Упатство за користење на шема за сертификација САЈБЕР ОДГОВОРНА ОРГАНИЗАЦИЈА

Верзија 1.1, 09.12.2021 година

Содржина

Вовед

Почитувани, пред вас е Упатство за користење на шема за сертификација во областа на сајбер-безбедност под име „Сајбер Одговорна Организација“.

„Сајбер одговорна организација“ е сертификациска шема предложена од Агенцијата за електронски комуникации и Националниот центар за одговор на компјутерски инциденти MKD-CIRT, која има за цел да им помогне на организациите во државата да се заштитат од најчестите сајбер (кибер) напади и да имплементираат минимална група на контроли за заштита.

Шемата за сертификација „Сајбер одговорна организација“ што Ви ја предлагаме е одобрена како активност вклучена во Годишна програма за работа на MKD-CIRT за 2021/2022 година, од страна на Владата на РСМ.

Предложената шема дава насоки за заштита од широк спектар на најчести сајбер напади, па затоа Ве охрабруваме да ја прифатите, имплементирате и користите во вашето секојдневно работење. Ова е важно затоа што ранливоста на едноставни напади може да доведе до посериозни последици за организацијата како финансиска и репутациска штета.

Оваа сертификациска шема или рамка е наменета за сите организации во државата, независно од големината. Дел од оваа шема е Прашалник за самооценување што организацијата самостојно го пополнува со одговарање на прашањата. Прашањата се поделени во неколку теми, секоја од нив од основно значење за сајбер безбедноста во организацијата. Преку одговарање на прашањата, организациите ќе можат да детектираат технички и организациски контроли со чие користење ќе ја подобрат безбедноста. Пополнетиот Прашалник електронски потпишан се испраќа до MKD-CIRT на проверка на адреса за е-пошта info@mkd-cirt.mk или contact@mkd-cirt.mk. Прашалникот можете да го преземете и од веб-страницата на центарот за локално пополнување. Во случај на исполнување на Услови за сертификација за „Сајбер одговорна организација“ дадени во прилог на овој документ, Агенцијата за електронски комуникации и MKD-CIRT ќе и издаде на организацијата сертификат и бедж кој ќе може да го постави на својата веб страница и да го користи како знак за препознавање на заложбите на организацијата да ги заштити своето работење, вработените, услугите и корисниците од најчестите сајбер закани и напади.

MKD-CIRT на својата официјална веб страница https://mkd-cirt.mk ќе објавува листа со организации кои имаат валиден сертификат. Сертификатот за „Сајбер одговорна организација„ е со важност од 12 месеци. Организацијата која што еднаш добила сертификат, може повторно да го продолжи сертификатот со поднесување за проверка на ажуриран пополнет Прашалник за само оценување.

Шемата за сертификација „Сајбер одговорна организација“ е отворена и бесплатна за користење за сите организации во земјата, независно дали станува збор за приватна или државна компанија, микро, мало или средно претпријатие. Ова упатство и шемата можете да ги користите како насоки за тоа од каде да започнете со воведување на сајбер безбедносни мерки во организацијата. Оваа шема не е замена за воведување на национални или меѓународни стандарди за информациска безбедност како ISO 27001, или целосно усогласување со побарувањата на европската регулатива за заштита на (лични) податоци GDPR и националните закони. Шемата може да ви помогне во воведување на погоре спомнатите национални и меѓународни стандарди и побарувања.

Што е Сајбер одговорна организација?

Со цел да се мотивираат организациите да имплементираат мерки и добри практики за сајбер безбедност во своето работење, MKD-CIRT воведува Сертификација и Бец за Сајбер одговорна организација, кои ќе овозможат јасно препознавање на организациите што успешно ќе го завршат процесот на самооценување на своето работење во областа на сајбер-безбедност.

Бецот за Сајбер одговорна организација е визуелна ознака што секоја организација која успешно го завршила процесот за сертификација ќе може да го постави на својата на веб-страница и да го користи за свои потреби. На тој начин на своите корисници на производи и услуги ќе им предочи дека станува збор за организација што имплементира мерки и контроли за сајбер безбедност и следи добри практики во своето работење, согласно успешно завршениот процес за сертификација.

Бецот ќе биде поставен само кај организациите што доброволно и самостојно ќе се пријават за сертификација за „Сајбер одговорна организација“ и кои успешно го завршиле тој процес.

Придобивки

Процесот за сертификација и за самооценување ви дава заштита од широк спектар на најчести сајбер напади. Ова е важно затоа што ранливоста на едноставни напади може да ве обележи како цел на сајбер криминалци.

