Úprava konfigurace kryptografických prostředků ISZR

Seznam cipher suites, které budou povoleny na vnějším rozhraní ISZR po provedení změn:

ID	SUITE	BITS	PROT METHOD CIPHER	MAC	KEYX
47	AES128-SHA	128	TLS1.2 Native AES	SHA	RSA
53	AES256-SHA	256	TLS1.2 Native AES	SHA	RSA
60	AES128-SHA256	128	TLS1.2 Native AES	SHA	256 RSA
61	AES256-SHA256	256	TLS1.2 Native AES	SHA	256 RSA

Ověření přístupu z ISZR po provedení změn:

- Zkontrolujte, zda váš AIS má povoleny protokoly TLS 1.0 a 1.1 pro komunikaci s ISZR v testovacím prostředí.
    - Jestliže ano, pak protokoly TLS 1.0 a 1.1 ve vašem AIS pro komunikaci s ISZR vypněte pro testovací prostředí.
- Zkontrolujte, zda váš AIS má pro komunikaci s ISZR v povolen protokol TLS 1.2 pro testovací prostředí.
    - Jestliže ne, pak ve vašem AIS povolte pro komunikaci s ISZR v testovacím prostředí TLS 1.2.
- Zkontrolujte, zda váš AIS má pro komunikaci s ISZR pro testovací prostředí povolenu alespoň jednu cipher suite z výše uvedeného seznamu.
    - Jestliže ne, pak ve vašem AIS povolte pro komunikaci s ISZR v testovacím prostředí alespoň jednu cipher suite z výše uvedeného seznamu.
- V období od 1. 8. 2017 do 1. 8. 2018 otestujte v testovacím prostředí, že váš AIS bezproblémově komunikuje s ISZR i s takto změněným nastavením kryptografických protokolů.
- Předpokládané datum provedení analogické změny v produkčním prostředí vašeho AIS je 1. 8. 2018