МЕЃУНАРОДЕН СЛАВЈАНСКИ УНИВЕРЗИТЕТ
СВЕТИ НИКОЛЕ – БИТОЛА
РЕПУБЛИКА МАКЕДОНИЈА



ФАКУЛТЕТ ЗА ТЕХНИЧКИ НАУКИ И ИНФОРМАТИКА

СТУДИСКА ПРОГРАМА: КОМПЈУТЕРСКИ СИСТЕМИ И МРЕЖИ

МАГИСТЕРСКИ ТРУД

УЛОГАТА НА CISO, СИСТЕМСКИОТ СОФТВЕР И СВЕСТА И КУЛТУРАТА ЗА ИТ-БЕЗБЕДНОСТ ЗА ЗГОЛЕМУВАЊЕ НА САЈБЕР-БЕЗБЕДНОСТА ВО ОРГАНЗИАЦИЈАТА

СТУДЕНТ: **АЛЕКСАНДАР МАКАРИЈОСКИ**
БРОЈ НА ИНДЕКС: **M218011**
МЕНТОР: **ПРОФ. Д-Р ОРЦЕ СИМОВ**

Свети Николе, 2024

АПСТРАКТ

Во денешно време, бизнисот треба да ја разбере безбедноста на информациите не само на ниво на свесност, туку и на ниво на планирање, буџетирање и имплементација. Интегрирањето на безбедноста на информациите во деловните процеси станува предуслов за одржлив бизнис. Опасностите и компјутерските напади кои се насочени и кон организациите во корпоративниот свет и кон оние од јавниот сектор, бараат специјалисти кои ќе се фокусираат и ќе сносат одговорност за безбедноста на информациите. Ширината и сложеноста на оваа област бара стручност и искуство и постојана волја за стекнување нови знаења. Политичките одлуки и произлезеното законодавство се во прилог на формалните барања за спроведување на одредени активности во областа на информацискатa безбедност.

Тоа само по себе дава дополнително значење и обврска. Систематизацијата на позицијата менаџер за информациска безбедност (CISO) претставува одговор на горенаведените барања, а стручноста и сложеноста на активностите со кои треба да се занимава горенаведениот експерт претставуваат предизвици кои бараат постојано и доживотно учење.

Клучни зборови: менаџер за безбедност на информации, класифицирани податоци, безбедност на информации, управување со ризик, ISO/IEC 27001, контроли, безбедносен инцидент, криптографија, закон, ранливост, управување со ранливост, политика за безбедност на информации, правилник, процедури

ABSTRACT

Nowadays, business needs to understand information security not only at the level of awareness but also at the level of planning, budgeting and implementation. Integrating information security into business processes becomes a prerequisite for sustainable business. Dangers and computer attacks that are aimed both at organizations in the corporate world and at those from the public sector require specialists who will focus on and bear responsibility for information security. The breadth and complexity of this field requires expertise and experience and a constant will to acquire new knowledge. Political decisions and the resulting legislation are in support of formal requirements for the implementation of certain activities in the field of information security.

This in itself gives additional significance and obligation. The systematization of the position of information security manager is a response to the aforementioned requirements, and the expertise and complexity of the activities that the aforementioned expert should deal with represent challenges that require constant and lifelong learning.

Key words: Information security manager, classified data, information security, risk management, ISO/IEC 27001, controls, security incident, cryptography, law, vulnerability, vulnerability management, information security policy, rulebook, procedures

С О Д Р Ж И Н А

АПСТРАКТ 2

ABSTRACT 3

1. ВОВЕД 6

2. Вредноста на информациите и функциите на менаџерот за информациска безбедност 8

2.1. Основни вештини 17

2.2. CISO како раскажувач 19

2.3. Факторот на страв во информацискатa безбедност 21

2.3.1. Истакнување на позитивни аспекти 23

2.4. Потребно искуство и релевантно работно искуство за функцијата CISO 27

2.5. CISO како лидер 28

2.6. Учење од другите бизнис-лидери 29

3. Обврски и одговорности на функцијата CISO 34

3.1. Поддршка и одговорност за стандардизација 34

3.2. Управување со ризикот од безбедноста на информациите во согласност со стандардот ISO/IEC 31000 46

3.2.1. Комуникација и консултации 48

3.2.2. Опсег, контекст и критериуми 49

3.2.3. Евалуација на ризик 53

3.2.4. Обработка на ризик 64

3.2.5. Надзор и контрола 66

3.2.6. Евидентирање и известување 67

4. Релевантно законодавство за безбедност на информации во ЕУ 67
5. Опис на активностите и одговорностите на CISO 68
5.1. Раководител на информатичка безбедност во технолошки компании 69
5.1.1. Ревидирана директива за платежни услуги 69
5.1.2. Иницијатива NextGenPSD2 на Берлинската група 72
5.1.3. Организациска структура и активности и одговорности на раководителот за информатичка безбедност 75
5.1.4. Активности и одговорности на менаџер за информациска безбедност во технолошката компанија – студија на случај 76
5.2. Раководител за информатичка безбедност во јавниот сектор 88
5.3. Раководител за безбедност на информации во организации за плаќање со картички 93
5.3.1. Детектирање на пропусти 97
5.3.2. Преглед на детектираните пропусти 102
5.3.3. Управување со пропустите 104
5.4. Надворешен менаџер за информациска безбедност 109
6. Трендови во информацискатa безбедност 111
6.1. Резултати од истражувањето 112
7. Заклучок 119
Користена литература 122

1. ВОВЕД

Опсегот на оваа магистерска работа вклучува опис на активностите и одговорностите што треба да ги задоволи менаџерот за информациска безбедност. Трендовите во технологијата ги отсликуваат трендовите во информатичката технологија и ја претставуваат насоката во која се движат предизвиците за информациската безбедност. Cloud computing и добиените решенија во кои добар број деловни субјекти ја мигрираат својата ИТ-инфраструктура резултира со фактот дека денес се среќаваме со ИТ-инфраструктури кои или се целосно во облакот или се еден вид хибридно решение, она во кое компаниите одлучуваат дел од инфраструктурата да ја имаат локално, а другиот дел во облакот.

Со глобализација и своевидно приближување кон т.н. западен свет, се појавија и одредени прописи. Овие регулативи имаат за цел да ги заштитат економските системи и општеството, како и приватноста на граѓаните (GDPR, PCI DSS, PSD, итн.). Ова резултираше со одредени директиви, кои на крајот завршија со донесување на законите на земјите членки на ЕУ. Како резултат на тоа, горенаведеното стана обврска според која технологијата мора да се усогласи.

Сето горенаведено ги дефинира трендовите за кои секој менаџер за безбедност на информации треба да биде свесен и треба да поседува знаење, експертиза и мотивација за систематско усвојување на ново релевантно знаење. Комбинацијата на стручна литература и опишаните трендови од деловната практика ги покажуваат занимливоста и важноста на улогите и одговорностите на менаџерот за информациска безбедност. Функцијата менаџер на информатичка безбедност станува неопходност во одредени сектори, а потребата од неа се забележува во голем дел на други сектори.

Безбедносните инциденти се фактори на трошоци и репутација што деловните субјекти сакаат да ги избегнат и да ги минимизираат нивните последици. Горенаведеното го наметнува прашањето каков вид, по која цена и какви надлежности треба да има менаџерот за информациска безбедност. Во овој

труд ќе ги опишеме сите предизвици и одговорности со кои се соочуваат денешните менаџери за безбедност на информациите.

Целта на овој труд е да ја опише важноста на улогата на менаџерот за информатичка безбедност во организациите кои работат во сектори со поголема или помала регулатива во Република Македонија. Под регулирани сектори се подразбираат економски сектори кои имаат специфичен регулатор, а помалку регулирани сектори се сектори кои немаат законски дефиниран регулатор. Пример за регулатор за банкарскиот сектор е НБРМ, за осигурителни компании е Агенција за супервизија на осигурувањето, за телекомуникацискиот сектор е АЕК, додека орган за енергетика е Комисијата за енергетика.

Со опишување на секојдневните активности кои се во корелација со трендовите на заканите во информацискатa безбедност, целта на овој труд е да ја прикаже потребата од позицијата менаџер за информациска безбедност и да ги опише вештините, знаењата и искуството што треба да ги поседува истиот. Покрај горенаведеното, целта е и да се опише решение во форма на аутсорсинг на функцијата менаџер за информациска безбедност. Ова во голема мера ги решава проблемите како што се: недоразбирање, недостаток на свест, недостаток на персонал и регулирање на трошоците за безбедноста на информациите.

Трудот е поделен во седум поглавја. Во воведниот дел е претставен теоретскиот концепт на улогата на менаџерот за информациска безбедност. По теоретскиот дел, опишани се најчестите активности и одговорности на менаџерот за информациска безбедност, како што се поддршката за сертификација и управувањето со ризикот на информацискиот систем. Во овој дел се опишани секојдневните активности, одговорности и должности, а наведени се и очекуваните и потребните компетенции што треба да ги поседува наведениот експерт.

Потоа е даден преглед на релевантната законска регулатива за безбедност на информации во ЕУ и што сè Република Македонија треба да исполни на патот до полноправно членство во ЕУ. Во петтото поглавје, активностите и

одговорностите се прикажани на примерите на позицијата менаџер за информациска безбедност во организациите и опис на аутсорсингот на функцијата и нејзината понуда според SaaS (engl. Software as a Service) или FaaS (engl. Function as a Service) и се претставени некои од техничките алатки што ги користи менаџерот за безбедност на информации. Шестото поглавје ги опишува трендовите во индустријата за безбедност на информации од перспектива на менаџерот за информациска безбедност. Во седмото поглавје е претставен заклучокот од овој труд.

2. Вредноста на информациите и функциите на менаџерот за информациска безбедност

Во контекст на организацијата, информациите се тие што го овозможуваат водењето на бизнисот. Деловниот процес создава и обработува податоци што се претвораат во информации и знаење, кои се користат за создавање вредност и стимулирање на организацијата и нејзините процеси.[1]

Управувањето со информациите (eng. information management) го промени начинот на кој организациите управуваат со нивниот бизнис, начинот на кој тие се натпреваруваат и има клучна функција во постигнувањето стратешка и компаративна предност. Организациите донесуваат експлицитни и имплицитни одлуки за потребата од информации и нивната употреба. Одлуките се засноваат на проценка на трошоците и употреба на информации за деловната структура и стратегија.

Организациите се корисници, менаџери и креатори на информации, а нивната репутација во голема мера зависи од организациската интелигенција. Се манифестира во способноста за обезбедување, анализа и навремено враќање на информациите.

[1] ISACA, 2012. - Fundamental Concepts of IT Security Assurance, https://www.isaca.org/resources/isaca-journal/past-issues/2012/fundamental-concepts-of-it-security-assurance, 5.6.2024

Стандардот ISO 27000 ја дефинира безбедноста на информациите како процес кој мора да ја зачува доверливоста, интегритетот и достапноста (т.н. CIA), додека главната мисија е да се обезбеди континуитет на бизнисот и да се намали штетата со ограничување на негативните ефекти од безбедносните инциденти.[2] Управувањето со информацискатa безбедност ограничено само на технологиите и процесите на информатичката технологија не е доволно за да се обезбеди продорно влијание во големите организации.

Управувањето со безбедноста на информациите (engl. information security governance) се објаснува како процес на дефинирање, воспоставување и одржување на структурата и процесите на управување кои го поддржуваат усогласувањето на безбедноста на информациите со деловните цели, притоа усогласувајќи се со соодветните закони и прописи. Ова се постигнува со усвојување политики, контроли и воспоставување улоги и одговорности, кои поддржуваат подобро управување со ризикот во организацијата.[3] Процесот на организирање на информацискатa безбедност во организацијата треба да вклучува повеќе фактори, како што се: мисијата на организацијата, составот, овластувањата, одговорностите, улогите, комуникациските линии, координацијата и позицијата во организацискатa структура.

Кога ги дефинирал упатствата за управување со безбедноста на информациите, Basie von Solms претставил 13 димензии во 2001 година, кои, без оглед на нивната организација, треба да функционираат заедно за да создадат безбедна средина:[4]

1. димензија на корпоративна стратегија и менаџмент
2. димензија на организацијата

---

[2] International Organization for Standardization – ISO: ISO 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary https://www.iso.org/standard/73906.html, 11. 6. 2024.
[3] International Organization for Standardization – ISO: ISO 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary https://www.iso.org/standard/73906.html, 11. 6. 2024.
[4] Pedro Monzelo and Sergio Nunes: „The Role of the Chief Information Security Officer (CISO) in Organizations“, University of Lisbon, Lisbon, 2019. https://www.researchgate.net/publication/338833079 15.5.2024

3. димензија на политиката
4. димензија на најдобрата практика
5. етичка димензија
6. димензија на сертификација
7. правна димензија
8. димензија на осигурување
9. човечка димензија
10. димензија на свесност
11. техничка димензија
12. димензија на метриката
13. димензија на ревизија.

Затоа, безбедноста на информациите треба да се сфати и да се перципира како повеќедимензионално прашање и треба да се третира како одговорност на корпоративното управување и менаџментот. Менаџерите треба да развијат вештини за управувањето со ризикот, известувањето и одговорноста за да се обезбеди соодветно ниво на зрелост и безбедност на информации во организацијата.

Постоењето на функции на CISO во рамките на организациите предупредува дека менаџментот е одговорен и посветен на прашањата за безбедноста на информациите. Во организациите наидуваме на повеќе функции, како што се: директор за информациска безбедност, менаџер за информациска безбедност и раководител за информациска безбедност, но името на функцијата не е толку важно колку одговорностите на овие функции во рамките на организацијата.

Додека, на пример, функциите како што се главен извршен директор - CEO (engl. Chief executive officer) или главен финансиски директор - CFO (engl. Chief financial officer) се јасно дефинирани, дефиницијата за функцијата CISO сè уште е во еден вид развој. Историски гледано, функциите на CISO главно се фокусирани на дефинирање на стандарди за техничка безбедност и развивање политика за безбедност на информациите. Денес, организациите стануваат свесни дека

сајбер-ризикот е директно поврзан со нивните стратегии за иновации и раст. Денес, CISO сè повеќе се препознава како клучен елемент во дефинирањето на стратегијата за управување со информациски ризик, покрај неговите главни одговорности: развој, управување и операционализација на стратегијата за информациска безбедност; постојано следење и евалуација на практиката за безбедност на информациите; спроведување на ревизија и проценка на ризикот; управување, надзор и обука на вработени; усогласување на организацијата преку регулирање на безбедноста на информациите; развој и имплементација на план за континуитет на бизнисот; заштита на интелектуалната сопственост на организацијата; обука и подигање на свеста на вработените за ризиците од безбедноста на информациите; управување со буџетот за безбедност на информации и известување до Управниот одбор. Друга од главните одговорности на CISO е да биде активен член на врвниот менаџерски тим.

CISO има извршна улога во организацијата и е одговорен за воспоставување и одржување на визијата, стратегијата и програмата за организациска безбедност на информации, кои се усогласени со стратегијата на организацијата.

Ќе користиме илустративен пример за да ја опишеме позицијата на менаџерот за информациска безбедност и потребата од него (во подолгиот текст, CISO). Одговорноста и целта на директорот за финансии на компанијата SuperSoft doo., како дел од годишната ревизија, е да докаже дека компанијата е во согласност со Законот за Sarbanes-Oxley[5]. Постојаните напори на внатрешните ревизори да го разјаснат прашањето за резервната копија (engl. backup), што претставува проблем со неусогласеност со SOX, не резултирало со решение. Факт е дека директорот за финансии е стручен за сметководство, а не за технички

[5] SOX е кратенка за Законот за заштита на инвеститорите во хартии од вредност (Законот Sarbanes-Oxley), исто така познат како SOX Act. Станува збор за американски закон кој е донесен во 2002 година, како реакција на серијата финансиски скандали кои се случиле кон крајот на деведесеттите и почетокот на 21 век, како што се скандалите со Enron и WorldCom. Целта на SOX е да ја подобри транспарентноста и одговорноста на корпорациите и да ги заштити интересите на инвеститорите. Законот вовел голем број регулаторни барања и заштита за да се обезбеди интегритет на финансиското известување на компаниите. Одреден дел од законот става акцент на безбедноста на податоците, следењето на обидите за истекување податоци и водење дневници заради периодично следење

прашања. Напорот да се префрлат техничките проблеми на лицето чија одговорност е финансиското работење на компанијата резултирало со многу недоразбирања, додека пак обидот да се разјасни прашањето преку технички детали резултирало со уште повеќе недоразбирања. Наведениот проблем, кој сè повеќе ескалирал, одреден вработен во техничката струка го решил користејќи алегориски метафоричен пример. Тој го објаснил проблемот со техничката резервна копија со опишување на воз кој превезува патници од станицата А до станицата Б. Тој објаснил: „Еве, ова е точно резервна копија, пренос на податоци од нашите сервери на резервните коловозни ленти. Знаеме дека возот пристигнува на станицата Б, па можеме да потврдиме дека резервната е создадена. Но, ние исто така не знаеме колку патници пристигнале на станицата Б. Така, не можеме да тврдиме дека сме ги обезбедиле сите информации, а за да бидеме усогласени со SOX, треба да бидеме сигурни дека сите информации се безбедно зачувани“.

Метафорично поедноставен опис на ситуацијата довел до решение, на што не се успеало со традиционален пристап, со преведување на проблемот со техничката безбедност во терминологија што извршниот директор на бизнисот може да ја разбере и запомни. Ова илустрира една од клучните способности што треба да ги поседува CISO. Неопходно е да се прошири опсегот на безбедноста на информациите надвор од одделот за безбедност и ИТ со цел да се постигне јасна комуникација со влијателни поединци на сите нивоа и сите образовни средини во рамките на една организација.

Подолу ќе објасниме некои од вештините и особините што треба да ги поседува CISO за да ја изврши оваа предизвикувачка улога на главен службеник за безбедност на информации. Пред да го опишеме, ќе направиме чекор наназад и накратко ќе ја опишеме динамиката на фокусот на безбедноста на информациите.

За да остане на пазарот и да постигне одржлив резултат, секоја компанија мора да имплементира технологија до одреден степен. Од горенаведената причина, можеме да заклучиме дека секоја компанија со текот на времето

преминува во технолошка компанија. Исто така, потенцијалното влијание на ризикот од информации се шири, така што управувањето со безбедноста и приватноста станува категорија на корпоративна општествена одговорност. Според тоа, опсегот на функцијата CISO треба да се прошири до степен до кој може да ги покрие и управува сите ризици поврзани со безбедноста на информациите. Ова веќе се случува во многу организации. CISO презема одговорност за приватноста, законската усогласеност и безбедноста на производите и услугите, што симболизира промена и зголемување на важноста на позицијата во организацијата и промена во однос на традиционалното разбирање на ИТ-безбедноста. Оваа ситуација е можност за CISO да преземе поважна и помоќна функција во организацијата. Клучните вештини за професионалците за безбедност на информациите се проценката и ублажувањето на ризикот, кои стануваат неопходност за справување со новите ризици поврзани со безбедноста на производот, приватноста и усогласеноста со регулативата, покрај традиционалните вештини за ИТ-безбедност. Вака опишаната проширена функција отвора прашања како што е потребата од промена на името на самата функција, што подобро ја опишува конвергенцијата на активностите за проценка на ризикот. Така, во дискусиите во врска со имињата, може да се види, на пример, eng. Chief Trust Officer или Chief Information Risk Officer. Но, имињата и титулите во организациите се едно, а реалните одговорности се друго, а има и чести несовпаѓања. Прифаќањето на улогата на поголем опсег на одговорност бара поширока перспектива и поврзан сет на вештини. Потребно е разбирливо да се комуницира со „деловните луѓе“ и да се градат односи кои овозможуваат влијание на сите нивоа во организацијата. Покрај техничките компетенции, потребни се и менаџерски вештини за водење и управување со луѓе во оперативни и извршни функции и способност за мотивирање на луѓето кои се дел од проширениот тим за управување со ризик. Способноста да се управува со целиот опсег на ризици поврзани со информации е неопходност - не само за функцијата на CISO, туку и за целата организација. Доколку CISO не преземе поширок опсег на активности, организациите немаат друг избор освен да ја најдат потребната експертиза на друго место. Поради презентираните факти, вработениот кој ја извршува

функцијата CISO, а не е агилен во прилагодувањето на потребите што ги бара споменатата функција, ризикува да стане ирелевантен и непотребен. Алтернативно, ризичните области ќе се управуваат изолирано и на фрагментиран начин, доведувајќи ја организацијата во ситуација кога никогаш нема да управува со ризиците на сеопфатно ниво, а контролите на ризикот нема да бидат сеопфатни и неексклузивни. Ако тоа се случи, организациите сигурно ќе генерираат неуправувани ризици за себе, нивните клиенти и општеството.

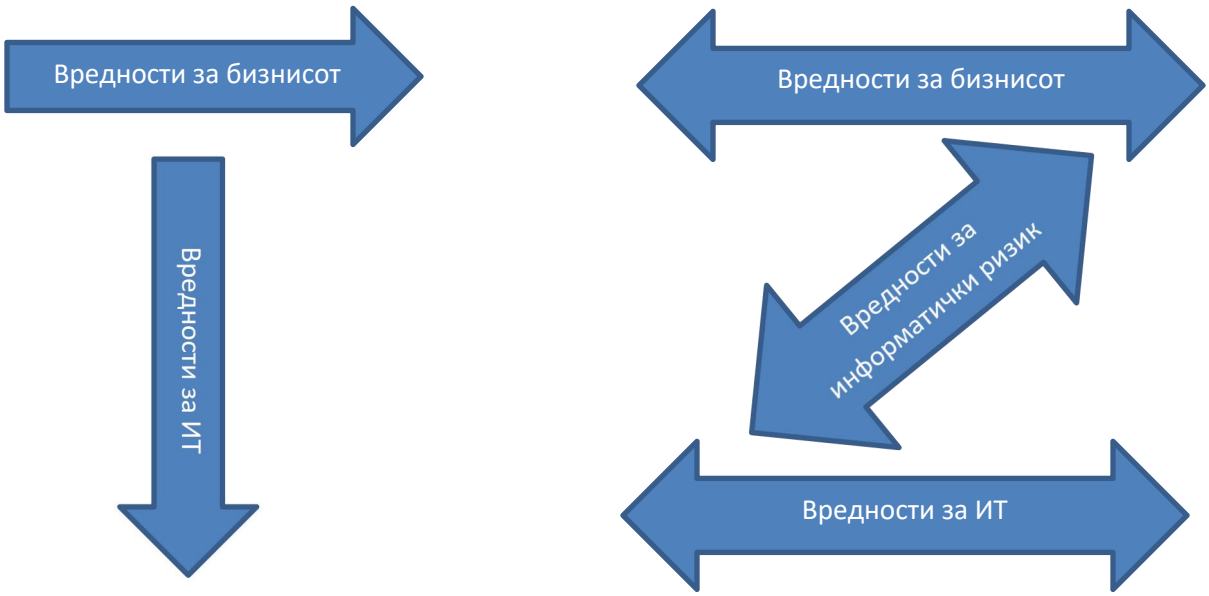
До неодамна една од најсложените задачи на функцијата на CISO беше да добие средства и одобрен буџет за безбедносни иницијативи во рамки на организацијата. Во денешно време, тоа не е случај, бидејќи честите и постојани безбедносни инциденти и големи протекувања на податоци и кражби, го фаворизираат буџетирањето за безбедноста на информациите. Меѓутоа, пообезбедените средства не секогаш нужно водат до повисоко ниво на безбедност или подобар исход за организацијата. Понекогаш стравот од безбедносен инцидент ги поттикнува организациите да инвестираат големи ресурси во контроли кои создаваат големи ограничувања, ограничувајќи ја способноста на корисниците и вработените да ги извршуваат своите работни места. На пример, некои организации воспоставија контроли кои ги спречуваат корисниците да преземаат апликации или датотеки и да пристапуваат до одредени веб-страници. Овие контроли се закана за способноста на корисникот да иновира и да ја забави севкупната деловна агилност. Од друга страна, го поттикнува решителниот корисник да најде начини да ја заобиколи контролата.

Функцијата CISO бара одредена деловна свест за процесите и организацијата чиј член е, со цел да се разбере влијанието на безбедносните контроли врз другите деловни функции. Денешниот пристап кон безбедносната архитектура треба да започне со разбирање на воспоставените контроли за надминување на ризиците, а дополнително, неопходна е свесност за влијанието на овие контроли врз другите процеси во организацијата. Деловната свест е исто така неопходна за да се пренесе ризикот од техничка природа на нетехничките вработени и да се разбере дека одреден ризик мора да се прифати. Преземањето

ризик, или прифаќањето на пресметаниот ризик, е основата на секој деловен модел. Без прифаќање ризик, не може да се создаде дополнителна вредност.

Ако не се поседуваат вештините потребни за CISO, истите треба да се научат и усвојат. Во продолжение ќе опишеме два модели на вештини и карактеристики диктирани од трендовите на времето во кое работиме. ИТ-професионалците мора да имаат деловна свест и да поседуваат длабинско разбирање за ИТ.

Концептот на Т-форма (eng. T-shaped) се применува за да се нагласи идејата дека ИТ-професионалците мора да бидат способни да испорачаат вредност хоризонтално - низ различни деловни оддели - и вертикално, на сите нивоа во рамките на ИТ-одделот. Споменатите концепти се прикажани на сликата 1.[6]



Слика 1: ИТ-експерт за Т-облик и Z-облик CISO

Извор: Malcolm W. Harkins: „Managing Risk and Information Security, Protect to Enable“, 2 ed., Folsom, Kalifornia, USA, 2016

[6] Malcolm W. Harkins: „Managing Risk and Information Security, Protect to Enable“, 2 ed., Folsom, Kalifornia, USA, 2016

CISO во 21 век мора доволно добро да ги разбере деловните приоритети и процеси за да разбере дали безбедносните контроли го поттикнуваат или го ограничуваат самиот бизнис-модел на организацијата. За да стекне доволно ниво на разбирање, неопходно е да има искуство во областа каде што е фокусиран бизнисот на организацијата. Ова, се разбира, варира од организација до организација и првенствено е определено од индустрискиот сектор на кој му припаѓа и од стратешките одлуки на менаџментот; на пример, CISO претходно работел во одделот за производство или во одделот за спојувања и преземања (eng. mergers and acquisitions).

CISO исто така треба да има одредено ниво на техничко знаење, иако во литературата може да се прочитаат многу дебати за тоа кое ниво на техничко знаење треба да го поседува.[7] На пример, на одреден број организации со различна големина и сложеност, можно е да се забележи следново: во помалите организации со помала сложеност, CISO е повеќе вклучен во длабочината на техничките барања и управувањето со луѓето, додека поголемите, а посложените организации се помалку склони да навлегуваат во техничките детали за секојдневните безбедносни прашања.[8] Без оглед на горенаведеното, CISO мора да знае доволно за технологијата за да може да го одвои суштинското од несуштинското и јасно и недвосмислено да ги пренесе безбедносните прашања на раководните луѓе надвор од безбедносниот оддел. Ова подразбира широк опсег на техничко знаење - од уреди до центри за податоци. Неопходно е да се поседува ниво на техничко знаење доволно за да може да се процени безбедносниот ризик, како и практичноста за постојано унапредување и менување на технологијата.

Управувањето со ризик и вештините во областа на безбедноста се алки кои го комплетираат т.н. Z-облик (eng. Z-shape), односно комбинација на технологија и деловни процеси. Разбирање на управувањето со ризик преку примена на

[7] Malcolm W. Harkins: „Managing Risk and Information Security, Protect to Enable“, 2 ed., Folsom, Kalifornia, USA, 2016

[8] International Organization for Standardization – ISO: ISO 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary https://www.iso.org/standard/73906.html, 11. 6. 2024.

процедури, технички и физички контроли; и заради исполнување на правниот аспект, барањата за приватност и безбедност; е најголемиот дел од одговорноста на функцијата CISO.

2.1. Основни вештини

Да се стане „поединец во облик на Z“ (eng. Z-shaped individual) е еден вид основа на секоја CISO функција. Неопходно е да се воспостави кредибилитет низ целата организација. Кредибилитетот е неопходен за градење квалитетни односи со менаџерите и специјалистите во организацијата, а се создава врз основа на експертиза, која пак доаѓа од разбирањето на бизнисот и технологијата - под услов знаењето за безбедноста да биде на високо ниво. Станувајќи „поединец во облик на Z“, CISO се става себеси во позиција да влијае на управувањето со ризикот на производите или услугите што ги нуди организацијата. Способноста на CISO да влијае на организацијата произлегува од јасната мисија. Јасно артикулирање на одреден случај е можно само ако CISO има силно чувство за постигнување на организациска цел. Доколку се исполни горенаведеното, одлуките на функцијата на CISO може да имаат директно влијание врз одлуките на CFO (eng. chief financial officer) или CEO (eng. chief executive officer), а одделот за безбедност на информации може да добие на важност.[9]

Таквото тврдење ја става организацијата во стратешка позиција: „заштити за да овозможи“ (eng. protect to enable). Во денешната глобална економија, повеќето организации работат на конкурентен пазар. Од аспект на безбедноста на информациите, задачата е да се овозможи слободен проток на информации и брзо спроведување на нови можности за да се обезбеди успех и долгорочна конкурентна одржливост. Улогата на CISO треба да одговара на нивото и карактеристиките на организацијата во која припаѓа, особено во однос на степенот на одбивност кон ризик. Мисијата на функцијата CISO мора секогаш да биде

[9] Malcolm W. Harkins: „Managing Risk and Information Security, Protect to Enable“, 2 ed., Folsom, Kalifornia, USA, 2016

усогласена со деловните приоритети на организацијата. Важно е мисијата да стане дел од тоа кој е CISO и зошто тој постои во организацијата. Обезбедува цел што резултира со автентичност и конзистентност на активноста и помага да се создаде кредибилитет низ целата организација.

Безбедноста како таква, вклучително и безбедноста на информациите, може да биде доста оттргнувачко занимање, со постојан прилив на дневни итни случаи и одвлекување на вниманието. Затоа е потребна јасна мисија за да се одржи јасна насока. Гореспоменатото ќе го опишеме со помош на метафора, со цел да го прикажеме што подобро. Како искусни морнари, можеме да напредуваме кон нашата цел и покрај секојдневните одвлекувања и пренасочувања, правејќи постојани прилагодувања и корекции за да останеме на патеката додека ветровите се менуваат.[10]

Исто така, неопходно е да се одржи чувството на љубопитност. Поврзувањето со другите бара вистински интерес за она што тие го прават. Љубопитноста ја поттикнува можноста за учење, што последователно го подига нивото и ширината на компетенциите, а тоа резултира со зголемување на кредибилитетот.