Сертификацијата ви дава потврда дека преземените мерки за одбрана ќе ја заштитат организацијата од мнозинството најчестите сајбер напади, едноставно затоа што овие напади бараат цели кои не ги имаат воспоставените технички контроли што се дел од процесот на самооценување и сертификација за „Сајбер одговорна организација“. Услугата за „Сајбер одговорна организација“ ви покажува како да ги имплементирате основните мерки и контроли за сајбер заштита и да ги спречите најчестите напади.

Поволности за организацијата

- Вашата организација е дел од листата на сертифицирани сајбер одговорни организации на MKD-CIRT
- Зголемување на посетите на Вашата веб страница и информирање за вашата организација како одговорна организација преку промотивните активности на MKD-CIRT
- Зголемена доверба кај постојните и нови корисници на вашите производи и услуги
- Зголемена препознатливост и доверба во вашата организација

Што бецот не претставува

Бецот не претставува потврда за успешна надворешна проверка за усогласеност на работењето на организацијата. Организацијата самостојно и доброволно изјавува дека ги користи најдобрите практики за сајбер-безбедноста во работењето.

Процедура за сертификација за „Сајбер одговорна организација“

Услугата за сертификација е достапна на веб-страницата на центарот на https://mkd-cirt.mk/odgovorno-rabotenje-na-internet/

Процедурата за сертификација и добивање на сертификат и бец за „Сајбер одговорна организација“ ги вклучува следните чекори:

- Потврдете дека вашите информациски и ИКТ системи се соодветно безбедни и ги исполнуваат барањата од шемата за сертификација „Сајбер одговорна организација“,
- Пополнете го онлајн прашалникот достапен на нашиот веб сајт https://mkd-cirt.mk. Потоа преземете го локално кај вас и потпишете го со електронски потпис од одговорното лице. Следно е да го испратите на адреса за е-пошта info@mkd-cirt.mk или contact@mkd-cirt.mk. Прашалникот може да го преземете од веб-страницата на центарот за локално пополнување, и потоа повторно да го испратите до нас.

Стручната служба на MKD-CIRT ќе ги провери внесените одговори согласно објавените Услови за сертификација за „Сајбер одговорна организација“ кои се објавени и ќе се ажурираат на веб страница на центарот и кои се дадени и во овој документ. Доколку пополнетиот прашалник ги исполнува барањата, MKD-CIRT ќе ви испрати информација и потврда/сертификат за евидентирање на вашата организација како „Сајбер одговорна организација“. Дополнително ќе Ви испратиме и насоки за користење и поставување на бец на вашата веб страница за препознавање на вашите заложби за заштита на корисниците на ваши услуги и самата организација. Периодот за ре-сертификација е 12 месеци. Во случај ако доставените одговори не ги исполнуваат Условите за сертификација за сајбер одговорна организација, MKD-CIRT ќе испрати известување до подносителот со насоки за следни чекори.

Упатство за пополнување на прашалник за самооценување како дел од шема за сертификација „Сајбер одговорна организација“

Од што всушност се состои шемата за сертификација „Сајбер одговорна организација“? Постојат неколку области за технички и организациски мерки и контроли што ќе треба да ги имплементирате и користите, со цел намалување на ризиците по сајбер безбедност за вашата организација, и тоа:

- Општ дел
- Огнени (заштитни) ѕидови / Firewalls и Безбедно мрежно работење;
- Безбедни конфигурации;
- Надградби и закрпи;
- Контрола на пристап, кориснички и администраторски сметки;
- Вируси, малициозен софтвер, сајбер напади и инциденти;

Сертификациската шема „Сајбер одговорна организација“ е збир на барања во овие контролни области и ќе треба да бидете сигурни дека вашите системи и софтвер ги исполнуваат овие пред да преминете на следната фаза на сертификација (следете ги насоките во остатокот од овој документ). Бидете сигурни дека бараните контроли и процеси се дефинирани, опишани и имплементирани бидејќи со вашиот потпис самата организација декларира дека ги задоволува минималните барања на оваа сертификациска шема.

Во продолжение следува појаснување за барањата за одговарање на овие прашања. Секое прашање е проследено со појаснување. Кај некои од прашањата ќе го сретнете и знакот ℹ каде се дадени дополнителни информации за насоки и прифатлив одговор за исполнување на барањето.

Општ дел

Во овој дел од прашалникот се побарува од организацијата да внесе општи податоци како целосен назив, седиште, матичен/регистарски број, дејност со избор од листата, главна веб-страница, име и презиме на одговорното лице, како и статистички податоци за организацијата.

