Управление на риска в МСП

Контролен списък за киберрискове и устойчивост

на Accountancy Europe

Информационен бюлетин

<https://accountancyeurope.eu/publications/sme-risk-management-cyber-risks-resilience-checklist/>

Акценти

Киберинцидентите могат да окажат значително въздействие върху способността на МСП да извършват стопанска дейност и да причинят големи финансови загуби. Изключително важно е МСП да идентифицират и намалят тези рискове в контекста на все по-голямата цифровизация на нашите икономики.

Счетоводителите на МСП са техни доверени съветници и могат да играят ключова роля в намаляването на киберриска за МСП. Този документ - последният от поредицата на Accountancy Europe - "Управление на риска в МСП" - предоставя контролен списък за счетоводителите за подобряване на киберустойчивостта на МСП. Самите счетоводни практики също могат да използват този инструмент, за да оценят собствената си киберустойчивост

Въведение

Малките и средни предприятия (МСП) са изправени пред нови рискове, които могат да окажат значително влияние върху техния бизнес. Тези рискове произтичат от глобални мегатенденции като климатичната криза, цифровизацията, глобалната икономическа интеграция и COVID-19.

Accountancy Europe публикува поредица материали, посветени на управлението на риска в МСП, за да осигури информация за МСП и техните счетоводители: устойчиво развитие (юли 2020 г.), контролен списък с въпроси относно устойчивостта на МСП (2021 г.), интелектуална собственост (2022 г.) и неплатежоспособност (2021 г.).

Този шести документ е посветен на киберрисковете. В него ще бъде обяснено защо и как МСП трябва да разглеждат и смекчават киберрисковете и как счетоводителят на МСП може най-добре да ги подкрепи. Документът включва контролен списък, който счетоводителят може да използва, за да подпомогне изграждането на устойчивост на киберриска на своите клиенти, които са малки или средни предприятия.

Контролният списък може да послужи като основа за обсъждане или първоначална оценка на киберустойчивостта на клиента. Той може също така да подпомогне изграждането на киберустойчивост и осведоменост за киберриска в самата счетоводна практика. Не е необходимо счетоводителите сами да се справят с всеки елемент от контролния списък, но те трябва да могат да разпознават кога да насочат клиентите си към съответната техническа експертиза.

Пред кои киберрискове са изправени МСП?

В доклада за глобалните рискове на Световния икономически форум за 2021 г. провалът в киберсигурността е посочен като четвъртият по големина ясен и съществуващ риск, който може да причини критична заплаха за света. Това го поставя непосредствено след други критични рискове, като например климатичните бедствия или инфекциозните болести.

Киберрисковете се пораждат от все по-цифровизираните икономики и бизнес модели, например в бизнес процесите, плащанията, списъците с клиенти и контакти или разработването на продукти и услуги. МСП могат да се възползват от подобрената ефективност, иновациите, производителността и управлението, които технологиите осигуряват. Но те също така трябва да са наясно с рисковете, които могат да възникнат заедно с тези възможности и да ги смекчават, за да се възползват напълно от потенциала на цифровите технологии.

Киберзаплахите са сред основните рискове, свързани с цифровизацията. Те могат да бъдат разделени приблизително на човешки грешки и кибератаки:

* Човешките грешки са резултат от неволни грешки на служители, мениджъри или бизнес партньори, които имат достъп до цифровизираните работни процеси или бази данни на предприятието. Примерите включват неволно публикуване на клиентски списъци или други чувствителни данни, забравяне на пароли, изтриване на цифрово съдържание или нарушаване на законодателство като Общия регламент за защита на данните (ОРЗД) на ЕС;
* Кибератаките се състоят в това, че злонамерени лица, които могат да бъдат както външни лица, така и бизнес партньори или служители на МСП, умишлено увреждат, унищожават, шпионират, споделят, публикуват или по друг начин злоупотребяват с цифровото съдържание и процеси на компанията (вж. по-долу конкретни примери).

Една ефективна стратегия за намаляване на киберриска трябва да обхваща и двете измерения, тъй като те са взаимосвързани. Човешките грешки могат да изложат бизнеса на кибератаки, докато кибератаките създават благоприятна почва за човешки грешки.

