Piotr Kluczwajd
Imperva

„Celem jest ochrona infrastruktury, czy ochrona danych biznesowych?"

Jednymi z najcenniejszych aktywów współczesnych firm są dane. Dane o klientach, zarobkach, numery kart kredytowych, informacje o transakcjach, czy warunkach współpracy kluczowych klientów, dane teleadresowe, plany strategiczne oraz wszelkie inne informacje poufne. Ponadto ustawa o ochronie danych osobowych, wspierana statutową działalnością GIODO nakłada na podmioty obowiązek ochrony tego typu informacji wraz z audytowaniem dostępu do nich przez wszelkich użytkowników zbiorów danych personalnych.

Amerykański operator telekomunikacyjny – Verizon – w tegorocznym raporcie *2013 Data Breach Investigations Report* wskazuje kilka zaskakujących aspektów: **75%** ataków jest oportunistycznych, **62%** naruszeń bezpieczeństwa czekało kilka miesięcy na wykrycie, 4% – kilka lat, czasy skutecznych ataków liczone są obecnie z minutach, maksymalnie godzinach (**84%**), **69%** wycieków informacji jest wykrywanych przez osoby/podmioty postronne, **96%** wykradanych rekordów danych pochodzi z baz danych (raport z 2012 roku).

Jak uchronić się przed takimi zagrożeniami? Jak audytować i kontrolować dostęp do danych poufnych, zapobiegać wyciekom i kradzieżom kluczowych informacji, jak wykrywać wykrywanie anomalie w zakresie dostępu do informacji nie wiedząc co jest „normalne"?

Zagrożenia ewoluują bardzo dynamicznie, rynek pokazuje jednak, że wciąż inwestujemy **95%** (źródło: IDC) budżetów m.in. w tradycyjną ochronę infrastruktury i stacji końcowych zaniedbując prawie zupełnie monitorowanie dostępu i ochronę samych danych biznesowych, które niejednokrotnie są głównymi aktywami naszych firm.