Ако организацијата овозможува за свои вработени да работат од дома, треба да им овозможи безбеден пристап до организациските системи, документи и информации. Ова влијае на контролите за заштита на уредите што овие вработени ќе ги користат за далечински пристап до организацијата, како и на мерките и алатките кои организацијата треба да ги воведе на своја страна, како VPN пристап и задолжителна антивирусна заштита на уредите со кои вработените пристапуваат од далечина.

Опсег на барањето

Во овој дел од прашалникот потребно е да го дефинирате опсегот на вашата сертификација. Ова одредува што е предмет на декларацијата за сертификација според шемата „Сајбер одговорна организација“. Често опсегот се дефинира со физичка локација, како што е вашата главна канцеларија, но можете да изберете дали да вклучите или не и други делови или подружници. Пополнувањето на останатите делови од прашалникот ќе се однесува на сите ИТ основни средства, мрежи и мрежна опрема, политики, процеси и апликации кои се користат во наведениот опсег., како што се и оддалечените канцеларии. Информациите за користени оперативни системи се важни за организацијата да покаже дека користи нови оперативни системи кои имаат активна поддршка од производителите. Многу е важно организацијата да има идентификувано лице кое е одговорно за управување со оваа опрема и ИТ основните средства. Вообичаено тоа лице ќе биде одговорно или ќе соработува со друго лице кое е одговорно за информацискатa безбедност во организацијата.

Огнени (заштитни) ѕидови / firewalls и безбедно мрежно работење

Безбедноста на компјутерската мрежа и услугите што се овозможени преку истата се од клучно значење за сајбер безбедноста на една организација, бидејќи нападите и инцидентите се случуваат преку неа. Една одговорна организацијата мора задолжително да го заштити своето работење со користење на Firewall (Заштитен/огнен ѕид), да воведе задолжителна промена на првичните лозинки и кориснички сметки на активната мрежна опрема пред истата да почне да се користи, и при тоа да користи силни лозинки. Организацијата треба да има ажурирана листа на дозволени сервиси или услуги до кој надворешните корисници пристапуваат преку овие огнени ѕидови, и треба да применува добра пракса за забрана на сите услуги и затворање на сите мрежни порти на Firewall кои не се користат. На тој начин организацијата го намалува ризикот од напади кои злоупотребуваат отворени услуги и порти кои не и служат на организацијата и кои не се под надзор. Многу важно е организацијата да користи софтверски Firewall на сите клиентски ИТ уреди кои излегуваат на интернет преку компјутерската мрежа на организацијата.

Безбедни конфигурации

Со основна стандардна инсталација и на почетокот на користењето, компјутерите, рутерите и другите информатички и мрежни основни средства најчесто не се доволно заштитени. Тие често можат да вклучуваат административна сметка со корисничко име Admin и стандардна, јавно позната лозинка, како и овозможена една или повеќе дополнителни и непотребни кориснички сметки (често со високи нивоа на пристап и привилегии) и претходно инсталирани, но непотребни програми, апликации или услуги (т.н. bloatware).Сите тие претставуваат безбедносни ризици кои организацијата треба да ги сведе на минимум.

Со одговарање на прашањата од овој дел на прашалникот, организацијата треба да појасни какви контролни, технички и организациски мерки презема за да ја подобри сајбер безбедноста на организацијата. Овие мерки вклучуваат задолжително користење на силни лозинки, креирање на индивидуални кориснички сметки за вработените, достапност на апликации,

документи и податоци преку Виртуелна приватна мрежа (VPN – Virtual Private Network) за вработените што работат од дома и за надворешните корисници. Организацијата треба да применува добра пракса како блокирање на автоматско извршување при вклучување на USB стик или DVD диск, како и забрана за работа со меморијата од мобилниот телефон кога тој се приклучува на компјутерот, и користење на ова поврзување преку USB кабел исклучиво за полнење на батеријата од мобилниот телефон.

На сите ИТ основни средства како компјутери, лаптопи, мобилни телефони и таблети треба да се инсталирани само оние апликации и услуги кои се потребни за вработените да ги извршуваат непречено работите задачи. Мора да постои сегрегација меѓу уредите кои се користат за службени потреби и колку е можно по строга забрана за нивно користење за приватни потреби, како и оневозможување на самостојна инсталација на нови апликации и услуги на уредите без одобрување на организацијата, т.е. одговорното лице за информациска безбедност.

Кога се креираат кориснички сметки, организацијата треба да го применува правилото за доделување на привилегии за една корисничка сметка што се само минимално доволни за вработениот/корисникот квалитетно и навремено да ја заврши работната обврска. Доделување на непотребни повисоки нивоа на привилегии го зголемува ризикот од инфекција на уредот, мрежата и системите на организацијата со можни финансиски и други штети.

