Доставка на софтуер - особености и процеси

Тема №3

Технологични ограничения при доставката на софтуер в зависимост от съответната нормативна уредба

Част 1: Регулаторни правила и процеси. Доставка на софтуер и услуги при високи нива на обща регулация – примери

Съдържание

1 Въведение

В тази лекция ще се впуснем в сложния свят на регулациите и технологичните ограничения, които се налагат в софтуерната индустрия на база регулаторните норми, прилагани в различни юрисдикции и индустрии.

Съвременният софтуер е неизменна част от нашето ежедневие, било то в областта на здравеопазването, образованието, финансите, правителствения сектор и други. Той обаче е засегнат от разнообразни регулации, които налагат изисквания, които компаниите трябва да покрият.

Съответствието с тези регулации не е избор за разработчиците на софтуер и организациите, стоящи зад този софтуер. Нарушаването на тези регулаторни изисквания и индустриални норми води до сериозни глоби или санкции. Затова всеки екип, участващ в стадиите на разработка и внедряване на софтуера, трябва да разбира основните изисквания за съответствие и да осъзнава тяхната критичност.

2 Същност на ограниченията

Съгласно дефиницията, технологичните ограничения в нашия контекст се отнасят до всички ограничения, изисквания и правила, които се налагат на софтуерната индустрия чрез регулаторни норми, закони и стандарти, както и тези на ниво организация или продукт, наложени от конкретните изисквания и среда. Те налагат норми върху процеса на разработка, доставка и използване на софтуер.

По своето естество ограниченията, въпреки тяхното различно съдържание и директно техническо влияние, могат да се категоризират с тип на ограничението, на база техническите или нетехническите аспекти, които засягат. Ще разгледаме някои основни категории.

- **Сигурност на софтуера**: Този тип включва множество мерки и техники, предназначени за защита на софтуера от различни заплахи и атаки. Те включват идентификация и коригиране на уязвимости и методи за откриване и предотвратяване на потенциални заплахи.

  Пример: Изисквания свързани с време за отстраняване на идентифицирани уязвимости в зависимост от тяхната оценка.

- **Защита на данните**: Ограниченията, свързани с защитата на данни, се отнасят до правилата и процедурите, които трябва да се спазват при съхранението, обработката и трансфера на данни. Те включват и мерки за предотвратяване на незаконния достъп до тези данни.

  Пример 1: В контекста на медицинските записи, съхранението и обработката на лични здравни данни изисква строги мерки за сигурност и защита.

  Пример 2: Изисквания за криптиране на данни с определени алгоритми и ключове.

- **Контрол на достъпа**: Този вид ограничения дефинират кои потребители или системи имат право на достъп до различни ресурси и функционалности на софтуера. Това включва определяне на роли и права на потребителите и съставяне на мерки за придобиване на ролите, автентикация и оторизация.

  Пример: Изисквания за достъп само на територията на ЕС.

- **Актуализации и поддръжка**: Този вид ограничения включва изискванията за редовни актуализации и поддръжка на софтуера, с цел гарантиране на съответствие и сигурност.

  Пример: Изискване за доставяне на нови версии на строго дефиниран период, регламентирани срокове за поправки и минимални периоди на поддръжка.

- **Съответствие със стандарти и регулации**: Този тип ограничения налага софтуерът да се съобразява със специфични стандарти и регулации, които се изискват в различни сфери. Тези стандарти и регулации са по своето естество колекция от ограничения, които под влияние на бизнеса или правителствения сектор са се превърнали в общоизвестна рамка. Ефективно така преизползваме утвърден списък от ограничения вместо да ги назоваваме индивидуално. Така ако съставяме списък от ограничения, то той би имал дървовидна структура, ако решим да изискаме съответствие със стандарти и регулации.

  Пример: В областта на здравеопазването, софтуерът за електронни медицински записи трябва да отговаря на HIPAA стандарта (Health Insurance Portability and Accountability Act).

- **Докладване и прозрачност**: Този вид ограничения изисква организациите да докладват и да бъдат прозрачни по отношение на начина, по който се използва и обработва информацията в софтуера.

