Cyberbezpieczeństwo

Realizując zadania wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Powiatowy Urząd Pracy w Kole przekazuje informacje mające na celu zwiększenie świadomości w zakresie zagrożeń cyberbezpieczeństwa oraz wskazanie skutecznych sposobów ochrony przed tymi zagrożeniami.

Cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające:

- poufność,
- integralność,
- dostępność,
- autentyczność

przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Najczęstsze zagrożenia w cyberprzestrzeni:

1. **Phishing**

Phishing to atak polegający na podszywaniu się pod zaufany podmiot lub osobę, np. bank, kontrahenta, serwis płatniczy lub instytucję publiczną, w celu nakłonienia użytkownika do wykonania określonych czynności, takich jak:

- podanie danych logowania,
- kliknięcie w złośliwy link,
- otwarcie zainfekowanego załącznika.

Osoba atakowana jest często przekonana, że działa na polecenie legalnego i wiarygodnego podmiotu.

2. **Malware (złośliwe oprogramowanie)**

Malware to oprogramowanie stworzone w celu zakłócenia prawidłowego działania systemów informatycznych bez wiedzy użytkownika. Do tej kategorii zalicza się m.in.:

- wirusy,
- robaki,
- konie trojańskie,
- oprogramowanie szpiegujące.

Złośliwe oprogramowanie może służyć do:

- kradzieży danych (w tym danych osobowych),
- przejmowania haseł i środków finansowych,
- blokowania dostępu do urządzeń lub systemów.

3. **DDoS (Distributed Denial of Service)**

Atak DDoS polega na zmasowanym, jednoczesnym wysyłaniu fałszywych zapytań do danej usługi internetowej z wielu komputerów.

Skutkiem jest:

- przeciążenie systemu,
- spowolnienie działania,
- całkowita niedostępność usługi.

Celem ataku może być wyłudzenie danych lub odwrócenie uwagi od innego incydentu bezpieczeństwa.

4. Zasady bezpiecznego korzystania z cyberprzestrzeni

Aby zwiększyć poziom bezpieczeństwa, zaleca się w szczególności:

- stosowanie sprawdzonego oprogramowania antywirusowego i antyspyware,
- regularne aktualizowanie systemu operacyjnego, aplikacji oraz baz sygnatur wirusów,
- cykliczne skanowanie urządzeń oprogramowaniem zabezpieczającym,
- nieotwieranie plików i załączników z nieznanych źródeł,
- nieklikanie w linki zawarte w podejrzanych wiadomościach e-mail,
- niepodawanie danych osobowych w niesprawdzonych serwisach internetowych,
- szyfrowanie danych poufnych przesyłanych drogą elektroniczną,
- niepodłączanie do komputera nośników danych niewiadomego pochodzenia,
- stosowanie silnych haseł (co najmniej 8 znaków, wielkie i małe litery, cyfry, znaki specjalne),
- używanie różnych haseł do różnych usług,
- nieudostępnianie haseł osobom trzecim,
- regularną zmianę haseł,
- korzystanie z ustawień ochrony prywatności w przeglądarkach internetowych,
- unikanie publicznych sieci Wi-Fi, zwłaszcza podczas operacji finansowych,
- wykonywanie kopii zapasowych danych oraz ich szyfrowanie.

5. Gdzie szukać rzetelnych informacji o cyberbezpieczeństwie

Powiatowy Urząd Pracy w Kole zachęca do korzystania z materiałów publikowanych przez krajowe zespoły reagowania na incydenty bezpieczeństwa teleinformatycznego oraz instytucje zajmujące się cyberbezpieczeństwem:

- CSIRT GOV – https://csirt.gov.pl
- NASK – Cyberbezpieczeństwo – https://www.nask.pl/pl/dzialalnosc/cyberbezpieczenstwo
- CERT Polska – publikacje – https://www.cert.pl/publikacje/
- CERT Polska – kampania „OUCH!” – https://www.cert.pl/ouch/