АГЕНЦИЯ НА ЕВРОПЕЙСКИЯ СЪЮЗ
ЗА КИБЕРСИГУРНОСТ

Ръководство за киберсигурност за МСП

12 СТЪПКИ ЗА СИГУРНОСТ НА ВАШАТА ДЕЙНОСТ

Кризата с COVID-19 показа колко важни са за МСП интернет и компютрите като цяло. За да просперират в икономическата си дейност по време на пандемията, много МСП трябваше да предприемат мерки за непрекъснатост на дейността, например преминаване към облачни услуги, подобряване на интернет услугите, надграждане на уебсайтовете и осигуряване на възможности за персонала да работи от разстояние.

В настоящата листовка се предоставят на МСП 12 практически стъпки за високо равнище и по-добра защита на техните системи и дейности. Това е придружаваща публикация към по-подробния доклад на ENISA **„Киберсигурност за МСП – предизвикателства и препоръки“**.

1 РАЗВИВАНЕ НА ДОБРА КУЛТУРА ЗА КИБЕРСИГУРНОСТ

ВЪЗЛАГАНЕ НА УПРАВЛЕНСКА ОТГОВОРНОСТ

Добрата киберсигурност е ключов елемент от трайния успех на всяко МСП. Отговорността за тази така важна функция трябва да бъде възложена на някой в организацията, който да осигури за киберсигурността да бъдат подсигурени подходящите ресурси, например време на персонала, закупуване на софтуер, услуги и
хардуер за киберсигурност, обучение на персонала и разработване
на ефективни политики.

СПЕЧЕЛВАНЕ НА УЧАСТИЕТО НА СЛУЖИТЕЛИТЕ

Участието на служителите трябва да се спечели чрез ефективна комуникация относно киберсигурността от страна на
ръководството, открита подкрепа от негова страна на инициативи
за киберсигурност, предоставяне на подходящи обучения за служителите и определяне на ясни и конкретни правила,
очертани в политиките за киберсигурност.

ПУБЛИКУВАНЕ НА ПОЛИТИКАТА ЗА КИБЕРСИГУРНОСТ

В политиката за киберсигурност трябва да бъдат очертани ясни и конкретни правила за служителите за това какво поведение се очаква да имат, когато използват ИКТ средата, оборудването и услугите на дружеството. В тази политика трябва също така да се акцентира върху последствията, с които служителят може да се сблъска, ако не спазва правилата в нея. Политиката трябва редовно да се преразглежда и актуализира.

ИЗВЪРШВАНЕ НА ОДИТИ ЗА КИБЕРСИГУРНОСТ

Трябва да се извършват редовни одити от лица с необходимите знания, умения и опит. Одиторите трябва да са независими, избрани като външен изпълнител или вътрешни служители в МСП, но независими от ежедневните ИТ дейности.

ДА НЕ СЕ ЗАБРАВЯ ЗАЩИТАТА НА ДАННИТЕ

Съгласно Общия регламент на ЕС за защита на данните[1] всички МСП, които обработват или съхраняват лични данни на лица, пребиваващи в ЕС/ЕИП, трябва да гарантират, че са налице подходящи мерки за сигурност с цел защита на тези данни. Това включва гаранции, че всички трети страни, работещи от името на МСП, разполагат с подходящи мерки за сигурност.

1 Общ регламент относно защитата на данните, https://ec.europa.eu/info/law/law-topic/data-protection_bg

2

ПРЕДОСТАВЯНЕ НА ПОДХОДЯЩО ОБУЧЕНИЕ

Осигуряване на редовни обучения за информираност относно киберсигурността за всички служители, за да се гарантира, че могат да разпознават и да се справят с различните заплахи за киберсигурността. Тези обучения трябва да са съобразени с конкретното МСП и да са фокусирани върху реални ситуации.

Осигуряване на специализирано обучение по киберсигурност за лицата, които отговарят за управлението на киберсигурността в рамките на дейността, за да се гарантира, че ще имат необходимите умения и компетенции да вършат работата си.

3

ГАРАНТИРАНЕ НА ЕФЕКТИВНО УПРАВЛЕНИЕ НА ТРЕТИ СТРАНИ

Осигуряване, че всички доставчици, особено тези с достъп до чувствителни данни и/или системи, се управляват активно и отговарят на договорените равнища на сигурност. Трябва да има договорни споразумения, в които да бъде регламентирано как доставчиците отговарят на тези изисквания за сигурност.

4

РАЗРАБОТВАНЕ НА ПЛАН ЗА РЕАКЦИЯ ПРИ ИНЦИДЕНТИ

деДа се разработи официален план за реакция при инциденти, който съдържа документирани ясни насоки, роли и отговорности, за да се гарантира, че на всички инциденти във връзка със сигурността ще се реагира своевременно, професионално и по подходящ начин. За да се реагира бързо на заплахи за сигурността, трябва да се проучат инструменти, чрез които те могат да се наблюдават и да се подават предупредителни сигнали, когато бъде отчетена подозрителна йност или пробиви в сигурността.