Прашањата во овој дел се однесуваат на: Сервери, компјутери, лаптопи, таблети и мобилни телефони.

Надградби и закрпи

За да ја заштитите организацијата, треба да обезбедите навремено ажурирање на апликативниот и системскиот софтвер, како и на т.н. firmware за сите ИТ уреди и основни средства во организацијата. Ажурирањето подразбира инсталирање нанови закрпи и безбедносни и функционални надоградби. Ако на кој било од вашите уреди кои се во опсег на сертификацијата користите оперативен систем што повеќе не е поддржан од производителот (на пр. Microsoft Windows XP / Vista / 2003, Ubuntu 17.10 или постар) и немате обезбедено редовни надградби од други доверливи извори, тогаш не ги исполнувате условите за успешно оценување. Мобилните телефони и таблетите што се во опсег исто така мора да користат оперативен систем што сè уште е поддржан од производителот. и вклучено ажурирање.

Секоја одговорна организација мора задолжително да користи исклучиво лиценцирани решенија, апликации кои имаат поддршка од производител или добавувач, како и да има дефинирано процес за задолжително инсталирање на критични надградби или закрпи објавени од производителите, во краток рок.

Прашањата во овој дел се однесуваат на: Сервери, компјутери, лаптопи, таблети, мобилни телефони, рутери и заштитени ѕидови

Контрола на пристап

Кориснички сметки

Една сајбер одговорна организација треба да го применува правилото за пристап со најниски можни привилегии за корисникот или вработениот да може непречено да ги заврши работните задачи и обврски. Важно е да им се овозможи на корисниците и вработените пристап до сите ресурси и податоци потребни за нивните улоги и работни места, но не и повеќе од потребниот минимум. Сите корисници треба да имаат единствени сметки и не треба да извршуваат секојдневни задачи како што се фактурирање или работа со е-пошта додека се најавени како

корисник со администраторски привилегии. Користењето на кориснички сметки со високо ниво на привилегии за извршување на секојдневните задачи е ризик за компромитација на компјутерот и преку него на целата организација. Користењето на „обичните“ кориснички сметки кои немаат привилегии за инсталација на софтвер помагаат да се спречи инфекција на уредот со вирус или друг штетен софтвер.

Организацијата треба да води евиденција за користени ИТ основни средства за секој вработен.

Прашањата во овој дел се однесуваат на: Сервери, компјутери, лаптопи, таблети и мобилни телефони.

Администраторски сметки

За администрација на системите, услугите и апликациите, организацијата може да има свои вработени или да ангажира надворешна стручна поддршка. Во секој случај мора да има процес за одобрување/доделување на администраторски пристап преку посебни кориснички сметки и профили што ќе се користат исклучиво за администраторски активности (инсталација на надградби и закрпи, промени во конфигурации и сл.). Многу важно е организацијата да има евиденција за овие активности.

Вируси, малициозен софтвер, сајбер напади и инциденти

Заштита од малвер

Малициозен софтвер (како што се компјутерски вируси) обично се користи за кражба на информации или за нанесување на финансиска и друг вид штета на организацијата. Антивирусните и антималвер софтверски решенија се достапни од комерцијални добавувачи, но има и некои што се бесплатни или се дел од пакет, на пр. оперативен систем.

Една сајбер одговорна организација треба да инвестира во квалитетна антивирус и антималвер заштита.

Најдобра заштита од рансомвер и понатаму е организацијата да има валиден и ажуриран бекап/заштитена копија од најважните податоци.

За организациите кои не дозволуваат подолготрајни прекини во работењето и достапноста на услугите за корисниците, потребно е да се имплементираат и периодично да се тестираат планови за опоравување и планови за континуитет во работењето. Организациите што ќе декларираат дека ги имаат овие контроли и процеси во своето работење, покажуваат високо ниво на сајбер заштита.

Резервна копија од важни податоци

Една сајбер одговорна организација мора задолжително да има процедура или процес за редовен бекап на важни податоци и системи. При тоа една опција е да го користите т.н. „Правило 1,2,3“, со кое организацијата треба да има 3 копии од важните податоци (првата копија е оригиналот - податоците снимени на уредите што се користа за работа, како и 2 резервни копии) на два различни медиуми (USB или надворешен диск, во облак како Google Drive, Microsoft Azure и сл, или на магнетна лента) со една од копиите надвор од физичката локацијата за враќање од катастрофи и од примарната физичка локација на организацијата. Честотата на снимање копии од податоците ќе зависи од самата организацијата, но мора задолжително да се прави целосен бекап на податоците во периоди не подолги од 1 месец. Се препорачува дневно и неделно снимање на резервни копии од податоците.

