IT4Sec Reports 139
https://doi.org/10.11610/it4sec.0139

Програма за киберсигурност на организацията

Венелин Георгиев

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

София, юли 2021

Венелин Георгиев, Програма за киберсигурност на организацията**,** *IT4Sec Reports 139* (юли 2021), https://doi.org/10.11610/it4sec.0139

IT4Sec Reports 139 „Програма за киберсигурност на организацията“ Често срещаното в литературата твърдение, че информационните технологии необратимо са навлезли в ежедневието на потребителите в личен и професионален план може да се приеме за вярно при условие, че степента за сигурност на тези технологии е на достатъчно високо ниво. Изпълнението на това условие намира израз в отношението на организациите и потребителите към сигурността на информационните системи, мрежи, приложения и информация. Възможните подходи за осигуряване на киберсигурност в организацията са два: ad-hoc подход и системен подход. В материала се аргументират ползите от използване на системния подход при третиране на проблемите с киберсигурността на базата на разработване, приемане, прилагане и обновяване на програма за киберсигурност на организацията.

Ключови думи: програма за киберсигурност, заплахи, уязвимости, контроли за киберсигурност, защита в дълбочина, противодействие на инциденти с киберсигурността

IT4SecReports 139 “An Organizational Cybersecurity Program” Information technologies have irreversibly entered the daily lives of consumers personally and professionally. This technology influx can be accepted as long as security is maintained at a sufficiently high level. The fulfillment of this condition is reflected in the attitude of organizations and users to the security of information systems, networks, applications and information. There are two possible options for ensuring cybersecurity in the organization: ad-hoc approach and systematic approach. This report expounds on the benefits of using a systematic approach in dealing with cybersecurity challenges based on the development, adoption, implementation and updating a dedicated organizational cybersecurity program.

Keywords: cybersecurity program, threats, vulnerabilities, cybersecurity controls, in-depth protection, managing cybersecurity incidents

ISSN 1314-5614

ВЪВЕДЕНИЕ

Погледнато в общия случай, подходът към киберсигурността на организацията може да се реализира по два начина. Първият начин е чрез прилагане на т.нар. ad-hoc подход, при който проблемите с киберсигурността се разрешават в движение, в оперативен порядък, без наличие на предварително разработена програма за киберсигурност. В този случай е налице висок риск за това организацията да се окаже неподготвена за възникващите инциденти с компютърните системи, мрежи, приложения и информация, от което да претърпи значими щети, в това число финансови и репутационни.

За втория начин е характерна по-висока степен на организираност и системност в отношението към проблемите на киберсигурността в организацията, което намира израз в разработване, прилагане, поддържане и актуализиране на програма за киберсигурност. Създаването на програма за киберсигурност се оказва не само въпрос на правилно разбиране на важността на проблемите в сферата на киберсигурността, но и измерител за зрелостта и ефективността на ръководството и мениджмънта на организацията като цяло.

СЪЩНОСТ НА ПРОГРАМАТА ЗА КИБЕРСИГУРНОСТ

Често пъти специалистите по киберсигурност срещат затруднения да комуникират със стратегическия мениджмънт на организацията по въпроси от полето на тяхната специалност. Обратното също е вярно, особено когато мениджърите трябва да комуникират с техническите изпълнители по въпроси от стратегията за киберсигурност на компанията. Отстрани ситуацията изглежда като че двете страни говорят на различни езици и не разполагат с необходимото знание за едно ползотворно съвместно общуване. В интерес на компанията е едно подобно несъответствие да бъде преодоляно. На практика това може да бъде постигнато чрез разработване и прилагане на програма за киберсигурност.

Ключови фактори за успех при разработване на една програма за киберсигурност могат да бъдат:

- поддържане и развитие на отношения от страна на ръководството на компанията със специалистите и по проблемите на киберсигурността;
- проектиране, разработване, внедряване, използване и актуализиране на програма за киберсигурност по същия начин, както при останалите функции на компанията;
- използване на стандартизиран рамков подход, който позволява разработването на програма за киберсигурност с възможност за нейното използване през по-дълъг период без необходимост от съществени промени и възможност за извършване на незначителни такива;
- създаване на възможност чрез подходяща система от метрики да бъде измервана ефективността на програмата за киберсигурност;
- разработване на достатъчно конкретни и ефективни стратегия и политика за киберсигурност;
- разработване и въвеждане на технология за своевременна проверка и актуализиране на документите за киберсигурност.

Проведени изследвания върху различни програми за киберсигурност дават основание да се твърди, че е възможно да се разработи универсална технология за разработване на програма за киберсигурност, която е приложима за различни бизнеси. В структурно отношение една такава технология включва три „опорни“ колони, всяка от които има свое отделно съдържание. Първата „опорна“ колона на технологията е стратегията за киберсигурност. Тя превръща и свежда решенията на мениджмънта до конкретни практически действия на

изпълнителите. В общия случай, в стратегията се посочва защо е важна киберсигурността за компанията, определят се насоките за разработване на програма за киберсигурност и т.н. Втората „опорна“ колона покрива оперативното ниво на мениджмънта. Чрез нейното съдържание се определя как програмата за киберсигурност отговаря на специфичните изисквания на стратегията, какви поддържащи функции са необходими и какво ниво на мониторинг и докладване се изисква. Третата „опорна“ колона представя тактическото или още технологическото ниво, което се занимава с въпросите какви контроли за киберсигурност да се прилагат по отношение на системите, мрежите и приложенията, как ще се доказва степента на тяхната ефективност и т.н.

Съдържанието на трите „опорни“ колони на технологията за разработване на програма за киберсигурност може да бъде разделено на седем области: изпълнителен мениджмънт, управление на риска, разузнаване в полза на киберсигурността, обучение и информираност на потребителите, сигурност на мрежите, сигурност на системите, сигурност на приложенията.

Програмата за киберсигурност може да бъде разглеждана като технология за регламентиране на съвкупност от взаимно свързани процеси и контроли. Тя следва да бъде достатъчно гъвкава, динамична и с възможност да се адаптира към непрекъснато променящите се условия на средата. Разработването ѝ изисква стратегически подход и се базира на политиката за киберсигурност на организацията. От своя страна, политиката за киберсигурност се основава на правила, стандарти, регулации и добри практики. От нея се очаква да обедини очакванията, дейностите, ролите, отговорностите и особеностите на организационната култура за киберсигурност в организацията. Като цели на политиката за киберсигурност, които имат отношение към програмата за киберсигурност, могат да бъдат посочени:

- защита на организацията, персонала, клиентите, доставчиците и партньорите от въздействия в резултат на умишлени и неумишлени увреждания, кражби, неправилно използване и унищожаване на информация;
- защита на интегритета на данните и информацията в рамките на техния жизнен цикъл;
- осигуряване на достъпност до данните, информацията и услугите при поискване от оторизирани потребители, с необходимото качество и в рамките на необходимото непрекъснато време за работа.

Характеристиките на успешната програма за киберсигурност показват какво и защо трябва да бъде направено, но не и как да бъде направено. За да бъде успешна програмата за киберсигурност трябва да бъде реалистична, да поставя изпълними цели и изисквания, да може да търпи необходимите промени, да включва изискванията на всички заинтересовани лица и да притежава съответния статут.

Ключовите аспекти на една успешна програма за киберсигурност, според Cisco, включват[1]:

- спечелване на подкрепата и ангажимента на стратегическия мениджмънт на компанията;
- разработване на стратегия за киберсигурност;
- създаване на работен план за разработване и въвеждане на програма за киберсигурност;
- установяване на реда за ревизиране и обновяване на програмата за киберсигурност и на свързаните с нея документи;

[1] Cisco, “Cybersecurity Management Program whitepaper,“ 2017, https://www.tylercybersecurity.com/information-security-program-template.

- разработване на стратегическите елементи на програмата за киберсигурност. Тези елементи могат да се разработват както последователно, така и паралелно при положение, че между тях няма силни зависимости. Като примери за стратегически компоненти на една програма за киберсигурност могат да бъдат посочени активите, заплахите, уязвимостите, рисковете и т.н.
- определяне на източниците на информация и на метрики за измерване на всеки от елементите на програмата за киберсигурност;
- определяне на ключовите бизнес процеси на компанията и връзката им с програмата за киберсигурност;
- йерархично структуриране на елементите на програмата за киберсигурност;
- разработване на документация, в която се описва какво, защо, кога, къде, как и кой е отговорен да следи, изпълни или контролира.

