организация по съставяне, връчване и събиране на наложени санкции и глоби, чрез акт за установяване на административни нарушения или глоба с фиш. Темата за собствените приходи на общините е необятна и изключително важна и според мен, ако дадена община няма законосъобразна и оптимална организация за събиране на собствени приходи, не може да получи финансова автономност и тук отново идва проблемът с общините с бюджет под 10 милиона.

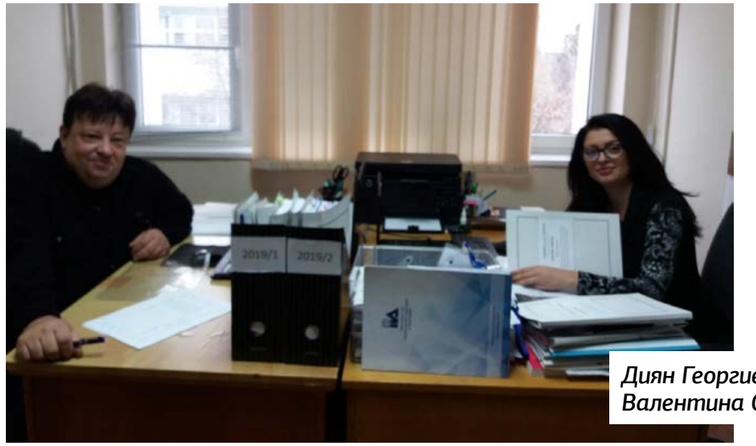
Може би ще се повторя, като отбележа, че ако държавата не въведе адекватен и всеобхватен вътрешен одит в общините, чрез критерии за численост на вътрешни одитори и ресурси - дейността по вътрешен одит, като качество и перспектива за утвърждаване, е обречена на провал и с все по-голямо затихване в бъдеще.

В подкрепа на моите виждания държа да акцентирам, че бюджетните функции и дейности в една община по видове и многообразие съвпадат с тези на държавата, т. е. говорим за компетентности на вътрешен одитор в общината в сферите на образование, здравеопазване, социални грижи и услуги, строителство, транспорт, общинска собственост, спорт, култура, обществени поръчки, местни данъци и такси и други дейности от така наречената необятна вселена на една община.

Видно е, че без определени средства в единен разходен стандарт в делегирана от държавата бюджетна дейност по осъществяване на вътрешен одит - на одиторите в общините не се осигурява достатъчно прилично възнаграждение и средства за обучение. Факт е, че в единния класификатор на длъжностите в администрацията и наредбата, в която са определени - минимални и максимални прагове на възнаграждения на одиторите са заложени прилични размери. Напълно възможно е чрез въвеждане на критерии като размер на бюджета на общината или населението в нея и чрез определяне да единен разходен стандарт да се формира размер на субсидия за общината за осъществяване на ефективен и ефикасен вътрешен одит.

И накрая, ще си позволя да споделя мнението си, базирано на публикации, статии и презентации на вътрешни одитори, че успели мениджъри и собственици на фирми споделят и мнението, че вътрешният одит е изключително необходим, полезен и много ценен. Той е особено ценен в западните фирми. За съжаление у нас все още ръководителите не го приемат като средство за подпомагане на законосъобразно, ефективно и ефикасно управление на дейността на бизнеса както в публичния, така и в частния сектор.

Разговорът проведе Валентина Пенчева



Диян Георгиев с колегата си Валентина Стоилова - стажант-одитор.

Редакционният съвет очаква и други мнения и предложения по проблеми на професията от ръководители на звена за вътрешен одит или споделяне на опит за тяхното решаване.

СЪОТВЕТСТВИЕ НА ИЗИСКВАНИЯТА ЗА КИБЕРСИГУРНОСТ

д-р Младен Младенов (MPS, LL.M, MPF, MSM), адвокат

Професионалната биография на д-р Младен Младенов е свързана с адвокатурата, съдебната система и държавната администрация.

Експертиза: право, юридически професии и дейности, нормотворчество, публична администрация, алтернативни методи за разрешаване на спорове, вътрешен одит, контролни дейности, етика, интегритет, методология, обучение.