Организацијата мора задолжително да има подготвено, пропишано и периодично да тестира Планови за опоравување од катастрофи (пожар, земјотрес и сл.) и Планови за континуитет на деловното работење. Организацијата мора да и ма дефинирано т.н. време за опоравување и прифатливо време за прекин во работата. Соодветно на овие времиња, потребно е да се прилагодат плановите, и во секој план да се дефинира организацискиот тим кој ќе ги реализира. Повеќе информации и насоки за плановите и ризиците ќе најдете на порталот на MKD-CIRT за обуки: https://lms.mkd-cirt.mk.

Сајбер напади и инциденти

Сајбер одговорна организација мора да има воспоставено процес за пријава на сомнителни активности и инциденти, до дедицирано лице во организацијата кое е одговорно за информациска безбедност, или за ИТ системите на организацијата. Организацијата мора да вложува во едукација на своите вработени за значењето на користење добри пракси за сајбер заштита.

Услови за сертификација за „Сајбер одговорна организација“

Основен услов за сертификација е претставниците на организацијата точно и искрено да ги одговараат прашањата и да го пополнат онлајн прашалникот.

Следува табела со потребни одговори од Прашалникот за самооценување со цел организацијата да ги исполни условите за добивање на сертификат како „Сајбер одговорна организација“

Прашање	Прифатлив одговор
A.1.1 Назив на организација	Точен назив – целосно име на организацијата
A.1.2 Регистарски (матичен) број	Точен регистарски/матичен број запишан во Централен регистар
A.1.3 Адреса на организација	Адреса на седиште на организацијата
A.1.4 Дејност на вашата организација	Точен избор/внесен текст согласно регистрација во Централен регистар
A.1.5 Адреса за веб-седиште на организацијата	Точна адреса согласно регистрација во Централен регистар
A.1.6 Емеил адреса	Адреса за е-пошта на одговорно лице во организацијата, потписник
A.1.7 Големина на организацијата	Точен избор од понудените опции
A.1.8 Колку вработени работат од дома	Избор на реален избор за големина на организацијата
A.1.9 Дали за прв пат поднесувате барање за проверка	Точен избор од понудените опции
A.1.10 Која е главна причина за поднесување на барањето	Главната причина зошто аплицирате за сертификација. Ако има повеќе причини, изберете ја онаа што ви е најважна

Опсег на барањето	
А.2.1 Дали опсегот на оваа проценка ја опфаќа целата ваша организација?	За избира од понудени опции
А.2.2 Ако опсегот не е целата организација, внесете опис за опсегот	Вашиот опис за опсег треба да дава детали за сите области на вашето работење. Се пополнува ако на 2.1. одговорите со Не
А.2.3 Опис на географските локации на вашата организација	Точен опис на реални локации за организацијата
А.2.4 Количини на лаптопи, компјутери и сервери во рамките на проценатa.	Точен опис за реални количини, типови и модели на ИТ основни средства во организацијата
А.2.5 Количини на таблети и мобилни телефони во рамките на проценатa.	Точен опис за реални количини, типови и модели на ИТ основни средства во организацијата
А.2.6 Список на мрежи што ќе бидат во опсегот на оваа проценка	Точен опис за компјутерските мрежи кои се вклучени во опсегот за работа на организацијата што е предмет на сертификација
А.2.7 Список на мрежна опрема	Треба да ја вклучите целата опрема што го контролира протокот на податоци, како што се рутери и заштитени ѕидови. Не треба да вклучувате свичеви или безжични пристапни точки за пристап што не содржат заштитен ѕид или не го насочуваат сообраќајот на Интернет.
А.2.8 Име, презиме и улога на лицето кое е одговорно за управување со информациските системи на организацијата	Организацијата мора да има формално одредено вработено или ангажирано лице кое е одговорно за управување со ИТ системите и нивната безбедност

Безбедно деловно работење	
Огнени (заштитни) ѕидови / Firewalls	
А3.1 Заштитен ѕид на границите помеѓу внатрешните мрежи и интернетот	Задолжително барање. Организацијата мора да користи Firewall за заштита на својата мрежа од интернет
А.3.2 Промена за почетни/стандардни лозинки кои се поставени со набавка на уреди и опрема?	Точен опис. Задолжително треба да се променат сите стандардни / default лозинки пред користење на опремата
А.3.3 Минимална комплексност на лозинките	Организацијата мора да воведе забрана за

