IT4Sec Reports 117
http://dx.doi.org/10.11610/it4sec.0117

Нива за обучение на персонала по проблемите на киберсигурността

Венелин Георгиев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, март 2015 г.

Венелин Георгиев, Нива за обучение на персонала по проблемите на киберсигурността**,** *IT4Sec Reports* 117 (София, Институт по информационни и комуникационни технологии, март 2015 г.), http://dx.doi.org/10.11610/it4sec.0117.

IT4SecReports 117 „Нива за обучение на персонала по проблемите на киберсигурността“ Стремежът на хората и организациите към постигане на желано ниво на киберсигурност може да бъде подчинен на прилагането на различни стратегии. В практиката са познати варианти, при които постигането на киберсигурност се основава на създаване на ефективни законодателни системи, иновативни технически решения, рационални организационни структури и т.н. В центъра на вниманието когато се говори по проблемите на киберсигурността остават хората и възможностите за тяхното обучение, с което да бъде снижена уязвимостта от кибератаки. Залагайки на подобна стратегия за изграждане на киберсигурност, важно е правилно да се разбира, че обучението на персонала по проблемите на киберсигурността може да бъде конструирано в няколко нива. Всяко от тези нива притежава специфични характеристики като подход и като използвани методи за обучение, а като следствие от това се свързва с различни резултати по отношение на постигнатата киберсигурност.

IT4Sec Reports 117 „Levels of Cybersecurity Training and Education“ The ambition of individuals and their organizations to achieve a desired level of cybersecurity may be subject to the application of different strategies. Known approaches to achieving cybersecurity involve the establishment of effective legal systems, innovative technical solutions, rational organizational structures, etc. The focus in discussions of cybersecurity remains on people and their training, which can lower the vulnerability to cyber attacks. Counting on such a strategy to build cybersecurity, it is important to properly understand that cybersecurity training can be constructed at several levels. Each of these levels has specific characteristics, such as the approach and methods used for training, and as a consequence is associated with different results in terms of the cybersecurity achieved.

ISSN 1314-5614

СЪДЪРЖАНИЕ

ВЪВЕДЕНИЕ

По отношение на термина „киберсигурност“ съществуват различни разбирания както в областта на неговата структура, така и в областта на неговата функционалност. В наши дни киберсигурността се превръща в модерна дума, която плаши със своята неопределеност, доколкото зад нея могат да стоят неограничен брой въпроси и проблеми на сигурността, започващи от техническата област, преминаващи през областта на поведението на хората и завършващи до областта на законодателството. Като цяло може да се каже, че понятието киберсигурност включва в себе си множество въпроси и едновременно с това множество отговори от техническо и нетехническо естество.

При всички положения сериозните дискусии в областта на киберсигурността изискват на първо място въвеждане и използване на единна дефиниция, която да осигури ако не общо, то поне сходно разбиране на проблемите на киберсигурността. Международната организация за стандартизиране дефинира киберсигурността като запазване на конфиденциалността, интегритета и достъпността на информацията в киберпространството. Киберсигурността се дефинира от някои автори и като съвкупност от политики, средства, концепции, ръководства, действия, обучение, добри практики и технологии, които могат да се използват за защита на киберпространството, организациите и потребителите. За киберсигурността може да се срещне определение, според което тя включва в себе си проблемите на сигурността, свързани с Интернет и други компютърни системи и мрежи, а също така и техническите и нетехническите способи за решаване на тези проблеми.

Независимо от това как точно е дефинирана киберсигурността, без съмнение остава нуждата от изучаване и отчитане на заплахите и рисковете за този специфичен тип сигурност, както и създаване и прилагане на подходящи стратегии за противодействие срещу тези заплахи и рискове, с което да се гарантира желано ниво на киберсигурност.

Една от възможните стратегии за противодействие на рисковете за киберсигурността е обучението на потребителите, с което да се намалят шансовете за успех на кибератаките благодарение на високото ниво на знание и подготвеност на персонала. В зависимост от целите и методите на едно подобно обучение същото може да бъде структурирано в три нива – обучение на базата на информираност, обучение на базата на изграждане на подходяща организационна култура и обучение на базата на управление на поведението на персонала.

Обучението на базата на информираност се основава на необходимостта потребителите да бъдат запознати със съдържанието и изискванията на политиката и програмата за киберсигурност на организацията. От този тип обучение се очаква, че подобна информираност ще бъде достатъчна за персонала да превърне изискванията за киберсигурност в свое разбиране, което да спазват в процеса на работа. Предимствата на обучението на базата на информираност са неговата опростеност и липсата на специални изисквания към трансфериране на необходимите знания в посока към потребителите. Най-просто казано, прочитането на съдържанието на документите, каквито са политиката или програмата за информационна сигурност, пред персонала на организацията се приема като достатъчно условие за това, че всички правилно са разбрали и възприели какво се очаква от тях по въпроса за спазване на правилата за киберсигурност. Неудобството в случая идва от риска, който се поражда предвид несигурността всички служители наистина правилно да са възприели поднесената им информация и да са я превърнали в свое знание и модел за практическо поведение. Прилагането на обучение, базирано на информираност на персонала налага въвеждане на строг и непрекъснат контрол по отношение на спазването на устано-

вените правила за киберсигурност от страна на персонала, което като следствие поражда недоволство от страна на служителите и оскъпява дейността на организацията.

