НОЕМВРИ 2022

ДОКУМЕНТ ЗА ДИСКУСИЈА

НАЦИОНАЛНА СТРАТЕГИЈА ЗА САЈБЕР БЕЗБЕДНОСТ 2023 -2026

Оваа публикација е изработена од страна на работната група задолжена за изработка на националната стратегија за сајбер безбедност. За содржината на овој документ единствено е одговорен тимот на стратегијата. Овој документ е изработен единствено за употреба и во корист на изработката на Националната стратегија за сајбер безбедност 2023-2026 година.

Вашите коментари и мислења можете да ги пратите на:

https://ener.gov.mk/

Или на емаил адресата: cyber_security@mioa.gov.mk

ВОВЕД

Интернетот е суштински дел од животот за многу наши граѓани. Го користиме на работа, го користиме за да останеме во контакт едни со други, го користиме како пристап до забава, плаќаме сметки и фактури. Во исто време, повеќе од предметите околу нас се поврзани на Интернет, вклучувајќи ги нашите автомобили, апаратите за домаќинство, индустриските машини и друго. Приклучувањето на Интернет носи огромна корист за сите нас, но истовремено не изложува и на нови безбедносни ризици.

Република Северна Македонија има национална стратегија за Сајбер безбедносност, донесена 2018-та година, за периодот 2018-2022 година, која има за цел креирање на безбеден Интернет простор за сите нас. За да се подготвиме за новите предизвици со кои се среќаваме во сајбер просторот, стратегијата за сајбер безбедност мора да покрива голем дел од клучните полиња во сајбер просторот, од заштита на државниот интегритет и на човековите права, до имплементирање на законите и спречување на кривични дела во онлајн просторот. Новата стратегија за сајбер безбедност, освен одржувањето на безбедноста и отпорноста (cybersecurity and resilience) на Интернет, треба да се насочи кон континуирано градење и зајакнување на сајбер отпорноста и безбедноста.

Неодамнешните инциденти врз нашите институции, како и компромитирачките сајбер напади и инциденти на државните мрежи на соседните земји, вклучително и на големи корпоративни правни субјекти во светот, покажуваат дека постои огромна реална закана за сите нас. Во таа смисла, не помалку важни, иако значително помали, се и сајбер инцидентите кои често ги погодуваат семејствата и локалните бизниси, а кои доведуваат до финансиски загуби, прекин на работата, кражба на идентитетот и психолошки стрес.

Во процесот на креирање на успешна стратегија за сајбер безбедност има потреба од дефинирање на безбедносните цели и одредување дали одговорностите се соодветно доделени во одржувањето на безбедноста и градењето на сигурен Интернет за државата и нашите граѓани. За да имаме успешна стратегија, потребно е истата да се креира во партнерство и во согласност со сите засегнати страни. Целта на овој документ е да се отпочне со отворена дискусија и да се чујат ставовите на сите засегнати страни, со што ќе се придонесе да се постигне значителен напредок на полето на сајбер безбедност, а тоа ќе води и кон поголем просперитет на Република Северна Македонија на полето на сајбер безбедност. Сајбер безбедноста е важна за

сите и затоа е важно да се чујат ставовите на малите, средните и големите бизниси, на индустриските тела, академијата, невладините организации, владините агенции, групи на заедницата и членови на јавноста. Во натамошниот текст на овој документ, со цел да ги осознаеме Вашите мислења и идеи на оваа тема, отвараме неколку теми и прашања за кои се надеваме дека би сакале да го дадете Вашиот придонес и да ги споделете со нас Вашите одговори.

Само со заедничка тесна соработка на Владата, академијата, индустријата и граѓанските заедници можат да ја зајакнат сајбер отпорноста на национално ниво и да обезбедат просперитет и заштита на онлајн интересите на сите.

КАДЕ СМЕ СЕГА?

