% badanych.

Ponad połowa pytanych stwierdziła, że restrykcje narzucane przez dział IT są dla nich problematyczne i starają się je omijać. Aż jedna trzecia przyznała, że samodzielnie instaluje na urządzeniach służbowych niezbędne oprogramowanie. 13% stwierdziło, że gdyby padli ofiarą ataku lub mieli takie podejrzenia, to nie powiadomiliby o zdarzeniu działu IT. W przypadku dochodzenia przyczyn naruszenia, 49% winą obarczyłoby właśnie dział IT.

Ponadto, aż 15% pracowników rozważyłoby sprzedaż haseł do usług informatycznych w swojej firmie, gdyby otrzymali taką propozycję. Kilku badanych zgodziłoby się to zrobić za kwotę poniżej 100 dolarów.

„W czasach, gdy coraz większą uwagę zwraca się na kwestie związane z bezpieczeństwem, bardzo niepokojące są wyniki wskazujące na lekceważące traktowanie przez pracowników obowiązku zachowania w tajemnicy haseł ” – informuje w raporcie zespół odpowiedzialny za badanie.

Obawy budzą również wyniki ankiety przeprowadzonej przez Ponemon Institute na próbie 1000 amerykańskich pracowników w wieku od 18 do 65 lat, korzystających z urządzeń służbowych poza firmą. Przedkładają oni wygodę – związaną z wszechobecnym dostępem do Internetu z niezaufanych źródeł oraz korzystaniem z nieautoryzowanych aplikacji – nad obowiązek przestrzegania zasad bezpieczeństwa. Według ankiety przyczyną 64% incydentów związanych z naruszeniem infrastruktury IT okazały się zaniedbania pracowników.

Powyższe dane, w zestawieniu z wynikami ankiety przeprowadzonej przez Ping Identity, według których 78% klientów zrezygnowałoby z usługi online po informacji, że została ona naruszona przez przestępców, a 36% zrezygnowałaby po takiej wiadomości ze wszystkich usług online, jednoznacznie wskazują, że lekceważące podejście pracowników do kwestii bezpieczeństwa stanowi dla przedsiębiorstw bardzo poważny problem.

Potwierdzają to wyniki badań przeprowadzonych przez IBM, które wskazują na błędy i lekceważące podejście pracowników do sprawy bezpieczeństwa jako przyczynę powodzenia 60% ataków. Naruszenia te kosztują firmy średnio 5 mln USD, w tym 0,35 mln USD to koszty śledztwa i przywrócenia sprawności operacyjnej organizacji.

„Powodzenie ataków w znacznej części zależy od czynnika ludzkiego. Powinniśmy zwracać szczególną uwagę na uświadamianie i kształcenie pracowników w zakresie cyberbezpieczeństwa. Wielokrotnie podstawowa wiedza na temat ataków, wirusów i zagrożeń ustrzegła firmy przed ogromnymi stratami” komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.