UPRZEJMY : CYBER ATAK CEL: WSZYSTKO	Arkusz refleksyjny RANSOMWARE – NIEDOSTĘPNOŚĆ OGROMNE STANOWISKA ROBOCZE	

1. Alarm

NIE RÓB	DO
NIE USUWAJ NIC : wszystkie informacje zostaną wykorzystane jako dowód w dochodzeniu	ZAalarmuj CENTRUM OPERACYJNE BEZPIECZEŃSTWA (SOC) ORAZ MENEDŻER BEZPIECZEŃSTWA SYSTEM INFORMACYJNY
NIE OTWIERAJ PLIKÓW LUB ZASZYFROWANYCH APLIKACJI: należy zatrzymać infekcję	UDOSTĘPNIJ WSZYSTKIE INFORMACJE SOC, aby to zrobić ocenić skalę ataku i priorytety reagowania kryzysowego
	PRZESTRZEGAJ INSTRUKCJI SOC

2. Działania awaryjne

1. Izoluj systemy krytyczne :
   - Odłącz wszystkie sieci
   - Odłącz kabel sieciowy od komputerów
   - Rozłącz połączenia Wi-Fi
2. Odłącz wszystkie urządzenia peryferyjne
3. Oceń zakres kompromisu i zbierz dowody

3. Rozwiązanie zapewniające ciągłość

Udostępnienie zwirtualizowanego środowiska pracy dostępnego z Internetu za pośrednictwem dowolnej stacji roboczej w kolejności ważności działań

4. Kryteria aktywacji Planu Ciągłości Działania

Ostateczną decyzję dotyczącą działań podejmuje jednostka kryzysowa podejmująca decyzje, czyli PCA
Kryterium 1: 5% stacji roboczych nie nadaje się do użytku
Kryterium 2: ryzyko rozprzestrzenienia się oprogramowania ransomware na inne witryny/podmioty/aplikacje