„Во 93 % од случаите, надворешен напаѓач може да го пробие мрежното опкружување на организацијата и да добие пристап до ресурсите на локалната мрежа.“

Со измените на Законот за електронските комуникации (Службен весник на Република Македонија број 188/2014), согласно член 26-а во состав на Агенцијата за електронски комуникации формирана е посебна организациона единица – Национален центар за одговор на компјутерски инциденти MKD-CIRT, која претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи и кој идентификува и обезбедува одговор на безбедносни инциденти и ризици.

Министерството за информатичко општество и администрација (МИОА) има одговорност за сите прашања кои се однесуваат на информатичката технологија. Министерството е одговорно за политиката и стратегијата во е-Влада. Со цел да се олеснат активностите кои се однесуваат на отпорноста на критичната национална инфраструктура за сајбер-безбедноста во Северна Македонија, под надлежност на МИОА а со подршка на УСАИД, во јуни 2021 година формирана е работната група за сајбер-безбедност за критична инфраструктура (CICWG). CICWG е форум креиран да ги олесни активностите кои се однесуваат на отпорноста на критичната национална инфраструктура за сајбер-безбедноста во Северна Македонија. Во работна група за сајбер безбедност на критичната информациска инфраструктура учествуваат претставници од повеќето релевантни институции, како и од приватниот сектор кои се од клучна важност за нашата држава. CICWG делува како механизам за координација на клучните чинители, форум за соработка и цел за дефинирање на критична

инфраструктура, проценка на ризик, планирање на начини за ублажување/ отстранување на ризици, и развој и имплементација на механизми за споделување информации.

Министерството за внатрешни работи (МВР) е водечка институција за борба против сајбер криминалот. За таа цел МВР создаде единствена и сеопфатна правна рамка за компјутерски криминал, истовремено ангажирајќи се во модернизацијата на релевантните институции за ефикасна борба против компјутерскиот криминал.

Министерството за одбрана (МО) е водечка институција за сајбер одбрана - Во 2021 година, по влезот во НАТО, Северна Македонија потпиша Меморандум за разбирање со цел унапредување на соработката за сајбер одбрана меѓу НАТО и одбранбените власти на земјата; Меморандумот за соработка особено се фокусира на споделување информации, размена на најдобри практики и зголемување на отпорноста кон сајбер заканите.

CSIRT - ФИНКИ (академски сектор) е основан во 2017 како организациска единица на Факултето за информатички науки и компјутерско инженерство. Мисијата на креирање на CSIRT на ФИНКИ е да се обезбеди детектирањето, решавањето и превенцијата во врска со безбедноста на информациите и мрежата при факултетот.

Во последно време, на глобално ниво, забележан е раст на нивото и сериозноста на злонамерните сајбер активности. Личните финансиски и другите вредни информации, кои можад да се користат за финансиски измами или други тешки кривични дела, се главна мета на овие сајбер напади. Злонамерните сајбер активности вклучуваат и обиди да се влијае на јавното мислење, а со тоа и вмешување во демократските процеси. Ова вклучува „хакирање и ослободување“ на чувствителни информации, што има за цел обезвреднување на одредени брендови кои се цел на сајбер нападите со што се нарушува нивниот углед во јавноста. Поголем инцидент ќе доведе и до нарушување на довербата на корисниците како и на репутацијата на самиот бренд. За жал, многу наши граѓани и понатаму стануваат жртви на вакви криминални дејствија, затоа што не успеваат да ги забележат обидите за инциденти или не знаат како да се заштитат затоа што не ги познаваат основните онлајн безбедносни практики.

Од друга страна пак, критичните системи во Република Северна Македонија, вклучително оние во секторот за енергетика, финансии, телекомуникации и транспорт, стануваат се повеќе дигитализирани. Меѓународен сајбер инцидент може да доведе до прекин во електричната мрежа, да ги деградира системите во јавното здравство и транспортните системи, и да доведе до оштетување на физичката инфраструктура. Доколку Република Северна Македонија стане мета на овие нови закани, истите би

можеле да ја загрозат физичката безбедност, економската стабилност и континуитетот на функционирањето на државата и на целокупното општествено живеење.