Преминаването към второ ниво на обучение на персонала, което се базира на изграждане на подходяща организационна култура, изисква на първо място правилно разбиране на това какво представлява организационната култура и как същата може да бъде използвана за постигане на целите на киберсигурността.

ДЕФИНИРАНЕ НА ПОНЯТИЕТО ОРГАНИЗАЦИОННА КУЛТУРА

Какво представлява организационната култура? Какво точно се има предвид под това общо и широкообхватно понятие? Защо е толкова важно организационната култура да бъде разбирана и управлявана? Това са част от въпросите, но които учени, изследователи и практици се опитват да намерят подходящи отговори.

Даването на отговори на изброените въпроси (и на редица свързани с тях) ще остави без съмнение факта, че организационната култура е от съществено значение за всички, които имат отношение към киберсигурността: професионалисти, ръководители, служители, партньори, потребители и т.н. Постигането на значително подобрение по отношение на киберсигурността в поведението на изброените категории от състава на човешкия фактор се нуждае от разбирането и способността да се повлиява върху организационната култура. В по-конкретен смисъл, без съмнение, е необходимостта от разработване и въвеждане на подходяща организационна култура по въпросите на киберсигурността.

Какво всъщност означава „подходяща организационна култура за киберсигурност“? От една страна това може да се разбира като поддържане на състояние на страх и параноя у служителите във фирмата или членовете на организацията, но от друга страна подходящата организационна култура за киберсигурност може да се базира на взаимното доверие и спазване на установените правила. На практика посочените два подхода могат да бъдат прилагани поотделно и в съвкупност при търсене на решение за създаване на подходяща организационна култура за киберсигурност. Страхът може да бъде работещо средство при определени условия и отделни възникнали ситуации, докато стратегиите, базирани на обучението и доверието биха работили при всички условия и по един по-добър начин.

Въпросът какво точно представлява организационната култура е вълнувал множество автори в различни аспекти и съдържание и по различно време. По някои аспекти на организационната култура авторите достигат до единодушие. Като примери за подобни аспекти могат да бъдат посочени следните:

- организационната култура оказва изненадващо мощно влияние върху възприятията, поведението и отношението на персонала;
- организационната култура не е понятие, което лесно може да бъде еднозначно дефинирано, нито пък понятие със статични (непроменливи, постоянни) значения и характеристики;
- организационната култура представлява по-скоро развиващ се феномен. Не всеки успява в един по-кратък срок да я възприеме, да я оцени и да се асоциира (приспособи, приеме) към нея;
- в съдържанието на организационната култура непрекъснато възникват нови и нови аспекти, а съществуващите претърпяват развитие. Често пъти тези аспекти се комбинират по най-непредвидими начини, създавайки разнообразие от влияние върху различни групи от персонала.

Една от причините за промените в организационната култура е преструктурирането и промените в персонала, които от своя страна водят до промени в отношението и опита на организацията. Глобализацията също оказва влияние върху организационната култура и нейното развитие. Преди време всяка страна или организация (фирма, корпорация) е изграждала собствен стил на бизнес операциите и собствен различен стил на работа дори в рамките на една международна организация. Централизирането на операциите, поддържани с помощта на компютърни мрежи, става предпоставка за създаване на глобални бизнес линии, а като резултат и въвеждане на значими промени в отношението към бизнеса и при взаимоотношенията между различните групи на човешкия фактор.

Един нов фактор, който участва във формирането на съвременните организации и тяхната организационна култура е нарастващото влияние на външните връзки на персонала с помощта на Интернет, социалните мрежи и т.н. Това осигурява нова перспектива пред човешкото мислене и едновременно с това замества вътрешните (локалните) контакти с най-близките колеги от фирмата. Направено изследване показва, че днес хората прекарват по-малко време в контакт със свои колеги, отколкото в контакт с колеги, намиращи се далеч извън офиса. Самият офис става все по-анонимен. При търсене на отговори на възникващи въпроси по-често служителите се обръщат към външни източници и по-рядко разчитат на дебати с колегите от офиса.

Като правило не се очаква даден вариант на организационна култура да оказва доминиращо влияние върху персонала в един дългосрочен период. Но в същото време същият този вариант на организационна култура може да остане достатъчно дълго съществен фактор, който създава (или блокира) възможности за успешното изпълнение на изискванията на една програма за киберсигурност.

В литературата могат да бъдат открити множество различни описания, с които се прави опит да се обясни какво представлява организационната култура. Всяко от тези описания представя различни гледни точки. Ако на преден план се постави съдържанието на организационната култура същата може да бъде определена като съвкупност от отношение, ценности, убеждения, норми и обичаи в организацията. Това определение без съмнение разкрива обхвата на понятието, но в същото време казва съвсем малко или нищо за това как изглежда организационната култура.

Друг начин, по който може да се погледне към понятието организационна култура е като се помисли с термините на нейния произход и нейното развитие. В този случай определението може да гласи, че организационната култура е резултат от общуването и преговорите между членовете на организацията. Друго определение за организационната култура в същия дух гласи, че тя представлява модел от базови допускания, които са доказали своята работоспособност и по тази причина същите са възприети като валидни.