	користење на лозинки со помалку од 8 карактери и ниско ниво на комплексност
А.3.4 Постапка или процедура за промена на пробиена лозинка	Точен опис. Задолжително треба да има установен процес за пријава и промена на компромитирани сметки и лозинки
А.3.5 Објава на јавни услуги и отворање на порти на Firewall само за реални потреби	Организацијата треба да користи принцип на овозможен надворешен пристап само за тие услуги кои постојат. Секоја услуга или порта што непотребно е отворена на Firewall го зголемува ризикот за напади
А.3.6 Проверка и ажурирање на овозможени услуги на Firewall	Точен опис. Организацијата мора да има воспоставено процес или пракса за периодична проверка и ажурирање на отворени порти и овозможени услуги на Firewall. Се пополнува ако на А.3.5. е одговорено со Да.
А.3.7 Конфигурациј ана рутери за блокирање на услуги и порти пто не с екористат	Стандардно, повеќето заштитени ѕидови го блокираат пристапот на сите услуги од Интернет што не се користат, но треба да ги проверите поставките за заштитен ѕид
А.3.8 Дали делот за конфигураиција на рутери и заштитни ѕидови е достапна преку интернет?	Понекогаш организациите го конфигурираат својот заштитен ѕид за да им дозволат на другите (како на пр. што е компанија за ИТ поддршка) да ги менуваат поставките преку Интернет. Препорака е да се оневозможи директен пристап од јавна мрежа на интернет
А.3.9 Документиран одобрен процес за пристап	Појаснување доколку на А.3.9 е одговорено со Да
А.3.10 Дали за пристап се користи 2FA или листа на дозволени јавни IP адреси	Точен опис. Појаснување доколку на А.3.9 е одговорено со Да
А.3.11 Firewall на компјутерите	Сите кориснички уреди (компјутери, лаптопи и сл.) треба да се заштитени со софтверски Firewall

Безбедни конфигурации	
А.4.1 Дали на вашите лаптопи, компјутери, сервери, таблети и мобилни телефони го отстранивте целиот софтвер што не го користите (секаде каде што е можно)? Опишете како го постигнувате ова.	Точен опис. Организацијата треба задолжително да го отстрани целиот непотребен софтвер од клиентските уреди
А.4.2 Дали проверувате дека сите сите компјутери имаат само кориснички сметки што ги користите во тековното работење?	Мора да отстраните или оневозможите кориснички сметки што не се потребни за секојдневна употреба на сите уреди.
А.4.3 Дали сте ја сменила стандардната лозинка за сите кориснички и административни сметки на сите ваши лаптопи, компјутери, сервери, таблети и паметни телефони во лозинка од 8 или повеќе карактери што тешко може да се погоди?	Силна лозинка е таа што е тешко да се погоди. Таа треба да е единствена и да не се користи кај повеќе кориснички сметки, и да не е составена од предвидливи зборови, како што се „Password“ или „administrator“, или да вклучува бројни

	секвенци како „12345678“.
А.4.4 Дали сите вработени и администратори користат лозинки од најмалку 8 карактери?	Колку е подолга лозинката, толку е потешко за компјутерските криминалци да ја погодат (напади со многубројни пробувања на предвидливи лозинки, т.н. Brute-force напад)
А.4.5 Дали имате апликации или софтвер преку кои се овозможува пристап до чувствителни или важни информации и документи за корисници што пристапуваат преку интернет	Вашата организација може да има софтвер што им овозможува на луѓето надвор од компанијата преку Интернет да пристапуваат до информации за вашата организација преку надворешна услуга. Ова може да биде сервер за VPN, сервер за е-пошта или интернет апликација што им ја давате на вашите клиенти како производ или услуга.
А.4.6 Ако да, дали сите корисници на овие услуги користат лозинки од најмалку 8 карактери и дали вашите системи не ја ограничуваат должината на лозинката на помалку од 8 карактери?	Се пополнува само ако на А.4.5 се одговори со Да
А.4.7 Ако да, дали имате обезбедено начин или процедура за промена на лозинки од страна на надворешните корисници но и од организациските администратори, во случај на нивна компромитација?	Се пополнува само ако на А.4.5 се одговори со Да
А.4.8 Ако да, дали вашите системи се поставени на автоматско заклучување на корисничката сметка по пет или помалку неуспешни обиди за најавување или го ограничуваат бројот на обиди за најавување на не повеќе од десет во рок од пет минути?	Се пополнува само ако на А.4.5 се одговори со Да
А.4.9 Ако да, дали имате пишана политика за лозинка што се однесува на сите ваши корисници (внатрешни и надворешни), која периодично ја проверувате и ревидирате?	Се пополнува само ако на А.4.5 се одговори со Да
А.4.10 Дали на сите компјутери и ИТ уреди е исклучено „автоматско извршување (auto-run)“ и „автоматско репродукција (auto-play)“ за надворешните USB уреди и оптички дискови.	Прифатливо е да се избере опцијата каде што ќе се побара од корисникот да направи избор за тоа какво дејствие ќе се случи секој пат кога ќе вметне мемориски стик. Ако сте ја одбрале оваа опција, можете да одговорите ДА на ова прашање