Програмата за киберсигурност се нуждае от правилно разбиране и ангажимент както от страна на ръководството на организацията, така и от страна на мениджмънта на организацията. Защо е важна ролята на ръководството на организацията по отношение на програмата за киберсигурност. Като правило, ръководството представлява съвкупност от принципи и ръководни действия, чието приложение води организацията към постигане на нейните цели. Ръководството е различно от реактивния мениджмънт и то е нужно за да бъдат постигани резултати. Принципите и ръководните дейности включват стратегията на организацията, метриките за измерване на успеха, начините за управление на риска, начините за определяне на защитата на активите и т.н.

По отношение на програмата за киберсигурност, разликата между ръководството и мениджмънта е в частта прилагане. Създаването на принципите и ръководните дейности е ангажимент на ръководството. Прилагането на принципите и ръководните дейности е ангажимент на мениджмънта.

По принцип в една организация съществува общо ръководство, но с помощта на филтри може да се достигне до ръководство на отделни сектори или отдели: ИТ отдел, отдел за киберсигурност, маркетингов отдел, отдел персонал и др.

Мениджмънтът се нуждае от информация от страна на ръководството за да прилага избраната стратегия и да постига желаните резултати. Обратната информация от страна на мениджмънта към ръководството е важна за валидиране и развитие на принципите и ръководните дейности.

Слабото или лошото ръководство не е задължително да се свързва със слаб или лош мениджмънт. Възможно е да съществуват лоши принципи, които да се прилагат по подходящ начин. За съжаление в тези случаи резултатите са далече от желаните. Обратното също е вярно, наличието на добро ръководство не гарантира наличието на добър мениджмънт. При добро ръководство и лош мениджмънт може да се очаква, че резултатите отново ще бъдат далече от желаните. Ръководството и мениджмънта са различни неща, но са еднакво важни, защото ако едно от двете не е на ниво, от това страдат резултатите на организацията.

В структурно-функционално отношение ръководството, мениджмънта и изпълнителите могат да бъдат описани по следния начин в тяхната свързаност по отношение на програмата за киберсигурност:

- ръководството разработва и утвърждава програмата за киберсигурност, в която задава целите, нивото на апетита към риска, условията за измерване, за изпращане на обратна информация и т.н.

- мениджмънтът прилага програмата за киберсигурност като разработва политики, стандарти, ръководства, процедури, контроли и осигурява обратна връзка към ръководството;
- изпълнителите изпълняват програмата за киберсигурност като спазват процедурите и прилагат контролите, дефинират поуки от практиката, документират резултатите и осигуряват обратна информация за мениджмънта.

СТРУКТУРА И СЪДЪРЖАНИЕ НА ПРОГРАМА ЗА КИБЕРСИГУРНОСТ

Прегледът и сравнението на структурата и съдържанието на конкретни програми за киберсигурност позволява създаване на представа за принципния модел на една такава програма. Подобен преглед и сравнение на съдържанието на три програми за киберсигурност е направен по-долу. Програмите за киберсигурност са сравнени на базата на критерии относно тяхната структура и съдържание, включената информация, степента на актуалност.

1. Програма за киберсигурност на компанията Tyler Technologies[2]. Тази компания предлага продукти и услуги на правителствени институции, институции от съдебната система, от сферите на здравеопазването и образованието.

- структурата и съдържанието на програмата включва следните области: въведение; управление на програмата за киберсигурност; поддръжка и преглед на програмата за киберсигурност; управление на риска за киберсигурността; класифициране на информацията; управление при инциденти с киберсигурността; контрол на достъпа; сигурност на информационната инфраструктура; оперативна сигурност; сигурност на жизнения цикъл на системите; планиране при извънредни ситуации; сигурност на персонала; управление и одит на трети страни; сигурност на on-line услугите; социални медии; съответствие на регулации и изисквания;
- информация: всеки от изброените по-горе елементи на програмата за киберсигурност съдържа кратко описание на съдържанието, предназначението и целите. След тях се посочват политики и контроли за постигане на тези цели.
- актуалност: политиките в програмата следват актуални стандарти, програми за обучение и сертификати в полето на киберсигурността.

2. Програма за киберсигурност на компанията ACME Business Consulting[3]. Тази компания предлага решения за информационна и мрежова сигурност.

- структурата и съдържанието на програмата включва следните области: обобщен преглед на програмата; структура на програмата; управление на конфиденциалността; мениджмънт на активите; непрекъснатост на бизнеса и възстановяване на работоспособността след инцидент с киберсигурността; планиране на капацитета и ефективността; управление на промените; cloud сигурност; съответствие на регламенти; конфигурации; мониторинг; криптографска сигурност; класифициране на данните и информацията; вградени технологии; сигурност на крайните устройства; сигурност на човешките ресурси; идентификация и автентикация; реакция при инциденти с киберсигурността; информационно осигуряване; мениджмънт на мобилните устройства; мрежова сигурност; физическа сигурност; поверителност; управление на проекти и ресурси; управление на риска; оперативна сигурност; обучения; мениджмънт на заплахите; мениджмънт на уязвимостите; уеб сигурност;

[2] Tyler Technologies, “Information Security/Cybersecurity Program,” 2018, https://www.tylercybersecurity.com/information-security-program-template.

[3] ACME Business Consulting, LLC, “Digital Security Program (DSP)” 2018, https://graphics.complianceforge.com/graphics/digital-security-program/example-digital-security-program.pdf.

- информация: програмата включва разнообразни политики, процедури, технологии и контроли с разяснение за това срещу какви проблеми се прилагат;
- актуалност: програмата поддържа актуален регистър на политики, процедури, документи, обучения, сертификати, както и списък с модерни софтуерни и хардуерни решения.

3. Програма за киберсигурност на Федералната комисия по комуникациите на САЩ[4].

- структурата и съдържанието на програмата включва областите: поверителност и сигурност на данните; противодействие срещу измами; мрежова сигурност; уеб сигурност; електронна поща; мобилни устройства; сигурност на персонала; защита на офиса; оперативна сигурност; реагиране при инциденти с киберсигурността; разработване на политики за киберсигурност; специализиран речник; линкове към публикации;
- информация: програмата съдържа информация за конкретните елементи на корпоративната инфраструктура и за тяхната специфична защита;
- актуалност: линковете водят към сайтове на лидери в областта на киберсигурността.

В съдържанието на една достатъчно изчерпателна програма за киберсигурност следва да бъдат включени раздели, които се отнасят до приложението на принципи, политики, стандарти и процедури за киберсигурност. Оперативната гледна точка на една програма за коиберсигурност се базира на концепциите за управление на риска и за киберустойчивост. Тези концепции позволяват системното разбиране и анализиране на заплахите, уязвимостите и рисковете за информационните активи, както и свързването на етапите за превенция, разкриване, дакладване, противодействие и извличане на поуки от практиката в единен жизнен цикъл на управлението при инциденти с киберсигурността и непрекъснатостта на бизнеса. Базова концепция за една програма за киберсигурност е тази за измерване на резултатите от мерките за постигане на киберсигурност с помощта на адекватна система от метрики.

Принципи за киберсигурност

Едно от познатите определения определя киберсигурността като процес за непрекъснато прилагане на най-добрите практики с цел да се осигури и защити конфиденциалността, интегритета и достъпността до информацията, както и безопасността на потребителите и средата. От даденото определение могат да бъдат изведени две от основните характеристики на киберсигурността, а именно динамична природа и фокусираност върху четири принципа: конфиденциалност, интегритет, достъпност и безопасност. Безопасността се добавя към познаните три принципа за да се отговори на заплахите от ежедневния живот, пред които ни изправя концепцията за интернет на нещата (IoT).

В кратка форма, съдържанието на четирите принципа, върху които се изгражда една програма за киберсигурност може да бъде представено по следния начин[5]:

- *конфиденциалност*, за която е характерно, че като термин в някои случаи се приема като синоним на частен или секретен. Кое е конфиденциално зависи от степента на приемливия риск, а той от своя страна зависи от апетита към риска. Сигурността не е черно-бял свят и в тази връзка следва да се говори за степени на конфиденциалност. Конфиденциалността има жизнен цикъл, в рамките на който се променят степените на конфиденциалност. Тези степени зависят от размерите на

[4] Federal Communications Commision, “Small Biz Cyber Planner 2.0,” 2012, https://www.fcc.gov/cyberplanner.
[5] Chris Maschovitis, *Cybersecurity Program Development for Business* (Wiley, 2018).

