WODOCIĄGI MIEJSKIE W RADOMIU Sp. z o.o.
ul. Filtrowa 4, 26-600 Radom, e-mail: woda@woda.radom.pl, www.woda.radom.pl

Radom, dn. 01.04.2021r.

PYTANIA I ODPOWIEDZI z dn. 01.04.2021r.

Dot. „Zakup rozwiązania UTM klasy Next generation Firewall z pełną ochroną sieci: informatycznej i przemysłowej – Implementacja: maszyna wirtualna”
nr sprawy: DZ/27/2021

Zamawiający, Wodociągi Miejskie w Radomiu Sp. z o.o. działając w trybie § 38 ust. 1 Regulaminu Udzielania Zamówień Sektorowych przez Wodociągi Miejskie w Radomiu Sp. z o.o. z dn. 18.09.2017r. odpowiada na pytanie zadane przez jednego z Wykonawców.

Pytanie 1

Prosimy Zamawiającego o doprecyzowanie czy ochrona protokołów przemysłowych opisana w punkt 10. Ochrona przed atakami podpunkt. 8. Ochrona protokołów przemysłowych, takich jak minimum:
• BACnet/IP,
• IEC-60870.5.104,
• Modbus,
• OPC,
• PROFINET,
• Siemens S7,
• EtherNet/IP.
ma polegać na przeprowadzaniu głębokiej analizy pakietów (tzw. DPI) dla wymienionych protokołów?

Aktualny zapis może dopuszczać rozwiązania, których mechanizmy ochrony oparte są tylko na sygnaturach ataków typowych dla wymienionych protokołów przemysłowych, umożliwiając ataki na infrastrukturę przemysłową Zamawiającego przy wykorzystaniu m.in.:
1. Nieznanych jeszcze podatności dla używanych protokołów przemysłowych, które mogą zostać wykorzystane do bardziej zaawansowanego ataku na infrastrukturę przemysłową.
2. Wstrzyknięcia zmodyfikowanych pakietów do komunikacji w nieszyfrowanych protokołach przemysłowych, a w następstwie zmianę pracy (zachowania) sterowników PLC.
3. Użycia zmodyfikowanych komend w obrębie poszczególnych protokołów przemysłowych, które mogą zakłócić pracę systemów automatyki przemysłowej.
4. Ataku typu DoS (Denial of Service), który może spowodować niedostępność danego elementu lub grupy elementów automatyki przemysłowej i w konsekwencji zatrzymać proces przemysłowy.

Odpowiedź 1

Aktualny zapis może dopuszczać rozwiązania, których mechanizmy ochrony oparte są tylko na sygnaturach ataków typowych dla wymienionych protokołów przemysłowych, umożliwiając ataki na infrastrukturę przemysłową Zamawiającego przy wykorzystaniu m.in.:

1. Nieznanych jeszcze podatności dla używanych protokołów przemysłowych, które mogą zostać wykorzystane do bardziej zaawansowanego ataku na infrastrukturę przemysłową.

2. Wstrzyknięcie zmodyfikowanych pakietów do komunikacji w nieszyfrowanych protokołach przemysłowych, a w następstwie zmienić pracę (zachowanie) sterowników PLC.

3. Użycie zmodyfikowanych komend w obrębie poszczególnych protokołów przemysłowych, które

mogą zakłócić pracę systemów automatyki przemysłowej.

4. Atak typu DoS (Denial of Service), który może spowodować niedostępność danego elementu lub grupy elementów automatyki przemysłowej i w konsekwencji zatrzymać proces przemysłowy.

Zamawiający doprecyzowuje:
Ochrona protokołów przemysłowych, takich jak minimum:
• BACnet/IP,
• IEC-60870.5.104,
• Modbus,
• OPC,
• PROFINET,
• Siemens S7,
• EtherNet/IP.
ma polegać na przeprowadzaniu głębokiej analizy pakietów (tzw. DPI).