  Пример: Спазването на GDPR изисква организациите да докладват за данните, които събират и обработват, както и да осигуряват на потребителите информация за този процес.

- **Интеграция и съвместимост**: Този вид ограничения се фокусира върху съвместимостта на софтуера с други системи или стандарти, които могат да се изискват в определени индустрии.

  Пример: Софтуерът, използван в банковата индустрия, трябва да бъде съвместим с банковите стандарти за електронни транзакции.

- **Административни и финансови изисквания**: Този вид ограничения включва изисквания, свързани с административни и финансови процедури, необходими за съответствие. Това може да включва лицензиране, такси и други финансови ангажименти.

Пример: Операторите на платформи за хазартни игри трябва да се регистрират и получат лиценз.

- **Интелектуална собственост и патенти**: Този вид ограничения се отнася до защитата на интелектуалната собственост и зачитането на патенти.

  Пример: Разработчиците трябва да проверяват патентната база данни, за да се уверят, че техният софтуер не нарушава патентни права.

- **Етика и корпоративна отговорност**: Този вид ограничения се фокусира върху етичните и социалните аспекти на софтуерната разработка, включително зачитане на правата на потребителите и въпроси за екологична отговорност.

  Пример: Разработчиците на софтуер за следене на потребителите трябва да спазват етични стандарти и правила за поверителност.

- **Ограничения върху оперираща организация**: Този тип ограничения се отнася до изискванията и ограниченията, които се налагат на организацията, която оперира софтуера. Такива ограничения може да са свързани със седалище на компанията, нейния тип, националност на служителите и т.н.

  Пример: Организация, предоставяща cloud решения за правителствения сектор, може да бъде задължена да оперира с местни партньори, съответстващи на определени правила.

3 Източници на ограниченията

Ограниченията при доставката на софтуер могат да произтичат от разнообразни източници, които заедно влияят върху начина, по който софтуерът трябва да бъде разработен и предоставен. Някои от основните източници на тези ограничения включват:

- **Глобални регулации и стандарти:** Софтуерната индустрия се подчинява на глобални регулации и стандарти, които се прилагат в множество региони и индустрии. Тези глобални стандарти налагат разнообразни изисквания, които трябва да бъдат изпълнени при доставката на софтуер. Произтичат от практиката (доказани бизнес практики) или като решения на международни организации.

  Пример: Стандартът ISO/IEC 27017:2015 за информационна сигурност е глобално валиден и не зависи от конкретни индустрии.

- **Национални закони и регулации:** Всяка държава може да има свои национални закони и регулации, които се съотнасят към софтуерната индустрия (било то директно целейки се в нея или не). Тези закони могат да обхващат различни аспекти като авторските права, данъци, лицензиране и дружествена отговорност. Националните регулации създават правила, които трябва да се спазват при предоставянето на софтуерни решения. Това би включило и държаво-подобни организации като ЕС.

  Пример: В медицинската индустрия в САЩ се прилага законът HIPAA (Health Insurance Portability and Accountability Act).

- **Индустриални стандарти и процедури:** Различни индустрии могат да създават свои собствени стандарти и процедури, които се изискват при разработката и доставката на софтуер. Те възникват за конкретните нужди на дадената индустрия и се утвърждават, благодарение на практиката.

  Пример: PCI DSS (Payment Card Industry Data Security Standard) е стандарт за сигурност на данните, който определя изискванията за защита на информацията, свързана с кредитни и дебитни карти, с цел предотвратяване на изтичане и злоупотреба с тази информация.

  Важно е да отбележим, че понякога стандарти в последствие залягат в законодателството, в други случаи пък стандарти възникват на база законодателство.

- **Клиентски изисквания и очаквания:** Нуждите на клиента също са важен източник на ограничения, базирани на стандарти и регулации. Организациите трябва да осигурят, че софтуерните решения, които предлагат на клиентите си, отговарят на изискванията за съответствие на съответните регулации в секторите, в които те действат.

  Пример: Софтуерен продукт, който по своето естество не е направен да работи в сферата на банковото дело, на база масово желание от банковия сектор да го използва, би обмислил съответствие с тези ограничения, с цел спечелване на този пазар.

