**Jak polityka bezpieczeństwa może chronić firmę przed cyberprzestępcami**

**Kaspersky Lab informuje o opublikowaniu artykułu poświęconego atakom ukierunkowanym na firmy. Tekst obejmuje informacje o trendach cyberprzestępczych oraz o metodach walki z zagrożeniami dla korporacji poprzez wykorzystanie skutecznej polityki bezpieczeństwa.**

Wykorzystywanie komputerów firmowych do prywatnych celów to nie tylko mniejsza produktywność pracowników, ale również strata czasu i pieniędzy. Co ważniejsze, takie działanie wystawia na ryzyko bezpieczeństwo sieci firmowej i stanowi zagrożenie dla krytycznych danych. Kontaktowanie się za pośrednictwem portali społecznościowych lub komunikatorów internetowych, odwiedzanie rozrywkowych stron WWW lub pobieranie plików z torrentów – takie działania są niezwykle powszechne wśród pracowników. Jednak wszystkie mogą być potencjalnie groźne dla komputerów firmowych, ponieważ zasoby, z których korzystają pracownicy, najczęściej wykorzystywane są również przez cyberprzestępców, którzy chcą przeniknąć do sieci korporacyjnej podczas przeprowadzania ataków ukierunkowanych.

Ataki ukierunkowane to jeden z najszybciej rozwijających się trendów w dziedzinie cyberzagrożeń. Przez ostatnie 3-4 lata zarówno małe firmy, jak i znane na całym świecie korporacje padały ofiarą cyberprzestępców. Aby uzyskać do dostęp do sieci firmowych, oszuści często stosują metody socjotechniki i wykorzystują luki w zabezpieczeniu oprogramowania.

Największym zagrożeniem związanym z atakiem ukierunkowanym jest to, że umożliwia on włamanie się do sieci korporacyjnej i uzyskanie dostępu do poufnych danych firmowych poprzez zainfekowanie tylko jednego komputera. Od tego momentu kontrolę przejmuje specjalne szkodliwe oprogramowanie, które znajduje inne podatne na ataki węzły w sieci korporacyjnej w celu uzyskania dostępu do danych, które interesują cyberprzestępców.

Technologie bezpieczeństwa mogą pomóc uniknąć takich incydentów. Na przykład, technologia ‘Automatyczne zapobieganie exploitom’ opracowana przez Kaspersky Lab uniemożliwia oszustom wykorzystywanie luk w oprogramowaniu, a nawet blokuje wykorzystywanie tzw. luk 0-day, czyli takich, które nie zostały jeszcze załatane przez producenta oprogramowania. Dzięki kontroli ruchu sieciowego administratorzy mogą zablokować niebezpieczną aktywność sieciową. Kontrola aplikacji blokuje uruchamianie i pobieranie nieznanych programów. Natomiast szyfrowanie plików lub całych dysków może pomóc wyeliminować ryzyko wycieków danych, nawet jeśli atak ukierunkowany powiedzie się.

Jednak żadna z wymienionych wyżej technologii nie może skutecznie chronić przed atakami ukierunkowanymi, jeżeli nie jest dobrze zintegrowana z firmowymi politykami bezpieczeństwa. Administratorzy oraz specjaliści ds. bezpieczeństwa IT powinni stosować środki administracyjne, aby zapobiec jakiemukolwiek ryzyku infekcji na skutek nieostrożności użytkowników lub braku ich wiedzy z zakresu IT. Obejmują one szkolenia użytkowników w zakresie bezpieczeństwa podczas pracy na komputerze, wprowadzenie kontroli nad prawami i przywilejami dostępu oraz skanowanie systemów w celu wykrycia luk w zabezpieczeniach oraz niewykorzystywanych usług sieciowych.

*„Niestety, obecnie nie istnieje żadna technologia, która mogłaby wyeliminować błąd ludzki w dziedzinie bezpieczeństwa sieci korporacyjnych. Jednak wzmocnienie polityk bezpieczeństwa za pomocą kilku odpowiednich technologii zapewnia skuteczną ochronę przed atakami ukierunkowanymi poprzez odpieranie ich na każdym etapie – od pierwszej próby wykorzystania luki w zabezpieczeniu po próby naruszenia bezpieczeństwa sieci”* – powiedział Kirył Kruglow, Senior Research Developer w Kaspersky Lab.

Więcej informacji na temat ochrony przed atakami ukierunkowanymi zawiera artykuł „Polityki dotyczące bezpieczeństwa: nadużywanie zasobów” opublikowany w serwisie SecureList.pl prowadzonym przez Kaspersky Lab: <http://www.securelist.pl/analysis/7234,polityki_dotyczace_bezpieczenstwa_naduzywanie_zasobow.html>.

Informację oraz artykuł można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.