Cyberbezpieczeństwo

Trendy, których nie zawsze zauważamy, a powinniśmy

Co warto zauważyć

- Działalność **najgroźniejszych grup APT** staje się zagrożeniem dla praktycznie każdej organizacji, a nie tylko infrastruktury krytycznej czy celów „państwowych”
- Zaczynamy przegrywać pojedynek w walce o prawidłowe zrozumienie czym jest **„zero-trust”**
- Nie zauważamy, że nie tylko my jesteśmy zachwyceni możliwościami **ChatGPT**

APT

- Cyberoperacje powiązane z wojną w Ukrainie zaburzyły modele atrybucji cyberataków
- Migracja technik i aktorów pomiędzy światami „state-sponsored” i „cybercriminals”
- Narzędzia GRU, FSB czy US Cyber Command w sieciach SME

Błędy w pojmowaniu ZERO TRUST

- Model Zero Trust oznacza brak zaufania do pracowników
- Model Zero Trust jest tylko dla dużych firm
- Model Zero Trust jest jednorazowym projektem
- Model Zero Trust jest zbyt drogi i skomplikowany
- Model Zero Trust wystarczy do zapewnienia pełnego bezpieczeństwa

AI (ChatGPT)

- Generowanie złośliwego kodu – przede wszystkim infostealers
- Generowanie treści oszukańczych
- „AI hallucinations” katalizuje problem asymetryczności pomiędzy atakującym a broniącym się