Има над 100 публикации в страната и в чужбина, като между тях изпъква книгата „Дескриптивна юриспруденция", разглеждаща множество аспекти на юридическите професии, длъжности и дейности.

ВЪВЕДЕНИЕ

Понастоящем целият модерен и цивилизован свят е ангажиран с разрешаването на множество тежки проблеми, като безспорно един измежду най-важните от тях е проблемът с киберсигурността. Той касае съюзи, държави, общества, организации и отделни граждани. Неговите аспекти са практически неизмерими, като постоянно се преформатират от развитието на технологиите и професионалните капацитети.

Националната ни държава адекватно е въвела във вътрешното законодателство изискванията на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.), както и е предвидила по нормативен път мерки по прилагане на Регламент за изпълнение (ЕС) 2018/151 на Комисията от 30 януари 2018 г. за определяне на правила за прилагане на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета по отношение на допълнителното уточняване на елементите, които трябва да се вземат предвид от доставчиците на цифрови услуги при управлението на рисковете за сигурността на мрежите и информационните системи, както и на показателите за определяне на това дали даден инцидент има съществено въздействие (ОВ, L 26/48 от 31 януари 2018 г.).

Това е постигнато със Закона за киберсигурност, Обн. ДВ. бр. 94 от 13 ноември 2018 година. Същият се състои от 3 глави и 31 основни разпоредби. Той е задължителен за всички:

- ***административните органи*** – тук спада всеки орган на власт, който принадлежи към системата на изпълнителната власт, както и всеки носител на административни правомощия, овластен въз основа на закон.
- ***операторите на съществени услуги*** и доставчиците на цифрови услуги - за всеки сектор, подсектор и услуги, посочени в приложения №1 и №2 към закона. Изброяването е доста подробно, като само някои от тези оператори и доставчици са: електроенергийни предприятия; оператори на система за втечнен природен газ; въздушни превозвачи; управители на инфраструктура; предприятия за вътрешноводен, морски и крайбрежен транспорт на пътници и товари; пътни органи; кредитни институции; здравни заведения, включително болници и частни клиники и други.
- ***лицата, осъществяващи публични функции***, които не са определени като оператори на съществени услуги, когато тези лица предоставят административни услуги по електронен път, като нотариусите, частните съдебни изпълнители, държавните и общинските

учебни заведения, държавните и общинските лечебни заведения.

- ***организациите, предоставящи обществени услуги***, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на този закон, когато тези организации предоставят административни услуги по електронен път, като тук влиза широка гама от организации в областта на образователните, здравните, водоснабдителните, канализационните, топлоснабдителните, електроснабдителните, газоснабдителните, телекомуникационните, пощенските, банковите, финансовите и други подобни по вид и важност услуги.

По същество

Във връзка с всички действия на горните задължени по закона субекти, касаещи съответствието със законодателството относно киберсигурността, мениджърите и одиторите в горните организации от частния и публичен сектор трябва да насочат своите усилия в няколко направления. **На първо място**, прецизно, акуратно и пълно разпределение на отговорностите за мрежовата и информационната сигурност. Тук не трябва да има нито непокриване, нито припокриване между задълженията на различните звена и служители в организацията. Например, условно наречените звена „Информационни технологии“, „Информационна сигурност“, „Вътрешна сигурност“ и „Правно обслужване“ трябва във всеки един момент да поемат своите ангажименти към киберсигурността на организацията. Те трябва да се допълват взаимно с нови подходи, мерки и стъпки за повишаването на нивото на тази сигурност и своевременно да уведомяват ръководството и едни други за евентуални проблеми, опасности и рискове в тази насока.

На второ място, действително прилагане на адекватна политика за мрежовата и информационната сигурност. От особена важност тук е правилата и принципите на тази политика не само да са разписани „на хартия“, но действително да се прилагат. Един от работещите методи, за да се случи това, е личната ангажираност с нея на всички ръководни служители в организацията и на водещите експерти в отделните области. Това може да бъде една от клаузите на техните длъжностни характеристики, като впоследствие се явява също така и критерий за оценяване на работата им и приносът им към резултатите на организацията.