Дополнителна причина зошто улогата на CISO бара постојано учење е да се остане пред злонамерните непријатели кои ја нарушуваат безбедноста. Таканаречените агенти на закана секогаш учат затоа што мораат. Како што се појавуваат нови закани, се воведуваат нови контроли. Но, штом овие контроли ќе бидат поставени, тие имаат тенденција да станат статични. Од друга страна, агентите за закана секојдневно иновираат и се обидуваат да смислат начини како да ги заобиколат контролите. Токму затоа индивидуите кои ја извршуваат функцијата CISO мора да размислуваат и да дејствуваат динамично и мора да учат секојдневно за да можат да ја заштитат организацијата од секојдневните закани кои напредуваат.

[10] Pedro Monzelo and Sergio Nunes: „The Role of the Chief Information Security Officer (CISO) in Organizations“, University of Lisbon, Lisbon, 2019. https://www.researchgate.net/publication/338833079 15.5.2024

2.2. CISO како раскажувач

Без комуникација со луѓето, не може да се влијае врз нив. Како што се проширува опсегот на информацискиот ризик, така се зголемува и потребата за комуникација со различни групи луѓе во организацијата. Таквата комуникација не е секогаш едноставна. Ако почнеме да ги пренесуваме техничките детали на нетехничари, нема да го привлечеме нивниот интерес. Напротив, постои ризик да го постигнеме спротивниот ефект, како што е опишано во примерот на почетокот на ова поглавје.

За да може успешно да комуницира, CISO мора да стекне способности на камелеон (способност да имитира), односно да се вклопи во различни средини. Потребно е ниво на знаење за различните деловни области на организацијата за да може да се комуницира на јазик што го разбираат вработените во тие одделенија. На пример, финансиските директори честопати сакаат да слушнат концизен преглед, изразен во смисла на финансиско влијание и поврат на инвестицијата, што често не е едноставно кога се разговара за безбедносни инвестиции насочени кон закани кои тешко се квантифицираат. Менаџерите на производи сакаат да ги слушнат безбедносните прашања изразени во термини кои се однесуваат на продажбата, маркетингот и оперативната ефикасност.

Раскажувањето приказни е несомнено моќна алатка за комуникација со различни луѓе во една организација. Кога безбедносните прашања се претставени како приказни и слики што луѓето можат да ги разберат, тие подобро се поврзуваат со тие прашања, дури и ако немаат техничко знаење. Метафорите и аналогиите се моќна алатка во комуникацијата. Тие се лесни за паметење и преведуваат сложени теми во едноставни концепти што секој може да ги разбере. Според тоа, ќе цитирам уште една метафора: „Диригентот на оркестарот не произведува звук“. Неговата сила доаѓа од можноста за будење кај другите. (Zander и Zander, 2000)“. На ист начин, силата на CISO доаѓа од подигање на свеста за ризикот кај луѓето низ организацијата, користејќи приказни засновани на

метафори за да се создаде таа свест. На пример, на вработените честопати им е тешко да ги разберат опасностите од скриените закани бидејќи тие се невидливи. Корисниците често не се свесни дека има проблем во нивниот систем. Тие сè уште го поврзуваат малициозниот софтвер со очигледни, иритирачки симптоми како пораки на екранот и паѓања на системот. Затоа, кога ќе им кажеме дека откривме опасен софтвер на нивниот компјутер, тешко е да се поверува дека тоа им е важно. Затоа мораме да се фокусираме на превенција, со примена на контроли. Ако не го постигнеме ова, ќе го продолжиме бескрајниот циклус на ризик со кој се соочуваме денес.

За да се привлече јасно внимание на опасноста и потребата од ефективни превентивни контроли, корисно е да се користи аналогија. Добро претставување на ситуацијата дава аналогијата помеѓу опасноста од мравки и опасноста од термити. Злонамерниот софтвер порано бил опишуван како обични мравки кои видливо се собираат околу остатоците од храна во кујната. Знаете дека сте заразени кога ќе видите дека мравките доаѓаат до остатоците од вашата храна низ ѕидовите и мебелот. Откако ќе станете свесни за горенаведеното, ќе направите нешто во врска со тоа. Но, во денешно време, безбедносната опасност е како термити кои можат да живеат незабележано во ѕидовите на нашите домови. Фактот што не ги гледаме резултира со тоа што мислиме дека едноставно ги нема. Но, тие некогаш прават многу поголема штета отколку обичните мравки. Термитите можат да го оштетат структурниот интегритет на целата куќа, особено на монтажните, со нарушување на статиката на зградата.[11] Од моето секојдневно деловно искуство, можам да потврдам дека со помош на аналогија пораката најбрзо стигнува до целта, до оној што треба да направи нешто во врска со тоа, а луѓето полесно разбираат дека невидливата закана може да ја загрози целата ИТ-инфраструктура, само бидејќи термитите можат да ја оштетат статиката на монтажната куќа. Разбирањето, а со тоа и свесноста, ја зголемува веројатноста вработените во организацијата да го прифатат следниот чекор – воспоставување безбедносни контроли, без разлика дали се тие превентивни или реактивни.

[11] Malcolm W. Harkins: „Managing Risk and Information Security, Protect to Enable“, 2 ed., Folsom, Kalifornia, USA, 2016

Со цел да се дискутира за управувањето со информацискиот ризик низ една организација, корисно е да се користи заеднички јазик што секој, вклучително и нетехничкиот персонал, може да го разбере. Рамката за безбедност на информации, NIST[12], е корисна. Развојот на горенаведеното датира од 2013 година, врз основа на наредба на претседателот на Соединетите Американски Држави за подобрување на безбедноста на критичната инфраструктура. Ова резултира со едногодишни активности водени и предводени од приватниот сектор за развој на доброволен водич за безбедност на информациите.

Рамката создава заеднички речник за управување со ризик, олеснувајќи ја комуникацијата помеѓу безбедносните тимови и другите, како и поттикнувајќи ја соработката. Дополнително, секоја организација може да го измери своето ниво на зрелост за управување со ризик според рамката. Како што повеќе луѓе ја користат, рамката помага да се зголеми општото разбирање на ризикот од информации и како да се управува со него.

2.3. Факторот на страв во информациската безбедност

Безбедносната индустрија генерално има тенденција да користи страв за да ги продаде сопствените производи и услуги. За жал, оваа тенденција го одразува фактот дека многу поединци во безбедносната индустрија профитираат од несигурноста, што е донекаде парадокс. Приходите на компаниите кои се занимаваат со безбедност на информациите растат кога има почесто протекување на доверливи податоци и кога има повеќе безбедносни инциденти. Во внатрешна ситуација, таквите околности ги користат безбедносните тимови за да добијат поголеми буџети или ресурси. Немаше да има безбедност без

[12] NIST (National Institute of Standards and Technology) Главната цел на NIST е да промовира индустриска конкурентност и иновации преку развој и примена на мерења, стандарди и технологија. NIST обезбедува техничка поддршка за индустријата, ги ажурира и одржува стандардите и упатствата и спроведува истражувања поврзани со широк опсег на научни и технички области; вклучувајќи технологија, електроника, компјутери, хемиски и физички науки, безбедност, кибернетика и други дисциплини. NIST исто така игра важна улога во безбедноста на информациите и сајбер безбедноста, обезбедувајќи насоки и ресурси за заштита на информациите и системите од сајбер-закани.

несигурност, која се состои од опасности, ранливости и ризици. Фокусот на стравот кој не е објективен, во никој случај не е добар. На самиот почеток може да понуди задоволство, но на крајот тоа не е објективно и оправдно и не ја поддржува функцијата на CISO, ниту на самата организација.

Краткорочно, стравот може да ги исплаши луѓето и да поттикне активности кои го поддржуваат финансирањето на безбедносните проекти. Поставувањето на безбедност врз основа на страв е краткотрајно и на крајот резултира со контраефект и со губење на кредибилитетот на CISO. Според одредени извори, бизнис-моделот заснован на страв придонесува за брзината на ротација на функциите на CISO од една организација во друга.[13] Поединците кои својата позиција ја градат премногу на страв, на крајот ќе бидат заменети, бидејќи организациите го забележуваат тоа на среден рок и на крајот не го толерираат.

Стравот не е добар и од други причини. Повеќето луѓе не сакаат да слушаат постојан прилив на негативни информации. Откако ќе почнат да го доживуваат како извор на негативност, тие не му придаваат значење. Ако перцепцијата е дека тоа е оддел со секогаш негативни одговори, со текот на времето ќе почнат да го игнорираат. Луѓето ќе најдат начини да ги заобиколат безбедносните барања за да постигнат деловна потреба и цел.

Дури и во организациите фокусирани на безбедноста, стравот може да стане гравитациона сила која го привлекува целото внимание и енергија кон негативните страни на безбедносните предизвици, наместо да се фокусира на деловните предизвици. Затоа е неопходна фокусираност кон решенија кои нудат три клучни придобивки:

1. докажлив и одржлив наклон на кривата на ризик (намалување на ризикот);
2. способноста да се намалат трошоците за контроли;
3. ниско ниво на контролни пречки, брзина и агилност на бизнисот и задоволството на клиентите.

[13] Malcolm W. Harkins: „Managing Risk and Information Security, Protect to Enable“, 2 ed., Folsom, Kalifornia, USA, 2016

2.3.1. Истакнување на позитивни аспекти

Позитивен пристап може да се преземе со концентрирање на мисијата на функцијата CISO, а тоа е: „да се заштити за да се овозможи“. Оваа мисија го менува акцентот од негативен во позитивен. Како можеме да ѝ помогнеме на компанијата да ги постигне своите цели преку решавање на информациските ризици и безбедносните проблеми?

Мисијата е усогласена со работата. Наместо да биде изолирана, таа се заснова на заеднички вредности, воспоставувајќи оптимистички пристап на долг рок, бидејќи оптимизмот е многу подобар мотиватор од песимизмот. Можеби опасностите се страшни, но целта е да се види можноста во заканите. Не постои проблем што не може да се реши без нова рамка.[14] Значи, ако не гледаме решение, користиме погрешна рамка. „Заштити за да овозможиш“ е новата рамка.

Да замислиме дека сме поканети на конкретен состанок за да разговараме дали организацијата треба да започне да користи бизнис-апликација базирана на облак која ја нуди нов потенцијален партнер за бизнисот. Јасно е дека овој производ претставува ризик бидејќи доаѓа од непознат продавач, до апликацијата се пристапува преку интернет, а чувствителните податоци ќе се складираат надвор од организацијата.

Тесниот поглед на безбедноста може да нè наведе да се фокусираме исклучиво на специфичен ризик. Меѓутоа, токму таквиот став може да нè доведе до ситуацијата на т.н „квака 22“ – со цел да се намалат ризиците, организацијата ја ограничува употребата на новата технологија. На пример, оваа технологија може да се користи само за податоци со низок ризик или може да се користи од тесен сегмент на вработени. Проблемот со овој пристап е што ограничувањето ги ограничува и придобивките од користењето на новата технологија, до тој степен што маргиналните придобивки од технологијата не ги оправдуваат трошоците и

[14] Marco Morana and co-autors: „ Application Security Guide For CISOs“, OWASP, 1.0 v, 2013. https://owasp.org/www-pdf-archive/Owasp-ciso-guide.pdf

активностите потребни за адаптација. Постои ќор-сокак. За технологијата да стане остварлива опција, треба да се прикаже деловна корист, но истата не може целосно да се демонстрира затоа што не се дозволува целосна употреба на технологијата.

„Заштити за да овозможиш“ нуди нова рамка која нè ослободува од прикажаните дилеми. Ни овозможува да се фокусираме на можностите и да ги идентификуваме придобивките што ги надминуваат ризиците. На пример, изборот на нов добавувач го подигнува нивото на конкурентност, што доведува до заштеди за организацијата во иднина. Оваа предност е во согласност со деловните цели на организацијата и е она што секој го разбира. На пример, помалку интуитивна, но подеднакво важна предност е фактот што овие заштеди може да се искористат за ублажување на ризиците кои произлегуваат од поширокатa примена на новата технологија. Во таква ситуација, предноста на новото решение ги надминува потенцијалните негативни последици. Со можноста за примена на нова технологија во поширок опсег, остваруваме поголема придобивка од трошоците за контролите што ги воспоставивме. Овој пример јасно покажува дека CISO мора да изгради деловна смисла, со која создава и открива можности за подобрување на бизнисот, а што, од друга страна, му овозможува да има преговарачка моќ во буџетирањето на безбедносните иницијативи.

Ќе опишеме уште еден пример што се случи во корпорацијата Интел. Пред извесно време беше откриен тежок и комплексен компјутерски црв (eng. worm), целосно активен во компјутерската инфраструктура на организацијата. За неговото откривање била потребна итна интервенција на безбедносниот тим. Со анализа и форензика на неговите активности, најдена е неговата трага и извор што довеле до надворешна компјутерска инфраструктура надвор од периметарот на организацијата која била во сопственост на еден од вработените во Интел.

Одговорот од безбедносниот оддел на организацијата бил прилично стереотипен. Тие ја исклучиле заразената компјутерска опрема, сервери и работни станици. Потоа ги заостриле безбедносните политики и сродните процедури за да се осигураат дека само работните станици во сопственост на

организацијата имаат право и можност за пристап до корпоративната мрежа. Ова било направено со правење обемен попис на сета компјутерска опрема, потоа скенирање на сè во рамките на мрежниот периметар и отстранување и исклучување на целата опрема што не се совпаднала со регистарот на имот на компјутерот.

Овој одговор на безбедносен инцидент бил успешен во контекст на намалување на ризикот од инфекција со малициозен софтвер, но во исто време довел до други ризици, кои не биле предвидливи. Забраната за пристап на персоналните компјутери во сопственост на вработените до корпоративната мрежа резултирало со потреба организацијата да издаде пропишан персонален компјутер за секој вработен со договор, вклучително и надворешни соработници. Можеме привремено да ги сметаме како трета страна. Накратко, многу луѓе за кратко време добиле пропишан персонален компјутер со кој можеле да пристапат до корпоративната мрежа. Ова, пак, резултирало со нагло зголемување на капиталните трошоци (eng. CAPEX). Поголемото влијание на таа одлука ги елиминирало сите потенцијални позитивни влијанија што би можеле да произлезат од вработените кои ги користат нивните персонални компјутери за работни цели.

По овој безбедносен инцидент и разрешница, овој случај по извесно време се вратил на разгледување, ревизија и потенцијална измена на одлуката. Водени првенствено од побарувачката на вработените и зголеменото усвојување на нови кориснички уреди, одделот за безбедност бил принуден да ја поправи својата првична одлука. Овој пат со примена на принципот „Заштити за да овозможиш“. Сè почнало од претпоставката како да се овозможи користење на компјутерски ресурси во лична сопственост за деловни цели, а во исто време да се намали безбедносниот ризик. Се покажало дека влијанието врз бизнисот е големо и позитивно. Овозможувањето на вработените да комуницираат едни со други од каде било и во секое време, може да има позитивно влијание врз продуктивноста. Забележано е и дека оваа можност ги прави вработените посреќни. Вработените едноставно сакаат да ги користат нивните приватни компјутерски ресурси, како

што се паметни телефони, персонални компјутери и таблети, и го ценеле фактот дека тоа им било озозможено. Исто така, треба да се нагласи дека одредена технологија не била достапна кога бил откриен безбедносниот инцидент. Поуката од овој пример е: ако прво се фокусираме на можностите, можеби е можно да се понуди одредено ниво на пристап додека се ублажува ризикот, а дополнително, да се намали влијанието на одлуката врз капиталните трошоци на организацијата.

Се разбира, улогата на безбедносниот оддел во организацијата сè уште е фокусирана на управувањето со ризиците, а тука е вклучена и вечната дебата за негативните последици што можат да ги предизвикаат човековите активности. Ако се контролира и структурира оваа дискусија, можно е да се информира во исто време без да се шири страв. Ова може да се постигне со јасно опишување на исходот и решението, без драматизирање или апострофирање на сериозноста и итноста на одредена ситуација, притоа јасно нагласувајќи ја сериозноста на безбедноста. Секоја функција на CISO создава контекст во кој организацијата може да донесе одлука која е најдобра за бизнисот. Иако функцијата на CISO во описот на работното место мора да нагласи непријатен исход, стравот не се шири сè додека информациите се засноваат на точноста и реалноста.

Подолу е уште еден пример од Интел. Клиентите сè повеќе користеле интернет, па затоа одделот за маркетинг, мотивиран од овој тренд, сакал да го зголеми присуството на компанијата на интернет. Логичниот деловен потфат резултирал со нарачка за создавање на неколку нови веб-страници на компанијата. Во согласност со процедурата, секторот за информациска безбедност започнал со проценка на ризиците и потребните контроли за наведените активности на креирање и објавување веб-страници. Голем дел од раководните луѓе на секторот за маркетинг не биле за наведените безбедносни активности. На сето ова гледале исклучиво како на деловна можност, за која мора да дејствуваат брзо и ефикасно за да ја искористат. Тие сметале дека ја имаат сета слобода да одлучуваат како да комуницираат надворешно и дека барањата на одделот за безбедност се само уште една административна пречка што ги забавува. Она што следело било многу поубедливо од првичните напори на

одделот за безбедност да спречи потенцијални проблеми. Неколку веб-локации биле лансирани без темелна контрола на квалитетот. Злонамерните хакери (во натамошниот текст хакери) нашле слабости на овие страници, но не ги симнале, ниту пак краделе информации. Наместо тоа, тие вметнувале линкови до страници со експлицитна содржина. Откако бил откриен овој немил случај, тој станал синоним и еден вид референтен пример, кој послужил да се научи нешто од него и да се подобрат безбедносните процедури. Тогашниот CISO го користел овој пример затоа што го сметал за доволно илустративен и ефективен од една страна, и доволно експлицитен за лесно да се запомни.

2.4. Потребно искуство и релевантно работно искуство за функцијата CISO

Ќе претставиме илустративен пример за вештините и искуството потребни за улогата на CISO. Истражувачите побарале од испитаниците да играат игра во која би можеле да ги максимизираат своите добивки со превртување карти од еден од двата сплава. Испитаниците не знаеле дека сплавовите се веќе подготвени. Тие би можеле да победат со избирање од еден сплав, додека извлекувањето од другиот сплав би резултирало со загуба. По околу 80 карти, испитаниците можеле да ја објаснат разликата помеѓу сплавовите. Но веќе по 50 карти имале чувство дека нешто не е во ред. Почнале да покажуваат знаци на стрес и да го менуваат своето однесување, по околу 10 карти и многу пред да сфатат на когнитивно ниво дека има разлика.

Лицето на позицијата CISO треба да биде на тоа ниво што, со комбинација на неговото деловно-техничко искуство, вештини и доживотно учење, може да забележи безбедносна закана пред сите други, вклучувајќи ги и експертите во неговиот тим. Многу често тоа е комбинација на когнитивни способности и искуство, што резултира со еден вид „шесто сетило“ за безбедност. Оваа комбинација на вештини и искуство е токму она што е потребно во областа на безбедноста, каде достапните информации се скоро секогаш скици или нецелосни.

Кога ќе се појави опасност, нема време да се спроведе опсежно истражување или да се чека да се соберат докази. Затоа е потребно да се дејствува одлучно, врз основа на достапните информации.

Ако идните ризици се идентификуваат доволно рано, може во целосно да се спречат или барем да се намали нивното влијание. Превентивните рани активности може да ги намалат целокупните активности потребни за контрола на ризикот. Раната акција може да ја избегне потребата за итен одговор и потенцијално големи напори за санација и обновување од безбедносен инцидент.

Сè што е споменато за способноста на функцијата CISO има смисла само ако организацијата има способност да дејствува брзо. За тоа да биде возможно, потребни се два клучни предуслови. Прво, потребна е храброст да се потпре на вербата и да преземеме акција за она во што веруваме. Друг услов е организацијата да реагира брзо кога ќе добие известување за безбедносен проблем. Неопходната брза реакција на компанијата е можна само доколку функцијата CISO постигнала и одржувала квалитетни односи со луѓето во целата организација. Можни се брзи, безболни одлуки бидејќи луѓето од искуство знаат дека информациите на функцијата CISO се сигурни и дека фокусот е на овозможување, а не на ширење страв.

2.5. CISO како лидер

Пред сè, денешниот CISO мора да стане ефективен лидер, охрабрувајќи го и мотивирајќи го својот тим од експерти ефективно да ја заштитат организацијата. Искуствено, за време на долга серија години на справување со безбедносни прашања, идентификувани се три клучни теми - од сите членови на тимот одговорен за безбедноста:[15]

1. мора да веруваат во мисијата на тимот
2. мора да чувствуваат припадност

[15] Harold F. Tipton and Micki Krause: „Information Security Mangment Handbook“, 6. izdanje, Boca Raton, Florida, USA, 2007.

3. мора да чувствуваат дека се важни.

Ако, од менаџерска и лидерска перспектива, можеме да ги натераме луѓето да чувствуваат дека веруваат, дека припаѓаат и дека се важни, тие ќе се справат со секој предизвик. Ако луѓето разберат повисока цел, тие можат да ја сфатат емоционалната поврзаност што владее со нивните секојдневни активности. Ова е една од клучните причини зошто е неопходно да се посвети многу време на дефинирање на мисијата. Дополнително, потребно е да се вложи време за пристап и разбирање меѓу членовите на одделот за безбедност на информации, дека нивната позиција и описот на работното место се тесно поврзани со деловните цели на организацијата.

Како пример, оперативна цел може да биде инсталирањето безбедносни закрпи во рок од една недела по објавувањето на новата верзија на софтверот. Целта е уште позначајна ако воспоставиме врска со компанијата користејќи ја премисата „Верувам, припаѓам и ми е важно“. Тие веруваат во мисијата „Заштити за да овозможиш“, односно доколку нѐ штитеа за да овозможат, другите вработени во организацијата немаше да можат да ја вршат својата работа, а организацијата немаше да ги исполни своите цели. Брзото распоредување на безбедносни закрпи е важно затоа што им помага на корисниците да ја завршат својата работа, што пак ѝ овозможува на организацијата да ги исполни своите цели.

2.6. Учење од другите бизнис-лидери

CISO менаџерот може да научи многу од другите деловни менаџери. Денес, менаџерските функции сѐ повеќе се оддалечуваат од работењето според принципот на „команда и контрола“ (eng. command and control) и се прилижуваат кон пристап на соработка што ја користи различноста на идеите на вработените. Овој принцип не е договор што води до бескрајни дебати и неодлуки. Целта на лидерот е да обезбеди усогласување со заедничката мисија и да го забрза донесувањето одлуки. Во опишаната рамка, различните погледи и дискусии ја

стимулираат креативноста, генерираат нови идеи и продуктивни тензии кои можат да го поттикнат резултатот.

Бидејќи безбедноста може да биде фрустрирачка, дури и страшна, важно е да се открие како да им се помогне на вработените да останат мотивирани. Важно е да им се помогне да почувствуваат дека напредуваат - не само кога постигнуваат големи цели, туку и кога ги решаваат помалите проблеми со кои се соочуваат секој ден.

Постојано се презентираат можности за лидерство, во секоја интеракција во тимот, со други вработени во ИТ-одделот и со други деловни партнери. Прашањето што треба да се постави овде е: Дали ја користиме секоја можност да ја наметнеме нашата мисија и со тоа да ѝ помогнеме на организацијата да постигне успех?

На техничките позиции или во организациите од техничкиот сектор, фокусот честооати е на технички прашања додека човекот паѓа во втор план. Од искуство, верувам дека е неопходно да се одржува меѓучовечкиот контакт, кој промовира чувство на припадност. Ако знаеме повеќе еден за друг, повеќе се грижиме. Секоја интеракција е можност за заемно учење и зголемување на компетенциите. Последниот и најважен критериум за ефективно лидерство е способноста да се развијат други лидери во рамките на безбедносниот оддел. Во спротивно, силата на тимот за управување со ризиците ќе биде присутна само додека сегашната CISO е таму. Со длабинско развивање на компетенциите, CISO може да обезбеди организацијата да дава одржливи резултати со текот на времето.

Во табелата 1 е прикажано истражување од извршната агенција Korn Ferry - што сугерира дека лидерите во сајбер-безбедноста треба да поседуваат уникатен сет на особини, вклучувајќи ја способноста да размислуваат надвор од рамката, да добијат длабок увид во проблемите, да применуваат расудување на ниво на одбор и да бидат доверлив деловен партнер.

Табела 1: Карактеристики на лидерите во областа на сајбер-безбедноста

Клучни карактеристики за извршните директори за сајбер-безбедност			
Стручност	Искуство	Карактеристики	Водство
Стратешки, глобално фокусиран мислител (способен да ја види големата слика) Размислувач надвор од кутија Аналитичар (навлегува длабоко во проблемите) Има деловна острина (разбира како информациите се применуваат во секојдневното работење) Ги балансира конкурентните приоритети Комуницира и влијае на широк простор (одбор на директори, врвен менаџмент). Привлекува, гради	Длабочина на техничко искуство Ги разбира правните и регулаторните рамки Во минатото успешно се справувал со безбедносни инциденти	Брзо учење (прилагодливост на нови и различни работи) Флексибилен Разбирање и толеранција за двосмисленост Интелектуално љубопитен	Бара улоги со висока видливост и одговорност Се стреми да биде агент за промени (наместо „не“ агент) Тој мора „да помине низ игла“ за да го балансира управувањето со промените и управувањето со ризикот на претпријатието Бара блиска соработка со деловни лидери (работи за да додаде деловна вредност)

и користи таленти.

Извор: Korn Ferry, 2021

Како што технолошката средина продолжува да се развива, многу луѓе веруваат дека се движиме кон иднина каде што организациите ќе ги нарачуваат повеќето од нивните ИТ-потреби и активности (engl. outsourcing). Доколку продолжи таквиот тренд, прашањето е какво влијание има тоа врз функцијата на CISO.

Во овој поглед на иднината, организацијата се оддалечува од ИТ-имплементација, кон набавка и управување со добавувачи и услуги, притоа поставувајќи насока и воспоставувајќи ја целокупната ИТ-архитектура.

Дополнително, организацијата ќе треба да ја задржи основната експертиза на одделот за безбедност, што е управување со ризикот од информации. Организациите не можат целосно да го пренесат ризикот на други. Организациите можат да бидат ангажирани да испорачуваат деловни системи, но одговорноста за усогласеност со прописите како SOX и HIPAA, GDPR сè уште се на организацијата. Доколку прекршувањето на податоците резултира со истекување на податоци за лична или интелектуална сопственост, организацијата останува одговорна за известување и пријава за безбедносниот инцидент. Дополнително, организациите често ги сносат последиците од штетите од некој инцидент, што честопати се рефлектира во намалување на вредноста на брендот, иако векторот на напад и причината за пристигнувањето до безбедносниот инцидент е недостаток и ранливост во системот на добавувачот. Со оглед на зголемениот број регулативи и фактот дека сè повеќе лични податоци се складираат во деловните системи, ризиците можат само да растат. Затоа, способностите на функцијата CISO ќе остане суштинска, дури и ако името на деловната функција во организацијата се промени. Сè додека функцијата CISO е во состојба да ја обезбеди потребната компетентност во постојано променливо опкружување на организацијата, така што е водена од мисијата „Заштити да овозможиш“, овој придонес во бизнисот на која било организација не е занемарлив. Прашање и одлука на секоја организација е дали постои свесност, волја или регулаторна

обврска да се систематизира ваквата деловна функција во форма на работно место. Дали таа позиција и функција ќе имаат единствена одговорност за безбедноста на информациите е прашање на регулатива, одлука на раководството на организацијата и, во крајна линија, способностите на поединецот што ќе ја извршува таа позиција.

Очигледно е дека лидерството подразбира преземање одговорност. Сепак, некои CISO се чини дека ја забораваат таа точка, барем повремено. Типична ситуација во пракса оди отприлика вака: CISO бил предупреден за безбедносно прашање, но не можел да добие буџет или ресурси за да го реши. Затоа, тој се откажал од одговорноста, бидејќи некој друг донел одлука да не го финансира решението. Авторот на овој труд има поинакво мислење - дури и да не се согласуваме со одлуката, треба да се потрудиме да ги изразиме нашите вредности. Треба да го артикулираме потенцијалното влијание врз организацијата, нашите клиенти и општеството. Како партнер во стратегијата на организацијата, CISO треба да се посвети на донесената одлука и да ја сподели целосната одговорност и одговорност пред колегите. За горенаведеното да биде остварливо, потребно е јасно да ги изразите личните вредности и да останете доследни на сопствените принципи. Почитувањето на личните вредности може да значи преземање ризици за вашата кариера. Затоа, од клучно значење е на поединецот кој ја извршува функцијата CISO да му се даде време да размисли за принципите и вредностите што тој навистина ги следи. Видот на самоиспитување низ кој треба да помине секој CISO додава друга димензија на концептот на поединецот во облик на Z - вредносната димензија, и тоа тој треба да биде со интегритет, да е чесен, посветен, храбар, несебичен и одговорен.

3. Обврски и одговорности на функцијата CISO

3.1. Поддршка и одговорност за стандардизација

Во овој дел од трудот ќе ги опишеме најчестите стандарди за сертификација, за чие сертифирање, одржување и ресертификација е одговорен CISO.

Развојот на стандардите за информациска безбедност на меѓународно ниво подразбира стандарди кои се специфицирани од Меѓународната организација за стандардизација, ISO (eng. International Organization for Standardization), Меѓународниот конзорциум за електроника и IEC (eng. International Electronics Consortium). Други организации обезбедуваат специфични стандарди за одредени сектори и често се засноваат или се повикуваат на стандардите „ISO“ (најчесто наречени ISO/IEC). Во Соединетите Американски Држави, оваа работа е управувана од Американскиот национален институт за стандарди (ANSI) и Меѓународниот комитет за стандарди за информатичка технологија (INCITS). Групата директно одговорна за развојот, придонесот и управувањето со оваа работа е INCITS CS/1, Cyber Security. Оваа група, CS/1, е исто така одговорна за стандардизација во областите на информатичката технологија (ИТ), безбедноста, приватноста, управувањето со идентитетот и биометриската безбедност. Една од главните области на фокус за CS/1 ги вклучува стандардите за безбедност на информациите познати како ISO/IEC 27001:2013 (Барања за управување со безбедноста на информациите - Систем за управување со безбедноста на информациите) и ISO/IEC 27002:2013 (Спецификација за управување со безбедноста на информациите). За поедноставување, овие стандарди отсега ќе ги нарекуваме „ISO 27002“ и „ISO 27001“. Исто така, важно е да се напомене дека од април 2007 година, ISO 17799 претрпел промена во означувањето и бил преименуван во ISO 27002. Последователно, биле направени промени и ревизии на двата стандарди во 2013 година, додека последната промена на ISO 27001 била направена во 2022 година.

