Прирачник за безбедност на интернет:

сајбер хигиена за јавни институции и мали и средни претпријатија

Владан Бабиќ и Александар Братиќ

Октомври 2022

DCAF Geneva Centre for Security Sector Governance

За ДЦАФ

ДЦАФ – Женевскиот центар за управување со безбедносниот сектор е посветен на подобрувањето на безбедноста на државите и нивното население во рамките на демократско управување, владеење на право, почитување на човечки права и родова еднаквост. Од своето основање во 2000. година, ДЦАФ има придонесено кон креирање на поодржлив мир и развој, помагајќи им на државите партнери и меѓународните актери кои ги поддржуваат тие држави во подобрувањето на управувањето со безбедносниот сектор преку инклузивни и партиципативни реформи. Тој креира иновативни производи на знаење, промовира добри норми и пракси, дава правни совети и совети за политиките и го поддржува градењето на капацитетот на државните и недржавните актери во безбедносниот сектор.

ДЦАФ – Женевски центар за управување со безбедносниот сектор
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Женева, Швајцарија
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Photo credit: Shutterstock, image contributor: Illus_man
Design & layout: DTP studio

Оваа публикација е развиена во рамките на проектот „Добро управување во сајбер безбедноста на Западниот Балкан“ на ДЦАФ – Женевскиот центар за управување со безбедносниот сектор, кој е поддржан од канцеларијата за односи со странство, Комонвелт и развој на Обединетото Кралство.

Содржина

Вовед

Овој документ е преглед на минималните стандарди за воспоставување на систем на сајбер хигиена во јавните институции и малите и средни претпријатија (МСП). Во него се претставени мерки кои секоја организација треба да ги воведе за да обезбеди соодветно ниво на информатичка безбедност за своите информатички системи.

Фокусот тука е однесува на давање вовед во важноста на сајбер хигиената и препораки за едноставни чекори за подобрување на сајбер безбедноста во вашата организација.

Накратко, хигиената во безбедноста е иста како миење раце. Кога унгарскиот доктор Игназ Семелвајс ги кажал трите едноставни збора „мијте ги рацете“ во 1850. година, тој создал револуција во медицината, дури и ако никој првично не го сфаќал сериозно. Тој увидел дека добрата хигиена е нераскинливо поврзана со доброто здравје, а со текот на времето податоците покажале дека превентивното миење на раце навистина ги намалува инфекциите.

Слично на тоа, сајбер хигиената се однесува на пракси кои имаат за цел спречување на инфекција со малициозен софтвер (малвер - malware), како и сајбер упади и губење или корумпирање на податоци и одржување на здраво сајбер опкружување. Со тоа се обезбедува здравјето на системот и се подобрува сајбер безбедноста на ист начин како што рутинското миење на раце помага во спречувањето на ширењето на болести.

Земајќи предвид дека сите организации денес користат информатички системи за своето работење, сите се под ризик од изложување на различни сајбер напади кои можат да го спречат функционирањето на информатичките системи или да го блокираат пристапот до податоците. Според тоа, секоја организација мора да ги заштити своите информатички системи и мора да воспостави процедури и политики и да понуди редовна обука, за да воспостави соодветни пракси на сајбер хигиена.

Дефиниции

Постојат многу различни дефиниции на сајбер хигиената и сите се точни.

- Digital Guardian ја нарекува сајбер хигиената како „пракса и чекори кои корисниците на компјутери и други уреди ги преземаат за да го одржат здравјето на системот и да ја подобрат безбедноста на интернет“.
- Kaspersky Lab потенцира дека сајбер хигиената се однесува на „обучување на сам себе за создавање на добри навики во врска со сајбер безбедноста, за да бидеме чекор пред сајбер заканите и безбедносните проблеми на интернет“.
- Списанието Security ја опишува сајбер хигиената во поглед на тоа „дека треба да бидете сигурни дека кај вас функционираат основните контроли за безбедност и дека тие конзистентно се применуваат во целото ваше опкружување“.
- CyberSecurity Forum кажува дека сајбер хигиената е „колоквијален израз кој се однесува на најдобрите пракси и другите активности кои можат да ги преземат администраторите и корисниците на компјутерските системи за да ја подобрат својата сајбер безбедност додека ги работат своите вообичаени активности на интернет, како пребарување на интернет, праќање на е-пошта, праќање на пораки, итн.“.
- Блогот Endpoint ја објаснува сајбер хигиената како „збирка на вообичаени пракси за безбедно ракување со податоци и обезбедување на мрежи. Тоа е како лична хигиена, кога ќе развиете рутина на малечки, посебни активности кои ги спречуваат или ублажуваат здравствените проблеми“.

Со други зборови, сајбер хигиената е збирка на основни безбедносни пракси кои може да ги преземе секој член на персоналот за да се заштити себе и здравјето на личниот и организацискиот хардвер и софтвер во компјутерските системи.

Вообичаени мерки

Добрата сајбер хигиена бара спроведување на вообичаени мерки, од воспоставување на стандардизирани процедури и политики, до редовни обуки кои им помагаат на вработените да ги разберат сајбер заканите кои постојано се менуваат. Природата и карактерот на некои од заканите се објаснети во понатамошниот текст (видете Вообичаени сајбер закани). Меѓутоа, прво се претставени клучните елементи на ефективната програма за сајбер хигиена, како и добрите практики.

Анализирајте ги системите и воспоставете процедури и политики

Попис на ресурси

Одржувајте попис на хардверот и софтверот

Управувањето со ИТ хардверот и софтверот (ИТ ресурси) може да биде огромна задача, особено ако опремата и персоналот постојано се движат и менуваат, но е од клучно значење. Хардверот, софтверот и сите мрежни уреди и уреди кои не се мрежни се сметаат за ресурси во овој поглед.

Одржување на попис на хардвер и софтвер ќе ги поддржи различните процеси во вашата организација, како:

- Управување со инциденти
- Управување со проблеми
- Управување со промени

Во текот на овие процеси се поставуваат слични прашања:

- Што прави одреден ИТ ресурс?
- Каков оперативен систем користи?
- Кои се апликациите кои се чуваат на/во ресурсот?
- Како изгледа топологијата на мрежата?
- Кој има пристап до ресурсот?
- Кој е одговорен за него?

За да одговориме на овие прашања, потребна ни е централизирана база на информации. Според тоа, првиот чекор во воспоставувањето на пракса на сајбер хигиена е **стандардизација на пописот на софтвер и хардвер** преку:

1. Документирање на основната безбедносна позиција на организацијата
2. Стандардизација на истата во целата организација на основа на политики и процедури
3. Мониторинг и реагирање на отстапувања
4. Намалување на сите слабости воведени со непознат хардвер и софтвер

Предностите од одржување на попис на хардвер и софтвер се очигледни и вклучуваат:

- Контрола на ИТ опкружувањето
- Контрола на софтверските ресурси (верзија, крпеница, зависност, одговорност и доказ на концепт)
- Контрола на хардверски ресурси (верзија, критичност, доказ на концепт, зависност)
- Ефективно управување
- Подобро просечно време до повторно воспоставување на услугите (MTTRS)

Попис на информации

Одржувајте попис на чувствителни или критични информации

Заштитата на чувствителните информации – која вклучува соодветно етикетирање, откривање и

раководење со нив – е исклучително тешка. Може да биде тешко да се разбере како корисниците стапуваат во интеракција со тие информации и како ги разменуваат. Според тоа, не е чудно што повеќе од половина од корпоративните податоци се „темни“, што значи дека не се класифицирани, заштитени или управувани.

Важно е да го **разберете вашето податочно опкружување и да ги идентификувате важните податоци во вашата средина**. За таа цел, важно е да се креира политика за **класификација на податоци**, како прв чекор. Постојат различни шеми за класификација кои можат да се користат според потреба, но подолниот пример содржи три нивоа:

Ограничено – чувствителни податоци кои претставуваат голем ризик ако бидат компромитирани; на нив им пристапуваат само оние кои имаат потреба за тоа.

Доверливо – умерено чувствителни податоци на кои им се пристапува само интерно.

Јавно – податоци кои не се чувствителни и претставуваат мал или никаков ризик ако им се пристапи.[1]

Како втор чекор, податоците требаат да бидат шифрирани, особено сите податоци со ознака „ограничено“.

На крајот, треба да се спроведе систем за спречување на губење на податоци за откривање на потенцијални упади во податоците/трансмисии за извлекување на податоците и нивно спречување преку следење, откривање и блокирање на чувствителните податоци во текот на употреба, во движење и во мирување.

Ова треба да вклучува одредено скенирање и автоматизација (за што Microsoft е добра алатка) и треба да покрива:

- Место за чување на самата локација
- Office апликациите
- SharePoint апликациите
- Размена
- Cloud (чување на податоци на интернет) и SaaS (софтвер како услуга) апликации кои не се Microsoft апликации

Проценка на ризик

Идентификација на ризик

Управувањето со ризик бара разбирање на заканите со кои е соочена вашата организација и чекорите кои можат да се преземат за да ги спречите, намалите или да се подготвите за ситуација која може, но не мора да се случи.