4 Какво се случва при нарушения?

Когато става дума за нарушения в контекста на регулаторни ограничения се има предвид ситуации, в които организацията или лицето, предоставящи софтуерни решения, не успяват да спазват изискванията и правилата, наложени от регулаторите. Нарушенията могат да имат сериозни последици, включително правни, финансови и репутационни такива.

Нарушенията може да имат различна степен на сериозност. От значение е и наличието на умисъл, и реално настъпилите поражения. Взимайки предвид множество фактори, последиците могат да варират значително. Ето няколко примера:

- **Кибер атаки и изтичане на данни:** Пропуски в сигурността и съответствието при разработката на софтуер могат да доведат до кибер атаки и изтичане на данни. Софтуерът става уязвим, което може да доведе до кражба на информация и други злоупотреби. В резултат на това, финансовите и репутационните загуби могат да достигнат огромни размери до предприемането на действие за ограничаване на щетите.

- **Загуба на репутация и доверие:** Клиентите спират да имат доверие на бизнеса и се обръщат към конкурентите. Техните данни са били изложени на риск, и вероятно са претърпели финансови загуби. Или пък, поради проблем със съответствието и те са имали проблем със съответствието. Каквото и да е станало, клиента вероятно най-малкото е бил изложен на риск. Освен доверието, цялостната репутация на бизнеса в индустрията страда. Особено в информационната ера, където лошата слава се разпространява изключително бързо.

- **Глоби:** Държавни/Федерални агенции/институции, отговарящи за определени регулации и закони, наказват нарушителите, в зависимост от естеството на нарушението. Например, нарушение на HIPAA може да доведе до глоби за над $250,000 за едно нарушение. Друг пример за това е, че през 2020 г. френските органи за защита на данните глобиха Google и Amazon съответно с $120 милиона и $42 милиона за несъответствие с правилата за получаване на съгласие от клиентите преди използване на не-критични бисквитки (non-essential cookies).

- **Съдебни искове:** Те могат да включват граждански и наказателни искове, които могат да доведат до финансови загуби. Клиентите могат да заведат съдебни искове срещу бизнеса поради нарушение на личната им неприкосновеност, загуба на данни и други поражения при нарушение в съответствието. Държавните институции могат да предприемат подобни действия също, където потенциалните последствия може да са още по-сериозни.

- **Банкрут:** Когато бизнесът загуби клиенти, бъде затрупан от множество съдебни искове, похарчи значителни суми за възстановяване на данни и стане ниско продуктивен, трудно може да избегне банкрут.

- **Загуба на лиценз:** Несъответствие с определените правила и стандарти за софтуера може да доведе до лишаване от лиценз.

  Пример: Загуба на лиценз за предоставяне на хазартни игри онлайн на даден национален пазар.

5 Как регулаторните правила се обвързват с процесите?

Регулаторните правила се обвързват с процесите в софтуерната индустрия посредством тяхното прилагане и следене за съответствие. Ето как това става на високо ниво:

1. **Изследване и интерпретация**: Софтуерният доставчик трябва да изследва и тълкува съответните регулаторни правила, които се съотнасят към техния бизнес. Това включва разбиране на изискванията, стандартите и директивите, които трябва да бъдат покрити при доставката на софтуер. От тях се дефинират конкретни изисквания и правила. Може да се подходи по два основни начина - преглед на регулациите и решаване до колко е релевантна всяка една от тях за продукта или пък на база типа на софтуер, търсене на релевантните регулации. На практика, работещо решение би било прагматична комбинация между двете.

2. **Интеграция в процесите**: След като са разбрани регулаторните изисквания, те трябва да бъдат интегрирани в различните процеси на софтуерната дейност. Това включва обновяване на процедурите, методите и корпоративните изисквания, за да се осигури съответствие с регулациите.

3. **Обучение**: Персоналът, работещ в сферата на софтуерната разработка и доставка, трябва да бъде обучен и осведомен за регулаторните правила и тяхното значение. Този процес на обучение помага на екипите да разберат как те могат да спомогнат за съответствието и какви са последствията при пропуски.

