СТРУКТУРИРАН ПОДХОД КЪМ ПРЕДИЗВИКАТЕЛСТВАТА, СВЪРЗАНИ С ИНФОРМАЦИОННАТА СИГУРНОСТ И ПОВЕРИТЕЛНОСТТА НА ЛИЧНИТЕ ДАННИ ПРЕЗ XXI ВЕК

Веселин Целков, Георги Средков
Университет по библиотекознание и информационни технологии

Резюме: Докладът представя виждането на авторите за структуриран подход в управлението на поверителността и сигурността на информацията, който да отговори на новите предизвикателства, породени от глобалната комуникационна свързаност и мащабното навлизане на нови технологии в организациите. Маркирани са основните области, които трябва да обхване програмата за поверителност и сигурност на една организация.

Ключови думи: информационна сигурност, поверителност, лични данни, предизвикателства, подход.

Въведение

Информационната революция преобрази света, цели държави, бизнеса и самите хора по един мащабен и задълбочен начин. Почти всички дейности на частни и държавни организации вече са дигитални, в резултат на което личните данни на всяко физическо лице се съхраняват в различни информационни системи.

От тази трансформация на дневен ред произлязоха две основни предизвикателства:

- да се защити личната информация от престъпни организации;
- да се гарантира, че личната информация се използва само за ясно заявени цели.

Трудностите при справянето с тези предизвикателства помогнаха да се подчертае значението на експертизата, която съчетава познания по киберсигурност и такива, свързани с поверителността на личните данни. Бяха създадени и приети множество регламенти, закони, разпоредби и стандарти за сигурност и поверителност, които налагат нови изисквания към организациите и правителствата за въвеждане на специфични практики за защита и контрол върху използването на нашата лична информация[1].

За да се справим с възникналите предизвикателства, трябва да можем ефективно да управляваме следните области [1]:

- Управление на поверителността – да бъде създадена и поддържана работна рамка:
  - за управление на поверителността;
  - за управление на риска и поддържащи процеси, за да се гарантира, че стратегията за поверителност е в съответствие с приложимите закони, с целите и задачите на организацията.
- Архитектура на поверителността – технологичната архитектура, инфраструктурата, оперативната дейност и контролът трябва да осигуряват адекватни предпазни мерки за защита и правилно използване на личната информация.
- Жизнен цикъл на данните – инвентаризация, разработване и поддържане на актуални регистри на обработваната информация и на самите процеси, за да се осигурят качество, ограничаване, минимизиране и защита на данните през целия документиран жизнен цикъл на данните.

Управление на поверителността

Добро ръководство

Доброто ръководство на неприкосновеността на личния живот е набор от установени дейности, фокусиран върху няколко основни принципа и очаквани резултата, предназначени да позволят на мениджмънта да има ясно разбиране за:

- състоянието на програмата за поверителност на организацията;
- съществуващите рискове;
- дейностите по привеждане и поддържане в съответствие на поверителността спрямо целите и практиките в бизнеса на организацията.

Целта на програмата за поверителност е да даде възможност за изпълнение на стратегията за поверителност, като сама по себе си тя да продължава да бъде в съответствие както с бизнес целите, така и с приложимите регулации. Процесите, подкрепящи тези принципи, включват:

- политика за поверителност;
- управление на данните;
- съответствие с изискванията на нормативните документи;
- управление на риска и на киберсигурността.

Доброто ръководство започва с установяване на стратегически цели от висшия мениджмънт, които се трансформират в действия, роли и отговорности чрез политики, процедури, процеси и други

дейности надолу по йерархията, до всички служители в организацията.

Поверителността вече твърдо се е установила като част от бизнеса на организациите и ако те не я ръководят правилно или не защитават адекватно личните данни, могат да имат сериозен проблем.