5 СИГУРЕН ДОСТЪП ДО СИСТЕМИ

Насърчаване на всеки да използва фраза парола, съчетание от най-малко три произволни често срещани думи, комбинирани във фраза, която е едновременно лесна за запомняне и сигурна. Ако бъде избрана типична парола:

- Нека бъде дълга, с малки и главни букви, ако е възможно също и с цифри и специални символи.
- Да се избягват очевидни, напр. „парола“, поредици от букви или цифри като „абв“ или напр. „123“.
- Да се избягва използване на лична информация, която може да бъде намерена онлайн.

Без значение дали се използват фрази пароли или обичайни пароли,

- те не трябва да се използват в същия вид другаде.
- Не трябва да се споделят с колеги.
- Трябва да се активира двуфакторна автентикация.
- Да се използва специален мениджър на пароли.

6

СИГУРНИ УСТРОЙСТВА

Осигуряването на сигурността на устройствата, които персоналът използва, независимо дали това са техните настолни компютри, лаптопи, таблети или смартфони, е ключов етап от програмата за киберсигурност.

ПОДДЪРЖАНЕ НА СОФТУЕРА С ВСИЧКИ ПОСЛЕДНИ КОРЕКЦИИ И АКТУАЛИЗАЦИИ

В идеалния случай трябва да се използва централизирана платформа за управление на корекциите. Силно препоръчително е за МСП:

- да актуализират редовно целия си софтуер;
- да включат функциите за автоматични актуализации, когато е възможно;
- да идентифицират софтуера и хардуера, които изискват ръчно актуализиране;
- да вземат предвид мобилните устройства и устройствата във връзка с интернет на нещата.

АНТИВИРУСНИ РЕШЕНИЯ

На всички видове устройства трябва да бъде внедрено централно управлявано антивирусно решение, което да се поддържа актуално, за да се гарантира неговата постоянна ефективност. Също така, не трябва да се инсталира пиратски софтуер, тъй като може да съдържа зловреден софтуер.

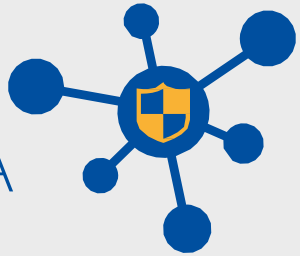
ИЗПОЛЗВАНЕ НА ИНСТРУМЕНТИ ЗА ЗАЩИТА НА ЕЛЕКТРОННА ПОЩА И МРЕЖИ

Използване на решения за блокиране на спам, електронни съобщения, съдържащи връзки към зловредни уебсайтове или зловредни прикачени файлове като вируси и фишинг съобщения.

КРИПТИРАНЕ

Защита на данните чрез криптиране. МСП трябва да гарантират, че данните, съхранявани на мобилни устройства, например лаптопи, смартфони и таблети, са криптирани. За данни, пренасяни по обществени мрежи, като Wi-Fi мрежи на хотели или летища, трябва да се осигури, че данните са криптирани, посредством използване на виртуална частна мрежа (VPN) или достъп до уебсайтовете през защитени връзки с помощта на SSL/TLS протокол. Осигуряване, че собствените уебсайтове използват подходяща технология за криптиране, за да бъдат защитени клиентските данни, когато се обменят през интернет.

7 ЗАЩИТА НА СОБСТЕНАТА МРЕЖА



ВНЕДРЯВАНЕ НА УПРАВЛЕНИЕ НА МОБИЛНИТЕ УСТРОЙСТВА

Когато съдействат на служителите си да работят дистанционно, много МСП позволяват да се използват лични лаптопи, таблети и/или смартфони. Това поражда някои опасения за сигурността на чувствителни данни на предприятията, съхранявани в тези устройства. Един от начините за управление на този риск е да се използва решение за управление на мобилни устройства (MDM), което позволява на МСП:

- да контролират на кои устройства е разрешен достъп до техните системи и услуги;
- да са уверени, че устройството има инсталиран актуален антивирусен софтуер;
- да могат да определят дали устройството е криптирано;
- да проверяват дали устройството има инсталирани актуални софтуерни корекции;
- да прилагат защита с ПИН и/или парола на устройството;
- да изтриват дистанционно от устройството всички данни за МСП, ако собственикът на устройството съобщи, че е изгубено или откраднато, или той повече не работи за това МСП.

ИЗПОЛЗВАНЕ НА ЗАЩИТНИ СТЕНИ

Защитните стени управляват трафика, който влиза и напуска мрежата и са средство от критично значение за защитата на системите на МСП. Защитните стени трябва да бъдат прилагани за защита на всички критични системи, и по-специално да се използват за защита на мрежата на МСП от интернет.

ПРЕГЛЕД НА РЕШЕНИЯТА ЗА ОТДАЛЕЧЕН ДОСТЪП

МСП трябва редовно да преглеждат всички инструменти за отдалечен достъп, за да се уверят, че са сигурни, и по-специално:

- да се уверят, че целият софтуер за отдалечен достъп е с последните корекции и актуализации;
- да ограничат отдалечения достъп от подозрителни географски точки или определени IP адреси;
- да ограничат отдалечения достъп на персонала само до системите и компютрите, които са необходими за работата;
- да използват сигурни пароли за отдалечен достъп и да активират двуфакторна автентикация, където е възможно;
- да се уверят, че са активирани функциите за наблюдение и сигнализация, за да се предупреждава за предполагаеми атаки или необичайна подозрителна дейност.

