ПРЕДЛОЖЕНИЕ

Съгласно член 116, параграф 6 от Акта за електронните съобщения (UL RS № 130/22 и 18/23 — ZDU-1O), Агенцията за комуникационни мрежи и услуги на Република Словения, като взе предвид процедурата за предоставяне на информация в съответствие с Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г. установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (OB L 241, 17.9.2015 г., стр. 1), издава следния

ОБЩ АКТ
за допълнителни изисквания и ограничения във връзка със сигурността

Член 1
(Съдържание на общия акт)

С настоящия общ акт се предвиждат:

1. насоки, които следва да се изпълняват от операторите на мобилни съобщителни мрежи (наричани по-нататък „оператори“), които предоставят тези мрежи на критични субекти, които са управители на критична инфраструктура в други области на регламентиране на критичната инфраструктура, както е посочено в закона за регламентиране на областта на критичната инфраструктура (наричани по-нататък „управители на критична инфраструктура“), доставчиците на основни услуги, както е определено в закона за регламентиране на информационната сигурност (наричани по-нататък „доставчици на основни услуги“), органите на държавната администрация, както е определено в закона за регламентиране на информационната сигурност (наричани по-нататък „органи на държавната администрация“), или носителите на ключови части от системата за сигурност на държавата; и
2. критичните елементи на мрежата и свързаните информационни системи с техните функционалности, посочени в член 116, параграф 6 от Акта за електронните съобщения (UL RS № 130/22 и № 18/23 — ZDU-1O; наричан по-нататък „Актът“), както е посочено в приложението, което представлява неразделна част от настоящия общ акт и е изготвено в сътрудничество с органа, отговарящ за информационната сигурност.

Член 2
(Значение на понятията)

(1) Понятията, използвани в настоящия общ акт, означават:

1. верига за доставки е цялата система от процеси, лица, организация и разпространение, които са част от проектирането, производството, съхранението, разпространението и доставянето, както и при монтирането и поддръжката на компоненти на критичните мрежови елементи, монтирани в мрежата на оператора или при доставчика на услуги „в облак“, който предоставя такива услуги на оператора.

2. Критичните елементи на мрежата са тези мрежови елементи, функции, услуги и информационни системи за поддръжка във физическа, софтуерна или виртуализирана форма при оператора или при доставчика на услуги „в облак“, както е изброено в приложението към настоящия общ акт.

3. Критичните субекти са управителите на критична инфраструктура в други области на регламентиране на критичната инфраструктура, определени в съответствие със закона за регламентиране на областта на критичната инфраструктура, доставчиците на основни услуги, определени със закона за регламентиране на информационната сигурност, органите на държавната администрация, определени със закона за регламентиране на информационната сигурност, и носителите на ключови части от системата за сигурност на държавата.

(2) Другите понятия, използвани в настоящия общ акт, имат същото значение, както е определено в Акта и Общия акт за сигурността на мрежите, услугите и данните.

Член 3
(Общи насоки)

(1) Операторите във веригата за доставки на компоненти на критични мрежови елементи и услуги за трето ниво на поддръжка за тези компоненти следва да вземат предвид най-малко следните насоки през целия жизнен цикъл на тези компоненти:

1. за отделен производител или доставчик и за доставчик на услуги за трето ниво на поддръжка в резултат на взаимоотношения и споразумения с тях, те извършват оценка на риска по отношение на доставките и потенциалните въздействия от страна на трети физически или юридически лица съгласно публичното или частното право (наричани по-нататък „трети страни“), на съвместимостта с оборудването от други производители, качеството и безопасността на продуктите, както и потенциалните отрицателни въздействия върху изпълнението на услугите на оператора и критичните субекти;
2. че сигурността е вградена и изпълнена още при проектирането и че договорите включват крайни срокове за отстраняването на забелязани уязвимости;
3. че основните характеристики във връзка със сигурността (наличност, поверителност, цялост и автентичност) се гарантират през целия жизнен цикъл на тяхното използване;
4. че сигурността и техните непрекъснати доставки са гарантирани и е потвърдено, че с тях се поддържат основни характеристики във връзка със сигурността с високо качество в съответствие с международно признатите стандарти (3GPP) и европейските технически стандарти (ETSI);
5. че насоките, посочени в точки 2—4 от настоящия параграф, могат да бъдат проверени в договорната документация с производителя или с доставчика;
6. за всеки производител или доставчик, рисковете, свързани с правата за използване на ключовите технологии, които са необходими за производството и използването на оборудването, както и рисковете, свързани с доставката на оборудване, резервни части или услуги за трето ниво на поддръжка, също така се оценяват и вземат предвид;

7. че използваните компоненти нямат некоригирани известни критични или активно експлоатирани уязвимости;
8. да се избягва обвързването със само един производител или доставчик, когато това е технически осъществимо и икономически устойчиво, с цел намаляване на зависимостта и повишаване на устойчивостта в случай на уязвимост на критични компоненти, катастрофална повреда на мрежата или заплаха за сигурността на мрежите и услугите на критични субекти от страна на трети физически или юридически лица, регламентирани с публичното или частното право.