Постојат три полиња на ризик за информатички системи:

- **Човечки ризик**, како измама, кражба или човечка грешка.
- **Природен ризик**, како поплава, пожар и земјотрес.
- **Технички ризици**, како дефекти во софтверот, хардверот или недостаток на знаење.

Како почетна точка, проценката на ризик вклучува доделување на вредности на критичните ресурси, вклучувајќи ги финансиските и репутациските. Тоа може да ви помогне да почнете со проценка на сериозноста на секоја посебна закана. Еден ефективен начин за ова е да доделите оценка на секое сценарио – прво во поглед на веројатноста дека нешто ќе се случи и друго, за штетата која ќе настане ако тоа се случи.

Тоа ќе ви даде подобра идеја каде да ги насочите вашите активности и ќе ви помогне да одлучите како да пристапите кон утврдените ризици, на пример преку:

- **Избегнување**, кога ризиците не создаваат директна закана по вашето работење
- **Намалување**, кога ризиците бараат имплементација на ново сигурносно решение
- **Прифаќање**, кога е мала веројатноста дека ризикот ќе се случи или е над тековните

1 https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data

капацитети
- **Пренесување**, кога ризикот може да се осигури

Процедура за бекап (правење резервни копии)

Воспоставете процедура за редовен бекап

Исклучително е важно да се има процедура за бекап. Целта е да се креира копија на податоците која може да се врати во случај на дефект во податоците – тоа може да биде резултат на софтверски и хардверски дефекти, корумпирање н податоци или човечки предизвикани настани како што се малициозни напади или случајно бришење. Добро осмислена политика за бекап и враќање на податоците е од суштинско значење и претставува последна линија на одбрана во една организација.

Скоро сите организации имаат поставени барем некакви системи за бекап. Прашањето е дали системот адекватно ги задоволува потребите на вашата организација и услугите кои ги давате? Важно е да не се работи бекап само во име на бекап, туку да правите бекап за да можат да се вратат клучните податоци по потреба и со што помало влијание по работењето.

На пример, резервните копии треба да ја покриваат секојдневната работа, но исто така треба да овозможуваат работење и кога системот не е во функција. Или, во случај на катастрофа, податоците треба да се чуваат на локација од која можат да бидат вратени.

Организацијата треба да биде реална при креирањето на бекап политики и треба да подготви пишан план за бекап кој содржи детали за тоа:
- Што се става на бекап?
- Каде се наоѓа бекапот?
- Колку често се врши бекап?
- Кој е задолжен да врши бекап?[2]

Секогаш дајте им највисок приоритет на клучните податоци

Утврдете го распоредот за бекап врз основа на тоа колку работа вашата организација е волна да изгуби. Имајте на ум дека базите на податоци и вашите сметководствени датотеки се вашите најкритични ресурси и дека треба да се направат резервни копии пред и по секое значајно користење. За повеќето организации ова значи дека бекапот на датотеките треба да се прави секој ден. Меѓутоа, непрофитни организации кои внесуваат големи количини на податоци треба да размислат за правење бекап на своите бази на податоци после секое значајно внесување на податоци, дури и ако тоа е неколку пати на ден. Бекап на основните датотеки како што се документите (во директориумот „Your Documents“, на пример) и датотеките на електронската пошта треба да са прави најмалку еднаш неделно или дури еднаш дневно.[3]

Секогаш тестирајте го вашиот бекап

Со тестирање на резервните копии можете да утврдите дали функционираат како што треба. Ова ви овозможува да измерите колку брзо вашето работење ќе биде вратено по дефектот и да ги утврдите сите прашања на кои треба да се одговори.

Користете го правилото 3-2-1 за бекап

Стручните лица препорачуваат пракса на редундантност на бекап позната како правило 3-2-1. Ова се преведува во три копии на вашите податоци, на два локални (но различни) уреди и една копија на уред кој се наоѓа надвор од локацијата. Со овој пристап во голема мерка се намалува шансата податоците да бидат изгубени.

Во суштина, копирањето на важни датотеки на хард диск или УСБ не претставува креирање на доволен бекап. Хард дисковите се расипуваат. Понатаму, УСБ дисковите и СД картичките се малечки и лесно се губат. Добриот бекап бара редундантност во форма на неколку копии кои се заштитени во случај на непредвиден инцидент.

2 Your Organization’s Backup Strategy | Articles and How-tos (techsoup.org)
3 Your Organization’s Backup Strategy | Articles and How-tos (techsoup.org)

Користете чување на податоци на далечина

Решенијата за чување на податоци надвор од локацијата или во „облак“ (cloud) се рентабилен и ефикасен начин да се осигурите дека вашите податоци се подалеку од вашата локација, но сè уште ви се достапни.

Правете бекап често и редовно

Денеска постојат алатки кои ви овозможуваат автоматски да правите бекап и тие се лесни за користење и евтини.

План за одговор во случај на инцидент

Воспоставете тим за реакција во случај на инцидент

Тимот за реакција во случај на инцидент е група на ИТ професионалци во организацијата кои се задолжени за подготвување и реагирање на секој итен ИТ случај што ќе настане.

Овие стручњаци вообичаено доаѓаат од различни струки и улоги и имаат комплементарни технички вештини, што му овозможува на тимот да биде способен да одговори на широк спектар на безбедносни инциденти, вклучувајќи и упади или сајбер напади.

Тимот за реакција на инциденти вообичаено е одговорен за подготовка на план за реакција (видете доле), за да може да се преземе методичен пристап во решавањето на безбедносните инциденти и управувањето со последиците. Тимот исто така мора да тестира и решава слаби точки во системот, одржува силни безбедносни пракси и дава поддршка на мерките за справување со инциденти.

Изгответе план за реакција на инциденти (ПРИ)

ПРИ е алатка за управување со ризик која ги дефинира контролите за намалување на упадот или инцидентот и кој утврдува што треба да се направи ако се случи упад. Со него ќе се намали ризикот од упад, под услов организацијата да има тим за реакција во случај на инцидент.

Важно е да се има на ум дека инцидентите редовно ќе се случуваат во секое работно опкружување. Вашиот тим за реакција на инциденти ќе мора да утврди приоритети и на кои инциденти мора веднаш да се реагира, а на кои може да се реагира подоцна. **Опсегот и целите на тимот за реакција на инциденти се утврдуваат од страна на раководството во ПРИ**.

Добро дефинирани процедури со кои се опишуваат соодветни одговори на инцидентите е од суштинско значење, особено бидејќи можат да се случат ситуации во кои инцидентот треба да се пријави на локалните органи, во зависност од прописите со кои се регулира вашата индустрија. Структурата на ПРИ зависи од рамката која се користи, како што се ISO 28035 или NIST (подготовка, откривање и анализа, изолација, искоренување и враќање, активности по инцидентот).

Кога ќе се случи инцидент клучно е да го следите вашиот ПРИ, кој ќе содржи процедури за реакција на различни видови на инциденти.

Многу инциденти се предизвикуваат од корисниците внатре, така што е важно да се обучат вработените и другите крајни корисници за соодветна компјутерска безбедност и исто така да се следи нивното користење за да бидеме сигурни дека тие не се вклучени во малициозни активности. За тоа да го направи, организацијата мора да:

- Им објасни на крајните корисници како да пријават инцидент, со соодветни информации за е-пошта, портали, телефонски централи и центри за помош.
- Подготви внатрешна страница која ги содржи потребните информации за исправна пријава.
- Организира годишни безбедносни обуки кои вклучуваат упатства за тоа што да се прави во случај на инцидент (малвер пријава, пријава за истекување на податоци, спам и фиш пријава, итн.).
- Ги обучи крајните корисници да ја исклучат машината од интернет кога ќе се случи инцидент, ако вашата организација нема поставени технички мерки за автоматска изолација на хостот.
- Ги научи крајните корисници да не преземаат никакво дејство по инцидентот, освен ако не е одобрено од тимот за реакција на инциденти, за да се зачуваат неопходните докази за

можна форензична истрага.

- Ги обучи крајните корисници да дадат што е можно повеќе информации по инцидентот, вклучувајќи:
  * Што се случило?
  * Кога тоа се случило?
  * Каде тоа се случило?
  * Кој бил вклучен?
  * Кои дополнителни информации можат да го забрзаат собирањето на информации во фазата на тријажа?

Континуитет и закрепнување од катастрофа

Подгответе план за континуитет и закрепнување од катастрофа

Додека работниот континуитет се однесува на враќање, закрепнување и одржување на севкупното работење на една организација во случај на неочекуван проблематичен настан, закрепнувањето од катастрофа тука се однесува на конкретни активности кои се поврзани со комуникација и технолошката инфраструктура и податоци.

Кога ќе се случи непланиран инцидент, суштинско е организацијата да може да продолжи со работа што е можно поскоро. Планот за континуитет на работењето е во целост насочен кон таа цел, а планот за закрепнување од катастрофа утврдува како организацијата може ефикасно и ефективно да се врати пристап до своите критични податоци и технолошки системи.

Според тоа, планот за закрепнување од катастрофа во суштина одговора на две работи:

- враќање на ИТ и комуникациските системи и технологии; и
- добивање на полн пристап до чисти податоци со добар квалитет на кои се потпира организацијата.

