АЕК
MKD-CIRT

АГЕНЦИЈА ЗА ЕЛЕКТРОНСКИ КОМУНИКАЦИИ

НАЦИОНАЛЕН ЦЕНТАР ЗА ОДГОВОР
НА КОМПЈУТЕРСКИ ИНЦИДЕНТИ

САЈБЕР-БЕЗБЕДНОСТ

ВОДИЧ ЗА МАЛИ И СРЕДНИ ПРЕТПРИЈАТИЈА

Верзија 1.0
октомври 2019 година

СОДРЖИНА

ПРЕДГОВОР

Овој водич е направен за да им помогне на микро, малите и средните претпријатија да се заштитат од најчестите сајбер-напади.

Секторот на микро, мали и средни претпријатија (ММСП) како целина е доминантен во македонската економија. Најновите податоци покажуваат дека 99,8% од претпријатијата припаѓаат во оваа група. Во 2013 година, 53.137 претпријатија биле ММСП, од кои 91,0% во земјата се микро претпријатија. ММСП, исто така, се најголемите работодавачи, обезбедувајќи 76,6% од вкупниот број вработувања.[1]

Во овој водич ќе најдете совети како да ја подобрите заштитата од најчестите видови сајбер-закани и сајбер-криминал. Водичот покрива 6 теми и секоја од нив содржи совети чија имплементација не побарува големи финансиски издатоци.

Ниту еден водич или упатство не може да ја гарантира заштитата од сите видови сајбер-напади, но овој документ е изработен во насока да објасни некои мерки за заштита на податоците, средствата и репутацијата на вашата организација.

Националниот центар за одговор на компјутерски инциденти MKD-CIRT како дел од Агенцијата за електронски комуникации, со овој водич и другите објавени документи и информации, работи активно на подигање на јавната свест за значењето на сајбер-безбедноста. Нашата мисија е да обезбедиме услови за безбедно користење на Интернет и онлајн работење.

Национален центар за одговор на компјутерски инциденти MKD-CIRT
Агенција за електронски комуникации

---

1) Национална стратегија за мали и средни претпријатија (2018-2023), http://economy.gov.mk/Upload/Documents/Strategija%20za%20MSP%20-%20finalna%20verzija%2003%2004%202018%20.pdf

1. РЕЗЕРВНА КОПИЈА НА ВАШИТЕ ПОДАТОЦИ (BACKUP)

Според најновата анкета на MKD-CIRT, 50% од граѓаните не прават бекап и само 11% снимаат резервни копии од важните податоци најмалку еднаш неделно.[2]

Размислете кои податоци се критични за вашето работење. Дали собирате и обработувате (лични) податоци за корисниците на вашите услуги и производи, или можеби евидентирате нарачки, фактури со банкарски сметки. Потоа размислете, колку долго би можеле да работите без нив.

Сите претпријатија треба да прават резервни копии на важните податоци, да се осигурат дека овие резервни копии се чуваат на безбедно место, истите се ажурирани и од нив можат да се вратат назад податоците. Креирањето на резервна копија обезбедува организацијата да може да продолжи со работа во случај на инциденти и прекини во достапноста на оригиналните податоци, во случаи на поплава, пожар, физичко оштетување или кражба на опрема и документи. Резервни копии на вашите податоци што можете брзо и целосно да ги повратите се најдобра заштита од сајбер-напади со софтвер за уцена - „рансомвер" (анг. ransomware).

СОВЕТ 1: ИДЕНТИФИКУВАЈТЕ ГИ ПОДАТОЦИТЕ ЗА КОИ ТРЕБА ДА НАПРАВИТЕ РЕЗЕРВНА КОПИЈА

Најпрво идентификувајте ги податоците кои се важни за вашето работење и без кои вашата организација не може да функционира. Често тоа се фактури, испратници и други документи со финансиски, лични и чувствителни податоци. Направете копија од овие податоци на надворешен уред и чувајте го на безбедно место подалеку од уредите на кои се запишани оригиналните податоци и документи.

2) Извештај од испитување на јавно мислење за примена на мерки за безбедност на Интернет, https://mkd-cirt.mk/2019/07/30/izveshtaj-od-ispituvanje-na-javnoto-mislenje-za-primena-na-merki-za-bezbednost-na-internet/

СОВЕТ 2: ЧУВАЈТЕ ЈА РЕЗЕРВНАТА КОПИЈА ПОДАЛЕКУ ОД РАБОТНОТО МЕСТО

Без разлика дали копијата е запишана на USB-стик, екстерен диск или посебен компјутер, ограничете го пристапот до нив така што:

- резервните копии да не бидат достапни за вработените
- уредите на кои тие се запишани, не се постојано поврзани (физички или преку локална компјутерска мрежа) на уредот на кој се наоѓаат оригиналните податоци

Доколку уредот за складирање каде е запишана резервната копија е постојано поврзан на локалната компјутерска мрежа, при инфекција со „рансомвер" или друг вид малициозен софтвер („малвер", анг. malware), малверот може автоматски да се пренесе и на уредот за складирање. Ова значи дека секоја таква резервна копија може да биде инфицирана, оставајќи ве без резервна копија од која би можеле да ги вратите податоците.

