**ПРИЛОГ 1**

**САДРЖАЈ ПРОЦЕНЕ РИЗИКА ОД СТРАНЕ ОПЕРАТОРА 5G МРЕЖЕ**

Основни елементи процене ризика од стране оператора 5G мреже обухватају:

**1. Процена осетљивости кључних компоненти 5G мреже и њихова категоризација**

Оператори могу да идентификују и додатне елементе и функције које представљају кључне компоненте 5G мреже у односу на списак који је дат у оквиру члана 5. став. 1 ове уредбе.

Сваки идентификовани елемент и функција у оквиру кључних компоненти 5G мреже треба да се процени са аспекта безбедносног ризика који се односи на доступност мрежних функција (како би се осигурао континуираног рада мреже), поверљивост информација (како би се заштитиле осетљиве информације), сигурност (заштита од неовлашћених приступа) и отпорност 5G мреже (способност опоравка од инцидената).

Категоризација осетљивости сваког елемента и функције у оквиру кључних компоненти 5G мреже на основу степена утицаја треба да обухвати следеће нивое осетљивости:

* + Критичан: Ова категорија обухвата елементе и функције чије компромитовање може изазвати:
    - Знатан прекид у раду 5G мреже који погађа велики број корисника;
    - Утицај на велики број базних станица или целокупне регионалне мреже;
    - Компромитовање поверљивих информација високог степена значаја.
  + Висок: Ова категорија укључује елементе и функције чије компромитовање може:
    - Значајно умањити функционалност појединачних сервиса или мреже у специфичним областима;
    - Утицати на осетљиве информације које су важне, али не критичне;
    - Захтевати брзу интервенцију ради ублажавања последица, али без дуготрајног утицаја на мрежу у целини.
  + Умерен: Ова категорија укључује елементе и функције чије компромитовање има:
    - Локализован и ограничен утицај на мањи број корисника или базних станица;
    - Минималан или привремен утицај на поверљивост или доступност информација.

За одређивање степена осетљивости користи се матрица ризика која укршта два кључна фактора:

* + - Вероватноћа претње (ниска, средња, висока);
    - Последице у случају компромитовања: (ниске, умерене, критичне).

**2. Идентификацију претњи и анализа рањивости везаних за кључне компоненте 5G мреже**

Оператори треба да идентификују све потенцијалне претње које могу утицати на кључне компоненте 5G мреже. Ове претње најчешће укључују:

* Сајбер претње као што су DDoS напади, неовлашћени приступ или манипулација подацима;
* Физичке претње као што су природне катастрофе, вандализам или намерно оштећење инфраструктуре које могу нарушити стабилност мреже;
* Унутрашње претње које потичу од запослених, трећих лица или партнера, укључујући могуће злоупотребе или немар;
* Претње повезане са добављачима које произилазе из процене ризика добављача у складу са тачком 3. овог прилога;
* Претње из ланца снабдевања односе се на претње које настају током различитих фаза набавке, производње, транспорта и интеграције компоненти у мрежу.

Анализа рањивости треба да идентификује све слабости у мрежи које могу бити искоришћене од стране идентификованих претњи које могу укључивати:

* техничке рањивости које могу произилазити из неажурних или застарелих софтверских пакета, неефикасног шифровања или слабих алгоритама, слабих механизама аутентификације и сл.;
* оперативне рањивости које могу да настану услед недостатка процедура за управљање инцидентима, лоше конфигурације система, недостатка обуке особља и сл.;
* организационе рањивости које произлазе из неуспелог спровођења безбедносних политика, лоше дефинисаних процеса итд.

Све идентификоване претње треба да буду систематизоване према њиховој вероватноћи настанка и могућем утицају на функционисање 5G мреже.

Вероватноћа настанка претње може бити класификована као ниска вероватноћа (ретки случајеви), средња вероватноћа (могуће, али не уобичајено) или висока вероватноћа (веома вероватно) узимајући у обзир факторе као што су историјски подаци о сличним претњама, ефикасност постојећих безбедносних мера и сл.