Видовите на непланирани проблематични настани кои можат да доведат до спроведување на планот за закрепнување од катастрофа вклучуваат:

- Природни катастрофи
- Војна или тероризам
- Јавни немири
- Несреќи или човечки грешки
- Компјутерски криминал

Тие настани можат да доведат до различни степени на проблемот, кои влијаат на:

- Еден центар за податоци или зграда
- Цела организација
- Локални системи или системи на ниво на град
- Регионални или национални системи
- Глобални системи

Ефективен план за закрепнување од катастрофа кој го сведува застојот на минимум, треба да ги земе предвид потенцијалните комерцијални загуби и влијанието врз репутацијата на организацијата и треба да и помогне на организацијата да ги избегне регулаторните или законските прекршоци.

Во планот за закрепнување од катастрофа треба детално да се опишат шест елементи:

1. Целосен попис на ресурсите (хардвер, софтвер и податоци)
2. Минимално прифатливо влијание (прекин на работа и ниво на услуга)
3. Документација за процесите и процедурите за закрепнување од катастрофа (договори на ниво на услуга, приоритети за закрепнување, ресурси за бекап, проверка на податоците)
4. Одговорности за закрепнување од катастрофа, оперативни и за овластување; т.е. кој ги работи активностите за закрепнување и кој ги одобрува
5. План за комуникација и односи со јавноста (за да се дадат одговори на клучните актери и регулатори и да се заштити репутацијата на организацијата)

6. Обука (планот е бескорисен ако никој не знае како да го употреби)

Заштитете го вашиот информатички систем

Крпеници (patch) и ажурирање (update)

Закрпете и ажурирајте го вашиот оперативен систем и софтверот на апликациите

Понекогаш може да биде заморно ажурирањето на вашите системи и апликации, но многу е важно тоа да се направи поради неколку причини:

1. **Безбедност**: ажурирањето помага во обезбедување на вашиот компјутер од напади. Како што се откриваат нови напади, така и се идентификуваат пропустите кои сајбер криминалците ги користат за да го компромитираат вашиот оперативен систем и апликации. Тие пропусти се решаваат со ажурирани верзии на софтверот (update).
2. **Нови можности**: Microsoft, Apple, Android и другите нудат нови можности кај ажурираниот софтвер, а софтверот на други компании понекогаш и не може да се користи ако овие системи не се ажурираат прво.
3. **Поправки**: не доаѓа секој проблем од вируси. Понекогаш проблемите се случуваат во системите и софтверите и едноставно треба да се поправат. Многу грешки кои влијаат врз крајните корисници се решаваат со ажурирани верзии.

Според тоа, паметно е да се **користи автоматско ажурирање на системите и апликациите**. На тој начин автоматски се преземаат основните безбедносни поправки кои ги решаваат слабите точки во системот.

Не заборавајте: кога ќе се појави малиот прозорец за ажурирање, тоа може да биде добра работа; но сепак не е добро да се клика на слепо.

Безбедни конфигурации

Користете безбедни конфигурации за сите уреди и софтвер

Еден начин да ги заштитите луѓето и организациите од малициозни активности е да користите безбедни конфигурации за уредите и софтверот. Истовремено, ова претставува голем предизвик бидејќи ја воведува скоро постојаната потреба за нови крпеници за оперативниот систем, надградување на апликациите и менување на мрежите. Според тоа, примарната цел е **документирање на сите ажурирања и промени**, за да се има увид во конфигурациите на сите системи.

Кога се прават промени во некоја апликација, тоа бара менување и ажурирање и на документацијата која е креирана за тој ресурс. Добрата документација треба да овозможи повторно градење на целата инстанца од самиот почеток и треба да вклучува:

- **Евиденција (лог - log) на промените** во оперативниот систем и апликациите (update), на промени во мрежата, итн. Сето тоа мора да биде соодветно документирано и следено.
- **Список на сите ресурси** во вашата организација. Целиот хардвер и софтвер треба да биде идентификуван и документиран.
- **Безбедносна основа** за ресурси. Тоа е договорен минимален стандард за безбедност кој се однесува, на пример, на исклучување непотребни услуги, бришење кориснички профили за гости, изложеност на јавен интернет, итн.
- **Постапка за проверка и одобрување** која лесно се следи. Добра пракса е да вршите проверка на вашите конфигурации и поставки од време на време, бидејќи инцидентите во вашето опкружување можат да ви дадат идеја за тоа што треба да се смени. Исто така, поединците не треба да ги менуваат поставките врз основа на сопствените потреби, туку треба да минат низ стандарден процес на одобрување.
- **Евиденција на промени во конфигурациите**.

Документацијата исто така треба да вклучува:

- Дијаграми на мрежи и уреди, како и шема на физичките центри на податоци
- Параметри за опкружувањето за работа на апликациите:
  * Воспоставена основа која треба да се следи
  * Поставки на ѕидот за заштита (firewall), верзиите на различните програми, верзиите на оперативниот систем
- Стандарди и конвенции за именување на:
  * Уредите (име и број на ресурсот на етикета, име на компјутерот, локација, сериски број)
  * Мрежата (етикетирање на портовите)
  * Конфигурацијата на доменот (имиња на кориснички налози, адреси на е-пошта)
- ИП шема

За крајните корисници, сигурната конфигурација бара:

- Отстранување и исклучување на сите непотребни кориснички налози
- Промена на фабричките лозинки или лозинките кои лесно се погодуваат („слаби лозинки“)
- Отстранување и исклучување на сиот непотребен софтвер
- Исклучување на сите опции за автоматско извршување на софтвер што овозможува извршување на датотеки без одобрување од корисникот

Чувствителни податоци

Шифрирајте ги сите чувствителни податоци

Шифрирање (енкрипција) е постапка за кодирање на податоците за да не можат да бидат прочитани без одреден клуч. На пример, сопствениците на шифрирани податоци можат да ги дешифрираат со користење на лозинка, биометриски информации или некој друг вид на клуч.

Шифрирањето е критичен елемент на сајбер безбедноста и може да се користи на различни начини за податоците да останат доверливи и приватни, како што се безбедните (HTTPS) веб сајтови, во безбедни апликации за праќање пораки и е-пошта и преку виртуелни приватни мрежи (VPN). Шифрирањето ги штити информациите додека тие активно се движат од една локација на друга (т.е. во транзит), од праќачот до примачот, а исто така ги штити и информациите во мирување. Ако некој добие пристап до база на податоци во која постојат шифрирани информации, шифрирањето претставува додатен слој на безбедност.[4]

Со други зборови, **шифрирањето помага во заштитата на чувствителни и приватни информации бидејќи ги прави нечитливи за сајбер криминалците**, дури и ако ги извлечат тие информации.

Препознавањето на чувствителните информации во вашето посебно опкружување кои треба да се шифрираат е од клучно значење и тие, меѓу другото, вообичаено вклучуваат:

- Информации со лични идентификатори
- Финансиски податоци
- Здравствени податоци
- Броеви на кредитни картички

Сузбивање на малициозен софтвер (малвер - malware)

Воведување на антималвер софтвер

Малвер или малициозен софтвер е секоја програма која е осмислена да врши несакани или штетни функции кои влијаат врз компјутерите, серверите и мрежите. Според тоа, антималвер софтвер е неопходен дел на безбедносните алатки.

Пред многу години, компаниите за сајбер безбедност се обидуваа да креираат едно универзално анти-вирусно решение кое да одговори на сите наши потреби во еден производ. Меѓутоа, тоа повеќе не е ефективно, бидејќи сајбер криминалците еволуираа. Заканата која ја претставуваат

4 Should I Encrypt Sensitive Files on My Computer? - Experian

постојано станува сè пософистицирана, што доведува до тоа компаниите да развијат конкретни антималвер програми.

Важно е да се разбере дека сите вируси се малвер, но не се сите малициозни софтвери вируси. Компјутерскиот вирус самиот се множи и се шири од корисник на корисник, додека антивирус програмата идентификува познати закани преку откривање на уникатни потписи. Меѓутоа, модерните малвер скенери користат хевристично откривање кое може проактивно да бара малициозен код.

Антималвер решенијата ќе го блокираат најголемиот дел од малициозните и потенцијално несакани програми и ќе ги скенираат влезните податоци за да го спречат малициозниот софтвер да се изврши на уредот, да менува поставки или да изврши некој дополнителен компромитиран софтвер. Тие исто така ги блокираат корисниците од пристап до веб сајтови за кои е познато дека дистрибуираат малициозен код (фишинг и рансомвер напади).

Покрај тоа, антималвер софтверот нуди:

- Заштита во реално време
- Скенирање при вклучување на уред
- Скенирање на надворешни уреди
- Заштитна на чувствителни информации
- Заштита од несакани пораки (спам) и кражба на идентитет

Фајрвол - Firewall (огнен ѕид)

Воведете фајрвол

Фајрволот дава заштита од сајбер напади и помага во чувањето на компјутерите и мрежите. Тој може да биде софтверски или хардверски, на уред или на мрежа, но сите работат на ист начин вршејќи проверка на сообраќајот и блокирајќи ги несаканите пакетчиња податоци.