На трето място, управление на риска. По автономното разбиране на този закон, Риск" е потенциалната възможност дадена заплаха да се осъществи, като се експлоатира уязвимостта на информационните активи, за да се причини вреда. Това означава, че вземащите решенията в организацията лица, както и одиторите би трябвало да са абсолютно наясно с уязвимостта на информационните активи – по тежест (висока, средна, ниска), по регулация (търговска, промишлена, производствена, служебна тайна; лични данни; класифицирана информация; данъчно-осигурителна информация и друга защитена от закона

информация), по материални носители (на хартиен или на електронен носител; текстови, образен или звуков вход и други), по местоположение на заплахата от уязвимост (външна или вътрешна за организацията). Също така, би трябвало да са класифицирани и квалифицирани всички възможни по вид и степен евентуални вреди от горната заплаха – независимо от предишните им наименования (щети, повреди и други) и честота им на сбъдване (дори и никога неслучилите се за организацията).

На четвърто място, управление на информационните активи, включително човешките ресурси. Сами по себе си, информационните активи могат да бъдат документи, регистри, процедури и други, намиращи се в уеб сайт, база данни или друго информационно пространство; както и компютърната система на организацията, ползващите я хора и цялостното хартиено информационно пространство на организацията. От особена важност е да се осигури лоялност, конфиденциалност и предпазливост от страна на служителите в организацията, по отношение на собствената ѝ информация. Това се отнася както към настоящите, така и към вече бившите служители. Тук биха могли да се предприемат адекватни законови или договорни мерки, гарантиращи съответната отговорност при увреждане на организацията. Една от тях е подсигуряването на "кибер-резерв" - допълнителен ресурс от експерти в областта на киберсигурността, защитата на информацията и информационните технологии с компетентности, свързани с осигуряване на защита и устойчивост на комуникационните и информационните системи.

На пето място, управление на инцидентите. Според легалната дефиниция на разглеждания закон, "Киберинцидент" е събитие или поредица от нежелани или неочаквани събития, свързани с киберсигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията. Подсигуряването на организацията чрез управление на инцидентите става чрез перманентен анализ на всички възможни (макар и рядко вероятни) нежелани или неочаквани събития, критични за сигурността на информацията на организацията. Добавянето на нови и нови хипотетични събития в аналитичния алгоритъм се налага от политическите, социални, икономически, финансови, институционални, юридически и персонални промени. Реакцията на който и да е инцидент трябва да е предвидена, ясно разписана и разиграна поне по един сценарий.

На шесто място, управлението на достъпите (физически и логически) включва не само всички входове, но и всички изходи на организацията. За да се идентифицират всички възможни такива е необходимо да се ползват и знанията и уменията на външни експерти, включително отговорът на такъв въпрос би могло да бъде бонус към критериите за интервю при постъпването в организацията. Стратегически и тактически погледнато, най-успешен пробив се прави на най-слабото място в която и да е система. По начало, в човешките организации най-слабото място се явява именно ***човешкият фактор***. Една перфектна система за киберсигурност, изградена преимуществено върху мрежовия си компо-

нент е абсолютно нелепа, ако не обръща също толкова внимание върху човешкия фактор, който е податлив на такива явления като корупция, мързел, безотговорност, предоверяване, немарливост, отмъстителност, ***функционална неграмотност*** и така нататък.

На седмо място, ***управление на измененията. Change Management Policy*** е необходимо еволюционно (а понякога и революционно) съществуване на модерните и преуспяващи организации. Променят се технологиите, променят се регулациите, променят се хората. Различни са изискванията, задълженията и отговорностите. Визията, мисията и стратегическите цели на организацията подлежат на постоянна ревизия. Всичко това рефлектира директно върху всеки един аспект на киберсигурността. Тук каквато и да е ***алиенация*** е вредна и не трябва да се толерира по никакъв начин.