последствията за организацията при увреждане на даден актив. Това изисква задаване на степен за конфиденциалност за всеки актив, която да бъде валидна определен период от време, както и указания какво следва след това.

- *интегритет*, който се осигурява за сметка на съвкупност от процедури и контроли, проектирани да защитават, поддържат и осигуряват едновременно точност и изчерпателност на данните в рамките на техния жизнен цикъл.
- *достъпност*, постигана за сметка на съвкупност от процедури и контроли, проектирани и прилагани с цел осигуряване на своевременен достъп до данните.
- *безопасност*, отнасяща се до случаите когато инцидентите с киберсигурността могат да доведат до нараняване или загуба на човешки живот или до проблеми във физическата среда. Тя превръща киберсигурността от технологичен подход в подход, поставящ в центъра човека.

Като обобщение може да се каже, че една достатъчно ефективна програма за киберсигурност следва да бъде изграждана на базата на тези четири принципа.

Политики, стандарти, ръководства и оперативни процедури за киберсигурност

На базата на формулираните по-горе принципи се разработват политиките, стандартите, ръководството и оперативните процедури, който са ключови компоненти на програмата за киберсигурност.

Политиките за киберсигурност представляват най-съществения документ, третиращ киберсигурността. Тея определят обхвата на необходимата сигурност, фиксират активите, които трябва да бъдат защитавани и степента на желаната сигурност. В политиките за киберсигурност се посочват целите и времевата рамка за тяхното постигане. Политиките за киберсигурност посочват функционалните области, в които се защитават данните и информацията.

Една кратка класификация на политиките за сигурност показва наличието на следните такива[6]:

- *организационна (обща) политика за сигурност*, която включва всички аспекти от дейността на организацията;
- *политики за сигурност по специфични проблеми:* фокусират се върху проблемите на сигурността на отделни мрежи, системи, отдели, функции, които са с висока стойност и приоритет за организацията;
- *политики за сигурност на отделни системи:* отнасят се до сигурността на конкретни системи или типове системи и предписват специфични процедури за тяхната защита.

Друга класификация на политиките за киберсигурност ги разделя на:

- *регулаторни:* използват в случаите, където съществуват конкретни регулации по отношение на сигурността, които следва да бъдат спазвани. В тях се описват изискванията на регулациите и процедурите, които осигуряват тяхното изпълнение;
- *подпомагащи:* определят приемливите действия и поведения, посочват последствията при тяхното нарушаване, изразяват вижданията на стратегическия мениджър по въпросите на сигурността. В практиката повечето от политиките за сигурност са от този тип;

[6] Mike Chapple, James Stewart, Darril Gibson, *Certified Information System Security Professional* (2018).

- *информационни:* осигуряват информация и знание за специфични обекти като цели и мисии на организацията, взаимодействие с партньори и клиенти и т.н. Тази тип политики за сигурност осигуряват поддръжка, изследване и основна информация за отделни компоненти на цялостната организационна политика за сигурност.

Стандартите за киберсигурност дефинират изискванията за използване на хардуера, софтуера, технологиите и контролите (мерките) за сигурност. Задават начина за действие при информирано прилагане на технологиите и процедурите. Те представляват документи от тактическото ниво на мениджмънта и посочват стъпките за постигане на целите, включени в политиката за сигурност.

Ръководствата за киберсигурност предлагат препоръки за изпълнение на стандартите и служат като оперативни ръководства както за професионалистите по киберсигурност, така и за потребителите. Характеризират се с гъвкавост, която ги прави приспособими към конкретни системи и среда. Могат да бъдат използвани при създаване на нови оперативни процедури за сигурност.

Стандартните оперативни процедури за киберсигурност представляват детайлни документи, описващи стъпка по стъпка изпълнението на изискващите се действия и контроли на сигурността. Процедурите могат да се отнасят до сигурността на цели системи или до отделни техни компоненти или аспекти на сигурността. Препоръчва се процедурите за сигурност да бъдат периодично обновявани, успоредно с развитието на софтуера и хардуера. Въвеждането на адекватни стандартни оперативни процедури за киберсигурност осигурява съответствие с политиката и стандартите за сигурност.

Понякога фирмите разработват един общ документ, в който включват елементи от политиката за сигурност, стандартите, ръководствата и процедурите за сигурност. Специалистите препоръчват подобен подход да се избягва, тъй като отделните документи изпълняват различни роли и са предназначени за специфични групи потребители. Отделното разработване на изброените по-горе документи по отношение на сигурността предоставя следните предимства:

- не всеки потребител трябва да бъде запознат със съдържанието на всеки от документите;
- при необходимост от промени, по-лесно и практично се оказва да се коригира и разпространи конкретен документ.

В литературата могат да бъдат намерени сравнения в документите за сигурност на базата на тяхната обобщеност. Политиката за киберсигурност е документ с най-висока степен на обобщеност и има отношение към съдържанието на всички останали документи. Стандартите се базират на политиката за сигурност, както и на съществуващи законови и регулаторни изисквания. От политиката за сигурност и стандартите се извеждат ръководствата. Накрая като резултат от трите типа документи, се разписват стандартните оперативни процедури за сигурност. При тези условия изглежда разбираемо защо в една организация има една политика за сигурност и множество стандартни оперативни процедури за киберсигурност.

Активи

На следващо място в програмата за киберсигурност следва да се направи описание и класификация на активите, чиято сигурност се защитава. Под актив се разбира всичко, което има стойност за компанията. Важно правило от гледна точка на сигурността е, че ако едно нещо има стойност за даден човек, то същото нещо ще има стойност и за друг човек. Като следствие от това възниква нуждата от грижа за активите и нужда от защитата им.

Активите на компанията могат да се разглеждат като цяло или в определен контекст. Такъв възможен контекст е киберсигурността. В тази група се включват онези активи, за които съществува риск от кибератака.

Ако съществуват съмнения за това дали даден актив има стойност от гледна точка на киберсигурността, то тези съмнения могат да бъдат разсеяни с помощта на отговори на следните въпроси[7]:

- какво ще се случи ако въпросният актив бъде разрушен, повреден, недостъпен;
- какво ще се случи ако активът стане публично достъпен или попадне в ръцете на зложелател.

Ако отговорът на горните въпроси е „нищо“, то тогава въпросният обект не може да се разглежда като актив от гледна точка или в контекста на киберсигурността.

Активите в контекста на киберсигурността могат да бъдат класифицирани в различни групи:

- данни: фиксирани стойности на параметри на системи, процеси, явления и т.н.
- хардуер под формата на оборудване, което съхранява, обработва и предава данни;
- софтуер във вид на операционни системи и приложения, използвани от хардуера за извършване на операции;
- системи, представляващи съвкупност от хардуер, софтуер и мрежи, които обработват данни;
- процеси, представляващи последователност от стъпки при създаване, трансформиране, обработване, съхранение и предаване на данни между системи. Процесите създават стойност за компанията и по тази причина се нуждаят от защита на тяхната сигурност.
- метаданни за активите, които показват онова, което трябва да се знае за активите. В един от моделите се изброяват следните метаданни за активите:
  - собственик/притежател: може да бъде компанията като цяло, отделна нейна структура, отделно лице;
  - пазач: може да бъде конкретно лице, структура на компанията, доставчик и т.н.
  - местоположение: в зависимост от мащаба на компанията може да се говори за местоположение в конкретна структура или работно място, както и за географско местоположение;
- ниво на конфиденциалност: определя се в зависимост от въведената в компанията класификация на нивата за конфиденциалност;
- ниво на критичност: определя се спрямо критичните функции и бизнес процеси, както и на базата на въведената в компанията класификация за критичност на активите;
- степен на влияние: определя се на базата на оценка за последствията в случай, че активът не е достъпен, ако е повреден или разрушен;
- максимално допустимо време, в рамките на което активът може да не бъде използван: след това време се приема, че влиянието се засилва във висока степен;

[7] Maschovitis, *Cybersecurity Program Development for Business*.

- точка за възстановяване: момент във времето, в който трябва да бъде възстановена работоспособността на актива;
- ресурси: кой ще възстанови работоспособността на актива (конкретни имена).

Централното място сред активите в полето на киберсигурността се отделя на хората или още на потребителите, които в тази си роля представляват критичния фактор за успеха на всяка програма за киберсигурност. У тях не бива да остава съмнение, че организацията разглежда киберсигурността като ключов фактор за успеха и като такава изисква наличие и спазване на ясни политики, стандарти, процедури и ръководства. Последните следва да са приложими, релевантни, измерими за всяко ниво в организацията, както и редовно да бъдат преглеждани и актуализирани. Персоналът в организацията следва редовно да бъде осведомяван и обучаван по проблемите на киберсигурността.