Фајрволот во голема мерка го намалува ризикот по поединци и организации. Организациите кои не користат фајрвол само им ја олеснуваат работата на сајбер криминалците, давајќи им потенцијален пристап до системите и датотеките, како и можност да шират малициозни содржини. Според тоа, адекватно конфигуриран, одржуван и следен фајрвол е клучен за заштита на вашите податоци, вашите мрежи и вашите уреди.

Меѓу другото, тој ве штити од:

- Пријавување од далечина
- Кражба на сесии на електронска пошта
- Слабите точки во апликациите и ОС
- Оневозможување на услуги (DoS)
- Бомби преку е-пошта
- Малициозни макроа

ВИ-ФИ мрежи

Заштитете ги вашите безжични мрежи

ВИ-ФИ мрежите мораат да бидат безбедни, шифрирани и сокриени:

- **Енкрипцијата на безжичните мрежи мора да биде вклучена**. Таа е од суштинско значење за безбедноста. Поради тоа, вашиот рутер мора да поддржува WPA2 енкрипција и мора да биде заменет ако не ја поддржува.
- **Ажурирајте го софтверот со нови безбедносни верзии и крпеници**.
- Размислите за локацијата на рутерот како за безбедносно прашање. Луѓето често не се свесни дека рутер кој се наоѓа покрај врата или прозорец ја зголемува шансата дека ВИ-ФИ сигналот ќе биде пресретнат од лице со малициозни намери. За да ја подобрите вашата ВИ-ФИ безбедност, **најдобро е да го поставите рутерот што е можно поблиску до средината на вашата канцеларија**, бидејќи со тоа ја намалувате шансата хакери да се поврзат на

вашата мрежа.
- **Вклучете филтрирање на MAC адреси** за да ги контролирате уредите кои имаат пристап до вашата мрежа.
- **Исклучете го управувањето од далечина**.
- **Креирајте посебна ВИ-ФИ мрежа за клиенти**, за да не ја користат вашата интернет мрежа.

Поставки на интернет пребарувачот

Конфигурирајте ги безбедносните поставки на интернет пребарувачот

Интернет пребарувачи постојат на скоро секој уред. Поради тоа што нив постојано ги користиме во секојдневниот живот, од суштинска важност е безбедно да ги конфигурираме, особено бидејќи тие вообичаено доаѓаат со основни фабрички поставки.

Интернет пребарувачите претставуваат важна мета за напад на сајбер криминалците, а небезбедниот пребарувач може да го изложи корисникот или организацијата на инсталирање малициозни содржини без знаење на корисникот. Во некои случаи, тоа може да доведе до губење на контрола над уредот, користење на корисничките информации или дури употреба на уредот за напад на други лица.

Секој интернет пребарувач (Firefox, Chrome, DuckDuckGo, Brave, itd.) треба да биде безбеден. Во тоа, секогаш направете го следното:

- Вклучете автоматско ажурирање. Овој клучен чекор ќе ја заштити вашата организација од многу слаби точки кои се откриваат секој ден. Тоа е суштинска компонента на добрата сајбер хигиена за вашиот интернет пребарувач која ќе ви помогне да останете сигурни и безбедни.
- Блокирајте ги поп-ап известувањата, софтверските додатоци (plugin) и фишинг сајтовите. Повеќето поп-ап известувања се реклами, кои можат да бидат заразени со малициозни содржини, а софтверските додатоци се познати по своите ризици по безбедноста.
- Немојте да чувате лозинки во пребарувачот. Оваа погодна навика не се препорачува, бидејќи ако пребарувачот е компромитиран, компромитирани се и сите акредитиви кои се чуваат во него.
- Исклучете ги колачињата (cookies) на трети страни.
- Деинсталирајте ги сите екстензии на пребарувачот кои не ги користите.
- Редовно ажурирајте ги сите екстензии кои ги користите.

Личниот избор исто така влијае врз безбедноста на пребарувачот, како што е пристапот на корисникот до **https сајтови наместо http сајтови**.

Мобилни уреди

Обезбедете ги мобилните уреди

Мобилните уреди можат да создадат значителни безбедносни и раководни предизвици, особено ако содржат доверливи информации или ако можат да пристапат до деловната мрежа.

За контрола на употребата на мобилните уреди, организациите треба да бараат од корисниците да:
- ги штитат уредите со лозинки;
- ги шифрираат сите податоци; и
- инсталираат безбедносни апликации кои спречуваат кражба на информации кога телефонот користи јавни мрежи.

Организациите исто така треба да:
- Воспостават процедури за пријавување во случај на изгубена или украдена опрема.
- Ги конфигурираат уредите автоматски да се заклучуваат по одредено време.

ИоТ уреди (Уреди поврзани на интернет)

Обезбедете ги сите ИоТ уреди

Сè поголемата важност на технологијата во нашите живот овозможи „интернет на работите“ или ИоТ (Internet of Things – IoT). Тоа значи дека широк спектар на уреди е поврзан на интернет преку ИоТ сензори кои им овозможуваат да собираат и разменуваат податоци во реално време. Поради тоа што собира податоци од физички и виртуелни системи, ИоТ претставува големо „поле за напад“ за сајбер напаѓачите, ако не е обезбедено.

Обезбедување на ИоТ мрежата значи обезбедување на уредите пред тие да се вклучат на мрежата. За да го направите тоа:

- Сменете ги фабричките лозинки
- Користете силни лозинки
- Ажурирајте го софтверот на уредите (секогаш проверете ги достапните верзии за ажурирање на интернет сајтовите на произведувачите пред да ги инсталирате на уредите)
- Шифрирајте го и проверете ја автентичноста на уредот
- Сменете ги фабричките поставки за приватност
- Сменете ги фабричките поставки
- Осигурете ја вашата мрежа и ВИ-ФИ
- Креирајте посебна мрежа за гости

Физичка безбедност

Погрижете се за физичката безбедност на уредите, особено на мобилните уреди

Физичката безбедност е исто толку важна како и сајбер безбедноста. Ако крадец украде лаптоп, најдиректната штета е губење на самиот уред, но ако крадецот е во состојба да им пристапи на информациите на уредот, сите тие информации можат да бидат под ризик. Исто така постои и потенцијал да им се пристапи и на дополнителни информации користејќи ги податоците кои се наоѓаат на овие уреди, вклучувајќи и чувствителни информации за деловни кориснички профили или кориснички профили на клиенти – како што се лозинки или информации за кредитни картички – на кои не би требало да им пристапуваат неовластени лица.[5]

За да се заштитите себе и другите во организацијата:

- Обезбедете го вашиот уред со лозинка и вклучете двофакторска аутентификација (2FA)
- Секогаш чувајте ги вредните работи на себе и никогаш не ги оставајте уредите без надзор, особено кога патувате

Пристап од далечина

Ако вашата организација користи пристап на далечина, тој треба да биде безбеден, шифриран и сокриен. Тоа бара:

- Проверка дали целиот софтвер за пристап од далечина е закрпен и ажуриран.
- Ограничување на пристапот од далечина од сомнителни географски локации или ИП адреси.
- Ограничување на пристапот од далечина на вработените само на системите и компјутерите кои им се потребни да ја работат својата работа.
- Услов да имате силна лозинка за да добиете пристап од далечина.
- Вклучување на повеќефакторска аутентификација, ако е можно.
- Проверка дали следењето и предупредувањето е вклучено за да добиете предупредување за сомнителен напад или сомнителна активност.

5 https://www.cisa.gov/uscert/ncas/tips/ST04-017

Применете ги добрите пракси

Лозинки

Секоја организација треба да има политика за лозинки за да биде сигурна дека се користат ложени и посебни лозинки и дека тие редовно се менуваат. Лозинките се првата линија на одбрана од неовластен пристап.

Политиката за лозинки е неопходна за да се избегнат најчестите слаби точки, како што се:

- Навиката на корисниците да ги чуваат лозинките во белешки, текстуални датотеки и други незаштитени документи до кои сајбер криминалците можат лесно да пристапат.
- Тенденцијата на корисниците да ги чуваат лозинките во пребарувачите, што претставува уште една мета за сајбер криминалците.
- Лозинки кои вклучуваат лични информации кои многу лесно се наоѓаат на интернет.
- Користење на само една лозинка за поголем број на кориснички налози.
- Размена на лозинките со колегите или преку е-пошта, инстант пораки или други платформи (ова е особено голема слаба точка ако лозинките не се менуваат редовно).

Најлесниот начин да го промените или ублажите однесувањето на корисниците во поглед на лозинките е да **користите програма за управување со лозинките**. Тоа овозможува креирање на сложени лозинки за различни кориснички налози, кои потоа сите се шифрираат и чуваат, така што корисникот треба да запомни само една лозинка за да пристапи до сефот кој ги содржи неговите лозинки. Програмата за управување со лозинките им помага на корисниците да генерираат лозинки и дава приказ колку е силна лозинката, може да го извести корисникот за безбедносни упади поврзани со нивната е-пошта и повеќе.

Ако вашата организација не користи програма за управување со лозинки, еве неколку **совети за креирање на политика за лозинки**:

- **Подолгите лозинки се подобри** бидејќи е потребно повеќе време за да се хакираат. Според тоа, лозинките треба да содржат најмалку 12 карактери.
- **Сложеноста е клучна**! Лозинките треба да содржат симболи, комбинација на големи и мали букви и бројки. А потоа треба и да ги измешате.
- **Користете бесмислици** и избегнувајте предвидливост. Во идеален случај, лозинките не треба да содржат зборови кои можат да се најдат во речник (на ниту еден јазик).
- **Лозинките треба да бидат уникатни**. Правилото во секоја организација треба да биде: еден кориснички налог, една лозинка.