Овие стандарди, ISO 27001 и ISO 27002 (порано познат како ISO 17799) се однесуваат на полето на безбедноста на информациите. ISO 27001 е стандард за систем за управување со безбедноста на информациите (ISMS), додека ISO 27002 е најдобра практика за безбедност на информациите. Иако на прв поглед може да биде збунувачки, нивната врска не е тешко да се разбере. Многу луѓе ги мешаат ISO 27001 и ISO 27002 со британскиот стандард (BS) 7799, но иако се слични, тие не се исти. Важно е да се напомене дека голем дел од работата во оваа област започнала и се развивала врз основа на BS 7799, пред да биде изменет и одобрен како ISO стандард. Она што го имаме денес е резултат на таа почетна работа комбинирана со придонесот и учеството на многу земји.

ISO/IEC 27001 е меѓународен стандард кој поставува барања за креирање, структура и управување со ISMS (систем за управување со безбедноста на информациите). Овој стандард е една од поважните одговорности на функцијата на CISO бидејќи одржувањето, имплементацијата, сертификацијата и ресертификацијата се активности во кои е вклучен CISO, често како главен одговорен или како посредник помеѓу, на пример, надворешна компанија за сертификација и организација.

ISO 27001 содржи пет главни области, кои често се нарекуваат „делови од 4 до 8“. Овие области вклучуваат: ISMS, менаџмент одговорност, ISMS внатрешни ревизии, управување со преглед на ISMS и подобрување на ISMS. Овие четири делови ѝ овозможуваат на организацијата да креира програмска структура или ISMS. Повеќето професионалци за безбедност на информации се запознаени со ISO 9001, кој се занимава со системи за управување со квалитет. ISO 27001 може да се смета како слична структура, но во контекст на безбедноста на информациите. Може да се визуелизира како чадор. ISO 27001 го обезбедува горниот слој на дефинирање како да се документира, организира, зајакнува, ревидира, управува и подобрува програмата за безбедност на информации. Со други зборови, ISMS е структура на организацијата за управување со луѓе, процеси и технологија. Ова поглавје ќе даде информации за стандардите, но нема да навлегува во детални описи или списокот на контролни цели.

ISO 27002 обезбедува контролни цели со релевантни законски, регулаторни или деловни барања кои се однесуваат на организација за безбедност на информации. Постојат десет различни области кои ISO 27002 ги опфаќа:[16]

1. безбедносна политика
2. безбедносна организација
3. класификација и контрола на средствата
4. безбедност на персоналот
5. физичка и еколошка контрола
6. управување со комуникациите и операциите
7. контрола на пристап
8. развој и одржување на системот
9. управување со деловниот континуитет
10. усогласеност.

Заедно со правните, регулаторните и деловните барања на организацијата, овие контролни цели обезбедуваат основа за ISO 27001 ISMS (Систем за управување со безбедноста на информациите). Ако го погледнеме Анекс А на стандардот ISO 27001, ќе забележиме дека контролните цели од стандардот ISO 27002 се повторуваат. Кога менаџерот за безбедност, или практичар, сака да ја потврди програмата на неговата организација дека е усогласена со ISO 27002, тоа всушност го постигнува со сертификација според критериумите дефинирани во ISO 27001. Ова може да изгледа збунувачки, но треба да се разбере дека целта е да се покаже имплементацијата на применливите ISO контроли 27002 (исто така Анекс А на стандардот ISO 27001), и ISMS развиен според ISO 27001 (општи барања), што обезбедува начин да се постигне ова.

Дел 4 ги опфаќа барањата за развивање, имплементирање, управување и подобрување на ISMS. Еден од првите чекори во развојот на ISMS е да се дефинира опсегот. Овој опсег може да се заснова на физичка локација, функција, организациска култура, околина или логички граници. За да се поедностави, многу

[16] David Kim and Michael G. Solomon: „Fundamentals of Information Systems Security“ Burlington, USA, 2018.

организации користат физички или логички граници. Опсегот вклучува физички, технички, информациски и програмски елементи и човечки ресурси. Овде ќе погледнеме малку подлабоко во концептот на опсегот, бидејќи тој е клучен концепт во безбедноста на информациите и ревизијата.

Кога развивате програма за безбедност на информации базирана на ISO 27001, без цел за сертификација, опсегот ќе биде местото каде што ќе утврди дека одредена програма за безбедност на информации е применлива. На пример, може да станува збор за компанија со повеќе одделенија. Опсегот може да ја вклучи само поделбата за која CISO е одговорен, но не и другите или матичната корпоративна структура. Треба добро да се размисли за опсегот во однос на опсегот на контрола, што е клучно за успехот на која било програма. Може да се избере да се искористат предностите на градењето програма базирана на ISO 27001 за да се прошират постоечките контроли за конзистентност или управување со ризик.

Ако се креира простор за сертификација, има неколку важни работи што треба да се земат предвид:

1. Која е вредноста на содржината на доменот дефинирана со опфатот на организацијата?
2. Дали има опсег на контроли на тој домен?
3. Кои се улогите и одговорностите на лицата поврзани со тој домен?
4. Кои логички и физички граници може да се применат за да се дефинира тој домен?
5. Кои исклучоци постојат?
6. Дали саканиот опсег е разумен за сертификација?

Кога се одредува вредноста на содржината, постојат многу формули што може да се користат. Некои се засноваат на мерливи вредности, како што е паричната вредност на опремата. Другите се засноваат на ризик или влијание врз деловното работење (можност за големи деловни пореметувања поради

недостапност итн.). Честопати комбинацијата од овие пристапи се покажува како најуспешна.

Распонот на контрола е клучен концепт поврзан со успешното определување на обемот. Неопходно е да се анализира на што се има директна контрола, на што може да се влијае или на што не може да се влијае. Опсегот на сертификација обично се однесува на областите врз кои нема контрола или има ограничено влијание преку договор за ниво на услуга, меморандум за разбирање, документ за одговорност или други методи. Обидот да се создаде опсег со мала или никаква контрола можеби не е мудра идеја и може да доведе до фрустрација поради неефикасна програма или неуспешен обид за сертификација.

Во рамките на опсегот постојат улоги и одговорности кои треба да се објаснат и разберат за да се избегне преклопување и дуплирање. Треба да се додели одговорност за управување со ISMS, како и одговорност за активностите што го сочинуваат секојдневното функционирање на системот. Користењето на дијаграмот RACI (каде што задачите се поделени во четири типа на улоги: одговорен, одговорни, консултиран, информиран) или матрица за одговорност е одличен начин за јасно прикажување на сите овие информации.

Може да се применат физички и логички граници за да се дефинира каде постои опсегот и исто така може да помогне да се разјасни опсегот на контрола. Овие граници може да бидат ѕидови, подови, огради итн. (физички граници) или виртуелни локални мрежи, сегменти или филтрирани порти (логички граници). Ова е особено важно при подготовката на опсегот за центарот за податоци. Влезните и излезните точки, физички и логички, може да се идентификуваат и треба да се испитаат и документираат.

Друг важен чекор во опфатот е документирањето на исклучоците. Амандманите се сè што не е применливо според контролните цели во Анекс А. Барањата во деловите 4 до 8 се токму тоа – задолжителни. Исклучоците не можат да се документираат за овие области. Еден начин да се справите со ова е да креирате листа за развој или да имплементирате процес кој ги организира овие

исклучоци. Може да се дојде до ситуација кога треба да се бранат причините за исклучоци за време на ревизија.

Најважното прашање на кое треба да се одговори е последното прашање поставено претходно: Дали опсегот е разумен за обидот за ревизија на сертификација? Многу организации, кога првпат ќе решат да одат по овој пат, одлучуваат да ја сертифицираат целата организација. Иако ова може да биде успешно во помалите организации со силни контроли, тоа не е разумно за повеќето организации. Искуството покажа дека успешната сертификација се заснова на програма која е дизајнирана и имплементирана на ниво на претпријатие, но во која спецификите на сертификацијата се применуваат на ресурсите кои имаат најголема вредност за организацијата. Исходот е ситуација кога организацијата може да има корист од програмата за безбедност на информации што се развила (ISMS на организацијата) и сертификатот што е меѓународно признат и се применува на највредните ресурси или услуги. Најдобрата практика е да се разгледа опсегот на сертификација што има смисла. Некои од прашањата кои можат да водат се: Дали организацијата е давател на услуги? (размислување за потврдување на делови од организацијата кои ги обезбедуваат овие услуги на клиентите); Дали организацијата е финансиска институција? (размислување за сертификација на услуги или центри каде што се чуваат, користат и складираат информациите за клиентите). Ако треба да се сертифицира на ниво на претпријатие, препорачливо е да се поделат напорите на подрачја со кои може да се управува и да се примени истиот процес на определување на обемот на нив.

Дефинирањето на политиката ISMS значи токму тоа, пишување на политиката. Шаблоните за политики се популарни појдовни точки, но треба да се внимава кога се користи готов документ - ако целта е сертификација или создавање на ефективна програма. Секоја добра политика треба да биде темелно обмислена. Премногу често спецификациските компоненти (на пример, минимум 128-битна шифрирање) се вметнуваат во политиката и тоа ја спречува управливоста. Никој не сака да оди во одборот на директори секогаш кога ќе

треба да ги ажурира техничките поставки. Најдобра практика е кога одредена „политика“ одговара на културата и околината на одредена организација. Потребно е време за да се осигура дека не се создава нереална рамка за политика што не може да биде прифатена и да се осуди организацијата на неуспех.

Управувањето со ризик симболизира различни работи за различни луѓе, но секој треба да ја цени флексибилноста и пријателскиот пристап за бизнис што го нудат ISO стандардите. Од перспектива на ISO стандардите, поголема загриженост е тоа што има организациски пристап кон ризикот, критериумите или праговите и методологијата што може да се повтори. Постојат информативни референци (опционално, информативни) кои се директно применливи. Две од нив се:

1. ISO/IEC 27005 Information Technology – Security Techniques – Information Security Risk Management;
2. ISO/IEC TR 13335-3, Information Technology – Guidelines for the Management of IT Security – Techniques for the Management of IT Security.

Се препорачува овие документи да се користат како извор на информации. По спроведувањето на темелна проценка на ризикот, треба да се има многу добра идеја за тоа каде се важните ризици, какви контроли постојат и кој е преостанатиот ризик. Прифаќањето или преносот се исто така одобрени методи за управување со ризик.

Следење и одржување на ISMS – Овие барања гарантираат дека активно се управува со ISMS. Не е доволно само да се разбере што се поседува, туку треба и редовно да се следи. Неопходно е да се провери дали има грешки или безбедносни настани, да се прегледаат перформансите и да потврдите дека сè уште се усогласени со целите. Мора да се посвети време на подобрување на ISMS и истовремено да се осигура дека се идентификувани проблемите или дека се решени недостатоците.

Документите и записите мора да се одржуваат, како што е наведено во преостанатите барања од Дел 4. За ова се наведени одредени типови документи и барања за контрола на документи. Целата важна документација треба да се чува на лесно достапно место, притоа да се одржува интегритетот на тие информации. За таа цел често се користи систем за управување со содржина, портал или веб-сервер. Сепак, не постои услов овие записи да бидат електронски. Во сертификацијата, посебно треба да се обрне внимание на Дел 4.3.1, бидејќи ќе треба овие ставки да бидат на располагање и да бидат подготвени за ревизорите. Ова се основните категории на реални документи кои го сочинуваат ISMS.

Внатрешната ревизија е уште една задолжителна функција, чии барања се опишани во Дел 6. Тоа е функцијата што проверува дали ISMS е во согласност со барања на организацијата. Очекуваните аспекти поврзани со прегледот се опфатени во овој дел, вклучувајќи распоред, перформанси и барања за санација на дефекти. Внатрешниот преглед е важен процес бидејќи овозможува идентификација и решавање на проблемите помеѓу циклусите на ревизија на телата за сертификација. Ако се најде на проблем, истиот може да се поправи, но мора да се пријават сериозни проблеми или неусогласеност.

Прегледот на менаџментот е предмет на Дел 7. Овој дел е директно поврзан со моделот PDCA (планирај, направи, проверувај, дејствувај), кој е основа за сите ISO ISMS стандарди. Постапките на организацијата, промени во околината, мерењата и други работи се прегледани во овој дел. Се состои од два дела, едниот се занимава со „влезови“, а другиот се занимава со „излези“. Делот „излез“ помага да се документираат постапки, размислувања и резултати. Овие типови записи се важни за да се прикаже активното управување со ISMS.

Последниот дел, Дел 8, се занимава со подобрување на ISMS. Често се споредува со систематско подобрување на процесот, што во основа е тоа. Делот 8 може да се поедностави на следниов начин: корективни дејства, кои се фокусираат на идентификуваните проблеми и превентивни активности, преземени за да се избегнат негативни настани и влијанија. Честопати овие превентивни дејства се последица на прегледи на корективни дејства.

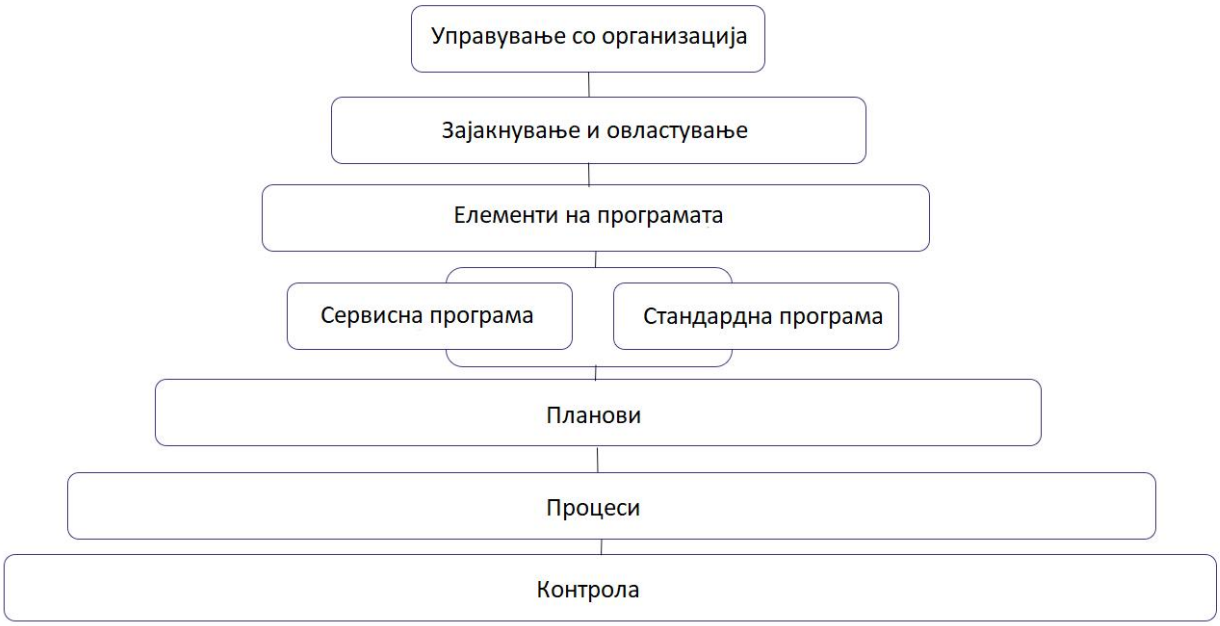
Ова треба да обезбеди основно разбирање за тоа што е покриено со општите барања на ISO 27001. Како што може да се види, постојат различни стандарди и документи кои заедно придонесуваат за ефективноста на ISMS.

Во контекст на активностите на CISO, групата стандарди ISO 27000 најчесто припаѓа на активностите и одговорностите кои се припишуваат на таа функција во рамките на една организација. Стандардите на групата ISO 27001 се предмет на постојани промени и дополнувања, според денешната динамика. ISO 27000 е стандард дизајниран да научи и информира за тоа што е семејството на документи 27000 и како тие се поврзани едни со други. Исто така, содржи терминологија специфична за оваа група ISO стандарди.

1. ISO 27002 (од април 2007 година) во моментов познат како ISO 17799;
2. ISO 27003 е упатство за имплементација на ISO 27001, фокусирајќи се на општите барања (од 4 до 8);
3. ISO 27004 собира мерења и метрика од ISMS (Information Security Management System);
4. ISO 27005 опфаќа управување со ризик во однос на ISO 27001 и ISMS;
5. ISO 27006 се занимава со барањата за телата за акредитација (лица кои вршат ревизија на сертификација).

По потреба ќе се додадат дополнителни стандарди во групата 27000 за поддршка на севкупните стандарди за системот за управување со безбедноста на информациите. На сликата 2 се наведени односите и функциите на стандардот.

Иако овие стандарди ја покриваат безбедноста на информациите, тие не постојат изолирано од другите. Има доста други стандарди кои се комплементарни на оваа група, на пример ISO 20000 (управување со ИТ услуги), кој е комплементарен и се вкрстува со ISO 27001 и ISO 27002.



Слика 2: Референтен модел на управување со безбедноста на информациите

Извор: Изработка на авторот

CISO експертите често се прашуваат како стандардите како COBIT (Control Objectives for Information and Related Technology) и Националниот институт за стандарди и технологија (NIST) се однесуваат на стандардите на ISO. Иако ISO 27001 нема директно да наложи блокирање на одредена порта на заштитниот ѕид, тоа ќе бара разбирање на ризичното опкружување и примена на соодветни контроли, односно сугестивно ќе доведе до заклучок дека блокирањето на таа порта е пожелно. Важно е да се разбере дека стандардите се пооперативни, ISO стандардите се занимаваат со прашањата за тоа како менаџерите за безбедност (вклучувајќи ги и CISO) всушност управуваат со безбедноста на информациите. Ова помага на тактичко и стратешко ниво, обликувајќи ги процесите на донесување одлуки кои влијаат на оперативното ниво. Оперативните барања произлегуваат од законски, регулаторни или деловни барања. Кога овие елементи се правилно комбинирани, резултатот е сеопфатна програма за безбедност на информациите.

Понатаму, секој CISO мора да ја разбере и да ја одвои потребата од доброволната одлука на раководството на организацијата за утврдување на потребата за сертификација врз основа на безбедноста на информациите.

Овие причини вклучуваат барање начини за обезбедување докази за активности, должно внимание, одговорност и усогласеност со регулативата. ISMS, според ISO 27001, јасно ги исполнува барањата на Sarbanes-Oxley Act и други слични закони во Соединетите Американски Држави или ширум светот, преку процесот на идентификација и исполнување на барањата. Други го гледаат како патоказ кон иднината, разбирајќи каде идните барања можат полесно да се исполнат со постоечка докажана и приспособлива структура.

Со воспоставен ISO 27001 ISMS, организациите добиваат основна структура за управување со безбедноста на информациите, која може да се прилагоди за да ги исполни идните барања. Оваа докажана и прилагодлива структура им овозможува на организациите полесно да се приспособат на променливите барања во областа на безбедноста на информациите и успешно да ги исполнат идните барања. Бидејќи безбедноста на информациите постојано се развива и се менува, организациите кои имаат имплементирано ISO 27001 ISMS имаат предност, бидејќи тие веќе имаат структурирана и тестирана рамка. Оваа структура им помага на организациите побрзо и поефикасно да одговорат на новите барања, бидејќи тие веќе имаат процеси, контроли и практики кои можат да се прилагодат и применат на нови сценарија.

Дополнително, ISO 27001 ISMS обезбедува рамка за постојано подобрување. Преку процесот на мониторинг и ревизија, организациите можат да ги идентификуваат недостатоците, ризиците и новите барања и да ги решат во согласност со целите за подобрување на безбедноста на информациите. Така, ISO 27001 ISMS делува како водич за иднината, овозможувајќи им на организациите да бидат подготвени за промени и да развијат безбедносни практики за да ги исполнат идните барања на најдобар можен начин.

Јасен пример за лидерство во индустријата покажуваат организации како Fujitsu, Premier Bankcard и Federal Reserve Bank of New York, кои беа меѓу првите во светот кои ги потврдија своите системи за управување со безбедноста на информациите според ISO 27001, кога стандардот беше објавен во ноември 2005 година. Различни организации прават напори за имплементација на ISMS за да ја забрзаат зрелоста во нивниот бизнис, притоа одржувајќи флексибилност. Сертификацијата ISO 27001 им дава на организациите признание за нивната посветеност и усогласеност со меѓународно признатите стандарди за безбедност на информациите. Организациите кои се меѓу првите што ги потврдија своите системи за управување со безбедноста на информациите според ISO 27001, покажуваат проактивност и посветеност на индустријата за обезбедување на високо ниво на безбедност на информациите.

Спроведувањето на ISMS според ISO 27001 им овозможува на организациите да воспостават сеопфатна рамка за управување со ризик - идентификување, оценување и управување со безбедносните закани. Оваа рамка им помага на организациите да изградат култура на безбедност на информации и постојано да се подобруваат.

Сертификацијата ISO 27001, исто така, покажува дека една организација сериозно ја сфаќа безбедноста на информациите и има систематски пристап кон управувањето со безбедноста на информациите. Ова може да обезбеди доверба на засегнатите страни, клиентите и партнерите, покажувајќи дека организацијата применува најдобри практики во областа на информацискатa безбедност.

Искористувањето на напорите за имплементација на ISMS им овозможува на организациите да го забрзаат созревањето во областа на безбедноста на информациите, применувајќи докажани упатства и практики кои се дел од стандардот ISO 27001. Во исто време, организациите ја задржуваат флексибилноста и можат да ги приспособат своите пристапи според нивните специфични потреби и деловни услови.

Севкупно, сертификатот ISO 27001 им обезбедува на организациите придобивки во однос на препознавање на нивната посветеност на безбедноста на информациите, подобрена деловна репутација и стекнување доверба од засегнатите страни. Сертификацијата, исто така, ги поддржува организациите во развојот на зрели практики за управување со безбедноста на информациите, што е од клучно значење за успехот во денешното дигитално опкружување.

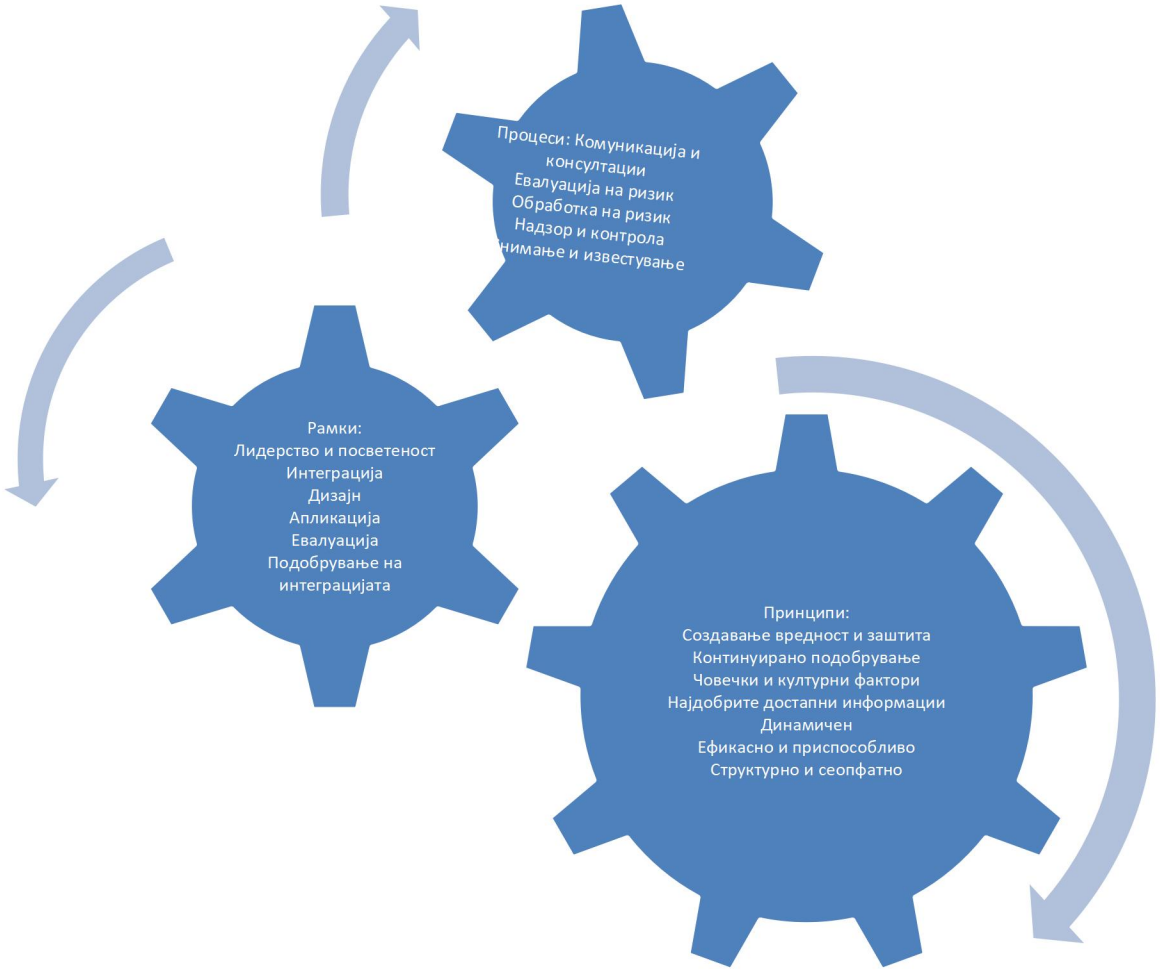
Една од клучните причини зошто ISO 27001 е стандард кој го фаворизира деловниот модел на организацијата е фактот што тој е заснован на ризик и на тој начин нема ригидност што може да го парализира бизнисот. CISO може да избере кои цели да ги следи, во зависност од ризикот, законот и регулаторните барања.

3.2. Управување со ризикот од безбедноста на информациите во согласност со стандардот ISO/IEC 31000

Како што е наведено во претходните поглавја, управувањето со ризикот е една од клучните задачи и одговорности на секоја функција на CISO. Управувањето со ризикот, односно проценката на ризикот за безбедноста на информациите е една од задолжителните активности за успешно сертифицирање според стандардот ISO 27001 и е задолжително да се спроведе.

Ризикот за безбедноста на информациите е комбинација од веројатноста за појава на несакан настан, односно закана што ја користи ранливоста на информацискиите средства и негативните последици од овој настан врз доверливоста, интегритетот и достапноста на податоците. Информацискиите средства, односно ресурсите, се сите средства што ги користи организацијата за да ги постигне своите деловни цели, како што се: инфраструктура, хардвер, софтвер и податоци. Управувањето со ризик од секаков вид се врши често и интерактивно и служи како помош за раководната структура на организацијата при усвојување на стратегија, постигнување цели и донесување аргументирани одлуки.

Според стандардот, за ефикасно и доследно управување со ризикот, постапката мора да се состои од меѓусебно зависни принципи, рамки и процеси[17]. На сликата 3 е прикажана сеопфатноста.



Слика 3: Презентирање на принципите, рамката и процесот на управување со ризик во согласност со стандардот ISO/IEC 31000

Извор: Образботка на авторот според International Organization for Standardization – ISO: ISO 31000:2018 Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 18.6.2024.

[17] International Organization for Standardization – ISO: ISO 31000:2018 Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 18.6.2024.

Управувањето со ризикот од безбедноста на информациите е сеопфатна процедура, која ја потврдува деловната оправданост на изборот на пропишаните мерки и стандарди со цел да се обезбеди доволно ниво на безбедност. На пример, телата и правните лица кои се занимаваат со класифицирани податоци, се обврзани да управуваат со ризикот од безбедноста на информациите, да прават континуираната проценка и избор на ризик во согласност со меѓународните стандарди и норми, како што се ISO/IEC 27005, ISO/IEC 31000, COSO итн. и да се спречи нивно неовластено обелоденување или губење.[18]

Процесот на управување со ризикот за безбедноста на информациите според стандардот ISO/IEC 31000 се состои од следните активности:

1. комуникација и консултации (eng. communication and consulting);
2. определување на опсегот, контекстот и критериумите (eng. scope, context and criteria);
3. проценка на ризик (eng. risk assessment)
    a) идентификација на ризик (eng. risk identification),
    b) анализа на ризик (engl. risk analysis)
    c) проценка на ризикот (eng. risk evaluation);
4. третман на ризик (eng. risk treatment);
5. следење и контрола (eng. monitoring & review);
6. евидентирање и известување (eng. recording & reporting).

3.2.1. Комуникација и консултации

Оваа активност им помага на сите главни надворешни и внатрешни чинители на организацијата или правното лице во разбирањето на ризиците, основата за одлучување и причините поради кои треба да се спроведат одредени активности. Главната цел е да се обезбедат различни ставови и експертиза при утврдување на критериумите за проценка на ризикот. Размената на податоци во комуникацијата и консултациите мора да биде заснована на факти, и да биде

[18] International Organization for Standardization – ISO: ISO 31000:2018 Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 18.6.2024.

навремена, релевантна, точна и разбирлива и постојана во текот на сите активности на процесот на управување со ризик.

На почетокот на процесот на управување со ризик, потребно е да се постави обемот на активностите што треба да се спроведат и да се усогласат целите на процесот со целите на организацијата или правното лице, притоа разбирајќи го контекстот во кој телото или работи правно лице.