Една организация може да поддържа ниско ниво на риск за поверителността само когато нейните служители – от висшия мениджмънт до отделните сътрудници – разберат важността на поверителността и сигурността в рамките на своите собствени роли и отговорности. Това отговорно отношение води и до идентифициране на потенциални събития, свързани със сигурността и поверителността, до по-малко инциденти с по-слабо въздействие върху текущата дейност и репутацията на организацията.

Дейностите, свързани с доброто ръководство, включват:

- привеждане в съответствие на бизнеса;
- разработване на стратегия за сигурност и поверителност;
- дейности по управление на сигурността и поверителността;
- ресурси, необходими за разработване и изпълнение на стратегията за сигурност и поверителност;
- показатели за сигурност и поверителност.

Ангажирането на висшия мениджмънт за поддържане на информационната сигурност и поверителността като част от бизнеса е вече задължително за всяка сериозна организация. Висшето ръководство е отговорно за прилагането на подходящ модел за управление на сигурността и поверителността, включващ стратегия за поверителност и стратегия за сигурност.

Програмите за сигурност и поверителност трябва да бъдат в съответствие с общите цели и задачи на организацията.

Ролите и отговорностите на една организация трябва да бъдат в синхрон с нейната култура на отчетност.

Сигурността и поверителността на информацията са отговорност на всеки служител в дадена организация; обаче средствата за възлагане и наблюдение на тези отговорности могат да се различават значително според ролите, които служителят изпълнява.

Стратегиите за сигурност и поверителност трябва да вземат предвид толерантността на всяка организация към промяна в рамките на даден период от време.

Всяка организация трябва да избере своя работна рамка за контрол (например тази на NIST), след което да направи необходимите корекции в прилаганите контроли спрямо нуждите на своя бизнес [2].

Всяка организация има своя собствена практика за разработване, представяне, обсъждане и одобряване на стратегически инициативи.

Стратегиите за сигурност и поверителност трябва да предвидят потенциалните пречки и ограничения, влияещи върху постигането на стратегическите цели, и да обмислят подобряването на тези цели, така че те да могат да бъдат реализирани.

Управление

Управлението на поверителността обикновено е фокусирано върху бизнес дейностите, свързани със събирането, обработката и трансфера на лични данни. Управлението на поверителността включва бизнес процесите и поддържащите ги информационни системи.

Важни за управлението на поверителността са следните елементи:

- роли и отговорности в областта на ИТ и в осигуряването на поверителност на личните данни;
- политика за поверителност;
- мониторинг на данни;
- работа със субекти на данни и регулаторни органи;
- обучение за поверителност на личните данни;
- управление на риска от трети страни;
- одит на процесите, системите и дейностите, свързани с осигуряването на поверителност;
- управление на инциденти, свързани с поверителността;
- постоянно подобряване на програмата за поверителност;
- обучение, изграждане и поддържане на осъзнато, отговорно отношение към поверителността;
- реакция при инциденти, свързани със сигурността и с поверителността.

Длъжността и йерархичното положение на даден служител в организацията следва да отразяват неговата роля, функция и сфера на отговорност.

Прилагането на „поверителност при проектиране“ и „поверителност по подразбиране“ засяга процесите, процедурите и дейностите на почти целия персонал в ИТ.

Наличието и използването на неструктурирани данни често представлява най-голямото предизвикателство за прилагане на подходящи защитни механизми от страна на длъжностното лице по защита на данни.

Колкото по-голям е броят на подизпълнителите на ИТ услуги или аутсорсинг, толкова по-голяма е нуждата от ефективна програма за управление на трети страни, като в тези случаи е задължително да има подписан Договор за обработка на данни с обработващ (*Data Processing Agreement*).

За да бъде ефективна програмата за поверителност, е необходимо партньорство между ИТ, Информационна сигурност, Човешки ресурси, Правен отдел и всички бизнес звена. Поверителността не може да работи във вакуум, защото всички тези други организации управляват ключови бизнес процеси, а информационните системи обработват лична информация.