Като пример за едно по-обобщено определение за термина организационна култура може да бъде дадено следното: организационната култура се изразява в това какво правят хората (персонала, служителите) в случаите, когато те не са следени (контролирани). Това определение отразява поведението на хората при отсъствие на институционален (фирмен) контрол върху тях и по-специално върху тяхната дейност. В този случай организационната култура се фокусира върху естественото и осъзнатото поведение, което от своя страна се определя, изгражда и развива под влияние на фактори на средата, инстинктите на човека и специфичните особености на извършваната дейност. В смисъла на даденото определение организационната култура изразява действията и поведението на хората в случай на премахване на управленския контрол и при условие на пълно доверие и трансфериране на правомощия.

СЪДЪРЖАНИЕ НА ОРГАНИЗАЦИОННАТА КУЛТУРА ЗА КИБЕРСИГУРНОСТ

Вниманието на множество изследователи и практици продължава да бъде привличано от проблемите, свързани с изучаването на поведението на човешкия фактор в полето на киберсигурността. Резултатите от проведено изследване показват[1], че голяма част от служителите в организациите гледат на отговорностите по отношение на киберсигурността повече като задължение на специалистите, работещи в тази област и по-малко като собствено задължение. Резултатите от проучването също така показват, че основната част от инцидентите с киберсигурността са свързани с несъобразяване с изискванията и малка част с провали на техническите системи. Като обобщение в изследването се отбелязва, че киберсигурността в организациите е застрашена в по-голяма степен от случайни или умишлени действия на своите служители независимо от наличието на политика и програма за киберсигурност, респективно на обучение на базата на информираност. Посочват се две възможни решения за справяне с това положение и за постигане на желаното ниво на киберсигурност:

- прилагане на система от мерки за стриктен контрол и евентуални санкции в случаи на констатирани нарушения. По този начин се очаква постигане на по-бързи резултати, но едновременно с това се очаква посрещане на новите мерки с неодобрение от страна на персонала. Постигнатите резултати могат да се окажат краткотрайни и при всички условия ще нараснат разходите (на различни ресурси) за гарантиране на киберсигурността.
- изграждане на високо ниво на организационна култура за киберсигурност, което да гарантира дълготрайни резултати при по-ниски разходи.

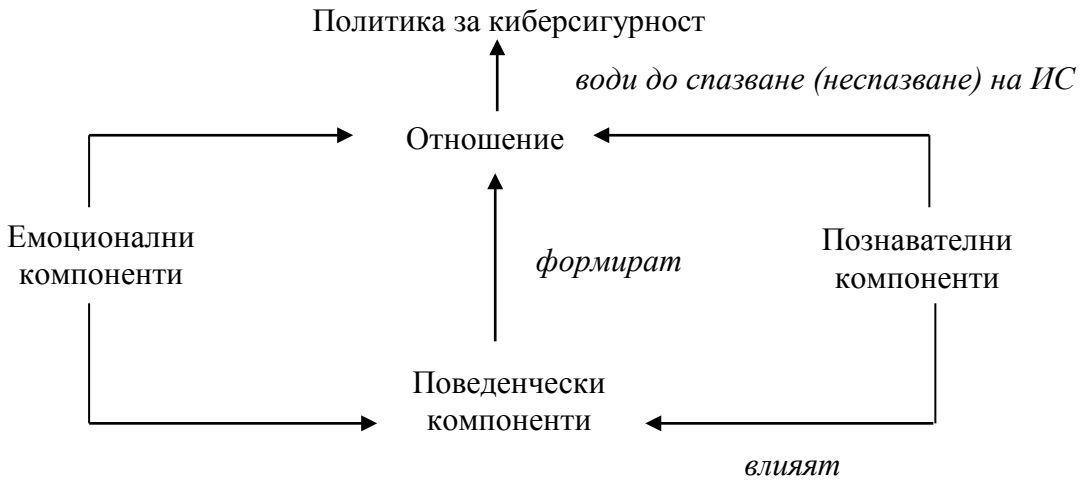
Организационната култура за киберсигурност включва стандарти за поведение и поведенчески модели, изградени и утвърдени в рамките на организацията. Първата стъпка към изграждане на организационна култура за киберсигурност е наличието на позитивно отношение от страна на персонала към целите и изискванията на киберсигурността и осъзнаване на нейната роля в цялостния процес на просперииране на организацията. От тук възниква въпросът какво означава правилно отношение към киберсигурността. По дефиниция отношението е израз на принадлежността на индивидуалностите към даден курс или начин на действие в определена обстановка или ситуация. Свързвайки всичко това с киберсигурността, за отношението към нея може да се каже, че е позитивно в случай на съобразяване с установените изисквания или негативно в обратния случай. Отношението може да бъде представено като съвкупност от емоционални, познавателни и поведенчески компоненти [2] (виж фиг. 1).

Емоционалните компоненти обикновено се отнасят до някое събитие или определен човек в рамките на организацията. Те се свързват с начина, по който хората оценяват обектите и събитията около себе си и изграждат съответен образ за тях. Този образ може да бъде използван при изграждане на подходяща организационна култура на киберсигурност. Като пример, осъзнаването на важността на опазването на чувствителната информация за организацията представлява емоционален компонент на отношението към киберсигурността. Друг подобен пример показва, че самият акт на пушене не е толкова интересен за младите хора, а по-скоро интерес предизвикват хората, които пушат и на които младите

[1] Alfawas S. M., Information Security Management: a case study of an information security culture, (Queensland University of technology, 2011).