4. **Мониторинг и оценка**: След първоначалното постигане на съответствие с регулаторните правила, е важно да се осигури непрекъснато мониторинг и оценка на процесите. Това включва провеждане на вътрешни и външни одити, както и оценка на рисковете. Целта е да не позволяваме да регресираме към липса на съответствие.

5. **Актуализация и промяна**: Софтуерните компании трябва да бъдат готови да актуализират и променят своите процеси, ако регулаторните правила се променят, допълват или възникнат нови. Този процес на постоянно усъвършенстване е ключов за запазването на съответствие.

6. **Докладване и одит**: Когато стане дума за регулаторни одити или докладване, софтуерните компании трябва да бъдат готови да предоставят доказателства за съответствие с регулаторните правила и стандарти. Това включва документация и други данни, които показват степента на съответствие.

6 Какво наричаме "обща регулация"?

Общата регулация представлява комплекс от ограничения и стандарти, които се прилагат върху софтуерната индустрия, както и върху свързани с нея области, като информационните технологии и цифровата сигурност. Тази регулаторна рамка обединява набор от различни изисквания и ограничения, които са насочени към определяне на общи норми, стандарти и насоки за проектиране, разработка, доставка и използване на софтуерни продукти и услуги. Общата регулация има за цел да предостави обширен и надежден набор от инструменти, който може да бъде приложен в различни контексти и индустрии, с цел осигуряване на съответствие със сигурността, качеството, защитата на данните и други критични аспекти на софтуерната дейност.

Такива регулаторни рамки се поставят най-често от различни регулаторни органи и правителствени институции, с цел контрол над индустрията и защита на интересите на потребителите, обществото и националната сигурност.

7 Примери за пазари с висока "обща регулация"

Сега ще разгледаме два примера, демонстриращи регулаторната сложност, която може да произтича от държавните органи и с която трябва да се справим, ако искаме да доставяме софтуерни продукти на конкретен пазар.

7.1 Облачен софтуер в Китайската Народна Република (КНР)

Китай е вторият по големина пазар за облачни услуги в света след Съединените щати и се очаква да продължи да се разраства. Според 14-тия петгодишен план за развитие на дигиталната икономика, публикуван от Китайския държавен съвет, Китай има за цел да развие дигиталната си икономика, която да допринесе с 10% от БВП до 2025 г. Също предвижда и сериозен прогрес в интегрирането на дигиталните технологии с "истинската" (традиционната) икономика. В резултат на това множество

китайски компании проявяват сериозен интерес към дигиталната трансформация. Пандемията от COVID-19 допринася за ускоряването ѝ и увеличава търсенето на облачни услуги, особено в сферите на продуктивността и колаборацията. Много чуждестранни компании вече оперират на китайския пазар, а още планират да го направят, тъй като местните правителства в различни градове привличат чуждестранни облачни компании с преференциални условия.

Въпреки че има множество възможности на пазара, чуждестранните компании, с намерения за навлизане в Китай, се сблъскват със сложни регулации и често изпитват трудности свързани с начина, по който да установят съответствие с правилата и да постигнат търсената възвращаемост от инвестициите си в Китай. Ще разгледаме в обобщен вид този казус и често използваните решения.

7.1.1 Влизане на китайския пазар - регулаторна рамка и изисквания за съответствие

Много услуги, предоставяни в облака, се считат за "телекомуникационни услуги", което е високорегулиран сектор в Китай. Основен въпрос е дали дадена компанията може да предоставя облачни услуги директно от страната си (посредством съществуващата си инфраструктура извън Китай) или трябва да функционира на място в Китай.

7.1.1.1 Предоставяне на облачни услуги отвъд границите на Китай

Много чуждестранни компании искат да използват глобалната си инфраструктура за предоставяне на услуги на клиенти в Китай. Обаче китайското правителство имплементира "портал за сигурност на данните при преминаване на границата" между мрежите на Китай и тези на останалия свят, което може да забави Интернет трафика и достъпа до световния интернет и сървърите извън Китай, съответно качеството на услугата да не може да достигне конкуренти стойности.