(2) При доставката на информационно и комуникационно оборудване, системи и услуги, операторите изпълняват изцяло насоките на Агенцията на Европейския съюз за киберсигурност (наричана по-нататък „ENISA“) и валидните разпоредби на Европейския съюз относно основните изисквания във връзка със сигурността при възлагането на обществени поръчки за сигурни ИКТ продукти и услуги. Агенцията публикува на своя уебсайт връзки към текущи документи на ENISA и разпоредби на ЕС в горепосочената област и редовно ги актуализира.

(3) При доставката на компоненти на критични мрежови елементи или използването на услуги „в облак“, дава се приоритет във връзка с избора на компоненти от тези производители, доставчици или услуги от доставчици на услуги „в облак“, които са сертифицирани от акредитирани органи за оценяване на съответствието и, ако е необходимо, с разрешение въз основа на член 60, параграф 3 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (наричан по-нататък „Регламентът“) за издаването на европейски сертификати за киберсигурност на определено ниво на увереност, както е определено с член 52 от Регламента.

(4) За целите на предходния параграф, операторът проверява специален уебсайт, създаден от ENISA в съответствие с член 55 от Регламента, предназначен да предоставя информация на обществеността относно европейските схеми за сертифициране на киберсигурността, европейските сертификати за киберсигурност и ЕС декларациите за съответствие, включително информация във връзка с европейските схеми за сертифициране на киберсигурността, които вече не са в сила, оттеглените и с изтекъл срок на действие европейски сертификати за киберсигурност и ЕС декларации за съответствие, както и хранилището на връзки към информацията за киберсигурността.

Член 4
(Оценка на риска)

(1) При определянето на риска, свързан с производителя или доставчика на компоненти и доставчика на услуги за трето ниво за критични елементи на мрежата, операторът взема предвид следните аспекти на риска, които оценява.

(2) При оценката, посочена в предходния параграф, операторът оценява и взема предвид най-малко:

1. общото качество (включително аспектите на безопасността) и надеждността;
2. степента на използване на отворени стандарти и интерфейси, които предотвратяват зависимостта и обвързването с продуктите на конкретен производител или доставчик;
3. съответствието с признатите международни и европейски технически стандарти (3GPP, ETSI) и разпоредбите на Европейския съюз, както и настройките за сигурност по подразбиране в съответствие с професионалните препоръки (GSMA — сдружение на операторите на мобилни мрежи);
4. степента на съвместимост с оборудването и мрежовите функции на трети страни;
5. способността да се предоставят актуализации и персонализации;
6. процеса на управление на уязвимостите, тяхното разкриване и наличието на съвременен процес за актуализации и корекции;
7. наличността и прозрачността на документацията относно:
   - ключовите функции и информацията за сигурността и други характеристики на компонента и възможните настройки, както и
   - използвания софтуер, включително такъв с отворен код (Опис на материалите — SBOM);
8. степента на зависимост от услуги за трето ниво на поддръжка при управлението и поддръжката на оборудването, ако операторът не извършва тези услуги самостоятелно със своите служители;
9. предварителната оценка на съответствието на оборудването или даден субект, който би предоставял услуга за трето ниво на поддръжка от страна на органи, акредитирани в Европейския съюз съгласно европейските схеми за сертифициране на киберсигурността, като акредитираните органи се публикуват в Официален вестник на Европейския съюз.

(3) Операторът документира рисковите фактори и резултатите от оценката на риска за всеки избран производител, доставчик или доставчик на услуги за трето ниво на поддръжка, посочени в параграфи 2 и 3 от настоящия член, както и редовно актуализира това.

Член 5
(Общи насоки относно експлоатацията на критични мрежови елементи)

(1) Компонентите на критичните мрежови елементи, техните експлоатация и настройки по подразбиране не следва да съдържат технически характеристики, които биха могли да окажат отрицателно въздействие върху сигурността или функционирането на критичните субекти, наред с другото поради саботаж, шпионаж, кражба на интелектуална собственост или тероризъм.

