Мотиви към Правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност

В изпълнение на чл. 243, ал. 3 на Закона за електронни съобщения (ЗЕС), Комисията за регулиране на съобщенията (КРС/Комисията) приема правила за минималните изисквания за сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска (Правила). При определянето им Комисията се съобразява с изискванията на приложимите актове на Европейската комисия и отчита в максимална степен препоръките, насоките, становищата, общите и добрите практики и методологии на Агенцията на Европейския съюз за киберсигурност[1], както и приложимите европейски схеми за сертифициране на киберсигурността, установени с актове на Европейската комисия, и приложимите европейски и международни стандарти и стандартизационни документи. Съгласно чл. 243б, ал. 7 на ЗЕС, в Правилата се определят критериите за определяне на въздействието като значително на инцидент свързан със сигурността, изисканата информация, форматът и начинът на уведомяване на инцидентите, свързани със сигурността. В допълнение с приемането на Правилата, комисията изпълнява относимите стратегически и технически мерки от Инструментариума на ЕС за киберсигурността в областта на 5G[2].

С Решение № 425/17.12.2020 г., допълнено с Решение № 34/28.01.2021 г. КРС създаде два консултативни съвета - по въпросите на сигурността на обществените фиксирани електронни съобщителни мрежи и фиксирани услуги и по въпросите на сигурността на обществените мобилни наземни електронни съобщителни мрежи и мобилни услуги. В консултативните съвети бяха включени представители на КРС, Министерството на транспорта и съобщенията, Държавна агенция „Електронно управление" и представители на предприятия, предоставящи обществени електронни съобщителни мрежи и услуги, както и техни браншови организации. Двата съвета приеха Позиции на разгледаните въпроси, които са публикувани на интернет страницата на КРС[3].

За различните обществените електронни съобщителни услуги, предприятията които ги предоставят прилагат различни мерки за сигурност. Също така при докладване на инцидент с въздействие определено като значително, предприятията трябва да докладват засегнатите услуги. В тази връзка и в съответствие с Техническите насоки на ENISA за докладване на инциденти, съгласно Европейския кодекс за електронни съобщения (Насоките на ENISA за докладване на инциденти)[4] услугите са категоризирани в Правилата. С цел постигане на общо разбиране по отношение на категоризацията и отчитайки разпоредбите на ЗЕС, консултативните съвети постигнаха съгласие, което е валидно и по отношение на прилагането на Правилата:

а) мобилна гласова услуга, включително гласова услуга, видео услуга, SMS[5], MMS[6];

---

[1] ENISA - European Union Agency for Cybersecurity

[2] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures
https://ec.europa.eu/bulgaria/news/secure-5g-networks-ec-endorses-eu-toolbox-and-sets-next-steps_bg

[3] https://crc.bg/bg/rubriki/229/sigurnost-i-cjalost-na-elektronnite-syobshtitelni-mreji-i-uslugi

[4] Technical Guideline on Incident Reporting https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

[5] Short Message Service (услуга за кратки съобщения) представлява възможност за изпращане и получаване на текстови съобщения.

б) мобилен достъп до интернет, предоставян без оглед на използваната технология чрез GPRS[7], 3G, 4G, 5G[8] и др;

в) фиксирана гласова услуга – гласова услуга използваща номера от национален номерационен план, различни от мобилни номера, без оглед на използваната технология;

г) фиксиран достъп до интернет са услуги за достъп до интернет в определено местоположение, без оглед на използваната технология, включително през RLAN[9];

д) междуличностна съобщителна услуга без номер – включва се само телефонна услуга без номера, съобщения, видеоразговори, електронна поща;

е) услуги за разпространение на радио- и телевизионни програми – включват наземно радиоразпръскване на радио- и телевизионни програми, кабелно разпространение на радио- и телевизионни програми; спътниково разпространение на радио- и телевизионни програми, IPTV[10] (с изключение на OTT [11]услуги);

ж) услуги, при които се използва комуникация Машина – Машина, включително 5G URLLC[12], MTC[13];

з) под други услуги за пренос на сигнали се разбира неизчерпателно изброяване на услуги за пренос, различни от достъп до интернет като линии под наем (в това число резервиран капацитет, осигуряващ логическа свързаност между две крайни точки в електронните съобщителни мрежи, без възможност за управление на комутацията/маршрутизацията от страна на крайния потребител), VPN[14] услуги (между три и повече крайни точки на мрежата с възможност за управление на комутацията/маршрутизацията от страна на крайния потребител) и други.

Аналогично за различните обществени електронни съобщителни мрежи, предприятията които ги предоставят прилагат различни мерки за сигурност и в тази връзка са категоризирани в Правилата. Разделението на мрежи и услуги отчита и факта, че съществуват предприятия, предоставящи единствено мрежата си, както и предприятия, които предоставят услугите си използвайки чужда мрежа.