Одитът на изпълнението на програмата за поверителност е важна проверка за това дали организацията извършва правилна, законосъобразна обработка на личните данни.

С относително незначителни допълнения планът за реакция при инциденти в областта на сигурността на организацията може да бъде разширен, за да служи ефективно и като план за реакция при инциденти, свързани с поверителността.

Висшето ръководство определя кога и къде трябва да се прилагат подобрения в процесите, процедурите и контролите.

Управление на риска

Този аспект включва:

- жизнен цикъл на управление на риска;
- риск регистър;
- заплахи за поверителността и уязвимости;
- оценки на въздействието върху поверителността;

Рискът за поверителността не може да бъде отделен от информационния риск.

Тъй като защитата на данните е част от поверителността, сигурността на информацията не може да бъде напълно отделена от поверителността. По този начин много процеси, включително управлението на риска, работят по-добре, когато засягат и сигурността, и поверителността.

Важни стандарти за управление на риска са:

- ISO/IEC 27005, Информационни технологии – Техники за сигурност – Управление на риска при информационна сигурност;
- ISO/IEC 27701, Техники за сигурност – Разширение на ISO/IEC 27001 и ISO/IEC 27002 за управление на поверителността на информацията – Изисквания и насоки.

Уязвимостта е слабост в системата, която може да позволи реализирането на атака. Уязвимостта не е векторът на самата атака или използваната техника – това се нарича заплаха.

Въпреки че въздействието на дадена заплаха може да бъде изчислено, като цяло е много по-трудно да се знае вероятността за възникване на заплахата.

Архитектура на поверителността

Инфраструктура

Този аспект включва:

- технологични стекове;
- облачни услуги;
- крайни точки;
- отдалечен достъп;
- техники за подсилване на системата.

Технологичната инфраструктура има пряко отношение към поверителността. От една страна, тя включва правилното управление на съхранената лична информация, а от друга – нейната защита.

Все по-често познанията за хардуера на сървърите се превръщат в абстракция с появата на облачните услуги. От друга страна, е важно да се разберат принципите на дизайна на хардуера, тъй като устройствата на крайните потребители продължават да се използват.

Работата на мрежовите TCP/IP протоколи и съответните сървиси остават непроменени, независимо от транспортната среда. Някои протоколи, като Bluetooth, имат присъщи уязвимости, които могат да бъдат редуцирани чрез въвеждане на подходящи мрежови контроли.

Криптирането е полезен инструмент за защита на личните данни, докато те се съхраняват или пренасят. То може също да предотврати неправилното използване или компрометирането на личната информация.

Все по-често мрежовите устройства, като защитни стени, системи за предотвратяване на проникване, филтри за уебсъдържание, фишинг филтри, проксита и др., могат да бъдат базирани на сървъри в облака, а не под формата на физически устройства.

IaaS, PaaS и SaaS са основни облачни услуги.

Докато използването на IaaS, PaaS и SaaS облекчава организациите от тежестта на управлението на хардуер и операционни системи, организациите трябва да са наясно с моделите на разпределение на отговорността в облака и да адаптират своите дейности, за да гарантират, че всички необходими услуги за сигурност се изпълняват ефективно.

Виртуалната преносима инфраструктура (VDI) може да бъде ефективно средство за защита при прилагане на Bring your own device (BYOD) политики и чрез преместване на чувствителни данни към бекенд сървъри, извън тези преносими устройства.

Нулевото доверие е нов подход към архитектурата на сигурността, който се фокусира повече върху защитените данни и по-малко – върху периметъра.

Свързаните устройства (IOT) често имат по-ниско ниво на сигурност и изискват допълнителни защитни контроли, например сегментиране на мрежата.

С миграцията на локални ресурси към облака парадигмата за отдалечен достъп се насочва към по-сигурни комуникации.

Усилването на защитата на системите без автоматизация е трудно, предвид големия брой необходими промени в конфигурацията.