Примери за кибератаки

Според доклад на Агенцията на ЕС за киберсигурност (ENISA) от 2021 г. най-често срещаните киберинциденти, с които са се сблъсквали европейските МСП, са били:

* 41% фишинг
* 40% уеб-базирани атаки
* 39% общ зловреден софтуер
* 19% злонамерен вътрешен участник
* 12% отказ на услуга
* 11% социално инженерство
* 7% компрометирано/откраднато устройство

**Мултиплициращият ефект на пандемията**

Киберрисковете се засилват допълнително от последните тенденции, породени от пандемията COVID-19, които подтикват предприятията да работят все повече дистанционно и онлайн. Така например, по време на пандемията броят на фишинг имейлите се увеличи с 667%.

Как киберрисковете могат да засегнат МСП?

МСП са все по-предпочитана мишена от извършителите на кибератаки. Три пъти по-вероятно е те да станат мишена на киберпрестъпници, отколкото големите предприятия.

Примерите за негативните последици от киберинцидентите за МСП включват следното:

* финансови загуби: киберинцидентите често водят до значителни финансови загуби, произтичащи от:
* кражба на фирмена информация, финансова информация, например, банкови данни или данни за платежни карти, или пари;
* прекъсване на търговията, например невъзможност за извършване на транзакции онлайн, значително прекъсване на производството или други ключови процеси, базирани на ИТ;
* разходи за ремонт на засегнатите системи, мрежи и устройства.
* бизнес загуби: доверието е съществен елемент от бизнес отношенията. Кибератаките могат да навредят на репутацията на МСП и да подкопаят доверието на клиентите и бизнес партньорите. Това, от своя страна, може да доведе до загуба на клиенти, бизнес партньори и продажби.
* правни последици: законите за защита на данните и неприкосновеността на личния живот изискват от предприятията да управляват сигурността на всички лични данни, които притежават - независимо дали става въпрос за служители, клиенти или бизнес партньори. Ако тези данни са случайно или умишлено компрометирани и МСП не е въвело подходящи мерки за сигурност, то може да бъде подложено на глоби и регулаторни санкции.

Кои са основните пречки пред киберустойчивостта на МСП?

Укрепването на киберустойчивостта е от решаващо значение за МСП, за да се намалят рисковете от киберинциденти и отрицателните въздействия, описани по-горе. Съществуват някои пречки, които могат да възпрепятстват усилията в тази област, както е подчертано от ENISA.

Недостатъчна информираност

Липсата на осведоменост и ангажираност на ръководството са най-съществените пречки пред намаляването на киберрисковете. На практика това означава отпускане на бюджет, ресурси и прилагане на ефективни процеси за киберсигурност.

Много собственици на МСП са заети с ежедневната работа и може да не осъзнават мащаба на риска, който грешките и атаките, свързани с киберсигурността, могат да представляват за техния бизнес. Поради това те може да не дават приоритет на предприемането на превантивни мерки за защита на бизнеса си и да открият разходите едва след като киберрискът се е реализирал.

Проблем е и ниската осведоменост на персонала за киберриска. Всяко лице в МСП, което има достъп до неговите системи за информационни технологии, може несъзнателно да предизвика киберинцидент. Ето защо е жизненоважно целият персонал да бъде нащрек за потенциални проблеми, свързани с киберсигурността.

Слаба защита на критична и чувствителна информация

МСП боравят с разнообразна информация, като например данни за персонала, информация за клиентите, данни за производството и доставките, финансови данни, политики, процедури и др. Всички те са от съществено значение за компанията. Законите, нормативните разпоредби или споразуменията също може да изискват от МСП да ги защитава.

Липсата на конкретна политика за създаване на резервни копия, на актуални решения за защита от зловреден софтуер за всички видове устройства или използването на остарял или неактуализиран софтуер може сериозно да застраши критичната и чувствителна информация на компанията. Това би превърнало МСП в лесна мишена за видовете кибератаки, описани по-горе.

Недостатъчен бюджет

Усилията в областта на киберсигурността са свързани със значителни инвестиции, включително обучение за повишаване на осведомеността, въвеждане на механизми за контрол на киберсигурността, ангажиране на външни експерти и специализирано обучение на служителите. Много МСП гледат на киберсигурността като на разход, а не като на съществена инвестиция в бизнеса си. Поради това МСП следва да разбират по-добре рисковете, които проблемите на киберсигурността представляват за техния бизнес, и да отделят подходящи бюджети, за да инвестират в необходимите контроли за защита на критичните области на техния бизнес.