Надградби и закрпи	
А.5.1 Дали сите оперативни системи на вашите уреди се поддржани од производител или добавувач што доставува редовни поправки и надградби за какви било безбедносни проблеми? Опишете.	Точен опис. Наведете ги оперативните системи што ги користите за да може да се процени и провери дали сите ваши оперативни системи сè уште имаат поддршка од производителите.
А.5.2 Дали сите канцелариски апликации што ги користите во организацијата и кои се	Точен опис. Наведете ги апликациите што ги користите за да се разбере начинот на

инсталирани на вашите уреди се поддржани од снабдувач што редовно објавува поправки и надградби за какви било безбедносни проблеми? Опишете.	поставување во вашата организација и за потврда дека сите ваши апликации имаат обезбедена поддршка.
А.5.3 Дали целокупниот софтвер е лиценциран во согласност со препораките на производителот?	Целиот софтвер мора да биде лиценциран. Прифатливо е да користите бесплатен и софтвер од тип „отворен извор“ (Open source), сè додека ги исполнувате сите услови за лиценцирање, подмирени права за негово користење и поддршка.
А.5.4 Дали сите важни или критични безбедносни ажурирања за оперативните системи се инсталирани во рок од 14 дена од објавувањето? Опишете.	Точен опис. Секоја сајбер одговорна организација задолжително треба да ги инсталира сите вакви надградби во одреден претходно договорен рок, на пр. две недели од денот на објава и јавна достапност од страна на производителот
А.5.5 Дали сите важни или критични безбедносни ажурирања за апликациите (вклучително и додатоци како на пример Java или Flash) се инсталирани во рок од 14 дена од објавувањето? Опишете	Точен опис. Секоја сајбер одговорна организација задолжително треба да ги инсталира сите вакви надградби во одреден претходно договорен рок, на пр. две недели од денот на објава и јавна достапност од страна на производителот.
А.5.6 Дали ги отстранивте од компјутерите и другите ИТ средства оние апликации кои повеќе немаат поддршка од производителот и за кои не можете да добивате редовни надградби и безбедносни поправки?	Задолжително треба да ги отстраните постарите апликации од уредите во моментот кога ќе дознаете дека производителот веќе не ги поддржува.

Контрола на пристап	
А.6.1 Дали на корисниците им се доделуваат кориснички сметки за пристап и користење на ИТ уредите и апликациите само по претходно одобрување од одговорно лице?	Точен опис. Мора да се осигурате дека корисничките сметки што се користат за најавувања на компјутерите, како и кориснички или администраторски сметки на сервери, се доделени само откако ќе бидат одобрени од лице со одговорна улога во организацијата.
А.6.2 Дали можете да пристапите до лаптопите, компјутерите и серверите во вашата организација, како и до апликациите што се инсталирани на нив, САМО преку внесување на уникатно корисничко име и лозинка?	Мора да бидете сигурни дека не може да се пристапи до ниту еден важен уред без да се внесе корисничко име и лозинка. Корисниците не смеат да споделуваат сметки.
А.6.3 Како обезбедувате бришење или блокирање на кориснички сметки, како и раздолжување со компјутер или друг ИТ уред, за вработени кои повеќе не се во вашата организација или сменile работно место?	Точен опис. Кога вработен ќе ја напушти вашата организација, треба да спречите пристап до кој било од вашите системи. Истовремено треба да обезбедите информациите, документите и податоците што ги користел тој вработен да останат во владеење на организацијата
А.6.4 Дали обезбедувате дека вработените	Точен опис. Кога некој вработен го менува