Софтуерни приложения

Този аспект включва:

- концепция за прилагане на сигурност и поверителност при проектиране, а не впоследствие;
- бизнес процеси, използвани за придобиване, разработване и поддържане на приложения;
- техники, използвани, за да направят приложенията устойчиви на атаки и злоупотреби;
- механизми за проследяване на действията на потребителите.

Софтуерните приложения са свързани с поверителността. Когато отделните потребители си взаимодействат с информационните технологии предимно чрез бизнес приложенията или в интернет, системите често имат средства, с които проследяват и записват самите действия на потребителите или други поведенчески данни. Такива са например „кукитата“.

- Жизненият цикъл на разработването на системите е нов начин за изразяване на традиционния жизнен цикъл на разработка на софтуер, за да се подчертае преминаването от чисто разработване на софтуер към две отделни дейности: проектиране и управление на ИТ инфраструктурата и придобиване на SaaS бизнес приложения.
- Диаграмите на потока от данни и диаграмите на релациите между обектите трябва да бъдат включени в документацията за проектиране на системата, така че специалистите по сигурност и поверителност да могат да гарантират защитата и правилното използване на личната информация.

- Разработката на сигурни оперативни дейности включва възможности за проектиране и тестване на защитата, които са част от процеса на бързо развитие и автоматизирано тестване.
- Прилагат се модули за сканиране на сигурността на кода и други интегрирани функции за гарантиране на сигурността на разработваните приложения.
- Прилаганите техники за мониторинг на работното място са необходими за защита на организацията от кибератаки и злонамерен софтуер. Тези техники обаче трябва да бъдат съобразени с изискванията на приложимите регулации за защита на личните данни.

Технически контроли за поверителност

Темата за техническите контроли за поверителност включва:

- контроли, работни рамки за контрол и поддържане на сигурност и поверителност;
- комуникационни протоколи на мрежата, използвани за предаване на лична информация;
- техники за криптиране и управление на ключове, използвани за защита на личната информация;
- регистриране и наблюдение на събития, свързани със сигурността и поверителността;
- управление на идентификаторите и на достъпа.

Целите на контрола на поверителността са в контекста на информационната сигурност.

Правилният подход за избор на работна рамка за контрол е свързан повече със структурата на контролите, отколкото със самите контроли.

Видът на мрежовите елементи обикновено не зависи от използваните протоколи. По-новите типове мрежови елементи обаче обикновено не поддържат по-стари протоколи.

Ethernet и Wi-Fi са доминиращите видове свързаност, използвани в бизнес и домашните мрежи за данни, а TCP/IP е универсален мрежов протокол.

Сегментирането на мрежите само по себе си не означава дали съществуват подходящи контроли за достъп до мрежата за отделяне на мрежовите сегменти.

Криптирането се смята за добра форма на защита на достъпа. Макар и мощно средство, криптирането трябва да бъде внимателно обмислено, проектирано и внедрено, за да бъде ефективно.

Системите за управление на събития, свързани със сигурността на информацията (Security information and event management, SIEM),

често се използват не само за събития, свързани със сигурността, но и за такива, свързани с оперативната дейност или с поверителността.

Потенциалът и честотата на заплахите в системата са пряко пропорционални на възприетата стойност на активите, които системата съхранява или защитава.

Поради миграцията на локални системи към облака, концепцията и практиката за отдалечен достъп отстъпват място на VPN с цел защита на мрежовия трафик за персонала, работещ извън офисите на организацията.

Честотата и строгостта на различните видове проверки на достъпа трябва да се определят както от нивото на автоматизация, така и от историческите резултати от предходни прегледи.

Жизнен цикъл на данните

Предназначение на данните

Този аспект включва:

- компоненти за управление на данни: политика, контроли, оценки и отчетност;
- създаване и поддържане на списък с данните – първа стъпка за управление на поверителността;
- политика за класифициране на данните и стандарти за обработка;
- класифициране на системите, локациите и сайтовете;
- техники и инструменти за предотвратяване на загубата на данни;
- качество и точност на данните;
- ограничение на използването на данни и анализ на данните.

