HSBCnet

Złośliwe oprogramowanie (malware)

Ryzyko dla firmy:

- Utrata danych
- Straty finansowe
- Uszkodzenie sprzętu
- Paraliż działalności gospodarczej

Zadaniem złośliwego oprogramowania jest wyrządzenie szkód ofierze ataku. Działanie wymierzone przeciwko zarówno użytkownikom prywatnym, jak i korporacyjnym, może prowadzić do kradzieży informacji, uszkodzenia danych, przejmowania stron internetowych i szpiegowania działań w internecie. Przekierowanie użytkowników bankowości internetowej na strony spreparowane przez przestępców jest coraz częstszą formą ataku.

Czym jest złośliwe oprogramowanie (malware)?
Złośliwe oprogramowanie może kryć się za oprogramowaniem internetowym sprawiającym wrażenie nieszkodliwego (konie trojańskie) lub rozprzestrzeniać się między komputerami bez interakcji między użytkownikami (robaki komputerowe). Może być zaprojektowane w taki sposób, aby unikać mechanizmów zabezpieczających i wykonywać konkretne zadania.

Po jego nieumyślnym zainstalowaniu, złośliwe oprogramowanie może realizować wiele zadań w sposób niezauważony. Może szpiegować wizyty na stronach internetowych, niszczyć dane lub wyszukiwać i dopasowywać hasła. Coraz częściej wykorzystywane jest przez przestępców do szyfrowania ważnych informacji biznesowych do czasu, aż firma zapłaci „okup". Użytkownicy bankowości internetowej mogą być również przekierowywani do fałszywych stron internetowych, które rejestrują ich dane logowania w celu późniejszej kradzieży środków.

Złośliwe oprogramowanie jest zazwyczaj dostarczane z wykorzystaniem socjotechniki (np. phishingu) lub fałszywych łączy internetowych. Smartfonom i komputerom mogą zagrażać także złośliwe aplikacje oraz odpowiednio spreparowane pamięci USB.

Złośliwe oprogramowanie może pozostawać w uśpieniu miesiącami zanim zostanie uruchomione.

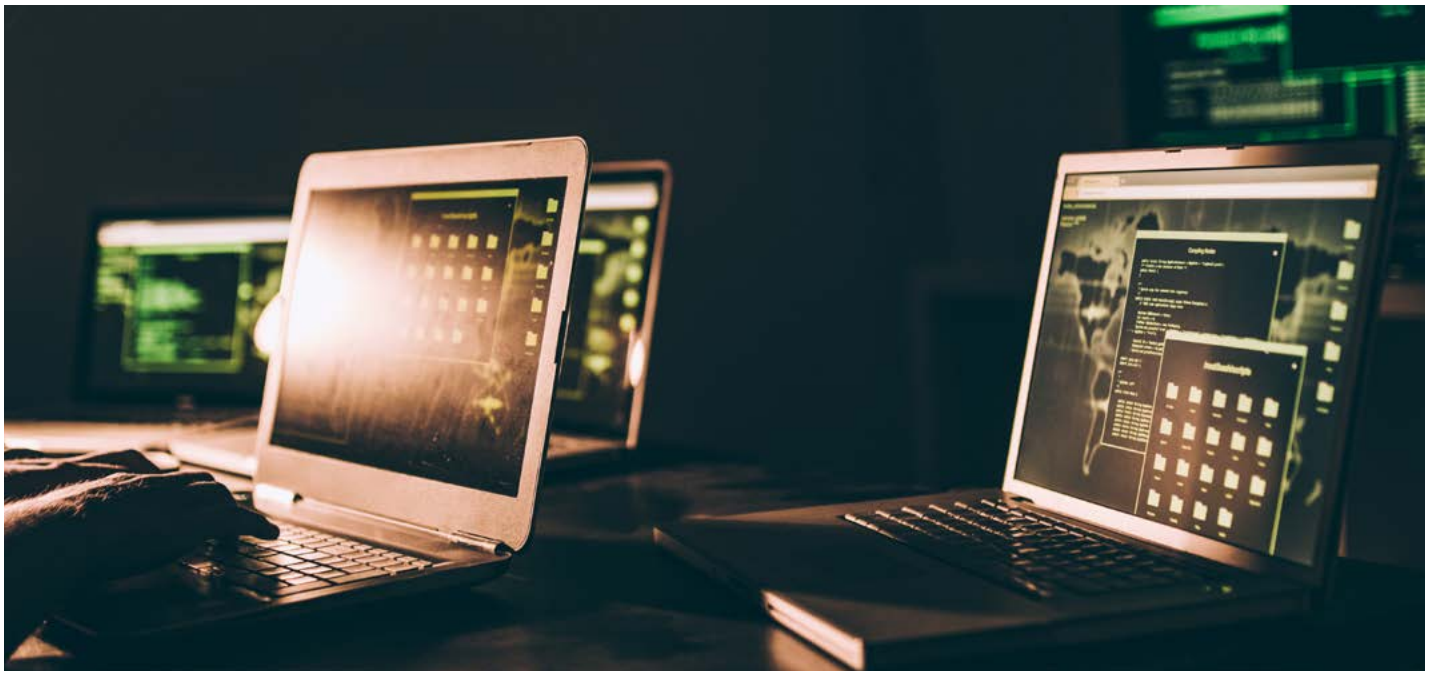
68% **przypadków naruszenia bezpieczeństwa w systemie informatycznym firm wynika z działania wirusów oraz szpiegowskiego i złośliwego oprogramowania**

Źródła: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016; http://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

Rodzaje złośliwego oprogramowania:

- Oprogramowanie szpiegowskie
- Oprogramowanie ransomware (wymuszające okup)
- Konie trojańskie
- Oprogramowanie keylogger (rejestrujące dane wpisywane na klawiaturze)

HSBC



Instytut AV-Test odnotowuje codziennie

390,000

złośliwych programów

Źródła: https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016; http://www.clearswift.com/blog/2016/05/24/10-shocking-malware-and-ransomware-statistics

Jak zabezpieczyć swoją firmę:

Oszustwo może wydać się jeszcze bardziej przekonujące, jeżeli złodzieje pozyskają informacje na temat kierownictwa i zespołu finansowego firmy, na przykład z jej strony internetowej.

- Należy wdrożyć silne procedury reagowania, odzyskiwania systemu oraz tworzenia kopii zapasowych.
- Należy regularnie przeprowadzać kontrole wszystkich urządzeń w firmie przy pomocy aktualnego oprogramowania antywirusowego. Częste skanowanie antywirusowe może pomóc zminimalizować ryzyko ataku dokonanego przy użyciu złośliwego oprogramowania.
- Należy aktualizować komputery, serwery i powiązany sprzęt, instalując najnowsze poprawki bezpieczeństwa, niezwłocznie po ich udostępnieniu.
- Należy upewnić się, że personel unika wątpliwych stron internetowych i wie, że nie może pobierać bezpłatnego oprogramowania/aplikacji, uruchamiać makr pakietu MS Office w załącznikach do emaili ani używać nośników pamięci USB z niezweryfikowanych źródeł.
- Należy rozważyć stosowanie białej listy aplikacji (blokowanie oprogramowania, które nie zostało autoryzowane).
- Należy stosować różne hasła dla różnych loginów używanych w firmie.

W przypadku podejrzenia, że firma padła ofiarą oszustwa, należy skontaktować się bezpośrednio z przedstawicielem HSBC.