За поголема безбедност и отпорност, размислите за складирање на резервните копии на друга физичка локација, така што во случај на пожар или кражба нема да ја изгубите резервната копија. Решенијата за складирање во облак - cloud storage (види подолу) се економичен и ефикасен начин за да се постигне ова.

СОВЕТ 3: СКЛАДИРАЊЕ НА ПОДАТОЦИ ВО ОБЛАК

Голема веројатност е дека секојдневно користите услуги за складирање на податоци во облак. Доколку не користите ваш сопствен сервер за е-пошта, вашите електронски пораки се веќе „во облак" и се запишани на сервер надвор од организацијата. Многу често контактите запишани на мобилниот телефон автоматски се запишуваат во облак, исто како и копија од комуникацијата преку апликациите како Viber, Messenger и WhatsApp.

Услугата за складирање на податоци во облак значи дека давателот на услуги ги чува вашите податоци на негова инфраструктура достапна преку

Интернет. На тој начин податоците се физички одделени од вашата локација и се обезбедува складирање на податоци и обезбедување на веб-услуги без да инвестирате во скап хардвер. Дополнителна придобивка е високото ниво на достапност. Повеќето даватели на услуги за складирање на податоци во облак нудат бесплатен, но ограничен простор за складирање податоци, кој со доплата може да се зголеми.

СОВЕТ 4: ПРАВЕЊЕ БЕКАП КАКО ВАША СЕКОЈДНЕВНА АКТИВНОСТ

Решенијата за складирање преку мрежа или во облак овозможуваат автоматско правење на резервни копии без да поседувате напредни технички предзнаења. Автоматизираното правење резервни копии заштедува време и Ви гарантира дека секогаш ќе ги имате најновите верзиии на вашите документи.

Многу од овие решенија се лесни за инсталирање и прифатливи во однос на цената со оглед на заштитата на важните податоци што ја нудат. Анализирајте колкав капацитет Ви е потребен за складирање на резервната копија од важните податоци, без разлика дали складирањето ќе го правите во облак или локално на надворешен диск. При изборот на начинот на кој ќе ги запишувате податоците, многу важно е да утврдите кое е максималното време за враќање на податоците кое вашиот бизнис може да го поднесе. Користете ја оваа информација како дополнителен критериум за избор на начинот на складирање на резервната копија од податоците.

2. ЗАШТИТА ОД МАЛИЦИОЗЕН СОФТВЕР

Малициозен софтвер (познат како „малвер" - анг. malware) е софтвер кој може да и наштети на вашата организација преку бришење на важни податоци, злоупотреба на вашите уреди за напади и уцени преку заклучување или шифрирање на документите, како што беше неодамнешната појава на WannaCry и NonPetya. Најпозната форма на малициозен софтвер се

вирусите, програми кои се само-реплицираат и го заразуваат легитимниот софтвер.

Следуваат 5 едноставни совети за имплементирање кои можат да помогнат во заштита од малициозен софтвер и спречување на штета по работата на организацијата.

СОВЕТ 1: КОНТИНУИРАНО АКТИВЕН И АЖУРИРАН АНТИВИРУСЕН СОФТВЕР

Антивирусниот софтвер кој честопати е вклучен бесплатно во популарните оперативни системи, треба да се користи на сите компјутери, лаптопи, таблети и смартфони. Голема е веројатноста дека вашиот компјутер и мобилен уред веќе имаат антивирусна софтверска заштита што доаѓа со самиот уред, но истата вообичаено е бесплатна и нуди минимална заштита. Сепак размислете за набавка на лиценцирани комерцијални решенија за антивирусна заштита кои ќе ја подобрат безбедноста на уредите и организацијата.

СОВЕТ 2: ВКЛУЧЕТЕ ЗАШТИТЕН SИД (FIREWALL)

Заштитните sидови создаваат „тампон-зона“ помеѓу вашата компјутерска мрежа во организацијата и надворешните мрежи како што е Интернетот. Најпопуларните оперативни системи вклучуваат бесплатен заштитен sид, кој е едноставен за активирање и препорачливо е да биде постојано вклучен.

СОВЕТ 3: СПРЕЧЕТЕ ГИ ВРАБОТЕНИТЕ ДА СИМНУВААТ СОМНИТЕЛНИ АПЛИКАЦИИ

При симнување или инсталирање од Интернет на уредите треба да се користат исклучиво апликации од е-продавници одобрени од производителот на оперативниот систем (за мобилните телефони и таблетите тоа се Google Play Store или Apple App Store). Овие апликации се проверуваат од страна на про-

изводителот на оперативниот систем за да обезбедат одредено ниво на заштита од малициозен софтвер што може да предизвика штета. Треба да се спречат вработените да симнуваат и инсталираат апликации од трети лица, од непознати добавувачи/извори или пиратски софтвер, бидејќи истите не се проверени и најчесто содржат вируси или друг малициозен код.