Съгласно чл. 2 от ЗЕС, изискванията на Правилата към услугите за разпространение на радио- и телевизионни програми не се отнасят към съдържанието на радио- и телевизионните програми. Поради характера на междуличностните услуги без номера, изискванията които се отнасят към тях не се отнасят към мрежите, чрез които се предоставят. Поради липсата на техническа възможност от страна на предприятията, предоставящи междуличностните услуги без номера, да контролират мрежата, чрез която се предоставя услугата, за тях не важат мерките за сигурност относими към електронните съобщителни мрежи.

---

[6] Multimedia Messaging Service (услуга за мултимедийни съобщения) е услуга за изпращане и получаване на съобщения, които включват мултимедийно съдържание.

[7] General Packet Radio Service (Обща пакетна радио услуга) е услуга за предаване на пакети данни, като надстройка към мобилния стандарт GSM.

[8] 3/4/5 Generation (3/4/5 поколение) са безжични мобилни телекомуникационни технологии

[9] Radio Local Area Network (радио локална мрежа) е локална мрежа, използваща безжична връзка вместо кабелна.

[10] Internet Protocol Television (телевизия през интернет протокол) представлява услуга за предоставяне на мултимедийно съдържание чрез платформа, базирана на интернет протокол с гарантирано качество.

[11] Over-The-Top („над върха“) са услуги за предоставяне на допълнително съдържание през интернет при поискване.

[12] 5G Ultra-Reliable Low-Latency Communication (ултра надеждна комуникация с ниска латентност) е услуга за чувствителни към закъснение устройства, като автономношофиране, автоматизация и други.

[13] Machine Type Communication (комуникация машина- машина).

[14] Virtual Private Network (виртуална частна мрежа).

Управлението на риска на сигурността, включва оценка на риска, изготвяне на мерки за намаляване на риска, изследване на инциденти и одит на сигурността. В Глава втора от Правилата са включени конкретни изисквания за различните електронни съобщителни мрежи и/или услуги за всеки един етап от управлението на риска.

Всяко предприятие, предоставящо обществените електронни съобщителни мрежи или услуги, изготвя собствена методика за управление на риска, съобразно предоставяните мрежи или услуги. Методиката може да е базирана на приложими хармонизирани международни стандарти, например ISO27000. Примерна методика за управление на риска е разработена и в Приложение №1 на Позицията на Консултативния съвет по въпросите на сигурността на обществените фиксирани електронни съобщителни мрежи и фиксирани услуги, чиято цел е да подпомогне малките и средни предприятия в изпълнение на настоящото задължение. В случай че предприятията имат вече установени политики, процеси и рамки за управление на риска, е достатъчно същите да се съобразят и/или допълнят с изискванията на Правилата. При изготвяне на оценка на риска, е важно всяко предприятие да оцени активите си и да документира изготвената оценка.

На втори етап, предприятията трябва да изберат подходящите технически и организационни мерки за намаляване на риска. В тази връзка в Правилата в Приложение №1 се съдържат изисквания за технически и организационни мерки. Същите са базирани на Насоките на ENISA за мерките за сигурност, съгласно Европейския кодекс за електронни съобщения, (Насоките на ENISA за мерките за сигурност)[15]. Предприятията са запознати с тях по време на консултативните съвети и са част от приетите Позиции. Мерките са групирани на три нива, като всяко следващо ниво на сигурност включва изискванията за предходното. С други думи, на ниво 2 не се повтарят мерките за сигурност от ниво 1, но се разбира, че са включени. По същия начин, на ниво 3 мерките за сигурност включват и тези от нива 1 и 2.

Изискването на чл. 11, ал. 1 по отношение на обществените мобилни електронни съобщителни мрежи отговаря на Насоките на ENISA за мерките за сигурност. Същевременно по този начин се изпълняват технически мерки ТМ01: Осигуряване на прилагането на базови изисквания за сигурност, ТМ02: Осигуряване и оценка на прилагането на мерките за сигурност в съществуващите 5G стандарти, ТМ03: Осигуряване на строг контрол на достъпа, ТМ05: Осигуряване на сигурни управление, експлоатация и мониторинг на 5G мрежите, ТМ06: Укрепване на физическата сигурност, ТМ07: Укрепване на целостта на софтуера и управлението на актуализациите и кръпките и ТМ08: Повишаване на стандартите за сигурност в процесите на доставчиците чрез стабилни условия за обществени поръчки от Инструментариума на ЕС за киберсигурността в областта на 5G.

