КИБЕРСИГУРНОСТТА Е ОТ РЕШАВАЩО ЗНАЧЕНИЕ ЗА ВСИЧКИ ОРГАНИЗАЦИИ – ГОЛЕМИ И МАЛКИ

Steve Ursillo, Jr. ***Christopher Arnold***

Въведение

В днешния компютъризиран свят всеки час се появяват нови рискове. Свързването с интернет отваря възможността хакер да атакува вашата организация. Киберпрестъпността се превръща в голям бизнес, а киберрисковете – във фокус на организациите и правителствата в световен мащаб. Финансовите рискове и рисковете за репутацията са високи, ако организациите не разполагат с подходящ план за киберсигурност.

Киберсигурността и нарушенията на сигурността на данните продължават да се увеличават и да засягат организации от всички размери и сектори. Най-новият Доклад 2023 г. на Hiscox за готовността за кибератаки показва, че кибератаките се увеличават непрекъснато в продължение на четири последователни години, като се наблюдава забележителен ръст на атаките срещу по-малки предприятия, достигащ 36%. Според Statista през 2022 г. производственият сектор е бил засегнат от най-голям дял кибератаки в сравнение с други отрасли, следван плътно от финансовия и застрахователния. Последните случаи са свързани с кражби на чувствителна информация, което води до значителни финансови загуби за засегнатите компании.

Какво представлява киберсигурността?

Киберсигурността гарантира, че данните на вашата организация са защитени от атаки от вътрешни и външни злонамерени участници. Тя може да обхване съвкупност от технологии, процеси, структури и практики, използвани за защита на мрежи, компютри, програми и данни от неоторизиран достъп или увреждане. Целта на всяка стратегия за киберсигурност е да се гарантира поверителност, цялостност и наличност на данните.

Съществуват няколко основни начина, чрез които проблемите с киберсигурността могат да засегнат (или дори да унищожат) организацията и нейната репутация. Съществува риск хакер да получи чувствителна информация, като например данни за банкови сметки или кредитни карти. В „тъмната мрежа“ има свободно достъпни пазари за такава информация. Ако други лица получат достъп до такава чувствителна информация, организацията може да се окаже с отнети банкови или кредитни карти или в нарушение на законите за защита на личните данни. Всеки месец в световен мащаб се съобщава за значими нарушения на сигурността, които засягат лични данни.

Вторият, но свързан с това проблем е, че когато хакер получи чувствителна информация за организацията, тя може да се окаже с разрушена репутация. Много малък брой малки организации могат да преживеят щетите, които може да нанесе на репутацията им подобна загуба на данни. Увреждането на репутацията и доброто име може да бъде по-унищожително от самата загуба на данни. Загубата на данни на клиенти може да доведе до правни или регулаторни искове срещу организацията. Трета страна може да заведе дело срещу организацията, тъй като самата тя е претърпяла загуба. Организациите могат да бъдат подложени на значителни санкции и/или съдебни дела, произтичащи от нарушения на законите за защита на личните данни в много юрисдикции.

Най-новият и тревожен аспект на киберсигурността, който създава значителни проблеми на организациите, е изнудваческият софтуер. Още през 2012 г. се появиха съобщения за кампании с програми с искания за откуп, които възприеха търговски бизнес модели. В много случаи зловредният софтуер е прикрит и вграден в друг вид документ, който само чака да бъде изпълнен от целевия потребител. След като се изпълни, зловредният софтуер може да криптира данните на организацията с таен 2048-битов ключ за криптиране или да се свърже с централизиран сървър за управление и контрол, за да изчака инструкциите, изпълнявани от нарушителя. Веднъж заразени, данните на организацията продължават да бъдат недостъпни, тъй като те се криптират с ключа за криптиране на нарушителите. След като всички достъпни данни бъдат криптирани, включително в много случаи резервните данни и системи, организацията ще бъде инструктирана как да плати откуп в рамките на няколко дни или нарушителят ще премахне ключа за криптиране и данните ще бъдат загубени. В буквалния смисъл на думата недоброжелателят иска откуп за данните и оттук наименованието на английски език – „рансъмуер“ (от англ. „ransom“ – откуп). Ключът за криптиране е достатъчно силен, така че разбиването на ключа вместо плащането на откуп е икономически неизгодно – според някои оценки на средностатистически настолен компютър ще са му необходими пет квадрилиона години, за да декриптира данните без ключа. В някои случаи таргетираната организация може да се надява, че някои изследователи може да са открили начин за декриптиране на данните въз основа на конструктивен недостатък. В противен случай организацията ще

трябва да потърси начин да възстанови системите и данните от сигурно резервно копие или да обмисли плащането на откупа. Имайте предвид, че дори възстановяването на данните не елиминира риска рансъмуерът да не бъде активиран отново или да се върне въз основа на компрометираната цялост на средата.

