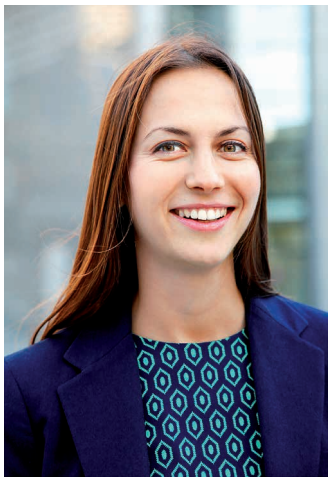
КИБЕРСИГУРНОСТ ЗА МАЛКИ И СРЕДНИ ПРЕДПРИЯТИЯ

ВСИЧКО, КОЕТО ЕДИН БИЗНЕС ТРЯБВА ДА ЗНАЕ ЗА КИБЕРСИГУРНОСТТА

група на ЕНП в европейския парламент

ПРЕДГОВОР



Дигиталната трансформация на Европа предоставя огромен шанс и предизвикателство за всички държави-членки, техните граждани и бизнеса. През 2020-а година станахме свидетели на ускорена цифровизация. Малки и средни предприятия (МСП) трябваше да реорганизират и дигитализират процесите си в рамките на броени седмици, за да отговорят на променената икономическа ситуация. Това се оказа и отлична възможност за киберпрестъпниците, които атакуваха различни компании от цял свят всекидневно.

За да подпомогнем бизнеса в България и Европа и да намалим рисковете от кибер атаки, в групата на ЕНП в Европейския парламент (ЕП) поставяме киберсигурността и кибер хигиената като топ приоритети за постигане на безопасна онлайн среда в Европейския съюз. През годините работихме върху създаване на центрове за върхови постижения в киберсигурността, за увеличаване на правомощията и възможностите за реакция на Европейската агенция за киберсигурност (ENISA), както и за подобряване на международното сътрудничество в сферата.

Вярвам, че нормализирането на кибер инциденти не е правилният път пред нас. Правилният път пред нас е подобряване на координацията при атаки; усъвършенстване на дигиталните и кибер умения на всяко ниво; подобряване на капацитета за реакция при инциденти и повишаване на кибер устойчивостта. Това е моят фокус на работа като докладчик от групата на ЕНП за Директивата за мрежова и информационна сигурност за постигане на високо общоевропейско ниво на киберсигурност.

Също както при опазването на обществения ред, така и в кибер пространството, безопасността и сигурността зависят от действията на всеки един бизнес, институция и гражданин. Този наръчник е насочен да осведоми и подкрепи малките и средни предприятия в процеса им на безопасна дигитална трансформация. Той е част от усилията, които в най-голямото и отговорно политическо семейство на ЕНП в Европейския парламент полагаме, за да може всеки гражданин и бизнес във всеки град и регион да защити своите данни и активи.

СЪДЪРЖАНИЕ

I УВОД В КИБЕРСИГУРНОСТТА

Цифровизацията през последните 20 години е основен двигател на развитието на глобалната икономика и общество, като тази тенденция не подминава и България. Кризата с пандемията от COVID-19 придаде нов тласък на тези технологични процеси, като ги направиха задължителен елемент в новата реалност.

Само в рамките на няколко месеца през 2020 г. милиони малки и средни предприятия (МСП) трябваше да дигитализират голяма част от дейността си с рекордни темпове, за да отговорят на пандемията и необходимостта от социална дистанция. Онлайн или цифровите технологии се оказаха ключови за просперитета и устойчивостта им. В публичното пространство обикновено се говори за големите кибератаки, които засягат много потребители, чрез пробив на публични институции и глобални корпорации, но останалите такива остават в сянка. Това може да създаде измамно чувство на сигурност, че дребния и среден бизнес не е обект на подобна заплаха.

Според ENISA (Европейската агенция за киберсигурност), най-използваните услуги от МСП са свързани с работа от вкъщи, банкови трансакции, имейл и търсене на информация онлайн. Следващите по популярност сред малкия и средния бизнес са електронното обучение и търговия. В резултат на засиленият фокус върху дигитализацията, киберсигурността се превърна в основна грижа за МСП, като за 85% от тях киберсигурността е основен проблем (ENISA 2021). Това не е случайно, защото с въвеждането на новите технологии и прехвърлянето на ключови процеси на компаниите във виртуалното пространство, те стават уязвими за хакерски атаки, ако не бъдат предприети необходимите мерки

Киберинцидентите имат тежки последици - прекъсване на дейността или увеличаване на разходите за извършване на стопанска дейност. Три основни заплахи продължиха да са в основата на кибер инцидентите при 40% от анкетираните МСП, именно: **фишинг, малуер (зловреден софтуер), уеб-базирани атаки. Ботнет** атаките също са главен проблем за българските МСП.

Недостатъчно добрата подготовка да посрещнат новите заплахи във виртуалното пространство ги прави основна мишена за киберпрестъпниците. Три фактора играят ключова роля за увеличаване на изложеността на МСП: повишената зависимост от цифровите технологии за осъществяване и продължаване на работата им; секторът на дейност (например сегменти, които работят с много клиентски данни са по-атрактивни за киберпрестъпниците) и липсата на мерки и практики за киберсигурност.

Най-съществена възможност за подобрение на цифровата безопасност на МСП е въвеждането на мерки за киберсигурност. Те биват организационни и технически, като са разгледани в настоящия наръчник.

По-специално, той предоставя преглед на:

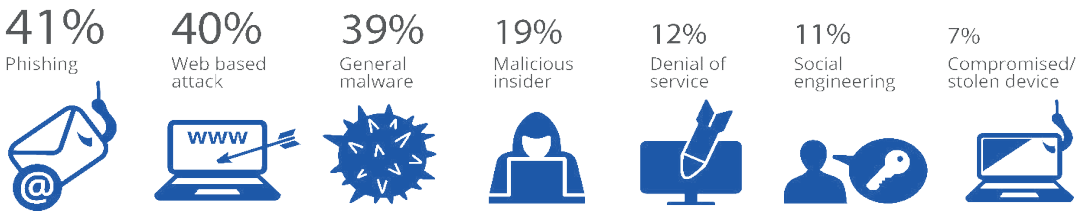
1. Информацията относно най-големите заплахи за киберсигурността на МСП
2. Съвети за основните мерки за сигурност, които всяко МСП може да приеме
3. Правна рамка и изисквания на ЕС и на ЕС за киберсигурност, както и препоръки за бъдещо развитие на политиките
4. Правителствени ресурси и контакти в България и ЕС за помощ с киберсигурността
5. Допълнителни насоки, образователни ресурси и инструменти за киберсигурността

Този наръчник надгражда и допълва работата на правителствените и неправителствените организации в ЕС (Европейската Агенция за Киберсигурност), САЩ, Обединеното кралство, Франция и Белгия, както и на Организацията за икономическо сътрудничество и развитие.

Графиките в този наръчник са заимствани от ръководството за киберсигурност за МСП на ENISA (Cybersecurity for SMEs, достъпен на https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes)

II ОСНОВНИ ЗАПЛАХИ

Тази глава разглежда основните заплахи, техния характер и цел, и предлага основните мерки за защита от различните специфични видове кибератаки.
Корпоративните и търговски тайни са основна цел на атакуващите заради стойността, която имат за собствениците им и тази на черния пазар. Инфраструктурата и потребителски данни (акаунт и парола) са друга привлекателна цел, представлявайки входна врата за последващи атаки. Както може да се очаква, финансова информация е също от интерес като елемент за осъществяване на финансови облаги от пробива в киберсигурността.
Според ENISA, най-голямата заплаха за МСП остава фишинг (phishing), уеб-базирани атаки (web-based attacks), злонамерен код (malware), като атаки от тип ботнет остават съществен проблем за България.