[2] Майерс Д., *Социалная психология*, 1997

хора се стремят да подражават. Ако се изберат подходящите лица от персонала на фирмата, които да изразяват (с които да се свързват) изискванията за киберсигурност, то може да се очаква, че по силата на подражанието останалият персонал също ще се стреми към спазване тези изисквания. Познавателните компоненти отразяват знанието за някои обекти, към които се формира отношение. Резултатното отношение зависи от точността и коректността на притежаваното знание от страна на изграждащия отношението. Познавателните компоненти нямат подчертан емоционален характер, за разлика от емоционалните. Това на практика означава, че те могат да бъдат променяни по пътя на рационалните доказателства. Като пример, обучението по киберсигурност може да доведе до повишаване на подготвеността и компетентността на персонала, което от своя страна е предпоставка за снижаване на броя на инцидентите, свързани с киберсигурността и предизвикани от липсата на достатъчно знания. Поведенческите компоненти дефинират поведението на хората и техните действия по определен начин и при определени условия. Като пример, негативният опит, извлечен от участие на лице в инцидент, свързан с киберсигурността, може да накара това лице да осъзнае по-добре важността на същата тази киберсигурност. В тези условия се придобива и ново знание, което увеличава подготвеността на персонала за изпълнение на неговите задължения по един по-сигурен начин.



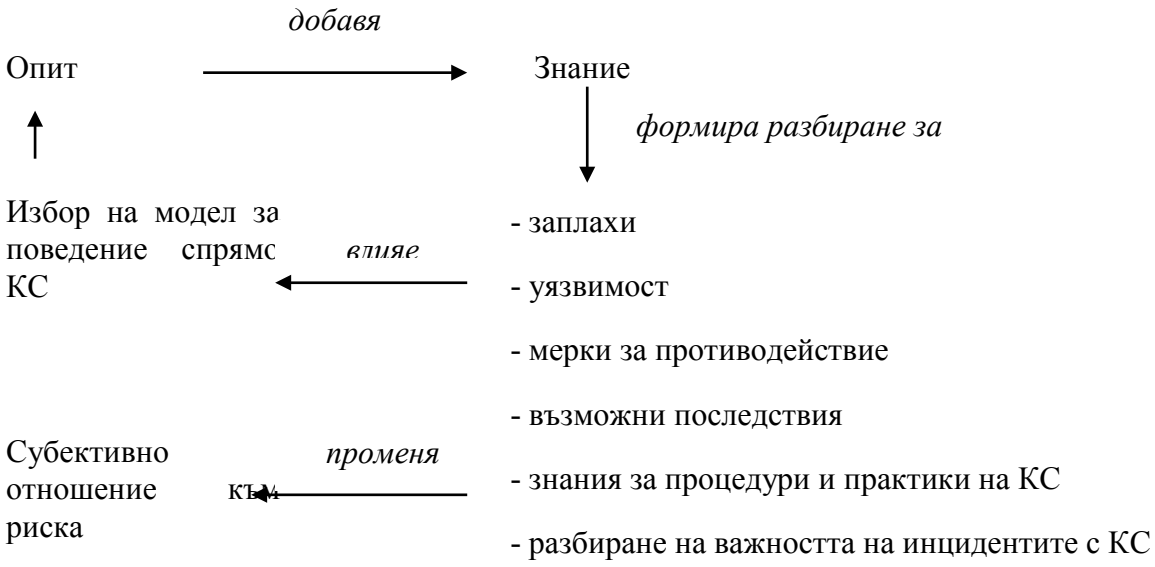
Фиг. 1. Компоненти на отношението към киберсигурност

ИЗГРАЖДАНЕ НА ОРГАНИЗАЦИОННА КУЛТУРА ЗА КИБЕРСИГУРНОСТ

Ако се приеме, че всеки служител в организацията притежава определени ценности, убеждения и модели за поведение, то може да се каже, че във всяка организация съществува някакво ниво на организационна култура за киберсигурност, т.е. не съществува нулево ниво на организационна култура за киберсигурност. Този факт на практика не означава, че във всяка организация съществува и се поддържа необходимото или изискващото се ниво на организационна култура за киберсигурност. Така възниква задачата за намиране на начини за изграждане на желано ниво на киберсигурност в организацията.

Доказано е, че между знанието на персонала и избора на поведенчески модели по отношение на киберсигурността съществува връзка, която схематично е представена на фигура 2. Разглеждани поотделно нито знанието, нито избрания поведенчески модел не

могат да гарантират високо ниво на организационна култура за киберсигурност. Дори при значителни знания от страна на персонала няма гаранция за това, че същият ще изпълнява задълженията си по един действително сигурен начин. От друга страна изглежда нереалистично да се смята, че изграждането на желаното ниво на организационна култура за киберсигурност е възможно единствено чрез задаване на модели за поведение на служителите.