Друг вид активи, свързани с киберсигурността, са данните. Гарантирането на сигурността на данните изисква намиране на отговори на следните въпроси:

- какви видове данни се използват в компанията. В повечето случаи компаниите използват различни видове данни, едни от които са по-чувствителни и по-ценни от другите. Независимо от това, при всички случаи данните, с които разполага и борави една компания представляват интерес и за други компании, за други потребители. Този факт поставя изискването за осигуряване на сигурност на данните на компанията;
- как се използват и как се защитават данните на компанията. Данните са изложени на най-висок риск когато се предават и предоставят на различни потребители. Ако данните се съхраняват на един компютър, който не е включен в интернет и не се предават по мрежа, то те биха били лесно защитими. За да бъдат обаче полезни данните, те трябва да бъдат достъпни и да се използват от потребители, да бъдат анализирани, да бъдат споделяни с партньори. При тези условия данните са изложени на различни заплахи. За всеки тип данни в компанията трябва да има правила за работа и защита в зависимост от условията, при които те се използват.
- кой има достъп до данните и при какви условия. Като правило се приема, че никой служител в компанията не се нуждае от достъп до всички данни за да изпълнява професионалните си задължения. Това прави от значение оценяването на разрешения достъп до информационните активи. На практика това може да се представи като съставяне на списък на служителите в компанията, на партньори и на други групи заинтересовани лица, в който се отбелязва до какъв тип данни и при какви условия ще имат достъп. Важно е също да се уточни как дадените привилегии ще се проследяват и управляват.

Политиката за защита на данните показва какви типове данни се събират, обработват и съхраняват в компанията, с каква цел и как се защитават. Защитата на личните данни все повече се превръща в приоритет за компаниите, което се изисква и налага с помощта на различни регулации. В съдържанието на политиката за защита на личните данни трябва да бъдат включени следните видове данни:

- данни, с помощта на които пряко и непосредствено може да се идентифицира конкретно лице. Такива са данните за имената, домашен и служебен адрес, адреси от електронната поща, номера на банкови сметки и кредитни карти, номера на социални осигуровки и т.н. Тук попадат също така и данни за възрастта на лицето, неговия пол, година и място на раждане, телефонни номера, номер на шофьорска книжка и др.

- данни, свързани със здравословното състояние на лицето. Попадането на подобен тип данни в ръцете на хакери може да създаде проблеми на лицето, за което се отнасят.
- данни за клиенти от рода на номера на техни дебитни и кредитни карти, с които извършват разплащания; имена и телефонни номера; данни за извършени сделки; използвани отстъпки и т.н.

Особен аспект на политиката за защита на сигурността на данните представлява защита на данни, добивани от интернет. Най-често такива данни се добиват от сайта на компанията, който представлява удобен и лесно достъпен източник на данни. Тяхното съдържание варира в широки граници: от данни за извършени сделки и стартирани проекти до данни от on-line анкети и поръчки на клиенти. Тези данни следва да бъдат надеждно защитени независимо от това дали сайта ползва сървър на компанията или е базиран на сървър на външна компания. Във втория случай успоредно с класифицирането на данните и управлението на достъпа до тях трябва да се контролира начина, по който третата страна защитава съхраняваните данни.

Заплахи

Сигурността на активите на компанията в полето на киберсигурността е подложена на въздействието на заплахи. В общия случай тези заплахи могат да бъдат умишлени (планирани) и неумишлени (инцидентни). Реализацията на една или друга заплаха намира израз под формата на кибератака, която от своя страна може да бъде определена като реализирана заплаха и включва организирани и целенасочени усилия на отделен човек или група от хора за експлоатиране на слабо място (уязвимост) в системата или в контролите за сигурност.

Агенти на заплахите за киберсигурността на активите са разнообразни и по тази причина подлежат на класифициране. Като пример, класификацията на ENISA разделя агентите на заплахите за киберсигурността в следните групи:

- киберпрестъпници с мотив най-често финансова изгода;
- инсайдери (вътрешни служители, потребители) с мотив най-често финансова изгода или отмъщение;
- хактивисти с мотив най-често защита на свободата на словото, борба срещу несправедливостта;
- кибербойци, представляващи национално мотивирани „патриоти“;
- кибертерористи, целящи създаване на страх, паника, хаос;
- script kiddies, най-често млади хора, хакващи за развлечение.

Ключовите тенденции, оказващи влияние върху агентите на заплахите срещу киберсигурността показват:

- консуматорска природа на киберпрестъпността, улеснявана от факта, че хакерски инструменти са лесно и свободно достъпни, както и че е възможно лесно наемане на хакери за конкретни цели;
- ниски бариери за навлизане на технически новости, при което всеки мотивиран може лесно да започне кариера на киберпрестъпник още повече, че съществуват университети за хакери;
- ниско ниво на противодействие, което прави почти невъзможно да бъде разкрит киберпрестъпника. Колкото е парадоксално да звучи, да си киберпрестъпник днес е ниско рискова и високо доходна професия.

Източникът на заплахата или още агентът на заплахата стартира събитието, което реализира заплахата под формата на атака. Атаката експлоатира една или повече уязвимости в системите, което води до нежелани или нежелателни последици за активите. Като следствие активът е изправен пред риск за неговата сигурност.

Най-често използваните атрибути на заплахите за киберсигурността са агент на заплахата, вероятност за проява на заплахата, влияние или резултат от реализиране на заплахата.

Разнообразието на заплахите за киберсигурността изисква тяхното класифициране. На първо ниво на класификация заплахите за киберсигурността се разделят на вътрешни и външни. Въпреки разделянето и при двете групи заплахи съществуват сходни мотиви: идеологически, лични, финансови и т.н.

Онова, което прави вътрешните заплахи опасни е, че агентът на заплахата има разрешен достъп до определени информационни активи. В допълнение към това може да се каже, че същият този агент познава стойността на тези активи[8].

По отношение на вътрешните заплахи се приема, че няма един общ или единен профил на агентите на тези заплахи. Агентът може да бъде нает в компанията на постоянен или на временен трудов договор, а може да бъде също така доставчик или отговарящ за поддръжката, който се нуждае от достъп до информационните активи. В общия случай се приема, че агентът на заплахата разполага със средства, мотив и възможност. Всеки, който разполага с достъп до информационните активи независимо от това дали е на място или отдалечен достъп, може да се превърне в агент на вътрешна заплаха.

Средства, използвани от агентите на вътрешните заплахи могат да бъдат изключително разнообразни – от получаване на информация от физически носители (като пример, копиране на хартиени документи) до копиране на информация в електронен вид (като пример, записване на информация на USB).

Мотивите на агентите на вътрешните заплахи за киберсигурността също са разнообразни, но в повечето случаи са сходни с мотивите при агентите на външните заплахи. Възможните варианти включват финансова изгода (в този случай необходимостта от финансови средства може да бъде предизвикана от натрупани дългове, зависимост от наркотици и т.н.), идеологически мотиви (несъгласие с политиката на компанията или с даден закон на държавно ниво), лични мотиви (недоволни служители) и т.н.

Възможностите пред агентите на вътрешните заплахи за киберсигурността се разкриват за сметка на съществуването на слаби процедури и контроли. Подобни възможности могат да възникнат за сметка на недостатъчното обучение на персонала, ниско ниво на контрола на физическия достъп, неефективен технически контрол на достъпа, отсъствие на разделяне на задълженията, липса на класифициране на информацията и т.н.

Според направено изследване съотношението между вътрешните и външните заплахи за киберсигурността е 40% към 60%.

Мотивите при агентите на външните заплахи за киберсигурността могат да бъдат различни:

- активизъм/тероризъм: тук е добре да се разбира, че за даден човек едно действие може да бъде форма на активизъм, а за друг човек същото действие да бъде тероризъм;

[8] Eric Cole, *Insider Threats and the Need for Fast and Directed Response—A SANS Survey* (Bethesda, MD: SANS Institute, 2016).