1 ФИШИНГ / СМИШИНГ

Фишинг е заплаха, както за големи, така и за малки предприятия. Този вид атака от т.н. тип социално инженерство примамва служителя неволно да асистира на атакуващия. Метод на атаката: служител получава съобщение по електронната поща или съобщение на телефона, SMS при смишинг, което изглежда изпратено от легитимен източник, например банка, управителя на фирмата, пощенски услуги или други доставчици на електронни услуги. Ако служителят се заблуди или не е наясно със заплахата, би последвал инструкцията, например да преведе финансови средства ньа атакуващите, представящи се за легитимна фирма или лице или да отвари вратата към данните и системата на компанията.

Два примера: фишинг имейл (публикуван на www.abv.bg) и смишинг SMS са представени по-долу.

Основните цели на фишинг/смишинг са:

- С инструкции за необходимостта от плащане (подобно на телефонните измамници), заблуждават жертвата и я подтикват, например, да плати фалшифицирана фактура.
- Кражба на данни, подобно на първия случай, тук инструкцията е да се въведат клиентски данни и пароли, например за отблокиране на сметката, с цел последваща атака чрез получените данни.
- Изнудване (т.н. рансъмуеър/ransomware), където се използва заразен файл или линк, при отварянето на който стартира злонамерен код на системата на служителя, който криптира всички достъпни данни. Жертвата получава съобщение с искане на откуп за ключа за декриптиране на данните. Откупа, в анонимна крипто валута, например биткойн, варира между няколко хиляди евро за МСП до няколко милиона евро при по-големи организации, средно 300 000 щатски долара през 2021 г.

За предпазване от фишинг/смишинг се използват:
- Информираността и обучението на персонала за разпозн аване и защита от този тип атака са най-важната и успешна мярка срещу фишинг;
- Блокиране на съобщението чрез защита на имейл с филтриращи и блокиращи функции срещу спам или фишинг кампании, които са забелязани, за да намали тази заплаха;

Защита на данните: създаване на резервно копие/backup не би спряло фишинг атаката, но ако архивирането е сигурно (на отделно място и с възможност за лесно извличане), ще предотврати последствията и финансовите загуби на компанията в случай на рансъмуеър.

За повече информация, виж т. 1.2 'Защити' и т. 6.4 'Допълнителна информация относно обучения и информираност на служителите', както и https://www.enisa.europa.eu/publications/phishing

2 ЗЛОНАМЕРЕН КОД (MALWARE)

Злонамерен код (malware) е вид електронна програма, разработена от злонамерени лица с цел заразяване на устройство (компютър, мобилно устройство) и извършване на неправомерни операции на заразеното устройство.

Основните цели на злонамерения код са:

- Криптиране, кражба или промяна на информацията, например за искане на откуп или препродажба на данните;
- ледене на потоците данни, например за корпоративен шпионаж;
- Отнемане на контрола върху устройството, например за предизвикване на инцидент или за блокиране на дейността на дружеството (инцидентът с Colonial Pipeline в САЩ е пресен пример, макар и за голяма по мащабите си атака).

За предпазване от злонамерен код бихте могли да:

- Инсталирате и поддържате специализиран софтуер за защита срещу злонамерен код (anti-malware): такъв софтуер се инсталира върху мобилни устройства, операционни системи и мрежи. Програмата сканира входящите данни за зловреден софтуер и блокира (или поставя под карантина) съмнителен или доказано зловреден код преди използването им. На пазара има много видове защитен софтуер, всеки с различна цена и предлагани допълнителни услуги за сигурността.

За повече информация, виж т. 1.2 'Защити' и глава 6 'Полезни контакти и допълнителна информация' (т. 6.1 и т. 6.2), както и https://www.enisa.europa.eu/publications/malware

3 УЕБ БАЗИРАНИ АТАКИ

Уеб базирана атака е вид атака, която използва интернет инфраструктурата на компанията, по-конкретно нейните слабости в сигурността и, за извършване на кибер атака върху индивидуални потребители или уеб сайтове (например търсачки, корпоративен сайт).

Основните цели на уеб базирана атака са:

- Инсталиране на злонамерен код на устройството на жертвата с цел извличане на чувствителна информация или вземане на контрол върху устройството;
- Кражба на (чувствителни) данни, които се съдържат в интернет сайтове, например клиентска база данни, включително и кредитни карти;
- Промяна на данни в интернет сайтове, например промяна на цената на продукт в количката за електронно пазаруване с цел облагодетелстване от ниска цена;
- Саботаж, например прекъсване на достъпа до сайта или изтриване на данните съдържани в него.

За предпазване от злонамерен код се използват:

- Поддържайте уеб приложенията си (например уеб хостинг, търсачки) и операционни системи според последната версия публикувана от доставчика и инсталирайте наличните софтуерни пачове;
- Активирайте опциите за сигурност на уеб приложенията, например криптиране, силна автентикация, архивиране.
- Ограничете съдържанието на уеб-базираните приложения. Улесняването на инструменти, като например блокери на реклами или JavaScript, също ще ограничат възможността за изпълнение на злонамерени кодове при посещение на определени уебсайтове.
- Следете съдържанието на пощата и страницата за откриване и предотвратяване на доставката на злонамерени URL адреси и файлове и пакети.

За повече информация, виж т.1.2 'Защити' както и https://www.enisa.europa.eu/publications/web-based-attacks

4 БОТНЕТ АТАКИ

Ботнет атака в същността си е автоматизирана (роботизирана) компютърна атака, която използва злонамерен код за да създаде мрежа от заразени компютри (ботове или зомбита), които биват контролирани от атакуващите и участват в други атаки. Може дори да не подозирате, че сте жертва на ботнет атака, а Вашите устройства да са част от кибератака, например да разпространяват спам или да участват в масивна атака от тип "разпределен отказ от услуга" (Distributed Denial of Service, DDoS), която цели прекъсване на достъпа до определен уеб сайт чрез претоварване на сървъра с хиляди едновременни фалшиви заявки.

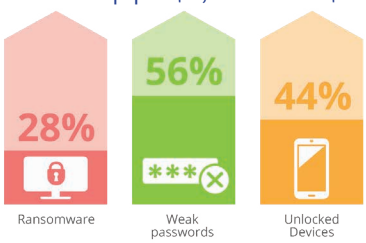
Основните цели на уеб базирана атака / web-based attack са:

- Инсталиране на злонамерен код с цел вземане на контрол върху устройството на жертвата;
- Саботаж, като например прекъсване на достъпа до определен уеб сайт;
- Масово разпространение на спам или злонамерен код.

За предпазване от ботнет атаки се използват:

- Инсталирайте и поддържайте специализиран софтуер за защита срещу злонамерен код (anti-malware): той се инсталира върху мобилни устройства, операционни системи;
- Инсталирайте и/или активирайте защитна стена (firewall) на Вашите операционни системи, имейл и мрежа, която може да блокира злонамерения код преди да достигне Вашите устройства.
- Поддържайте уеб приложенията си (например уеб хостинг, търсачки) и операционни системи според последната версия публикувана от доставчика и инсталирайте наличните софтуерни пачове;
- Активирайте опциите за сигурност на уеб приложенията, например криптиране, силна (или многофакторна) автентикация, създаване на редовни резервни копия.

За повече информация, виж т.1.2 'Защити', както и https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-botnet



В заключение, 84% от всички атаки се базират на някаква форма социален инженеринг, залъгвайки служители/потребители неволно да участват в атаката. Този факт, поставя огромна отговорност на служителите за запазване на сигурността, както и отговорност на управителите да предоставят необходимите обучения и информация за да могат служителите да разпознават и да се предпазят от този тип атаки.

Освен към външните заплахи разгледани по-горе, липсата на хигиена за киберсигурността при служителите (несигурни пароли и незаключени устройства) остава основният проблем за сигурността на МСП, по-сериозен дори от злонамерен код.

Повече подробности и мерки за сигурността са изброени в следващата глава.

III МЕРКИ ЗА КИБЕРСИГУРНОСТТА

Всяко едно предприятие е създадено с определен бизнес модел и работни процеси, които в повечето случаи се различават от друга фирма. Понякога това се случва, дори когато са от един сектор и със сходни мащаби. Основната роля на киберсигурността е да позволи на предприятието да извършва нормално своята дейност, като взима предвид неговите ресурси, потребности и клиенти. Именно поради тези особености, подходящите мерки по киберсигурността на едно предприятие биха се различавали от тези на друго такова. Тази глава цели да изложи основните действия, които са валидни за всички малки и средни предприятия, вземайки предвид ограничените им ресурси.

