**Hakerzy testują nasze wodociągi**

**Zmiana ciśnienia w rurach, przejęcie PIN-ów i transmisja ataku w rosyjskich mediach społecznościowych. Ostatnie cyberataki na wodociągi nie pozostawiają złudzeń. Chodzi o to, by pokazać, że nie jesteśmy bezpieczni – ostrzegają eksperci z Łukasiewicz – Poznańskiego Instytutu Technologicznego. Jak przedsiębiorstwa wodno-kanalizacyjne mogą się przed nimi bronić? Czy nie zabraknie nam wody w kranach?**

- Tego problemu nikt wcześniej nie zauważał. Jednak wysyp prób, z jakimi mamy ostatnio do czynienia, pokazuje, że jest on poważny. I że będzie jeszcze gorzej – diagnozuje dr inż. Maciej Niemir, który na co dzień zajmuje się sztuczną inteligencją i cyberbezpieczeństwem.

O jakie cyberataki chodzi? Na przykład na stacje uzdatniania wody (w lutym tego roku w Tolkmicku, Małdytach i Sierakowie, w maju w Szczytnie) czy oczyszczalnie ścieków (w Wydminach i Kuźnicy w 2024 roku) czy też sierpniowy atak, który pozbawiłby mieszkańców jednego z dużych miast wody. Było ich więcej, ale nie o wszystkich informacje podawano do publicznej wiadomości.

Jak wyglądał lutowy atak? Wiemy to z nagrania udostępnionego przez rosyjskich hakerów na kanale w Telegramie. Ustawili oni do maksymalnych wartości wszystkie parametry – np. ciśnienie, objętość przefiltrowanej wody na filtr czy czas sedymentacji. Zmienili też dostępowe PIN-y do urządzeń.

Jak ocenił CERT Polska, atak był możliwy przez błędną konfigurację urządzenia dostępnego z internetu. Nie spowodował jednak żadnych skutków dla środowiska i ludzi.

- Widzimy, że na razie ktoś to robi dla zabawy, testowo, dla zbudowania reputacji grupy przestępczej – mówi dr inż. Maciej Niemir. – Ale za tym kryje się też przekaz: nie jesteście bezpieczni. Przestępcy włamują się do łatwiejszych miejsc na zasadach treningowych. Potem możemy się spodziewać gorszych, celowanych ataków – dodaje.

**Koniec zabawy?**

- Widzimy, że hakerzy uznali przedsiębiorstwa wodno-kanalizacyjne za łatwy cel. Tutaj często nikt ataku nawet nie zauważy i nie zgłosi. Cyberprzestępcy sondują, czy łatwiej jest zakłócić pracę np. 70 proc. małych wodociągów, czy jednego dużego. Skutki mogą być podobne – zauważa Włodzimierz Woźniak, ekspert od AI i cyberbezpieczeństwa z Łukasiewicz – Poznańskiego Instytutu Technologicznego.

Wspomnianym efektem może być brak wody lub zmiana jej parametrów (np. za dużo chloru), przez co będzie szkodliwa dla zdrowia.

Wodociągi należą do infrastruktury krytycznej, co oznacza, że muszą być szczególnie chronione, także przed cyberatakami. Ochrona wymaga jednak nakładów finansowych, a wielu przedsiębiorstw na nią nie stać. Są jednak trzy rzeczy, które każde przedsiębiorstwo może wprowadzić szybko i bez większych kosztów, mówią badacze z Łukasiewicz – PIT.

Po pierwsze, **zinwentaryzować wszystkie urządzenia** pod kątem tego, w jakim miejscu jest do nich dostęp i w jaki sposób można się do nich włamać.

Po drugie, **wprowadzić segmentację sieci**, czyli oddzielić sieć biurową od tej, która ma dostęp do urządzeń. Włamania często są wynikiem nieuwagi lub braku wiedzy (np. otworzą załącznik, klikną w link). Jeśli funkcjonują np. dwie osobne sieci, szkody związane z cyberatakiem powstaną tylko w jednej.

Po trzecie, **przygotować scenariusze na sytuacje kryzysowe** (tzw. „what if”). Pozwoli to szybciej i sprawniej reagować, jeśli takie wystąpią.

**AI wkroczyła do gry**

Sztuczna inteligencja dała nowe możliwości cyberprzestępcom (np. prowadzenia bardziej spersonalizowanych ataków) i specjalistom od cyberbezpieczeństwa (np. wykrywanie podejrzanych aktywności).

- Niepokojące są wyniki badań Carnegie Mellon University we współpracy z firmą Anthropic, które wykazały, że w środowisku symulowanym sztuczna inteligencja potrafi samodzielnie przeprowadzić wieloetapowy cyberatak. W dziewięciu na dziesięć prób udało się jej osiągnąć przynajmniej częściowy sukces, a w połowie scenariuszy – pełny. – To tylko kwestia czasu, aż podobne techniki zostaną wykorzystane w realnych systemach – ocenia Włodzimierz Woźniak.

W Polsce działa ok. 1900 przedsiębiorstw wodno-kanalizacyjnych, sieć zarządzana przez te podmioty ma ponad 515 tys. km długości.