12 października Dzień Bezpiecznego Komputera

Zagrożenia:

Zagrożeń związanych z komputerami jest wiele. Najbardziej narażone na niebezpieczeństwa są komputery, które pracują w sieci i mają dostęp do Internetu.

- Kradzież z włamaniem - w sieci działa wiele osób, które wykorzystując luki w oprogramowaniu uzyskują nielegalny dostęp do cudzych zasobów, uzyskane w ten sposób dane mają zapewnić im finansowe korzyści;
- Spam - elektroniczne wiadomości masowo rozsyłane do osób, które ich nie oczekują;
- Wirus - to najczęściej prosty program komputerowy, który w sposób celowy powiela się bez zgody użytkownika;
- Dialer - to program komputerowy do łączenia się z Internetem za pomocą modemu, jeśli działa bez wiedzy użytkownika może spowodować wielokrotne zwiększenie typowych kosztów dostępu do Internetu;
- Sniffing - skuteczna i trudna do wykrycia technika przechwytywania danych;
- Trojany i robaki - programy działające w ukryciu, ich zadaniem najczęściej jest przekazanie zdalnej kontroli nad systemem osobie nie posiadającej odpowiednich uprawnień.

Zasady bezpiecznego użytkowania komputera

1. Korzystaj z zapory połączenia internetowego
   - Należy uniemożliwić osobom z zewnątrz włamanie do sieci za pośrednictwem Internetu przez zainstalowanie sprzętowej zapory sieciowej oraz tzw. zapory programowej.
2. Pobieraj aktualizacje
   - Należy pobierać i instalować najnowsze aktualizacje oprogramowania. Osoby atakujące wyszukują i wykorzystują błędy i luki w popularnym oprogramowaniu, głównie dla emocji z tym związanych, dla zysku lub chęci spowodowania zamętu.
3. Korzystaj z oprogramowania antywirusowego
   - Należy zapobiegać infekcjom wirusami, instalując oprogramowanie antywirusowe i regularnie je aktualizując oraz używać wbudowanych funkcji zabezpieczeń programów pocztowych. Nie należy otwierać podejrzanych plików.
4. Używaj silnych haseł lub technologii silnego uwierzytelniania
   - Nie ułatwiaj hakerom dostępu do systemu przez używanie haseł, które łatwo odgadnąć lub złamać. Należy wybierać tzw. silne hasła i regularnie je zmieniać.
5. Przeglądaj sieć Web, zachowując środki ostrożności
   - Należy zadbać, aby przeglądanie sieci Web odbywało się w bezpieczny sposób. Strony sieci Web mogą zawierać programy. Te programy są na ogół nieszkodliwe i pożyteczne (np. animacje i menu wyskakujące), ale czasem zawierają wirusy.
6. Korzystaj z poczty e-mail w bezpieczny sposób
   - Poczta e-mail to najczęściej używana usługa internetowa i dlatego jest częstym obiektem ataków. Należy nauczyć się wykorzystywać jej zalety przy jednoczesnym ograniczeniu związanego z jej używaniem ryzyka.
7. Regularnie twórz kopie zapasowe i odtwarzaj dane
   - Tworzenie kopii zapasowych to ważny element zasad bezpieczeństwa. Należy je testować przez okresowe ich odtwarzanie, aby zagwarantować poprawne procedury.