3.2.2. Опсег, контекст и критериуми

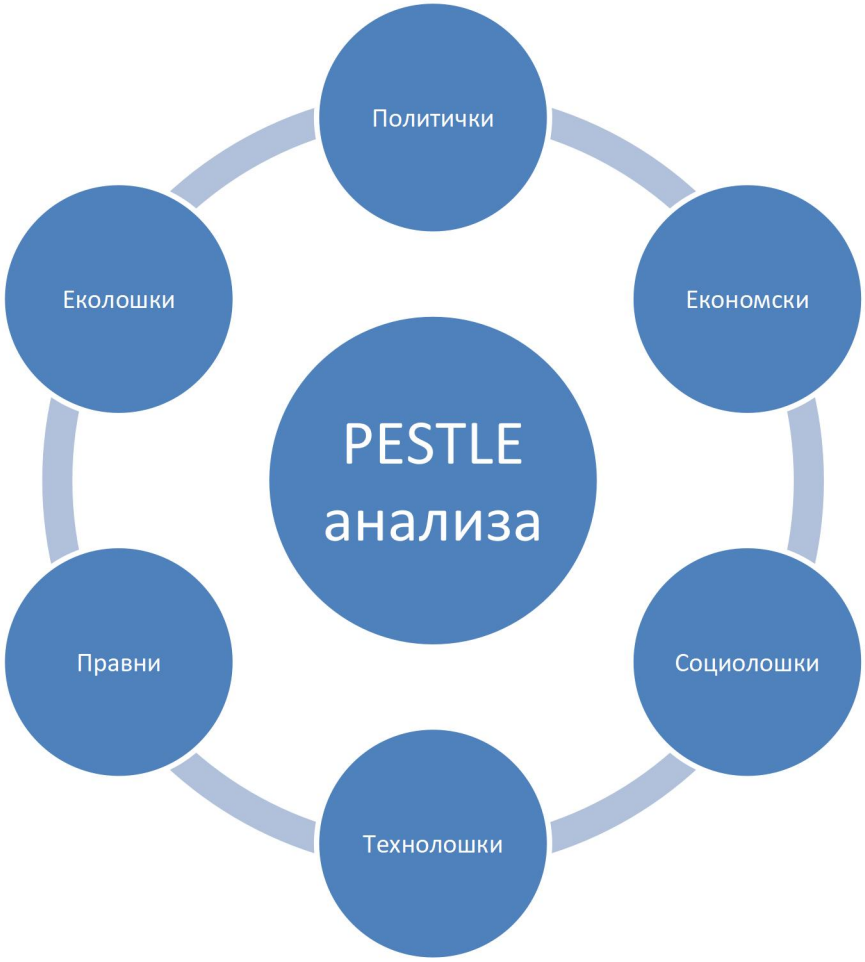
Целта на оваа активност е да се прилагоди процесот на управување со ризик на карактеристиките на организацијата или правното лице со цел ефикасно да се спроведе проценката на ризикот и соодветно да се обработи ризикот. На почетокот на самиот процес на управување со ризик, потребно е да се објасни обемот на активностите што треба да се спроведат и да се усогласат целите на процесот со целите на организацијата, но во контекстот во кој работи организацијата. За да се постигне разбирање на контекстот, неопходно е да се препознаат, анализираат и да се земат предвид надворешните и внатрешните фактори, односно пазарот на кој работи организацијата. Неопходно е да се препознае како тие се поврзани со активностите и процесите за управување со ризик. Анализата PESTLE[19] се користи за идентификување на надворешни фактори, а SWOT[20] анализата се користи за идентификување на внатрешните влијанија.[21][22]

[19] PESTLE, или PEST анализа, е воведена во 1967 година како метод за откривање и квантифицирање на фактори кои се надвор од контрола на компанијата и влијаат на нејзиното работење. Зборот PESTLE е акроним од почетните букви на зборот, кои во англискиот јазик означуваат политички (eng. Political), економски (eng. Economic), социолошки (eng. Social), технолошки (eng. Technological), правни (eng. Legal) и фактори на животната средина (eng. Environmental).

[20] SWOT анализата или SWOT матрицата е една од најпознатите и најосновните техники на стратегиска анализа во областа на деловните науки, воведена во 1969 година. Со цел да се стекне стратешко знаење и да се преземат вистинските мерки и активности за постигнување на деловните и другите цели на компанијата, се анализираат и се идентификуваат нејзините четири аспекти: силни страни (S,скратено eng. Strengths), слабости (W, скратено eng. Weaknesses), можности (O, кратенка за eng. Opportunities) и закани (T, кратенка за eng. Threats).

[21] City University of Seattle: Business & Management, https://library.cityu.edu/researchguides/business/swot, 21.5.2024.

Анализата на PESTLE, прикажана на слика 4, ги зема предвид политичките, економските, социолошките, технолошките, правните и еколошките фактори, без разлика дали ја разгледуваме организацијата на меѓународно, регионално или локално ниво. Покрај опишаните фактори, надворешните влијанија можат да се однесуваат и на договорните обврски, перцепцијата на клучните чинители или организацијата, трендовите и слично.



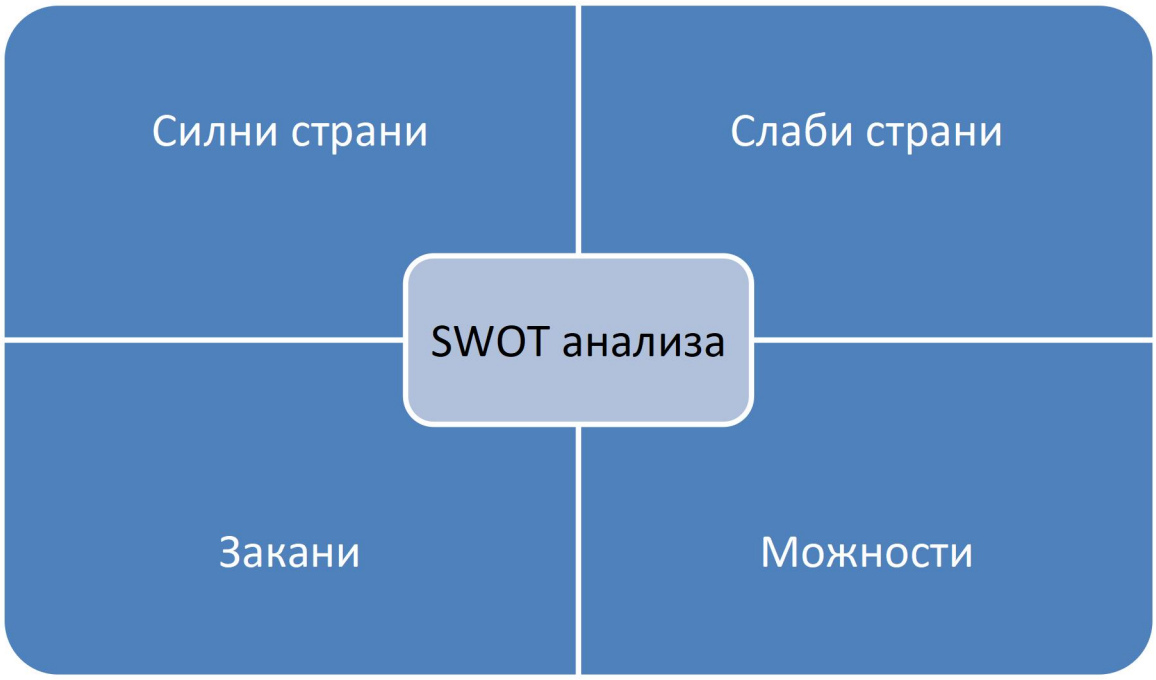
Слика 4: PESTLE анализа

Извор: Изработка на авторот според de Bruin, Lars: Scanning the Environment: PESTEL Analysis, https://www.business-to-you.com/scanning-the-environment-pestel-analysis/, 21.5.2024.

[22] de Bruin, Lars: Scanning the Environment: PESTEL Analysis, https://www.business-to-you.com/scanning-the-environment-pestel-analysis/, 21.5.2024.

Една од најпознатите и во исто време основна техника на стратегиска анализа, претставена уште во 1969 година во доменот на бизнис-науката, е SWOT анализата, односно SWOT матрицата. За да се стекне стратешко знаење, за да може да се преземат соодветни мерки и активности за постигнување на деловните и другите цели на организацијата, анализирани се четири аспекти:

1. јаки страни (S, кратенка од eng. Strengths),
2. слабости (W, скратено од eng. Weaknesses),
3. можности (O, кратенка од eng. можности),
4. закани (T, кратенка од eng. Threats).



Слика 5: SWOT анализа

Извор: Изработка на авторот според Schoenbeck, Dave: Essential Ingredients of a Small Business SWOT Analysis, , https://daveschoenbeck.com/essential-ingredients-small-business swotanalysis/, 21.5.2024.

Покрај тоа, се анализираат: визијата, мисијата, вредностите на организацијата (човечки ресурси, технологии, податоци, информациски систем итн.), методот на циркулација на податоци, организациската структура и култура, стратегијата, целите, политиките, стандардите и препораките усвоени од организацијата. SWOT анализата може да се користи за да се идентификуваат надворешните и внатрешните влијанија. Во оваа ситуација, силните и слабите страни на организацијата се класифицирани како внатрешни влијанија, додека можностите и заканите се класифицирани како надворешни влијанија.[23] На слика 5 е прикажан аспект на SWOT анализата.

На крајот од оваа активност, потребно е да се утврдат критериуми, односно вредности на ризик, кои се прифатливи или неприфатливи за организацијата во контекст на целите. Покрај самите цели, при утврдувањето на критериумите, потребно е да се земат предвид и вредностите, постоечките политики, обврските и мислењата на клучните чинители, како и техниката што ќе се применува при проценката на вредноста на нивото на ризик.

Иако тие се одредуваат на почетокот на процесот на управување со ризик, одредниците треба систематски да се ревидираат и, доколку е потребно, да се менуваат за време на траењето на процесот. Според поставените критериуми, во крајна линија, за секој поединечен ризик се носи одлука како да се обработи. Пример за стандардните критериуми и опсегот на вредности добиени со модифицирано-квантитативната техника е прикажан во табела 2.

Табела 2: Пример за критериуми за прифаќање ризици за безбедноста на информациите

Опсег на вредности	Ниво на ризик	Опис на ризикот
1-20	Низок	Ризикот е доволно мал, така што не е

[23] Schoenbeck, Dave: Essential Ingredients of a Small Business SWOT Analysis, , https://daveschoenbeck.com/essential-ingredients-small-business swotanalysis/, 21.5.2024.

		потребно да се применуваат дополнителни контроли за мали или занемарливи штети, односно за веројатноста за реализација на заканата.
21-45	Среден	Ризикот е на средно ниво, и потребно е да се планира начинот на обработка за појава на значителни штети, односно веројатноста за реализација на заканата.
46-75	Висок	Ризикот е на високо (критично) ниво, и потенцијалната штета може да го загрози работењето на организацијата, односно реализацијата на заканата е речиси сигурна во период од една година.

3.2.3. Евалуација на ризик

Во контекст на безбедноста на информациите, ризикот за одреден ресурс или средство се проценува земајќи ја предвид неговата вредност (eng. Assets Value – AV), ранливоста на тој ресурс (eng. Vulnerability – V), закани кои можат да ја искористат таа ранливост (eng. Threat - T), веројатноста за реализација на заканата (eng. Probability – P) и последиците (eng. Impact – I) кои можат да настанат доколку се реализира одредена закана. Математичкиот ризик е функција од горенаведените варијабли:

$$R=f(AV,\ V,T,R,I)^{24} \quad (1)$$

За да може резултатите од проценката на ризикот да се сметаат за валидни, самата постапка мора да ги исполнува следниве критериуми:[25]

[24] Šegudović, Hrvoje: „Prednosti i nedostaci metoda za kvalitativnu analizu rizika“,Infigo IS d.o.o., Zagreb, 2006
[25] Idibem

1. уникатност
2. сигурност
3. објективност
4. повторливост.

Проценката на ризикот е најважниот, најчувствителниот и најдолгиот дел од процесот на управување со ризикот, кој содржи три активности: идентификација, анализа и евалуација на ризиците.

Идентификацијата на ризикот се врши со пронаоѓање, препознавање и опишување на сите можни ризици кои би можеле негативно да влијаат на постигнувањето на целите на организацијата и нивните извори, односно ранливости и закани поврзани со одредена ранливост, без разлика дали се под нејзино директно влијание или не. Од суштинско значење е да се идентификуваат сите можни извори на ризик, бидејќи оние ранливости и закани кои не се идентификувани, ќе бидат исклучени од понатамошниот процес на управување со ризик. За време на идентификацијата, организацијата може да примени различни алатки и техники, како што се: преглед на системот, анализа на документација, интервјуа, прашалници, безбедносно тестирање, тестирање со пенетрација и слично - прилагодени на сопствените цели и услови - и да користи претходно искуство со ризици.[26] За идентификација на ранливости и закани, од суштинско значење е собраните информации да бидат релевантни и ажурирани. Во оваа активност потребно е да се вклучат сите клучни учесници кои се адекватни во своето знаење за областа за која се спроведува.

По завршената фаза на идентификација на ризиците и нивните извори, следи процедурата на анализа на ризик со цел да се добие разбирање за природата и карактеристиките на идентификуваните ризици. Постапката вклучува идентификација, распределба или проценка:[27]

1. група на средства

[26] Idibem
[27] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection Guidance on managing information security risks https://www.iso.org/standard/80585.html, 18. 5. 2024

2. вредности на нивото на ризик
3. нивоа на ранливост на средствата
4. сопственост на имот
5. ефективност на претходно применетите мерки
6. вредности на имотот
7. веројатности за појава на закани.

Во пракса, средствата често се групирани според постоењето на исти или слични карактеристики и барања за безбедност на информациите и ефектите од слични видови закани. Во табелата 3 е прикажана една таква групација, а терминот „сопственик“ во овој контекст треба да се сфати како оној кој има одговорност за користење, развој и одржување на безбедноста и имотот, а не како некој што има сопственички права. Во оваа фаза, исто така, од суштинско значење е да се идентификуваат применетите мерки. Идентификувањето на мерките помага да се процени ефективноста и оптимизацијата на постоечките мерки. Проценката на ефективноста на утврдените мерки се врши со анализа на постапката со која тие го намалуваат нивото на ранливост на средствата или веројатноста за реализација на закана.

Табела 3: Пример за каталог на средства со ранливости и закани

Група на средства	Ранливост	Закани
Хардвер и инфраструктура	Употреба на опрема без соодветна TEMPEST заштита	Шпионажа и прислушкување
	Несоодветно сместување и физичка заштита	Физичка манипулација или кражба на имот
	Несоодветна климатизација и/или напојување	Неисправности, дефект или уништување на хардверот и недостаток на сервис
	Несоодветно одржување	

	со неуспех да се одделат тест и производствени средини	
	Несоодветен капацитет (eng. singl point of failure)	Нефункционалност или преоптоварување на услугата
		Губење на податоци
Софтвер	Несоодветно управување со зафати за надградба или одржување	Дефекти, неисправности и недостапност на услугите
		Познати пропусти, малициозен софтвер
		Привремена недостапност или трајно губење на податоци поради дејство на малициозен софтвер
	Неодвојување на средини за тестирање и производство	Дефекти, неисправности и недостапност на услугите
		Привремена недостапност или трајно губење на податоци поради дејство на малициозен софтвер
	Не постои антивирусен софтвер или антивирусните дефиниции не се ажурираат редовно	Познати пропусти, малициозен софтвер
		Привремена недостапност или трајно губење на податоци поради дејство на малициозен софтвер
	Несоодветна контрола и надзор на употребата	Неовластени дејства
	Неправилна конфигурација	

	Несоодветно управување со овластувањата	Неовластен пристап и истекување на податоци
Услуги и процеси	Несоодветно управување	Недостапност или неефикасност
	Несоодветна документација	Неправилно формулирани или извршени процедури
Податоци	Отсуство на правење резервни копии на податоци	Губење на податоци
	Несоодветно складирање на резервни копии на податоци	
	Неправилна размена или дистрибуција на податоци	Губење, истекување или манипулација со податоци
	Можност за изнесување на податоци	
	Неправилно уништување или бришење на податоци	
	Отсуство на шифрирање на безбедносно чувствителни податоци	Прислушување или откривање информации
	Неконтролирано изложување на печатени документи чувствителни на безбедност	Неовластен пристап до податоци
		Протекување податоци
	Презентација на податоци на екранот на компјутерот	Неовластен пристап до податоци
Просторни ресурси	Несоодветна заштита на просторот од несакано електромагнетно зрачење (TEMPEST)	Шпионажа и прислушување

	Несоодветен надзор на просториите	Физичка манипулација или отуѓување на имот
	Несоодветна контрола на пристапот до просториите	Нелегален пристап
		Губење или истекување на податоци
		Шпионажа или прислушување
	Несоодветна заштита на просториите од кражби	Кражби
	Несоодветна заштита од пожар	Пожар
	Чувствителноста на објектот на надворешни услови	Виша сила (време, удар на гром, поплава, земјотрес)
Човечки ресурси	Несоодветно управување	Недостапност или губење на персонал
	Несоодветен или необучен кадар	Работни грешки и неодговорност
	Недоволно образование од областа на информацискатa безбедност	Социјален инженеринг и шпионажа
	Незадоволен или несигурен персонал	Отуѓување или злонамерно уништување на имот
		Ширење неточни информации
	Несоодветна заштита на идентитетот и ингеренциите	Кражба на идентитет и неовластен пристап до услуги
	Неправилно ракување со имотот	Отуѓување на имот
		Губење или истекување на податоци

		Злоупотреба на правата за пристап
	Пристап до кадровски средства од трета страна	Губење или истекување на податоци
		Повреда на интегритетот на информацискиот систем

Извор: Авторот според ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection Guidance on managing information security risks https://www.iso.org/standard/80585.html, 18. 5. 2024

Најчестиот начин за одредување на вредноста на имотот се заснова на параметри, како што се:

1. куповна вредност, трошоците за замена или повторно создавање на имотот;
2. трошоците што би настанале поради губење на доверливост, интегритет и достапност на средствата;
3. губење на репутацијата.

Со избирање на еден или повеќе параметри, на средствата им се доделуваат соодветни нумерички вредности врз основа на проценките на сопствениците на информативни средства, ангажираните проценители или интервјуата со корисниците и системските администратори. Потоа следува одлука за тоа дали средството влегува во процедура за процена на ризик или не, врз основа на нумеричката вредност што му е доделена. Пример за проценка на податоците врз основа на трошоците или штетата предизвикана поради загуба, доверливост, комплетност и достапност е прикажан во табела 4.

Табела 4: Пример за одредување на вредноста на податоците врз основа на параметрите на CIA (Confidentiality Integrity Availability)

Нумеричка вредност	Ознака	Опис		
		Confidentiality	Integrity	Availability
1	Многу ниска	Јавно достапни информации	Промена која не предизвикува дополнителна работа или заостанати работи	Недостапност што не предизвикува заостанати работи
2	Ниска	Информации достапни за вработените	Промената предизвикува дополнителна работа или заостанати работи	Недостапност што предизвикува заостанати работи
3	Средна	Интерни информации за кои е потребно овластување	Промената предизвикува доцнење во работата и можна финансиска загуба	Недостапност предизвикува значителни оперативни проблеми и можна финансиска загуба
4	Висока	Информации за бизнис партнери	Промената предизвикува одредена финансиска загуба	Недостапност предизвикува одредена финансиска загуба

5	Многу висока	Деловна тајна	Промената предизвикува дополнителна работа или заостанати работи	Недостапност што предизвикува значителни проблеми и претставува можна финансиска загуба

Вредноста на ризикот може да се процени со користење на квалитативни и квантитативни методи. Секој од методите, без разлика на категоризацијата, поради своите недостатоци, не е погоден за управување со ризикот од безбедноста на информациите, поради што се предлага нивно комбинирање во модифицирана квалитативна техника.[28]

Модифицираната квалитативна техника се заснова на одредени претпоставки, кои се:[29]

1. секое средство има своја вредност;
2. ранливост може или не може да постои за поединечни средства (ако постои силна заштита и контрола);
3. ранливоста и заканите се меѓусебно зависни (ако има ранливост, постои и закана, а ако има закана, постои и ранливост);
4. заканата има веројатност која зависи од околностите;
5. заканата има можни последици чија големина зависи од околностите.

Ако ги земеме предвид сите горенаведени претпоставки, проценката на ризикот со помош на изменетиот квалитативен метод може да се претстави како

[28] Šegudović, Hrvoje: „Prednosti i nedostaci metoda za kvalitativnu analizu rizika“, Infigo IS d.o.o., Zagreb, 2006.
[29] Ibidem

производ на вредноста на имотот, веројатноста за појава на закана и ранливоста на имотот:

$$R = AV * P * V \quad (2)$$ [30]

Опсегот на вредности што може да го земе секој од наведените параметри е произволен. Пример за опсегот на вредностите на средствата е прикажан во табела 5, пример за опсегот на вредности на веројатноста за реализација на заканата е прикажан во табела 6 и пример за опсегот на вредности на ранливоста на средствата е дадена во табела 7.

Табела 5: Пример за опсег на вредност на имотот

	Нумеричка вредност	Ознака	Опис
Вредност на имотот	1	Многу ниска	Многу ниска вредност
	2	Ниска	Ниска вредност
	3	Средна	Средна вредност
	4	Висока	Висока вредност
	5	Многу висока	Многу висока вредност

Табела 6: Пример за опсегот на вредности на веројатноста за реализација на заканата

Опсегот на вредности на веројатноста за реализациј	Нумеричка вредност	Ознака	Опис
	1	Многу ниска	Многу мала веројатност за појава на закана
	2	Ниска	Ниска веројатност за појава на закана

[30] Šegudović, Hrvoje: „Prednosti i nedostaci metoda za kvalitativnu analizu rizika“,Infigo IS d.o.o., Zagreb, 2006

а на заканата	3	Средна	Средна веројатност за појава на закана
	4	Висока	Висока веројатност за појава на закана
	5	Многу висока	Многу висока веројатност за појава на закана

Табела 7: Пример за низа вредности на ранливост на средствата

Опсег на вредност на ранливоста на средствата	Нумеричка вредност	Ознака	Опис
	1	Ниска	Многу мала веројатност за појава на закана
	2	Средна	Мала веројатност за појава на закана
	3	Висока	Средна веројатност за појава на закана

Врз основа на равенката (2) и вредностите од табелите 5, 6 и 7, може да се пресмета дека најмалата проценета вредност на ризик $Rmin$ е еднаква на 1, максималната вредност на проценетиот ризик $Rmax$ 125 е еднаква на 125. Во табелата 8 е прикажува изменетата матрица за проценка на вредноста на ризикот со применетите критериуми за прифаќање ризик од табела 1.

Табела 8: Изменета матрица за проценка на вредностите на нивото на ризик

Закани и ранливост на средства	Нивото на веројатност да се реализира заканата	1	2	3	4	5

	Ниво на ранливост на средства	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
Вредност на средства	1	1	2	3	2	4	6	3	6	9	4	8	12	5	10	15
	2	2	4	6	4	8	12	6	12	18	8	16	24	10	20	30
	3	3	6	9	6	12	18	9	18	27	12	24	36	15	30	45
	4	4	8	12	8	16	24	12	24	36	16	32	48	20	40	60
	5	5	10	15	10	20	30	15	30	45	20	40	60	25	50	75

Врз основа на податоците добиени од извршената анализа на ризик, се врши проценка на ризикот со цел да се донесат одлуки за понатамошни активности. Одлуките се носат врз основа на споредба на нивоата на проценетите вредности на ризик со критериумите за прифаќање ризик на организацијата.[31] Одлуките може да резултираат со непреземање понатамошни активности за одредени ризици, разгледување на опциите за третман, преземање понатамошни активности, спроведување дополнителни анализи за подобро разбирање на ризиците, одржување на применетите мерки или преиспитување на целите на организацијата.

3.2.4. Обработка на ризик

Обработката на ризик е итеративен процес кој вклучува избор, планирање и примена на нови мерки, проценка на ефективноста на применетите мерки и донесување одлуки за прифатливоста на преостанатиот ризик. Дополнително, вклучува преземање понатамошни чекори во случај избраните и применетите мерки да не го постигнат посакуваниот ефект.[32]

[31] International Organization for Standardization – ISO: ISO 31000:2018 Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 18. 5. 2024.
[32] International Organization for Standardization – ISO: ISO 31000:2018 Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 18. 5. 2024.

Оттука, обработката на ризикот е постапка во која се одредува степенот на прифатливост на ризикот за секој проценет ризик, со цел да се прифати, намали или избегне.

3. Ризикот би можел да се прифати доколку настанатата штета би била помала од штетата што би била предизвикана со неизвршување на одредена активност.
4. Намалувањето на ризикот се врши со примена на безбедносни мерки за спречување на уништување, отуѓување, губење и неовластен пристап до класифицирани податоци.
5. Избегнувањето на ризик подразбира преземање организациски мерки со цел да се избегнат дејствија кои би можеле да предизвикаат ризик.

Одлуката за тоа како да се справи со преостанатиот ризик ја носи одговорното лице за управување со организацијата по обработката на ризикот. Кај деловните субјекти од корпоративниот свет најчесто се работи за извршен директор, главен извршен директор (CEO), додека во јавниот сектор најчесто е директор на одредена институција.

Покрај горенаведеното, ризикот може да се пренесе на трето лице, на пример, осигурителна компанија или добавувач, т.е. трето лице.[33]

При изборот на стратегија за управување со ризик, потребно е да се води сметка за ефективноста на мерките во остварувањето на целите на организацијата во однос на трошоците и посветеноста што мора да се преземат при нивната примена. Покрај економската пресметка, потребно е да се води сметка и за претходно преземените обврски и мислењето на клучните чинители на органот или правното лице. Исто така, изборот мора да биде во согласност со претходно утврдените критериуми за прифаќање ризик и со ресурсите со кои располага органот или правните лица.

Преостанатиот (резидуален) ризик е оној кој ги вклучува сите оние ранливости и закани за кои се смета дека не бараат дополнителна обработка во

[33] Ibidem

смисла на нивно намалување, а за кои е утврдено дека трошоците за спроведување на можни мерки не се профитабилни и за кои моментално не постои соодветна можност за обработка или за кои обработката не го постигнала посакуваниот ефект. Таквиот ризик мора да биде документиран, мора да биде формално прифатен од раководителот на органот или правно лице и мора да стане предмет на понатамошен надзор и контрола.

Резултатите од оваа активност обично се комбинираат во Планот за управување со ризик, фундаментален документ кој овозможува имплементација на управување со ризикот на информацискиот систем и кој одредува како, по кој редослед и во која временска рамка ќе се применат избраните мерки.[34]

Таквиот план мора да биде интегриран во документите за управување на организацијата и да им се достави на сите заинтересирани страни, а меѓу другото, треба да вклучува:[35]

1. ризици кои треба да се обработат
2. приоритет на обработка
3. избрани мерки за поединечни ризици
4. лица одговорни за спроведување на избраните мерки
5. ресурсите потребни за спроведување на мерките
6. ограничувања
7. датумите на почеток и крај на спроведувањето на избраните мерки.

3.2.5. Надзор и контрола

Може да се случи постапката за обработка на ризик да не ги постигне посакуваните ефекти и предизвици, непланирани и несакани последици без оглед на планирањето и дизајнирањето на самиот процес. Постојаниот надзор и наизменичното контролирање на процесот на управување со ризик и резултатите

[34] International Organization for Standardization – ISO: ISO 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, 18. 5. 2024.
[35] ibidem

што произлегуваат, треба да бидат дел од самата процедура и да се спроведуваат во сите нејзини фази, особено при обработката на ризикот, бидејќи обработката на поединечен ризик може да предизвика нов ризик, што треба да биде идентификуван и обработен според методот.[36]

3.2.6. Евидентирање и известување

Процесот на управување со ризик и резултатите од тој процес мора систематски да се евидентираат и да се известуваат наизменично. Целта на известувањето е сите заинтересирани чинители на организацијата во секое време да бидат информирани за важни факти и да помогнат во обезбедувањето информации неопходни за донесување одлуки. Одлуките што можат да се донесат врз основа на резултатите од проценката на ризикот за безбедноста на информациите и може да имаат значителни последици за сите процеси во организацијата, вклучувајќи ги и оние кои се критични за бизнисот. Евидентирањето, документирањето и јасното известување е неопходно за ефективно управување со ризикот на информацискиот систем.

4. Релевантно законодавство за безбедност на информации во ЕУ

Со отпочнување на процесот за полноправното членство на Република Македонија во ЕУ и последователните натамошни интегративни процеси, како што се влезот во еврозоната и Шенген, одлуките на Европскиот парламент и другите законодавни и регулаторни тела на Европската Унија, мора да станат дел од законодавството на Република Македонија. Овде ќе истакнеме некои од

[36] International Organization for Standardization – ISO: ISO 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, 18. 5. 2024.

важните закони и нивното влијание врз потребата од функцијата на CISO, како и нејзините одговорности и активности.

Некои од важните закони кои треба да се доенсат или изменат, како и одлуки и акти се:

1. Законот за критични инфраструктури
2. Одлуки за соодветно управување со информацискиот систем
3. Упатства за соодветно управување со ризиците на информацискиот систем на субјектот на супервизија
4. Закон за информациска безбедност
5. Закон за сајбер-безбедност на операторите на клучните услуги и давателите на дигитални услуги
6. Кривичен законик
7. Закон за електронски комуникации
8. Законско решение за спроведување на Општата регулатива за заштита на податоци.

Без оглед на тоа што поголемите и посериозни организации во својата структура имаат правни одделенија, во кои има експерти специјализирани за горенаведеното законодавство, функцијата на CISO, која не е дел од правната служба, треба да има свест и одредено разбирање за горенаведените закони и одлуки.

5. Опис на активностите и одговорностите на CISO

Во овој дел од трудот е даден преглед на студии на случај на пример на неколку различни ангажмани на менаџери за информациска безбедност во организации во Република Македонија, кои припаѓаат на различни сектори на економијата. Студиите на случај се примери и описи на активности и одговорности во изминатите пет години од времето на пишување на овој труд.

Времето и актуелноста на примерот е важен параметар за прикажување на оптимален преглед, бидејќи технологијата, безбедноста на информациите и информациите се динамични и многу променливи. Развојот на новата технологија е постојан процес, кој ја става легислативата, а потоа и регулативата, во позиција каде што постојано доцни, но и постојано се менува и се прилагодува на новото ниво на развој. Токму оваа заемно-консеквентна динамика ги прави динамични активностите и одговорностите на менаџерите за информациска безбедност.

5.1. Раководител на информатичка безбедност во технолошки компании

Постојат бројни фактори кои би можеле да се наведат, а кои одат во прилог зошто технолошките компании ја воспоставиле функцијата на CISO - менаџер за информациска безбедност во нивната организациска структура. Двата доминантни фактори се:

1. растечки тренд на бројот, сложеноста и потенцијалната штета на нападите врз информацискиот систем, како и
2. регулатива, како одговор на трендовите и либерализацијата на одредени сектори, како што се платните трансакции.