Воведете користење на „администраторски" кориснички сметки само во исклучителни случаи. Корисничките сметки на вработените за пристап до уредите и податоците на организацијата треба да имаат само пристап кој е доволен за извршување на нивната улога, со дополнителни дозволи (т.е. за администраторите) кои им се даваат само на оние на кои им се потребни. Кога се креираат административните сметки, истите треба да се користат само за таа конкретна задача, при што за секојдневните работни задачи се користат стандардни кориснички сметки. Не дозволувајте вработените да ги извршуваат секојдневните работни задачи на компјутер најавени како администратори.

СОВЕТ 4: ОДРЖУВАЈТЕ ЈА ИНФОРМАТИЧКАТА ОПРЕМА АЖУРИРАНА (НАВРЕМЕНО ИНСТАЛИРАЊЕ НА ЗАКРПИ - PATCHING И АЖУРИРАЊЕ - UPDATING)

За информатичката опрема (компјутери, лаптопи, мобилни телефони и таблети), осигурете дека софтверот и фирмверот се секогаш ажурирани со најновите верзии од производителите и добавувачите на софтвер и хардвер. Примената на овие надградби (процес кој е познат како инсталација на закрпи или „печинг" - ang. patching) е една од најважните работи што можете да ги направите за да ја подобрите безбедноста. Оперативните системи, апликациите, мобилните телефони и таблетите треба секогаш кога е можно да бидат поставени на „автоматско ажурирање".

Кога ќе заврши официјалната поддршка за надградби која ја пружа производителот на уредот или апликацијата, треба да размислите за ризиците од понатамошното користење на тој уред или софтвер бидејќи новите откриени слабости нема да бидат санирани со закрпи од

производителот, што ќе ја зголеми ранливоста за напади и ќе го зголеми ризикот по работењето.

По истек на официјалната поддршка на производителите за уредите и софтверите што ги користите, размислете за можноста истите да се заменат со нови.

СОВЕТ 5: КОНТРОЛА ПРИ КОРИСТЕЊЕТО НА USB - ДИСКОВИ И МЕМОРИСКИ КАРТИЧКИ

USB-дискови и мемориски картички денес масовно се користат за пренос на датотеки помеѓу организации и луѓе. Доволно е само еден невнимателен корисник ненамерно да приклучи инфициран мемориски уред (USB-диск што содржи малициозен софтвер) за да ја оштети организацијата. Бидејќи тие слободно се споделуваат и често се користат за приватни и службени работи, тешко може да се следи што тие содржат, каде биле и кој ги користел. Веројатноста за инфекција преку користење на USB-диск или картичка може да ја намалите со:

- блокирање/забрана за пристап до физичките USB порти од уредот или компјутерот за повеќето вработени;
- користење на антивирусни алатки кои при секое приклучување на меморискиот уред кон компјутерот ќе ја провери содржината на уредот;
- ограничување на само одобрени дискови и картички да се користат во рамки на вашата компанија - и никаде на друго место;

Направете ги овие правила дел од процедурата за прифатливо користење на ИТ опрема на вашата организација. Едуцирајте ги вработените да пренесуваат датотеки преку е-пошта или со користење на услуги за складирање во облак.

3. ЗАШТИТА ОД ФИШИНГ НАПАДИ

Во типичен фишинг напад (напад со намамување), измамниците (анг - scammers) испраќаат лажни пораки до илјадници луѓе, барајќи чувствителни информации (како што се банкарски податоци) или содржат линкови до опасни веб-страници. Истите можат да одлучат да ве измамат да пратите пари, да ви украдат детали за да ги препродадат или пак може да имаат политички или идеолошки мотиви за пристап до информациите на вашата организација.

Фишинг пораките се сè пософистицирани, и можат да ги измамат и највнимателните корисници. Голема е веројатноста да се соочите со фишинг напади. Во продолжение се неколку совети што можат да ви помогнат во идентификација на фишинг-нападите, но сепак треба да бидете свесни дека постои граница за тоа што можете да очекувате корисниците да направат.

СОВЕТ 1: БЕЗБЕДНОСНИ СОВЕТИ ЗА КОРИСНИЧКИТЕ СМЕТКИ НА ВРАБОТЕНИТЕ

При конфигурирање на корисничките сметки за вашите вработени треба да го применувате принципот „најмалку потребни привилегии" - вработените да имаат привилегии и пристап до уредите и документите до она ниво кое е доволно за успешно и навремено извршување на работните задачи. Прекумерните и непотребни привилегии го зголемуваат ризикот за успешен фишинг-напад.

