**Pracownicy korzystający z internetu a bezpieczeństwo w firmie**

**Poza atakami ukierunkowanymi wykorzystywanymi przez cyberprzestępców do penetrowania firmowych sieci, istnieje jeszcze jedno potencjalne zagrożenie dla każdej firmy: pracownicy.**

Celowo lub przez przypadek mogą oni przyczynić się do ujawnienia poufnych informacji lub naruszenia praw autorskich, co z kolei może doprowadzić do kłopotliwej i niebezpiecznej sytuacji. Eksperci z Kaspersky Lab przygotowali artykuł o tego typu incydentach, wraz z poradami, w jaki sposób można zapewnić firmie bezpieczeństwo.

Pracownicy, którzy wysyłają na adresy prywatne e-maile związane z pracą, pobierają nielegalne treści lub używają pirackiego oprogramowania na swoich komputerach firmowych, są często nieświadomi, że taka aktywność może zaważyć na reputacji pracodawcy. W jednym z przypadków zgłoszonych Kaspersky Lab pracownik przechowywał w swojej prywatnej poczcie kopie różnych firmowych dokumentów, które następnie wyciekły do internetu. Gdy specjaliści IT zajęli się tą sprawą, na badanym komputerze znaleźli oprogramowane szpiegowskie, które rejestrowało informacje wprowadzane przy użyciu klawiatury, łącznie z danymi logowania do poczty e-mail. Posiadając dostęp do konta pocztowego pracownika, cyberprzestępcy mogli zidentyfikować firmowe dokumenty i ukraść je.

Innym razem pracownik przyniósł swojego domowego laptopa i połączył go z siecią firmową. Na komputerze zainstalowany był klient BitTorrent, przy pomocy którego pracownik pobierał oprogramowanie, łącznie z pirackimi aplikacjami, do celów osobistych. Trzy miesiące później w firmie zjawili się stróże prawa z nakazem przeszukania. Firmę podejrzewano o naruszenie praw autorskich poprzez korzystanie z nielegalnego oprogramowania. W efekcie musiała ona zapłacić grzywnę.

Istnieje wiele prostych technologii, które w połączeniu z polityką bezpieczeństwa mogą pomóc w uniknięciu większości tego typu przypadków. W opisanych powyżej sytuacjach sieci firmowe były kanałami, przez które ujawnione zostały poufne informacje oraz pobrane zostało pirackie oprogramowanie. Z tego powodu pierwszym krokiem powinno być ograniczenie pracownikom dostępu do zasobów online, gdyż może to zagrażać firmie, a także zablokowanie wszystkich portów i protokołów, które nie są wykorzystywane w ramach pracy. Aby ograniczyć pracownikom dostęp do aplikacji, należy włączyć politykę „domyślnej odmowy”, która zezwala na używanie jedynie takiego oprogramowania, które zostało autoryzowane przez specjalistów IT – może to zabezpieczyć firmę zarówno przed szkodliwym, jak i pirackim oprogramowaniem. Ponadto, należy zapewnić poufność i integralność firmowych dokumentów, wykorzystując technologie szyfrowania plików. Nawet jeśli cyberprzestępcy uzyskają dostęp do firmowych dokumentów, nie będą w stanie odczytać ich zawartości.

“Poza stosowaniem różnych technologii w celu identyfikowania i zapobiegania incydentom, specjaliści ds. IT powinni pamiętać również używaniu środków administracyjnych” – powiedział Kirył Kruglow, ekspert ds. szkodliwego oprogramowania, Kaspersky Lab. “Użytkownicy powinni wiedzieć, co jest dozwolone, a co zabronione przez politykę bezpieczeństwa, a także muszą mieć świadomość potencjalnych konsekwencji nadużycia tych reguł”.

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

Pełna wersja artykułu jest dostępna w serwisie SecureList.pl prowadzonym przez Kaspersky Lab: http://securelist.pl/blog/7241,polityka\_bezpieczenstwa\_nieproduktywne\_wykorzystywanie\_zasobow.html.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie http://www.kaspersky.pl/news.