По отношение на средно-статистическото европейско МСП, в своя наръчник от 2021 г., ENISA предоставя обзор на

Графиките в този наръчник са заимствани от ръководството за киберсигурност за МСП на ENISA
(Cybersecurity for SMEs, достъпен на https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes)

предприетите мерки за киберсигурност. Най-голям дял от действията, които предприемат или обмислят фирмите при повече от 70% от анкетираните са: създаване на резервни копия на данни (backup), антивирусни програми (antivirus), защитна стена (firewall) и системно актуализиране на софтуера (systematic updating of software). Доклад на Организацията за икономическо сътрудничество и развитие (ОИСР) допълва този списък с използването на силни пароли от европейските МСП (OECD, 2020, Digital Security in SMEs).

Организационните мерки, макар и в основата на киберсигурността, не попадат във фокуса на МСП. Според ENISA, по-малко от 30% от анкетираните малки и средни бизнеси имат система за управление на информацията (ISMS, Information Security Management System), плановете за реакция при инцидент и за непрекъснатост на дейността и възстановяване след бедствия (Business continuity and disaster recovery plan).

Докладът на ОИСР допълва, че обучение на персонала за рисковете на киберсигурността е заложено при повече от половината анкетирани МСП. Останалите технически мерки, като контрол на достъпа до мрежата, използване на VPN, криптране на данните и мониторинг, както и организационни мерки (политики, управление на риска за киберсигурността) биват основно приети от големи предприятия.

1 Организационни мерки

Внедряването на надеждна киберзащита може да се окаже по-сложен процес от инсталирането само на антивирусни програми, например. За по-ефективно предпазване от подобен тип заплахи е необходимо, тя да бъде интегрирана на ниво процеси в съответната компания. Както и да обхване пълния набор от мерки, не само за отбиване на кибератаки, но и за тяхната превенция.

Основният процес за управление на киберсигурността използван от МСП е систематизиран в конкретни стандарти за информационна сигурност, които имат за цел да улеснят интеграцията в отделните фирми. Серията 27000 е разработена съвместно от Международната организация по стандартизация и Международната електротехническа комисия и включва основни насоки, организационни действия и изисквания за подобряване на дигиталната защита.

Най-съществения стандарт за МСП е БДС ISO/IEC 27001, последната версия на който датира от 2013 г. и предлага основните мерки за информационна сигурност, както и насоки за въвеждането им на практика. Организацията, продукта, услугата или персонала могат да бъдат сертифицирани в съответствие с този стандарт.

Стандартът излага изискванията за създаване на Система за управление на информационната сигурност, базирана на управление на риска, и в Приложение А, изброява 114 контрола (мерки) за информационната сигурност, разделени на 14 области на информационната сигурност. Тези области са:

- Политики за информационна сигурност (2 контрола/мерки)
- Организация на информационната сигурност (7 контрола/мерки)
- Сигурност на човешки ресурси (6 контрола/мерки)
- Управление на активите (10 контрола/мерки)
- Контрол до достъпа (14 контрола/мерки)
- Криптография (2 контрола/мерки)
- Физическа сигурност и околна среда (15 контрола/мерки)
- Сигурност на операциите (14 контрола/мерки)
- Комуникационна сигурност (7 контрола/мерки)
- Закупуване, разработване и поддръжка на системите (13 контрола/мерки)
- Връзки с доставчиците (5 контрола/мерки)
- Управление на инциденти свързани с информационната сигурност (7 контрола/мерки)
- Информационната сигурност при управлението на непрекъснатостта на дейността (4 контрола/мерки)
- Съответствие със законови мерки и лицензи (8 контрола/мерки)

Структурата на документацията за изискванията на ISO 27001 е подобна на структурата за изискванията на ISO 9001 и се базира на мантрата на всички ISO стандарти - планирай, изпълни, провери, подобри.

Този наръчник разглежда основните мерки включени в двата стандарта и се придържа към структурата на рамката за киберсигурност на Американския Национален институт за стандарти и технологии (NIST framework), изграден върху четири основни процеса: идентификация, защита, установяване на инцидент, отговор на атаката, възстановяване на сигурността.

1.1 Идентифицирайте

- **Критичните процеси и ресурси на предприятието**

Трябва да разберете кои са основните ресурси и процеси, които трябва да защитавате. Сигурността изисква организация, внимание и средства, които трябва да се концентрират върху тези критични ресурси и процеси.
Пример: електронен магазин има нужда от система за приемане и обработване на поръчки и данни на клиенти; строителна фирма има нужда от счетоводните книги, проекти, договори и разрешителни; ИТ компания има нужда да осигури надежден процес на разработване на продукти и канал за обратна връзка с клиента за решаване на технически проблеми.

- **Заплахите, уязвимостите и риска за активите**

Разработете и поддържайте процеси за управление на риска, за идентифициране, оценяване и документиране (в регистрите) на риска, включително актуалните заплахи и налични уязвимости. Гарантирайте, че възможните мерки за намаляване на риска са идентифицирани и въведени според техния приоритет. Препоръчително е да се следят техните резултатите.
Пример: създайте и редовно попълвайте риск регистъра на предприятието, опишете възможните мерки за предотвратяване или намаляване на риска, създайте проект за въвеждане на всяка избрана мярка, проследете и преизчислете риска след въвеждане на тези мерки (виж Приложение 1 с шаблон на регистър на риска).

- **Хардуера и софтуера**

Изучете и поддържайте устройствата и софтуера си. Инвентар/списък с хардуер и софтуерните активи би Ви помогнал да премахвате ненужните такива, които макар и не в употреба, биха могли да са входна врата за атакуващите. Този инвентар улеснява поддръжката на софтуера (неговата версия, пачове), както и управлението на софтуерните лицензи.
Пример: една електронна таблица включваща марка, модел, отговорно лице, идентификационен номер (MAC) адрес, версия, лиценз за всички мобилни устройства, лаптопи, рутери на компанията.

- **Политики за киберсигурност**

Важно е да опишете и въведете елементи на киберсигурността в политиките на предприятието и инструкциите за работа. Политиките за киберсигурност следва да бъдат интегрирани с други съображения за риска на предприятието (напр. инвестиционен, финансов, репутационен).

Както при Общия регламент относно защита на личните данни (GDPR, Регламент (ЕС) 2016/679), въведете роля на отговорник за киберсигурността и инструктирайте персонала относно техните отговорности при защитата на киберсигурността.

Пример: включете в трудовия договор обща политика за сигурност, която може да включва или допълва отделни политики за разрешено използване на хардуера и софтуера, при инструкциите за управление на персонала включете политики за контрол на достъпа (вкл. управление на акаунти и пароли); в инструкциите за работа включете мрежова сигурност и управление на инциденти; в процедурите за закупуване включете глава за защита от злонамерен код, за разработване, закупуване и поддръжка на софтуера.

1.2 Защитете

- **Управление на достъпа до активи и информация**

Проверявайте автентичността на потребителите (напр. пароли, многофакторна идентификация), преди да им бъде предоставен достъп. Подсигурете уникален, личен акаунт на всеки служител с достъп само до приложения и данни необходими за изпълнение на задачите свързани с тяхната длъжност.

Пример: счетоводителят не трябва да има достъп до базата клиенти, както и търговският представител не бива да има достъп до счетоводен софтуер и банковите сметки на предприятието.

По този начин, защитавате достъпа до информацията в случай, например, на откраднатата парола на някой от служителите. Не забравяйте, че защитата на физическия достъп до фирмените обекти и устройствата също е необходим за защита на данните.

- **Обучение на потребителите**

Редовно обучавайте всички потребители, за да сте сигурни, че те са запознати с политиките и процедурите за киберсигурност на предприятието и поддържат добро ниво на осведоменост по отношение на заплахите. Инструктирайте всеки служител за отговорностите по отношение на киберсигурност при тяхната специфичната роля.