- шпионаж: в днешно време огромна част от актовете на шпионаж, независимо от това дали са финансиране от страна на държавите или на определена компания, се извършват в интернет. Мотивите в различните случаи на шпионаж са сходни, но използваните методи са различни. Атаките изискват множество комплексни умения, а последствията са катастрофални за жертвата. В най-честите случаи атаките са насочени към кражба на интелектуална собственост, към сигурността на обекти от критичната инфраструктура, комуникациите, енергетиката, държавното управление и т.н.
- финансова изгода: представлява най-често срещания мотив за атаките на киберсигурността на активите. Този факт се аргументира с разнообразието на методите, които могат да бъдат използвани, както и с това, че съществуващите бариери стават все по-ниски, т.е. лесно преодолими;
- патриотизъм: мотивираните от този фактор агенти на външните заплахи аргументират своите действия с патриотичен дълг, разбиран по специфичен, техен начин. В повечето случаи техните действия са финансирани от страна на държавата;
- отмъщение: този вид атаки засяга най-често лични отношения. При тях не е задължително да се стига до разрушаване на актив. Може да бъде под формата на кражба на информация, продаване на същата на заинтересовани лица или публикуването ѝ в публичното пространство.

Необходимостта от ресурси за противодействие срещу заплахите за киберсигурността налага въвеждане на процес за оценяване на тяхната значимост. Ранжирането на заплахите се изразява в определяне при всеки конкретен случай на най-вероятните агенти на заплаха и техните мотиви. За целите на това ранжиране може да бъде използвана скала с четири степени: малко вероятни; вероятни; много вероятни; изключително вероятни. Като пример, атаките от страна на вътрешните агенти са много вероятни като най-често срещаните мотиви са финансови облаги или отмъщение.

Даването на отговори на въпросите „кой“ и „защо“ не е достатъчно за познаване на заплахите и свързаните с тях атаки срещу киберсигурността. Необходимо е също така да бъдат дадени отговори и на въпросите „как“ и „кога“.

Начините за реализиране на заплахите за киберсигурността са изключително разнообразни, което усложнява намирането на отговор на въпроса „как“. Като практически пример може да се разгледа едно изследване на ENISA от 2015 г., което сравнява различни начини за извършване на атаки срещу сигурността на информационните активи. Обобщените резултати от изследването дават основание да бъдат направени следните изводи:

- някои от методите и средствата за атака запазват местата си при сравнението за изследвания период. Такива са зловредния код, www-базираните атаки, бетнет, отказ на услуги;
- други методи и средства повишават степента или честотата на използване. Такива са физическите увреждания; кражбите и загубите; вътрешни агенти на заплаха;
- при трети средства и методи се отчита намаляване на честотата за използване. Примери в този случай са спам и фишинг атаките.

За да се даде верен отговор на въпроса „кога“ може да се очаква извършването на кибератака е необходима своевременна информация, която се добива с инструментите на разузнаването на заплахите в реално време. Въпросите, които следва да бъдат задавани са от типа: какъв зловреден код наскоро е разпространен, какви нови уязвимости са разкрити наскоро и какво е направено във връзка с тях или в отговор на тях, какъв тип са най-често констатираните атаки и т.н. Разузнаването в посока на заплахите за киберсигурността събира

информация и вътре в компанията по отношение на състоянието на активите, кой потребител какъв достъп има и кога, нетрадиционни поведения или трафик и т.н. Освен, че е огромна по обем, информацията от разузнаването на заплахите изисква специфични знания и умения при нейния анализ.

Много често въпросът със заплахите за киберсигурността се свързва с действията и мотивите на т.нар. хакери. В тази връзка възникват няколко въпроса от рода на: агенти на заплахите ли са хакерите или престъпници ли са хакерите. В по-далечни времена с термина хакер се е изразявало респект и уважение. Създателите на интернет са наричали себе си хакери и под това са разбирали хора с умения да изграждат, използват и разширяват способностите на всякакъв вид системи.

От негативна гледна точка хакерите се свързват с кражби, вандализъм, престъпни действия. В днешно време определението хакер далеч не е комплимент. В същото време не всички хакери са еднакви и разликите между тях могат да бъдат толкова съществени, колкото са разликите между деня и нощта, черното и бялото, доброто и лошото.

От историческа гледна точка може да се приеме, че всички хакери са имали нещо общо и то е нивото на техните технически знания и умения. Хакерите изследват детайлно системите и намират начини за компрометиране на тяхната сигурност. За добрия хакер се изискват едновременно вроден талант и безкрайно обучение и практика.

Уязвимости

Уязвимостите на системите се дефинират като слаби места в информационните системи, процедурите за сигурност, вътрешните контроли и начините за тяхното приложение, които могат да бъдат експлоатирани или определени като цели на заплахите. Всяка система има слаби места, определяни като уязвимости от гледна точка на киберсигурността. Освен съществуващите или още известните, които далече не са една или две, ежедневно се появяват нови уязвимости. Не всички обаче са релевантни към конкретна среда и усилията следва да се насочат към идентифициране на релевантните за дадената компания уязвимости.

При идентифициране на уязвимостите могат да бъдат използвани готови бази от данни, като пример NIST National Vulnerability Database (NVD), която включва близо 80 000 общи уязвимости на киберсигурността, както и ръководства за тяхното смекчаване или преодоляване.

Контроли за киберсигурност и защита в дълбочина

Едновременното наличие на заплахи, уязвимости и агенти на заплахите поставят под риск сигурността на информационните активи. Снижаването на този риск до нивата на апетита към риска става с помощта на разработваните и прилагани контроли за киберсигурност.

Контролите за киберсигурност представляват действия, които водят до снижаване на риска или с други думи играят превантивна роля, откриват, коригират и противодействат срещу риска за киберсигурността. Според съществуващи класификации тези контроли могат да бъдат разделени в следните групи[9]:

- превантивни контроли, които играят превантивна роля срещу атаките за да не успеят те да достигнат до информационните активи. Някои автори наричат

[9] Federal Communications Commission, *Cyber Security Planning Guide* (San Jose, CA: NBU Company, 2021).

превантивните контроли пътни бариери по магистралите на информацията. Проектирани са с цел да спират атакуващите в тяхното желание да осъществят неправомерен достъп до активите. Ако за сигурността на активите са предвидени физически контроли, то пример за превантивна контрола е физическата охрана. Техен дигитален еквивалент могат да бъдат:

- антивирусни програми: функцията им е да сканират трафика, да го сравняват с въведените в базата от данни заплахи и да взимат съответни решения. Ефективността им зависи от капацитета на базата от данни и своевременното й обновяване.
- обучение и осведоменост на потребителите за проблеми с киберсигурността: представлява най-ефективната превантивна контрола. Успехът на обучението зависи от конкретиката и спецификата на програмата, от методите за обучение, както и от времето и периодичността на провежданите обучения.
- превенция от загуба на данни (DLP): тези средства следят специфични видове данни (като пример, номера на кредитни и дебитни карти, номера на социални осигуровки, номера на банкови сметки и т.н.) и ограничават достъпа до тях само за оторизирани потребители. Могат също така да инспектират трафика с цел да откриват предаване на чувствителна информация по нерегламентиран начин. Ефективността на системите зависи от тяхната конфигурация и от степента за познаване на средата на данните и политиките за сигурност. Предимство е, че могат да подават сигнали за евентуални вътрешни заплахи.
- защитни стени, които се грижат за защитата на вътрешните мрежи на компанията от заплахи, идващи от интернет. Могат да се различават по конфигуриране, способности, степен на сложност. Могат също така да криптират данни и да следят трафика като го сравняват с данни за заплахи. В най-висока степен ефективността на защитните стени зависи от конфигурирането им.

- детективски контроли, използвани за откриване на атаката в случай на проява. Дават възможност да се определи вида на атаката, от къде идва, какви средства се използват и т.н. Също могат да бъдат физически, под формата на датчици за движение и дигитални, под формата на антивирусни системи, системи за откриване на проникванията. Ако превантивните контроли се сравняват с бариери по пътищата, детективските контроли са датчиците за движение, които позволяват да се откриват случаи когато има някой на пътя, преминал без разрешение зад бариерите. Целта им е да откриват състояния, които не са типични или характерни за средата и да подават сигнал. Някои от превантивните контроли могат да работят и като детективски (антивирусни програми, системи за разкриване на проникванията в системите и т.н.). Като други примери за детективски контроли могат да бъдат посочени системи за защита от проникване в системите, системи за мениджмънт на събития с информационната сигурност и т.н.