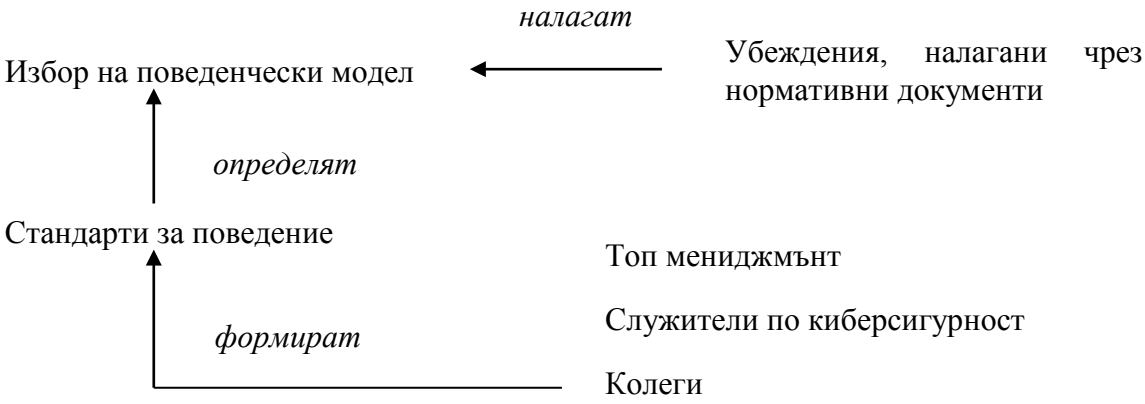


Фиг. 2. Връзка между знанието и изборът на модел за поведение спрямо КС

Както се вижда от фигура 2, от служителите се очаква на базата на своите знания да имат правилно разбиране за заплахите, уязвимостите, мерките за противодействие и очакваните последици от инциденти с киберсигурността. Тези знания помагат на служителите при избора на модел за поведение. Служителите също така имат знания за същността и приложението на процедурите и практиките на киберсигурността, както и за възможните инциденти при тяхното пренебрегване. Всичко това им помага да изградят правилно отношение към асоциирания към киберсигурността риск. Знанията на служителите могат да бъдат развивани чрез подходящо обучение или по пътя на практиката чрез натрупване на опит.

По-доброто разбиране на същността и значението на киберсигурността подпомага служителите при избор от тяхна страна на поведенчески модел при изпълнение на служебните задължения. На същия този избор влияние оказват и други фактори, сред които могат да се отбележат убежденията, налагани отвън чрез нормативните документи и изградените стандарти за поведение (фиг. 3).

Новоназначените служители в организацията в периода на адаптиране се ръководят при избора на поведенчески модел от приетите стандарти за поведение. По този начин тяхното поведение се регулира от изградената организационна култура. В същото време следва да се отбележи следния парадокс: организационната култура за киберсигурност от една страна регулира поведението на служителите, а от друга се явява резултат от тяхната дейност.

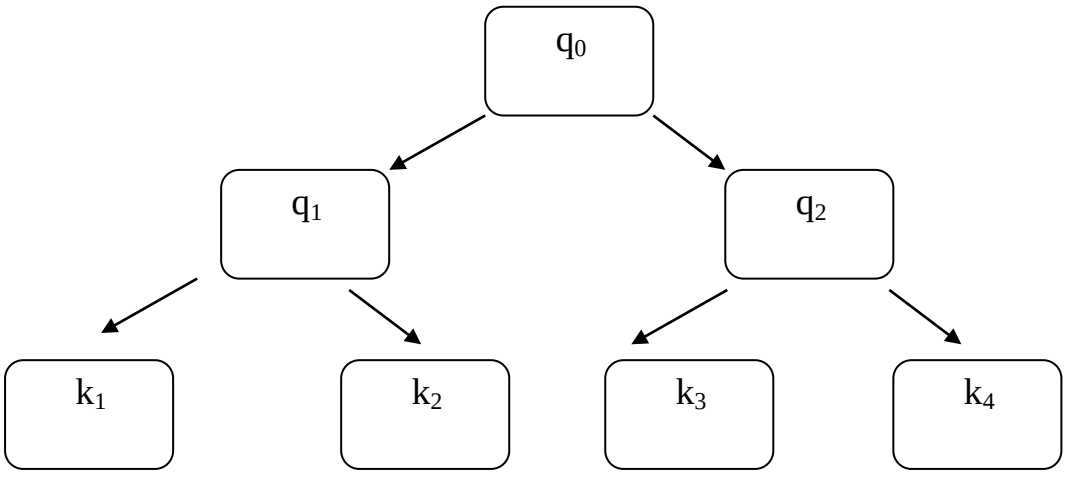


Фиг. 3. Фактори, влияещи върху избора на поведенчески модели

МЕТОД ЗА КОМПЛЕКСНО ОЦЕНЯВАНЕ НА ОРГАНИЗАЦИОННАТА КУЛТУРА ЗА КИБЕРСИГУРНОСТ

Възможен подход при оценяване на нивото на организационна култура за киберсигурност е прилагането на метод за комплексно оценяване, при който няколко параметри (показателя) се интегрират в един общ, с помощта на който се описва състоянието на системата за киберсигурност. Ако за такъв общ параметър се избере нивото на организационна култура за киберсигурност, то той може да бъде дефиниран и измерен с помощта на два отделни индикатори, каквито са „възприемане" и „дисциплинираност". От своя страна критерият „възприемане" се описва с помощта на два параметъра „обхват" и „дълбочина", а критерият „дисциплинираност" се описва с помощта на „стабилност" и „контролопригодност".