Пример: представете политиката за сигурност на всички служители на годишно събрание и всеки път, когато постъпва нов служител, изпращайте редовна комуникация относно нашумели кибер инциденти, както и споделяйте кампаниите за киберсигурност организирани от партньори, доставчици или правителствени организации (виж глава VI Полезни Контакти за повече информация).

Насърчавайте добра кибер хигиена - ежедневни прости правила за сигурност. Допълнителна информация за атаките и уязвимостите, както и информационни кампании за потребители биват публикувани на сайта на CERT-BG и други (виж глава VI Полезни Контакти и допълнителна информация). Тази информация е особено подходяща за ИТ отдела на МСП или еднолични търговци, които искат да разширят познанията си в областта на киберсигурността.

Пример: насърчавайте кибер хигиена чрез ежедневни прости правила, като например да се заключва компютъра, да не се съхраняват важни файлове на десктопа или бюрото, да не се използва обществен или непознат безжичен интернет, да не посещават неблагонадеждни сайтове, да не се споделя ненужна информация онлайн.

- **Защита на чувствителни данни**

Уверете се, че чувствителни данни за Вашия бизнес или клиенти са защитени чрез криптиране, както докато се съхраняват на компютрите (data at rest), така и по време на пренос (data at transit, например по електронна поща). Помислете за използване на проверка на целостта, за да сте сигурни, че са направени само одобрени промени в данните.

Пример: криптирайте хард драйва, електронните съобщения и безжичен интернет.

Не забравяйте да подсигурите сигурно унищожаване на данните и устройства, когато вече не са необходими, което е изискване и според чл. на GDPR.

Пример: унищожете ненужни хартиени или електронни носители и изтривайте данните на хард драйв чрез специализиран софтуер или следвайки инструкциите на производителя.

- **Създавайте редовно резервни копия на данните/backup**

Редовно създавайте резервни копия на данните си (архивиране). Архивирането е все по-разпространена практика и според ENISA, след Ковид кризата все-повече МСП архивират данните си (94% срещу 90% преди кризата).

Тези копия трябва да се съхраняват извън мрежата, например в отделен облак (автоматично) или на устройство, което не е свързано с вътрешната Ви мрежа. По този начин, при евентуална фишинг атака хакери няма да имат достъп до тези копия. За сигурно архивиране се водете по схемата 3-2-1 представена по-долу: 3 копия, на 2 различни места, 1 от които извън Вашата мрежа.

Пример: ежемесечно копирайте последните данни свързани с управление на критичните процеси и ресурси на предприятието (виж т. 1.1 Идентифицирайте).

- **Поддържайте информационните си системите**

Поддържайте системите си и инсталирайте софтуерни пачове веднага след като са налични. При всички системи, софтуер и хардуер би могло да се намерят пропуски в сигурността, които биват използвани от злонамерени страни за да проникнат или променят Вашата система. По-голямата част от производителите / доставчиците поддържат продуктите и услугите си, т.е. предоставят пачове (корекции) които поправят тези пропуски при обновяване на версията.

Пример: Редовно следете за обновления на сайта на производителя или при настройки на мобилните устройства, и при първа възможност, инсталирайте последната версия на продукта. Потърсете допълнителни средства за защита, като удостоверяване на електронна поща, и ги настройте да се актуализират автоматично на компютрите Ви.

Графиките в този наръчник са заимствани от ръководството за киберсигурност за МСП на ENISA
(Cybersecurity for SMEs, достъпен на https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes)

1.3 Установете инцидента

- **Поддържайте процедури за установяване на инциденти**

Подгответе и тествайте процеси и процедури за откриване на непозволени действия по електронни системи или в обекти на предприятието. Персоналът трябва да е наясно с отговорността си да установи и сигнализира за всяко неправомерно действие по електронните системи или в обекта на предприятието при екипите за сигурност или управителите на предприятието.

Пример: симулирайте инцидент (например фишинг мейл) и изискайте от персонала да подаде сигнал до ИТ екипа/екипа Ви за сигурност. Опишете как да се действа оптимално при такава ситуация.

- **Поддържайте дневници за сигурност (security logs)**

За да се установи аномалия е необходимо да се съхраняват дневници от действията по устройствата и приложенията на Вашето предприятие. Системите предоставят такъв дневник за основните събития от интерес.
Пример: съхранявайте регистър на промените в акаунтите (създаване или повишаване на привилегиите), промяна на настройките, използване на админ акаунти, достъп или отказ на достъп до системите.
Важно е и да решите за какъв срок тези дневници биха се съхранявали, като добрите практики посочват архивиране за около 12 месеца, минимум 6 месеца. Имайте предвид, че съхранението на данни изисква средства,
но това е средно-статическия срок след започването на атаката през който се очаква да разберете, че сте обект на атака.

- **Познаване на обичайните потоци от данни**

Ако знаете какви са и как вървят потоците от данни за Вашето предприятие, бихте могли да забележите необичайни транзакции или потоци. Ако използвате облачни услуги, обърнете се към доставчика на услугата, за да следи и алармира необичайни събития.
Пример: съмнителни потоци биват експортирани на клиентската база данни, подаване на команди от чужбина (държави, в които нямате служители), или извършване на операции през нощта или по време на празници.

1.4 Отговорете на атаката

- **Запознайте се с възможните сценарии за атака**

В случай на атака, предварително подготвени отговорности и план за действие биха били от съществено значение за прекратяване и преодоляване на инцидента.

Пример: разработете подробни план за действие в случай на основните заплахи разгледани в този наръчник: фишинг, злонамерен код, уеб-базирани и ботнет атаки (виж глава II). Опишете процеса на реакция стъпка по стъпка, например изолиране на засегнатото устройство от мрежата, деактивиране на засегнатия акаунт, блокиране на злонамерения код или уеб сайт, сканиране на мрежата, промяна на настройките, иницииране на контакт със засегнатите лица. Виж Приложение 2 с примерен план за действие при фишинг.

Не се колебайте да потърсите помощ (виж глава VI Полезни контакти и допълнителна информация). Не пропускайте тази възможност да подобрите политиките и процесите си на база на знанията относно Вашата система, заплахи и защита придобити по време на инцидента.

- **Подсигурете добра координация със заинтересованите страни**

Важно е да се уверите, че плановете за реакция и актуализациите на Вашето предприятие включват всички ключови екипи, заинтересовани страни и външни доставчици на услуги.

Пример: Навременна и точна комуникация с доставчик, партньор или клиент биха им позволили да се защитят от атаката, например да блокират злонамерен код или променят паролите си, и така да съхраните доверието помежду си.

1.5 Възстановете сигурността

- Поддържайте планове за възстановяване

Както и при плановете за реагиране, тествайте възстановителните процедури за да подобрите процеса и поддържате добрата информираност на служителите. Не забравяйте да използвате извлечените поуки за актуализиране на плана.

Пример: Въпроси относно детайлите, която трябва да се публикуват и в какви сроковете биха били изчистени по време на един тест на възстановителните процедури.

- **Сигнализирайте инцидента**

Плановете Ви за възстановяване трябва да опишат в детайли каква информация и как и кога да бъде споделяна, така че всички заинтересовани страни да получат необходимата им информация, без да се разпространява неподходяща информация.

Пример: сигнализирането на инциденти които създават риск за защита на личните данни, в съответствие с чл. 33 от Регламент (ЕС) 2016/679 (GDPR), следва да бъдат заявени при КЗЛД не по-късно от 72 часа след установяването на такова нарушение.

2 Технически мерки

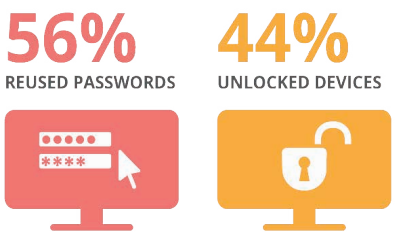
Като общо правило, всички услуги трябва най-малкото да бъдат защитени със силна защита на достъпа, антивирусна програма, защитна стена, и защитени комуникации.