Също така, предоставянето на облачно решение включва съхранение на данни на клиенти и понякога дори на лични данни. Законите за сигурност на данните (Data Security Law of the People's Republic of China) и защита на личните данни (Personal Information Protection Law of the People's Republic of China) в Китай, както и другите, специфични за сектора, регулации, допълнително усложняват възможността за прехвърляне на данни при използване на облачно решение извън Китай.

Комерсиално погледнато, ако облачното решение се предоставя отвъд границата на Китай, обикновено бива считано за по-слабо конкурентно от китайските клиенти в сравнение с други решения, предоставяни на място, особено ако клиентите са държавни предприятия. Затова за чуждестранните компании, които се целят в китайския пазар, този модел не е приемлива опция.

7.1.1.2 Предоставяне на облачни услуги на място в Китай

7.1.1.2.1 Изисквания за притежание на лиценз за предоставяне на облачни услуги на територията на Китай

Облачните услуги по своята същност включват използването на Интернет ресурси. Китай регулира множество услуги, които използват Интернет ресурси като вид телекомуникационен бизнес. В случай, че услугата попада в Каталогът за класификация на телекомуникационни услуги (Telecom Service Classification Catalogue), който за напред ще наричаме Каталогът, публикуван от Министерството на индустрията и информационните технологии (MIIT), ще бъде наложено изискване за притежание на лиценз.

Според Каталогът, ако облачната услуга включва "предоставянето на съхранение на данни, среда за разработка на Интернет приложения, внедряване на Интернет приложения, услуги за опериране и управление с помощта на оборудване и ресурси, разположени в центрове за данни (data centers), с функцията на достъп при поискване, употреба според нуждите, разширяемост при поискване и колаборация чрез Интернет или други мрежи", тази услуга се счита за "услуга за сътрудничество посредством Интернет ресурси (IRC)", която е вид услуга с добавена стойност в телекомуникационния бизнес ("VAT service"). Доставчикът на IRC услугата е задължен да получи лиценз за услуги с добавена стойност в телекомуникационния бизнес (VAT Service License), преди да предостави такива услуги.

В този контекст самият термин "IaaS", "PaaS" или "SaaS", използван от доставчика на услуги, не определя конкретната класификация на услугата според Каталогът. Обикновено услугите IaaS и

PaaS вероятно попадат в обхвата на дефиницията за IRC услуга. За SaaS това, което има значение при определянето на приложимостта на конкретно изискване за лиценз, е дали същността(ядрото) на услугата се побира в описанието на Каталогът. Практиката показва, че е възможно някои SaaS услуги да бъдат обхванати от Каталогът и да бъдат предмет на лиценз за услуги с добавена стойност в телекомуникационния бизнес.

7.1.1.2.2 Ограничения за чуждестранни инвестиционни компании за получаване на лиценз за услуги с добавена стойност в телекомуникационния бизнес

Главната юридическа пречка за чуждестранните компании, желаещи да предоставят облачни услуги на територията на Китай, е свързана с ограниченията и забраните, наложени от китайските закони и регулации за получаване на лиценз за услуги с добавена стойност в телекомуникационния бизнес. Например, за IRC услугите, в съответствие с Протокола на Китай за присъединяване към Световната Търговска Организация(CTO) (China's WTO Accession Protocol) и Негативния списък за достъп на чуждестранни инвестиции (Negative List for the Access of Foreign Investment), чуждестранните инвеститори нямат право да инвестират в, и предоставят IRC услуги на територията на Китай и следователно нямат право да получат лиценз за услуги с добавена стойност в телекомуникационния бизнес за IRC услуги.

Има ограничени изключения за инвеститорите от специалните административни региони на Китай, като Хонконг и Макао, които се считат за "чуждестранни инвеститори" за целите на управлението на инвестициите. Споразумението за по-тясно икономическо партньорство (Closer Economic Partnership Arrangement / CEPA) и съответните споразумения и известия не забраняват на "допустими доставчици на услуги" от Хонконг и Макао да създадат предприятие с чуждестранни инвестиции (Foreign Invested Enterprise / FIE), за да предоставят IRC услуги на територията на Китай, при условие че собствеността на доставчик на услуги от Хонконг и Макао в предприятието не надвишава 50%. Трябва да се отбележи, че CEPA също установява редица изисквания за това, какво се счита за "допустим доставчик на услуги". Например се изисква, че обхватът и същината на бизнеса на дружеството от Хонконг/Макао включва IRC услуги, както и да бъде регистрирано и да извършва съществена бизнес дейност за определен период от време.