Осигурете се дека вработените не користат администраторски сметки на уредите поврзани на Интернет во секојдневното работење и за извршување на работните задачи. Администраторска сметка е корисничка сметка која овозможува да направите промени што ќе влијаат и на другите корисници. Администраторите можат да ги менуваат безбедносните нагодувања, да инсталираат софтвер и хардвер и да пристапуваат до сите датотеки на компјутерот/уредот. Доколку напаѓачот

добие пристап до корисничка сметка со администраторски привилегии, штетата по организацијата може да биде огромна.

Користете двофакторска автентикација (анг. 2FA - two factor authentication) на вашите важни сметки, како што е е-пошта. Ова значи дека дури и ако напаѓачот ги знае вашите лозинки, тој сепак нема да може да пристапи до таа сметка бидејќи освен лозинката, ќе му треба на пр. и код кој ќе го добиете на вашиот мобилен телефон.

СОВЕТ 2: РАЗМИСЛЕТЕ ЗА ТОА КАКО ГО ОРГАНИЗИРАТЕ ВАШЕТО РАБОТЕЊЕ

Размислете за начините на кои некој би можел да ја нападне вашата организација и бидете сигурни дека вашите вработени ги разбираат вообичаените начини на работа (особено во однос на соработката со други организации), така што се едуцирани да ги забележат барањата кои не се вообичаени. Вообичаена измама вклучува испраќање на фактура за услуга што не сте ја користеле, па кога ќе го отворите прилогот (attachment), малициозен софтвер без ваше знаење, автоматски се инсталира на вашиот компјутер.

Друг начин да се измамат вработените е да се префрлат пари на непроверени сметки или да доставуваат чувствителни информации со испраќање на одговор на пораки по е-пошта кои изгледаат автентични.

Размислете за вашите вообичаени практики и како можете да помогнете овие обиди да имаат помала шанса за успех. На пример:

- Дали вработените знаат што да прават со невообичаени барања, кому да пријават и каде да добијат помош?
- Запрашајте се дали некој што се претставува како важно лице (клиент или менаџер) преку е-пошта треба да биде проверен (или да го потврди неговиот идентитет на друг начин, на пример со потврда испратена по SMS порака) пред да се преземе одредено дејство како исплата на парични средства, испраќање на важни информации и др.
- Дали ги разбирате вашите вообичаени деловни односи? Измамниците честопати испраќаат фишинг-пораки од големи организации

(како што се банки), со надеж дека некои од примачите на е-пошта ќе имаат врска со таа организација. Ако добиете порака по е-пошта од некоја организација со која не соработувате, третирајте ја истата со сомнеж и претпазливо. Веднаш известете го претпоставениот или лицето одговорно за ИТ во организацијата.

- Размислете како можете да ги поттикнете и поддржите вашите вработени да препознаат сомнителни или едноставно невообичаени барања, дури и ако изгледа дека се од важни лица. Да се има самодоверба да се праша „дали оваа порака е автентична?" може да биде разликата помеѓу одржување на безбедноста во компанијата или грешка што може скапо да ве чини.

СОВЕТ 3: ЗНАЦИ НА ФИШИНГ ВО ПОРАКИТЕ

Очекувањето вашите вработени да ги идентификуваат и избришат сите фишинг-пораки е невозможно. Сепак, едуцирани вработени кои се охрабрени да ги пријавуваат сомнителните пораки се најдобрата заштита за вашата организација од фишинг-напади. Следуваат неколку знаци за препознавање на овие напади за кои вработените треба да се едуцираат:

- Многу фишинг-напади потекнуваат од странство и честопати правописот, граматиката и интерпункцијата на текстот во пораките се лоши и наведуваат на користење на автоматизирани сервиси за превод на текстови како Google translate. Некои напаѓачи ќе се обидат да создадат пораки кои се многу слични на официјални пораки со вклучување на логоа и графики слични на вашите или на компаниите со кои соработувате. Детално разгледајте ја пораката за знаци за фалсификување.
- Доколку во насловот од пораката ви се обраќаат со вашата адреса за е-пошта или пишува „почитуван", „колега" или се користи сличен генерички термин, тоа може да биде знак дека испраќачот не ве познава и пораката можеби е испратена за фишинг-измама.
- Бидете сомнителни на пораките во чиј текст од вас се бара брзо да дејствувате. Бидете сомнителни доколку во пораката сретнете збо-

рови како „испратете ги овие детали во рок од 24 часа“ или „Вие сте жртва на криминал, веднаш кликнете тука“.