- коректив контроли, чиято цел е да минимизират негативните последици от атаката. Корективните контроли са концентрирани върху възстановяване на увреждания, получени по време и след кибератаката. Като пример, пачване на съществуващи уязвимости, обновяване на операционните системи и приложенията и т.н. Като коректив средство се използва и резервното копиране, което служи за възстановяване на данни, компрометирани по време на атаката. Съществуват различни видове резервно копиране:
  - пълно копиране на данните, при което не се прави разлика между данните с които работи компанията и всички данни се копират по установените правила;

- диференцирано копиране, при което се обновяват само данните, които са претърпели промени след последното обновяване;
- частично копиране, при което се обновява само променената информация от определен вид.

Кой от трите вида резервно копиране ще избере компанията зависи от вида и мащаба на бизнеса, вида и обема на данните, стойност на данните, стойност на операциите за резервно копиране. При по-малки организации е възможно да се извършва пълно ежедневно копиране на данните. Големите организации по-скоро избират периодичното (седмичното) пълно резервно копиране плюс подходяща комбинация от диференцирано и частично копиране. При пълното копиране времето за възстановяване на данните е сравнително малко, но самият процес за копиране е продължителен и тежък.

- компенсиращи контроли, които компенсират липсата или провала на други контроли и снижават степента на увреждане на активите. Като примери могат да бъдат посочени изолиране на критичните системи от интернет, планове за възстановяване, резервно копиране и т.н.

Най-добрият начин за прилагане на горните типове контроли за киберсигурност е тяхното разполагане около информационния актив по начин, по който се постига т.нар. защита в дълбочина[10]. Това играе ролята на поставяне на поредица от бариери между информационния актив и атакуващия.

Концепцията за защитата на информационните активи в дълбочина има своите противници като техните аргументи се свеждат до това, че границите на защитаваните активи непрекъснато се променят и не могат точно да бъдат фиксирани, както и че способностите на атакуващите, заедно с векторите на атака непрекъснато са развиват и усъвършенстват. В информационната ера традиционното разбиране на идеята за концентричната защита в дълбочина от типа „замък“ не е напълно адекватно. Не е възможно да бъдат построени толкова високи стени, с които да се покрият всички потребители и използваните от тяхна страна разнообразни технологии. Идеята за защита на информационните активи в дълбочина не трябва да се разглежда и разбира само от най-високо ниво, което означава изграждане на замък с пет защитни стени, а между тях водни площи, в които живеят кръвожадни крокодили. Защитата в дълбочина трябва да се прилага спрямо всеки отделен актив и да се отнася към потребителите, технологиите и процесите, т.е. към върховете на т.нар. „златен триъгълник“.

При защитата на активите не бива да се разчита на едно единствено средство. Като пример, ако данните са защитени с парола, то при нейното компрометиране те на практика остават без защита. При тези условия се препоръчва защитата на данните да се изгражда в няколко слоя (защита в дълбочина) с помощта на различни контроли.

Създаването на многослойна защита на активите минава през следните стъпки:

- анализ на използваните видове активи с цел изграждане на общата картина. Важно е анализът да бъде достатъчно изчерпателна за да не бъде пропуснат някой вид чувствителни активи;
- идентифициране и защита на чувствителните активи с висока стойност, висок приоритет. Класифицирането на активите е една от най-важните стъпки в процеса за постигане на сигурност. Защитата на всички активи в еднаква степен изисква разход на ресурси, който не винаги е оправдан. Снижаването на защитата на активите води до риск за тяхната сигурност. Като пример, чувствителните данни следва да се защитава с по-сериозни мерки докато публичните данни се нуждае от по-

[10] Chapple, Stewart, Gibson, *Certified Information System Secur ity Professional*.

либерални мерки за сигурност. В общия случай категориите за класифициране на данните включват:

- данни с висока конфиденциалност, които включват най-чувствителните бизнес данни, които са предназначени за използване само в рамките на компанията. Неоторизираният достъп до този тип данни би довел до сериозни щети за компанията, за партньорите, клиентите, доставчиците и т.н. В групата на тези данни попадат номера на кредитни карти, на банкови сметки, имена и адреси на партньори и клиенти и т.н.
- чувствителни данни, които също са предвидени за използване само вътре в компанията и освен това са лични данни. Като пример, доклади от вътрешни одити, финансови доклади, оценки за персонала, проектна информация за продукти и услуги, договори и т.н.
- данни само за вътрешно използване, които са достъпни за по-широк кръг служители, но не могат да се споделят извън компанията.

- контрол на достъпа до активите. Подобен контрол е необходим за всички категории активи, включени в класификацията. Правилото в случая гласи, че колкото по-чувствителни са активите, толкова по-ограничен трябва да бъде достъпа до тях. В основата на контрола на достъпа до активите трябва да бъде правилото „необходимо да се знае“, т.е. само потребители, които имат изрична нужда от даден вид активи получават достъп до тях при спазване на правилото за минимизиране на привилегиите. Управлението на достъпа до активите изисква определяне на това кои от служителите до какви активи ще имат достъп; при какви условия; какво могат и какво не могат да правят с тези активи; какви правила за защита на активите следва да спазват. За всеки тип активи трябва да се разработят указания за начина на тяхната употреба и защита, за нивото на тяхната защита и за потребителите, които имат разширен достъп до активите.
- постигане на сигурност за активите. След административните въпроси по защитата на активите следва да се обърне внимание на технологичната/техническата страна на защитата. В тази посока най-често използваните средства са потребителските имена и паролите, криптиране на данните и т.н. Към използваните пароли следва да се поставят изисквания за сложност, дължина, период за валидност и смяна, запазване в тайна. Възможно е да се прилага двуфакторна или многофакторна автентикация, при което паролите се комбинират с други фактори за автентикация (като пример, биометрични данни). Едни от най-популярните модели за двуфакторна автентикация включва нещо, което потребителя знае (парола), нещо което потребителят притежава (четец за смарт карти) и нещо, което потребителят предоставя (биометрични данни). Криптирането също е популярен начин за защита на данни. То има своята история във времето, в което алгоритмите за криптиране непрекъснато са усъвършенствани. Днес методите и средствата за криптиране са лесни за използване, с висока ефективност и достъпни като цена.

Измерване на киберсигурността

Един от въпросите, които възниква при разработването на програма за киберсигурност е свързан с това как да се измерва онова, което се прави с идеята за постигане на сигурност? Отговорът е – с липсата на въздействие и последици за организацията. Като примери: алармените системи в домовете предпазват от въздействие от страна на крадците и последствията от евентуална кражба; бронираните автомобили предпазват от въздействие на престъпници и последствията от евентуален инцидент. Успехът на дейностите в полето на

киберсигурността се измерва с липсата на въздействие и последици за конфиденциалността, интегритета и достъпността до информационните активи. Въпросът с безопасността стои по различен начин. Липсата на въздействие и последици обаче не означава, че усилията в полето на киберсигурността не могат да бъдат измерени.

Какво означава да осигуряваш и защитаваш конфиденциалността, интегритета и достъпността до информационните активи, както и безопасността на потребителите и средата. NIST дава отговор на този въпрос като го разглежда като процес с пет фази:

- *идентифициране*, което означава да се познават активите, да се разбират заплахите, уязвимостите и рисковете, да се познават собствените способности за защита на активите;
- *защита*, включваща съвкупност от планове и действия, които водят до прилагане на адекватни контроли за защита на активите;
- *разкриване*, изискващо наличност на планове и действия, позволяващи разкриване, класифициране и докладване на възникнали инциденти;
- *отговор* под формата на конкретни действия в отговор на атаката;
- *възстановяване*, изискващо разработване и прилагане на планове и протоколи, които възстановяват нормалната среда след края на инцидента/атаката.

Горните етапи или функции могат да варират при различните бизнеси и различните потребители. Програмата за киберсигурност трябва да разполага със свобода при нейното създаване в това отношение.

От дадения по-горе пример се вижда, че липсващият етап или функция е превенцията. Тук възниква въпросът винаги ли може да бъде използвана силата на превенцията и възпирането. Отговорът е, че съществуват възможности за превенция и възпиране на киберпрестъпниците. С помощта на достатъчно адекватни юридически и технически мерки е възможно киберпрестъпниците да бъдат възпирани да извършват престъпления. Най-ефективната мярка е обучението на потребителите. В организациите, в които се води подходящо обучение на персонала по проблемите на киберсигурността инцидентите са с 40% по-малко. Възпирането е критична функция за всяка програма за киберсигурност. То напомня, че киберсигурността е фокусирана върху потребителите, а не толкова върху технологиите. Потребителите от своя страна могат да направят една програма за киберсигурност успешна, но могат също така да я провалят. Възпирането зависи от намаляване на повърхността за атака. Внимание следва да се обръща на организацията като цяло: какви са бизнес процесите; какви са заплахите за тяхната сигурност; как тези заплахи се променят. Организационната култура за киберсигурност също допринася за възпиране на киберпрестъпниците.

Съответствие на закони и регулации

Всяка програма за киберсигурност следва да осигури изпълнението на изисквания, произтичащи от закони и регулации във връзка с киберсигурността на активите, като в някои случаи това изискване може да бъде достатъчно съществено. Всеки бизнес е длъжен да се съобразява със законодателството, което от своя страна може да се разглежда в различни мащаби: местно или локално, национално, международно. Характерна особеност за законите и регулациите на национално ниво, които касаят киберсигурността е, че понякога те са доста различни, а понякога и несъвместими за различните държави.

Планиране за отговор при инцидент с киберсигурността

За някои може да изглежда учудващо, че след отделеното време и вложените усилия за категоризиране, оценяване, класифициране, тестване, планиране, въвеждане и обучение, при разработването на програма за киберсигурност трябва да се пристъпи към планиране за отговор при инцидент с киберсигурността. Този план става полезен когато всичко направено с помощта на изброените усилия се провали. На пръв поглед подобен сценарий изглежда невъзможен, но практиката показва, че инциденти с киберсигурността се случват и те са факт. Това изисква от организацията да бъде подготвена за подобни случаи. Не бива да се забравя, че в определени случаи разработването на план за отговор при инцидент с киберсигурността се изисква по силата на закон или друга регулация.

Планирането за отговор при инцидент с киберсигурността е като предпазните колани в автомобила: и двете не водят до превенция от катастрофа/инцидент, но помагат за намаляване на нежелателните последствия. Добрата новина в случая е, че съществуват множество указания как се разработва подобен план. Лошата новина е свързана с това, че разработването на достатъчно ефективен план за отговор при инцидент с киберсигурността представлява сложен и комплексен процес. Сложността и мащаба на плана зависят от вида и мащаба на бизнеса, отделените финансови средства и т.н. При малките фирми планът за отговор при инцидент с киберсигурността може да включва само идентифициране на инцидента и докладване на външни експерти.

В общия случай разработването на план за отговор при инцидент с киберсигурността представлява процес, преминаващ през различни фази и в същото време представлява непрекъснато развиваща се програма. Посочените фазите включват[11]:

- подготовка за противодействие срещу инцидента;
- идентифициране появата на инцидента;
- ограничаване на инцидента;
- третиране на инцидента (унищожаване на вируси, лишаване от неоторизиран достъп и т.н.);
- възстановяване на последствията от инцидента;
- анализ на инцидента;
- формулиране на поуки от практиката.

Добрата програма за киберсигурностт в частта й за отговор при инцидент с киберсигурността изисква наличието на:

- план за непрекъснатост на бизнеса;

- план за възстановяване при бедствия;

- план за отговор/реакция при инцидент с киберсигурността.

Планът за непрекъснатост на бизнеса осигурява постигане на непрекъснатост на бизнес операциите и създаване на стойност в условия на инцидент/смутена среда. Средата може да бъде смутена в следствие на природни бедствия, умишлени или неумишлени действия на потребителите, кибератаки, терористични атаки и др.

В плана за непрекъснатост на бизнеса се съдържа информация, която е полезна за плана за отговор при инцидент с киберсигурността. Като пример, политики и структура на непрекъснатостта на бизнеса; кой и кога задейства плана за непрекъснатост на бизнеса; информация за контакти със служителите и с външни лица; стратегии за промяна в работните места; процедури за възстановяване и др.

[11] Tim Bandos, *Incident Responder's Field Guide* (Waltham, MA: Digital Guardian, 2016).

Планът за възстановяване при бедствия поставя във фокуса технологиите и съответната инфраструктура. В плана се използват понятия като време за възстановяване, начална точка за възстановяване, максимално време за възстановяване и т.н. Тези понятия имат директно отношение към плана за отговор при инцидент с киберсигурността.

Разработването на план за отговор при инцидент с киберсигурността на практика означава намиране на отговор на редица въпроси, от рода на: кой какво прави, как и кога; как и каква информация осигурява, на кого я предава, кога и по какви канали.

Идентифицирането на инцидент с киберсигурността изисква средата като цяло и в частност отделните системи и мрежи да се следят в режим 24x7x365. Следенето следва да включва всяко устройство и всяко събитие. Предвид големия брой обекти, които трябва да се следят става ясно, че това е непосилно за персонала без използване на средства и системи за автоматизиране.

В същото време много от действията, свързани с бизнеса могат да бъдат отчетени като инциденти, а една част от тях остават неразкрити за дни, седмици и дори месеци. Всяко събитие, което показва отклонение от нормалната работа следва да бъде подложено на анализ и оценка, на базата на които да се реши дали става дума за нещо рутинно или напротив – става дума за инцидент с киберсигурността.

Ограничаването на възникнал инцидент с киберсигурността представлява процес, който преминава през следните стъпки:

- запазване на устойчив режим без изпадане в паника;
- определяне на вида на инцидента и какво казват детективските контроли;
- анализиране на инцидента, което изисква специфични знания и умения, както и специализирани средства/инструменти;
- предприемане на действия, като в този случай са възможни различни варианти:
  - събиране на доказателства в интерес на бъдещи действия по разследване на инцидента;
  - връщане колкото е възможно най-бързо към нормалната оперативна среда.

Тези варианти следва предварително да са обмислени и утвърдени в програмата за киберсигурност.

За да бъде ограничен инцидента с киберсигурността по достатъчно подходящ начин следва да бъдат дадени отговори на три въпроса:

- кой: кой стои зад атаката; събитието отговаря ли на определението за инцидент; вътрешен или външен е агента на заплахата; какви могат да бъдат мотивите. Отговорите на тези въпроси подпомагат избора на средства за ограничаване и третиране на инцидента;
- как: какъв е векторът на атаката; вирус или зловреден код; червей или троянски кон; как е реализирана атаката (кликване върху линк, отваряне на писмо от електронната поща, използване на заразено USB и т.н.).
- какво е увредено: отделен краен потребител; множество потребители; сървъри; приложения; мрежи и др. Проследяват се следи, оставени от атакуващия. Уточнява се времевия график на атаката: кога започва, за колко време протича и т.н.

В тази фаза е еднакво важно да се знае „какво да се прави“, както и „какво да не се прави“. Това се осигурява чрез предварителното разработване и изучаване на плана за отговор при инцидент с киберсигурността. Познаването на това какво и как да се прави при

появата на инцидент с киберсигурността представлява половината от работата при решаване на проблема.

Следващите етапи от процеса за планиране за отговор при инцидент с киберсигурността са третиране на инцидента, възстановяване на работоспособността на системите, анализ на причините за инцидента и формулиране на поуки от практиката.

Като частен случай на планирането за отговор при инциденти с киберсигурността и планирането на действията при кражба на данни и информация. Подобни инциденти повлияват не само върху престижа/реномето на компанията, но могат да доведат и до наказания и глоби на базата на съществуващи регулации. Това налага познаването на регулациите по отношение на защитата на данните и на санкциите при тяхната загуба или кражба и взимане на съответните мерки за сигурност. Необходим е план за действие при кражба/загуба на данни, който създава увереност за своевременна и адекватна реакция при подобни инциденти. Информацията за кражба или загуба на данни могат да подават както служителите на компанията, така и технически системи. Необходимо е уточняване на реда за подаване на подобна информация: на кого, в какви случаи и т.н.

Действията, свързани със защитата на данните могат да бъдат обобщени в няколко групи:

- обучение на персонала да разпознават атаки от типа социално инженерство. Социалното инженерство се използва от киберпрестъпниците в on-line и off-line режим за да убедят жертвите да предоставят чувствителна информация или да имат поведение и да предприемат действия, които позволяват постигане на целта на атакуващия. Векторите за атаки от този тип могат да бъдат различни: по телефона, по електронната поща, on-line режим, чрез физически контакт.
- защита срещу on-line измами като индикатори за подобен тип атаки се явява искания за предоставяне на лични данни, отправяне в on-line режим чрез електронната поща или социалните мрежи.
- защита от фишинг атаки. Този тип атаки се използват от киберпрестъпниците за да убедят жертвата, че използва сигурен сайт или друг ресурс, през който да предостави чувствителна информация. Фишинг атаките използват предимства, създадени от текущи събития като природни бедствия, епидемии, икономически кризи, политически събития, пандемии и т.н.
- сигурни вътрешни мрежи и облачни услуги: вътрешните мрежи се препоръчва да бъдат отделени от интернет с достатъчно сериозни механизми за автентикация и други технически средства. Допълнителни решения за проследяване и защита като антивирусни програми, системи за разкриване на проникванията могат да бъдат използвани за разкриване и спиране на зловреден код и неоторизиран достъп. След определяне на крайните/граничните точки на вътрешните мрежи, същите следва да бъдат анализирани за да се изберат адекватни контроли за сигурност.
- политика за сигурност на служебните пароли: статичните пароли все по-трудно отговарят на изискванията за сигурност и се заместват от двуфакторна и многофакторна автентикация. Политиката за сигурност трябва да изисква от персонала да използва максимално сигурни пароли, без да се налага да записват тези пароли на външни носители и без да ги затрудняват да ги запомнят. Препоръчва се паролите да бъдат достатъчно дълги (8-10 знака), да са комплексни (малки и големи букви, цифри, знаци), да се сменят периодично без да се повтарят, да не се споделят с други лица.
- сигурност на електронната поща: електронната поща се превърна в съществена и неотменна част както на днешния бизнес в различни аспекти (мениджмънт на

персонала, контакти с клиенти и т.н.), така и на личните комуникации. Ползите, които предоставя електронната поща чувствително превишават негативните страни. При всички случаи обаче се налага създаване, въвеждане и спазване на правила за сигурност, като пример за които могат да бъдат посочени следните:

- създаване на филтър за спам съобщения по електронната поща. В настоящия момент спам съобщенията представляват 70-80% от общия трафик. Имейлите са основен вектор за разпространение на вируси и зловреден код. Защитата на служебната електронна поща се свързва с използване на имейл филтри, които освен всичко друго могат да подпомогнат антивирусните програми.
- обучение на служителите за използване на електронната поща по сигурен начин. Последната линия на защитата на данните са служителите, които използват тези данни, както и средствата да работа с тях. Сами по себе си технологиите за сигурност не са панацея и не могат да създадат желаната сигурност на данните. Необходими са вниманието и усилията на персонала, който в този случай следва да бъде обучен да идентифицира рисковете, свързани с имейлите, как и кога да ги използват в тяхната работа и кога да търсят помощ от специалистите. Еднакво важни се явяват както първоначалните, така и опреснителните/периодичните обучения. Формите за обучение могат да бъдат различни: ежемесечни бюлетини, постери в общодостъпни места и т.н.
- ограничаване изпращането на чувствителна информация по електронната поща. Електронната поща често пъти се използва за споделяне на чувствителна информация. В тези случаи трябва да се постигне увереност, че данните ще са достъпни само за адресата. Случаи на неправилно адресиране могат да доведат до разкриване на информация. Решенията са или да се криптира предаваната информация или чувствителна информация изобщо да не се споделя по електронната поща.
- политика за използване на имейли. Този тип политика следва да бъде лесна за четене, разбиране и прилагане от страна на персонала. Ясно трябва да посочва в какви случаи се разрешава и в кои случаи не се разрешава използване на електронната поща, какви данни могат да бъдат изпращани и т.н. Възможно е да се налага следене на имейлите, което също следва да бъде документирано в политиката.
- сигурност на мобилните устройства: в случай, че компанията разрешава на персонала да използва мобилни устройства за техните професионални нужди следва да се обърне внимание на заплахите, които могат да компрометират сигурността на мрежата. Приема се, че служителите са по-продуктивни когато използват мобилни устройства, както и че ползите от тези устройства са толкова големи, че не бива да се игнорират. В същото време мобилните устройства създават допълнителни предизвикателства пред сигурността на данните. Като пример може да се посочи кражбата на мобилно устройство, което води до загуба или кражба на данни. Защитата на сигурността на данните обработвани с помощта на мобилни устройства може да включва следните действия:
- използване на софтуер за защита на всяко мобилно устройство, който може да намали вероятността за хакерска атака, да предпазва от кражба на данни, да предпазва от шпиониране при използване на публични мрежи, да открива и отстранява вируси, да елиминира спам съобщения;
- своевременно обновяване на софтуера, инсталиран на мобилните устройства. Отношението към мобилните устройства следва да бъде като към настолните персонални компютри по отношение на обновяването на софтуера.

Комуникации

Успехът на програмата за киберсигурност зависи от нейното комуникиране с различните групи заинтересовани лица. Комуникирането на програмата за киберсигурност се извършва с помощта на:

- политики, които представляват указания от най-високо ниво в организацията. Разработват се най-често от специалистите по киберсигурност, съгласуват се с правния отдел на организацията и се утвърждават от висшето ръководство. Добре е да следват едно общо съдържание, което може да се постигне чрез разработване на примерен модел за разписване на политика за киберсигурност, който да се прилага при всеки възникнал случай;
- стандарти, които задават екосистемата на политиката. С тяхна помощ се фиксира рамката за разбиране и прилагане на политиките за киберсигурност;
- процедури, представляващи списък от действия, изпълнението на които удовлетворява стандартите и създава условия за изпълнение на политиките. Пример за процедура: когато пътувате с колата си в зимни условия – 1. Трябва да сте сигурен, че разполагате с достатъчно гориво; 2. Трябва да се сигурен, че носите свидетелството за управление на автомобил и застраховката; 3. Да разполагате с вериги и други технически средства, които се изискват при шофиране в снежна обстановка; 4. Да заредите мобилния си телефон; 5. Да включите GPS-а. В този случай стандартите ще определят каква карта на GPS системата да се използва, какви технически средства за сигурност се препоръчват и т.н. Често пъти организациите сливат стандартите с процедурите;
- ръководства, които се разработват при нужда за да пояснят начина за изпълнение на процедурите.

Политиките и стандартите за киберсигурност са общи или единни за организацията, докато процедурите и ръководствата са специфични за различните информационни активи.

- политика за въвеждане на програмата за киберсигурност и свързаните с нея стандарти. Има следното съдържание:
  - заглавие на политиката, което показва за какво се отнася конкретната политика. Тук принципът, който трябва да се спазва гласи „по-кратко е по-добре“.
  - описание на политиката, което показва нейното предназначение;
  - защо е необходима политиката, от което всеки трябва да може да разбере защо е разработена и защо се въвежда тази политика, както и защо същата трябва да се спазва;
  - за кого се отнася политиката. Тъй като киберсигурността на организацията е дело и отговорност на всеки служител нормално е да се приеме, че в общия случай политиката за киберсигурност се отнася до всички служители;
  - кои са свързаните стандарти, които поясняват съдържанието на политиката;
  - с какви отговорности натоварва потребителите тази политика.

Обобщение

Като обобщение може да се каже, че разработването и прилагането на програма за киберсигурност представлява един от ключовите фактори за успех при защитата на информационните системи, мрежи, приложения, данните и информация на организацията. В

съдържанието на една такава програма могат да съществуват нюанси, но в същото време има задължителни елементи, които следва да бъдат в йерархическа зависимост, логическа свързаност, достатъчна изчерпателност и конкретност. Програмата за киберсигурност гарантира системност в усилията за постигане на киберсигурност, което без съмнение е по-добрия подход в сравнението му с ad-hoc решаването на възникнали инциденти.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Cisco, “Cybersecurity Management Program Whitepaper,” 2017, https://www.tylercybersecurity.com/information-security-program-template.

[2] Tyler Technologies, “Information Security/Cybersecurity Program,” 2018, https://www.tylercybersecurity.com/information-security-program-template.

[3] ACME Business Consulting, LLC, “Digital Security Program (DSP)” 2018, https://graphics.complianceforge.com/graphics/digital-security-program/example-digital-security-program.pdf.

[4] Federal Communications Commision, “Small Biz Cyber Planner 2.0,” 2012, https://www.fcc.gov/cyberplanner.

[5] Federal Communications Commission, *Cyber Security Planning Guide* (San Jose, CA: NBU Company, 2021).

[6] Chris Maschovitis, *Cybersecurity Program Development for Business* (Wiley, 2018).

[7] Tim Bandos, *Incident Responder’s Field Guide* (Waltham, MA: Digital Guardian, 2016).

[8] Eric Cole, *Insider Threats and the Need for Fast and Directed Response—A SANS Survey* (Bethesda, MD: SANS Institute, 2016).

[9] Mike Chapple, James Stewart, Darril Gibson, *Certified Information System Security Professional* (2018).

[10] Венелин Георгиев, *Основи на киберсигурността* (София: Авангард, 2019).