Исто така важно е да се сменат фабричките лозинки пред да го дадете уредот на вработените, за да го избегнете ризикот од можно изложување на хакери или некој друг голем упад.

Повеќефакторска аутентификација

Користете повеќефакторска аутентификација секогаш кога можете

Постојат три начини на кои компјутер, или било кој систем, може да го идентификува корисникот. Може да постави прашање за тоа што корисникот го знае, е или има. Тоа се **трите фактори на аутентификација**. Златниот стандард за проверка на идентитет е повеќефакторска аутентификација која користи најмалку два од овие фактори.

Идејата е дека две различни лозинки не се многу подобри од една, но дека два фактори се. Тоа е причината зошто повлекување на пари од банкомат бара двофакторска аутентификација: нешто што лицето го има (картичка за банкомат) и нешто што лицето го знае (својот ПИН).

Лозинките сами по себе веќе не се сметаат за безбедни, бидејќи хакерите имаат развиено безбројни методи со текот на години за кражба на потребните акредитиви за добивање на неовластен пристап до приватните кориснички налози. Тажната вистина е дека скоро 90% од тие инциденти можеле да бидат блокирани со користење на повеќефакторска аутентификација.

Секогаш кога тоа е можно, организациите треба да воведат двофакторска аутентификација за корисниците (2FA), за да:

- ги обезбедат корисниците од кражба на идентитет поради кражба на лозинка.
- ја заштитат организацијата од слабите лозинки на вработените.
- ја намалат употребата на неконтролирани уреди, особено со зголемената стапка на работа од дома поради КОВИД пандемијата.
- ја зголемат ефективноста на другите безбедносни мерки.
- и помогнат на организацијата да ги исполни законските барања.

Кориснички налози (профили)

Користете ограничени кориснички налози за редовни и секојдневни цели

Со корисничките налози треба да се ракува многу внимателно, бидејќи нивната злоупотреба може да доведе до губење на информации, репутација на организацијата и пари.

Постојат два вида на кориснички налози: Стандарден корисник и Администратор.

Карактеристиките на Стандардниот кориснички налог се дека тој е:

- посоодветен за секојдневни задачи (користење на апликации, пребарување на интернет);
- конфигуриран да го заштити вашиот систем од очигледни напади; и
- не им дозволува на корисниците да направат промени кои влијаат на сите лица кои го користат компјутерот.

Корисничките налози на Стандардниот корисник имаат помала флексибилност од корисничките налози на Администраторите. Меѓутоа, од друга страна, малициозен софтвер инсталиран во рамки на Стандарден кориснички налог не може да направи многу штета на системските датотеки. Тоа е поради фактот дека напаѓачите кои добиле пристап преку Стандарден кориснички налог можат само да им пристапат на датотеките на тој корисник. Во таа смисла, ограничувањата на Стандардниот кориснички налог се од полза за организацијата ако непријател или малициозен програм добијат пристап.[6]

Пристап на вработените

Пристапот треба да биде ограничен за ниеден вработен да нема пристап до сите системи

Се препорачува на ниту еден вработен да не му се даде пристап до сите системи со податоци. Вработените треба да добијат пристап само до одредени системи кои содржат податоци кои им се потребни да ја работат својата работа.

Не им дозволувајте на вработените да инсталираат софтвер без одобрување

Вработените никогаш не треба да бидат во можност да инсталираат софтвер без дозвола.

Логирање (евидентирање)

Спроведување на логирање

Од безбедносна перспектива, лог (евиденција, запис) функционира како црвено знаменце кога нешто лошо ќе се случи. Редовното прегледување на логови може да помогне во откривањето на малициозни напади врз вашиот систем.

Лог на кој лесно може да му се пристапи и кој вклучува критични информации може да ги спаси информациите или компјутерскиот систем. Логирањето помага со:

- Откривање на грешки во програмата
- Следење на грешките
- Решавање на проблеми со перформансите

6 Why You Shouldn't Use an Admin Account as Your Main Account - Make Tech Easier

- Сметководство
- Ревизија
- Безбедност

Лог датотеките исто така можат да се користат за да се одржи усогласеност со законските барања. Многу организации мораат да бидат во согласност со различни прописи кои бараат редовна ревизија на активности, вклучувајќи и давање на кориснички налози или пристап до финансиски системи.

Најголемиот проблем поврзан со логирањето е недостатокот на мониторинг. Важно е да се разбере што треба да се евидентира, врз основа на најдобри пракси, и логовите да се разгледуваат секојдневно барајќи грешки, аномалии или сомнителни активности. Сепак, прекумерното логирање не е од помош, бидејќи создава премногу „бучава“ и бара поголем капацитет за чување на податоци. Според тоа, некои активности можеби имаат поголем приоритет за логирање од другите.

Свест за сајбер безбедност

Вообичаени сајбер закани

Сајбер нападот е малициозен и намерен обид од страна на лице или организација за влез во информатички систем на друго лице или организација. Вообичаено, напаѓачот сака да добие одредена корист од нарушувањето на мрежата на метата. Организациите се соочени со огромен број на сајбер напади, а напаѓачите користат различни стратегии за да се обидат или да ги извршат нападите.

Напади со социјален инженеринг

Нападите со социјален инженеринг ги доведуваат во заблуда и ги манипулираат метите, со цел добивање на информации или пристап до нивните компјутери. Овие видови на напади се потпираат на човечката интеракција и вообичаено вклучуваат манипулација на корисникот за да ги прекрши безбедносните процедури и најдобрите пракси за така да добијат неовластен пристап до системи или за корисниците да им дадат чувствителни информации.

Во нападите со социјален инженеринг, сајбер криминалците ги кријат своите прави идентитети и мотиви и се претставуваат како лица од доверба. Нападот потоа се врши преку мамење на корисникот да кликне малициозен линк или преку добивање на физички пристап до компјутерот.

Фишинг (Phishing)

Повеќето сајбер напади почнуваат со фишинг е-пошта. Фишинг е вид на социјален инженеринг во кој сајбер криминалците ја мамат жртвата да им даде чувствителни информации или да инсталира малвер.

И покрај тоа што техничките мерки за безбедност стануваат сè подобри, фишингот останува еден од најевтините и најлесните начини сајбер криминалците да добијат пристап до чувствителни и лични информации. Корисниците само треба да кликнат на линк и нивната безбедност може да биде загрозена до таа мерка да станат жртви на кражба на идентитет. Корисниците исто така можат да ги компромитираат своите лични информации, акредитиви за најави (кориснички имиња и лозинки) и финансиски информации (броеви на кредитни картички), ако кликнат на линкот.

Напаѓачите често го постигнуваат ова со малициозна е-пошта која делува како да е од извор од доверба, но понекогаш користат и други методи.

Како функционира фишинг?

Повеќето фишинг кампањи вклучуваат една од две основни методи:

Малициозен прилог (attachment) во е-пошта, кој вообичаено има алармантен наслов како „ФАКТУРА“. Кога ќе бидат отворени, овие прилози инсталираат малвер на машината на корисникот.

Линкови до малициозни веб сајтови кои често се клонови на легитимни сајтови. Посетувањето на сајтот може да доведе до преземање на малициозен софтвер или страницата за најава на сајтот може да содржи скрипти кои крадат акредитиви.[7]

Видови на фишинг напади

Целен фишинг (Spear Phishing)

Целен фишинг е малициозен напад со лажна е-пошта која е насочена против одредена организација или лице и претставува обид за добивање неовластен пристап до чувствителни информации Мала е веројатноста дека овој напад ќе биде извршен од случајни напаѓачи, туку од сајбер криминалци кои сакаат на тој начин да постигнат финансиска добивка или да соберат вредни информации.[8]

Во целниот фишинг напад, се праќа е-пошта од извор од доверба, но таа води кон лажен веб сајт кој е миниран со малициозен софтвер. Оваа е-пошта најчесто користи креативни методи за привлекување на вниманието на корисникот.

Целниот фишинг напад е далеку поефективен од другите фишинг напади, бидејќи бара од криминалците потрошат време и ресурси во истражување пред нападот, заради тоа што ќе бидат многу поуспешни ако научат за нивната мета пред нападот.

Лов на китови (Whale Phishing/Whaling)

Лов на китови (whale phishing) е сличен со целниот фишинг, со неколку важни разлики. Додека целниот фишинг е вообичаено насочен против членови на одредена група, ловот на китови е насочен против конкретно лице – вообичаено „најголемата риба“ во целната организација или лице со значително богатство и моќ.

Вишинг (Vishing)

Вишинг или „гласовен фишинг“ вклучува манипулација на луѓе преку телефон. Напаѓачите ја заведуваат метата да им открие чувствителни информации во обид да ги искористат тие податоци за своја лична корист, вообичаено финансиска.