7.1.2 Възможни модели за предоставяне на услуги

В случай, че облачната услуга не може да бъде предоставена директно от FIE и чуждестранната компания не отговаря на изискванията за достъп на пазара, определени от CEPA, първото важно решение е как да бъде структуриран моделът за предоставяне на услугата, така че да бъде в съответствие с китайското законодателство (това е съществено за изграждането на съответния канал за доставка на фирмата). Практиката показва, че моделите, по които компаниите оперират на територията на Китай, варират в зависимост от обхвата и характера на предоставяните услуги, но винаги се взимат мерки за спазване на приложимите ограничения по отношение на китайските закони и регулации. Въпреки че има предимства и недостатъци при всеки от моделите, най-важното е да се оцени, кой модел най-добре постига бизнес целите на компанията.

7.1.2.1 Модел на напълно чуждестранно дружество (Wholly Foreign-Owned Enterprise / WFOE)

Ако след правна оценка от местен юрист услугите на чуждестранната компания не станат предмет на изисквания за лицензиране, чуждестранната компания може да учреди напълно чуждестранно дружество (WFOE) на територията на Китай и да предлага услугите/решението директно. Въпреки че може да няма бариери при влизане на пазара за чуждестранната компания, винаги може да има други регулаторни изисквания (като тези, свързани с рекламата, данните, мрежовата сигурност, домейн името, криптирането и съдържанието), които да се прилагат към нейната дейност на територията на Китай.

7.1.2.2 Модел с местен партньор

На територията на Китай обичайната практика за предоставяне на услуги с изисквания за лицензиране, е съвместно действие с лицензиран местен партньор. Този модел се използва широко от някои от технологичните гиганти, за предоставяне на облачни услуги, които изискват лиценз за услуги с

добавена стойност в телекомуникационния бизнес. Подходът е считан за най-приемлив от регулаторите в Китай. По този модел чуждестранната компания сключва сътрудническо споразумение с местен партньор, който разполага с лиценз, отговарящ на изискванията, и предоставя необходимите технологични лицензи на местния партньор. След това местният партньор сключва договори с крайни клиенти в Китай и оперира, предоставя и управлява услугите, като заплаща на чуждестранната компания такси или хонорари.

7.1.2.3 Модел на дружества с променлив капитал (Variable Interest Entity / VIE)

Схемата на дружества с променлив капитал (VIE) се използва обикновено като бизнес модел за чуждестранните компании, които искат да инвестират в сектори, в които китайските закони и регулации ограничават директните чуждестранни инвестиции. Под тази схема чуждестранната компания учреждава напълно контролирано дружество в Китай (например, WFOE или частично контролирана китайска компания), което управлява друго предприятие, което притежава необходимите лицензи за предоставяне на съответната услуга. Макар че тази схема е използвана широко през последните години, със затягането на регулациите в сектора на телекомуникациите и Интернет, моделът на VIE става все по-непопулярен и се сблъсква със значителни рискове за съответствие.

7.1.2.4 Модел на разпространение под on-premise форма

Докато някои чуждестранни компании избират да реорганизират организацията си или да си сътрудничат с местни партньори, други в крайна сметка модифицират услугите си и създават локален бизнес в Китай, който се различава малко от глобалното им предложение. Има чуждестранни компании, които решават да предлагат своите продукти или услуги като on-premise софтуер чрез упълномощени дистрибутори в Китай, за да се съобразят с приложимото китайско законодателство. По този модел, китайските крайни потребители получават лиценз за решението директно от чуждестранната компания и след това избират да внедрят решението на китайски облак или собствена инфраструктура по свое усмотрение.