- Внимавајте на пораки што наизглед се испратени од високо-рангирана личност во вашата организација, со барање за брза реализација на плаќања на одредени банкарски сметки. Проверете дали ви е позната адресата за е-пошта од која е испратена пораката или е само слична на адреси кои често ги користите за комуникација. Проверете ја точноста на наведената банкарска сметка и дали таа навистина припаѓа на компанијата која ви е позната и со која во минатото сте соработувале и сте изградиле доверба. Побарајте потврда по SMS или друг канал за комуникација, за вистинитоста на барањето.
- Не одговарајте на пораки по е-пошта, SMS, Viber или WhatsApp во кои ви се нудат пари или наследство од странство испратени од лица и адреси за е-пошта кои не ги познавате, или во кои ви се нуди пристап до скриени или компромитирачки информации на Интернет.
- Не одговарајте на пораки во кои ве уценуваат со објава на компромитирачки информации и слики доколку не платите уцена во Bitcoin валута на одреден паричник, а за кои се тврди дека се испратени од вашата адреса за е-пошта. Многу често овие закани се лажни и само изгледаат како да се испратени од вашата адреса за е-пошта. Побарајте помош од лицето или компанијата одговорни за вашата комуникација по е-пошта со цел да се идентификува вистинската адреса за е-пошта од која ви е испратена пораката, а која е маскирана за да изгледа исто со вашата адреса за е-пошта.

СОВЕТ 4: ПРИЈАВУВАЈТЕ ГИ СИТЕ ФИШИНГ НАПАДИ

Едуцирајте ги вработените да ги пријавуваат СИТЕ сомнителни пораки. По пријавата, доколку се сомневате дека сте цел на фишинг напад, итно преземете чекори за скенирање на уредите за постоење на малициозен софтвер (малвер) и осигурајте редовна промена на лозинките.

Не очекувајте вработените да ги препознаат сите обиди за фишинг-напади. Охрабрете ги да ги пријавуваат сите грешки во работењето и

уверете ги дека за ненамерното отворен додаток од порака испратена преку е-пошта нема да бидат казнети. Не ги казнувајте вработените ако се измамени. Заканите со казнување може да ги обесхрабри вработените да пријавуваат идни обиди за фишинг измами. На тој начин може да се предизвика поголема штета на вашето работење.

Доколку се сомневате дека вашата организација е цел или жртва на онлајн измама, изнуда (ransomware) или фишинг-напад, тоа треба да го пријавите во Министерството за внатрешни работи во најблиската станица или по телефон. Можете да пријавите и до MKD-CIRT со пополнување на онлајн образецот достапен на нашата веб-страница https://mkd-cirt.mk или по е-пошта на адреса info@mkd-cirt.mk, и во тој случај MKD-CIRT ќе Ви прати насоки за справување со пријавениот напад и по потреба ќе ја препрати пораката со пријава до МВР по е-пошта.

4. ЛОЗИНКИ И ПРИСТАП

На прашање, дали имате лозинка на уредите што ги користите, 75% од корисниците на дигиталните уреди што користат Интернет во државата одговориле дека користат лозинки. Едукацијата на вработените за важноста од користење на лозинки како примарна заштита е од голема важност. Вашите лаптопи, компјутери, таблети и паметни телефони може да содржат критични податоци за бизнисот, лични податоци на вашите клиенти, како и деталите за онлајн сметките на кои пристапувате. Со користење на лозинки се обезбедува најниско ниво на заштита на пристап до вашите податоци, се спречува неовластен пристап и користење.

Следуваат совети за правилно користење на лозинките за поголема безбедност.

СОВЕТ 1: КОРИСТЕТЕ ЗАШТИТА НА ПРИСТАП ДО ПОДАТОЦИ СО ЛОЗИНКИ ТАМУ КАДЕ Е ПОТРЕБНО

Без разлика дали станува збор за компјутер, телефон, таблет или онлајн услуга, поставете лозинка за ограничување на пристап до овие уреди и услуги доколку тие содржат осетливи или податоци важни за вашето работење. Освен со лозинки, пристапот треба да го обезбедите и со дополнителна заштита секаде каде е можно, на пр. со користење на PIN (Personal Identification Number), скен од прст или скен на лице, како начини за дополнителна автентикација.

Осигурајте дека ИТ опремата како компјутер и лаптоп користи енкриптирање или шифрирање на податоците кои се запишани на нив. Пример за ова е BitLocker за Windows и FileVault за macOS. Активирајте ја енкрипцијата пред компјутерот да почне да се користи. Побарајте од ИТ лицата кои се одговорни за одржување на опремата да ја активираат оваа можност.

СОВЕТ 2: КОРИСТЕТЕ СИЛНИ ЛОЗИНКИ

Ако Вие сте одговорни за политиките за користење на ИТ уредите во вашата организација, осигурете дека вработените знаат како да креираат силни лозинки кои ќе бидат лесни за запомнување, но истовремено и тешки за откривање од криминалците. Вообичаена пракса е должината на лозинките да биде најмалку 8 карактери, и да содржат три од четирите групи на знаци (мали букви, големи букви, броеви и специјални знаци).

Осигурете се дека секој корисник има личен пристап до соодветните системи и дека нивото на даден пристап е секогаш на најниското потребно ниво за да ја завршат својата работа.