На фигура 4 е представено дървото на целите, което се използва при прилагане на подобни методи за комплексно оценяване. Параметърът q0 се определя като функция на двата параметъра q1 и q2 от по-ниското йерархическо ниво. От своя страна параметрите q1 и q2 се изразяват като функции съответно на параметрите k1, k2 и k3, k4.



Фиг. 4. Дърво на целите

В случай, че общите параметри от фигура 4 бъдат заменени с избраните параметри за описание на нивото на организационна култура за киберсигурност, то ще се получи резултат, показан на фигура 5. При така възприетите означения нивото на култура за информационна сигурност може да бъде описано с помощта на функцията от вида:

$$q0 = f(q1,q2) = \varphi1[(\varphi2(k1, k2)\ \varphi3(k3, k4))] \qquad (1)$$

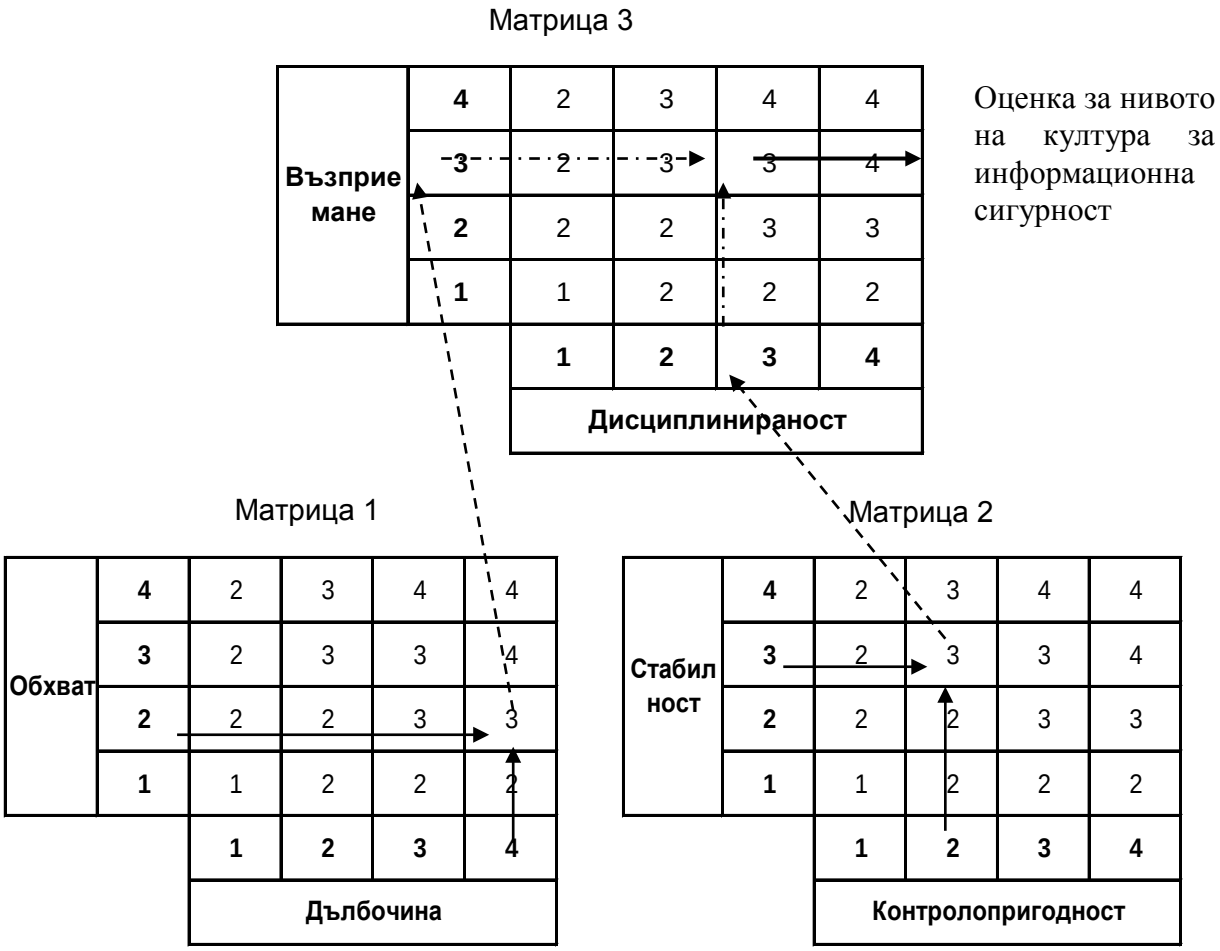
Фиг. 5. Дърво на целите за определяне на нивото на организационна култура за киберсигурност

Технологията за практическото използване на функция (1) за определяне на нивото на организационна култура за киберсигурност включва следните стъпки:

- използване на скала с четири нива за оценка на параметрите от дървото на целите: 1 – ниско, 2 – средно, 3 – високо, 4 – отлично.
- с помощта на матрици 1 и 2 и при зададени стойности на показателите от най-ниското ниво на дървото на целите се определят стойностите на показателите от второто ниво на дървото (виж фиг. 6)
- на базата на така определените стойности се преминава към матрица 3, от която се определя стойността на нивото на организационна култура за киберсигурност.