Програмите за поверителност изискват ефективна програма за управление на данните, която да осигурява прозрачност на управлението и контрол на личната информация. Управлението на данни включва: инвентаризация, класифициране и обработка на данните, допълнена от инструменти и техники за предотвратяване на загуба на данни (Data Loss Prevention, DLP), както и прилагане на мерки за гарантиране на качеството и точността на данните и такива за гарантиране на ограничаването на използването на данни.

Предизвикателство в дейността на организацията е обработката на неструктурирани данни, защото те се променят често и по-трудно биха могли да бъдат описани.

Политиките и стандартите за класифициране на данни трябва да бъдат възможно най-прости, за да могат да бъдат по-лесно въведени и прилагани в организацията.

Длъжностното лице по защита на данните и мениджърите по информационна сигурност трябва да са напълно наясно с потенциалното въздействие на класификацията на данните върху корпоративната култура.

Организациите прилагат като първа стъпка статични инструменти за превенция на изтичането на информация (DLP), за да идентифицират какви чувствителни данни се намират на споделени ресурси, например на файлови сървъри.

Прилагането на динамично DLP изисква да се вземат предвид идентифицираните рискове и съществуващите контроли, за да могат да бъдат разрешени ефективно потенциалните проблеми.

Устойчивост на данните

Този аспект включва:

- техники за минимизиране на данните, псевдонимизация и анонимизация;
- съображения за поверителност при миграцията на данни;
- идентифициране на изискванията за поверителност и проблеми при съхраняване на данни;
- техники и предизвикателства при унищожаване на данни.

Програмите за поверителност изискват активно и целенасочено управление на личната информация в базите от данни на организацията и в неструктурираните хранилища на данни. Длъжностното лице по защита на данните трябва да идентифицира и управлява чрез прилагане на добрите бизнес практики, които включват минимизиране на данните, съхраняване на данните само толкова, колкото е необходимо, и унищожаване на данните [3].

Може да бъдат прилагани допълнителни контроли за мониторинг и защита на личната информация, за да се намалят рисковете от злоупотреба и компрометиране, например DLP системи.

Организациите трябва да са наясно в детайли с всеки модел на споделена отговорност, прилаган от доставчиците на интернет услуги, облачни услуги и др., за да се гарантира, че са налице всички необходими контроли.

Ако от организацията не се изисква да съхранява лична информация за дълги периоди от време, преместването на записи в отделно хранилище на данни може да бъде добра възможност за идентифициране на тези записи, тъй като те ще са премахнати от производствената среда.

При разработването на графици за задържане на данните организациите трябва да идентифицират всички приложими

разпоредби и изисквания, които се отнасят до минимални и максимални периоди, през които могат да се съхраняват лични данни.

За безопасното унищожаване на данни трябва да се отчитат:

- чувствителността на данните, които се унищожават;
- оценката на риска или на заплахата, които помагат да се определи степента, до която нарушител би се опитал да възстанови изхвърлените или унищожени носители на данни.

Заключение

Развитието и навлизането в глобален мащаб на новите технологии във всички сфери на живота, заедно с новото законодателство, поставиха редица предизвикателства както към информационната сигурност, така и към осигуряването на неприкосновеност на личните данни.

Това, както и други фактори породиха необходимостта от рисково базиран, структуриран подход, надграждащ информационната сигурност с прилагането на принципите и защитните механизми за поверителност и неприкосновеност на личните данни.

Авторското виждане, изложено в настоящия доклад, за прилагане на структуриран подход в управлението на поверителността и сигурността на информацията, маркира основните области, които трябва да обхване програмата за поверителност и сигурност на една организация. Материалът може да послужи като основа за подготовка за отговор на новите предизвикателства, породени от глобалната комуникационна свързаност и мащабното навлизане на нови технологии в организациите.