Смишинг (Smishing)

Терминот смишинг се однесува на фишинг преку СМС пораки и вклучува текстуална порака наместо е-пошта. Метите вообичаено добиваат текстуална порака која содржи измама и која ги присилува да дадат лични или финансиски информации на сајбер криминалците кои се преправаат дека се државен орган, банка или друга легитимна компанија.

Смишинг напаѓачите често бараат лични или банковни податоци, како што се акредитиви на кориснички налози, броеви на кредитни картички и броеви за идентификација. Потоа, тие ги користат тие информации за спроведување на различни видови на напади, вклучувајќи и финансиски измами, измами со подароци и измами со поддршка за клиенти.

Како да ги спречиме фишинг нападите

Во електронска пошта: научете внимателно да ја гледате е-поштата, особено ако содржи прилози или интернет линкови

7 What is phishing? Everything you need to know | IT Governance U

8 Types of Cyber Threat in 2019 | IT Governance USA

Обучете ги вработените да ги препознаат обидите за фишинг и да пријават сомнителни инциденти. Еве неколку типични знаци дека е-поштата може да биде малициозна:

- **Лош правопис и граматика**. Професионалните компании или организации вообичаено имаат лекторски персонал за нивните клиенти да добијат висококвалитетни и професионални содржини на е-поштата. Ако пораката е полна со грешки, многу е поголема веројатноста дека се работи за измама.
- **Сомнителни линкови**. Корисниците никогаш не треба да кликаат линкови во е-пошта за кои се сомневаат дека се малициозни. Еден начин за тестирање на легитимноста на линкот е да ја држите стрелката на глувчето преку линкот – без кликање – за да утврдите дали адресата одговара на информациите во пораката.
- **Сомнителни прилози**. Ако корисникот добие е-пошта со прилог или од лице кое не го познава или од лице од кого не очекува дека ќе им прати прилог, тие мораат да размислат дали се работи за обид за фишинг. Се препорачува прилозите никогаш да не се отвораат пред да се провери нивната автентичност. Поради тоа што постојат различни начини напаѓачите да ги измамат примателите во верување дека приложената датотека е легитимна, важно е корисниците да знаат:
  * На иконката поврзана со прилогот не може да и се верува без друга потврда.
  * Треба да внимаваат на комбинирани екстензии на датотеките како што се „pdf.exe“, „rar.exe“ или „txt.hta“.
  * Во случај на сомнеж, најдобро е да се стапи во контакт со лицето кое наводно ја пратило конкретната е-пошта и да се праша за потврда дали пораката и прилогот се легитимни.
- **Присилни пораки**. Оваа е-пошта има за цел да створи чувство на паника или притисок и да доведе до брз и непромислен одговор на примателот. На пример, тие можат да вклучуваат изјави како „Морате да одговорите до крајот на денот!“ или можеби индицираат дека примателот ќе биде соочен со потенцијални финансиски последици ако не одговори.
- **Маскирање (spoofing)**. Оваа е-пошта користи **сомнителни линкови** кои делуваат како да се поврзани со легитимни веб сајтови или компании и можат да покажуваат поп-ап прозорци кои делуваат легитимно, но ги водат корисниците до лажни сајтови за измама. Еден вид на маскирање користи **сменети интернет** адреси кои во голема мерка личат на имињата на веб сајтовите на добро познати компании како „www.micorsoft.com“ илиі „www.mircosoft.com“.
- **Неусогласености**. Примателите треба да бидат сомничави ако текстот на одреден линк и URL не одговараат или ако не се усогласени името на праќачот, потписот и URL.[9]

Јавни ВИ-ФИ мрежи: внимавајте кога користите јавни ВИ-ФИ мрежи

Опкружени сме со јавни ВИ-ФИ мрежи во хотели, трговски центри, кафулиња, аеродроми итн. Многу од нас ја имаат лошата навика да се поврзуваат на овие мрежи без било какво размислување за безбедноста. Меѓутоа, тие претставуваат вистински безбедносни ризици и треба внимателно да се користат.

Најголемиот безбедносен проблем со јавните ВИ-ФИ мрежи е тоа што корисниците не знаат кој оперира со мрежата или кој друг е поврзан на мрежата.

поред тоа, организацијата треба да:

- **Ги обучи вработените за ризиците од користење на јавни ВИ-ФИ мрежи**.
- **Им забрани на вработените да пристапуваат до чувствителни податоци кога користат јавни ВИ-ФИ мрежи**.
- **Им даде упатства на вработените само да се поврзуваат на мрежи од доверба**.
- **Им забрани на вработените да се поврзуваат на сајтови заштитени со лозинки користејќи јавни ВИ-ФИ мрежи**.

Треба да се разгледаат други опции, наместо користење на јавни ВИ-ФИ мрежи. На пример, телефонот може да послужи како мобилна ВИ-ФИ мрежа, што му овозможува на корисникот да ја контролира мрежата и кој ја користи. Ако мора да се користи јавна ВИ-ФИ мрежа, може да се употреби виртуелна приватна мрежа (VPN) за да се шифрираат податоците кои се праќаат преку ВИ-ФИ мрежата, со што се кријат овие податоци од сите кои „слушаат“ на таа мрежа.

9 Protecting against coronavirus themed phishing attacks (microsoft.com)

Компромитирање на деловна е-пошта (Business Email Compromise)

Компромитирање на деловна е-пошта (BEC) е вид на измама која цели на компании кои користат електронски трансфери и имаат снабдувачи во странство. Корпоративните или јавно достапните адреси на е-пошта на извршните лица или вработени на високо ниво кои работат со финансии или се вклучени во електронски плаќања или се лажираат или се компромитираат со програми за снимање на отчукувања на тастатура (key logger) или со фишинг напади за да се направат лажни трансфери. Тоа може да доведе до загуби од стотици илјади долари.[10]

Преземање на податоци во „проаѓање“(Drive-By Downloads)

Во напади со преземање на податоци во „проаѓање“ се преземаат малициозни скрипти на компјутерите или други уреди без знаење на корисникот, со што корисникот се изложува на различни сајбер напади. Тоа може да се случи на секој уред и на било кој оперативен систем и вообичаено се случува кога корисникот ќе посети и пребарува компромитиран веб сајт.

Напад Човек-во-средина (Man in the Middle (MITM))

Овој напад се случува кога сајбер криминалецот тајно ќе се вклучи меѓу два уреда или меѓу уред и небезбедна ВИ-ФИ мрежа, со цел пресретнување на комуникациите кои потоа тој може да ги чита и/или менува. Во тој случај, корисникот може ненамерно на сајбер криминалецот да му прати акредитиви или други информации.

Напади со фрлен УСБ уред

Во овој напад, УСБ уред кој содржи малициозен код се приклучува на компјутер.

Вообичаено, сајбер заканата претставена со овој напад е инфекција со малициозен софтвер или вирус. Инфекциите преку УСБ дискот можат да бидат намерни и ненамерни, зависно од конкретниот малициозен софтвер.

Би било паметно организациите да прекинат да и веруваат на застарена УСБ технологија и да почнат да ја користат моќта на безбедните дигитални мрежи и чување на податоци на облак (cloud).

Малвер (malware – малициозен софтвер)

Малвер е генерален термин кој што се користи за дефинирање на секоја датотека или програма која има за цел да оштети или наруши компјутер. Тој вклучува:

- **Ботнет софтвер** кој е осмислен да инфицира голем број на уреди кои се поврзани на интернет. Некои ботнет (мрежи на роботи) се составени од голем број на уреди од кои секој користи релативно мала процесорска сила. Со тоа се отежнува откривањето на овој вид на малициозен софтвер, дури и кога ботнетот е во функција.
- **Рансомвер напади (напади со софтвер за уценување)**, кои ги шифрираат информациите на корисникот и бараат плаќање за клуч за дешифрирање за да се вратат информациите. Меѓутоа, плаќањето на откупот не гарантира секогаш дека шифрираните податоци ќе бидат вратени.
- **Спајвер (шпионски софтвер)** се користи за незаконско следење на активностите на корисникот на компјутерот и собирање на лични податоци.
- **Тројанските вируси** делуваат како легитимен софтвер, но прават малициозни активности откако ќе бидат извршени.
- **Вируси и црви**, кои се малициозен код инсталиран без знаење на корисникот. Вирусите можат и да се множат и да се шират на други компјутери со тоа што се прикачуваат на други

10 https://www.trendmicro.com/vinfo/hk/security/definition/business-email-compromise-(bec)

компјутерски датотеки. Црвите исто така се множат сами, но тие не мораат да се прикачат на друга програма за да го направат тоа.[11]

DoS/DDoS напади

Дистрибуиран напад за оневозможување на услуги (DDoS) е сајбер напад во кој напаѓачот го преплавува серверот со интернет сообраќај за да ги спречи корисниците да пристапат до поврзаните интернет услуги и сајтови.

