Тема 9

Архивиране (Back Up) и Възстановяване (Recovery)

Увод

- В много случаи дори и на най-големите организации с необходимия квалифициран персонал, политики и процедури за сигурност, мерки и т.н. се случва бедствието.
- Осъществена е успешна атака върху информационните системи, в някои случаи са откраднати данни, друг път се спрени самите информационни услуги.
- Много важно за хората в личен план и организациите е как ще реагират в такива ситуации, имат ли копия на данните, могат ли да възстановят услугите в най-кратки срокове и др.
- Тези процеси са известни като ***Disaster recovery***, като основна роля играят т.нар. ***Back Up - архиви.***

Основни понятия

- ***Disaster*** - бедствие се определя обикновено, като а) "внезапно, непредвидено събитие, което води до големи щети или загуби „ или б)" всяко събитие, което създава невъзможност на дадена организация да осигури критичните бизнес функции за определен период от време".
- ***Disaster recovery*** - е набор от политики и процедури, които да позволят възстановяването или продължаването на работата на технологичната инфраструктура и информационните системи след природно или предизвикано от човека бедствие.
- ***Backup*** – е процес на копиране и архивиране на данните на една организация с цел осигуряване на източник за възстановяване след настъпило бедствие.
- ***Business Continuity Planning*** - включва възстановяване след бедствие заедно с процедурите за възстановяване на бизнес операциите и на функционалността на бизнес инфраструктурата.

Disaster recovery

- Без съмнение почти всяка организация с развита информационна инфраструктура и услуги се сблъсква със ситуация на пробив, отказ на системите, природни бедствия и други ситуации, които нарушават нормалната работа.
- За по-лесното преодоляване на тези ситуации организациите следва да имат наличен план за действие, който се нарича **disaster recovery plan** или DRP.
- DRP представлява набор от документи и процедури описващи процеса на защита и възстановяване на информационната инфраструктура, данни и услуги.
- Планът трябва да засяга времето **преди, по време и след бедствието**.

Disaster recovery plan

Планът за възстановяване след бедствие трябва да отговаря на следните основни въпроси:

1. Как обектите на атаката да бъдат изолирани от незасегнатите и как да се ограничи атаката от разпространение?
2. По какъв начин бизнес функциите и услугите да останат достъпни за потребителите?
3. Как увредените или унищожени обекти да бъдат възстановени след края на атаката?

Изготвя се на хартия и в цифров вид и се разпространява сред всички засегнати, включително и сред партньори.

Цели на DRP

- защита на организацията от отказ на основни системи;
- ефективна координация на всички ангажирани в процеса на реакция и възстановяване;
- свеждане до минимум на риска за организацията от закъснения в предоставянето на услуги;
- гарантиране на надеждността на системите в състояние stand by чрез тестване и симулация;
- свеждане до минимум на необходимостта за вземане на решения от страна на персонала по време на бедствие.

Какво съдържа планът

1. Дефиниране на ключовите активи и потенциалните заплахи.

- В началото следва да се идентифицират ключовите активи на организацията и какво е въздействието, ако се изгуби този актив. С други думи да се изясни какво трябва да се защити и колко е важно за организацията. Примери за такива активи са: счетоводната ИС, имейл сървъра, файлове, спецификации на продукти, договори, всякакви архиви с документи и др.
- На следващо място се идентифицират потенциалните заплахи за активите. Заплахите могат да бъдат, както природни бедствия (земетресения, пожари, наводнения и т.н.), така и резултати от човешки действия (кражба, хардуерни и софтуерни прекъсвания, компютърни вируси и др.)
- На базата на идентифицираните активи и заплахи могат да се дефинират и сценарии за реакция в зависимост от различните активи и заплахи.

Какво съдържа планът? (прод.)

2. Дефиниране на времена за възстановяване.

За всеки актив трябва да се определи максималното време за което този актив следва да се възстанови. За някои активи това време може да бъде няколко часа, за други няколко дни, затова и защото цената като загуби за организацията може да бъде голяма за дългите периоди, тази информация е много важна.

3. Дефиниране на решения за възстановяване.

На базата на първите две стъпки се изготвят стратегии и решения за всяка ситуация. Например, ако е засегнат сайтът на организацията за електронна търговия възможно решение може да бъде преместването на друг хост, а ако е засегната базата от данни то да бъде възстановена, чрез резервно копие или т.нар. реплика.