имаат само привилегии што им се потребни за да ја извршат својата тековна работа?	работното место, можеби ќе треба да ги промените неговите привилегии за пристап до системите, апликациите, документите и податоците.
А.6.5 Дали имате процес за доделување на администраторски пристап до системите и услугите на организацијата за вработено или надворешно ангажирнао лице?	Точен опис. Мора да имате формален, запишан процес што го следите кога одлучувате да му дадете некому пристап до системите на администраторско ниво. Овој процес може да вклучува одобрување од лице кое е сопственик / директор...
А.6.6 Како обезбедувате дека вработените користат администраторски сметки само за извршување на администраторски активности	Точен опис. Мора да се осигурате дека администраторските сметки се користат само кога е апсолутно неизбежно, како на пример при инсталирање на софтвер.
А.6.7 Како забранувате користење на администраторските сметки за пристап до е-пошта или прелистување на веб?	Точен опис. Мора да обезбедите администраторските сметки да не се користат за пристап до веб-страници или работа со е-пошта.
А.6.8 Дали водите евиденција за тоа кои корисници имаат администраторски сметки во вашата организација?	Една сајбер одговорна организација треба да води список или да има ажурирана и точна евиденција на сите луѓе на кои им биле доделени администраторски сметки, со податоци за корисничко име, систем, услуга, уред до кој им е доделен администраторскиот пристап, како и електронска евиденција (логови)
А.6.9 Дали редовно или периодично проверувате и ревидирате кој треба да има администраторски пристап?	Мора редовно да го прегледувате списокот со луѓе со администраторски пристап. Во зависност од вашето работење, ова може да се прави на одреден временски период, на пр. месечно или годишно
А.6.10 Дали за администраторски пристап користите дво-факторска автентикација?	Ако вашите системи поддржуваат автентикација со користење на два фактори (каде покрај лозинката за успешна најава е потребно да добиете текстуална порака, еднократен код, или да користите читач за отпечаток од прст или имате имплементирано препознавање на лице), тогаш треба да го овозможите овој начин за најава и пристап за администраторските сметки.

Вируси, малициозен софтвер, сајбер напади и инциденти	
А.7.1 Дали сите ваши сервери, компјутери, лаптопи, таблети и мобилни телефони се заштитени од малициозен софтвер со ...	Изберете една или повеќе од понудените опции.
А.7.2 (А) Таму каде што имате инсталирано	Се пополнува ако на А.7.1 е избрано А

антивирус или друг софтвер за заштита од малвер (МАЛициозен софтВЕР), дали истиот е конфигуриран да се ажурира најмалку еднаш дневно и автоматски да ги скенира датотеките во системот/уредот?	
А.7.3 (А) Таму каде што имате инсталирано антивирус или друг софтвер за заштита од малвер (МАЛициозен софтВЕР), дали истиот е конфигуриран да ги скенира веб-страниците што ги посетувате и да ве предупредува за пристап до потенцијално штетни веб-страници?	Се пополнува ако на А.7.1 е избрано А
А.7.4 (Б) Кога за преземање и инсталација на апликации користите официјални продавници или инсталирате апликации со валиден сертификат и потпис од производителот, дали на корисниците им е оневозможено да инсталираат непотпишани апликации или апликации преземени од сомнителни извори?	Се пополнува ако на А.7.1 е избрано Б
А.7.5 (Б) Кога за преземање и инсталација користите официјални продавници за апликации или инсталирате апликации со валиден сертификат и потпис од производителот, дали ги ограничувате корисниците да инсталираат апликации само одобрени од вашата организација и дали евиденција/листа на одобрени апликации?	Се пополнува ако на А.7.1 е избрано Б
А.7.6 (В) Доколку користите изолација на апликации преку sandoxing, дали обезбедувате забрана овие апликации да пристапат до организациските системи за складирање на податоци, чувствителните документи и надворешни уреди, како и до локалната компјутерска мрежа на организацијата?	Се пополнува ако на А.7.1 е избрано В. Точен опис.
А.7.7 Дали снимате резервни копии од важните податоци? Опишете.	Точен опис. Една сајбер одговорна организација мора задолжително да чува резервна копија од најважните податоци
А.7.8 Планови за опоравување од катастрофи и Планови за континуитет во деловното работење	Точен опис. Организацијата мора задолжително да има подготвено, пропишано и периодично да тестира Планови за опоравување од катастрофи (пожар, земјотрес и сл.) и Планови за континуитет на деловното работење.
А.7.9 Дали имате воспоставено процес или процедура за пријава на сомнителни пораки, инциденти и активности од страна на вработени? Опишете.	Точен опис. Сајбер одговорна организација мора да има воспоставено процес за пријава на сомнителни активности и инциденти,
А.7.10 На кој начин ги едуцирате вработените за сајбер заканите на интернет и за користење на добри практики за сајбер заштита? Опишете.	Точен опис. Сајбер одговорна организација мора да вложува во едукација на своите вработе