Липса на експертни познания и персонал

Управлението на киберсигурността в МСП е голямо предизвикателство. Киберсигурността е тема, която изисква специализирани познания. Въпреки това в МСП е обичайно хората да работят по няколко задачи и да им се възлагат няколко роли. В резултат на това даден служител в МСП може да отговаря за киберсигурността и за други вътрешни процеси.

Много от решенията за киберсигурност изискват специализирани ИТ познания, за да бъдат приложени и управлявани правилно. От съществено значение е да се разпознаят потенциалните ограничения на служителя, отговарящ за киберсигурността, и кога например може да е необходим временно допълнителен експертен опит.

Когато бизнесът на едно МСП се разраства и променя, технологиите, които използва, също се променят. Това означава, че пейзажът на киберзаплахите ще се развива. Ето защо МСП ще трябва да гарантират, че усилията им за управление на киберсигурността са непрекъснати и последователни. Ако дружеството не разполага с пряк служител със специализирани познания в областта на информационните и компютърните технологии (ИКТ) (което е типично за нетехнологичните МСП), е необходимо да се инвестира във външна експертна помощ.

Липса на подходящи насоки

Наличието и пригодността на насоки под формата на стандарти, официални документи или други подобни е друго голямо предизвикателство. Такива документи вече съществуват, но ENISA твърди, че повечето от тях или предоставят твърде обща информация, или са твърде сложни за МСП и биха изисквали от тях да търсят специфични експертни познания в областта на ИТ. Освен това много МСП просто не знаят за съществуването на такива насоки, не знаят кои от тях биха били най-подходящи за техния бизнес или дори не знаят откъде да започнат.



Защо счетоводителят е в състояние да помогне?

Професионалните счетоводители са добре позиционирани да помогнат на МСП да преодолеят някои от пречките, очертани в предходния раздел. Повечето счетоводители не са ИТ експерти. Въпреки това те са в уникална позиция да подпомогнат изграждането на киберустойчивост на МСП, защото:

* те са доверени съветници на МСП;
* повечето МСП в Европа вече разчитат на счетоводители за услуги като бизнес планиране, управление на финансовите и паричните потоци, данъчно облагане и спазване на законодателството, водене на счетоводство и финансови консултации. Това означава, че те често имат подробни познания за ИТ системите на своите клиенти, особено по отношение на финансовите им системи;
* собствениците на МСП се срещат редовно със счетоводителите си и те могат да бъдат първата точка за контакт за МСП;
* малките и средните предприятия разчитат на счетоводителите да ги съветват и да подлагат на критична оценка предположенията за управлението на бизнеса им.

Всеки самостоятелен счетоводител или счетоводна фирма може да има стотици клиенти МСП. Така счетоводителите са натрупали богат опит в това какво върши работа за предприятията. По този начин счетоводителите разбират фундаменталните аспекти на бизнеса, който обслужват.

По-специално в областта на киберсигурността счетоводителите могат да помогнат за:

* повишаване на осведомеността на ръководството и персонала на МСП относно необходимостта от намаляване на киберрисковете;
* консултиране във връзка с това кои бизнес операции или практики най-вероятно пораждат киберрискове;
* идентифициране кои части на бизнеса са "най-съществени" за ежедневните операции и следователно се нуждаят от специално внимание и максимална защита. Например счетоводните системи трябва да бъдат архивирани, за да се гарантират сравнително минимални смущения, а спирането на производството, предизвикано от ИТ, може да има много по-сериозни последици за МСП и трябва да бъде съответно защитено;
* бюджетиране и планиране на инвестициите в киберустойчивост на МСП, консултиране относно най-критичните мерки, които трябва да бъдат предприети и съобразени с особеностите на конкретния бизнес;
* определяне на това кога и къде ще е необходима специализирана ИТ експертиза за въвеждането на конкретни стъпки за киберустойчивост и свързване на МСП със съответните експерти в мрежата на счетоводителя;
* информиране на МСП за съответното законодателство, като например ОРЗД, и оказване на помощ при спазването му;
* осигуряване на независимо изразяване на сигурност относно системите за киберустойчивост на МСП, стига това да е лице и фирма, различни от тези, които са консултирали МСП за създаването им;
* консултиране във връзка с разработване на планове за действие при извънредни ситуации в случай на кибератака.

Следващият раздел предлага прост контролен списък за счетоводителя, който да подпомогне работата му по изграждане на устойчивост на киберриска сред клиентите, които са МСП.