Директивата PSD, и особено нејзината ревидирана верзија, PSD2, донесе нови можности, кои технолошките компании вклучени во развојот на софтвер ги гледаа како можност за развој на апликации за финансиски увид или плаќање.

5.1.1. Ревидирана директива за платежни услуги

Ревидираната Директива за платежни услуги (PSD2) е водена од податоци и технологија и има за цел да ја зголеми конкуренцијата, иновативноста и транспарентноста на целиот европски пазар на плаќања, истовремено подобрувајќи ја безбедноста на онлајн плаќањата и пристапот до сметки.

Меѓу другото, Директивата пропишува правила за нови услуги што ги обезбедуваат трети лица даватели на платежни услуги (TTP) во име на корисниците на платежните услуги (PSU).

Услугите се како што следува:[37]

- Давател на услуги за иницирање плаќања (PIS, eng. Payment Initiation Service Provider), обезбеден од корисник на услуги (TTP, engl. Third Party Payment Service Provider), корисниците на платежните услуги (PSU, engl. Payment Service User), како што е пропишано во член 66.
- Услуга за информации за сметката (AIS, eng. Account Information Servic), обезбедена од TPP, Давател на услуги за информации за сметка (AISP, eng. Account Information Service Provider), како што е пропишано во член 67.
- Потврда за услугата за достапност на средства (CFS, eng. Confirmation on the Availability of Funds Service), која е обезбедена од TTP, давател на услуги за иницирање плаќања (PISP, eng. Payment Initiation Service Provider), како што е пропишано во член 65.

За да може горенаведените услуги да се имплементираат, со согласност на корисникот на платежните услуги (PSU), третиот давател на платежна услуга (TPP) треба да има пристап до сметката на PSU. Со сметката најчесто управува друг давател на услуги за плаќање (PSP), т.е. давател на услуги за иницирање плаќања (ASPSP, eng. Payment Initiation Service Provider). Во Република Македонија се уште најзастапени се банките. За да се поддржи TTP при пристап до сметките што ги одржува ASPSP (во Македонија, обично банка), секој ASPSP мора да обезбеди XS2A интерфејс[38] (XS2A, eng. Access to Account) за пристап до

[37] EUR-Lex: Direktiva (EU) 2015/2236, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32015L2366, 8. 5. 2024.

[38] Интерфејсот XS2A е технолошки стандард кој им овозможува на трети страни, како што се fintech компании или други финансиски институции, да пристапат до информации за корисничките сметки од банки или други даватели на финансиски услуги. Интерфејсот XS2A им овозможува на корисниците да дадат согласност на трети страни да пристапат до нивните финансиски информации и да вршат трансакции од нивните сметки. Ова дава можност за отворање нови услуги, како што се собирање на сметки (гледање на сите сметки на едно место), финансиско управување, иновативни мобилни плаќања и други финансиски услуги. Преку интерфејсот XS2A, трети лица можат да пристапат до податоците за состојбата на сметката, историјата на трансакциите и другите финансиски податоци на корисникот. Важно е да се напомене дека корисникот мора изречно да се согласи за пристапот и споделувањето на овие податоци.

сметката. Накратко, интерфејсот XS2A овозможува отворање на пазарот и иновации во финансискиот сектор, давајќи им на корисниците поголема контрола врз нивните финансиски податоци и овозможувајќи им пристап до нови и напредни финансиски услуги.

Прашањата во врска со одговорностите и правата на TPP и ASPS поврзани со интеракциите преку интерфејсот XS2A се утврдени и регулирани со самата регулатива PSD2. Деталните барања за имплементација и функционирање на интерфејсот XS2A се утврдени со техничкиот регулаторен стандард на Европската банкарска супервизија EBA-RTS[39].

Клучни цели на Директивата[40]:

- придонес кон интегриран и поефикасен европски пазар на плаќања
- подобрување на условите за еднакви услови за давателите на платежни услуги (вклучувајќи ги и новите учесници на пазарот)
- зголемување на безбедноста и заштитата на плаќањата
- заштита на потрошувачите
- поттикнување пониски цени за плаќање.

Од друга страна, основана е основата на регулаторните барања, која се состои од следниве документи:[41]

- PSD2 – Директива (Eu) 2015/2366
- регулаторни технички стандарди за доверлива автентикација на клиентот (SCA) и заеднички и безбедни стандарди за отворена комуникација (CSC)
- локални закони за транспонирање на директивата во законодавство.

[39] EBA-RTS (eng. European Banking Authority Regulatory Technical Standards) се технички стандарди развиени од Европската банкарска агенција (EBA) во согласност со Директивата за платежни услуги PSD2. Тие поставуваат правила и стандарди за безбедност и интероперабилност поврзани со пристапот до сметката и извршувањето на електронските плаќања, обезбедуваат заштита на податоците на корисниците и усогласеност со прописите од Директивата PSD2.
[40] EUR-Lex: Direktiva (EU) 2015/2236, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32015L2366, 8. 5. 2024.
[41] EUR-Lex: Direktiva (EU) 2015/2236, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32015L2366, 8. 5. 2024.

Иако регулативите PSD2 и EBA-RTS не налагаат експлицитно постоење и организација на функцијата CISO - менаџер за информациска безбедност во организацијата, тие имаат за цел да промовираат високи безбедносни стандарди во контекст на обезбедувањето платежни услуги, и финансиските институции и давателите на платежни услуги кои работат во согласност со Директивата PSD2 се обврзани да обезбедат соодветни безбедносни мерки за заштита на податоците на корисниците и спречување на злоупотреба.

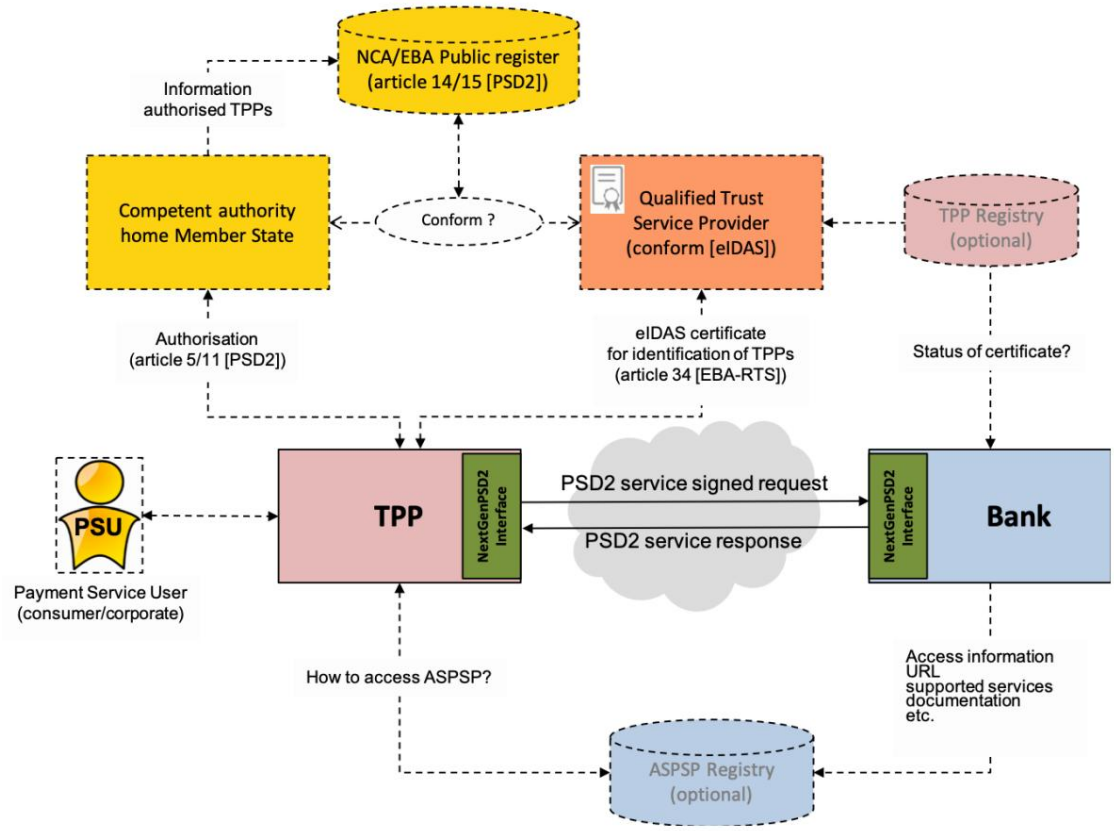
5.1.2. Иницијатива NextGenPSD2 на Берлинската група

Иницијативата NextGenPSD2 е специјална работна група во рамките на Берлинската група[42], со цел да се создаде заеднички, отворен и усогласен европски стандард за апликативни програмски интерфејси (API, eng. Application Programming Interface) кои им овозможуваат на трети лица, даватели на услуги (TPP), да пристапат до банкарски сметки во согласност со Директивата PSD2. Во одредена форма на единствено партнерство, учесниците во иницијативата NextGenPSD2 работат заедно за да ја реализираат визијата за отворени и хармонизирани PSD2 стандарди и XS2A интерфејси за процедури, податоци и инфраструктура, неопходна компонента на отворен и интероперабилен пазар. Вистинската интероперабилност е клучна компонента на конкурентните паневропски услуги PSD2 XS2A, што ќе придонесе за понатамошен напредок кон единствениот пазар на ЕУ. Дополнително, тој е наменет да има корист за целата индустрија за платежни услуги, со акцент на европските потрошувачи и бизниси [28].

Иако е неопходен хармонизиран интерфејс XS2A за да се овозможи развој на услугите XS2A во нивниот обем и со релативно ниски трошоци, комплетниот

[42] Берлинската група е европска иницијатива која ги обединува финансиските институции, давателите на платежни услуги и технолошките компании, со цел развивање и промовирање на стандарди и технички решенија за отворени банкарски услуги. Групацијата Берлин е основана во 2002 година, со првичен фокус на развивање стандарди за SEPA (Единствена област за плаќање во евра). Меѓутоа, со стапувањето во сила на Директивата за платежни услуги PSD2 (Payment Services Directive 2) во Европа, Берлинската група исто така се вклучи во развојот на технички стандарди за пристап до сметки (XS2A) и извршување на електронски плаќања.

екосистем PSD2 XS2A вклучува други технички, функционални, оперативни и управувачки области со (понекогаш опционални) комплементарни услуги, како што е прикажано на слика 6.



Слика 6: PSD2 и XS2A околина

Извор: https://www.hub.hr/en/psd2-open-api, посетено на 24.06.2024

Клучните карактеристики и компоненти се:[43]

- модерен „RESTful“ сет на API што користи HTTP/1.1 со TLS 1.2 (или повисоко) како протокол за пренос на податоци;
- интегрирање на повратни информации од јавните консултации во првата верзија на нацртот;
- Идентификација на TPP преку ETSI viii - дефинирани eIDAS сертификати; QWACS е задолжителен (едноставна мерка за заштита од на пример,

[43] https://www.hub.hr/en/psd2-open-api, посетено на 24.06.2024

DDOS напади), а QSEALS е изборен за банките (TPP ги следи упатствата на банката)

- ги поддржува сите потребни за PSD2 случаи на обезбедување услуги за иницирање плаќања, услуги за информации за сметки и услуги за потврда на достапноста на средствата, додека идните, повеќекратни/големи и повремени плаќања се опционални (во зависност од поддршката во рамките на онлајн банкарството или националното законодавство);
- целосна поддршка за повеќевалутна сметка;
- четири модели на архитектура за сигурна автентикација на клиентот (SCA); пренасочување, OAuth2, одвоено и „вградено“, со влијание на TPP врз преференциите за пренасочување;
- пристап на SCA на повеќе нивоа за компаниите, на пример, поддршка на принципот на двојна проверка („во четири очи“);
- поддржува сметки за порамнување за трансакции со картички;
- користи „корпи“ за потпишување, како инструмент за потпишување групирани трансакции (наместо повеќе функции за плаќање);
- транспарентна структура на ресурси (им овозможува преглед на TPP дури и во сложени деловни процедури);
- посебна согласност за API, која ја одвојува обработката на согласноста од пристапот до сметката, истовремено усогласувајќи се со барањата PSD2 и GDPR;
- опционална поддршка за време на сесија (збир на последователно извршени трансакции), предмет на соодветна согласност на клиентот;
- структури на податоци, во зависност од барањата за малопродажба;
- JSON со модел на податоци базиран на ISO 20022 или
- XML s pain.001 за PISP и camt.05x за AISP;
- интегрирана формална и транспарентна процедура за управување со промени и креирање верзии;
- можност за дополнителни проширувања кои овозможуваат изградба на („non-core “ PSD2) услуги со додадена вредност;

5.1.3. Организациска структура и активности и одговорности на раководителот за информатичка безбедност.

Барањата за усогласеност со Директивата PSD2 во Република Македонија и Регистарот на даватели на платежни услуги и издавачи на електронски пари, ги следи и управува Народната банка на Република Македонија преку Законот за платен промет, во кој е интегрирана Директивата PSD2. CNB ја следи усогласеноста и ја следи безбедноста на информациите. Откако ќе се регистрираат, деловните субјекти кои се во регистарот на даватели на платежни услуги се обврзани да се усогласат со Директивата и да пријават до CNB на барање. Тие се должни да спроведат проценка на ризик, вклучително и проценка на ризикот поврзан со ИКТ (информациско-комуникациска технологија), а должни се и еднаш годишно да вршат ревизија на информатичко-комуникациската технологија.

Во регистарот на даватели на платежни услуги и издавање електронски пари, за првпат се најдоа деловни субјекти кои биле класифицирани во технолошкиот сектор и чија примарна дејност е изработка на софтверски решенија. Поради специјализација и ориентација кон примарни активности, како што е развој на софтвер, некои од таквите организации ја воспоставија функцијата менаџер за информациска безбедност помеѓу внатрешните вработени, а некои од нив најдоа решение во користење на услугите на надворешен менаџер за информациска безбедност. Во таква ситуација се појави услугата на надворешниот менаџер за информациска безбедност FaaS (eng. Functions as a Service). Горенаведеното е исто така формално можно со длабинска проценка на ризик од трета страна (надворешен давател на услуги CISO) откако ќе биде испратено и одобрено од НБРМ.

Поголемиот дел од активностите што ги спроведува таков договорен менаџер за информациска безбедност зависи од моделот за кој се одлучила технолошката компанија. Доколку се работи за внатрешен вработен, многу често тој првенствено е одговорен за некои други активности од развој на софтвер, одржување на системот и мрежата, а понекогаш и финансии, а овие активности

поврзани со безбедноста на информациите му се само дополнителна одговорност и работа.

Со аутсорсинг моделот на функцијата менаџер за безбедност на информациите (модел FaaS), можно е да се добие конкретен поединец со повисоко ниво на компетентност од постоечкиот внатрешен персонал. CISO, како услуга и поединецот што ја врши, може да има тимови и одделенија во рамките на организацијата каде што е вработен, кои се специјализирани за одредени сегменти од безбедноста на информациите. Така, може да понуди дополнителна вредност на својата услуга, а организацијата која се одлучува за таков модел, може да види дополнителна вредност во него.

Активностите што таквиот менаџер за информациска безбедност ги спроведува најчесто се: проценка на ризикот од ИКТ, кореспонденција со регулаторот, ревизии на информативниот систем, решавање на безбедносни инциденти, известување до раководството и регулаторите, одржување на документацијата ISMS (ISO 27001) и поддршка и координација на процесот на сертификација и ресертификација на безбедноста на информациите. Покрај горенаведеното, секој стандард за безбедност на информации има свои барања, а исполнувањето на овие барања и усогласеноста со стандардот е одговорност на менаџерот за безбедност на информациите.

5.1.4. Активности и одговорности на менаџер за информациска безбедност во технолошката компанија – студија на случај

Авторот на овој труд е аутсорсинг менаџер за информациска безбедност (во остатокот од ова поглавје CISO) во технолошка компанија која развива апликации[44]. Либерализацијата на одредени пазари, како што се платежните трансакции, стимулирана со директивите PSD и PSD2, отвори можност за технолошката компанија да ја развие финансиската апликација SmartFIN. Целта на апликацијата е да им понуди на корисниците, кои се физички лица и жители на

[44] Името на компанијата нема да се спомнува во магистерскиот труд заради клаузула на доверливост во договорот со компанијата

една од земјите членки и кандидати за членки на ЕУ, напредна аналитика и проекција на нивната способност за плаќање. Врз основа на податоците за платежните трансакции и моментално достапното салдо на банкарските сметки на корисникот, користејќи машинско учење и напредни алгоритми, SmartFIN нуди проекција на способноста за плаќање на корисникот. Точноста и корисноста на апликацијата зависи од количината и квалитетот на податоците достапни на алгоритмите за предвидување. Предвидувачките модели, условно кажано, се обучуваат за податоците што им се достапни во базата на податоци. Колку повеќе реални податоци се обучуваат моделите, толку се попрецизни проекциите.

SmartFIN е инсталиран на мобилниот уред на корисникот и со негово официјално одобрение се користи со посветен API што се поврзува со еден или повеќе банкарски интерфејси каде што корисникот на апликацијата има отворени сметки. Горенаведеното беше овозможено со директивата PSD2, според која на трети страни, во овој контекст на технолошка компанија, им е дозволено да нудат услуги за информации за сметки, т.н. AISP. За да може услугата да биде возможна и да биде комерцијално понудена на пазарот, потребно е формално одобрение од регулаторот за платен сообраќај на земјата членка на ЕУ каде што е регистрирана активноста на технолошка компанија. За технолошка компанија тоа е национална банка[45] на земја членка на ЕУ, бидејќи компанијата е ќерка на компанија од земја членка на ЕУ. Националната банка донесува решение за упис во регистарот на даватели на платежни услуги и издавачи на електронски пари, доколку врз основа на барањето и доставената документација оцени дека се исполнети сите услови пропишани со Законот за платни трансакции на Романија.

Технолошката компанија, со споменатото решение ја отвори потребата за подигнување на нивото на информациска безбедност во целата организација, а тоа е една од главните задачи и обврски на CISO - менаџерот за информациска безбедност. Организациската структура во која вработениот во технолошка компанија, до одобрување од националната банка, ја извршуваше е функцијата

[45] Името на банката нема да се спомнува во магистерскиот труд заради клаузула на доверливост во договорот со компанијата

одговорен за безбедност на информации покрај неговата примарна функција менаџер за системска поддршка, па со воведување на апликацијата, таа стана несоодветно решение. Создадени се условите и регулаторните барања за формирање на наменска функција CISO - менаџер за безбедност на информациите.

Една од првите задачи на менаџерот по добивањето на одобрението од AISP беше да го спроведе т.н. gap-анализа, т.е. анализа на усогласеноста на технолошка компанија со тогашните нови и променети упатства: EBA Guidelines за управување со ИКТ ризици и безбедносни ризици (во натамошниот текст овој дел од Упатствата). CISO направи gap-анализа, во која утврди дека насоките се напишани на тој начин што ги насочуваат големите финансиски системи кои нудат платежни услуги, а кои во ЕУ се претежно банки. Без разлика за кого индиректно е напишано упатството, бил донесен заклучок. Упатствата во голема мера се засноваат на контроли од стандардот ISO 27002:2013. Со воспоставување и имплементирање на сите задолжителни контроли од ISO 27002 и сертификација во однос на стандардот ISO 27001, ќе се реши целата неусогласеност на технолошка компанија со упатствата. CISO го истакна гореспоменатиот заклучок во анализата на празнините и го презентираше на раководството на технолошката компанија. Менаџментот формално донесе одлука да иницира сертификација во однос на стандардот ISO 27001:2013. За раководител на проектот е избран раководителот на одделението за информатичка безбедност од Романија. Горенаведеното резултираше со промена на политиката за безбедност на информации, во која опсегот на применливост беше проширен на сите поврзани компании во кои технолошка компанија има мнозински удел. Раководителот за информациска безбедност ја подобри политиката за информациска безбедност така што таа се однесуваше на одредени прописи и процедури кои допрва требаше да се напишат и кои на крајот требаше да бидат усвоени од администрацијата.

CISO го подели проектот за сертификација врз основа на стандардот ISO 27001, кој ќе обезбеди усогласеност со горенаведените упатства, во четири основни фази, и тоа:

- Фаза 1 – креирање и усвојување на документација поврзана со безбедноста на информациите;
- Фаза 2 – спроведување на она што е пропишано со документацијата;
- Фаза 3 – внатрешна ревизија на сè што произлезе од претходните две фази;
- Фаза 4 – писмо од раководството со акцент на важните резултати од сите претходни фази.

Во првата фаза, CISO ги создаде и менаџментот ги усвои следните документи:

- Правилник за управување со правата за пристап;
- Правилник за управување со физичка безбедност;
- Правилник за управување со шифрирање;
- Правилник за управување со ресурсите на информацискиот систем;
- Правилник за управување со лозинка;
- Правилник за оценување на ефективноста на безбедносните контроли;
- Правилник за улоги и одговорности за безбедност на информациите;
- Правилник за аутсорсинг;
- Правилник за управување со промени во информацискиот систем;
- Правилник за управување со ранливоста;
- Правилник за управување со инциденти;
- Правилник за управување со складиштето;
- Правилник за управување со оперативна и системска евиденција;
- Регулатива за следење на усогласеноста;
- Правилник за класификација на информациите;
- Правилник за управување со промени во информацискиот систем;
- Правилник за соодветно користење на информацискиот систем;
- План за континуитет на бизнисот;
- Политика за управување со континуитет на бизнисот;
- Постапка за проценка на ризик и можности;

- Постапка за управување со човечки ресурси.

Во оваа фаза, главниот предизвик за CISO беше да им ја пренесе важноста на разбирањето и усвојувањето на политиките, регулативите, процедурите и плановите на членовите на одборот. Во технолошка компанија, одборот се состои од три члена, од кои еден е извршен директор, еден технички директор и еден финансиски директор. Без оглед на одлуката на менаџментот да го подигне нивото на безбедност на информациите, преку сертификација и со тоа усогласување со упатствата, недостигаше разбирање и свест за неговото значење. Недостигаше разбирање за тоа што значи за компанијата да се усогласи и на крајот да се воспостави систем за управување со безбедноста на информациите. Во оваа фаза, менаџерот за информациска безбедност требаше да најде начин да се позиционира и јасно и недвосмислено да комуницира со раководството за да добие разбирање. Официјалното писмо од националната банка во кое се истакнува потребата да се достави одредена документација, како што се Политиката за безбедност на информации, резултатите од внатрешната ревизија и, на крајот, проценката на ризикот од ИКТ и експерт и искусен менаџер за информациска безбедност - полека создаде свест кај извршниот директор за усвојување и спроведување на опишаните документи.

По усвоената документација, CISO иницираше креирање на целосен и сеопфатен регистар на информациско-комуникациски средства, вклучително и податоци во сопственост на компанијата. Точен и сеопфатен регистар на средства беше главниот предуслов за значајна проценка на ризикот од ИКТ. За да може регистарот да биде комплетен, извршени се повторувања на креирање и дополнување, како и контрола на самиот регистар. Овие повторувања беа сведени на фактот дека раководителот за информациска безбедност за време на двочасовни работилници со сопственици на деловни процеси кои користеа одредени ИКТ средства, ги помина нивните деловни процеси и се обидуваше да ги поврзе што е можно подобро со користените ИКТ средства. По поврзувањето на деловниот процес и ИКТ средствата, на вработените во технолошка компанија

им беше доделена сопственост и одговорност над процесот и средствата. Потоа, средствата се поделени на логички групи.

Преку повторувања, CISO ја утврди заканата и ранливоста за секоја група на средства и пресмета квантитативен показател за критичност. Покрај горенаведеното, тој ги наведе постоечките и планираните контролни мерки за секоја група.

По оваа фаза на проценка на ризик, имаше одреден хаос во самиот проект со откриен и успешно решен безбедносен инцидент, кој се наоѓаше во периметарот на системската инфраструктура на технолошката компанија. На некој начин, ова беше пресвртница, во која преостанатите двајца членови на одборот ја вклучија безбедноста на информациите меѓу приоритетните цели на компанијата. Да се постапеше побрзо и превентивно, немаше да се случи безбедносниот инцидент. Постоењето на одредени безбедносни контроли на раководителот за информациска безбедност резултираше со тоа што причините за појава на инцидентот беа откриени, изолирани и на крајот отстранети.

Од веќе наведените документи, три добија посебно значење и се покажаа како корисни и неопходни. Тоа беа: Правилник за управување со ранливоста, Уредба за управување со инциденти, и нешто помалку, Уредба за управување со резервно складирање.

Меѓу другото, Правилникот за управување со инциденти ја дефинира подготвителната фаза, која ги опфаќа следните активности:

- воспоставување и редовно ажурирање на внатрешните акти за управување со инциденти;
- воспоставување и редовно ажурирање на каталогот на средства во чии рамки се дефинираат сопствениците на поединечните системи и нивната критичност;
- воспоставување на функционален систем за управување со резервни копии според деловните потреби на технолошката компанија;

- инсталација, конфигурација и редовно одржување на системи и алатки кои се користат за идентификација и одговор на инциденти.

Анализата на дневниците на воспоставеното SIEM решение предупреди на постоење на безбедносен инцидент, чие решавање го презеде CISO. Во Правилникот, членот ја пропишува фазата на идентификација, во која се наведува дека за идентификација на безбедносен инцидент, потребно е внимателно да се следат следниве критериуми:

- необични процеси кои се изведуваат на одредени системи;
- необични датотеки или вредности на клучот во регистарот;
- индикатори за присуство на активен злонамерен софтвер;
- големи количини на шифриран мрежен сообраќај кои излегуваат од мрежата на технолошката компанија кон сомнителни дестинации;
- нови (непознати) кориснички сметки;
- необичен појдовен мрежен сообраќај;
- аномалии во активностите на привилегираните кориснички сметки;
- географски аномалии;
- сомнителни обиди за логирање во системот;
- Сообраќајни аномалии на DNS.

Преку дневниот автоматски извештај од SIEM решението, во кое беше поставено автоматско правило кое ја комбинира променливата на необичен процес на одреден сервер, CISO несомнено ја идентификуваше аномалијата на сообраќајот на DNS и географската необичност, како и инсталираната нелегална апликација , поточно т.н. crypto miner. Самата регулатива ја пропишува фазата на отстранување и обновување и известување. Со помош на администраторот на тој сервер, менаџерот ги отстрани и поврати сите технички и деловни процеси и напиша и презентираше извештај за безбедносниот инцидент до администрацијата. Од една страна, опасната и непријатна ситуација за технолошката компанија резултираше со научена лекција и јасен став на целата администрација за важноста на безбедноста на информациите. Од тој момент, фазата 1 и фаза 2 од опишаниот проект за CISO продолжија да се одвиваат

побрзо, појасно и поконкретно. Речиси немаше отпор од вработените на оперативните нивоа и средното раководство. На крајот од фазата 2, менаџерот ги создаде следниве документи:

- Каталог на ризици
- Каталог на трета страна
- Каталог на ризици и можности
- Опсег на ISMS
- Извештај за анализа на влијанието на бизнисот
- Извештај за проценка на ризик
- Извештај за проценка на ефективноста на безбедносната контрола.

Последните три документи беа извештаи во кои CISO ја презентираше проценката на ризикот до менаџментот и извештајот за проценката на ефективноста на безбедносните контроли, со што беше завршена Фаза 3 од опишаниот проект.

Во последната фаза пред вистинската сертификација, менаџерот креираше документ во кој сумираше сè што е важно за целиот процес и безбедноста на информациите на технолошката компанија. Документот, кој е формално насловен Управување со безбедноста на информациите - менаџмент проценка, ги содржи резултатите од внатрешната ревизија, неусогласеноста во однос на барањата на нормата, наоди, ризици и препораки, повратни информации од заинтересираните страни, предлози и подобрување на ефикасноста на системот ISMS, статусот и исполнувањето на целите на ISMS, резултатите од мерењето на ефективноста на безбедносните контроли и предлозите за подобрување на ISMS. Во табела 9 се прикажани сите воспоставени безбедносни контроли, кои менаџерот ги подели на организациски и технички, а во табелата 10 се прикажани целите на системот за управување со безбедноста на информациите.

Табела 9: Организациски безбедносни контроли

	Контрола	Ниво на ризик

ОРГАНИЗАЦИСКИ БЕЗБЕДНОСНИ КОНТРОЛИ		
КО-01	ISMS документација - изготвување и дополнување на внатрешни акти (политики, регулативи, процедури, каталози) на начин на адресирање на регулаторните барања (ISO 27001 стандард, CNB/EBA упатства, GDPR)	Висок
КО-02	Едукација на клучни вработени за информациска безбедност - формално образование за внатрешен ревизор ISO 27001	Висок
КО-03	LMS - набавка и имплементација на систем за едукација и подигање на свеста на вработените за безбедноста на информациите	Висок
КО-04	Ревизија на доделените права за пристап – на сите системи	Среден
КО-05	Прилагодување на корисници	Среден
КО-06	Ажурно снимање на промени во апликацијата	Среден
КО-07	Автоматско спроведување на тестирање на апликации по промени	Среден
КО-08	Размена на знаење	Среден
КО-09	Ротација на должностите во рамките на организацијата	Среден
КО-10	Подобрување на нивото на грижа за вработените - спроведување на анкета за задоволството на вработените и собирање предлози за подобрување	Среден
ТЕХНИЧКИ КОНТРОЛИ ЗА БЕЗБЕДНОСТ		
КТ-01	Имплементација на нова алатка за резервна копија	Среден
КТ-02	Енкрипција на хард дискови - работни станици	Висок
КТ-03	Проширување на опсегот на примена на системот за проценка на ранливост - да го вклучи целиот ISMS	Среден
КТ-04	Имплементација на 2FA за контрола на пристапот до	Среден

	клучните системи	
КТ-05	Имплементација на напредни алатки за тестирање на апликации	Среден

Извор: Изработка на авторот согласно студија на случај

Табела 10: Цели на системот за управување со безбедноста на информациите

	ISMS цели	Опис	статус
1	ISO 27001:2013 сертификација.	Успешно завршување на сертификатот ISO 27001:2013.	Реализацијата е во завршна фаза.
2	Целосно усвојување на ISMS на ниво на компанија.	Сите вработени ја прочитале и усвоиле Политиката за информациска безбедност и придружните ISMS документи, како и нивните улоги и одговорности во системот ISMS.	Реализацијата е во тек.
3	Успешно завршување и позитивен одговор на сите барања за оцена на сообразност.	Компанијата треба успешно да ги исполни и одговори на сите барања за оцена на сообразност упатени од клиенти или регулатори.	Имплементацијата е во тек (систематска имплементација).
4	Програма за подигање на свеста за безбедноста на	Воспоставување на програма за подигање	Редовно информирање на

	информациите за сите вработени.	на свеста за безбедноста на информациите, на која присуствуваат сите вработени.	сите вработени со месечен Билтен. Имплементацијата на LMS системот е во тек.
5	Безбедност од трета страна.	Развивање и имплементирање прашалник за безбедносна проценка од трета страна како дел од процесот на длабинска анализа.	Реализирано.
6	Спроведување на критични безбедносни контроли идентификувани во текот на годишниот процес на проценка на ризикот.	Спроведување на безбедносни контроли кои се идентификувани и формално прифатени преку процесот на управување со ризик.	Реализацијата е во тек.