2.1 Осигурете защита на достъпа

Многофакторна идентификация / multifactor authentication
Когато е налична опция, активирайте многофакторна идентификация/multi factor authentication за продуктите и услугите които използвате. Това на практика означава, че се използват поне два от следните начина за всяка успешна идентификация:

- нещо което знаете, например потребителско име и парола;
- нещо което имате, например код получен на регистрирано мобилно устройство, друго приложение или електронна поща, както и електронен идентификатор;
- нещо което сте, например биометрични данни, най-често пръстов отпечатък.

Силни пароли



Уверете се, че системите Ви изискват силна парола. Паролите все още са основен начин за автентификация на служителите, но са лесни за отгатване и хакване. Силна парола е стриктно лична (да не се споделя), комплексна (например да е от поне 8 знака, съчетание от главни букви, малки букви, символ и цифри) и уникална (т.е. да не се използва същата парола за други лични услуги, например социални мрежи или лична поща, където паролата може да изтече в интернет).

Паролите остават основен проблем за киберсигурността и според ENISA, в 56% случаите една и съща парола се използват за различни услуги продукти, докато 44 % от устройствата не са дори защитени от парола.

Добра практика и улеснение за служителите е използването на мениджър на пароли, приложение което генерира уникални силни пароли за всяко приложение/уеб адрес и ги съхранява в сейф, който се отключва с една единствена парола. Тогава, служителят няма нужда да 'рециклира' същата парола в множество сайтове.

Може също да насърчите служителите си да използват фраза вместо парола. Така не само ще подсигурят по-добра защита, но би могли да я използва като мотивираща мантра, която е лесно за запомняне.

Пример: '**М**оята**Ц**еле**Д**а**С**тана**Т**оп**К**онсултант@**Ф**ирматапрез2021!', което е '**МЦеДСТК@Фп2021!**' или '**MZeDSTK@Fp2021!**'. Друг пример е '**Н**ямам**Т**ърпение**д**о**В**аканцията@**Р**импрез**Д**екември**2021**!', което също е '**НТдВ@РпД2021!**' или '**NTdV@RpD2021!**'

Графиките в този наръчник са заимствани от ръководството за киберсигурност за МСП на ENISA
(Cybersecurity for SMEs, достъпен на https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes)

2.2 Инсталирайте антивирусна програма

Инсталирайте и редовно актуализирайте антивирусната програма, която Ви предпазва от добре познати злонамерени кодове, компютърни вируси, или спам. Настройте антивирусния софтуер да сканира с операционната система, устройство или апликацията след всяка актуализация. Инсталирайте други ключови софтуерни актуализации веднага щом бъдат налични.

2.3 Криптирайте данните и устройствата си

Когато данните Ви не са криптирани, те са като 'отворена книга' за злонамерени лица, които могат да проникнат във Вашето устройство или да ги прочетат/свалят по време на преноса на данни по интернет. Също така, мобилните устройства (лаптопи, телефони, флашки) често биват откраднати или загубени - в злонамерени ръце Вашето устройство би издало цялата Ви информация (документи, кореспонденция) и дало достъп до електронните Ви услуги (например запазени пароли за онлайн банкиране, социални мрежи, имейл акаунти).

За да защитите фирмената и личната си информацията трябва да криптирайте устройството и данните си:

- устройство (устройства/диск, в облак, датабази): Активирайте опцията за криптиране при настройките за сигурност на устройството или услугата. За флашки, инсталирайте програма (например BitLocker).
- данни при пренос: Активирайте опция WPA3 (или WPA2) за криптиране на рутера и използвайте криптирани канали за дата пренос в интернет (HTTPS, SSL, TLS, FTPS,..).

2.4 Инсталирайте защитна стена (firewall)

Обмислете инсталиране на защитна стена директно на устройствата (уеб-базирана стена) в допълнение на защитната стена на рутера си. Така, ако защитната стена на рутера е пробита при атака, уеб-базирана стена предоставя допълнителна защита.

2.5 Защитете безжичния си интернет (Wireless/WiFi)

Безжичен интернет остава един от най-лесните начини да се проникне във Вашето устройство и да се следи информацията, предаване по интернет (например пароли, данни за кредитна карта, или лични файлове). За да се намали риска от кибератака през безжичния интернет, МСП трябва да вземат следните мерки:

- Променете първоначалната парола: фабричните пароли често биват публикувани в интернет - така всеки би могъл да проникне във Вашата мрежа и да следи данните които изпращате по интернет. Паролата трябва да е силна (виж т. 2.1 защита на достъпа) и ако е възможно, да се променя редовно.
- Ограничете достъпа: Използвайте инвентара на устройствата и софтуера (виж глава II, т. 2.1 'Идентифицирайте') за да лимитирате достъпа до Вашата мрежа на тези одобрени устройства (техния MAC код изписан на устройството). Настройките са достъпни в потребителската документация на рутера. За не-регистрирани устройства, използвайте отделен безжичен канал ('guest' account). Този тип канал използва различна мрежа, сигурност и парола от основния, които е за ползване на персонала.

2.6 Използвайте виртуална частна мрежа (VPN)

VPN е вид подсигурен криптиран канал за комуникация, който позволява на служителите да се свързват сигурно с мрежата, когато са извън офиса. Ако разполагате с VPN, не забравяйте да влезете в нея всеки път, когато трябва да използвате публична точка за безжичен достъп. Избягвайте употребата на програми за достъп до Вашата система от разстояние (Remote Desktop Connection), както и уеб програми за обмен на файлове, защото тези не са достатъчно защитени за да предпазят информацията Ви от трети лица.

IV ПРАВНА РАМКА И ИЗИСКВАНИЯ ЗА КИБЕРСИГУРНОСТ

През 2016 г. бе приета първата Европейска Директива за киберсигурност, Директива EU 2016/1148 относно Сигурността на Мрежите и Информационните Системи (EU Network and Information Systems Security, NIS Directive). С приемането ѝ, страните членки на ЕС, включително България, се ангажираха да идентифицират така наречените оператори на основни услуги за икономиката и обществото си (критична инфраструктура, например транспорт, финансови институции, енергийно и водоснабдяване) и да транспонират в националната правна рамка минимални мерки за киберсигурност. Тези мерки биват основно: въвеждане на система за управление на риска за киберсигурността, въвеждане на политика за киберсигурност и докладване на инциденти свързани с нея на критичните услуги предлагани от оператори на основни или цифрови услуги.

Европейската директива бе транспонирана в българското законодателство през 2018 чрез приемането на Закон за Киберсигурност. Той урежда дейностите по организация и управление на киберсигурността, както и определя минимални мерки за киберсигурността.

Дейностите по организация и управление на киберсигурността биват:

1. разпределение на отговорностите за мрежовата и информационната сигурност;
2. прилагане на политика за мрежовата и информационната сигурност;
3. управление на:
а) риска;
б) информационните активи, включително човешките ресурси;
в) инцидентите;
г) достъпите (физически и логически);
д) измененията;
е) непрекъснатостта на дейността и/или услугите (съществени, цифрови);
ж) взаимодействията с трети страни.'

Тези организационни мерки са представени детайлно в международния стандарт за информационна сигурност ISO 27001 и неговото приложение А. Повече от тях са разгледани и в настоящия наръчник, с изключение на д) измененията и ж) взаимодействия с трети страни.

Минималният обхват на мерките за мрежова и информационна сигурност, както и други препоръчителни мерки, се определят с наредба на Министерския съвет по предложение на председателя на Държавна агенция „Електронно управление".

Макар и не в обхвата на Наредба за минималните изисквания за мрежова и информационна сигурност (Постановление № 186 от 19 юли 2019 г.), МСП могат да се информират относно минималните мерки за сигурност, изисквани от публичната администрация, от лица и организации, които осъществяват публична длъжност, както и от операторите на основни / доставчиците на цифрови услуги. Наредбата урежда:

1. изисквания за минималните мерки за мрежова и информационна сигурност;
2. препоръчителни мерки за мрежова и информационна сигурност;
3. правила за извършване на проверките за съответствие с изискванията на тази наредба;
4. редът за водене, съхраняване и достъп до регистъра на съществените услуги по чл. 6 от Закона за киберсигурност;
5. образец на уведомленията за инциденти.'