Управление на киберсигурността

Трябва да бъде създадена програма за управление на киберсигурността и за управление на риска, която да е подходяща за размера на организацията. Рискът за киберсигурността трябва да се разглежда от собствениците и директорите като значителен бизнес риск. Той следва да бъде на същото ниво като рисковете, свързани със спазване на изискванията, оперативните, финансовите и репутационните рискове, с подходящи критерии за измерване и резултати, които се наблюдават и управляват.

Съществуват доброволни рамки, които могат да се използват за разглеждане на оценката на риска и свързаните с нея най-добри практики. Така например Рамката за киберсигурност на Националния институт по стандартизация и технологии (NIST) включва пет едновременни и непрекъснати функции:

1. Идентифициране: Разработване на организационно разбиране за управление на риска за киберсигурността на системите, хората, активите, данните и способностите.
2. Защита: Разработване и прилагане на подходящи предпазни мерки за гарантиране предоставянето на критично важни услуги.
3. Разкриване: Разработване и прилагане на подходящи дейности за идентифициране на възникването на събитие в областта на киберсигурността.
4. Отговор: Разработване и прилагане на подходящи дейности за предприемане на действия във връзка с разкрит инцидент в областта на киберсигурността.
5. Възстановяване: Разработване и прилагане на подходящи дейности за поддържане на плановете за устойчивост и за възстановяване на всички способности или услуги, които са били нарушени вследствие на инцидент, свързан с киберсигурността.

Защита от злонамерен софтуер и външни атаки

Продължават да се появяват нови заплахи и всяка организация трябва да е сигурна, че е подготвена да се справи с динамичния пейзаж на заплахите. По-долу са изброени някои от най-важните системни помощни програми и решения, използвани за смекчаване на тези злонамерени атаки:

- Защитните стени са софтуер (а също и хардуер), предназначен да защитава системата от атаки от хора, които имат достъп до системите на организацията чрез вътрешни и външни комуникационни връзки.
- Решенията за защита от зловреден/шпионски софтуер и уеб прокси сървъри защитават системата от софтуерен код, който може да е от изскачащи прозорци или да има по-коварни намерения, като например въвеждане на потребителски имена и пароли с цел измама.
- Софтуерът за борба със спама предпазва пощенските кутии от задръстване с нежелани излъчени имейли.
- Софтуерът за борба с фишинга защитава потребителите, които посещават уебсайтове, предназначени за улавяне на потребителска информация, която след това може да се използва за измамни цели.

Всички те са задължителни за всяка добре управлявана система, използваща стратегия за защита в дълбочина. Цената на една атака може да бъде значителна, включваща загуба на данни, измами и разходи за възстановяване на системите, и следва да се анализира спрямо разходите за защита срещу такива заплахи.

Препоръчително е да използвате добре познат и реномиран доставчик. Някои компании претендират, че предоставят такива помощни програми, но в действителност самите програми могат да бъдат зловреден софтуер. Бъдете предпазливи при използването на безплатен софтуер или софтуер от неизвестен доставчик. Обикновено е най-добре да се използват помощните програми, препоръчани от организацията за системна интеграция (техническа поддръжка) на предприятието, тъй като тя ще отговаря за тяхното инсталиране, конфигуриране и поддръжка.

Поддръжката на тези приложения е от решаващо значение. Всеки ден се появява нов зловреден софтуер. Повечето доставчици на софтуер осигуряват поне ежедневно автоматично обновяване на своите бази данни, за да се гарантира, че системата продължава да бъде ефективно защитена. Гарантирането на правилното прилагане на тези актуализации е от съществено значение.

Планове за поддръжка на хардуера

С доставчиците на хардуер трябва да се сключват договори за поддръжка, за да могат бързо да се отстраняват хардуерни повреди. В тези договори следва да се посочат нивата на обслужване, които доставчикът ще спазва в случай на повреда. Критичният хардуер, като например сървъри, комутатори и технологии за архивиране, изисква незабавно внимание. В много от договорите се посочва четиричасова реакция при повреда на тези компоненти. Друг по-малко критичен хардуер, като например отделни работни станции, може да има по-дълги срокове за реакция.