Извор. Изработка на авторот согласно студија на случај

Со презентирање и потоа усвојување на документот за проценка на управувањето со ISMS, CISO ги создаде сите предуслови за ангажирање на акредитирана компанија за формална сертификација на технолошката компанија врз основа на ISO 27001, по што овластените ревизори на надворешно друштво за акредитација ја извршија сертификацијата. CISO беше тој што одговараше на прашања и презентираше докази.

Прашањата беа ограничени на тоа дали постојат одредени документи што ги бара стандардот и дали навистина се спроведуваат пропишаните процедури и прописи. Едно од многу честите прашања, за кое е потребно да се доставуваат

докази, се сведува на должината и сложеноста на лозинката, што е пропишано со Правилникот за управување со лозинка.

Во правилникот CISO пропишал, а менаџментот усвоил дека сите апликации, вклучувајќи ги директориумите - услуги како што е Active directory, во кои се креираат кориснички сметки, се обврзани на следново: за сметки со обични права, лозинките мора да имаат минимум 12 знаци, меѓу кои, покрај алфанумеричките знаци, мора да има најмалку еден посебен знак. Сите сметки со привилегирани права, како што се сметки за услуги, администраторски сметки и сметки на надворешни партнери мора да имаат лозинки од најмалку 14 знаци и мора да содржат најмалку еден посебен знак, покрај алфанумеричките знаци. Дополнително е пропишано дека сите лозинки мора да се менуваат најмалку на секои три месеци. Наведените барања од правилникот CISO можеше да ги спроведе со помош на принуда на сопствениците и администраторите на сите апликации и системи. Процесот на ревизија на горенаведеното беше сведен на фактот дека ревизорот побара од менаџерот список на сите сметки на клучните системи на компанијата. Истовремено ја побара актуелната листа на сите вработени од кадровскиот сектор, а од менаџерот за комуникација со добавувачи побара список на сите добавувачи со лице за контакт. Прво, тој го спореди бројот на вработени во технолошката компанија со бројот на сметки во Active Directory и врз основа на случаен примерок, ги провери безбедносните поставки за лозинка за корисничка сметка со обични права и за корисничка сметка со привилегирани права.

Потоа, истото го направи и за корисничките сметки на надворешните партнери кои имаат право на пристап до системите на технолошката компанија. Сето горенаведено го провери врз основа на случаен и репрезентативен примерок. Репрезентативноста, а со тоа и точноста на споменатиот ревизорски процес е сомнителна, но дозволена со самиот стандард. За ревизијата и на крајот, барањата на стандардот, таа беше спроведена на задоволително ниво. Горенаведеното не беше задоволително за внатрешните барања на CISO, кој самиот иницираше сеопфатна внатрешна ревизија на сите кориснички сметки, која

не беше спроведена врз основа на примерок, туку врз основа на увид во сите сметки и нивните безбедносни поставки поврзани со сложеноста, должина и времетраење на лозинките за пристап. Тие наоди ја покажаа вистинската состојба и предупредуваа на непочитување на правилникот и прекршување на безбедносните мерки, додека ревизијата за сертификација овде не откри никакво неусогласеност со стандардот. Внатрешната ревизија, иницирана од CISO, констатира прилично голем број на непочитување на Правилникот и прекршување на неговите барања. Внатрешните сознанија резултираа со покренување на корективни активности, а надзорот над спроведувањето на корективните активности го презеде раководителот на информатичката безбедност.

Проектот за сертификација на технолошката компанија врз основа на стандардот ISO 27001 беше успешно имплементиран со обврска да се имплементираат одредени корективни активности и препораки до следниот циклус на сертификација.

Покрај гореспоменатата внатрешно иницирана ревизија (иницирана од CISO), откриен е простор за подобрување на безбедноста на информациите. Некои од препораките се: затворање на одреден број AD-сметки кои им припаѓале на поранешни вработени, барање за надградба на понова верзија на одредени оперативни системи на одредени серверски компјутери, подигање на свеста и знаењето за безбедноста на информациите кај сите вработени и воспоставување двојна автентикација за внатрешно развиено решение во кое се сместени сите суштински деловни апликации.

Сите цели за одржување на системот за управување со безбедноста на информациите и спроведување на воспоставените контроли прикажани во табела 9 станаа главни активности и одговорности на CISO.

5.2. Раководител за информатичка безбедност во јавниот сектор

Според искуството на авторот на овој труд, носителот на позицијата CISO - менаџер за информациска безбедност во голема мера зависи од тоа дали

организацијата, во која оваа функција е одговорна за безбедноста на информациите, е дел од критичната национална инфраструктура или не. Доколку е така, организацијата е должна да ги усогласи своите активности и одговорност рпозитивните законски прописи и препораките на ЕУ. Како што веќе спомнавме, еден од законите кои треба да се донесе е Законот за критична инфраструктура, кој е резултат на европското законодавство вградено во националните закони на земјите членки и земјите кандидати за членство, меѓу кои е и Република Македонија. Организацијата потоа мора да го почитува Законот за критична инфраструктура, а формирањето, изборот и активностите на CISO се јасно пропишани со Законот.

Доколку јавната институција не е дел од критичната инфраструктура, слободата и систематизацијата на функцијата на CISO - менаџер за безбедност на информации зависи од администрацијата и/или менаџментот на таа институција. Примерот на овој труд е организација, која поради природата на сите активности и сопственичката структура, може да се смета за орган од јавниот сектор. Пред десет години, таа ја препозна важноста и вредноста на безбедноста на информациите. Можеме само да ја погодиме причината и одлуката да се покренат активности поврзани со воспоставување на одредено ниво на информациска безбедност, а од записникот од седниците на менаџментот, можеме да заклучиме дека причината била предвидувањето на зголемена закана за безбедноста на информациите. Имајќи предвид дека организацијата е комбинација од испреплетени комерцијални активности и активности кои можат да се класифицираат во доменот на јавните добра и услуги, воспоставувањето и одржувањето на безбедноста на информациите е сложена задача.

Со воспоставувањето на информациската безбедност, започна подготовката за сертификација според меѓународниот стандард за информациска безбедност ISO 27001:2013. Формално, со развивање збир на основна документација, беше воспоставен ISMS (eng. Information Security Management System). Станува збор за комбинација во која директорот на секторот за ИТ, со

ангажман на трето лице давател на услуги, разви, а потоа усвои од раководството основен сет на документи како што се:

- Политики
    - Политика за безбедност на информации
    - Политика за контрола на правата на пристап
    - Политика за користење на интернет и е-пошта
    - Политика за употреба на преносливи компјутери и пренослива опрема
    - Политика на криптографски контроли
    - Политика за набавки за развој и одржување на информациски системи
    - Правила за празна табела и празен екран
    - Политика за усогласеност
    - Политика за управување со имот
    - Политика за управување со капацитети, планирање и прифаќање на понудите
    - Политика за лозинка
- Процедури и постапки
    - Барање до добавувачот за промена
    - Постапка за внатрешна верификација
    - Процесот на изработка на каталог и класификација на средствата
    - Постапка за резервна копија
    - Постапка за корективна акција
    - Постапка за мерење на ефективноста на ISMS контролите
    - Процедура за следење на антивирусен систем
    - Постапка за следење на користењето на системот
    - Постапка за преземање на компјутерот од корисникот
    - Постапка за превентивно дејствување
    - Процесот на прифаќање на испораката на добавувачот
    - Постапка за соодветно постапување со доверливи информации

    - Работна процедура во системски области
    - Постапка за управување со документи и евиденција
    - Постапка за управување со кориснички и привилегирани права
    - Процедура за управување со промени
    - Постапка за управување со безбедноста на вработените
    - Постапка за управување со безбедносни слабости и инциденти
    - Безбедност и мрежни контроли за пристап за оперативни системи и апликации
    - Упатства за креирање корисничко име
    - Управување со услуги од трета страна
- Обработка и анализа на ризик
    - Каталог и класификација на средствата
    - План за обработка на ризик
    - Извештај за процена на ризик
    - Методологија на проценка и критериуми за обработка на ризик
- Регистар на безбедносни инциденти
- Извештаи и одлуки
    - CISO ізвештај
    - Евалуација на менаџментот
    - Програма за внатрешни проверки и извештај за внатрешни проверки
    - Стратегија за безбедност на информациите.

Горенаведениот сет на документи, вклучувајќи ги внатрешните политики, правила и процедури и сеопфатна проценка на ризикот за безбедноста на информациите, се според стандардот ISO 27005.

ISO 27005 го опишува процесот на управување со ризиците за безбедноста на информациите користејќи пристап заснован на анализа на ризик. Овој пристап во организацијата иницира постапка за идентификација и проценка на ризиците, избор на соодветни мерки за управување со ризици и следење и ревизија на овие мерки.

Со ова е овозможено да се воспостави рамка за управување со ризиците од безбедноста на информациите и да се идентификуваат и проценат ризиците поврзани со безбедноста на информациите, како и да се изберат и применат контроли и мерки за управување со ризик.

Идентификувањето и проценката на ризикот се сведува по сеопфатна листа на средства за информатичка и комуникациска технологија. Во оваа фаза, за првпат во организацијата се профилира вработен кој е доволно одговорен и компетентен за да биде унапреден во CISO – менаџер за информациска безбедност. Со помош на трето лице и со соработка на одделенијата за финансии и сметководство, контрола и други од ИТ-секторите, се креира документација и процедури со цел одржување и подобрување на безбедноста на информациите. На крајот, одделот за ИТ во организацијата треба успешно да се сертифицира од акредитирана меѓународна компанија за сертификација. На овој начин се подигнува свеста на менаџментот и свеста и обврската на вработените во однос на безбедноста на информациите.

По успешната сертификација, се создава свест за потребата да се инвестира во безбедноста на информациите, а како резултат на тоа, се наметнува потребата од вработување на CISO - менаџер за информациска безбедност. Покрај одржувањето на основниот сет на опишана документација, CISO е одговорен за спроведување на сите мерки пропишани во документацијата ISMS. Покрај наведеното, тој е задолжен за подучување на вработените, создавање свест при пишување месечни извештаи за актуелни теми; како што се нови пропусти, нови форми на хакерски напади и пропусти во старата и новата технологија. Покрај горенаведеното, тој има советодавна улога за одделот за системска поддршка, мрежни технологии и одделот за поддршка на апликации.

Некои од активностите се: ревизија на конфигурацијата на заштитниот sид и правила и предлози за нивно подобрување, ревизија на мрежната топологија, сегментација на мрежата и дефинирање на листи за пристап, организација и координација на тестирање на пенетрација, третман и отстранување на наодите од тестирањето на пенетрација, третман и отстранување на наодите од

внатрешна и надворешна ревизија, одговор на безбедносен инцидент, одржување на циклус на ресертификација, следење и предлагање нови решенија и/или подобрување на постоечките и известување до раководството за нивната работа и состојбата на информацискатa безбедност во организацијата. Покрај горенаведеното, CISO мора да ги следи прописите и сите закони кои се однесуваат на безбедноста на информациите кои влијаат на организацијата.

Од сè што е опишано, може да се забележи широчината на активности кои бараат стручност, искуство и постојано учење за поединецот кој ја врши наведената функција CISO - менаџер за информациска безбедност. Според студијата на случај опишана овде, менаџерот за безбедност на информации е надворешен соработник кој е специјализиран за безбедност на информации и кој има на располагање луѓе кои се специјализирани во различни области на безбедноста на информациите - од тестирање на пенетрација, следење на мрежниот сообраќај, управување со инциденти, до компјутерска форензика и повеќе. Токму поради оваа ситуација, тој може да побара совет од колеги кои се поголеми експерти од него во одредена област, а тука дополнителна вредност има и моделот FaaS на обезбедување на услугата на надворешен менаџер за информациска безбедност. Од друга страна, овој тип на модел е договорен со одредена саатница, што исто така е пречка - и во однос на времето и на трошоците.

5.3. Раководител за безбедност на информации во организации за плаќање со картички

Организација од овој сектор е организација која не е дел од банка или банкарска групација, а како таква е на територијата на Република Македонија. Основниот закон кој ги пропишува клучните деловни параметри е Законот за платежни трансакции, а клучниот стандард е PCI DSS[46] (eng. Payment Card

[46] PCI DSS (Payment Card Industry Data Security Standard) е безбедносен стандард кој се применува во индустријата за плаќање со кредитни картички. PCI DSS беше развиен од Советот за безбедносни стандарди на индустријата за платежни картички со цел да се заштитат

Industry Data Security Standards). Активностите на CISO - менаџерот за безбедност на информации најмногу се поврзани со барањата на овој безбедносен стандард и областа на неговата примена. Во овој дел од трудот е претставена студија на случај со акцент на активностите за управување со ранливоста. Во табела 11, ова се точките 5 и 6.

Табела 11: Основни барања за PCI DSS

Стандард за безбедност на податоци PCI - Преглед на барања	
Изградба и одржување безбеден мрежен систем!	1. Инсталирајте и одржувајте контроли за безбедност на мрежата! 2. Применете безбедни конфигурации на сите компоненти на системот!
Заштита на информациите за дадена сметка!	3. Заштита на зачуваните податоци на сметката! 4. Заштита на податоците на сопственикот на картичката со силно шифрирање при пренос преку јавно достапни мрежи!
Одржување на процесот на управување со ранливоста!	5. Заштита на сите системи и мрежи од малициозен софтвер! 6. Развој и одржување безбеден систем и софтвер!
Воспоставање на силен процес на управување со правата за пристап!	7. Ограничување на пристапот до системските делови и податоците за сопственикот на картичката врз основа на принципот на потреба за деловни цели! 8. Идентификување на корисници и потврда на пристапот до делови од системот!

информациите за картичката и да се намали ризикот од кражба или злоупотреба на информациите за кредитната картичка. Стандардот ги дефинира безбедносните барања и препораки кои мора да ги исполнат организациите кои обработуваат, складираат или пренесуваат податоци од кредитните картички. Ова ги вклучува трговците, обработувачите на плаќања, трговците, банките и другите вклучени во синџирот за обработка на трансакции со картички.

	9. Ограничување на физичкиот пристап до податоците на сопственикот на картичката!
Често следење и тестирање на мрежата!	10. Ги следи сите дневници за пристап до системот и податоци за сопственикот на картичката! 11. Редовно тестирање на безбедноста на системот и мрежата!
Одржување на политика за безбедност на информациите!	12. Поттикнување на безбедноста на информациите со организациски политики и програми!

Извор: Security Standards Council, LLC : Payment Card Industry Data Security Standard: Requirements and Testing Procedures v4.0,

https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

За да се исполни стандардот, воспоставен е систем за управување со ранливост; низ системот и мрежната инфраструктура и внатре и надвор од мрежниот периметар, воспоставен е систем на автоматско скенирање на ранливости, користејќи готови комерцијални решенија.

Qualys[47], кој е интегриран со платформата ServiceNow[48], се користи за автоматско скенирање на ранливости. Покрај автоматското скенирање и примената на базите на знаење, пакетот услуги што ги нуди лиценцата Qualysa го вклучува модулот VMDR, односно модул развиен за управување со ранливости. Сликата (слика 7) ги прикажува сите фази на управување со ранливости во рамките на VMDR модулот.

[47] Qualys е безбедносна платформа базирана на облак, обезбедена од истоимената компанија. Тоа е сеопфатно решение за управување со безбедноста што им овозможува на организациите да ги идентификуваат, проценат и управуваат пропустите во нивните информациски системи, мрежи, уреди и апликации.

[48] ServiceNow е платформа базирана на облак која служи за управување со работните процедури и организации, овозможувајќи автоматизација, стандардизација и управување со различни деловни процеси и услуги. Тоа е сеопфатна платформа, која обединува различни функционалности за поддршка на различни аспекти на управувањето со деловните операции.



Слика 7: VMDR модул на Qualys

Извор: Qualys, Inc.: Qualys Vulnerability Management (VMDR), https://www.qualys.com/apps/vulnerability-management-detection-response/, 12.5.2024.

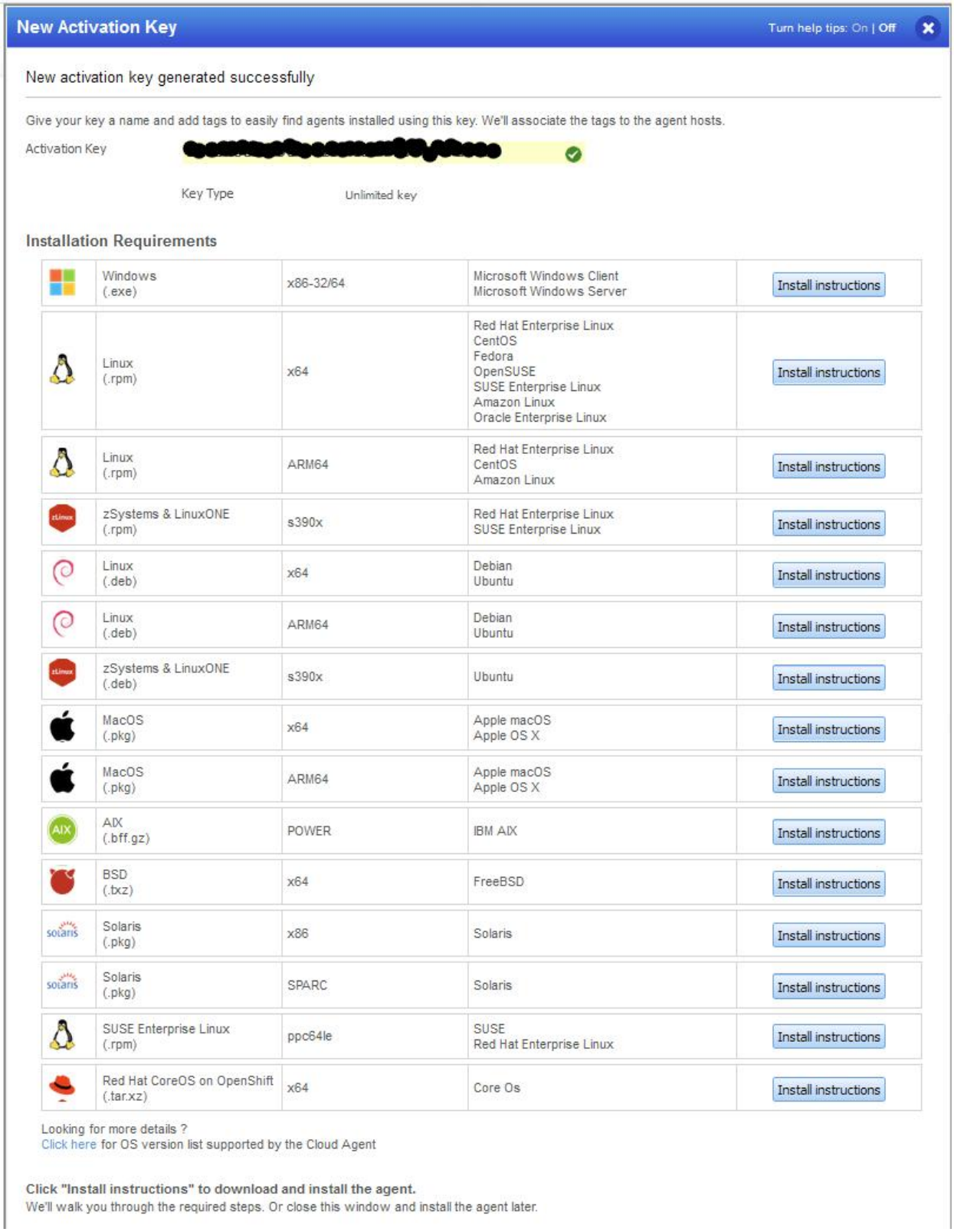
Процесот на управување со ранливоста е под директна одговорност на CISO - менаџерот за безбедност на информациите. Организацијата е глобално присутна и распространета, а активностите и платежната мрежа, со целокупната придружна инфраструктура, имаат глобални размери со регионални особености. Причината за регионалната посебност е делумно правна, а делумно техничка по природа бидејќи не сите региони имаат иста легислатива, ниту иста развиена техничка инфраструктура и регулатива, што е предуслов за поврзување со платниот систем на регионот каде што е присутна организацијата. Покрај сето горенаведено, карактеристика на овој потсектор од финансискиот систем е тоа што регулативата е строга и присутна кај неколку регулаторни тела истовремено. Дополнителна специфичност на индустријата за плаќање со картички е тоа што постојано има купопродажба на организации или одредени делови од други деловни субјекти (M&A трансакции, eng. mergers and acquisitions). Во таква организација, свесноста за горенаведените факти е пожелна за CISO - менаџерот

за информациска безбедност, бидејќи сето тоа влијае на неговите активности, кои не се само управување со ранливости. Во оваа студија на случај, опишана е само активноста за управување со ранливост.

5.3.1. Детектирање на пропусти

Постапката за управување со ранливоста се сведува на дефинирање на опсегот на внатрешни IP адреси и подмрежи, во кои има компјутери и мрежни уреди со поврзани внатрешни IP адреси и имиња на DNS. Во првата фаза од основањето, откако ќе се утврди опфатот, започнува инсталацијата на Qualys агентите на компјутерите и мрежните уреди. Процесот на инсталација зависи од оперативниот систем инсталиран на конкретниот сервер или клиентски компјутер.

На сликата 8 е прикажана процедурата за генерирање на клучот за активирање, како и понудените оперативни системи. Во зависност од оперативниот систем, во понатамошниот чекор на инсталација, кој е прикажан подолу, има неколку линии на команди што треба да се внесат во терминалот на машината каде што треба да се инсталира агентот.



Слика 8: Генерирање на клучот за активирање на Qualys агентот

Извор: Авторот со сопствено истражување

Команда за инсталација за терминал со оперативен систем Windows:

```
QualysCloudAgent.exe CustomerId={XXXX-XXXX-XXXX}
ActivationId={XXXX-XXXX-XXX-XXXX}
WebServiceUri=https://qagpublic.qg1.apps.qualys.eu/CloudAgent/
```

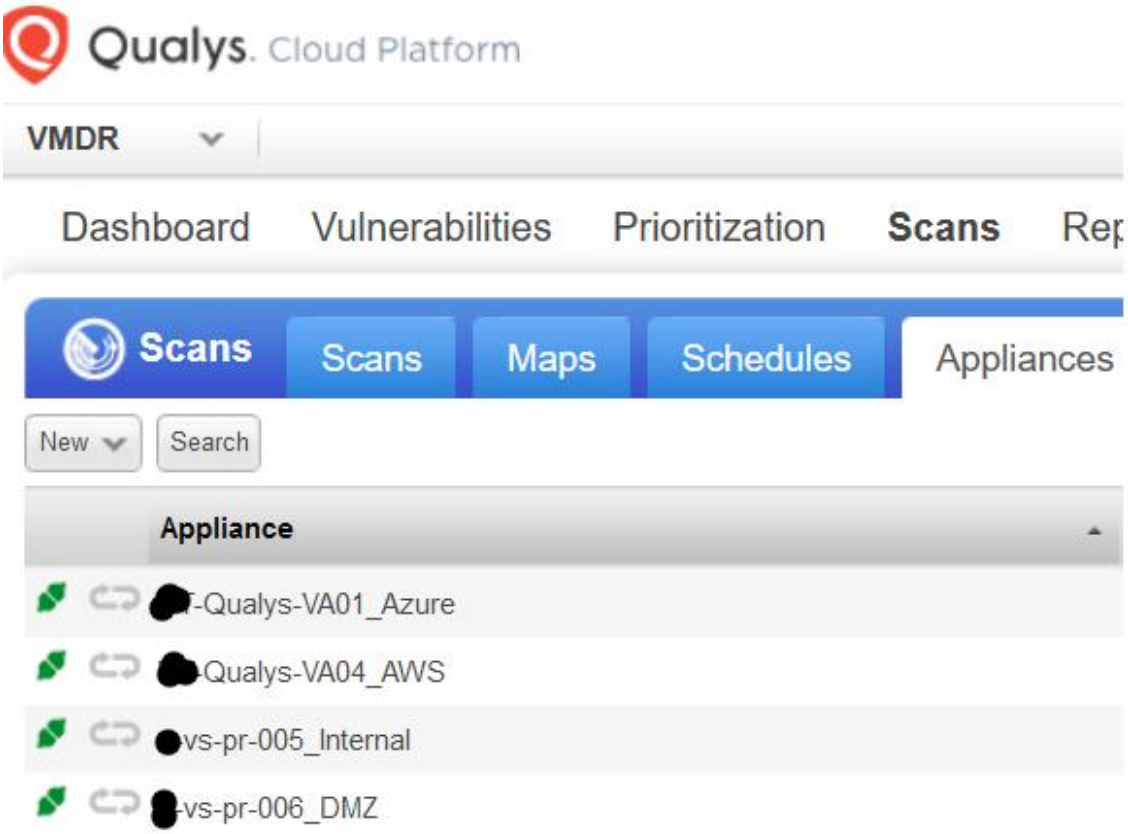
Команда за инсталација за терминал со оперативен систем Linux:

```
sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId=XXXX-XXXX-XXXX-XXXX-XXXX
CustomerId=XXXX-XXXX-XXXX-XXXX-XXXX
```

По успешната инсталација, се започнува процес на автоматско скенирање со почетна цел за мапирање на сите инсталирани и активирани агенти. Во оваа фаза, по активирањето на агентот, кое се врши преку централизиран мрежен интерфејс, се прави првата врска помеѓу агентот и скенерот сместен во облакот (виртуелен скенер апарат).

Скенерите се регионално наменети, односно се наоѓаат во центри за податоци ширум светот, а активниот агент првично се обидува да се поврзе со сите достапни скенери во регионот каде што се наоѓа машината на која е инсталирана. На сликата 9 се прикажани скенерите достапни за активниот агент Qualys.

По изборот на скенерот и почетното мапирање, се закажуваат автоматски или рачни скенирања, во зависност од договорот во организацијата и според барањата на стандардот PCI DSS. Главната поделба на скенирањата по метод на закажување е поделбата на автентицирани и неавтентицирани скенови.



Слика 9: Qualys скенери

Извор: Авторот со сопствено истражување

Неавтентицирано скенирање: во овој тип на скенирање, Qualys се користи со метод каде што не се потребни параметри за пристап или акредитиви за пристап до целниот систем. Ова значи дека Qualys го скенира системот од надворешната мрежа, користејќи достапни податоци и техники за скенирање за да ги идентификува пропустите. Неавтентицираното скенирање е побрзо и поедноставно бидејќи не бара автентикација на целниот систем, но обично обезбедува помалку детали за ранливостите и е ограничено во откривањето на одредени видови проблеми.[49]

Автентицирано скенирање: за да се автентицира на целниот систем, во овој тип на скенирање Qualys користи податоци за пристап и ингеренциите кои се

[49] Qualys, Inc.: Qualys Vulnerability Management (VMDR), https://www.qualys.com/apps/vulnerability-management-detection-response/,

обезбедени однапред. Овој метод на скенирање му овозможува на Qualys пристап до подлабоки системски нивоа, како што се: инсталиран софтвер, поставки за конфигурација и системски датотеки.

Автентицираното скенирање обезбедува подетални податоци за ранливоста и подобро разбирање на целокупната безбедносна положба на целниот систем, но бара податоци за пристап и подолго време на извршување.[50]

Редовните активности што ги спроведува CISO - менаџерот за информацискатa безбедност на оваа организација вклучуваат планирано автентицирано скенирање на сите 65536 порти, во дефиниран опсег и според геолокациите, и по опсег на внатрешни IP-адреси.