Какво съдържа планът? (прод.)

4. Събиране на данни. На тази стъпка се събира цялата необходима информация за плана в действия. Такава информация може да бъде: списъци с телефонни номера на отговорните лица, местоположението на файлове с резервни копия, списъци за известяване на администратори или др., местоположение на хардуер и софтуер, на застрахователни документи, на офис оборудване или средства за комуникация.
5. Оформяне и документиране. Тук се извършва фактическото изготвяне на плана. Оформят се документите, присъединяват се вече направените по другите стъпки списъци, таблици, документи и др. Изготвят се документи за съгласуване и одобрение.
6. Утвърждаване. Съответните отдели и ръководни органи утвърждават плана и го официализират.
7. Провеждане на обучения и тренировки.

Примерен шаблон

- https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf
- https://www.smartsheet.com/disaster-recovery-templates
- http://templatelab.com/disaster-recovery-plan/

Тестване на плана

- За да бъде плана ефективен и да работи както се очаква е необходимо на определен период да се тества.
- Следва да се направи преглед на плана, да се допитат служителите за предложения и да се направят необходимите промени.
- Необходимо е и плана да се тества в хипотетична ситуация на бедствие нарича се DR Drill Tests и да се проследят реалните действия на служителите и отговорните лица.
- Препоръката е да се прави на половин година.

Back Up (архивиране, резервни копия)

- Един от най-полезните методи при възстановяване след бедствие е използването на т.нар. резервни копия на информацията.
- Те представляват съхранена (архивирана) на определен момент във времето информация(данни) от дадена информационна система.
- Системата може да бъде: за електронна поща или е-търговия, база от данни, папки и файлове и други.
- Информацията, която се съхранява е както цифрови данни, така и системни настройки, конфигурация на инсталиран софтуер и хардуер и др.

. . .

- Съхраняването на информацията може да бъде реализирано по два начина: офлайн или онлайн.
- При **офлайн** режим се използва някакво устройство локално. Процесът е много кратък и защитата на информацията е на високо ниво. Съществува риск от загуба на информация, ако устройството за бекъп се повреди.
- При **онлайн** се използва облачна или интернет базирана услуга. Характеризира се с по-голямо време за съхранение, възможни са и рискове за сигурността.
- От съществено значение е и интервалът на съхраняване на информацията. Може да бъде на часове, дневно, седмично или произволен. Колкото интервалът е по-кратък, толкова риска от загуба на информация е по-малък.

Стратегии

Методът 3-2-1

- 3 - съхраняват се 3 копия за всеки важен файл: 1 основен/работен и 2 backup-а.
- 2 – съхраняване върху 2 различни типа устройства - напр. диск и NAS(Network-attached storage).
- 1 – съхраняване на 1 copy извън системата/организацията (напр. клауд или друга сграда).

Стратегии

Честота на архивиране

- В зависимост от естеството на данните
- Например:

➢ сървърният системен дял/диск да се архивира веднъж на един месец и да се съхранява от половин до една година

➢ работните данни/БД всеки работен ден и всеки дневен архив да се съхранява между 3 и 5 цикъла

Традиционни методи

- В традиционния процес на архивиране, данните се копират на носител, главно дискове – SSD, магнитни или оптични или лента(в близкото минало), в предвидим и подреден начин за сигурно съхранение, както на място или извън организацията.
- Носителят по този начин може да се направи достъпен за възстановяване на данни за нови или възстановени след срив системи.
- Освен данните, архивът може да се използва от съвременните операционни системи и за архивиране на конфигурациите и на потребителски приложения.
- Това осигурява по-бързо възстановяване на системите и често това е единственият начин за възстановяване на системи, където приложенията, които поддържат данни са тясно интегрирани със системата.

Видове архивиране

- **Пълно (Full)**: архивират се всички данни, независимо дали или не са се променили от последния процес на архивиране. Определението на пълен архив варира за различни системи. На някои системи пълно резервно копие включва критични файлове на операционната система, необходими за напълно възстановяване на системата, но на други системи се архивират само данните на потребителите.
- **Копие (Copy):** данните се копират от един диск на друг.
- **Прогресивно (Incremental)**: при всяко архивиране към архива се добавят само новите или променените данни.
- **Диференциално (Differential):** при всяко архивиране към архива се добавят само новите или променените данни, но към момента на пълно архивиране.