Тази Наредба би била от интерес в случай, че целите да предоставяте услуги на лица и организации в обхвата на наредбата. В такъв случай, подгответе се да въведете изискванията (покрити също в този наръчник) за да отговорите на зл. 10 (1) Управление на взаимодействията с трети страни, и по-специално:

- за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити;
- за прозрачност на веригата на доставките; третата страна трябва да е способна да докаже произхода на предлагания ресурс/услуга и неговата сигурност.

Тази наредба също би била полезна като изискване за доставчиците Ви в обхвата на наредбата, които въвеждайки тези законови изисквания, биха защитили и Вас като техен клиент.

В допълнение, българската стратегия за Киберсигурност от 2016 г. начертава националните приоритети за киберсигурност. Стратегията би била от интерес за МСП по отношение на основните мерки и органи за управление на киберсигурността на национално ниво политическо, стратегическо, операционно, техническо ниво и на ниво сегмент от кибер пространството. МСП могат да се потърсят помощ от институциите на техническо и операционно ниво (виж глава VI Полезни контакти и допълнителна информация).

V ПРЕПОРЪКИ ЗА РАЗВИТИЕТО НА ПОЛИТИКИТЕ

Необходимо е създаването на Европейски консултативен орган за МСП, който подобно на националния консултативен орган за публичните и обществени услуги, да подготвя политики и конкретни мерки за подобряване на киберсигурността на МСП. ENISA поема тази роля до голяма степен, но за да бъде в позиция да предлага ефективна и навременна подкрепа за сигурността на МСП, ENISA трябва да развие допълнителни дейности. Тези дейности са основно:

• Подготвяне на обучения за МСП за разработване на политики за киберсигурност, управление на риска за киберсигурността, управление на инциденти и кризи, както и технически обучения свързани със специфични мерки за киберсигурността (например, мрежова сигурност, управление на достъпа до информационни активи, защита на лични данни, обучения за персонала).

• Създаване на Европейски публичен регистър на експертите по киберсигурността. МСП имат нужда от консултация с експерти в областта на киберсигурността, правото, управлението на инциденти и кризи, и технически експерти, но идентифицирането на нужните експерти и осъществяване на връзка с тях изисква време и знания. Този регистър може да е единен европейски или да централизира мрежа от национални регистри за кибер експерти.

• Откриване на 'гореща линия' за киберсигурността на МСП за случаите, когато МСП имат нужда от съвет за справяне с конкретен проблем или инцидент. ENISA трябва да подпомогне МСП действайки като "бърза помощ" (при случай на инцидент или криза) или като общопрактикуващ лекар за останалите случаи чрез идентифициране на специалността, към която МСП трябва да се обърне за помощ и насочване към Европейски публичен регистър предложен по-горе.

• Насърчаване и предоставяне на необходимите материали за ежегодни кампании за киберсигурност и кибер хигиена в страните членки на ЕС. използвайки своята експертиза и икономии от мащаба, би било най-разумно ENISA да подготвя промоционални материали и кампании, които да бъдат превеждани и разпространявани от националните органи в съответната държава. Това е единствения възможен към момента начин, с наличните човешки и финансови ресурси за киберсигурността в Европа, да се осигурят ефективни кампании и материали, за да обхванат всяка част от обществото (от детската градина до пенсия).

• Насърчаване на създаването на Европейски секторни центрове за обмен и анализ на информация (European Information Sharing and Analysis Centre - ISAC) по примера на тези създадени за сектор енергетика, финанси, жп и морски транспорт. Поради нарастващия дял на инциденти с кибер сигурността и/или сравнително ниско ниво на защита, приоритетни сектори трябва да са: здравеопазване, промишленост, облачни услуги, телекомуникации, туризъм.

VI Полезни контакти и допълнителна информация

1 Подаване на сигнал за кибер инциденти, както и информация относно заплахи, вируси и актуални съвети

• В случай, че МСП станат жертва на кибер престъпление в особено големи размери, например при масивна атака или при искане на откуп от кибер престъпници, МСП могат да се обърнат към отдел "Киберпрестъпност" при Главна дирекция "Борба с организираната престъпност" в МВР. Отделът разследва киберпрестъпления с потърпевши на територия на страната. Контакти: http://www.cybercrime.bg/

• В случай на инцидент с киберсигурността, или при идентифициране на кампании за фишинг и други подобни кибер заплахи, МСП могат да се обърнат към CERT Bulgaria. CERT BG е Националният екип за реагиране при инциденти с компютърната сигурност. Мисията на екипа е да подпомага ползвателите на услугите му в извършването на проактивни дейности за намаляване рисковете от инциденти в информационната сигурност и да асистира при разрешаването на такива инциденти в случай, че вече са възникнали. Екипът предоставя централизирана база данни с информация, свързана с осигуряване на сигурна и защитена информационна среда. Контакти:
https://www.govcert.bg/

• В случай на инцидент със сигурността на лични данни (изтичане на лични данни), МСП трябва да сигнализират Комисия за защита на личните данни (КЗЛД) не по-късно от 72 часа след научаване за инцидента. Уведомлението и инструкции са налични на сайта на КЗЛД: https://www.cpdp.bg/?p=pages&aid=61. КЗЛД предоставя съвети към администраторите и обработващите лични данни за защита на данните в киберпространството:
https://www.cpdp.bg/?p=element&aid=1316

• В случай на проблеми с киберсигурността в сектор „Транспорт“ можете да се обръщате към: NKOTransport@mtitc.government.bg, за проблеми с киберсигурността в сектор „Цифрова инфраструктура“ и „Цифрови услуги“ можете да се обръщате към: NKODigitIfra@mtitc.government.bg към Национален компетентен орган по мрежова и информационна сигурност към Министърът на транспорта, информационните технологии и съобщенията: https://www.mtitc.government.bg/bg/category/226

• В случай на рансъмуеър, може да потърсите актуална информация и средства за реагиране при Европейския Център за Кибер Престъпления към Европол (EC3): https://www.nomoreransom.org/

2 Допълнителна информация и материали относно обучения и информираност на служителите

• Национална Кампания за Кибер Хигиена: https://www.facebook.com/cyberneat18/
• Европол и Европейската банкова федерация кампания срещу седемте най-чести онлайн финансови измами: https://www.mvr.bg/docs/librariesprovider5/default-document-library/bg_0.pdf?sfvrsn=d3b7ae8f_0
• Онлайн бюлетин за киберсигурност на БАН и Британското посолство в България: https://www.iict.bas.bg/CS-News/contents-bg.html
• (EN) ENISA, 2021, Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/at_download/fullReport
• (EN) ENISA, 2017, Cyber Security Culture in organisations: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport
• (EN) Европейския Центъра за Кибер Престъпления към Европол (EC3), Public Awareness And Prevention Guides: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides

3 Допълнителна информация относно добри практики

• ENISA: Европейската Агенция за Киберсигурност е експертен център в областта на кибер сигурност в Европа: https://europa.eu/european-union/about-eu/agencies/enisa_bg
• (EN) Cybersecurity for SMEs: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes
• (EN) ENISA, 2021, SME Cloud Security Tool: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security/security-for-smes/sme-guide-tool
• (EN) Британски национален център за киберсигурност (NCSC), 2021, Cybersecurity Essentials Requirements for IT Infrastructure: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-1.pdf
• (FR) Френската Национална Агенция за Сигурност на Информационните Системи (ANSSI), 2021, La Cybersécurité pour les TPE/MPE en 12 questions: https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/
• (EN/FR/NL) Белгийската КиберКоалиция (Cybersecurity Coalition), 2016, Cybersecurity Guide for SME:
• https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-EN.pdf (EN)

- https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-FR.pdf (FR)
- https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-guide-sme-NL.pdf (NL)
- (EN/FR/NL) Белгийския Център по Киберсигурност, 2021, Cyberguide: https://cyberguide.ccb.belgium.be/en?advanced
- (EN) Global Cyber Alliance's (GCA) cybersecurity toolkit for small businesses with free cybersecurity resources: https://gcatoolkit.org/smallbusiness/
- (EN) CyberWatching.eu SMEs Guides: https://cyberwatching.eu/smes-guides
- (EN) NIST Small Business Cybersecurity Corner: https://www.nist.gov/itl/smallbusinesscyber
- (EN) OECD, 2021, Digital Security in SMEs: https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en#chapter-d1e7025