Контролен списък за счетоводителите

За МСП е скъпо да наемат собствени ИТ експерти или да се обръщат към специализирани ИТ експерти. Въпреки това има някои основни стъпки, които всяко МСП може да предприеме, за да подпомогне изграждането на своята устойчивост на киберрискове.

Счетоводителят на МСП може да използва този контролен списък, за да определи текущото състояние на МСП по отношение на киберрисковете и да помогне за предприемане на действия, когато е необходимо. Счетоводителят трябва също така да може да прецени и да даде съвет кога ще е необходима специализирана ИТ експертиза.

Учене чрез практика

Не всички счетоводни практики в Европа са на едно и също ниво по отношение на уменията за работа в киберпространството, осведомеността за киберриска и предоставянето на свързаните с това услуги. Всяка практика или практикуващ професионален счетоводител, който се интересува от предоставянето на услуги за киберустойчивост на клиенти, които са МСП, трябва да започне със собствената си практика. Те трябва да извършат самооценка на практиката си - например като използват за помощ посочения по-долу контролен списък - и постепенно да изградят своята киберустойчивост.

Това ще помогне да се гарантира, че практиката и нейните данни са защитени от киберрискове. Освен това то ще помогне за натрупване на опит и експертни познания в областта на киберустойчивостта и ще развие мрежа от киберексперти, към които счетоводителят евентуално може да насочи своите клиенти.

Стъпка 1 – мрежа

Счетоводителите трябва да започнат с изграждането на мрежа от експерти по ИКТ, на които могат да разчитат за допълнителна информация и към които да насочват при необходимост клиентите, които са МСП.

Счетоводителят може да запознае МСП с киберрисковете, да ги убеди да предприемат действия и да им даде съвети за някои прости първоначални стъпки. Повечето счетоводители обаче нямат опит в областта на ИКТ, за да въведат по-сложни решения, ако такива са необходими. Счетоводителите също така са обвързани с професионални изисквания, които гарантират, че няма да поемат работа, ако нямат необходимите умения.

Стъпка 2 – таблица да оценяване

Таблицата е базирана на прост инструмент, разработен от SMESEC, насочен специално към МСП с ограничени ресурси, опит и знания в областта на киберсигурността. Попълването на таблицата и предприемането на първоначалните стъпки за подобряване би трябвало да е лесно и икономически ефективно за много МСП. Счетоводителят следва да я използва като основа за разговорите си с клиенти - МСП относно тяхната устойчивост на киберрискове.

