НАЦИОНАЛНА КОНВЕНЦИЈА ЗА ЕВРОПСКАТА УНИЈА ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА (ВЕБ: nkeu.mk)

ПРЕПОРАКИ ОД

11-та Сесија на Работната група, 4 - Правда, слобода и безбедност

Тема: „ Зајакнување на отпорноста на институциите за одговор на хибридните закани“

1. Владата треба да преземе иницијатива за креирање на системски национален пристап за јакнење на отпорноста на институциите преку нормативна рамка која ќе биде основа за подготовка на акти и процедури за управување со сајбер-безбедност и заштита од хибридни во согласност со директивите на ЕУ и стандардите на НАТО.

2. Владата да ја разгледа потребата за измена на процедурите на огласите за јавни набавки кои се од областа на ИТ технологиите кои изнесуваат многу детали од техничка приода кои го зголемуваат ризикот од хибридни закани.

3. За јакнење на отпорноста на институциите од хибридните закани Владата да посвети посебно внимание на исклучително значајните технички стандарди за безбедност (заштита) на ИТ системите во институциите (информатичката инфраструктура).

4. Јавното обвинителство и судовите и другите институции надлежни за спроведување на законите, да ги зголемат своите истражни капацитети (технички и ресурсни) за справување со кривични дела од доменот на сајбер криминалот. Тоа подразбира да имаат наменски буџет и можност да користат услуги на надворешни специјализирани организации (outsourcing).

5. За поголема национална отпорност од хибридните закани потребно е Владата да ја зајакне комуникацијата и соработката со сите засегнати страни (претпријатијата од ИТ секторот и други претпријатија од доменот на безбедноста, граѓански здруженија, академската заедница, медиумите и друга експертска јавност) како и да развие концепт за јавно-приватно партнерство во оваа област.

6. Оперативниот тим за справување со сајбер-безбедност и хибридни закани да го забрза процесот на утврдување на листа на институции кои можат да бидат цел на хибридни закани, вклучително и да се спроведе приоритизација, бидејќи сите институции не бараат еднакво ниво на заштита, ниту пак, сите институции имаат подеднаква важност.

7. Со оглед на неизбежната масовна примена на информатичките технологии (ИТ) во сите сфери на општественото дејствување, ѝ се препорачува на

Владата да преземе иницијатива за менување на пристапот кон ИТ секторите во институциите преку соодветен менаџмент на човечки ресурси што би значело:

- привлекување на висококвлификувани кадри со висина на личен доход соодветен за ИТ секторот во целина;
- при регрутација на ИТ кадрите да се применува строго експертскиот критериум, односно професионалните квалификации;
- оптимизација на бројот на вработени според сложеноста, критичноста и ранливоста на институцијата;

8. Владата да иницира потесна соработка и партнерства меѓу националните безбедносни институции со оние од соседните држави за регуларно споделување на искуства од реализирани случаи на сајбер-напади и хибридни закани (редовни средби со ЕУ претставници и регионални експерти).

9. Со оглед на фактот дека за успешно справување со хибридните закани потребно е учество на сите засегнати страни, вклучувајќи ги и вработените во институциите, се препорачува: Владата да преземе иницијатива за утврдување на потребата од адекватни обуки со цел да ги запознае вработените со безбедносните стандарди, оперативните процедури и протоколите за заштита од можни хибридни закани.

10. Сајбер-културата како целина од технологии (од материјален, организациски и интелектуален карактер), но и практики, ставови, начини на размислување и вредности за сајбер-просторот се гради на спонтан начин од страна на сите членови на заедницата. Меѓутоа, поттикнувањето и поддржувањето на јавни дебати од страна на различни чинители може да ја зголеми осетливоста на граѓаните за овие прашања и да се развие критичката свест и култура на толеранција, преку активно вклучување и поддршка од граѓанскиот сектор

11. Да се обезбеди заштита и на изборниот процес од хибридни закани, непријателски сајбер-активности, информативни операции спроведувани од други државни и недржавни субјекти и финансирање на политички партии, политичари и невладини организации од страна на надворешни, непријателски фактори. За ефикасно постигнување на оваа цел, националните носители ќе ги користат научените лекции и експертиза од НАТО и ЕУ.