СОВЕТ 3: КОРИСТЕТЕ АВТЕНТИКАЦИЈА СО ДВА ФАКТОРИ ЗА „ВАЖНИТЕ“ СМЕТКИ

Според најновата анкета на MKD-CIRT, 70% од корисниците на Интернет во државата не користат автентикација со два фактора. Ако ви е дадена

можноста да користите автентикација со два фактори (исто така позната како 2FA – анг. "two factor authentication") за која било од вашите сметки, треба да ја искористите. Тоа дополнително ја зголемува безбедноста на организацијата. 2FA бара два различни методи да го „докажете" вашиот идентитет пред да можете да користите одредена услуга, обично лозинка плус уште еден метод. Ова може да биде код кој е испратен до вашиот паметен телефон (или код што е генериран од токен за банкарски услуги) што мора да го внесете покрај вашата лозинка.

СОВЕТ 4: ПОМОГНЕТЕ ИМ НА ВРАБОТЕНИТЕ ДА СЕ СПРАВАТ СО ГОЛЕМ БРОЈ ЛОЗИНКИ

Вработените веќе имаат повеќе лозинки што треба да ги помнат, за службени и приватни потреби. За да им помогнете, инсистирајте на пристап со лозинка само за услугите за кои тоа е навистина потребно. Веќе се напушта праксата за периодично менување на лозинките. Лозинките треба да се променат кога се сомневате дека се загрозени деталите за најава при користење на одредена услуга.

Обезбедете безбедно чување на лозинките. Вработените може да ги запишат лозинките за важните сметки (како е-пошта и банкарство) и да ги чуваат безбедно (но не на самиот уред). Бидејќи вработените може да ги заборават лозинките, осигурајте дека тие ќе можат да ги ресетираат сопствените лозинки на едноставен и брз начин. Доколку сте во можност во вашата организација користете т.н. менаџери за лозинки (анг. Password managers). Тоа се софтверски алатки кои можат на едно место да ги креираат и чуваат лозинките за повеќе услуги, до кои ќе се пристапува преку главна/мастер-лозинка. Таа треба да е доволно сложена, на пример со користење на фраза од три случајни зборови и вкупна должина од најмалку 8 карактери, како и дали содржи карактери од три од следните групи: големи букви, мали букви, броеви и специјални знаци.

СОВЕТ 5: ПРОМЕНЕТЕ ГИ СИТЕ СТАНДАРДНИ (DEFAULT) ЛОЗИНКИ

Честа грешка е, да не се променат стандардните лозинки поставени од производителите што доаѓаат со паметните телефони, лаптопите,

мрежните насочувачи и други видови на активна компјутерска и мрежна опрема. Променете ги сите стандардни лозинки пред вработените да започнат да ги користат. Правете редовни периодични проверки на уредите и апликациите за тоа дали стандардните лозинки се променети.

5. ТЕЛЕФОНИ, ТАБЛЕТИ И ПАМЕТНИ УРЕДИ

Реалноста е дека службените мобилни телефони и таблети често се користат и за приватни потреби, надвор од работно време и простор. Исто така, многу организации овозможуваат користење на приватни мобилни уреди за службени цели. Следуваат совети и препораки за безбедно користење на овие уреди во вашата организација.

СОВЕТ 1: ВКЛУЧЕТЕ ЗАШТИТА ЗА ПРИСТАП СО ЛОЗИНКА

Сложен PIN код или лозинка наспроти едноставни што лесно може да се погодат или извлечат од вашите профили на социјалните мрежи можат да ги спречат криминалците да пристапат до вашиот мобилен уред. Денес, многу од овие уреди вклучуваат препознавање на отпечатоци од прст за отклучување, без потреба од лозинка. Доколку овие функции се достапни но не се однапред овозможени, практикувајте нивно активнирање и користење.

СОВЕТ 2: ОСИГУРАЈТЕ СЕ ДЕКА ИЗГУБЕНИТЕ ИЛИ УКРАДЕНИТЕ УРЕДИ МОЖЕ ДА ГИ СЛЕДИТЕ, ЗАКЛУЧИТЕ ИЛИ ИЗБРИШЕТЕ

Има голема веројатност, таблетите или телефоните на вработените да бидат украдени (или да ги изгубат) кога тие се надвор од канцеларијата или домот. За среќа, поголемиот дел од уредите вклучуваат бесплатни веб-базирани алатки кои во случај на губење на уредот можете да ги користите за следење на локацијата на вклучениот уред, далечинско заклучување на уредот и далечинско бришење на податоците.

Овие алатки може да ги користите за вашите лични и службени уреди. Управување со поголем број на мобилни уреди се врши преку т.н. „mobile device management software“ за кој може да најдете повеќе информации на Интернет.

СОВЕТ 3: РЕДОВНО И НАВРЕМЕНО АЖУРИРАЊЕ НА УРЕДИТЕ

Многу важно е уредите секогаш да бидат ажурирани. Производителите на оперативните системи како Android или iOS редовно објавуваат критични безбедносни надградби. Уредите секогаш треба да бидат поставени на автоматско ажурирање. Едуцирајте ги вработените за важноста од навремено ажурирање и доколку е потребно објаснете им како тоа се прави. Во моментот кога производителот на уредот ќе престане со поддршка и издавање на нови критични безбедносни надградби за одреден тип на уреди, размислете за нивна замена со нови.