Контролният списък може да се използва и за подпомагане на изграждането на киберустойчивост и осведоменост в самата счетоводна практика. Не е необходимо счетоводителят да може да отговори директно на всеки от пунктовете на контролния списък, но трябва да може да разпознае кога да насочи клиентите си към съответната техническа експертиза.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Вид риск | Да | Не | Не зная |
|  | Дали клиентите на МСП са наясно с киберрисковете и дали е малко вероятно да изложат МСП на киберзаплахи? |  |  |  |
| Информираност | Знае ли персоналът на МСП как да разпознава и да се справя с подозрителни или несигурни имейли, уебсайтове с хипервръзки и хардуерни повреди и да предприема съответните действия?  *Например, опасни преносими USB устройства* |  |  |  |
| А доставчиците? |  |  |  |
| Получават ли служителите на МСП редовно обучение по киберсигурност? |  |  |  |
|  | Създало ли е МСП политика за информационна сигурност, разпространена и обяснена сред служителите? |  |  |  |
| Задачи и отговорности | Определило ли е МСП лице, което да отговаря за киберсигурността?  *т.е. доверен служител, на когото се докладват кибернарушения и грешки; отговаря за действията след кибератаката и за подобряване на осведомеността на персонала.* |  |  |  |
| Има ли това лице познания и умения за справяне с най-разпространените видове кибератаки, посочени в настоящия документ? |  |  |  |
| Има ли това лице правомощията в рамките на МСП да предприеме действия за подобряване? |  |  |  |
| Разполага ли МСП с план за смекчаване на отрицателните икономически последици в случай на успешна кибератака? |  |  |  |
| Защита на данните | Криптирани ли са чувствителните и критичните данни, съхранявани от МСП, включително данните в мобилните устройства? |  |  |  |
| Обработва ли МСП лични и чувствителни данни в съответствие с ОРЗД на ЕС? |  |  |  |
| Защитава ли МСП физическия достъп до своите компютри, сървъри и мрежа? |  |  |  |
| Външни акционери |  |  |  |
| Структура на собствеността |  |  |  |
| Основни източници на финансиране |  |  |  |
| Архивиране | Разполага ли МСП с актуално резервно копие на своите данни и системи? |  |  |  |
| Дали резервното копие се съхранява офлайн или поне на друго място и напълно изключено от съответните системи? |  |  |  |
| Опитало ли е МСП да възстанови резервно копие на данни и/или на системата и уверило ли се е, че това работи? |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Вид риск | Да | Не | Не зная |
| Администриране на пароли и потребители | Защитени ли са акаунтите чрез многофакторна автентикация (MFA)? *напр. парола, комбинирана с пин-код или токен за сигурност* |  |  |  |
| Сигурни ли са паролите на служителите на МСП, специфични ли са за всеки потребителски акаунт и система и променят ли се периодично? |  |  |  |
| Дали всеки един служител може да има достъп само до системите, до които трябва да има достъп? |  |  |  |
| Надеждно ли е блокиран достъпът на бивши служители до системите? |  |  |  |
| Ако даден служител е бил обект на кибератака, променена ли е паролата му? |  |  |  |
| Въведена ли е процедура за ограничаване и защита на използването на административните привилегии за системата? |  |  |  |
| Защита от зловреден софтуер | ИТ мрежата на МСП защитена ли е от защитна стена, която да предпазва системите им от външни атаки? |  |  |  |
| Защитени ли са устройствата, системите и приложенията на МСП срещу зловреден софтуер (напр. антивирусни програми, защита от софтуер за откуп, филтри за спам)? |  |  |  |
| Конфигурирало ли е МСП защитата си от зловреден софтуер за сканиране на прикачени файлове по електронна поща, изтегляния, файлове, получени по мрежи и свързани носители за съхранение? |  |  |  |
| Актуализации | Актуализира ли се редовно целият софтуер на устройствата на служителите на МСП (напр. приложения и операционни системи)? |  |  |  |
| Актуализира ли се редовно защитата на МСП от зловреден софтуер (напр. антивирусни програми, филтри за спам))? |  |  |  |
| Актуализира ли се редовно целият софтуер на сървърите и устройствата на собственика на МСП, включително защитната стена? |  |  |  |
| Защитена комуникация | Актуализира ли се редовно целият софтуер на сървърите и устройствата на собственика на МСП, включително защитната стена? |  |  |  |
| Криптирани ли са паролите и изпратените данни между клиентите и сървъра? |  |  |  |
| Криптирана и защитена ли е WLAN мрежата на собственика на МСП и собственикът изисква ли от служителите си да използват VPN в домашни условия, за да имат достъп до системите на компанията? |  |  |  |
| Реагиране при извънредни ситуации | В състояние ли е лицето, което отговаря за киберсигурността, да прекрати кибератака и да ограничи последиците от нея? |  |  |  |
| Знаят ли ръководителите и служителите на МСП какво да правят в случай на киберинцидент? Има ли въведени в действие процедури и ясно разпределени роли? |  |  |  |
| В случай че клиентите или доставчиците на МСП бъдат атакувани, ще информират ли те предприятието за атаката, ако то е засегнато? |  |  |  |
| Разполага ли МСП с контакт с експерт по ИКТ, който може да му окаже подкрепа в случай на спешна нужда? |  |  |  |
| Има ли МСП сключена застраховка за покриване на свързаните с ИТ прекъсвания на дейността, включително кибератаки, и съответния ефект върху дейността? |  |  |  |
| В случай на разработване на софтуер | Разделена ли е WLAN за служители от WLAN за гости? |  |  |  |
| Определило ли е МСП кой е отговорен за сигурността на всеки от неговите софтуерни продукти и услуги? |  |  |  |
| Извършва ли МСП проверка на кода, особено за откриване на уязвимости и пропуски в сигурността? |  |  |  |
| Извършило ли е МСП тестване по метода на черната кутия срещу често срещани заплахи за сигурността? |  |  |  |
| Резултати | |  |  |  |

Стъпка 3 – анализиране на резултатите и предприемане на подходящи действия

Ако общият брой на отговорите ви ДА е между:

|  |  |
| --- | --- |
| 0 - 10 | МСП е лесна плячка. Помогнете на МСП да определи най-лесните отговори „Не" или „Не зная" и да ги превърне в „Да" |
| 11 - 24 | МСП има добра изходна позиция, но е необходим по-голям напредък. Разработете план за промяна, който да ви помогне да постигнете резултат от 24 или повече точки в рамките на 6 месеца |
| 25 - 30 | МСП вече прави много в областта на киберсигурността. Обсъдете заедно къде може да се направи повече |
| 31 - 38 | МСП е еталон и пример за подражание за други |