DDoS е поткатегортија на поопшт напад за оневозможување на услуги (Denial-of-Service (DoS)). Во DoS напад, напаѓачот користи една конекција за да ја преплави метата о лажни барања или за да проба да искористи некоја слаба точка во сајбер безбедноста. Според тоа DDoS е со поголеми размери и користи илјадници (дури и милиони) поврзани уреди за да ја постигне својата цел. Самиот број на вклучени уреди ја прави борбата против DDoS многу потешка.[12]

Постојат три општи видови на DDoS напади:

- **Волуметриски напад**: во овој класичен DDoS напад, се користат методи за генерирање на масовен сообраќај за во целост да се засити мрежниот проток на веб сајтот, со што се кочи сообраќајот и станува невозможно легитимниот сообраќај да му пристапи на или од целниот сајт.
- **Напади на протоколите**: овие напади се осмислени да ја изедат процесорската моќ на мрежните инфраструктурни ресурси како што се серверите, фајрвол и сервисите за поделба на мрежното оптоварување целејќи на Слој 3 и Слој 4 од протоколарната комуникација со барања за малициозни конекции.
- **Напади на апликации**: едни од пософистицираните DDoS напади, овие напади ги користат слабите точки во слојот на апликации – Слој 7 – со отворање на конекции и иницирање на процеси и барања кои ги трошат ограничените ресурси како просторот на дискот или достапната меморија.[13]

Редовни обуки

Со цел **подигање на свести за сајбер заканите и информатичката безбедност**, еден од најважните елементи на сајбер хигиената кој може да се спроведе во било која организација е обуката за безбедносната свест, за да се научат вработените да ги избегнат, идентификуваат и пријават потенцијалните закани.

Вклучувањето на персоналот во робустен курс за обука за безбедноста е проактивна мерка која организацијата може да ја преземе како заштита од сајбер напади. Ако не се земе предвид овој човечки елемент, вратите на вашата организација ќе бидат широм отворени за сајбер заканите.

Обуката за подигање на свеста за безбедноста го подобрува знаењето на корисниците за потенцијалните закани, со што се:

- намалуваат ризиците;
- спречува времето на неактивност;
- подобрува самодовербата на вработените; и
- поттикнува довербата на клиентите.

Според тоа, обуките за подигање на свеста за безбедноста е од витално значење во ефективната сајбер безбедност и сајбер хигиена. Исто така, со текот на времето, годишните обуки за дигање на свеста можат да ја сменат културата на сајбер безбедност во вашата организација. Во најмала рака, овие обуки треба да вклучуваат информации за:

- Чувствителни информации: што се и како да се ракува со нив
- Како да се препознае фишинг е-пошта
- Како соодветно да се користат службени уреди

11 Types of Cyber Threat in 2019 | IT Governance USA

12 https://www.fortinet.com/resources/cyberglossary/ddos-attack

13 https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained

- Како да се пријават инциденти
- Што да се направи во итен случај кој влијае врз компјутерските и информатичките системи
- Како да се ракува со информации кои содржат лични идентификатори (PII)
- Основна сајбер хигиена: што е и како да се примени

Напредните обуки треба да се фокусираат на содржината, материјалите за поддршка, фишинг тестирање, метрика, извршување и анкети.

Успешните програми за подигање на свеста за безбедноста:

- Ги образуваат и поддржуваат вработените, а притоа не ги обесхрабруваат или посрамотуваат.
- Не се фокусираат само на фишинг кампањи (целта е вработените да научат да ги препознаваат и пријавуваат заканите во реално време, кои имаат бројни појавни облици кои секогаш се менуваат).
- Избегнуваат повторување на иста содржина и сакаат да ги збогатат вработените со нови информации на секоја обука.
- Вклучуваат материјали кои одат подалеку од професионалниот свет до приватните животи на вработените, бидејќи со тоа се персонализира содржината и вработените имаат повеќе волја да слушаат.

Се препорачува исходите од обуките – позитивни или негативни – да останат интерни и да не се споделуваат со различните актери.

Резиме

Скоро сите сајбер напади ги искористуваат условите кои спаѓаат под лоша сајбер хигиена. Тоа вклучува крпеници на софтверот кои недостасуваат, лоши конфигурации и ниска свест кај корисниците. Според тоа, недостатокот на конзистентна сајбер хигиена е една од најопасните закани која може да се јави внатре во организацијата. За да поттикнете добра сајбер хигиена во целата ваша организација:

- Обезбедете доволно обуки за вашите вработени да ги идентификуваат и пријават сомнителните сајбер активности.
- Осигурете се дека сите сервери, работни компјутери, паметни телефони и други уреди кои ги користат вработените често безбедносно се ажурираат.
- Имплементирајте строга политика за пристап до системот која бара повеќефакторска аутентификација секаде каде што тоа е можно и строги стандарди за лозинки.
- Вложете во систем и решенија кои овозможуваат јасна видливост и грануларна контрола на пристап до целата мрежна инфраструктура на организацијата.

Иако можеби делува дека сложеноста е непријател на сајбер криминалците, таа всушност е непријател на вашата сопствена сајбер безбедност. Во сложениот и динамичен сајбер свет, вашата најдобра одбрана е да се вратите на основите.

За да го подобрите и проширите опсегот на сајбер хигиената, не е доволно организацијата само да им понуди примери на вработените и да зборува за важноста на сајбер хигиената во организацијата. Во секоја организација, сајбер хигиената мора да биде конкретно дефинирана, а потоа и поддржана со метрика и образование.

Рамката за безбедност е одлична почетна точка, но таа мора да биде:

- Со вистинска големина за потребите на вашата организација
- Усогласена со вашите единствени законски услови
- Придружена со обука која е достапна и која вашата организација може да си ја дозволи
- Одржлива/повторлива со ресурсите на вашата организација
- Да ги поддржува вашите деловни и оперативни цели

Заклучок

На крајот, лошите сајбер навики – или ниската сајбер хигиена – се причина за најуспешните сајбер напади. Заради тоа е толку важно организацијата да развие култура на добра сајбер хигиена. Меѓутоа, мерките препорачани во овој Прирачник, иако главно претставени од перспективата на организациска безбедност, се применливи и на организации и на поединци. Според тоа, организациите треба да им потенцираат на вработените да размислат за примена на навиките на сајбер хигиена и во домот. Сепак, добрите навики на сајбер хигиена кои се користат во домот веројатно повеќе ќе се користат и на работа. Понатаму, сите ние сме побезбедни во сајбер светот во кој културата на сајбер хигиена се однесува и на личниот и на професионалниот простор.

Референтни материјали

ENISA: Review of Cyber Hygiene practices https://www.enisa.europa.eu/publications/cyber-hygiene

Centre for Cyber Security Belgium: Cyber security guide for SME https://ccb.belgium.be/sites/default/files/CCB-EN%20-C.pdf

ANSSI: Guideline for a healthy information system https://www.ssi.gouv.fr/uploads/2013/01/guideline-for-a-healthy-information-system-in-42-measures_v2.pdf

CPME-ANSSI: Guide Des Bonnes Pratiques De L'informatique https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

NIST: Small business information security: the fundamentals https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

CISA: Cyber Essentials Starter Kit https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

CMU SEI: Cyber Hygiene: 11 Essential Practices https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/

Canadian Centre for Cyber Security: Cyber Hygiene https://cyber.gc.ca/en/guidance/cyber-hygiene

Kaspersky: Good cyber hygiene habits to help you stay safe online https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

ANSSI: 40 Essential measures for a healthy network https://www.ssi.gouv.fr/uploads/2013/01/guide_hygiene_v1-2-1_en.pdf

US House of Representatives: Promoting Good Cyber Hygiene Act of 2017 https://www.congress.gov/115/bills/hr3010/BILLS-115hr3010ih.pdf

NCSC NL: Cyber Hygiene in the Netherlands https://english.ncsc.nl/research/research-results/cyber-hygiene-in-the-netherlands

NIST NCCoE: Critical Cybersecurity Hygiene: Patching the Enterprise https://www.nccoe.nist.gov/projects/critical-cybersecurity-hygiene-patching-enterprise

CISA: Cyber Hygiene Services https://www.cisa.gov/cyber-hygiene-services

CYBER4Dev: Cyber Security Hygiene/Awareness https://cyber4dev.eu/cyber-security-hygiene-awareness/

eGA: What is Cyber Hygiene? https://ega.ee/blog_post/podcast-what-is-cyber-hygiene/

Анекс: Листа на добри пракси

АНАЛИЗИРАЈТЕ ГО СИСТЕМОТ И УТВРДЕТЕ ГИ ПРОЦЕДУРИТЕ И РИЗИЦИТЕ		
Категорија	**Добри пракси**	**Релевантни чинители**
Попис на хардвер и софтвер	- Одржувајте попис на хардвер и софтвер - Стандардизирајте го вашиот попис на хардвер и софтвер -	Јавни институции и МСП
Попис на чувствителни или критични информации	- Одржувајте попис на чувствителни или критични информации - Разберете го вашето податочно опкружување и идентификувајте ги важните податоци во вашата средина - Креирајте политика за класификација на податоци - Шифрирајте ги податоците, особено податоците класифицирани како „ограничени“ - Воведете систем за спречување на губење на податоци	Јавни институции и МСП
Анализа на ризик	- Идентификувајте ги ризиците • човечки ризик (измама, кражба, човечка грешка) • природен ризик (поплави, пожари, земјотреси, итн.) • технички ризици (дефект на софтвер, хардвер, недостаток на знаење) - Избегнувајте го ризикот – ако не претставува директна закана по вашето работење - Намалете го ризикот – со воведување на нови безбедносни решенија - Прифатете го ризикот – кога е мала веројатноста дека ризикот ќе се случи или е надвор од тековните капацитети - Пренесете го ризикот – со осигурување	Јавни институции и МСП
Процедури за бекап (резервни копии)	- Воспоставете процедура за редовен бекап - Бидете реални при креирањето на бекап политики и подгответе пишан план за бекап кој пропишува: • Што се става на бекап? • Каде се наоѓа бекапот? • Колку често се врши бекап? • Кој е задолжен да врши бекап? - Секогаш дајте им највисок приоритет на клучните податоци - Секогаш тестирајте го вашиот бекап - Користете го правилото 3-2-1 - Користете чување на податоци на далечина/cloud - Често и редовно ажурирајте го бекапот	Јавни институции и МСП
Реакција на инциденти	- Изгответе план за реакција на инциденти или ПРИ - Кога ќе се случи инцидент клучно е да го се следи ПРИ	Јавни институции
Континуитет на работење и закрепнување од катастрофа	- Подгответе план за континуитет и закрепнување од катастрофа	Јавни институции