4 Допълнителна информация относно заплахи и уязвимости за киберсигурност

- (EN) ENISA, 2021, A complete list of Threat Landscape reports, available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends?tab=publications
- (EN) ENISA, 2020, Artificial Intelligence Cybersecurity Challenges, available at: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
- (EN) EUROPEAN CYBERCRIME CENTRE - EC3 updates: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-2
- (EN) Verizon, 2020, Data Breach Investigation Report, available at: https://enterprise.verizon.com/resources/reports/dbir/
- (EN) Google, 2021, Project Zero - Bug Tracker: https://bugs.chromium.org/p/project-zero/issues/list
- (EN) NIST, 2021, National Vulnerability Database: https://nvd.nist.gov/
- (EN) ENISA, 2019, Cloud Computing Risk Assessment: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport
- (EN) NIST, 2021, Workshop Summary Report for "Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices" Virtual Workshop: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8333.pdf
- (EN) MITRE Attack V8: https://attack.mitre.org/versions/v8/

5 Допълнителна информация относно стандарти за киберсигурност

- БДС ISO/IEC 27000 – Информационни технологии – Методи за сигурност – Системи за управление на сигурността на информацията – Общ преглед и речник
- БДС ISO/IEC 27001 – Информационни технологии – Методи за сигурност – Системи за управление на сигурността на информацията – Изисквания
- БДС ISO/IEC 27002 – Информационни технологии – Методи за сигурност – Кодекс за добра практика за управление на сигурността на информацията
- БДС ISO/IEC 27003 – Информационни технологии – Методи за сигурност – Указания за внедряване на системи за управление на сигурността на информацията
- БДС ISO/IEC 27004 – Информационни технологии – Методи за сигурност – Управление на сигурността на информацията – Наблюдение, измерване, анализ и оценяване
- БДС ISO/IEC 27009 – Информационни технологии – Техники за сигурност – Специфично за секторите прилагане на ISO/IEC 27001 – Изисквания
- БДС ISO/IEC 27005 – Информационни технологии – Методи за сигурност – Управление на риска за сигурността на информацията
- БДС ISO 31000 – Управление на риска – Указания
- БДС 31010 – Управление на риска – Методи за оценяване на риска
- БДС ISO 9001 - Системи за управление на качеството
- (EN) NIST Framework: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- (EN) NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
- (EN) NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- (EN) CIS Controls V7.1: https://learn.cisecurity.org/cis-controls-download

Приложение 1 Пример и шаблон за регистър на риска

ИДЕНТИФИКАЦИЯ НА РИСКА	
Идентификационен номер	
Наименование на риска	Уязвимости в софтуера
Област на риска (външна естествена заплаха, проблемна инфраструктура, външна целенасочена атака, вътрешна злоупотреба, неправилна употреба, зловреден софтуер, системна повреда / грешка)	Проблемна инфраструктура, системна повреда
Описание на риска	Уязвимости в софтуера е част от софтуера, която съдържа слабост или грешка, които биха били на хакер да компрометира системата.
Собственик	Собственик на продукта
Съществуващи мерки за противодействие (и тяхната оценка)	Следене на всеки софтуер, инсталиран на всяка точка от системата; Добро ниво на информираност относно софтуер, за който се знае, че има уязвимости, актуализация на системите; внедряване на стабилна система за защита от злонамерен програмен код.
Свързани рискове	
АНАЛИЗ И ОЦЕНКА НА РИСКА	
Вероятност за поява (оценява се с помощта на качествена скала с три нива: ниска (<1 на 10 години), средна (<1 на 1 година), висока (<1 на месец))	висока
Вид на нежеланите последствия (репутационни, правни, финансови)	репутационни, правни, финансови
Размер на нежеланите последствия (оценяват се с помощта на качествена скала с три нива: значими, средни, незначими)	значими
Оценка на риска (оценява се с помощта на матрица на риска с три нива: висок, среден, нисък)	висок
Преценка на риска (приема се че рисковете, оценени като ниски и средни са приемливи, а високите рискове са неприемливи)	неприемлив
ПРОТИВОДЕЙСТВИЕ СРЕЩУ НЕПРИЕМЛИВИТЕ РИСКОВЕ	
Подход за противодействие (игнориране, приемане, снижаване, избягване, трансфериране, повишаване)	Снижаване
Съдържание на стратегията за противодействие (изписват се основните мерки под формата на нормативни, мениджърски или технически решения, процедури и т.н.)	Следене на всеки софтуер, инсталиран на всяка точка от системата; Добро ниво на информираност относно софтуер, за който се знае, че има уязвимости, актуализация на системите; внедряване на стабилна система за защита от злонамерен програмен код.
Кризисен план (действия за елиминиране на последствията в случай на трансформиране на риска в проблем)	Поправете уязвимостта и в случай на невъзможност изолирайте и премахнете уязвимата функционалност.

Графиките в този наръчник са заимствани от ръководството за киберсигурност за МСП на ENISA
(Cybersecurity for SMEs, достъпен на https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes)

Приложение 2 План за действие при инцидент от тип фишинг

1. Увод	Фишинг е атака от т.н. тип социално инженерство. Служител получава съобщение по електронната поща (гласово съобщение или SMS при смишинг) което изглежда изпратено от легитимен източник с инструкции (обикновено 'спешно' и 'много важно'), но което е заразено със злонамерен код, който се активира при клик/отваряне
2. Цел на документа	Стъпка по стъпка план за реакция в случай на инцидент от тип фишинг, предизвикан от фишинг имейл насочен към персонала на компания XX. Спазването на тази процедура ще помогне на организация XX да намали последствията от инцидента, както за своите активи и репутация, така и за своите клиенти и партньори. Документът взема предвид задълженията за компания XX да уведоми регулатора КЗЛД в съответствие с чл. 33 от Регламент (ЕС) 2016/679 (GDPR) за инциденти свързани със защита на личните данни.
4. Реакция на атаката	
Установяване на инцидента	• Известие от служители • Известие от клиенти, партньори или регулатори
Анализ	• Анализ на типа инцидент: дали става въпрос за насочена или масова атака? Какъв вид информация е използван? Какъв канал е използван (електронна поща, SMS, гласова поща)? Какво е нареждането (за въвеждане на лични данни, за отваряне на заразен файл, за насочване към заразен уеб адрес, за изпращане на пари)? Какъв е професионализма на атакуващия (има ли очевадни грешки, грешки в правописа и стила на съобщението, доколко съобщението прилича на легитимна заявка, какъв имейл акаунт е използван - легитимен или не, какъв уеб сайт е използван - фалшифициран или непознат) • Интервю с потърпевши служители: каква информация са видели, какво се е случило при клик, откъде може да е изтекла информация за контактите • Има ли опасност за сигурността на критичните активи и процеси на предприятието? Един или множество устройства/програми са засегнати? • С каква скорост се развива атаката? • Оценка на последствията за активите, репутацията и операциите на организацията, например: не е инцидент, незначителен инцидент, инцидент с известни последствия, сериозен инцидент, криза
Овладяване на инцидента	• Събери налична информация, например скрийншот на сайта и копие на имейла (така че името и контактите на изпращащата страна да са достъпни) • Блокирай разпространението на заплахата: изолирай засегнатите устройства и програми от интернет и от вътрешната мрежа входящата поща на служители от злонамерения акаунт, блокирай достъпа на служители до заразения сайт. • Информирай служителите за опасността с ясни инструкции ако получат подобен имейл да не го отварят а само изпратя като прикачен файл до екипа/служитя, който работи по инцидент. Информирайте партньори и CERT-BG за фишинг кампанията.
Възстановяване	• Потвърди блокиране на сайта и имейлите свързани с фишинг кампанията • Потвърди блокиране на разпространението на заплахата • Запази събраните доказателства и журнали за сигурност • При нужда, възстанови данните (от архива) и се увери, че не са засегнати от атаката • На база на натрупаната информация, обмисли кои мерки за овладяване на инцидента да бъдат свалени или продължени • В случай на инцидент свързан със защита на личните данни, подай заявление (проформа) пред КЗЛД относно инцидента до 72ч
Извличане на поуки	• Потърси основната причина за инцидента • На база на опита при овладяване на инцидента, обмисли да актуализира плана за действие при инцидент и политиките и процедури за сигурността • Информирай служителите и заинтересованите страни за преодоляването на инцидента и предложи съвети за бъдещо избягване на подобен инцидент