Някои организации, особено в отдалечени райони, закупуват определени критични компоненти, които са по-склонни към повреда, като например захранващи устройства, като резервни части, които могат бързо да заменят повредения компонент. Организациите, които разчитат на договори за поддръжка, трябва да гарантират, че фирмата за поддръжка поддържа адекватни доставки на резервни компоненти, за да изпълни ангажиментите на организациите за ниво на обслужване.

Качеството на външната компания за ИТ поддръжка на организацията е от решаващо значение за гарантиране на правилното внедряване и поддръжка на системите. Въпросите, които трябва да се вземат предвид при избора на подходяща компания, включват:

- техните познания и опит с конфигурацията на хардуера и операционната система на организацията;
- техните познания и опит с приложния софтуер на организацията;
- сертификати, издадени от големи хардуерни и софтуерни компании, които дават гаранция за компетентността на хората в организацията;
- броят на хората в компанията, които имат необходимите познания за поддръжка на системата – това е от решаващо значение, тъй като разчитането на един-единствен човек може да доведе до значителни забавяния и разходи, ако този човек не е на разположение по някаква причина;
- способността им да предоставят услуги за поддръжка от разстояние, за да могат да реагират бързо на проблеми на разумна цена;
- надлежна проверка и управление на риска при доставчиците, за да се гарантира, че третата страна предоставя услугите в съответствие с очакванията на организациите.

Хора и документация

Всяка организация трябва да изготви план за намаляване на риска от недостъпност на ключови хора в случай на срив на системата. Съхранявайте списък с данни за контакт с техниците, отговорни за резервните копия. Документирайте конфигурацията на хардуерните и софтуерните приложения и я актуализирайте, така че нов техник да може бързо да възстанови системата.

Политики и процедури

Правилните процедури за управление на ИТ в една организация са от решаващо значение. Внедрете официален процес за оценка на риска и разработете политики, за да гарантирате, че системите не се използват неправомерно и се уверете, че приложимите политики се преразглеждат и

актуализират непрекъснато, за да отразяват най-актуалните рискове. Това включва разработване на политики и процедури за реагиране при инциденти, за да се отговори правилно на потенциално нарушение, да се отчетат и намалят разходите при такова потенциално нарушение.

Продължаващото обучение на всички служители относно технологичните рискове трябва да бъде част от рамката за управление на риска на организацията, като потенциалните нарушения на сигурността се смекчават в резултат на обучението и политиките, които се популяризират на всички нива на персонала. Политиките трябва да включват, но не се ограничават до:

- Управление на потребителски акаунти: правила и политики за всички нива на потребителите; процедури за осигуряване на своевременно откриване на инциденти, свързани със сигурността; ИТ системите и поверителните данни са защитени от неоторизирани потребители.
- Управление на данните: създаване на ефективни процедури за управление на хранилищата, архивиране и възстановяване на данни и правилно унищожаване на носителите. Ефективното управление на данните помага да се гарантира качеството, навременността и наличността на бизнес данните.
- ИТ сигурност и управление на риска: процес, който поддържа целостта на информацията и защитата на ИТ активите. Този процес включва установяване и поддържане на роли и отговорности в областта на ИТ сигурността, политики, стандарти и процедури.

Отделните юрисдикции вероятно са приели законодателство, което може да изисква адресиране на конкретни политики или въпроси в рамките на конкретна политика. Често срещаните политики са изброени по-долу и обхващат използването на системата, използването на електронна поща, използването на интернет и отдалечения достъп.

Политика за използване на системата

Обикновено политиката за използване на системата очертава правилата, по които могат да бъдат използвани ИТ системите на организацията. Примерните елементи, които трябва да се вземат предвид при тази политика, включват:

- задължително използване на пароли във всички системи, като например телефони и таблети, включително необходимост от редовна смяна на паролите и забрана за предоставяне на пароли на други членове на екипа или на трети страни;
- забрана за копиране на данни на организацията и изнасяне на данни от офиса без разрешение;
- криптиране на памети/USB стикове;

- физическата сигурност на оборудването;
- използване на системата в работно време;
- правила за частно използване на системата, ако е разрешено, извън работното време;
- многофакторно удостоверяване – използване на повече от един метод за удостоверяване от независими категории удостоверения за проверка на самоличността на потребителя за влизане в системата.

Политика за използване на електронна поща

Примерните елементи, които трябва да се вземат предвид при политиката за използване на електронна поща, включват:

- забрана за използване на лични имейл акаунти за служебни въпроси;
- забрана за отваряне на прикачени файлове към имейли от непознати източници (тъй като те могат да съдържат зловреден софтуер);
- забрана за достъп до имейл акаунти на други лица;
- забрана за споделяне на пароли за имейл акаунти;
- забрана за прекомерно лично използване на електронната поща на организацията;
- уведомяване, че организацията ще следи електронната поща.

Политика за използване на интернет

Примерните елементи, които трябва да се вземат предвид при политиката за използване на интернет, включват:

- ограничаване използването на интернет за служебни цели;
- уведомяване за възможността на организацията да проследява използването на интернет;
- забрана за достъп до сайтове, които са обидни за пола, сексуалността, религията, националността или политическите убеждения на дадено лице;
- гарантиране, че изтеглянето се извършва само от сигурен и реномиран уебсайт;
- забрана за изтегляне на изпълними (програмни) файлове, тъй като те могат да съдържат зловреден софтуер, както и забрана за изтегляне на пиратска музика, филми или софтуер;
- забрана за предоставяне на служебния имейл адрес на потребителя, за да се ограничи вероятността от спам;

- последици от нарушението.

Политика за отдалечения достъп

Примерните елементи, които трябва да се вземат предвид при политиката за отдалечен достъп, включват:

- изискване на одобрения за външен достъп;
- възстановяване на разходите за външен достъп;
- процедури за сигурност (включително разкриване на пароли, използване на системата от трети страни, изключване от други мрежи по време на достъпа до системите на организацията, използване на защитни стени и инсталиране на подходящ софтуер за защита на отдалечената система от злонамерени атаки и многофакторно удостоверяване);
- физическа сигурност на предоставеното от организацията оборудване, като например лаптопи;
- съобщаване за всяко възможно нарушение на сигурността, неоторизиран достъп или разкриване на данни на организацията;
- съгласие, че организацията може да наблюдава дейностите на външния потребител, за да идентифицира необичайни модели на използване или други дейности, които могат да изглеждат подозрителни;
- последици от неспазването на изискванията.

Застраховане

Адекватната застраховка трябва да покрива разходите за подмяна на повредената инфраструктура, както и разходите за труд за разследване на инцидента, възстановяване на системите и възстановяване на данните. Помислете и за застраховка за загуба на производителност в резултат на голям срив на системата или катастрофично събитие.

Steve Ursillo, Jr.

Съдружник, Застраховане на риска и консултации, национален ръководител: гарантиране на информацията и киберсигурност, Cherry Bekaert LLP

Съдружник в групата Cherry Bekaert's Risk Assurance & Advisory Services (RAAS) и изпълнява длъжността национален ръководител по отношение на практиката по гарантиране на информацията и киберсигурност. Специализира в областта на управлението на технологичния риск,

вътрешния контрол върху финансовото отчитане, сигурността на информационните системи, неприкосновеността на личния живот, кибер измами, управлението на киберсигурността, информационното осигуряване и консултантските услуги в областта на информационните технологии. С повече от 20 години опит Steve предоставя разнообразни услуги за ИТ одит и сигурност на своите клиенти в различни индустрии. Steve притежава няколко професионални квалификации, които имат отношение към неговия опит и практиката на фирмата, а именно: CPA, CIA, CGMA, CFE, CISA, CISM, CITP, CISSP, CGEIT, CRISC, CEH и CCSFP.

Christopher Arnold

Директор

Christopher Arnold е директор в Международната федерация на счетоводителите (IFAC). Той ръководи дейностите, свързани с допринасянето и насърчаването на разработването, приемането и прилагането на висококачествени международни стандарти, включително програмата за съответствие на членовете, интелектуалната собственост и преводите. Christopher отговаря също така и за инициативите на IFAC по отношение на малките и средни предприятия (МСП), малките и средни практики (МСПрак.) и научноизследователската дейност, които включват развитие на лидерство в областта на анализа и научните изследвания, обществената политика и застъпничеството. Преди това той е бил одит мениджър в Deloitte и придобива квалификация професионален счетоводител в счетоводна практика със средна големина в Лондон (сега „PKF-Littlejohn LLP“). Christopher започва кариерата си като съветник по политиката за малкия бизнес в Асоциацията на дипломираните експерт-счетоводители (ACCA).