Нашите граѓани, приватниот сектор па и државниот сектор се потпираат се повеќе и повеќе на Интернетот и дигиталните услуги понудени на Интернет. Технологиите како што се автоматизација, вештачка интелигенција, виртуелна реалност и Интернетот на нештата (IoT) ќе продолжат во континуитет да го трансформираат начинот на кој живееме, работиме и комуницираме едни со други. Адаптацијата на ваквиот брз технолошки развој и искористувањето на можностите што ги нуди, допринесува на квалитетот на животот на сите.

Сепак, прифаќањето на овие нови технолошки решенија истовремено нè прави се повеќе зависни од технологијата, а со тоа и не прави потенцијално ранливи во однос на злонамерни сајбер активности.

Во поглед на ова, Ве молиме споделете ги со нас Вашите ставови за:

1. Каков е Вашиот став за заканите во сајбер просторот кај нас?

2. На кои закани треба да се фокусира Владата?

ДА СЕ ПОЗИЦИОНИРАМЕ ЗА ИДНИНАТА

Постојаните промени што се случуваат во сајбер безбедносната средина не наведуваат да размислиме и да се подготвиме за подобро да се заштитиме од ваквите закани. Еден од клучните чекори за тоа е навременото откривање на потенцијалните закани и нашиот соодветен одговор на истите. При зачувувањето на сајбер безбедноста на Република Северна Македонија, важно е дефинирањето на соодветните улоги во владините установи, индустријата и заедницата. Сајбер безбедноста отсекогаш била, и ќе биде заедничка одговорност на повеќе актери.

Крајните корисници, како што се поединци и малите бизниси, носат високо ниво на ризик при нивните онлајн активности и често сами се справуваат со загубата предизвикана од злонамерна активност. Тие често пати не знаат и не можат да идентификуваат или да одговорат на сајбер ризик, ниту пак можат да ја проценат тежината на последиците доколку се случи некој сајбер инцидент. Иако ова најчесто се однесува на поединци и мали бизниси, истото важи и за некои големи бизниси.

Од друга страна, професионалните даватели на стоки и услуги кои им помагаат на клиентите да пристапат или да имаат корист од Интернетот, имаат тенденција за подобро разбирање за сајбер ризиците и нивните потенцијални последици. Некои производители на хардвер и софтвер, сопственици на инфраструктура и интернет базирани платформи, имаат инсталирано софистицирана заштита во нивниот простор, додека другите не се толку зрели во овозможувањето на сајбер безбедносна подршка на нивните клиенти.

Улогата на државата во сајбер безбедноста е традиционално ограничена на заштита на владината мрежа, системите кои ги поседува и нудењето совети. Сопствениците на компромитирана мрежа можат да ја известат Владата и да помогнат во санирањето кога национално значаен сајбер инцидент се случува, но немаат законска основа да го сторат тоа. Од бизнисите обично се бара само да пријават значителни компромиси на личните податоци, па Владата затоа и нема јасна и комплетна слика на значајни инциденти кои се закануваат на националната безбедност или на економскиот просперитет освен ако, компанијата не го пријави инцидентот во MKD-CIRT или пак ако тој инцидент на некој начин не се обелодени во јавноста.

Импликацијата на досегашниот сајбер простор кај нас е таква што крајните корисници носат значителен дел од ризикот, а Владата има ограничена улога во заштитата на голем број системи од клучно значење за нашите секојдневни активности. Нашите моментални поставки се базираат на личен избор и одговорност и поттикнување на бизнис инвестиции во дигиталната економија. Алтернативен пристап може да биде и

давањето приоритет на сајбер безбедноста како клучна цел, со пренесување на одговорноста за управување на сајбер ризиците од крајните корисници кон индустријата и бизнисот.

Во поглед на ова, Ве молиме споделете ги со нас Вашите ставови за :

3. Дали се согласувате со нашето разбирање во однос на тоа кој е одговорен за управување со сајбер ризиците во економијата?