На осмо място, управление на непрекъснатостта на дейността и/или услугите. Според законовата дефиниция, "Съществени услуги" са услуги, които имат съществено значение за поддържането на особено важни обществени и/или стопански дейности в един от следните сектори: енергетика, транспорт, банково дело, инфраструктура на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода или цифрова инфраструктура. От друга страна, "Цифрови услуги" са каквито и да са услуги на информационното общество, тоест, каквато и да е услуга, нормално предоставяна срещу възнаграждение, от разстояние, чрез електронно средство и по индивидуална молба на получателя на услугите. Непрекъснатостта означава ***времеви континуитет***, тоест – ***непрекъснатост в хронологичен план***. По друг начин казано – дори наличието на инцидент не би трябвало да прекрати дори за миг възможността да се търси или да се предоставя такава услуга.

На девето място, управление на взаимодействията с трети страни. Тук трябва да се имат предвид не само съконтрагентите по евентуалните търговски, облигационни, вещни или административни договори, но и всички категории клиенти, които са потребители на предоставяни от организацията услуги. Но не само – трябва да се идентифицират и подсигурят от гледна точка на киберсигурността и всички стажанти, външни експерти, вещи лица, преводачи и тълковници, които имат достъп до информация на организацията. Съвместни проекти с други организации, аутосорсване, извършване на каквито и да е действия по делегация също трябва да се отчитат и рисковете, свързани с тях, трябва да се калкулират внимателно и разумно. Управлението на взаимодействието с трети страни е един от категоричните тестове за интелигентността на организацията. А една ***конвергенция*** между взаимодействащи си субекти в областта на киберсигурността би била повече от печеливша.

На последно **десето място**, управление на натрупването на организационната памет. За вторично, третично и т.н. подсигуряване трябва да е ясно кой от служителите и/или кое звено биха могли да възстановят при съществен киберинцидент информация, алгоритми, работни процеси и т.н. Това означава, че важната за организация информация трябва да съществува поне в три информационни полета: хартиено, електронно и персонално (човешко). Образно казано – след потъването на Атлантида, важната за цивилизацията информация трябва да продължи да съществува, независимо дали на някакъв алгоритмичен или друг символен носител, дали в съзнанието и паметта на хората. А за това е нужна предвидливост, експертност, ерудираност и мнемоника. Последното качество се развива чрез специални техники за лесно запомняне на огромен обем информация чрез асоциативни способи. Именно тук е ролята на истинските експерти в организацията, които са създали, поддържат и развиват определена база данни. Затова те са безценни за организацията. Категорично трябва да се избягва концентрирането на информация само в едно лице. Омнипотентността е опасна както за киберсигурността, така и за модерните организации.

В допълнение

Във връзка с изискванията за киберсигурност с действащото законодателство на национално и европейско ниво, всяка уважаваща себе си организация от частния и от публичния сектор би трябвало да развива и по-високи стандарти от нормативно изискуемите в областта на киберсигурността. От една страна, това би могло да произтича от вътрешноведомствените актове, които въвеждат такива завишени изисквания съобразно принципите на предпазливост и предвидимост. От друга страна, това може да е следствие от многостранни и двустранни договори, по които организацията е страна.

Заключение

Управленската отговорност и ангажираността на одитните звена в организациите със съответствието на изискванията за киберсигурност може да се разглежда и като сегашна кибер-устойчивост и като подготовка за бъдеща киберотбрана. Последната представлява комплекс от мерки и способности за защита и активно противодействие на кибератаки и хибридни въздействия върху комуникационните и информационните системи и системите за управление на отбраната и въоръжените сили, както и върху системите за управление на страната при извънредно положение, военно положение или положение на война и върху стратегическите обекти, които са от значение за националната сигурност. Чрез тази концепция, киберсигурността на която и да е частна или публична организация под юрисдикцията на националната ни държава се превръща в неразделно звено от националната ни сигурност.

Именно интелигентният, системен и комплексен подход към проблематиката на киберсигурността има потенциал за успех. Като начало би трябвало да се положат сериозни усилия за повишаване на личната почтеност и професионална етика на ръководството и персонала на организацията, както и за качествени и перманентни обучения на персонала на организацията по всички аспекти на киберсигурността.