В чл. 13 са разработени детайлни договорни условия, които да предвидят предприятията, предоставящи обществените мобилни електронни съобщителни мрежи и/или обществени електронни съобщителни услуги, в отношенията си с доставчици на оборудване и софтуер. Същите са в изпълнение на стратегическа мярка 3: Оценяване на рисковия профил на доставчиците и прилагане на ограничения за доставчиците с висок риск от Инструментариума на ЕС за киберсигурността в областта на 5G. Също така, договорните условия фигурират, като цел на сигурност 04 от Приложение №1 на Правилата и в тази връзка КРС препоръчва подобни клаузи да се сключват и от останалите предприятия.

---

[15] Guideline on Security Measures under the EECC https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

Последен етап от метода за управление на риска са включените общи правила за извършване на одити. При изготвянето им са заложени общи правила, включени в повечето системи за одит, като например този в серията стандарти ISO27000. Предвиден е начина, по който да се доказва съответствие с техническите и организационните мерки за сигурност. Предвидена е възможност одита да бъде вътрешен за малките и средни предприятия, с цел предотвратяване на допълнителни разходи и възможност одита да се извърши от квалифициран независим орган за предприятията, имащи вече въведени системи за сигурност на информацията. Тригодишният период за периодичен одит е съобразен с въведените системи за сигурност на предприятията, като същевременно няма да бъде утежняващ за тези предприятия, на които предстои въвеждането на системи или за тези предприятия, които ще разчитат единствено на вътрешен одитор. Предвидената в чл. 18 възможност е в съответствие с изискването за докладване на инцидент свързан със сигурността, оказал значително въздействие. По този начин се завърта пълния цикъл от метода за управление на риска.

Глава трета се отнася до инциденти, свързани със сигурността. При определянето им КРС се съобразява с чл. 243б, ал. 6 и Насоките на ENISA за докладване на инциденти. Причините за възникване на инциденти, оказали значително въздействие са включени в чл. 20.

Съществуващите критерии за докладване на инциденти, оказали значително въздействие, свързани с наличността на услугите са включени в Приложение №2 на Правилата, като за мобилните услуги показателя „брой ползватели, засегнати от инцидента“ е увеличен. Основната причина за разделяне на критериите по услуги е свързана с различния брой на ползвателите на услуги. Във връзка с разширената дефиниция за сигурност в ЗЕС, в Правилата е определен критерий за докладване на инциденти, свързани с нарушение на автентичността, целостта и поверителността. В съответствие с Насоките на ENISA за докладване на инциденти, този критерий е определен на база „брой ползватели, засегнати от инцидента“. В изпълнение на чл. 243б, ал.6, т.3 е заложен критерий за географски обхват на възникналия инцидент. Считаме, че този критерий ще даде възможност на предприятията, предоставящи електронни съобщителни мрежи да извършат оценка на инцидента, доколкото за тях оценката на база „брой засегнати ползватели“ не е възможна. В изпълнение на чл. 243б, ал.6, т.5 са качествените критерии, свързани с достъпа към единния номер за спешни повиквания и системите за предупреждение на населението.

Формата за докладване на инциденти е изменена, като са добавени новите изисквания от ЗЕС по отношение на компрометираната компонента на сигурността, критериите за докладване на инциденти и разширения обхват на услугите. Същевременно от формата е отпаднала събираната до сега информация за предприетите действия след възникналия инцидент. КРС счита, че предвидената възможност в чл.18 е достатъчна, в случай на необходимост. В Правилата е предвидена една форма за докладване на инциденти, като при първоначално уведомление не е необходимо да се попълва цялата информация.

Промяна има в процедурата за докладване на инциденти, оказали значително въздействие. В чл. 26 от Правилата е определено, че „незабавно“ уведомяване означава до 24 часа. От направен от КРС анализ на инцидентите, оказали значително въздействие за периода от 2012 г. до 2021 г., повече от половината инциденти са приключили в рамките на първите 24 часа, обикновено това са инциденти свързани с проблеми в оборудването. В тази връзка, считаме, че по този начин се дава възможност предприятието спокойно, след приключване на инцидента, оказал значително

въздействие, да изпрати необходимата информация. Същевременно, т.к. ще разполага с цялата необходима информация по отношение на инцидента, ще изпрати едно уведомление, в което ще попълни исканата информация. По отношение на останалите инциденти, оказали значително въздействие, обикновено причината за тяхното възникване е свързана с природно бедствие, прекъсване на кабел или друго подобно. Характерно при тези инциденти е, че приключват след няколко дни. В тази връзка на предприятието ще се наложи да изпрати две уведомления.

Правилата са нов административен акт, КРС счита че по отношение на разпоредбите на глава втора, ще е необходим период през който предприятията да изготвят управлението на риска на сигурността. От друга страна, отчитайки че по време на дейността на Консултативните съвети, предприятията са запознати с част от техническите и организационни мерки за намаляване на риска, КРС счита че една година е достатъчен период.