4. Дали мислите дека Владата треба да има повеќе одговорност?

УЛОГАТА НА ДРЖАВАТА ВО СВЕТОТ ШТО СЕ МЕНУВА

„ Во 2021 година 22 милијарди податоци биле неовластено откриени од протекувањето на податоците. “

Многу е важно да се зајакне улогата на Владата во насока на тоа да понуди поголема помош за безбедно присуство во онлајн просторот, за воспоставување на минимални стандарди, како и за воспоставување на превентивни мерки за заштита од високо софистицирани злонамерни актери.

Владата е најзагрижена за заканите врз секторите кои обезбедуваат суштински услуги за граѓаните, како што се енергија, вода, телекомуникации, финансискиот сектор, владините ИКТ системи и транспортот. Таа во моментов ги користи своите сајбер безбедносни капацитети во рамките на законодавна рамка и во согласност со Националната стратегија за сајбер безбедност. Ова е поизразено откако нашата држава стана членка на НАТО, но и понатаму не се забележува позначајно прилагодување кон модерните злонамерни сајбер активности кои ги преминуваат и традиционалните географски граници.

Довербата на граѓаните е прв приоритет кога се размислува како и кога Владата треба да ги користи своите капацитети за сајбер безбедност.

Во поглед на ова, Ве молиме споделете ги со нас Вашите ставови за:

5. Дали сметате дека Владата може да стори повеќе за да се соочи со компјутерскиот криминал?

6. Каква улога треба да има Владата во решавањето на потенцијалните закани за институциите и бизнисите лоцирани во Република Северна Македонија?

7. Како Владата може да ја задржи довербата во македонските граѓани во процесот на развој на своите сајбер безбедносни капацитети?

8. Дали имаме потреба од Агенција за сајбер безбедност во државата и кои, според вас, би биле нејзините надлежности?

УЛОГАТА НА ОРГАНИЗАЦИИТЕ, ПРИВАТНИОТ СЕКТОР И НАЦИОНАЛНИТЕ ИНФОРМАТИЧКИ СИСТЕМИ ВО САЈБЕР БЕЗБЕДНОСТА

„Во просек, само 5 % од податоците на компаниите се соодветно заштитени.“

Технолошкиот сектор е камен-темелник за раст на дигиталното општество и дигиталната економија. Тој ги дизајнира, произведува и управува со нашите онлајн искуства. Приватниот сектор е клучен за дигиталната економија, која е од суштинско значење за нашиот просперитет.

Владата придонесува за поголема успешност на приватниот сектор, било да се поединци, мали, средни или големи претпријатија. Јасни и разумни правила кои би ги заштитиле крајните корисници се добри за сите. Овие правила треба да бидат во чекор со брзите технолошки промени во брзо растечкиот економски сектор . Променливоста во безбедноста на сајбер добрата и услугите го поставува прашањето дали е разумно да се очекува од провајдерите да сторат повеќе за да ги заштитат

своите клиенти. Дополнително на ова е и прашањето, дали купувачите се соодветно спремни за да се заштитат.

Ова им дава можност на потрошувачите да изберат дали ќе пристапат до производи кои ги изложуваат на висок степен на ризик или не. При тоа останува на страна на потрошувачот да реши дали ќе го прифати ризикот и да процени дали користа што ја носи производот го надминува ризикот при пристапувањето на тој производ.

За да ги идентификуваме сите недостатоци, во тек е подготовка на легислативата која би обезбедила потрошувачите да можат да бидат сигурни дека производите и услугите имаат разумна заштита на полето на сајбер безбедност, без разлика дали тоа се однесува на поединци, бизниси или влади. При сајбер напад сите сме потенцијални жртви.