(2) Критичните мрежови елементи обикновено се намират в Република Словения или, като се вземат предвид всички рискове за сигурността и се гарантира висока степен на мерките за сигурност, и, ако не е предвидено друго в приложимите разпоредби, в Европейския съюз. Операторът информира Агенцията за комуникационни мрежи и услуги на Република Словения (наричана по-нататък „Агенцията“) и органа, отговарящ за информационната сигурност, за тяхното планирано преместване най-малко 30 дни преди преместването извън Европейския съюз.

(3) Услугите за трето ниво на поддръжка за критични елементи на мрежата обикновено се извършват в Република Словения или, като се вземат предвид всички рискове за сигурността и се гарантира висока степен на мерките за сигурност, и, ако не е предвидено друго в приложимите разпоредби, в Европейския съюз. Операторът уведомява Агенцията и органа, отговарящ за информационната сигурност, за планираното преместване на своите услуги за трето ниво на поддръжка най-малко 30 дни преди преместването извън държавите от Европейския съюз.

(4) Изпълнението на услуги за трето ниво на поддръжка не застрашава сигурността или изпълнението на услугите на критичните субекти или националната сигурност.

(5) Операторът установява и редовно прилага процеса на идентифициране на критичните мрежови елементи. Това трябва да се извършва най-малко веднъж годишно или когато компонентите на критичните мрежови елементи се доставят.

(6) Ако отделен компонент само частично представлява критичен мрежови елемент, той се счита за част от критичен мрежови елемент.

(7) Операторът поддържа актуален списък на всички компоненти на критичните мрежови елементи, техните функции, местоположения, администратори и управители, техните доставчици на услуги за трето ниво на поддръжка и техните производители или доставчици. При поискване, списъкът се предоставя на Агенцията и орган, отговарящ за информационната сигурност.

Член 6
(Мерки за сигурност при доставката на компоненти на критични мрежови елементи)

(1) Операторът е запознат с цялата верига за доставки и свързаните с нея рискове, включително подизпълнителите във връзка с отделни компоненти на критични мрежови елементи, които включват също така криптографски ключове, UICC/eUICC и други елементи на сигурността, злоупотребата с които би могла да застраши сигурността на критичните субекти.

(2) Операторът гарантира, че изискванията във връзка със сигурността между оператора и производителите или доставчиците на компоненти на критични мрежови елементи или неговите доставчици на услуги за трето ниво на поддръжка са разписани в договор и документирани, както и изисква от производителите или доставчиците да спазват договорените мерки за сигурност по цялата верига за доставки.

(3) За да се предотврати своевременно злонамереното използване на уязвимостите от злонамерени участници, операторът гарантира, че производителят или доставчикът на компоненти на критичен мрежови елемент са задължени с договор незабавно да информират оператора за установената уязвимост и за мерките за намаляване на рисковете, както и да предоставят указания относно защитните или коригиращите мерки, които операторът може да предприеме в отговор на заплахата.

(4) Най-малко веднъж годишно операторът проверява адекватността на правата за достъп по отношение на критичните мрежови елементи или ги актуализира незабавно с оглед на настъпилите промени в организацията или от страна на доставчиците на услуги за трето ниво на поддръжка.

(5) Операторът предотвратява своята обвързаност с отделен доставчик на стоки или доставчик на услуги за трето ниво (т.е. „зависимост от определен доставчик“), когато това е технически осъществимо и икономически устойчиво, с цел намаляване на зависимостта и повишаване на устойчивостта в случай на уязвимости на критични компоненти, включително чрез избягване на дългосрочни договори с отделни производители, доставчици или доставчици на услуги за трето ниво на поддръжка, или като има възможност да ги сменя с цел намаляване на смущенията при предоставянето на услуги на критични субекти до възможно най-ниската степен.

Член 7
(Договорни условия с производители, доставчици или доставчици на услуги за трето ниво на поддръжка)

За да се гарантира високо ниво на сигурност, операторът включва най-малко следното в новите договорни условия с производители, доставчици или доставчици на услуги за трето ниво на поддръжка:

1. декларация от производителя или доставчика, че компонентът или неговите настройки по подразбиране нямат недокументирани възможности за достъп или каквото и да било отрицателно въздействие върху функционирането на критичните субекти;
2. ангажимент от страна на производителя, доставчика или доставчика на услуги за трето ниво на поддръжка за защита на данните, с които те се запознават при предоставянето на услугите или достъпа до тях във връзка с предоставянето на услугата за достъп;
3. ангажимент от страна на производителя, доставчика или доставчика на услуги за трето ниво на поддръжка да информира незабавно оператора в случай на нарушения на защитата на комуникационните данни или данните за трафика, които оказват въздействие или биха могли да окажат въздействие върху оператора или критичните субекти, посочени в член 1, точка 1 от настоящия общ акт;
4. ангажимент от страна на производителя, доставчика или доставчика на услуги за трето ниво на поддръжка да уведоми незабавно оператора за каквито и да било инциденти и уязвимости, свързани със сигурността, които биха могли да окажат въздействие върху сигурността на мрежата, свързаните услуги или данните на оператора;
5. ангажимент от страна на производителя, доставчика на стоки или доставчика на услуги за трето ниво на поддръжка да изпълнява стандартите и правилата за сигурност, установени от оператора, и да предприема подходящи мерки за сигурност, за да се гарантира сигурността на информационните системи и мрежи, както и данните на оператора или критичния субект;
6. способността на оператора по всяко време да прави преглед на средата, процедурите, мерките за сигурност и инструментите, използвани от доставчика

на услуги за трето ниво на поддръжка при осъществяването на достъп до мрежата и данните на оператора;

7. отговорността на производителя, доставчика или доставчика на услуги за трето ниво на поддръжка за вреди, които биха били причинени от установени уязвимости или злоупотреба с компоненти на критични мрежови елементи, техните настройки по подразбиране или при предоставянето на услуги за трето ниво на поддръжка, които производителят, доставчикът или доставчикът на услуги за трето ниво на поддръжка са пренебрегнали или умишлено са извършили;
8. задължение за редовно обучение на персонала на производителя, доставчика или доставчика на услуги за трето ниво на поддръжка в областта на сигурността на данните и информационните системи и мрежи.

Член 8

(Правила относно достъпа до и използването на критични мрежови елементи)

(1) При осъществяването на физически или логически достъп до компонентите на критичните мрежови елементи, техните настройки и данните на оператора, съхранявани, обработвани или изменяни в тях, операторът гарантира, че:

1. достъпът е строго ограничен до лица, които преди това са получили разрешение;
2. всички работи по критичните мрежови елементи, извършвани на място или чрез отдалечен достъп, се контролират от оператора;
3. се извършва многофакторно удостоверяване на самоличността за потребители, на които са предоставени изключителни права в най-голяма степен за достъп до отделни компоненти на критични мрежови елементи, техните настройки или данните, съхранявани или обработвани в тях;
4. всяко упълномощено лице, на което е предоставен достъп, има уникален потребителски профил и парола;
5. се използват само пароли, които се сменят редовно или незабавно в случай на установена злоупотреба и съдържат най-малко 15 знака и включват главни и малки букви, цифри и специални символи, ако софтуерът позволява това;
6. концепцията за нулева толерантност или доверие се прилага при осъществяването на достъп, когато е възможно;
7. сигурността на комуникационната връзка от упълномощения потребител към отделните компоненти е защитена чрез използване на криптиране, като се вземат предвид най-новите технологични разработки и най-добрите браншови практики в областта на информационната сигурност или препоръчаните такива от установени институции в областта на информационната сигурност;
8. е направен незаличим запис на достъпа и опитите за достъп, който се съхранява най-малко 6 месеца, включително резервно копие, но може да бъде също така за по-дълъг период, когато анализът на управлението на риска и оценката на приемливото ниво на рисковете показват, че рисковете следва да се управляват по подходящ начин чрез съхраняване на регистрационните файлове за по-дълъг период;
9. когато е възможно, се извършват записване и наблюдение на всички интервенции във връзка със софтуера относно компонентите, включително промени в конфигурацията. Записите, включително резервно копие на тези данни, се съхраняват толкова дълго, колкото е посочено в предходната точка;

10. достъпът до отделните компоненти и данните, съхранявани или обработвани в тях, е ограничен във времето и е отворен само за времетраенето на необходимата работа.