Предимства и недостатъци на пълното архивиране

Предимства:

- Всички файлове от избраните устройства и папки се архивират до един бекъп сет.
- В случай, че се наложи да се възстановят файлове, те лесно се възстановява от единния бекъп сет.

Недостатъци:

- Пълното архивиране отнема повече време, отколкото други методи за архивиране.
- Пълни резервни копия изискват повече пространство на твърд диск, оптичен диск или мрежов диск.

Предимства и недостатъци на прогресивното архивиране

Предимства:

- Времето е по-кратко, отколкото пълните архиви. Изисква по-малко пространство на диск, оптичен диск или мрежов диск.
- Може да се запазят няколко версии на едни и същи файлове на различни архивни масиви.

Недостатъци:

- За да се възстановят всички файлове, трябва да има всички архиви на разположение.
- Отнема повече време да се възстанови определен файл, тъй като трябва да се намери повече от един бекъп сет и да се намери най-новата версия на дадения файл.

Предимства и недостатъци на диференциалното архивиране

Предимства:

- Времето е още по-кратко, отколкото при пълното и прогресивното архивиране.
- Изисква много малко пространство на диск, оптичен диск или мрежов диск.

Недостатъци:

- Възстановяването на всички файлове може да отнеме значително по-дълго време, тъй като може да се наложи да се възстанови, както последната разлика, така и пълния архив.
- Възстановяването на индивидуален файл може да отнеме повече време, тъй като, за да се намери файла се търси и на диференциалния и на пълния архив.

Съвременни методи

- **Hierarchical storage management** (**HSM**) е метод за съхранение, при който данните автоматично се преместват от един носител на друг. Например данните, които се използват много интензивно се съхраняват на solid state drive дискове, а тези които се използват рядко на твърди дискове или оптични носители. Прил. при ОС Oracle Solaris, HP-UX и други Linux дистрибуции.
- **Shadow Copy** е технология използвана в Windows системите за архивиране на данни дори и да се използват в момента на архивиране. Предимството на метода се състои в това, че дори и данните да се променят в момента на архивиране, то промените ще се запазят в архива.
- **Online backup** е онлайн услуга, която автоматично и редовно се свързва с хост или хостове и прави копия на определени данни на онлайн сървър. Могат да бъдат направени резервни копия на всичко - само на потребителски данни, или на конкретни набори от данни.
- **Storage area network (SAN)** е метод за свързване на отдалечени(в локална мрежа) компютърни запаметяващи устройства (твърди дискове, др. устройства) към сървърите по начин, при който за операционната система тези устройства изглеждат локално свързани, но не са достъпни от други устройства в локалната мрежа.

Възстановяване (Recovery)

- Преди пристъпване към този етап следва да се отстранят всякакви причини, последствия и др., довели до бедствието.
- Процесът на възвръщане на оперативното състояние на системите и данните до това преди бедствието.
- Може да отнеме както много кратко, така и по-продължително време.
- При правилно построен план възстановяването може да бъде и пълно.
- В противен случай може да се стигне до загуба на данни.
- Преди пристъпване към възстановяване е препоръчително да се тестват данните в архива за цялостност, актуалност и надеждност(например за зловреден код)

• • •

- Архивните копия трябва периодично да се тестват за това дали са способни да възстановят данните коректно
- Възстановяването може да се извършва ръчно или автоматично
- Това зависи от възможностите на информационните системи, СУБД или ОС
- След възстановяване също трябва да се проведат цялостни тестове на системите и да се инсталират последните патчове за сигурност

Заключение

- Избягването на проблемни моменти при функционирането на информационната инфраструктура е невъзможно
- Затова е много важно отделния човек или организацията да бъдат подготвени за такива ситуации
- В зависимост от мащаба могат да се прилагат единични или комплексни адекватни мерки при настъпване на бедствие в зависимост от планирането на ранен етап
- Архивирането на данни е отлична мярка в такива ситуации

Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата понятия, дефиниции и аспекти. Търсенето може да направите и на чужди езици, които владеете.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Проучете устройствата с които разполагате какви възможности за архивиране и възстановяване разполагат.
- Определете информацията, която е нужно да запазите сигурно и направете архивни копия.