ЗАШТИТЕТЕ ГО ВАШИОТ ИНФОРМАТИЧКИ СИСТЕМ		
Оперативниот систем и софтверот на апликациите	- Закрпете и ажурирајте го вашиот оперативен систем и софтверот на апликациите, поради: • Безбедност • Нови можности • Поправки - Вклучете автоматско ажурирање на системите и апликациите	Јавни институции и МСП
Безбедни конфигурации	- Користете безбедни конфигурации за сите уреди и софтвер - Документирајте ги сите ажурирања и промени • Евидентирајте ги промените • Утврдете ја безбедносната основа • Спроведете процес за проверка и одобрување • Евидентирајте ги промените на конфигурациите	Јавни институции и МСП
Чувствителни податоци	- Шифрирајте ги сите чувствителни податоци - шифрирањето помага во заштитата на чувствителни и приватни информации бидејќи ги прави нечитливи за сајбер криминалците, бидејќи на нив може да им се пристапи само со клуч	Јавни институции и МСП
Антималвер софтвер	- Користете антималвер софтвер - Антималвер решенијата ќе го блокираат најголемиот дел од малициозните и потенцијално несакани програми	Јавни институции и МСП
Фајрвол (Firewall – огнен ѕид)	- Користете фајрвол за да го: • блокирате најголемиот дел малициозни и потенцијално несакани програми • спречите извршувањето на малициозен софтвер на уредот • спречите малициозниот софтвер да ги смени поставките • пречите малициозниот софтвер да изврши дополнителен компромитиран софтвер	Јавни институции и МСП
ВИ-ФИ мрежи	- Заштитете ги ВИ-ФИ мрежите - Користете енкрипција на безжичните мрежи - Ажурирајте го софтверот со нови безбедносни верзии и крпеници - Поставете го ВИ-ФИ рутерот што е можно поблиску до средината на вашата организација - Вклучете филтрирање на MAC адреси - Исклучете го управувањето од далечина - Поставете посебна ВИ-ФИ мрежа за гости	Јавни институции и МСП
Поставки на интернет пребарувачот	- Секогаш конфигурирајте ги безбедносните поставки на интернет пребарувачот - Блокирајте ги поп-ап известувањата, софтверските додатоци (plugin) и фишинг сајтовите - Немојте да дозволите лозинки да се чуваат во пребарувачот - Исклучете ги колачињата (cookies) на трети страни - Деинсталирајте ги сите екстензии на пребарувачот кои не ги користите - Редовно ажурирајте ги сите екстензии кои ги користите - Поттикнете ги корисниците да користат https сајтови наместо http сајтови	Јавни институции и МСП
Мобилни уреди	- Барајте од корисниците да: • Ги заштитат уредите со лозинки • Ги шифрираат податоците • Инсталираат безбедносни апликации кои ги спречуваат сајбер криминалците да крадат информации кога телефонот е поврзан на јавни мрежи • Ги конфигурираат уредите автоматски да се заклучуваат - Воспоставување на процедури за пријавување на изгубена или украдена опрема	Јавни институции и МСП

ИоТ уреди (уреди поврзани на интернет)	- Обезбедете ги ИоТ уредите: • сменете ги фабричките лозинки • користете силни лозинки • редовно ажурирајте го софтверот на уредите • шифрирајте го и проверете ја автентичноста на уредот • сменете ги фабричките поставки за приватност • сменете ги фабричките поставки • осигурете ја безбедноста на мрежата на организацијата и ВИ-ФИ мрежата • креирајте посебна мрежа за гости • секогаш проверете ги достапните верзии за ажурирање на интернет сајтовите на производувачите пред да ги инсталирате на уредите	Јавни институции и МСП
Физичка безбедност на уредите	- Погрижете се за физичката безбедност на уредите, особено на мобилните уреди: • Заштита на уредот со силни лозинки • Постојано чување на уредот кај корисникот/сопственикот	Јавни институции и МСП
Пристап на далечина	- Проверете дали целиот софтвер за пристап од далечина е закрпен и ажуриран - Ограничете го пристапот од далечина од сомнителни географски локации или ИП адреси - Ограничете го пристапот од далечина на вработените само на системите и компјутерите кои им се потребни да ја работат својата работа - Барајте силни лозинки за добивање на пристап на далечина - Вклучете повеќефакторска аутентификација, ако е можно - Проверете дали следењето и предупредувањето е вклучено за да добиете предупредување за сомнителен напад или сомнителна активност	Public institutions & SMEs

ПРИМЕНЕТЕ ДОБРИ ПРАКСИ		
Лозинки	- Подолгите лозинки се подобри - Сложеноста е клучна! Барајте симболи, комбинации на големи и мали букви и бројки - Користете бесмислици и избегнувајте предвидливост - Лозинките треба да бидат уникатни - Сменете ги сите фабрички лозинки	Јавни институции и МСП
Повеќефакторска аутентификација	- Користете повеќефакторска аутентификација секогаш кога можете - Користете два или три фактора за проверка на автентичност – нешто што корисникот го знае, е или го има	Јавни институции и МСП
Кориснички налози	- Користете ограничени (Стандардни кориснички) налози за редовни и секојдневни цели - Воспоставете Стандардни кориснички и Администраторски налози за различни цели	Јавни институции и МСП
Пристап на вработените	- Немојте на ниту еден вработен да му дадете пристап до сите системи со податоци - На вработените дајте им пристап само до оние системи кои содржат податоци кои им се потребни за нивната работа - Не им дозволувајте на вработените да инсталираат софтвер без дозвола	Јавни институции и МСП
Логирање (евидентирање)	- Одржувајте конзистентно логирање - Разберете што треба да се евидентира, врз основа на најдобри практики, и разгледувајте ги логовите секојдневно барајќи грешки, аномалии или сомнителни активности	Јавни институции

<table>
<tr><th colspan="4">СВЕСТ ЗА САЈБЕР БЕЗБЕДНОСТА</th></tr>
<tr><td>Вообичаени сајбер закани</td><td>ВИД НА САЈБЕР ЗАКАНА</td><td>ПРЕПОРАКА</td><td rowspan="2">Јавни институции и МСП</td></tr>
<tr><td></td><td>- Социјален инженеринг
- Фишинг напади (Phishing)
• Spear Phishing (целен фишинг)
• Whale Phishing/Whaling (лов на китови)
• Vishing (гласовен фишинг)
• Smishing (СМС фишинг)
- Компромитирање на деловна е-пошта (BEC)
- Преземање на податоци во „проаѓање“ (Drive-By Downloads)
- Напади Човек-во-средина (MITM)
- Напад со фрлен УСБ уред
- Малвер (малициозен софтвер)
• Ботнет софтвер
• Рансомвер напад
• Спајвер
• Тројански вирус
• Вируси и црви
- DoS/DDoS напади (оневозможување на услуга)
• Волуметриски
• Напади на протокол
• Напади на апликации</td><td>- Е-ПОШТА: внимателно гледајте ја е-поштата, особено ако содржи прилози или веб линкови. Барајте:
• Правопис и лоша граматика
• Сомнителни линкови
• Сомнителни прилози
• Закани во јазикот
• Маскирање
• Сменети веб адреси
• Неусогласености
- ЈАВНИ ВИ-ФИ МРЕЖИ: секогаш внимавајте кога се поврзувате на јавни ВИ-ФИ мрежи:
• Не пристапувајте на чувствителни податоци
• Поврзувајте се само на мрежи од доверба
• Одберете ја опцијата да не се поврзува автоматски</td></tr>
<tr><td>Редовни обуки</td><td colspan="2">- Подигнете ја свеста за сајбер заканите и информатичката безбедност со годишни или почети обуки
- Робустен курс за обука за дигање на свеста за безбедноста треба да покрива:
• Чувствителни информации: што се и како да се ракува со нив
• Како да се препознае фишинг е-пошта
• Како соодветно да се користат службени уреди
• Како да се пријават инциденти
• Што да се направи во итен случај кој влијае врз компјутерските и информатичките системи
• Како да се ракува со информации кои содржат лични идентификатори (PII)
• Основна сајбер хигиена: што е и како да се примени</td><td>Јавни институции и МСП</td></tr>
</table>

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva