Błędy w konfiguracji skrzynek e-mail a cyberataki – rekomendacje Prezesa UTK

13.03.2024

Prezes Urzędu Transportu Kolejowego (UTK) obserwuje wzrost liczby fałszywych wiadomości e-mail. Wykorzystują one nieprawidłowo zabezpieczone domeny internetowe m.in. podmiotów kolejowych.

Analiza domen internetowych podmiotów kolejowych, dostawców (zakłady naprawcze, dostawcy części), a także mediów branżowych wskazuje, że zdecydowana większość nie jest prawidłowo skonfigurowana. Pozwala to cyberprzestępcom w prosty sposób sfałszować informacje o nadawcy. Mogą się oni podszyć pod dowolnego nadawcę z domeny zaatakowanego podmiotu. Tego typu wiadomości, wykorzystując wizerunek i zaufanie do podmiotu kolejowego, pozwalają zaatakować odbiorcę i zainstalować złośliwe oprogramowanie lub wykraść hasła.

CERT Polska zaleca wykonanie przez administratora czynności, które zminimalizują ryzyko podszycia się cyberprzestępców pod podmiot kolejowy.

Wielu administratorów IT, pomimo prawidłowej konfiguracji, wybiera komfortowe, ale szkodliwe rozwiązanie – wiadomości e-mail, które są negatywnie zweryfikowane, nie są odrzucane (ustawienie w polityce DMARC parametru „none” zamiast „quarantine” lub „reject”). W efekcie przestępcy nadal mają możliwość podszycia się pod zaatakowany podmiot.

REKOMENDACJE PREZESA UTK

Prezes UTK zaleca niezwłoczną weryfikację domeny za pomocą narzędzia przygotowanego przez CERT Polska i dostępnego pod adresem https://bezpiecznapoczta.cert.pl. Kompleksowe zastosowanie wskazanych na stronie CERT Polska czynności konfiguracyjnych mechanizmów SPF, DKIM oraz DMARC zabezpiecza domenę przed nieuprawnionym wykorzystaniem.

Prezes UTK zaleca także niezwłoczne uruchomienie mechanizmów dwuetapowego uwierzytelnienia do poczty elektronicznej oraz innych systemów, które są dostępne z Internetu.