7.1.3 Съображения за компанията-доставчик

Несъмнено, ако облачната услуга/решение, предоставяна от чуждестранна компания, подлежи на изисквания за лицензиране съгласно китайското законодателство, най-сигурният начин за влизане на китайския пазар е да намерите подходящ местен партньор. Тази съвместна работа не е лесна по никакъв начин:

- Стратегически, чуждестранната компания трябва да намери подходящ местен партньор, като вземе под внимание фактори като мащаба на партньора, структурата на акционерите, позицията на пазара, правителствените ресурси и други.
- От комерсиална гледна точка, чуждестранната компания трябва да обмисли стратегия за марката (branding) и ценообразуване, такси и структура за споделяне на печалби и други.
- Правно, чуждестранната компания и местният партньор трябва ясно да определят отговорностите и ролите на всяка от страните.

Фокусът при проектиране на тези договорености трябва да бъде, да се гарантира, че сътрудничеството няма да надвишава никакви правни или регулаторни ограничения, в противен случай то може да се разглежда като "незаконно отдаване или прехвърляне на лицензите за телекомуникации по маскиран начин" и може да доведе до неблагоприятни последици. С оглед на бързо развиващия се регулаторен климат в Китай, чуждестранната компания трябва също така да следи актуалните законодателни актуализации и най-добрите практики на пазара, за да вземе информирано решение относно инвестицията си в Китай.

7.2 Софтуер, използван от правителствения сектор в САЩ

Традиционно софтуерът, използван за нуждите на правителствения сектор подлежи на огромно количество разнообразни регулации. Правителственият сектор на САЩ е един от най-големите потребители на софтуер, разполагащ с доста сериозен бюджет за целта. Това го прави много

привлекателен за софтуерните компании. Но за да спечелят поръчка от американското правителство (или по-точно агенции в него), необходимите регулации трябва да са покрити. Ще разгледаме някои основни изисквания с уточнението, че не търсим изчерпателност.

7.2.1 OMB Меморандум M-22-18 и M-23-16 (изискване за добри практики при разработката на софтуер, отнасящи се до сигурността)

OMB (Офис за управление и бюджет) издава меморандум M-22-18 (и M-23-16, който го потвърждава) с нови изисквания за сигурност, налагайки на федералните агенции да се уверят, че всички софтуерни продукти от трети страни (тоест от компании-доставчици на софтуер), които използват, отговарят на стандартите за сигурност при разработката на софтуер и насоките, издадени от Националния институт за стандарти и технологии (NIST).

Правилата, които имат за цел да подобрят сигурността във веригата за доставка на софтуер на федералното правителство на САЩ, са част от усилията за киберсигурност и сигурност на доставките. Те изискват разработчиците на софтуер да потвърдят съответствие с насоките на NIST за сигурност при разработката на софтуер.

7.2.1.1 Значение на правилата

Правилата изискват от разработчиците на софтуери да оценяват и потвърждават, че техните практики за разработка се придържат към насоките на NIST, които се актуализират редовно и се съдържат в рамката за сигурно разработване на софтуер (Secure Software Development Framework) и Насоките за сигурност при доставката на софтуер (Software Supply Chain Security Guidance). По своята същност, документите съдържат практически насоки и рамки, които разработчиците могат да използват, за да подобрят сигурността на своя софтуер. В крайна сметка, насоките насърчават разработчиците да използват базиран на оценка на риска подход към разработката на софтуер, който е адаптиран към техния конкретен софтуер и среда за разработка.

7.2.1.2 Обхват на "Софтуер"

Обширната дефиниция на "софтуер", използвана от OMB в правилата, означава, че много организации, които си партнират с правителството на САЩ, ще бъдат засегнати. Например, софтуерът включва "фърмуер, операционни системи, приложения и услуги (например, облачен софтуер), както и продукти, съдържащи софтуер". По тази дефиниция, всички продукти, съдържащи софтуер, вероятно са предмет на този вид самооценка. В определени случаи, където организацията не разработва основната софтуерна част, като например базова библиотека с отворен код, може да се използва оценка от трета страна на софтуера вместо самооценката.

7.2.1.3 Рискове при несъответствие

Федералните агенции са задължени да търсят самооценки за софтуера, който използват в момента и в бъдеще. Несъответствието може да означава, че разработчиците рискуват да не могат да предоставят своя софтуер на федералното правителство. Очаква се, че правилата ще бъдат интегрирани или допълнени към развиващите се изисквания за сертификация на киберсигурност на Министерството на отбраната на САЩ.

