Tomasz Widomski
Członek Rady Nadzorczej
ELPROMA Elektronika sp. z o.o.

„Analiza zjawiska desynchronizacji czasu jako nowej cyberbroni destabilizującej infrastruktury krytyczne państwa"

Czy czasem UTC w systemach IT/OT można manipulować? Czy uprawnieni jesteśmy do stwierdzenia, że desynchronizacja to nowy rodzaj współczesnego cyber-zagrożenia dla coraz silniej automatyzującej się, zbyt silnie zależnej od GPS nowoczesnej gospodarki państwa?

Czy zamiast włamywać się do dobrze zabezpieczonych kryptograficznie sieci TCP/IP (często nawet tych całkowicie odizolowanych od Internetu) nie prościej jest destabilizować sieć pośrednio desynchronizacją? Czy obecne ataki zakłócania GPS nad Polską są w istocie atakiem, a może ma to na celu przyzwyczajenie nas do problemu, abyśmy nie zareagowali, gdy przyjdzie pora.

Desynchronizacja, to inaczej mówiąc proces rozsynchronizowania zegarów. Nie jest to jednak rozprawa na temat zegarów sprzętowych, ani wyświetlaczy informacyjnych. To dyskusja nad mechanizmami dostępnych dziś technik manipulacji zegarami programowymi reprezentowanymi kodem programu we wnętrzu systemów operacyjnych Windows, Linux i Unix. Dyskusja nad niedoskonałością istniejących rozwiązań w IT/OT – tych związanych z synchronizacją i ryzykiem, jakie niesie desynchronizacja nawet rozwiązań, które do tej pory nie wykazały żadnych cech niestabilności i podatności na ataki. Autor definiuje dwa nowe rodzaje cyber-ataków dla każdej współczesnej infrastruktury krytycznej zdefiniowanej w dyrektywie NIS-2:

- Time Synchronization Attack (TSA - atak na czas)
- Time Delay Attack (TDA - atak na opóźnienia w sieci)

i wykazuje, że czasem UTC i jego synchronizacją, w tym sygnałami satelitarnymi GPS można manipulować, odnosząc pośrednio większą skuteczność ataku niż cyber-atakiem bezpośrednim.