Предимство на описания метод за определяне на оценката за нивото на организационна култура за киберсигурност е неговата опростеност, което предполага по-лесно използване в практиката. Като недостатък може да се приеме необходимостта от предварително определяне на стойностите на параметрите от най-ниското ниво на дървото на целите, както и съдържанието на клетките на използваните матрици.

Проблемът с измерване и повишаване на нивото на организационна култура за киберсигурност все повече се възприема като един от съществените за осигуряване на желаната киберсигурност като цяло. Важността на този въпрос налага изисквания към управлението на процеса по повишаване на организационната културата на персонала с помощта на общоприети подходи и методи, което да се превърне в елемент от повишаване на киберсигурността на организацията.



Фиг. 6. Матричен метод за определяне на оценката за нивото на култура за информационна сигурност

ОБУЧЕНИЕ ЗА КИБЕРСИГУРНОСТ НА БАЗАТА НА УПРАВЛЕНИЕ НА ПОВЕДЕНИЕТО НА ПЕРСОНАЛА

Третото ниво на обучението на персонала в областта на изискванията за кибер-сигурност си поставя амбициозната задача да постигне резултати на базата на оказване на влияние върху поведение на същия този персонал. За целите на такъв тип обучение се използват подходящи методи, сред които са т.нар. баланс на последствията и атрибутив-ната теория.

"Балансът на последствията" е техника, разработена през 70-те години на миналия век от поведенческите психолози. Идеята е да се идентифицират всички потенциални благоприятни и неблагоприятни фактори, които могат да действат за или против пости-гането на желаното поведение. Този тип анализ не само помага да се разбере защо хората не се държат по начина, по който бихме искали, но също така да се определят условията, които трябва да се създадат, променят или премахнат за да се насърчи желаното пове-дение. Предположението е, че за да се промени поведението на хората, вниманието трябва да се съсредоточи върху осезаемите последици от техните действия, към осезаемите

резултати, които се очакват от поведението, а не върху нещата, които го активират, като политики, правила и команди.

Последиците, които са най-силните мотиватори са тези, които са лични, незабавни и сигурни. Мотиваторите ще трябва да бъдат определени по някакъв начин. Отправната точка в случая е да се определи желаното поведение, което следва да се насърчава, както и поведението, което е необходимо да се премахне. Така например, в областта на кибер-сигурността може да се избере "осигуряване сигурността на компютъра" като желано поведение и "загуба или кражба на компютъра" като поведение, което трябва да бъде отстранено.

Следващата стъпка е да се изготвят списъци, както е показано на фигура 7. Тези списъци представляват четирите набора от последици, които работят за или против както за желаното така и за нежеланото поведение. При изготвянето на тези списъци може да се появи неизбежно дублиране, но това няма да навреди на прилагането на метода. На този етап доброто въображение на изследователя е критичен фактор за успеха. В действи-телност, изследването е най-добре да бъде изпълнено като групова "мозъчна атака".

ПОСЛЕДСТВИЯ, НАСЪРЧАВАЩИ ЖЕЛАНОТО ПОВЕДЕНИЕ	**ПОСЛЕДСТВИЯ, ДЕЙСТВАЩИ ПРОТИВ ЖЕЛАНОТО ПОВЕДЕНИЕ**
Списък на факторите, които да бъдат подкрепени	**Списък на факторите, които да бъдат премахнати**
ПОСЛЕДСТВИЯ, ДЕЙСТВАЩИ ПРОТИВ НЕЖЕЛАНОТО ПОВЕДЕНИЕ	**ПОСЛЕДСТВИЯ, НАСЪРЧАВАЩИ НЕЖЕЛАНОТО ПОВЕДЕНИЕ**
Списък на факторите, които да бъдат подкрепени	**Списък на факторите, които да бъдат премахнати**

Фиг. 7. Баланс на последствията

Нека разгледаме факторите, които може да се идентифицират. Като се има предвид желаното поведение - "осигуряване сигурността на компютъра", може да се идентифицират следните последици, които насърчават желаното поведение: “това запазва данните на компанията“, или "това осигурява наличност на данните“. Последната последица е мощен стимул, тъй като действа лично, незабавно и сигурно.

След това могат да се добавят допълнителни фактори, за да се засили мотивацията за това поведение, като: "възнаграждение за осигуряване на сигурността на компютъра". Това е силен личен, незабавен и сигурен фактор, въпреки че изисква известно творческо мислене, за да се определи подходяща мярка и подходяща награда.

Относно факторите, които възпират желаното поведение на "осигуряване сигурността на компютъра“, може да се идентифицират последици като "спестено време, ако не се вземат предпазните мерки за сигурност". Това е също много личен, незабавен и сигурен фактор, а също и много мощен фактор. Но това не подобрява поведението, което искаме, така че трябва да се стремим да се елиминира или сведе до минимум влиянието на този фактор, например чрез въвеждане на автоматизация или по-добър дизайн на функциите за киберсигурност.

