Експерт по киберсигурност – 0% безработица, бързо израстване и висока заплата

Как се обучават младите експерти в сферата, какви умения трябва да притежават, кои са предизвикателствата, с които се сблъскват

——— Мария Динкова

shutterstock

С РАЗВИТИЕТО НА ТЕХНОЛОГИИТЕ дигиталното пространство заема все по-голяма част от нашия живот, а с него се увеличава и значението на киберсигурността. Затова в днешно време на компаниите се налага да инвестират сериозни парични суми, за да гарантират защитата на своята информация и да се предпазват от злонамерени действия. По данни на Gartner само след две години глобалните разходи за киберсигурност се очаква да достигнат 133.7 млрд. долара. В същото време обаче загубите от пробиви ще продължават да се увеличават, като според IBM средно това ще струва на компаниите 3.9 млн. долара.

На този фон организациите все повече усещат нуждата от добре подготвени специалисти по киберсигурност, които да внедрят правилните решения, да наложат точните политики и да реагират бързо и адекватно в кризисни ситуации. До 2021 100% от големите компании вече ще имат директор по информационната сигурност, но се прогнозира, че фирмите ще продължат да усещат силен недостиг на квалифицирани кадри, а незаетите позиции в сферата ще бъдат около 3.5 млн., посочват от Cybersecurity Ventures. В тази връзка обучението по киберсигурност ще бъде както широко търсено от бизнеса, така ще се превърне и в добра възможност за развитие на младите експерти.

Какви обаче са изискванията към бъдещите кадри в областта? Какви умения и знания те трябва да притежават, за да бъдат успешни? Кои са предизвикателствата и често допусканите грешки по пътя на кариерното развитие? На тези и още много други въпроси отговаря доцент Галина Момчева, която е председател на управителния съвет на ИКТ „Клъстер Варна", а също така е ръководител на катедра "Информатика" и на магистърската програма „Киберсигурност" във Варненския свободен университет (ВСУ).

Компютърни науки или киберсигурност?

Изборът на специалност за висше образование е един от най-важните въпроси пред младите хора, но същевременно е и един от най-трудните. За онези с изявен интерес към информационните технологии вероятно очакваната нулева безработица в сферата на киберсигурността е изключително изкушаваща възможност. Момчева обаче съветва да не се бърза с тясната специализация, колкото и обещаваща да изглежда ситуацията в момента.

„Много ученици избират специалност, която им се иска да работят. Например търсят конкретен профил на бакалавърска програма в много тясна специализация. Аз и колегите ми обаче смятаме, че това не е най-правилното решение, тъй като по отношение на динамиката на развитието на процесите човек трябва да е готов за повече неща и за повече длъжности. В тази връзка не бива да отиваш първи курс с нагласата, че точно разработчик на игри или специалист по киберсигурност ще бъдеш. С каквото и конкретно да се занимаваш впоследствие, ще имаш нужда от базисни познания по всички основни дисциплини", отбелязва Момчева.

В тази връзка тя и нейните колеги препоръчват да се избират специалности като компютърните науки, които предлагат широк спектър от избираеми и факултативни дисциплини. Впоследствие в магистърските програми студентите могат да постигнат вече по-тясна специализация, включително в полето на киберсигурността. По този начин с една добра основа младите експерти ще могат много по-лесно да се приспособяват в бъдеще към промените в динамичния ИТ пазар.

Кандидатстването

След като бъде взето решение и е направен изборът за специалност, идва моментът на кандидатстването. Поради регулациите у нас в повечето университети това се случва чрез конкурсен изпит. По думите на Момчева обаче по отношение на киберсигурността е особено важно да се провеждат и интервюта с бъдещите студенти, за да се определи дали те наистина са подходящи за специалността и дали ще се справят с нея. За тази цел експертът от ВСУ съветва хората – особено тези, които нямат предишно ИТ образование – да преминат неформален курс например по програмиране, за да разберат дали материята им е интересна и им се удава.

Важно е обаче да се отбележи, че в сферата на киберсигурността не работят само експертите, завършили това направление. Специалистите в науката за данните също могат да се реализират в областта, като те ще бъдат фокусирани повече върху самия анализ на данните. „В тази връзка слагането на клишета какво е името на специалността и какво работиш не е особено точно", изтъква Момчева.

Уменията и знанията

Обучението по киберсигурност обикновено е с продължителност два или три семестъра, като в него се залагат традиционни курсове за специалността като „Сигурност на данните", „Мрежова сигурност", „Криптография", „Разпределени изчисления и сигурност" и други. Момчева подчертава, че освен върху тези типични дисциплини е важно да се наблегне и върху човешкия аспект, включвайки предмети като „Социално инженерство", „Анализ на риска" и др. Също така повечето магистърски програми предлагат и редица избираеми дисциплини, които да помогнат на студентите да създадат свой собствен профил и съответно да се насочат към мрежова сигурност, софтуерна сигурност или анализиране на сигурността.

