Złośliwe oprogramowanie – ransomware

Złośliwe oprogramowanie może powodować przejęcie kontroli nad urządzeniem, kradzież danych, haseł lub plików. Przestępcy wykorzystują je, by żądać pieniędzy w zamian za zlikwidowanie blokady, odszyfrowanie danych lub obietnicę nieupubliczniania wykradzionych informacji.

Jak dochodzi do infekcji urządzenia?

- Zainfekowane pliki
- Fałszywe strony internetowe
- Słabe hasła, brak dodatkowych zabezpieczeń
- Nieaktualizowane systemy i aplikacje

Co zrobić, gdy Twoja organizacja padła ofiarą ataku typu ransomware?

1. **ODŁĄCZ URZĄDZENIE OD INTERNETU I INNYCH POŁĄCZEŃ SIECIOWYCH** (np. sieci Wi-Fi) – zapobiega to dalszemu rozprzestrzenieniu się szkodliwego oprogramowania.
2. **ZGŁOŚ INCYDENT DO WYZNACZONYCH OSÓB** – każda instytucja powinna mieć osobę lub zespół zajmujący się incydentami oraz określoną procedurę reagowania w przypadku tego typu zagrożenia.
3. **POSTĘPUJ WEDŁUG WYTYCZNYCH W SWOJEJ ORGANIZACJI** – po zgłoszeniu incydentu postępuj zgodnie z zaleceniami specjalistów, którzy zajmą się urządzeniem firmowym.
4. **JEŚLI PLIKI ZOSTAŁY ZASZYFROWANE I NASTĄPI ŻĄDANIE OKUPU, ZRÓB ZDJĘCIE LUB ZRZUT EKRANU KOMUNIKATU, KTÓRY POJAWIŁ SIĘ NA URZĄDZENIU** – może to pomóc specjalistom w łatwiejszej identyfikacji ataku.
5. **NIE PŁAĆ OKUPU!** – przekazując pieniądze, nie masz pewności, że odzyskasz swoje dane lub, że nie zostaną upublicznione.

Zapoznaj się ze stroną nomoreransom.org, na której znajdziesz więcej informacji na temat ataków typu ransomware.

NASK
EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA
PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTRA CYFRYZACJI