СОВЕТ 4: РЕДОВНО И НАВРЕМЕНО АЖУРИРАЊЕ НА АПЛИКАЦИИ

Исто како и оперативните системи на уредите на вашата организација, сите апликации што ги имате инсталирано треба редовно да се ажурираат со закрпи (patches) од производителите на софтвер. Овие ажурирања не само што ќе додадат нови функции, туку ќе ги поправат и сите безбедносни ранливости што биле откриени. Осигурајте се дека вработените знаат кога се спремни надградбите, како да ги инсталираат и дека е важно веднаш да се направи тоа, без одложувања.

СОВЕТ 5: НЕ СЕ ПОВРЗУВАЈТЕ НА НЕПОЗНАТИ WI-FI ХОТСПОТОВИ

Проблем со користење на јавни или отворени Wi-Fi хотспотови како тие во хотелите и ресторанте е што не знаете кој го контролира хотспотот. Ако се поврзете на вакви хотспостови, ризикувате некој непожелен да има пристап до вашите документи и тоа што го работите, како и до вашите чувствителни податоци како корис-

ничко име и лозинка, или шифри за најава на онлајн банкарство или социјални мрежи. Наједноставната мерка на претпазливост е да не се поврзете на интернет, користејќи непознати хотспотови, и наместо тоа да ја користите вашата 3G или 4G мобилна мрежа, која веќе има вградено безбедносни мерки. Користите „tethering" (кога вашите други уреди, како лаптопи, ја споделуваат вашата 3G/4G конекција од мобилниот телефон), или стик за безжично поврзување (dongle) од вашата мобилна мрежа. Дополнителна мерка е да користите виртуелни приватни мрежи (VPN) со што се енкриптираат податоците пред да бидат испратени преку Интернет.

6. САЈБЕР-ИНЦИДЕНТИ

Сајбер-инцидент е неовластен пристап (или обид за пристап) до ИТ системите на една организација. Тука спаѓаат малициозните напади кои имаат за цел кражба на податоци, уцени или злоупотреба на вашите податоци и ИТ системи или предизвикување на штета. Примери за сајбер-инциденти се негирање на услуга (анг. Denial of Service - DoS), напад со кој се оневозможува достапноста на вашите услуги и се прекинува вашето тековно нормално работење, како и нападите со „рансомвер". Причини за инциденти може да бидат и физички оштетувања, природни непогоди или кражба. Справување со инцидентот е процес кој ги опфаќа следните чекори.

ЧЕКОР 1: БИДЕТЕ ПОДГОТВЕНИ ЗА ИНЦИДЕНТ

Оваа фаза се однесува на вашата отпорност на инциденти и вклучува идентификација на важните податоци и системи за организацијата кои се критични за нејзиното работење. Потребно е редовно снимање на заштитна копија од овие податоци што ќе се чува на друго безбедно место, ефективен План за управување со ризици и План за континуитет на работењето и опоравување од катастрофи. Повеќе информации за процена на ризиците ќе најдете со пребарување на Интернет и на веб-страницата на центарот. Пожелно е да имате документирани процедури за управување со ИТ системи кои се критични за вашите

услуги и работење. Такви се на пример системите за е-пошта и вашата веб-страница, сметководство и архивско работење. Ефективно управување со ризиците и успешно спроведување на планот на опоравување по инцидент подразбира идентификувани лица кои се одговорни за критичните ИТ системи и кои ќе имаат важни улоги при реализација на плановите, без разлика дали тие се ваши вработени или се дел од надворешна организација со која имате договор.

Направете План за инциденти. Размислете што би се случило доколку одеднаш немате пристап до критичните системи или податоци кои претходно ги идентификувавте. Направете листа на критични системи кои се подредени според приоритет, базирана на разбирање на тоа што е важно за да нема прекин во работењето, зошто е тоа важно и што преземате за заштита.

ЧЕКОР 2: ИДЕНТИФИКАЦИЈА НА СЛУЧЕН САЈБЕР-ИНЦИДЕНТ

Некои од знаците дека ви се случил сајбер-инцидент или дека инцидентот се случува во овој момент се ако компјутерите работат бавно, ако добивате пораки по е-пошта со уцена, кога вработените не можат да пристапат до своите сметки и документи или ако други луѓе ве известуваат дека добиваат чудни пораки по е-пошта испратени од ваши адреси.

Доколку се сомневате дека се случил сајбер-инцидент, следен чекор е да откриете што точно се случило. Во тоа може да Ви помогнат одговорите на прашањата кој и кога пријавил проблем, кои услуги и системи се опфатени со проблемот, кои податоци се избришани или недостапни (доколку ги има), кога за прв пат сте дознале за проблемот, и кои делови од работењето на организацијата се опфатени.