Приложение 3 Реални инциденти и поуки

Източник на представените реални инциденти по-долу е ENISA, 2021, Cyber **Guide for SMEs**

Вид атака	**Описание**	**Поуки**
МСП: правна фирма **Брой заети лица:** < 25 служителя **Тип инцидент:** Откраднат лаптоп	По време на пандемията с Ковид 19 правна фирма разрешава на служителите си да работят от вкъщи. За да улесни работата от вкъщи, компанията разрешава на тези служители, които нямат корпоративен лаптоп, а вместо това използват настолен такъв, да използват личните си лаптопи за да се свържат с корпоративната мрежа. Един от тези служители бива жертва на кражби, които влизат с взлом в дома му и крадат, освен други ценности, лаптопа използван за работа в къщи. Лаптопа съдържа конфиденциални корпоративни документи и данни, които служителят запазва на устройството за изпълнение на ежедневните си задължения. За съжаление, за разлика от корпоративните лаптопи, които са обект на мерки за сигурност, личния лаптоп на служителя не е защитен чрез силна парола или криптиране на диска.	• Не позволявайте на служителите Ви да използват лични устройства за да се свързват с корпоративната мрежа или да съхраняват конфиденциална информация на личен имейл, облачни услуги или устройство. • Подсигурете информация и мерки за криптиране на всички мобилни устройства. • Подсигурете мерки за физическа защита на устройствата (например заключващ кабел) за устройства които не са под наблюдение. Насърчете служителите да заключват документи и мобилни устройства съхраняващи конфиденциална информация в сейф или на друго защитено/скрито място. • Подсигурете информационна сесия за служителите за рисковете и мерки за защита на конфиденциална информация.
МСП сектор: Спортен клуб **Брой заети лица:** <75 **Тип инцидент:** Рансъмуеър атака	Спортен клуб затваря врати по време на пандемията от Ковид 19 и позволява на служителите да работят от вкъщи. За да даде достъп до корпоративната мрежа, ИТ компанията обслужваща фирмата, инсталира програми за достъп до система от разстояние (Remote Desktop Connection) на всеки корпоративен настолен компютър, който дава достъп на служителите до настолните компютри от личните им устройства докато работят от вкъщи. Един от служителите получава имейл с приложение, който гласи: 'Това твоя снимка ли е?'. При сваляне на приложения файл, зловреден код с цел рансъмуеър се инсталира на компютъра му и криптира всички данни на устройството и тези, които са достъпни чрез корпоративната мрежа. Така, цялата корпоративна информация и база данни бива криптирана. ИТ компанията обслужваща фирмата успява да възстанови информацията и данните благодарение на Центъра за Кибер Престъпления към Европол (EC3,'No-MoreRansom'уебсайт, https://www.nomoreransom.org/), който предоставя ключове за де-шифроване на данни свързани с известни атаки. Последващо разследване разкрива, че поради липса на персонал в отдела, който да провери състоянието на наличните устройства, заразеният компютър не разполага с актуализирана антивирусна програма, нито с пачове и обновления на софтуера.	• Архивирайте критичните данни на компанията на място, различно от това където се съхраняват оригиналите и не на същата мрежа. По този начин, ще може да използвате архивите в случай на атака. • Обновявайте най-редовно антивирусната си програма и софтуера си (вкл. инсталирайки последните налични пачове). • Подсигурете редовни информационни сесии за служителите за рисковете и мерки за защита от фишинг.
МСП: маркетингова компания **Брой заети лица:** < 25 служителя **Тип инцидент:** Присвоена електронна поща / имейл акаунт	Маркетингова компания въвежда облачна услуга - имейл система за да позволи на служителите си да работят от вкъщи по време на Ковид 19 пандемията. Един от служителите бива жертва на фишинг атака, при която атакуващите се представят за доставчика на имейл услуги и изисква въвеждане на акаунт и парола за потвърждение на сесията. Въвеждайки своите данни, служителя дава достъп на атакуващите до своя акаунт и те го използват за да изпратят фалшиви имейли на всички клиенти на фирмата от легитимния имейл акаунт. Атакуващите разпращат два вида имейл, един който оповестява 'новата' банкова сметка на маркетинговата компания, изисквайки всички бъдещи плащания да бъдат извършени на тяхната банкова сметка. Вторият имейл съдържа злонамерен линк към 'неплатени фактури' и при отваряне на линка, от клиентите на маркетинговата компанията се изисква да въведат своите потребителски пароли. Атаката бива разпозната от един от клиентите на маркетинговата компания и я сигнализира преди да прекъсне всички договори с маркетинговата компания заради притеснения свързани с киберсигурността. Така, от инцидента струва на маркетинговата компания бизнес за поне 200 000 евро - 300 000 евро годишно от напусналия клиент.	• Активирайте многофакторна автентификация на всички платформи. • Подсигурете редовни информационни сесии за служителите за рисковете и мерки за защита от фишинг. • Използвайте силни пароли и изискайте същото от клиентите и доставчиците си.
МСП: технологична компания **Брой заети лица:** < 75 служителя **Тип инцидент:** Измама Описание на инцидента	Технологична компания специализирана в уеб разработване става жертва на измама при която служител изпълнява инструкциите на фалшив имейл претендиращ да идва от Изпълнителния директор на компанията. Поради бавната връзка до имейл сървъра при работа от вкъщи, персоналът използва личните си имейли за по-бърза комуникация. Един от служителите в счетоводството получава на личния си имейл съобщение от атакуващ, който се представя за изпълнителния директор с инструкции за незабавно плащане на фактура на нов доставчик, необходима за изпълнение на проект с наближаващ краен срок. Измамата излиза наяве на следващия ден, след извършване на плащането, при разговор с реалния Изпълнителен директор.	• Изисквайте от персонала и от управителите да спазват стриктно вътрешните процедури и процеси, включително тези свързани с използване на разрешени информационни системи. • Подсигурете редовни информационни сесии за служителите за рисковете и мерки за защита на киберсигурността, като особено внимание трябва да се наблегне на 'чувствителните' екипи: тези с по-високо ниво на достъп до системите и чувствителни данни, или с възможност да изпълняват финансови транзакции.

Автор: **Ива Ташева,** съосновател и ръководител на киберсигурността в CYEN и
съветник по киберсигурност
С подкрепата на **Ева Майдел**, евродепутат от групата на ЕНП

1-во издание

Графиките в този наръчник са заимствани от ръководството за киберсигурност за МСП на ENISA
(Cybersecurity for SMEs, достъпен на https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes)

ИНФОРМАЦИЯ ЗА АВТОРА:

Ива Ташева е съосновател и ръководител на киберсигурността в CYEN, семейна микроконсултантска компания, създадена в Брюксел през 2018 г. Ива специализира в киберсигурността на сектори: финансови услуги, транспорт, здравеопазване, както и публични политики по киберсигурност.

В допълнение към работата си за CYEN, Ива е член на Ad-Hoc работната група на ENISA по корпоративна сигурност и член на управителния съвет на DPO Circle (общност от професионалисти в областта на GDPR и сигурността на данните).

В периода 2013 - 2018 г. Ива заема позиции в Европейския център за политики (think tank), DigitalEurope (браншова асоциация), Европейския парламент, Obelis (консултантска компания). Започва кариерата си в частния сектор в България през 2009 г. Ива има магистърски степени по бизнес администрация (KU Leuven) и по киберсигурност (Нов Български Университет). Ива е сертифициран професионалист по внедряване на международните стандарти за информационна сигурност ISO 27001 и ISO 27799.

група на
ЕНП
в европейския парламент