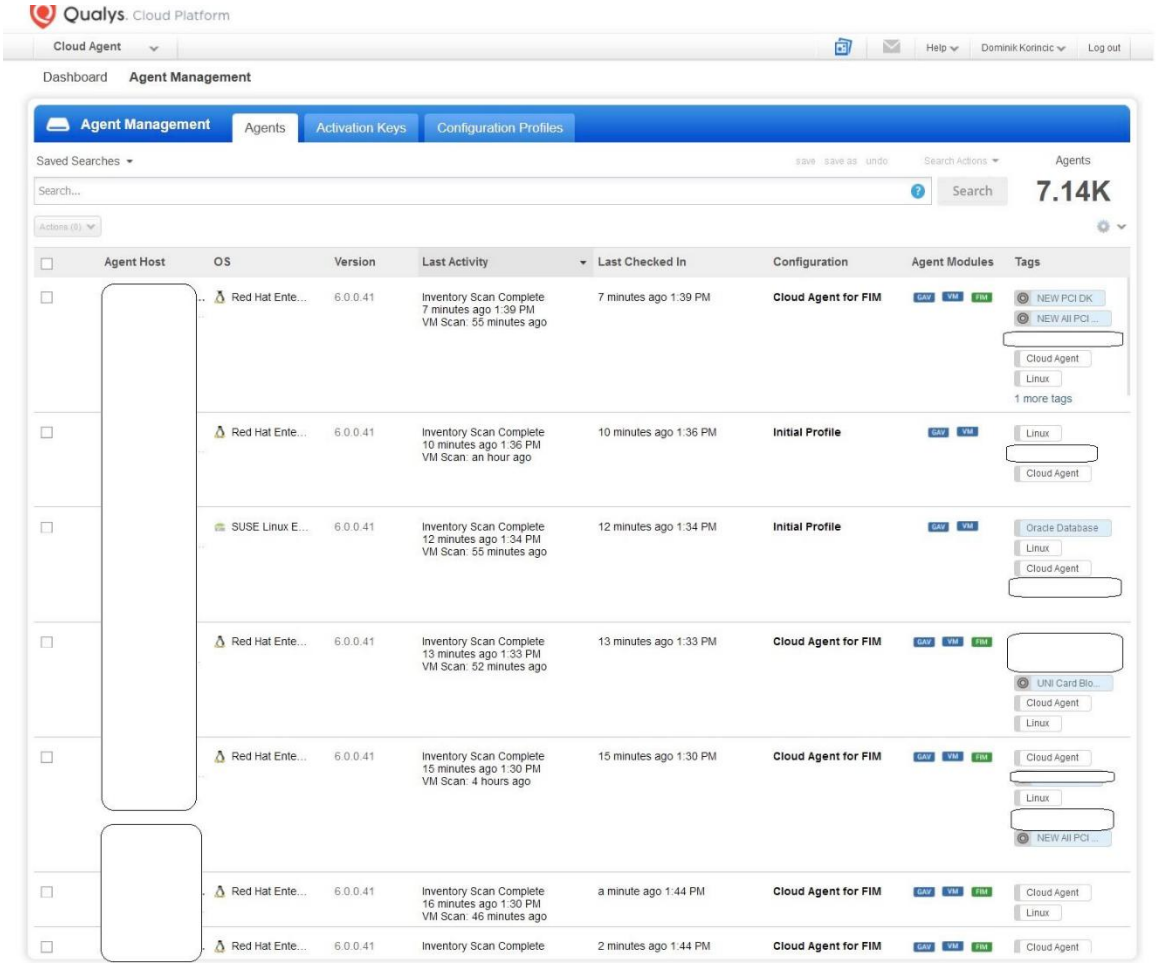
Откако ќе се воспостават, активните агенти на Qualys се управуваат или преку централизиран мрежен интерфејс или со директно поврзување со терминалот на одредена машина - било да е тоа физичка или виртуелна. Во оваа организација, агентите на Qualys се инсталирани на сите машини, кои вклучуваат клиентски компјутери, серверски компјутери и одредена мрежна опрема. Со одлука на менаџерот за информациска безбедност, клиентите се конфигурирани да се поврзуваат со централниот сервер на секои 15 минути, при што истата динамика ја отстранува делтата (т.е. разликата) во познатите пропусти во однос на претходната врска.

Неавтентицирано скенирање се врши само кога се додаваат нови опсези на IP-адреси каде што се наоѓаат машините и мрежната опрема. Ова најчесто се усогласува со претходно наведениот факт дека овој сектор се карактеризира со чести преземања и продажби на други компании од истата гранка. Неавтентицираното скенирање, кое е побрзо, е само преодна фаза пред да се мапираат сите нови машини и да се воспостават процедури за скенирање и управување со динамиката и ранливоста.

[50] Qualys, Inc.: Qualys Vulnerability Management (VMDR), https://www.qualys.com/apps/vulnerability-management-detection-response/

5.3.2. Преглед на детектираните пропусти

На слика 10 е прикажан пример на централизиран интерфејс за управување со агенти.



Слика 10: Qualys интерфејс

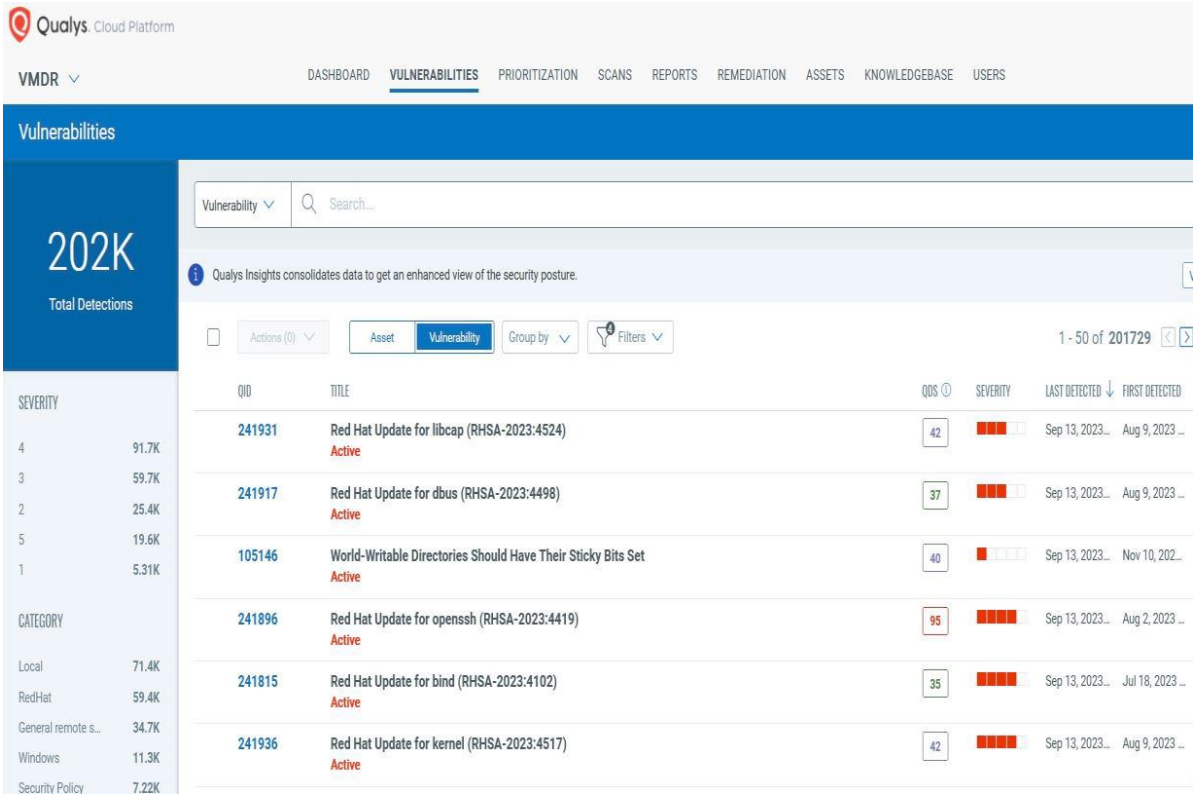
Извор: Авторот со сопствено истражување

Преглед на сите пропусти на дефиниран опсег на IP-адреси се следи преку маркерот QID[51]. На сликата 11 е прикажан преглед на сите пропусти откриени на машините во рамките на мрежниот периметар. Може да се прочитаат детали за

[51] Qualys QID (Qualys ID) е идентификациски број што се користи во рамките на платформата Qualys за да се идентификуваат одредени пропусти или безбедносни проблеми. QID е единствен идентификатор што Qualys го доделува на секоја ранливост што ја детектира или следи во системот.

секој QID, како и како да се отстрани ранливоста и статусот. Тие се динамични и тековни според поставената конфигурација.[52]

Главниот параметар според кој се одредува брзината и начинот на третирање на ранливостите е критичноста (engl. severity), но со оглед на тоа што Qualys е првото ниво на управување со ранливости кое исклучиво се занимава со скенирање, оваа технологија не ги решава пропустите, иако постои модул кој овозможува ова. Откриената ранливост се третира во понатамошна постапка, која е интегрирана со системот ServiceNow.



Слика 11: Преглед на ранливост од страна на Qualys

Извор: Авторот со сопствено истражување

Во Qualys, откако ќе се извршат скенирањата, извештаите за пронајдените пропусти може автоматски да се конфигурираат, генерираат и испраќаат. CISO - менаџерот за безбедност на информации ги конфигурира извештаите за

[52] Qualys, Inc.: Qualys Vulnerability Management (VMDR), https://www.qualys.com/apps/vulnerability-management-detection-response/

ранливост и испраќа извештај до сопствениците на опремата на кој се пронајдени ранливости. Има повеќе сопственици на машини во оваа организација бидејќи сите пропусти на машината се поделени според слојот што го покрива ранливоста. Ние првенствено го користевме моделот моделот TCI/IP[53]. На пример, на слојот на апликацијата е оперативниот систем, како и одредена апликација. Со внатрешна одлука, сопственикот, односно лицето одговорно за безбедноста на оперативниот систем и одредени апликации на тој апликативен систем, не се исто лице или функција во организацијата, а најчесто тоа се менаџерот на серверот, кој на него е инсталиран Windows OS[54] и, на пример, раководителот на одделот, задолжен за апликацијата за овластување за извршување на трансакција. Одговорност на CISO менаџерот за безбедност на информации е да распредели и испрати извештај за ранливост до лицето одговорно за таа ранливост. Одговорното лице, односно сопственикот на таа опрема, е одговорен за отстранување на ранливоста или, со соодветна аргументација, прифаќање на безбедносниот ризик во одреден период.

5.3.3. Управување со пропустите

Во оваа фаза се применува ServiceNow, кој е интегриран со Qualys. Сите наоди и податоци за ранливости се пренесуваат во апликацијата ServiceNow преку базата на податоци CMDB[55]. Пример за резултатот од таквата интеграција на овие две решенија е прегледот на сите пронајдени и мапирани пропусти, прикажан на сликата 12.

---

[53] Моделот TCP/IP е референтен модел за архитектурата на мрежните протоколи кои се користат за пренос на податоци преку мрежи. Се состои од четири слоеви: слој за пристап до мрежа, слој за интернет, слој за транспорт и слој на апликација. Секој слој има свои функции и одговорности во преносот на податоци. TCP/IP моделот е основа на интернет протоколот и овозможува комуникација помеѓу компјутерските системи во мрежата.

[54] Windows OS е семејство на популарни оперативни системи развиени и дистрибуирани од Microsoft Corporation. Тоа е широко користен оперативен систем на различни платформи, вклучувајќи компјутери, лаптопи, сервери и мобилни уреди. Windows OS обезбедува кориснички интерфејс, поддршка за апликации, управување со датотеки, мрежно поврзување и други функционалности. Доаѓа во различни изданија како Windows 10, Windows 8 и Windows 7 со различни карактеристики и приспособени верзии.

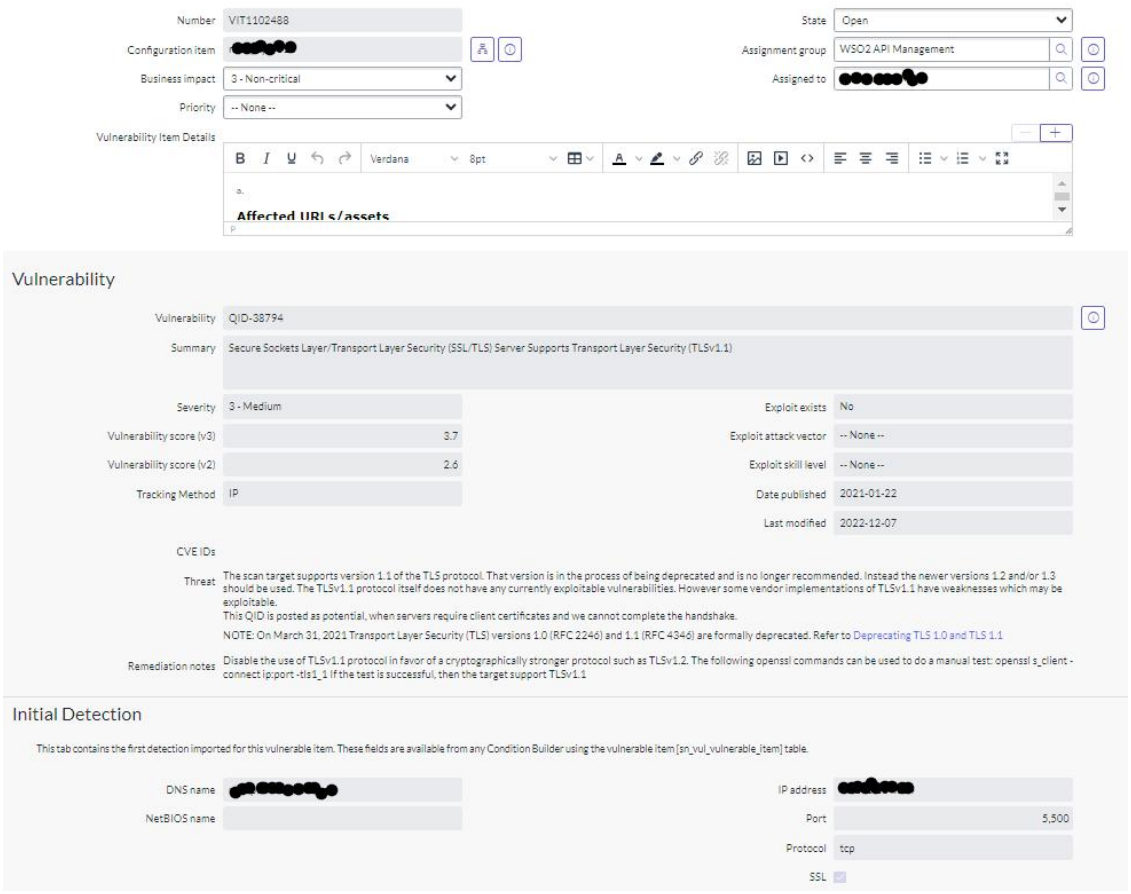
[55] CMDB (Eng. Configuration Management Database) е база на податоци што ги содржи сите информации за хардверските и софтверските компоненти што ги користиме за ИТ услугите на компанијата. Односите помеѓу овие компоненти се исто така фиксирани во CMDB. CMDB нуди јасен преглед на конфигурациските податоци и начин да се гледаат од посакуваната перспектива.

Number	State	Opened	Last found	Proof
Search	Search	Search	Search	Search
VIT0109286	Closed	2019-10-31 00:00	2023-06-14	EOL Software:jQuery Version 1.x or 2.x Detected. jquery-1.12.4.min.js
VIT1089166	Closed	2022-11-02 00:00	2022-11-02	
VIT1218939	Open	2023-06-04 00:00	2023-09-12	Install Location Version Detection Type /u01/app/oracle/product/13.2.0/agent/agent_13.4.0.0.0/oracle_common/jdk/bin/java 1.8.0_231-b34 Enhanced /u01/app/oracle/product/13.2.0/agent/agent_13.4.0.0.0/oracle_common/jdk/jre/bin/java 1.8.0_231-b34 Enhanced
VIT0288188	Closed	2019-11-11 00:00	2023-09-12	intclr 5810 0.4 0.6 11054476 1277168 ? Sl Aug 18 02:29:13 java -Djava.io.tmpdir=/opt/intclr/jetty_tmp -Dfile.encoding=UTF-8 -Duser.timezone=UTC -Xms256m -Xmx1024m -Dprocess.name=reachable-participant-app -Djava.security.egd=file:///dev/urandom -XX:+HeapDumpOnOutOfMemoryError -Dsun.net.inetaddr.ttl=30 -Djdk.security.allowNonCaAnchor=true -Xdebug -Xnoagent -Djava.compiler=NONE -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=*:7007 -jar curr/reachable-participant-app.jar debug --spring.config.location=./etc/,optional:./secure/secure-environment.properties
VIT1218872	Open	2023-06-04 00:00	2023-09-13	Vulnerable version of OpenSSH Detected: OpenSSH_7.4p1, OpenSSL 1.0.2k-fips 26 Jan 2017
VIT0625682	Closed	2020-12-11 00:00	2023-09-11	Install Location Version Detection Type /u01/app/oracle/product/13.2.0/agent/agent_13.2.0.0.0/oracle_common/jdk/jre/bin/java 1.7.0_111-b13 Enhanced /u01/app/oracle/product/13.2.0/agent/agent_13.2.0.0.0/oracle_common/jdk/bin/java 1.7.0_111-b13 Enhanced
VIT0134837	Closed	2019-11-11 00:00	2023-06-18	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\RebootPending exists
VIT1079599	Closed	2022-10-18 00:00	2022-10-18	
VIT1218981	Open	2023-06-04 00:00	2023-09-13	Install Location Version Detection Type /u01/app/oracle/product/13.2.0/agent/agent_13.4.0.0.0/oracle_common/jdk/bin/java 1.8.0_231-b34 Enhanced /u01/app/oracle/product/13.2.0/agent/agent_13.4.0.0.0/oracle_common/jdk/jre/bin/java 1.8.0_231-b34 Enhanced

Слика 12: Базата на податоци за сите ранливости на организацијата

Извор: Авторот со сопствено истражување

Во системот ServiceNow, на секоја ранливост му е доделен маркер RII (Vulnerability Identified Asset) по QID и IP адресата на машината. Во оваа фаза на мапирање, секој RII добива одредени неопходни параметри за понатамошно управување со оваа ранливост. Пример за еден таков RII е прикажан на сликата 13.



Слика 13: Детали за RII и потребните параметри

Извор: Авторот со сопствено истражување

Ранливоста понатаму допира до CISO - менаџерот за информациска безбедност, кој назначува одговорен оддел и менаџер на одреден RII, кој на крајот е одговорен да постапува на следниов начин во одредено време, што зависи од критичноста на самата ранливост:

1. Отстранување на ранливоста;
2. Прифаќање на ризикот со валидна аргументација;
3. Префрлање на одговорноста на друг оддел, со валидни аргументи.

За првото решение, CISO - менаџерот за безбедност на информации добива информации при понатамошното скенирање дали ранливоста е решена или не. За второто или третото решение, за да биде одобрено, потребно е CISO - менаџерот за информациска безбедност да го потврди внесениот избор во системот ServiceNow. Важен фактор во управувањето со ранливоста е прашањето

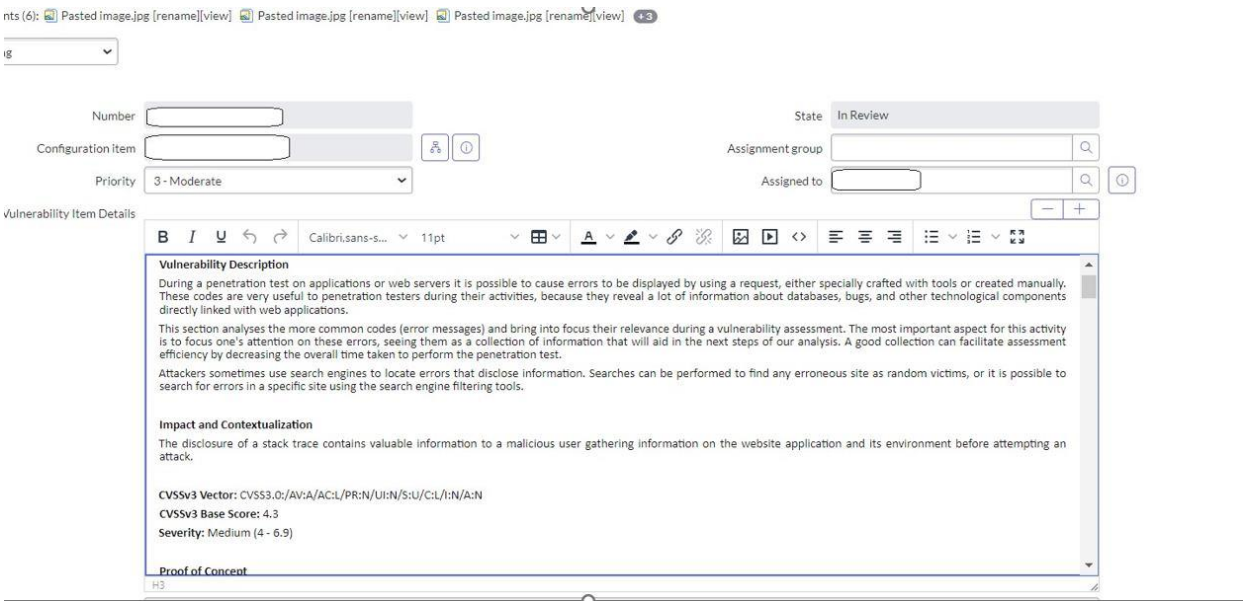
дали опсегот на IP е во опсегот на PCI DSS сертификацијата или не. Она што е, истовремено е критично средство за деловното работење на организацијата за картички и приоритет во преземањето заштитни активности.

Покрај автоматското пронаоѓање на ранливости со скенирање со решението Qualys, стандардот PCI DSS во делот 11.4.2 и 11.4.3 бара од професионалните и квалификувани поединци да спроведуваат внатрешен и надворешен тест за пенетрација најмалку еднаш годишно и по секоја значајна промена во инфраструктурата.[56] Тестирањето на пенетрацијата е задолжително на инфраструктурата која е во опсегот на самиот стандард и на сѐ што е класифицирано како критична инфраструктура неопходна за работа.

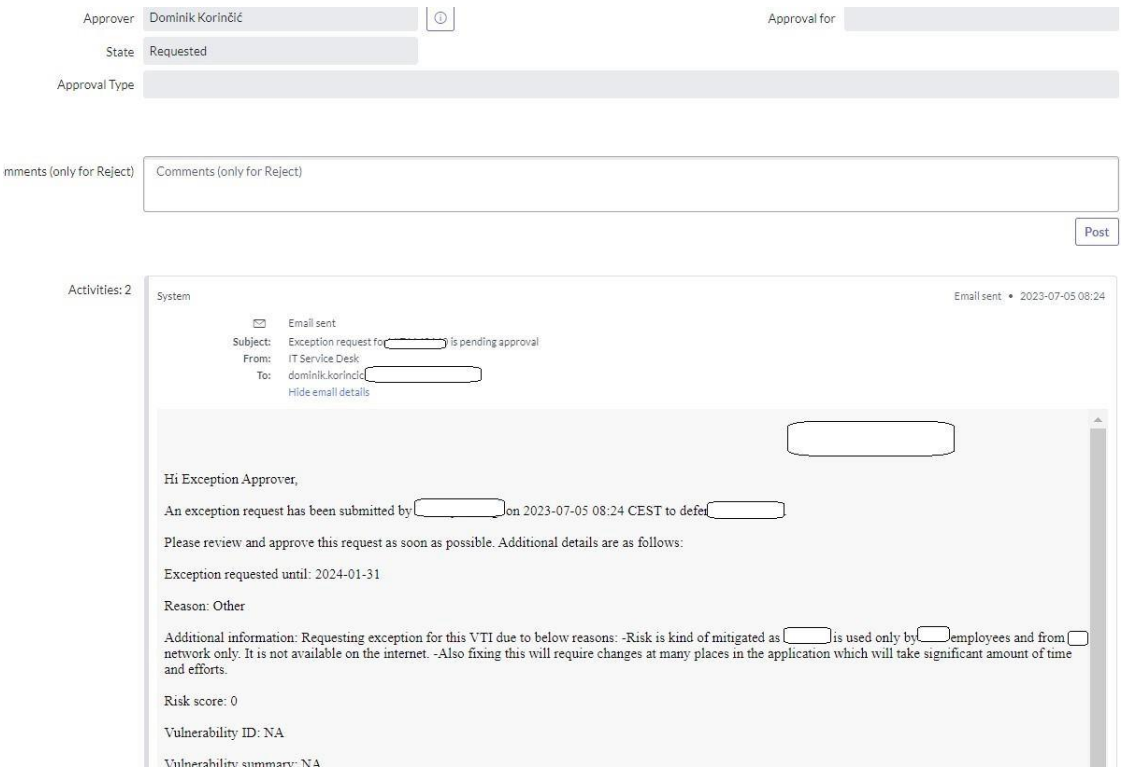
Резултатите од тестирањето за пенетрација се доставуваат истовремено до раководителот на одделот, кој е сопственик на ранливиот информациски ресурс, и до CISO - менаџерот за безбедност на информациите. CISO - менаџерот за информациска безбедност, на примерот на оваа организација, има цел тим од луѓе специјализирани за одредена област за информациска безбедност. Во зависност од критичноста на ранливоста пронајдена со тестот за пенетрација и дали таа е на информациско средство кое е покриено со безбедносниот стандард, се постапува според процедурата. Постапката е пропишана со Правилникот за управување со ранливоста и е задолжителна за сите вработени во организацијата. На крајот на краиштата, мора да се отстранат сите пропусти на средствата што се покриени со стандардот PCI DSS. Во случај на ранливости што не се на средство кое е под стандардот, сопственикот на тоа средство мора да одлучи дали да го прифати ризикот од таа ранливост или ќе ги преземе неопходните чекори за да го отстрани. Доколку го прифати ризикот од ранливост, ова прифаќање не може да биде подолго од една година, по што е должен да ја отстрани ранливоста или да понуди алтернативно решение. Без разлика на одлуката, целиот процес на крајот завршува со тоа што CISO - менаџерот за безбедност на информации го одобрил или не го одобрил бараното барање на сопственикот на ресурсот на кој се наоѓа ранливоста (сопственикот на ранливоста). Пример за едно такво барање за

[56] Security Standards Council, LLC : Payment Card Industry Data Security Standard: Requirements and Testing Procedures v4.0, https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf, 11.6. 2024.

одобрување на наодите за ранливост од тестирање на пенетрација е прикажан на сликата 14, а описот на ранливоста е прикажан на сликата 15, кои се направени од авторот.



Слика 14: Опис на наодите од тестот за пенетрација



Слика 15: Барање за одобрување третман на ранливост

5.4. Надворешен менаџер за информациска безбедност

Покрај опишаните примери на CISO - менаџери за информациска безбедност, во Република Македонија вакви функции најчесто се среќаваат во банките, осигурителните компании и телекомуникациите. Без разлика дали постои законска обврска за формирање на таква функција, функцијата CISO - менаџер за информациска безбедност постои во организациите од горенаведените сектори. Организациите, како резултат на тоа, за трендовите, регулаторните барања и барањата на нивните клиенти, ги направија свесни дека барањата за безбедност на информациите стануваат сè почести, поважни и постојано се менуваат. Еден од гореспоменатите аргументи беше доволен за да се одреди лицето одговорно за безбедноста на информациите, имено CISO. Од организација до организација нејзината систематизација во рамките на организационата шема на организацијата варира и подлежи на промени, но и на различни ставови и одлуки на менаџментот, од кои е јасен односот на менаџментот кон раководителот за информациска безбедност. Односот на CISO - менаџментот кон безбедноста на информациите може да се определи токму во однос на раководителот за информациска безбедност. Во корпоративниот свет, одредени поголеми организации често имаат главен службеник за безбедност (CSO, engl. chief security officer) кој поднесува извештај до CISO, а тој е одговорен за безбедноста на информациите пред раководството. Сепак, поради сложеноста на самата тема и важноста на безбедноста на информациите, дали CISO е член на одборот или не, зависи од тоа колку е важна безбедноста на информациите за таа организација.

Друг фактор кој влијае на тоа дали функцијата менаџер за безбедност на информациите е систематизирана во организацијата е искуството со безбедносни инциденти. Доколку организацијата имала безбедносен инцидент, чии последици имале финансиско влијание врз работењето на организацијата, веројатноста за вработување менаџер за безбедност на информации е голема. Во таа ситуација,

CISO е исто така многу оперативна функција, која навлегува во сите деловни и технички процеси на организацијата.

Ситуацијата во која регулативата и клиентите бараат сè повеќе и повеќе, вклучително и во однос на безбедноста на информациите, создава дополнителни активности и работа за постојните вработени кои често ги немаат потребните компетенции или искуство во прашањата за безбедноста на информациите, како што се: проценка на ризикот на информацискиот систем, ранливост управување, тестирање на пенетрација и решавање на безбедносни инциденти.

Ова создава потреба за функција CISO - менаџер за безбедност на информации која не е проформа позиција, туку личност која може да преземе одговорност и да се справи со ризиците. Во моментот на пишување на овој труд, има многу малку поединци кои ги поседуваат сите потребни компетенции на пазарот, а оние кои ги имаат веќе имаат работа со натпросечни услови. Не е лесно да се најде и привлече соодветен специјалист. Како одговор на недостатокот на специјалисти и/или неможноста на организацијата да понуди соодветна компензација на таков вработен, можно е да се договори со надворешен менаџер за безбедност на информации според моделот FaaS.

Договорот за аутсорсинг на таква функција мора да подлежи на длабинска проверка од страна на регулаторот, потоа мора да ги исполнува професионалните критериуми - искуство, соодветно образование и сертификација. Кога ова е задоволено, можно е да се има договорна функција на менаџер за информациска безбедност, кој може да исполни одредени регулаторни и безбедносни барања со соодветна месечна стапка на час. Предноста на таквата форма е што таков поединец може да дојде од организација која е специјализирана за безбедност на информации и има на располагање неколку експерти од различни области на информацискатa безбедност. Недостаток е фактот што саатнината на таков поединец може да биде ограничена и дека познавањето на внатрешните организациски процеси и технологии може да биде на пониско ниво отколку во ситуацијата на внатрешно вработување и систематизација на функцијата менаџер за безбедност на информациите.

6. Трендови во информацискатa безбедност

Трендовите за безбедност на информациите во контекст на функцијата на CISO - менаџерот за безбедност на информации во текот на 2023 година и во првата половина на 2024 година може да се опишат како повеќе од сè - повеќе ризици, повеќе можности и повеќе материјални надоместоци. На глобално ниво, функцијата на CISO - менаџер за информациска безбедност созрева во согласност со технолошките потреби на организацијата и придружните ризици, а тоа го става фокусот на безбедноста на информациите. Организациите и нивните менаџери мора да гледаат на иднината на функцијата CISO за да обезбедат успех и постојана организациска одржливост. За да биде возможно горенаведеното, потребно е да се инвестира во развој на функцијата на CISO, за да се инвестира во зголемување на знаењето и стручноста, лидерски вештини и соодветна компензација.

Според истражувањето спроведено во 2023 година, менаџерите за безбедност на информации ги истакнале следните ризици:[57]

- напредок во вештачката интелигенција и машинското учење;
- геополитички ризици поврзани со воени конфликти;
- хакерски напади, спонзорирани од државата и оние на криминални групи.