Процена потенцијалног утицаја на функционисање 5G мреже се врши узимајући у обзир како идентификована претња може утицати на доступност мрежних функција, поверљивост информација, сигурност и отпорност 5G мреже, а процене се класификују да имају ниски утицај (локализоване и брзо решиве последице), средњи утицај (делимично угрожавање кључних функција) или високи утицај (велике и дуготрајне последице које угрожавају интегритет целе мреже).

За систематизовање претњи користи се матрица ризика која укршта два кључна фактора:

* + - Вероватноћа настанка (ниска, средња, висока);
    - Утицај на функционисање 5G мреже (низак, средњи, висок).

**3. Процена ризика добављача 5G опреме, укључујући и процену ризика добављача услуга управљања мрежом**

Процене ризика добављача 5G опреме која припада некој од кључних компоненти 5G мреже, укључујући и процену ризика добављача услуга управљања мрежом треба да садржи:

a) Идентификацију добављача:

Направити списак свих постојећих добављача кључних компоненти 5G мреже и добављача услуга управљања мрежом, као и добављача од којих се планира набавка опреме и/или услуга за кључне компоненте 5G мреже у наредне две године, који укључују:

* + Тип опреме или услуге коју добављач пружа;
  + Локације на којима се користи опрема или услуга датог добављача.

б) Процену безбедносног профила добављача:

* + Испитати безбедносне политике добављача, укључујући мере заштите података, контроле приступа и процедуре за одговор на инциденте;
  + Проценити транспарентност добављача у вези са пореклом компоненти и софтвера који се користе у 5G мрежи;
  + Проверити компатибилност са националним и европским безбедносним стандардима (нпр. ISO 27001);
  + Описати историјат безбедносних инцидената у које је добављач укључен уколико постоји;
  + Историја претњи или рањивости у испорученој опреми или услугама;
  + Оценити спремност на сарадњу у области информационе безбедности.

в) Техничку процену опреме и услуга

* + Спровести техничко тестирање опреме и софтвера на потенцијалне рањивости, укључујући анализу кода и проверу могућих „задњих врата“ (backdoors) или
  + Проценити усклађеност са међународним техничким стандардима и примену најбољих пракси у дизајну и развоју.

**4. Диверзификација добављача**

Проценити зависност од добављача за сваку од кључних компоненти 5G мреже на основу параметара као што су број различитих добављача за исте елементе и функције које припадају кључним компонентама 5G мреже и географска и технолошка разноврсност.

**5. Предложене мере за елиминисање или ублажавање идентификованих претњи, рањивости и ризика**

На основу идентификованих претњи, рањивости и процене ризика, оператори 5G мреже предлажу мере које укључују али се не ограничавају на:

* + Техничке мере које се односе на употребу шифровања, ограничење приступа, сегментацију мреже и мултифакторску аутентификацију, редовна ажурирања софтвера, успостављање система за праћење активности добављача у реалном времену, уз логовање свих приступа;
  + Организационе мере укључујући обуку особља, процедуре за управљање инцидентима итд.;
  + Укључивање безбедносних клаузула у уговоре са добављачима, укључујући извештавање о безбедносним мерама и инцидентима, пружање подршке у случају инцидената и сл.;
  + Мере које се односе на диверзификацију добављача и с тим у вези имплементацију стандарда који омогућавају интероперабилност различитих решења.

За све предложене мере оператори достављају и план за спровођење.

Поред наведеног оператори могу користити и стандардизоване методологије као што су NIST SP 800-30 и/или ISO/IEC 27005 за идентификовање претњи, анализу рањивости, утврђивање ризика и предлог одговарајућих мера за њихово елиминисање или ублажавање.

Сви подаци и анализе који се користе у процени ризика морају бити образложени и документовани.