(2) В случай на достъп до отделните компоненти на критичните мрежови елементи от страна на персонала или служителите на доставчик на услуги за трето ниво на поддръжка, те:

1. използват единствено сигурна междинна специална работна станция („jump server“), която е предмет на редовни проверки за сигурност;
2. монтират на специална работна станция единствено абсолютно необходимите инструменти, компоненти и активни услуги за достъп до други ресурси в мрежата, които са абсолютно необходими и трябва да бъдат актуализирани с най-новите програми за сигурност;
3. използват сигурни криптографски операции и ключове на специална работна станция, която трябва да се намира в мрежата на оператора и да е единствено под негов контрол;
4. всеки достъп се одобрява и активира ръчно от оператора и само за времетраенето на достъпа;
5. всички осъществявания на достъп и дейности физически се контролират и записват от оператора;
6. използват двуфакторно удостоверяване на самоличността и пароли, които съдържат най-малко 15 знака и включват главни и малки букви, цифри и специални символи, които следва да се сменят въз основа на оценените рискове.

(3) Преди операторът да прехвърли услугата за управление, поддръжка или актуализиране на критичните мрежови елементи или техните отделни компоненти на трета страна, той проверява и гарантира, че тя разполага най-малко със същите или по-добри механизми за сигурност и процеси за управление на сигурността в сравнение с неговите механизми и процеси. Операторът незабавно информира съответния критичен субект, Агенцията и органа, отговарящ за информационната сигурност, за намерението за прехвърляне.

(4) Операторът проверява действителното състояние на процесите за сигурност преди началото на предоставянето на услугата и след това най-малко веднъж годишно. Операторът води документация за вътрешните прегледи и проверки относно предоставянето на услуги за поддръжка от трети страни и ги съхранява за времетраенето на предоставянето на услугите и в продължение на една година след тяхното приключване, но не повече от пет години.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 9
(Преходни разпоредби)

(1) Операторът уведомява Агенцията и органа, отговарящ за информационната сигурност, за съществуващите местоположения на критични мрежови елементи в срок от 30 дни от влизането в сила на настоящия общ акт.

(2) Операторът уведомява Агенцията и органа, отговарящ за информационната сигурност, за съществуващите местоположения на услуги за трето ниво на поддръжка на критични мрежови елементи в срок от 30 дни от влизането в сила на настоящия общ акт.

(3) Агенцията публикува за първи път документите, посочени в член 3, параграф 2 от настоящия общ акт, считано от датата на влизането му в сила.

Член 10
(Влизане в сила)

Настоящият общ акт влиза в сила на тридесетия ден след публикуването му в Държавен вестник на Република Словения, съгласно който операторите могат да използват оборудването и поддържат предоставянето на услуги за трето ниво на поддръжка до изтичането на крайните срокове, посочени в член 312, параграфи 2 и 3 от Акта.

№ _____ маг. Marko Mišmaš

Любляна, дата _____ директор

EVA 2023-3150-0034

ПРЕДЛОЖЕНИЕ

Приложение

Списък на критичните мрежови елементи и свързаните информационни системи:

Критични мрежови елементи	**Функционалности на мрежовите и информационните системи**
Управление на абонатите и механизми за криптиране	- Управление на сесията (глас и данни), - удостоверяване на самоличността на потребителите и автентичността на оборудването по отношение на мрежата, - управление и съхранение на ключове за упълномощаване на абонати и мрежови компоненти (UICC/eUICC, цифрови сертификати/HSM), - функции за сигурно удостоверяване на автентичността, защита на целостта на комуникацията (криптиране) и съхранение на потребителски ключове, мрежови и управленски компоненти, - управление на правата за достъп.
Взаимно свързване	- Характеристики на хостинга и интерфейси към други мрежи и услуги.
Управлявани мрежови услуги	- Регистрация и разрешаване на мрежови услуги, - съхранение и обработка на данни за комуникация, местоположение и трафик, - експозиция на мрежи и мрежови функции на външни приложения и услуги.
Управление и оркестрация на виртуализирани мрежови функции (NFV) и мрежова оркестрация (MANO), включително инфраструктура за виртуализация	- Управленски функции за оркестрация и конфигурация на NFV независимо от вида на изпълнението (VM, контейнер, микроуслуги), - функции за виртуализация за изпълнението и използването на NFV, - функция за избор на мрежови сегмент (NSSF).
Мрежа за радиодостъп	- Базови станции, които поддържат 5G или по-висока технология.
Системи за управление и други системи за поддръжка	- Наблюдение на функционирането и управлението на мобилната комуникационна мрежа, включително частта за достъп (RAN/O-RAN), - системи за откриване на събития, аномалии и заплахи, свързани със сигурността, както и тяхното управление (функции по сигурността, включително SIEM/SOAR).
Законно прихващане	- Функции за достъп до съдържанието на съобщението и данните за трафика на потребителите от компетентния орган.

ПРЕДЛОЖЕНИЕ