Сега да обърнем внимание на факторите, които могат да насърчат присъствието на нежелано поведение при "загуба или кражба на компютъра". Бихме могли да идентифицираме последствия като "получавам като заместител най-новия, последен модел". Това със сигурност е истински мотиватор за загуба или повреда на по-малки елементи на оборудването.

И накрая, факторите, които могат да разубедят персонала от загуба на техния лаптоп. В действителност има доста малко. Те могат да включват последствия като "неспособност за работа" или "загуба на лични данни" или "неприятностите при замяната", всички от които са много силни фактори. Може също да се добави "загуба на данни на предприятието", но това не е много силен фактор, освен ако не се въведе още един фактор "дисциплинарни мерки", който е много силен фактор когато е справедливо и последователно прилаган.

Какви са изводите от това упражнение? И как то може да промени съществуващото мислене? Ако преди това избраната политика е била за изпращане на неефективни съобщения като: "Грижете се за вашия лаптоп, защото това е ценен актив и неговата загуба може да причини сериозно увреждане на дългосрочните интереси на организацията", то тя не би представлявала силен фактор и следователно не би постигнала абсолютно никакъв ефект. След упражнението, посланията към служителите могат да включват следните, помощни и ориентирани съобщения: "Ако загубите вашия лаптоп, вие не ще бъдете в състояние да работите и ще загубите вашите лични данни" ; "Това ще създаде за вас неприятности при смяната на загубения лаптоп" "Вие ще навредите на колегите си“. „Може да загубите премиите си и ще бъдете изправени пред дисциплинарни наказания." Може също така да се съобщи, че ще се въведат нови системи, които ще премахнат или ще намалят времето, което е необходимо, за да се прилагат предпазните мерки за киберсигурност.

Всички тези съобщения ще послужат за насърчаване на правилното поведение и за премахване на лошото поведение. Този тип упражнение може да доведе до известни малки затруднения, но това е естеството на ефективната промяна в поведението. Всичко се свежда до внимателен анализ на проблемните области, идентифициране на идеи, последвано от корекции и до набор от фактори, които биха изглеждали маловажни за по-малко просветените наблюдатели.

СИЛАТА НА АТРИБУЦИЯТА

Явлението да се рационализира дадено поведение и да се оправдават собствените действия като се обвинява някой друг за тях се изучава от т.нар. "атрибутивна теория", прилагана в кръговете на социалната психология, която се занимава с начина, по който хората приписват причини за действия или събития.

Такива атрибуции се правят не само по отношение на други хора, обекти или събития. Понякога вината или по-вероятно похвалата е насочена към самия себе си. Например, ако рибар улови голяма риба, той би твърдял, че това е умение, а не късмет.

Когато хората правят атрибуции за своите действия, те също коригират своите нагласи и вярвания за себе си. Това е възможност за промяна в поведението. Ако успеем да убедим хората да приемат, че техните действия са пряко отговорни за добрия резултат, който желаем, ние всъщност може да ги насърчим да поддържат поведението, което осигурява този резултат. Не е от голямо значение дали хората действително имат нещо общо с това, колкото дали има надеждна връзка, която те приемат. Например, може да се

каже на служителите, че огнището на компютърен вирус е погасено заради доброто поведение, изразяващо се в неотваряне на прикачени файлове в спам пощата. Това ще има по-голямо въздействие, отколкото ако им се дават съвети да не се отварят прикачените файлове, тъй като ще се подчертае пряката връзка между тяхното поведение и нивото на вирусни епидемии в компанията. Хората са по-склонни да полагат усилия в нещо, ако те смятат, че е вероятно да се получи резултат. Атрибутивната теория показва, че хората са по-склонни да смятат, че изходът е резултат на техните действия, а не само на обстоятелствата по това време.

Прилагането на такива интервенции ще работи най-добре, когато хората действително мислят за това, което причинява въпросното събитие. За създаването на такъв климат би спомогнало да се подходи чрез задаване на въпроси за мнението на хората от типа "Какви са според теб причините за неотдавнашния спад на вирусни епидемии?", след което да се предложи: "Отговорът сте вие и вашето разумно поведение".

Насърчаване на служителите да развиват атрибуции към собственото си поведение за желаните резултати може да бъде много по-ефективен метод от прилагане на външен контрол, като надзор или мониторинг. Ако хората смятат, че някой друг ще спре нещо да се случи, те ще имат по-малко отговорен подход. Това в никакъв случай не е ограничаване на външните фактори, като наблюдение или специални награди и наказания. Те трябва да се прилагат непрекъснато, за да бъдат ефективни. За разлика от тях, няколко уместни предложения към персонала може да помогнат за изграждане на вътрешните мотиватори, които да насърчават правилното поведение по отношение на киберсигурността.

ЗАКЛЮЧЕНИЕ

Необходимостта от обучение на персонала по въпросите на киберсигурността остава неоспорим факт. В тази връзка наличието на различни нива на обучение и свързани с тях обучителни подходи и методи само може да стимулира креативността на обучителите. Описаните нива за обучение на персонала по проблемите на киберсигурността не се разглеждат в тяхното противопоставяне като по-добри или по-лоши. С тях просто се разкриват алтернативни възможности, сред които изборът се базира на фактори като ниво на амбиция при изграждане на състояние на киберсигурност, способности на лицата, планиращи и провеждащи обучението, апетит към рисковете за киберсигурността на организацията и т.н.