ЧЕКОР 3: ПРЕКИН И РЕШАВАЊЕ НА ИНЦИДЕНТОТ

Прва работа е да се провери активноста на антивирусната заштита, преку чија анализа може да дојдете до информации за типот на настанатиот инцидент и опфатот на штета. Доколку не можете ова да го нап-

равите сами, ангажирајте надворешен експерт кој ќе направи ревизија на тоа што се случило. Користете ги информациите што сте ги собрале за да побарате совет преку Интернет од доверливи извори. За надминување на одредени проблеми, упатства може да најдете на Интернет.

Решавање на инцидентот значи повторна достапност на услугите, системите и информациите кои биле недостапни поради тој инцидент. Во оваа активност клучна улога имаат лицата кои ги одржуваат вашите ИТ системи. Овие лица треба да Ви дадат точна информација за типот на инцидентот и неговиот опсег, како и да предложат и реализираат соодветни активности за надминување на истиот. Во зависност од видот на инцидентот на кој реагирате, ова може да вклучува чистење на заразени машини, промена на лозинки, враќање на податоци од бекап, инсталација на надградби и закрпи на оперативни системи и апликации.

ЧЕКОР 4: ИЗВЕСТУВАЊЕ ЗА ИНЦИДЕНТ И СПОДЕЛУВАЊЕ НА ИНФОРМАЦИИ

Откако ќе се реши сајбер-инцидентот, може да е задолжително да известите некоја организација или регулатор за случениот инцидент и претрпената штета. Не заборавајте дека сајбер-нападот, неовластениот пристап до ИТ системи и кражба или уништување на податоци и средства се кривични дела. Чувајте ги сите информации од инцидентот, како логови за пристап и променети датотеки. Надминете ги предрасудите дека е срамно да се извести за нападот кој ви се случил. Известувањето и споделувањето информации со колегите и другите засегнати страни ќе спречи повторување на истиот инцидент кај друга организација. Доколку со инцидентот на било кој начин се компромитирани податоци за вашите клиенти, вработени или соработници, задолжително истите известете ги во најкраток рок.

Пријавете го инцидентот во МКD-CIRT и побарајте информацијата да се сподели со другите организации. МКD-CIRT на ваше барање ќе ја анонимизира информацијата пред да ја сподели и ќе ве заштити како пријавувач. Повеќе за пријава на инцидентите до МКD-CIRT ќе најдете

на веб-страницата на центарот. Колку повеќе лица пријавуваат, толку е поголема веројатноста сторителите да бидат уапсени, обвинети и осудени. Доколку инцидентот значително влијаел на вашето работење, размислете да побарате и правна помош.

ЧЕКОР 5: НАУЧЕТЕ ОД ИНЦИДЕНТОТ

По случен инцидент важно е да направите преглед на слученото и да научите од откриените грешки. Потоа треба да преземете активности да се надминат откриените недостатоци, а со тоа ќе ја намалите веројатноста за повторно случување на сличен инцидент и ќе ја зголемите отпорноста на вашата организација.

Доколку е потребно ревидирајте ги плановите и преиспитајте ги ризиците. На пример, ако сте жртва на напад со лозинка, можеби ќе треба да креирате нова политика за лозинки, да обезбедите нова обука, да обезбедите физичко безбедно складирање на лозинки (или апликации за управување со лозинка) за вашите вработени.

Доколку надворешни лица се задолжени за одржување на ИТ системите во организацијата, ревидирајте ги договорите за одржување со цел времето на одговор и опоравување да се усогласи со максималното прифатливо време во кое вашите услуги може да бидат недостапни.

Издавач:	Агенција за електронски комуникации
Подготвил:	Националниот центар за одговор на компјутерски инциденти MKD-CIRT
Лектура и коректура:	Сузана Стојановска
DTP и печат:	ГЛОБАЛ Комуникации
Тираж:	4.000 копии

САЈБЕР-БЕЗБЕДНОСТ
Водич за мали и средни претпријатија

НАКРАТКО...

- РЕДОВНО ПРАВЕТЕ БЕКАП НА ВАЖНИТЕ ПОДАТОЦИ
- КОРИСТЕТЕ АНТИВИРУСНА ЗАШТИТА И ЛЕГАЛЕН СОФТВЕР
- ЗА ПРЕНОС НА ДОКУМЕНТИ КОРИСТЕТЕ Е-ПОШТА И ОБЛАК, А НЕ USB
- КОРИСТЕТЕ ОГНЕН ЅИД МЕЃУ ЛОКАЛНАТА МРЕЖА И ИНТЕРНЕТ
- ЕДУЦИРАЈТЕ ГИ ВРАБОТЕНИТЕ ДА ПРЕПОЗНАВААТ ФИШИНГ ИЗМАМИ И ДА ПРИЈАВУВААТ ИНЦИДЕНТИ

Повеќе информации и совети за сајбер-безбедност ќе најдете на веб-страницата на Националниот центар за одговор на компјутерски инциденти MKD-CIRT https://mkd-cirt.mk

Прашања и пријави на инциденти испраќајте на info@mkd-cirt.mk или 02/3091232