Фирмите, пак, од Интернет напади се штитат индивидуално со свои механизми и ресурси. За многу бизниси и за потрошувачи, тешко е да разберат кое ниво на безбедност е вградено во дигиталните производи или услуги кои ги користат, и на кое ниво би можеле професионално да го обезбедат истото. Идеално, дигиталните производи и услуги треба да имаат безбедност вградена „by design“, за која корисниците секогаш треба да бидат информирани. Од постојаното зголемување на ризиците и последиците од злонамерни сајбер активности произлегува потребата да се навратиме кон Законот за безбедност на мрежи како приоритет за воспоставување на основите на сајбер безбедност во нашата земја.

Во поглед на ова, Ве молиме споделете ги со нас Вашите ставови за :

9. Каква улога можат да имаат Владата и индустријата во поддршката на сајбер безбедноста на потрошувачите?

10. На кој начин Владата и бизнисите можат да ја зголемат безбедноста, квалитетот и ефективноста на сајбер безбедноста и дигиталните понуди?

11. За кои конкретни пазарни стимулации или регулаторни промени би било добро Владата да размисли?

12. Што треба да се направи за сајбер безбедноста да биде „вградена“ во дигиталните производи и услуги?

СВЕСНОСТ, ОБУКИ, ВЕЖБИ И ДОБРО ОБУЧЕНИ ЕКСПЕРТИ ЗА САЈБЕР БЕЗБЕДНОСТ

„43 % од сите прекршувања се инсајдерски закани, било намерни или ненамерни.“

Зголемената зависност од технологијата ја нагласува потребата од повисоки стандарди за сајбер безбедност во процесот на одржување на достапноста и интегритетот на критични услуги во критичните сектори. Овој тренд значи дека во иднина, побарувачката за безбедни производи и услуги, како на пример потреба од квалификувани сајбер професионалци, ќе продолжи да расте.

Човечкото однесување е најзначајната слабост која се искористува во компјутерскиот криминал. Успешните сајбер напади често се засновани на недостатокот на разбирање за сајбер безбедноста на крајниот корисник. Овие напади користат методи како што се масовни кампањи за е-пошта, за кражба на идентитет, како и повеќе насочени напади.

Ние не сме родени со знаење за сајбер безбедноста. Преку едукацијата се ценат ризиците и се учат мерките за нивно ублажување. Но, како и сите други форми на безбедност, свесноста е дополнување, а не замена за достапноста на безбедните функции. На пример, на возачите им се обезбедува сигурносен појас и покрај едукацијата за важноста на безбедноста на патиштата и стимулации за користење на појасот. И истите очекувања и барања што ги имаме таму каде безбедноста е најважна, треба да важат и во сајбер-просторот.

Владата продолжува да добива повратни информации за големиот недостаток на експерти на полето на сајбер безбедност во Република Северна Македонија, иако овој недостаток не е карактеристичен само за нашата држава.

Тука најголемо внимание и загриженост треба да се посвети во образованието и системот за обуки кои би требало повеќе да се вклучи во образовните програми и во обуките за административни службеници. Исто така, треба да се работи и на подигнување на свеста кај нашите политички лидери за да се ангажираат повеќе на полето на сајбер безбедност. Главната цел е да ја подигнеме свеста за безбедност на информации во нашата држава, како на корисниците, така и на снабдувачите на мрежни уреди, софтвер и интернет пристап и на самите вработени во администрацијата.

Ве молиме, споделете ги со нас Вашите ставови за:

13. Дали треба учениците во нашите училишта да имаат програма за сајбер безбедност и сомнителни онлајн содржини?

14. Дали сметате дека административните службеници треба да добијат елементарно знаење за препознавање и одбрана на напади од сајбер безбедносен карактер?

15. Како би можела македонската Влада и приватните субјекти да изградат висококвалитетни професионалци за сајбер безбедност?