Бележки

[1] **Reglament (ES)2016/679** na Evropejskiya parlament i syveta ot 27 april 2016 gogina...

[**Регламент (ЕС) 2016/679** на Европейския парламент и съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО на Конвенцията на Съвета на Европа за защита на гражданите по отношение на автоматичната обработка на личните данни.]

References/Литература

1. **Tselkov**, V., D. **Petkov**, G. **Sredkov**, Pl. **Georgiev**. Zashtita na dannite. Printsipi i praktiki. Vtoro, prereboteno izdanie. Sofia: Za bukvite – O pismeneh, 2020. 333 s. ISBN 978-619-185-441-7.

[**Целков**, В., Д. **Петков**, Г. **Средков**, Пл. **Георгиев**. Защита на данните. Принципи и практики. Второ, преработено издание. София: За буквите – О писменехъ, 2020. 333 с. ISBN 978-619-185-441-7.]

2. **Tselkov**, V., S. **Denchev**, I. **Peteva**. Sigurnost na informacionnite resursi. Sofia: Za bukvite – O pismeneh, 2020. 268 s. ISBN: ISBN 978-619-185-432-5.

[**Целков**, В., С. **Денчев**, И. **Петева**. Сигурност на информационните ресурси. София: За буквите – О писменехъ, 2020. 268 с. ISBN: ISBN 978-619-185-432-5.]

3. **Tselkov**, V., G. **Sredkov**. Zashtita na lichnite danni i syotvetstvie s Reglament (ES)2016/679. – V: *Nauchni* trudove na UniBIT, tom 18, 2020.

[**Целков**, В., Г. **Средков**. Защита на личните данни и съответствие с изискванията на Регламент (ЕС) 2016/679. – В: *Научни* трудове на Университета по библиотекознание и информационни технологии, том 18, 2020.]

За авторите

Веселин Целков е професор, доктор на техническите науки в Университета по библиотекознание и информационни технологии. Автор и съавтор на 10 монографии и учебници и на над 250 научни публикации. Основните му интереси са в областта на информационната сигурност, защита на данните, управление на риска.

За контакт с автора: v.tselkov@unibit.bg

Георги Средков е магистър със специализация по „Икономическа информатика“ и доктор с дисертационен труд „Моделиране на взаимодействията в системата за защита на личните данни в Република България“ от Университета по библиотекознание и информационни технологии.

Член е на работната група Data Protection, Trust and Security Working Group на длъжностните лица по защита на данните към European Telecommunications Network Operators’ Association (ETNO) – Брюксел.

За контакт с автора: gsredkovtselkov@abv.bg

A STRUCTURED APPROACH TO THE CHALLENGES RELATED TO INFORMATION SECURITY AND CONFIDENTIALITY OF PERSONAL DATA IN THE XXI CENTURY

Veselin Tselkov, Georgi Sredkov
University of Library Studies and Information Technologies

Abstract: This paper presents the authors' vision for a structured approach to the management of privacy and security of information to meet the new challenges posed by the global connectivity and the invasion of new technologies in organizations. It is focused on the main areas that should be covered by the privacy and security program of an organization.

Keywords: information security, confidentiality, personal data, challenges, approach.

About the authors

Vesselin Tselkov is a professor, doctor of technical sciences at the University of Library Studies and Information Technologies. Author and co-author of 10 monographs and textbooks and over 250 scientific publications. His main interests are in the field of information security, data protection, and risk management.

To contact the author: v.tselkov@unibit.bg

Georgi Sredkov, PhD graduated from the University of National and World Economy with a master's degree in Economic Informatics.

In December 2019 he defended his dissertation "Modeling of Interactions in the System of Personal Data Protection in the Republic of Bulgaria" for the educational and scientific degree "Doctor".

He is a member of the Data Protection, Trust and Security Working Group of the European Telecommunications Network Operators' Association (ETNO) – Brussels.

To contact the author: gsredkovtselkov@abv.bg