Също така, лъжливата самооценка може да доведе до наказателна отговорност съгласно Закона за неверни твърдения (False Claims Act).

7.2.2 OMB Меморандум M-21-07 (преход към IPv6)

На 19 ноември 2020 г., OMB (Офис за управление и бюджет) издава Меморандум M-21-07, с който се налага на всички федерални агенции да прекратят използването на IPv4 и да преминат към IPv6.

За да улесни тази промяна в рамките на Министерството на отбраната (DoD), на 29 юни 2021 г. DoD издава заповед, с която се осигурява, че "всички нови мрежови информационни системи на DoD, използващи IP технологии, ще използват IPv6 преди внедряването и оперативната употреба до края на 2023 г." и предоставя постъпков план за пълна имплементация на IPv6 до края на 2025 г., подобно на този, съдържащ се в OMB меморандумът. Информационни системи, използващи

IPv6, са системи, в които IPv6 е "включен" за употреба в реална среда. Според заповедта на DoD, Изпълнителният комитет за цифрово модернизиране на инфраструктурата (DMI EXCOM) ще служи за управление и осъществяване на усилията по преход към IPv6 на ниво DoD, също така поемайки ролята на ръководител на проекта.

Планът за имплементация на IPv6 на DoD включва инкрементални milestones от 20%, 50% и 80% на активите, върху федералните мрежи, работещи само с IPv6, до края на фискалните години 2023, 2024 и 2025. Освен това, DoD ще извади от употреба системите, които не могат да преминат към IPv6.

Общата цел на задълженията относно IPv6 е да осигури, че всички федерални информационни системи и услуги ще преминат към IPv6 до края на 2025 г.

7.2.3 Изисквания за облачните услуги използвани от федералните агенции - FedRAMP

FedRAMP е програма на правителството за акредитиране на облачни услуги за използване от агенции на САЩ и DoD. Нейната цел е да обхване сигурността в облачните услуги в целия правителствен сектор, като предостави стандартизиран подход към оценката на сигурността, одобрението и непрекъснатото наблюдение на облачните технологии. Програмата се управлява от Агенцията за обществени услуги (GSA) - Управление на програмата FedRAMP (PMO). Всяка облачна услуга

- софтуер като услуга (SaaS)
- платформа като услуга (PaaS)
- инфраструктура като услуга (IaaS),

трябва да получи одобрение преди да бъде използвана от агенция на правителството на САЩ. В тема 4 от курса ще обърнем специално внимание на този стандарт.

7.2.4 Множество други закони и стандарти

Гореспоменатият Национален институт за стандарти и технологии (NIST) разработва и множество други стандарти, които правителствения сектор може да изиска. FIPS е такъв пример, налагащ изисквания върху обработката на данни.

Също така правителственият сектор трябва да използва софтуер, който може да отчита и докладва за използването на данни и ресурси. Този вид софтуер трябва да спомага за осигуряване на прозрачността на дейностите на правителството и за съблюдаване на законите за свободен достъп до информацията (Freedom of Information Act).

И това са само някои от примерите. Правителственият сектор в САЩ е доста силно регулиран и постоянно регулаторната рамка подлежи на еволюция. Също така в зависимост от по-конкретните подсектори в него, приложимата регулация е възможно да се допълни.

8 Заключение

Софтуерната индустрия е от изключително значение за функционирането на модерния свят. В резултат на това има огромен интерес към регулирането и контрола на софтуера, с цел постигане на необходимите качества и съответствие с различни закони. В резултат на тези дейности, върху софтуерът се налагат множество технически и нетехнически ограничения. Тези ограничения имат разнообразни източници и могат да се комбинират в регулаторни рамки и утвърдени стандарти. Често се случва (особено по инициатива на правителствата по света) да се разработват изключително сложни и всеобхватни регулаторни рамки, затрудняващи сериозно постигането на съответствие на софтуерните продукти с тях, без юридическа помощ. Въпреки това, тази инвестиция често си заслужава поради важността на пазарите, които въпросните рамки обхващат.