МИНИМИЗИРАЊЕ НА ВЛИЈАНИЕТО НА САЈБЕР ИНЦИДЕНТИТЕ И ЗАКАНИТЕ

„37% од најчести типови на малициозни прикачувања преку е-пошта се .doc и .dot, а следен најчесто користен е .exe со 19,5 %.“

Мерките за минимизирање на влијанието на сајбер инцидентите и заканите можат да вклучат собирање на информации за актери насочени кон Република Северна Македонија, споделување совети за непријателска активност помеѓу вклучените субјекти во одбрана на мрежи или блокирање на познати злонамерни актери. MKD-CIRT и другите сектори на министерствата во нашата земја веќе тесно соработуваат со меѓународните партнери за споделување информации, со цел да се изгради поддршка за меѓународни правила и норми за регулирање на одговорното користење на сајбер просторот.

Ве молиме споделете ги со нас Вашите ставови за:

16. Какви промени може да направи Владата за да ја спречи можноста за делување на злонамерни сајбер актери?

17. Како владите и приватните субјекти можат да ја подобрат проактивноста при идентификацијата и спречувањето на сајбер ризиците на основните приватни мрежи?

18. Кои приватни мрежи треба да се сметаат за критични системи на кои им треба посилна сајбер заштита?

ЗАКЛУЧОК

Остварувањето на сајбер безбедноста е фундаментална задача на државата во безбедносна средина во која државните институции треба да одговорат адекватно со соодветни сајбер безбедносни ресурси. Нашата определба е сите граѓани да се вклучат во градењето на сајбер безбедноста во онлајн заедницата и економијата. Новата стратегија за сајбер безбедност ќе не однесе напред на ова поле, но би било нереалистички да се очекува од Стратегијата да ги реши сите проблеми. Само добро дефиниран опсег кој се фокусира на безбедноста на дигиталните активности осигурува дека може да постигнеме значајни промени во насока на подобра заштита на сите нас.

Однапред Ви благодариме за вашиот интерес и придонес за развојот на новата Национална стратегија за сајбер безбедност и со нетрпение очекуваме да го слушнеме и Вашето мислење.

ПОСТАВЕНИТЕ ПРАШАЊА:

1. Каков е Вашиот став за заканите во сајбер просторот кај нас?
2. На кои закани треба да се фокусира Владата?
3. Дали се согласувате со нашето разбирање во однос на тоа кој одговорен за управување со сајбер ризиците во економијата?
4. Дали мислите дека Владата треба да има повеќе одговорност?
5. Дали сметате дека Владата може да стори повеќе за да се соочи со компјутерскиот криминал
6. Каква улога треба да има Владата во решавањето на потенцијалните закани за институциите и бизнисите лоцирани во Република Северна Македонија?Како Владата може да ја задржи довербата во македонските граѓани во процесот на развој на своите сајбер безбедносни капацитети?
7. Дали имаме потреба од Агенција за сајбер безбедност во државата и кои, според вас, би биле нејзините надлежности?
8. Дали имаме потреба од Агенција за сајбер безбедност во државата и кои, според вас, би биле нејзините надлежности?
9. Каква улога можат да имаат Владата и индустријата во поддршката на сајбер безбедноста на потрошувачите?
10. На кој начин Владата и бизнисите можат да ја зголемат безбедноста, квалитетот и ефективноста на сајбер безбедноста и дигиталните понуди?
11. За кои конкретни пазарни стимулации или регулаторни промени би било добро Владата да размисли?
12. Што треба да се направи за сајбер безбедноста да биде „вградена“ во дигиталните производи и услуги?
13. Дали треба учениците во нашите училишта да имаат програма за сајбер безбедност и сомнителни онлајн содржини?
14. Дали сметате дека административните службеници треба да добијат елементарно знаење за препознавање и одбрана на напади од сајбер безбедносен карактер?
15. Како би можела македонската Влада и приватните субјекти да изградат висококвалитетни професионалци за сајбер безбедност?
16. Какви промени може да направи Владата за да ја спречи можноста за делување на злонамерни сајбер актери?
17. Како владите и приватните субјекти можат да ја подобрат проактивноста при идентификацијата и спречувањето на сајбер ризиците на основните приватни мрежи?
18. Кои приватни мрежи треба да се сметаат за критични системи на кои им треба посилна сајбер заштита?