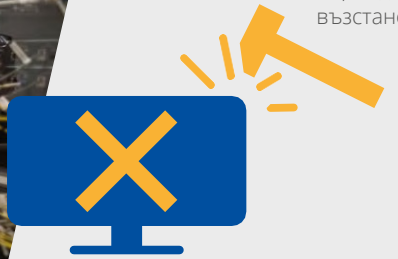
8 ПОДОБРЯВАНЕ НА ФИЗИЧЕСКАТА СИГУРНОСТ

Навсякъде, където има важна информация, трябва да се прилагат подходящи мерки за физически контрол. Например фирмен лаптоп или смартфон не трябва да се оставя без надзор на задната седалка в колата. Всеки път, когато потребител се отдалечи от компютъра си, трябва да го заключи. В противен случай трябва да се активира функцията за автоматично заключване на всяко устройство, използвано за стопански цели. Чувствителните отпечатани документи също не трябва да се оставят без надзор и когато не се използват, да се съхраняват на сигурно място.

9 СИГУРНИ РЕЗЕРВНИ КОПИЯ

За да има възможност за възстановяване на важна информация, трябва да се правят резервни копия, тъй като те са ефективен начин за възстановяване от инциденти като атаки на софтуер за изнудване. Трябва да се прилагат следните правила за резервно копиране:

- резервни копия да се правят редовно и автоматизирано, когато е възможно;
- резервните копия да се съхраняват отделно от производствената среда на МСП;
- резервните копия да са криптирани, особено ако ще бъдат премествани между обекти;
- да се тества възможността за периодично възстановяване на данни от резервните копия; в идеалния случай трябва периодично да се тества дали може да се извърши пълно възстановяване от началото до края.



10

РАБОТА В ОБЛАК

Въпреки че предлагат много предимства, облачните решения поставят някои специфични рискове, които МСП трябва да имат предвид, преди да се ангажират с доставчик на облачни услуги. ENISA публикува „Ръководство за МСП за сигурност в облак"[2], което МСП трябва да ползват при преминаване към работа в облак.

Когато избират доставчик на облачни услуги, МСП трябва да гарантират, че не нарушават никакви закони или разпоредби, когато съхраняват данни извън ЕС/ЕИП, особено лични данни. Например ОРЗД на ЕС изисква личните данни на пребиваващи в рамките на ЕС/ЕИП лица да не се съхраняват или предават извън ЕС/ЕИП, освен при много специфични условия.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 СИГУРНИ ОНЛАЙН САЙТОВЕ

От съществено значение е МСП да гарантират, че техните уебсайтове онлайн са конфигурирани и поддържани по сигурен начин и че всички лични данни или финансова информация, като данни за кредитни карти, са подходящо защитени. Това се изразява в провеждане на редовни тестове за сигурност на уебсайтовете, за да се открият евентуални слабости в сигурността, и извършване на редовни прегледи, за да се гарантира, че сайтът се поддържа и актуализира правилно.

12 ТЪРСЕНЕ И ОБМЕН НА ИНФОРМАЦИЯ

Ефективно средство в борбата с киберпрестъпността е споделянето на информация. Споделянето на информация във връзка с киберпрестъпността е от ключово значение, за да могат МСП да разберат по-добре рисковете, пред които са изправени. Дружествата, които научават за предизвикателствата във връзка с киберсигурността и как такива предизвикателства са били преодолени от техни колеги, е по-вероятно да предприемат стъпки за защита на своите системи, отколкото ако научат подобна информация от доклади в сектора или от проучвания за киберсигурността.

АГЕНЦИЯ НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА КИБЕРСИГУРНОСТ

ЗА ENISA

Агенцията на Европейския съюз за киберсигурност (ENISA) е агенцията на Съюза, насочена към постигане на високо равнище на киберсигурност в цяла Европа. Създадена през 2004 г. и укрепена с Акта за киберсигурността на ЕС, Агенцията на Европейския съюз за киберсигурност допринася за политиката на ЕС в областта на киберсигурността, повишава надеждността на ИКТ продукти, услуги и процеси със схеми за сертифициране на киберсигурността, сътрудничи си с държавите членки и органите на ЕС и помага на Европа да се подготви за бъдещи предизвикателства в областта на киберсигурността. Агенцията работи съвместно с ключовите си партньори — чрез обмен на знания, изграждане на капацитет и повишаване на осведомеността — за повишаване на доверието в свързаната с интернет икономика, за стимулиране на устойчивостта на инфраструктурата на Съюза и в крайна сметка за гарантиране на цифровата сигурност на обществото и гражданите на Европа. За повече информация посетете www.enisa.europa.eu.

ENISA
Агенция на Европейския съюз за киберсигурност

Управление в Атина
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki,
Гърция

Офис в Ираклион
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Гърция

enisa.europa.eu