На следващо място, младите експерти трябва да отделят внимание и на своите практически умения, които най-добре могат да се развият чрез провеждането на симулации. По света, а и у нас студентите често се обучават, като бъдат разделяни на два екипа – нападащи и защитаващи, което им помага да се подготвят по-добре за реалните ситуации. Симулации на големи атаки, например срещу цели заводи, обаче трудно могат да се проведат на университетско ниво.

> Студентите често се обучават, като бъдат разделяни на два екипа – нападащи и защитаващи.

Това съвсем скоро се очаква да се промени, тъй като предстои откриването на симулатора Cyber Range в Черноморската академия за сигурност, която е част от ВСУ. Нашите студенти ще могат да го

използват безплатно, като той ще им даде възможност да участват в симулации с различна степен на сложност, разкрива Момчева. Самият проект е уникален за Балканите и се реализира в партньорство с Центъра за иновации и сигурност на Израел към Университет „Ариел".

Въпреки че конкретните знания и умения са изключително необходими, те са само едната страна на монетата. Според Момчева още от ранна детска възраст трябва да се възпитава и изгражда усет към темата за сигурността, тъй като реалните ситуации често са изключително предизвикателни и изискват не само прилагане на установените правила, но и добро ниво на социални умения. В тази връзка ВСУ организира специална програма за деца, наречена „Кибермагьосници", която има за цел както да разшири познанията на учениците по математика и компютърни науки, така и да развие у тях една по-широк поглед за сигурността.

Към работното място

В днешния динамичен свят малко са специалностите, които не започват работа още по време на обучението. Сферата на ИТ технологиите определено не прави изключение в случая. Статистиката показва, че повечето бакалаври още след първия семестър си намират стаж или работа. Младите специалисти обикновено търсят успешна реализация във фирми, които харесват. Освен това те предпочитат да се насочат към организации, които са динамични, създават модерни решения и прилагат нови технологии.

Интересна тенденция през последните години е, че все повече специалисти от други направления се насочват към ИТ сферата, за да придобият нови умения и квалификации и да сменят работното си място. „Това не са хора, които просто са си объркали първата специалност или не са попаднали там, където трябва. Един голям процент от тях са били успешни в своята област, но искат да надграждат. А за тази цел те всъщност трябва да усвоят нови умения, които са свързани с анализи на данни или сигурност", разкрива експертът от ВСУ. Все по-често към придобиването на такива допълнителни знания се насочват юристите, финансовите и маркетинг специалистите, които се стремят да постигнат едно по-високо аналитично ниво в своята работа.

Предложенията на пазара

У нас пазарът в сферата на киберсигурността тепърва започва да се развива. Големите компании все по-често наемат експерти с нужните умения, които да се грижат за защитата на фирмени данни и системи. В същото време малките и средните предприятия трудно могат да отделят ресурс само за толкова тясно специализирани кадри и предпочитат да наемат човек с по-широки ИТ познания, който гъвкаво може да се адаптира към конкретните нужди на организацията.

„Лично аз считам като председател на ИТ клъстера във Варна, че в страната няма достатъчно нови позиции, които да се определени точно като специалист по сигурността – независимо дали е в ИТ отделите или в ИТ компании-

> Реалните ситуации често са изключително предизвикателни и изискват добро ниво на социални умения.

те като цяло. Това предстои да се развива, тъй като на световно ниво вече имаме такива анализатори и проектанти на сигурността, например на самоуправляващите се автомобили. Ние нямаме толкова големи компании, които да са така персонализирани и конкретизирани като профили. Именно заради местните компании ние се стремим обучението да може да се доспециализира от студента", споделя Момчева.

В тази връзка, за да могат образователните институции да отговарят на нуждите на пазара, те трябва да поддържат тясно партньорство с бизнеса в страната. ВСУ дава добър пример в това отношение, като се стреми да разширява кръга от компании, с които работи. По този начин не само се осигуряват стажове за студентите, но и обучението се адаптира към търсените от бизнеса компетентности и към изискванията.

Въпреки тези особености на пазара възможностите за бързо и успешно развитие, които предлага сферата на киберсигурността, са безспорни. Тя позволява на младите специалисти бързо да навлязат в нея, да придобият нужните умения, а след това сравнително лесно да си намерят високоплатена позиция. Това определено не е така при други ИТ специалности. Момчева дава за пример кариерното развитие на софтуерните архитекти, на които са им нужни години, за да натрупат опит за позиция с наистина привлекателна заплата– включително да са преминали през работата на програмист, да са управлявали екип и да са били проектни мениджъри.

„Докато в киберсигурността и в науката за данните тези неща много бързо можеш да ги направиш, имаш бърза пътечка до много голяма заплата, ако, разбира се, знаеш, можеш и си адекватен. Много е важно също така да изградиш доверие, защото отговорността в този вид работа е от съществено значение", заключава Момчева.