Заключение

Киберинцидентите - както умишлени, така и дължащи се на човешка грешка - могат да окажат сериозно въздействие върху бизнес дейностите и оцеляването на МСП. От изключителна важност е собствениците и служителите на МСП да са наясно с потенциалните киберрискове, да работят заедно за тяхното намаляване и да действат ефективно, ако се стигне до киберинцидент.

Счетоводителите на МСП могат да помогнат. Те познават МСП и са в състояние да дават съвети в области като картографиране на киберриска, стъпките за смекчаване, повишаване на осведомеността и др. Контролният списък в този документ е предназначен да помогне на счетоводителя да проведе първоначален разговор за картографиране на киберпространството със своите клиенти, които са МСП.

Но въпреки всички усилия за намаляване на киберрисковете, те все пак могат да се реализират. Малките и средните предприятия и техните счетоводители трябва да създадат ефективни процедури, резервни копия и системи, за да осигурят непрекъснатост на дейността и възстановяване на системите, когато рисковете се материализират. Контролният списък може да помогне и тук.



Приложение – дефиниции и терминология

**Фишинг:** вид социален инженеринг, при който нападателят изпраща измамно (например подправено, фалшиво или друго заблуждаващо) съобщение, целящо да подмами дадено лице да разкрие чувствителна информация на нападателя или да разположи зловреден софтуер в инфраструктурата на жертвата, например софтуер за откуп**.**

**Отказ на услуга:** атаката DoS не позволява на потребителите да получат достъп до дадена услуга, като претоварва нейните физически ресурси или мрежови връзки.

**Уеб-базирани атаки:** когато престъпниците използват уязвимости в кодирането, за да получат достъп до сървър или база данни, тези видове кибервандалски заплахи са известни като атаки на ниво приложение. Потребителите се доверяват, че чувствителната лична информация, която разкриват на вашия уебсайт, ще бъде запазена в тайна и безопасност.

**Зловреден софтуер:** общото наименование на вариантите на зловреден софтуер, включително вируси, софтуер за откуп и шпионски софтуер. Съкратено наименование на злонамерен зловреден софтуер, зловредният софтуер обикновено се състои от код, разработен от лицата, извършващи кибератаки, предназначен за причиняване на големи щети на данни и системи или за получаване на неоторизиран достъп до мрежа.

**Злонамерен вътрешен участник:** познат също като Turncloak, човек, който злонамерено и умишлено злоупотребява със законни пълномощия, обикновено за да открадне информация с цел финансови или лични стимули.

**Социално инженерство:** това е техника за манипулиране, при която се използва човешка грешка, за да се получи лична информация, достъп или ценности.

**Многофакторна автентификация:** MFA е метод за електронно удостоверяване, при който на потребителя се предоставя достъп до уебсайт или приложение само след успешно представяне на две или повече доказателства.

**Софтуер за откуп:** представлява вид зловреден софтуер, който заплашва да публикува личните данни на жертвата или да блокира трайно достъпа до тях, ако не бъде платен откуп.

**Административни привилегии за системата:** това е възможността да се правят значителни промени в дадена система, обикновено операционна система. Те могат да означават и големи софтуерни програми, като например система за управление на бази данни.

**Бял списък, разрешителен списък или пропусквателен списък:** механизъм, който изрично позволява на някои идентифицирани субекти да имат достъп до определена привилегия, услуга, мобилност или разпознаване, т.е. това е списък на разрешените неща, когато всичко е забранено по подразбиране.

**WLAN**: Безжична зонална мрежа.

ОГРАНИЧАВАНЕ НА ОТГОВОРНОСТТА: Accountancy Europe полага всички усилия, за да се увери, но не може да гарантира, че информацията в настоящата публикация е точна, и не може да поеме никаква отговорност във връзка с тази информация. Насърчаваме разпространението на настоящата публикация, ако сме посочени като източник на материала и има хиперлинк, който препраща към нашето оригинално съдържание. Ако желаете да възпроизведете или преведете тази публикация, моля, изпратете запитване на адрес [info@accountancyeurope.eu](mailto:info@accountancyeurope.eu).