Некои од заклучоците се како што следува: Може да се очекува дека заканите по безбедноста на информациите ќе продолжат да се развиваат со брзо темпо, што често е непредвидливо и неочекувано. Тие сметаат дека систематскиот ризик ќе продолжи да се зголемува поради зависноста од само неколку производители. Трендот во кој сè повеќе инфраструктура се пренесува на давателите на облак услуги, а покрај тоа, забележлив е недостаток на вештини за примена на облак решенија, што во крајна линија е ризик.[58]

---

[57] Hedrick & Struggles: „ 2023 Global Chief Information Security Officer Survey“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief- information-security-officer-survey, 10.6.2024.
[58] Ibidem

Знаењето и експертизата се сè поважни, не само на оперативно ниво, туку и на ниво на управување на организациите. Потребата за високо ниво на стручност повлекува ризик - ризик од талент. Неверојатни 41 % од испитаниците потврдиле дека нивните организации немаат разработен план за замена на CISO - менаџерот за безбедност на информациите. Организациите треба да се подготват за ситуација во која актуелниот шеф на информацискатa безбедност ја напушта организацијата.[59]

Во 2023 година, во споредба со истиот период минатата година, уделот на менаџерите за безбедност на информации кои се членови на управни одбори е двојно зголемен, но сепак е мал, што докажува фактот дека во одборите на организациите има удел на членови кои разбираат и /или ги имаат потребните вештини за безбедност на информациите е мал.[60] Во Соединетите Американски Држави, SEC (eng. Securities and Exchange Commission) за првпат објави упатства според кои наскоро сите организации кои котираат на берзата треба да објават кој член на одборот, доколку ги има, има соодветно познавање на безбедноста на информациите.[61] Горенаведеното претставува дополнителен простор за унапредување на функцијата на менаџерот за безбедност на информациите, но од друга страна, поставува сложени прашања, како на пример: Кое е соодветно ниво на компетентност за безбедноста на информациите за член на одборот на таква организација?

6.1. Резултати од истражувањето

Клучните показатели на истражувањето се дадени во табелата 11.

Табела 11: Трендови на функцијата CISO

Организациска структура и ризици	Надомест
41 % од испитаниците кои ја	CISO во САД се меѓу најплатените

[59] Hedrick & Struggles: „ 2023 Global Chief Information Security Officer Survey“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief- information-security-officer-survey, 10.6.2024.
[60] Ibidem
[61] Ibidem

извршуваат функцијата на CISO во организацијата потврдиле дека нивната организација нема план за замена на CISO, а 13 % од нив потврдиле дека организацијата дури не ни планира да направи таков план.	професионалци во ИТ со просечен бруто годишен приход од 620.000 УСД, со дополнителни бенефиции во опциите и акциите на компанијата од 1.100.000 УСД. Горенаведеното претставува раст од 6 % во однос на 2022 година.
Ова е загрижувачки ако се земе предвид важноста на оваа функција. Според истражувањето, 76 % од сите испитаници потврдиле дека се целосно отворени за промена на работодавачот во следните три години. Недостигот на план за замена е организациски ризик.	Истите бројки за ЕУ + Обединетото кралство се 457.000 УСД во бруто приход и 552.000 УСД во опции и акции. Нема веродостојни податоци за Република Македонија, но таа е земја кандидат за ЕУ, така што трендовите и конвергенцијата во поразвиените области треба да ги стимулираат трендовите и во Македонија.
Не е изненадување што вештачката интелигенција е прогласена за најголема закана во следните пет години. Оваа закана бара еволуција и систематски развој на функцијата на CISO и потребните вештини. Горенаведеното е во прилог на фактот и трендот дека функцијата CISO станува се повеќе и повеќе техничка функција. Постои значителен услов за CISO да го разбере софтверското инженерство и безбедноста на cloud computing. Општо земено, од CISO се бара да имаат технички вештини.	Во Австралија се наведени показателите за приход од 368.000 УСД и 586.000 УСД во опции и акции.
Охрабрувачки е што 80 % од испитаниците потврдиле дека се	На глобално ниво, најплатените CISO се во финансискиот сектор, додека оние

способни да инвестираат во лидерство и развој за да го подигнат нивото на експертиза во тимот.	со највисоки придобивки во опциите и акциите доаѓаат од технолошкиот и услужниот сектор во економијата.
Севкупно, половина од испитаниците потврдиле дека мислат дека менаџментот делумно или целосно не ги разбира наодите што им ги презентира CISO, додека во исто време 30% од нив се дел од раководството во организацијата, наспроти 14% во 2022 година.	

Извор: Hedrick & Struggles: „ 2023 Global Chief Information Security Officer Survey“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief-information-security-officer-survey, 10.6.2024.

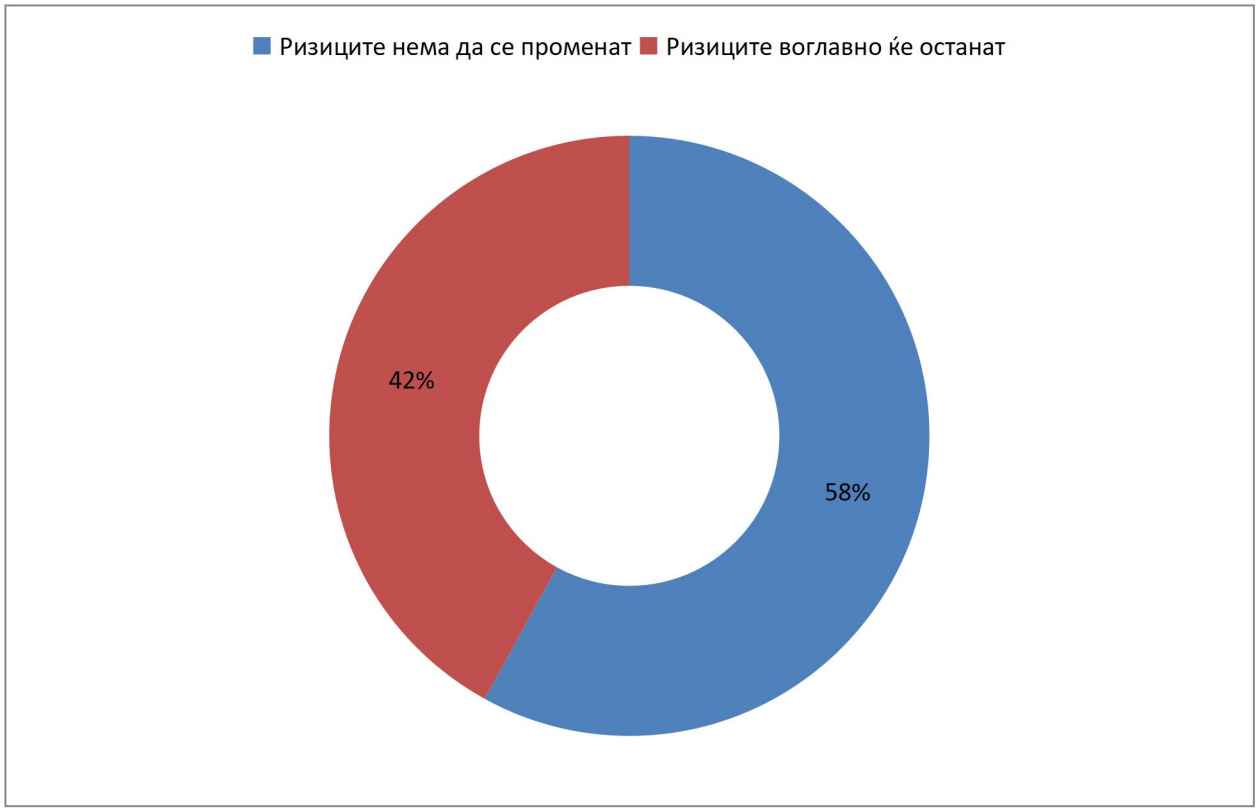
Фактот дека 41 % од испитаниците потврдиле дека не постои план во организацијата да го замени сегашниот CISO - менаџер за информациска безбедност е сериозен проблем бидејќи организациите не можат да си дозволат да имаат отворена позиција на CISO, поради повеќе причини, вклучувајќи:

- Закана – безбедносните закани со кои се соочуваат организациите денес резултираат со недостаток на план за замена за CISO - менаџерот за безбедност на информации, што не е само проблем со човечките ресурси, туку е и деловен проблем за целата организација.
- Регулатива - ризикот од безбедноста на информациите е ризик на ниво на управување на компаниите во регулираниот сектор. Тоа е забележливо и од страната на регулаторните тела, кои постоењето и непостоењето на CISO - менаџер за информациска безбедност го третираат како клучен показател за подготвеност за безбедносен инцидент, каде што регулаторот ја пропишал неопходноста од постоење на информациска безбедност. Во Македонија овие субјекти се сметаат за критична инфраструктура.

- Достапност – експертите кои ја извршуваат функцијата на CISO тешко може да се разберат надвор од доменот на нивната дејност, така што во случај на промена на работодавачот, најверојатната промена е на истата функција. Наоѓањето соодветна замена бара и значителна количина на ресурси, како што се време, пари и напор.

  Според горенаведеното се поставува прашањето: Како да се најде CISO - менаџер за безбедност на информации? Ова прашање содржи голем број фактори, како што се сегашната и идната деловна стратегија, регулаторните барања, корпоративната култура и пазарните трендови. Од горенаведените причини, потребно е организацијата да има разработен план за замена на CISO - менаџер за безбедност на информации.

Важноста на CISO - менаџер за безбедност на информации продолжува да добива на значење и во 2024 година, пред сè поради развојот на вештачката интелигенција и особено поради стравувањата од хакерски напади (ransomware). Според истражувањето, резултатите прикажани на сликата 16 - Ризици за безбедноста на информациите во следните пет години и слика 17 - Главни фактори на ризик, покажуваат дека повеќето менаџери мислат дека вештачката интелигенција и машинското учење, потоа геополитичкиот ризик и хакерските напади се главните ризици. Исто така, во 2023 година, повеќе од половина од испитаниците сметаат дека овие ризици за безбедноста на информациите ќе бидат доминантни за пет години.



Слика 16: Ризици за безбедноста на информациите во следните пет години

Извор: Hedrick & Struggles: „2023 Global Chief Information Security Officer Survey“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief-information-security-officer-survey, 10.6.2024.

На прашањето кој е најголемиот ризик за CISO - менаџерите за безбедност на информации на лично ниво, одговорот бил проследен со коментари, како што се:[62]

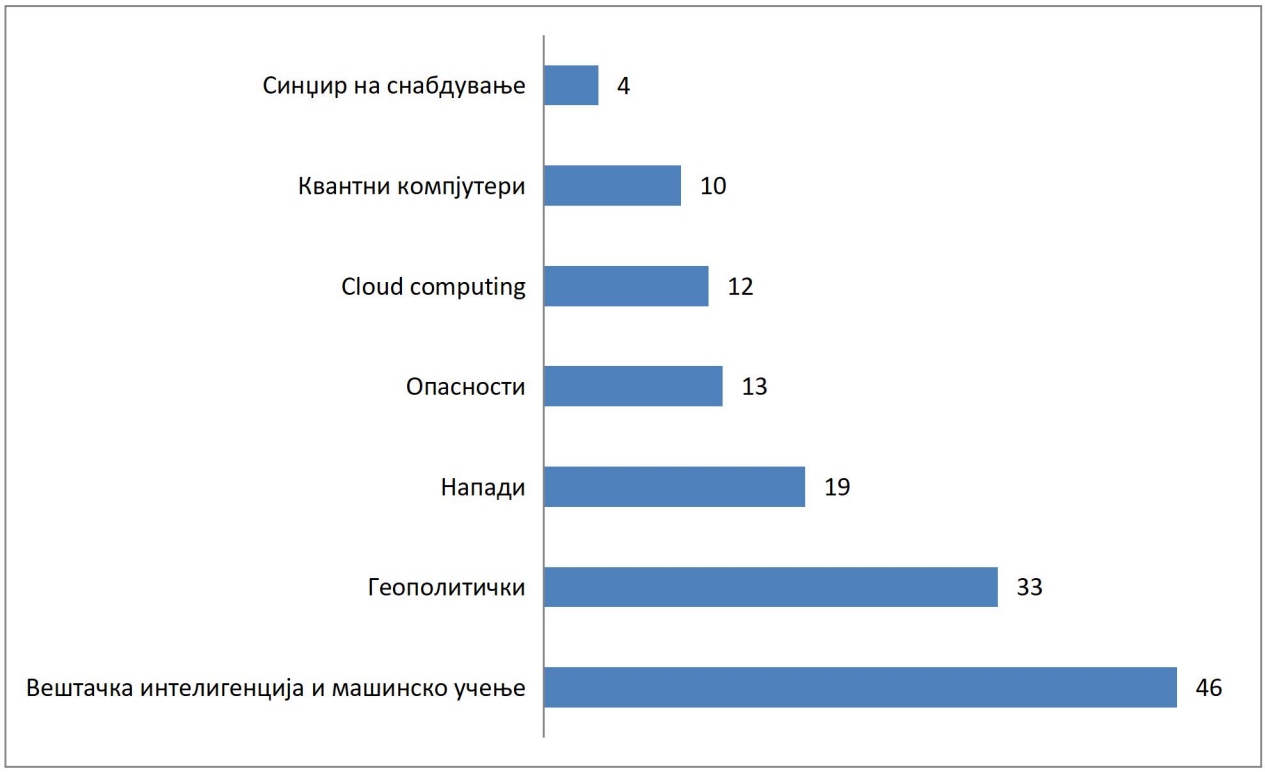
Трката за автоматизирање на активностите ќе продолжи.

Сè почести напади бараат побрзи и побрзи одговори.

Нападите стануваат сè побрзи и побрзи, до ниво на автоматизација, додека одговорите остануваат на ниво на човечка способност.

[62] Hedrick & Struggles: „ 2023 Global Chief Information Security Officer Survey“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief- information-security-officer-survey, 10.6.2024.

Развојот на компетенциите потребни за одговор на безбедносен инцидент не се во чекор со развојот на методите за напад.



Слика 17: Главни фактори на ризик

Извор: Hedrick & Struggles: „ 2023 Global Chief Information Security Officer Survey“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief-information-security-officer-survey, 10.6.2024.

Според истражувањата, стресот, исцрпеноста и заситеноста се најголемите предизвици и проблеми за повеќето CISO - менаџери за безбедност на информациите, во малку поголема мера отколку што било во 2022 година.[63]

Во 2023 година, за здравствениот и финансискиот сектор, безбедносните инциденти се најголемиот предизвик, пред сè затоа што овие сектори минуваат низ брз процес на дигитализација на процесите и активностите.[64] Поттикнувањето

[63] Hedrick & Struggles: „ 2023 Global Chief Information Security Officer Survey“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief- information-security-officer-survey, 10.6.2024.
[64] Ibidem

на дигитализацијата на процесите и постоечките активности го комплицира прашањето за безбедноста. 89 % од CISO - менаџерите за безбедност на информациите се согласуваат со фактот дека пребрзата дигитализација овозможува појава на непредвидливи ризици за податоците на овие организации.[65] 47 % од менаџерите за безбедност на информации веруваат дека здравствениот сектор има најмногу проблеми со безбедносни инциденти, додека 42 % од нив сметаат дека тоа е финансискиот сектор.[66]

Горенаведеното е последица на тоа што организациите од здравствениот и финансискиот сектор би останале конкурентни, а за да ги исполнат очекувањата на своите клиенти, тие се принудени да ги забрзаат процесите на дигитализација на нивните услуги. Брзината многу често ја исклучува соодветната безбедност и отвора можност на злонамерните актери да ја искористат. Парадоксален за овој резултат е резултатот од истражувањето кое предупредува дека секторите здравство и финансии се токму секторите во кои е најтешко да се оправдаат буџетите за информациска безбедност.[67] Сето горенаведено покажува дека во никој случај не е лесно за менаџерите за безбедност на информации во здравството и финансиите.

Речиси половина од анкетираните CISO - менаџери за безбедност на информациите се загрижени дека нарушување на безбедноста и инцидентите може да резултираат со нивна лична одговорност, што ќе доведе до кривично гонење и казни за нив. 99 % од испитаниците признаваат личен предизвик кој произлегува од нивната работа, од кои 48 % се однесуваат на загриженост за судските процеси, а 45 % се однесуваат на зголемена лична одговорност.[68] За да се ублажи овој предизвик, организациите треба да понудат соодветни безбедносни процеси и алатки кои му даваат на CISO - менаџерот за безбедност на информации задоволителен поглед на сите безбедносни ризици. Само од оваа позиција, поединецот кој е одговорен може да ги затвори сите несогласувања во безбедносните контроли и состојбата на информациската инфраструктура. Така

[65] Salt Security: „State of the CISO, A global report on priorities, pain points, and security gaps 2023“, https://content.salt.security/global-state-ciso-report-2023.html, 11.5.2024.
[66] Ibidem
[67] Ibidem
[68] Ibidem

може да се намали стравот од лична одговорност. Во денешно време, во кое CISO - менаџерот за информациска безбедност станува сè поважна функција во организацијата, менаџментот на истата организација не може да си дозволи ризик CISO да си замине поради страв од лична одговорност.

Безбедноста на API беше нагласена од 78 % од CISO како една од приоритетните активности, а 95 % од нив потврдија дека мора да се изврши безбедносна ревизија на постоечките API во следните две години. Во согласност со трендовите на пазарот, во последните две години, употребата на API - директно или индиректно - резултира со безбедносно неусогласеност со препорачаните безбедносни практики. API имаат најголем потенцијал да влијаат на успехот на дигиталната трансформација на организацијата, имајќи предвид дека тие се интегрирани во повеќето денешни апликации. Во овој поглед, главниот предизвик за CISO се API кои се применуваат во процесот на обезбедување на организацијата. Тие имаат интегрирано дел од апликациите кои комуницираат со апликации од трети страни, така што зголемувањето на нивната безбедност е приоритет и една од главните активности на CISO - менаџерите за информациска безбедност.[69]

7. Заклучок

Како резултат на постојаните промени, без разлика дали преку технолошкиот развој или општествено донесените одлуки, средината во која функционираат денешните организации - деловна или не, јавна или приватна, профитна или непрофитна - сите тие имаат своја цел која зависи од овие промени. Следствено, безбедноста како фактор во постигнувањето на целите со нејзината, условно кажано - подмножество на информациска безбедност, станува сè повидлив фактор на ниво на поединци кои носат одлуки кои ги засегаат

[69] Salt Security: „State of the CISO, A global report on priorities, pain points, and security gaps 2023“, https://content.salt.security/global-state-ciso-report-2023.html, 11.5.2024.

организациите, а следствено и на сите оние кои зависат од нив. Безбедносните инциденти кои се манифестација на хакерски напади, во кои векторот на нападот е технологија поврзана со деловните процеси на нападнатата организација, сè повеќе се придружени со детални извештаи, кои најчесто се и медиумски експонирани. Покрај финансиската штета, тие резултираат и со штета на угледот, а по самиот инцидент, честопати следат промени во организацијата кои ги погодуваат сите членови/вработени во организацијата. За да се намали ризикот од инцидент, потребна е свест и компетентност. Овој труд го опишува решението за споменатите предизвици, така што организациите ги систематизираат функциите на менаџерот за безбедност на информации, т.е. CISO, или ја обезбедува наведената функција преку ангажирање на надворешен партнер. Даден е теоретскиот концепт, како и карактеристиките и неопходните компетенции, знаења и вештини кои се резултат на долгогодишно искуство на релевантните поединци, од кои јасно е видливо дека менаџерот за безбедност на информации, покрај техничките вештини, мора да биде свесен за деловните процеси и да поседува лидерски вештини. Една од главните активности и одговорности на менаџерот за безбедност на информации е проценката на ризиците поврзани со информациско-комуникациските технологии. Ова е клучна активност и предуслов за воспоставување на ISMS и сите потребни политики и процедури за управување со безбедноста на информациите. Комплетен регистар на информациски средства со јасни и реални закани и ранливости е основа за воспоставување контроли за намалување на ризикот, процедури за спроведување, сертификација поврзана со безбедноста на информациите и исполнување на регулаторните барања и барањата на клиентите.

Во дадениот преглед на директиви на ЕУ, може да се заклучи дека постои правна основа за воспоставување на функцијата менаџер за информациска безбедност. Во одредени директиви тоа е експлицитно наведено, додека во други индиректно се отвора можноста за многу потребни активности, без експлицитно да се забрани воспоставување на самата функција менаџер за безбедност на информации.

Во студиите на случај кои ги опишуваат активностите на менаџерите за информациска безбедност во различни организации во Република Македонија, може да се заклучи дека функцијата CISO е добро позната и барана, а самите активности и одговорности значително зависат од секторот на кој организацијата припаѓа и на големината и структурата на самата организација. Трендовите диктирани од поразвиените пазари се прелеваат на територијата на Република Македонија преку филијалите на мултинационалните корпорации, додека трендовите и новитетите на полето на опасноста сепак имаат глобален карактер. Организациите во Република Македонија не се изолирани, а глобално присутните закани за безбедноста на информациите се присутни и во Република Македонија.

Менаџерот за безбедност на информации треба да покрива широк опсег на активности, да има знаење и искуство, како и карактер кој може да се вклопи во организацијата. Покрај наведеното, треба да се поседува љубопитност и волја за постојано и доживотно образование и учење за технологијата и безбедноста на информациите. Глобалните барања, условите за работа и придобивките, како и недостатокот на експерти за информациска безбедност, кои исто така ги имаат сите гореспоменати карактеристики, ги прават менаџерите за безбедност на информации многу барани и дефицитарни - глобално и во Република Македонија. Главниот компаративен недостаток на Република Македонија е тоа што организацијата на нејзината територија не може да понуди работни услови кои се конкурентни на поразвиена средина - како во ЕУ, така и пошироко.

Како што веќе споменавме, едно од понудените решенија е договор за услуги на надворешниот менаџер за безбедност на информации според принципот FaaS, што има свои предности и недостатоци. Предноста е поширокиот дофат на различни експертизи во областа на информацискатa безбедност, а недостаток се ограничените саатнини, недоволното познавање на внатрешните процеси, ризикот и одговорноста од трета страна. Од истражувањето спроведено во 2023 година, јасно може да се заклучи дека најчеста причина за заминување на менаџерите за безбедност на информации е проблемот со немањето план за замена на овие лица. Склучувањето договор со надворешен CISO според

принципот FaaS, со континуирана контрола на неговиот ангажман и придонес, е решението за овие предизвици.

Според сè што е претставено во овој труд, новите регулативи и трендови ќе ја направат функцијата менаџер за безбедност на информации сè поважна - и на глобално ниво и во Република Македонија.

Користена литература

1. Aronson, E., The Social Animal. New York: W. H. Freeman and Company.Tipton, Harold F., and Micki Krause. Information Security Management Handbook, Fifth Ed. Auerbach Books, 1995
2. Barron, R. A. and Neuman, J. H., Workplace violence and workplace aggression: Evidence on their relative frequency and potential causes. Aggressive Behavior, Vol. 22, pp. 161–173, 1996
3. Baxter, V. and Margavio, A., Assaultive violence in the U.S. post office. Work & Occupations, Vol. 23, pp. 277–296, 1996
4. Carnegie, Dale. How to Win Friends and Influence People. BBS Pub. Corp., 1936.

5. Byham, William C., and Jeff Cox. Zapp! The Lightning of Empowerment. Ballantine Books, 1988.
6. Covey, Stephen F. The 7 Habits of Highly Effective People. Simon& Schuster, 1989.
7. Brinkman, Rick, and Rick Kirschner. Dealing with People You Can't Stand. McGraw-Hill, 2002.
8. David Kim and Michael G. Solomon: „Fundamentals of Information Systems Security" Burlington, USA, 2018.
9. Buckingham, Marcus, and Curt Coffman. First, Break All the Rules.
10. Simon & Schuster, 1999.
11. Hammer, Michael, and Steven A. Stanton. The Reengineering Revolution. HarperBusiness, 1995.
12. Baird, Michael L. Engineering Your Start-Up. Professional Publications, 1999.
13. Dobyns, Lloyd, and Clare Crawford-Mason. Think About Quality, Random House, 1994.
14. Bridges, William. Managing Transitions. Perseus Books, 1991
15. Yourdon, Edward. Death March (The Complete Software Developer's Guide to Surviving "Mission Impossible" Projects). Prentice Hall, 1997.
16. McCarthy, Jim. Dynamic of Software Development. Microsoft Press, 1995.
17. Malcolm W. Harkins: „Managing Risk and Information Security, Protect to Enable", 2 ed., Folsom, Kalifornia, USA, 2016
18. Beckwith, Harry. Selling the Invisible (A Field Guide to Modern Marketing). Warner Books, 1997.
19. Beckwith, Harry. What Clients Love (A Field Guide to Growing Your Business). Warner Books, 2003.
20. Peters, Tom. Reinventing Work: The Brand You 50, Alfred A. Knopf, 1999.
21. Shonka, Mark, and Dan Kosch. Beyond Selling Value: A Proven Process to Avoid the Vendor Trap. Dearborn Trade Pub. 2002.
22. Peters, Tom. Re-Imagine. Dorling Kindersley Pub. 2003.
23. Manning, Tony. Making Sense of Strategy. AMACOM, 2001.

24. Buckingham, Marcus, and Clifton, Donald O. Now, Discover Your Strengths. Free Press (Simon & Schuster), 2001
25. Burke, W. W., The new agenda for organization development. Organizational Dynamics, 26, 1, 7–20, 1997
26. (ISC)2 Common Body of Knowledge.
27. Maxwell, John. The 17 Essential Qualities of a Team Player: Becoming The Kind Of Person Every Team Wants. Thomas Nelson, 2002.
28. Marco Morana and co-autors: „ Application Security Guide For CISOs“, OWASP, 1.0 v, 2013. https://owasp.org/www-pdf-archive/Owasp-ciso-guide.pdf
29. Wood, Charles Cresson. Information Security Policies Made Easy: A Comprehensive Set of Information Security Policies (Version 9). 2004.
30. Covey, Stephen, Roger A. Merrill, and Rebecca R., First Things First. Fireside (Simon & Schuster), 1994.
31. Snead, G. Lynne, and Joyce Wycoff. To Do Doing Done!: A Creative Approach To Managing Projects and Effectively Finishing What Matters Most. Fireside (Simon & Schuster), 1997.
32. Fisher, Roger, and Alan Sharp. Getting It Done: How To Lead When You’re Not In Charge. Harper Business, 1998.
33. Herriot, P. and Pemberton, C., Contracting careers. Human Relations, Vol. 49, pp. 757–790., 1996
34. Harold F. Tipton and Micki Krause: „Information Security Mangment Handbook“, 6. izdanje, Boca Raton, Florida, USA, 2007.
35. Schoenbeck, Dave: Essential Ingredients of a Small Business SWOT Analysis, , https://daveschoenbeck.com/essential-ingredients-small-business swotanalysis/, 21.5.2024.
36. Herold, R. Ethics section, in Official (ISC) Guide to the CISSP CBK, H. Tipton and K. Henry (Eds.), pp. 71–86, Auerbach, Boca Raton, FL, 2006
37. Levinson, M.,CIO Magazine, CXO Media, Inc. http://www.cio.com/ archive/060106/ag_edwards.html, 2006
38. Musashi, Miyamoto. The Book of Five Rings (Gorin No Sho): A Guide To Winning Strategy. Bantam New Age Books, 1982.

39. Roberts, Wess, Leadership Secrets of Attila the Hun. Warner Books, 1990.
40. Tzu, Sun. The Art of War [Translated by Thomas Cleary]. Shambhala Pub. 1988.
41. Benton, D.A. Executive Charisma. McGraw-Hill, 2003.
42. Šegudović, Hrvoje: „Prednosti i nedostaci metoda za kvalitativnu analizu rizika“,Infigo IS d.o.o., Zagreb, 2006

Интернет-извори:

1. www.cisohandbook.com
2. www.isc2.org
3. www.sans.org
4. www.securityfocus.com
5. www.csrc.nist.gov
6. City University of Seattle: Business & Management, https://library.cityu.edu/researchguides/business/swot, 21.5. 2024.
7. de Bruin, Lars: Scanning the Environment: PESTEL Analysis, https://www.business-to-you.com/scanning-the-environment-pestel-analysis/, 21.5.2024.
8. ISACA, 2012. - Fundamental Concepts of IT Security Assurance, https://www.isaca.org/resources/isaca-journal/past-issues/2012/fundamental-concepts-of-it-security-assurance, 5.6.2024
9. International Organization for Standardization – ISO: ISO 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary https://www.iso.org/standard/73906.html, 11. 6. 2024.
10. International Organization for Standardization – ISO: ISO 31000:2018 Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en, 18.6.2024.
11. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection Guidance on managing information security risks https://www.iso.org/standard/80585.html, 18. 5. 2024

12. Pedro Monzelo and Sergio Nunes: „The Role of the Chief Information Security Officer (CISO) in Organizations“, University of Lisbon, Lisbon, 2019. https://www.researchgate.net/publication/338833079 15.5.2024
13. EUR-Lex: Direktiva (EU) 2015/2236, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32015L2366, 8.5.2024.
14. https://www.hub.hr/en/psd2-open-api, 24.6.2024
15. Hedrick & Struggles: „ 2023 Global Chief Information Security Officer Survey“, https://www.heidrick.com/en/insights/cybersecurity/2023-global-chief-information-security-officer-survey, 10.6.2024.
16. Salt Security: „State of the CISO, A global report on priorities, pain points, and security gaps 2023“, https://content.salt.security/global-state-ciso-report-2023.html, 11.5.2023.

Список на табели

Табела 1: Карактеристики на лидерите во областа на сајбер-безбедноста

Табела 2: Пример за критериуми за прифаќање ризици за безбедноста на информациите

Табела 3: Пример за каталог на средства со ранливости и закани

Табела 4: Пример за одредување на вредноста на податоците врз основа на параметрите на CIA (Confidentiality Integrity Availability)

Табела 5: Пример за опсег на вредност на имотот

Табела 6: Пример за опсегот на вредности на веројатноста за реализација на заканата

Табела 7: Пример за низа вредности на ранливост на средствата

Табела 8: Изменета матрица за проценка на вредностите на нивото на ризик

Табела 9: Организациски безбедносни контроли

Табела 10: Цели на системот за управување со безбедноста на информациите

Список на слики

Слика 1: ИТ-експерт за Т-облик и Z-облик CISO

Слика 2: Референтен модел на управување со безбедноста на информациите

Слика 3: Презентирање на принципите, рамката и процесот на управување со ризик во согласност со стандардот ISO/IEC 31000

Слика 4: PESTLE анализа

Слика 5: SWOT анализа

Слика 6: PSD2 и XS2A околина

Слика 7: VMDR модул на Qualys

Слика 8: Генерирање на клучот за активирање на Qualys агентот

Слика 9: Qualys скенери

Слика 10: Qualys интерфејс

Слика 11: Преглед на ранливост од страна на Qualys

Слика 12: Базата на податоци за сите ранливости на организацијата

Слика 13: Детали за RII и потребните параметри

Слика 14: Опис на наодите од тестот за пенетрација

Слика 15: Барање за одобрување третман на ранливост

Слика 16: Ризици за безбедноста на информациите во следните пет години

Слика 17: Главни фактори на ризик