Өгөгдлийн сангийн аюулгүй байдал

Өгөгдлийн сангийн аюулгүй байдал : Санаатай болон санамсаргүй аюулаас өгөгдлийн санг хамгаалах механизм юм.

Аюулгүй байдлын асуудал нь дан ганц өгөгдлийн санд дахь өгөгдөлд хамаардаггүй :

Аюулгүй байдлын цоорхой нь системийн бусад хэсэг болон өгөгдлийн санд ч нөлөөлж болно.Иймд өгөгдлийн сангийн аюулгүй байдалд тоног төхөөрөмж , програм хангамж , хүмүүс , өгөгдлийн сан багтдаг. Аюулгүй байдлыг үр дүнтэйгээр хэрэгжүүлэхийн тулд зохих хяналт , системд тодорхой үүрэг зорилтуудыг тодорхойлсон байхыг шаарддаг. Аюулгүй байдлын энэ хэрэгцээг өмнө нь ихэнхдээ байгуулгууд үл тоогдог байсан бол одоо хүлээн зөвшөөрч сайжруулж байна.

Байгуулгын чухал өгөгдлийн сан зохих хяналтын дагуу хамгаалагдсан байх ёстой. Өгөгдлийн сангийн аюулгүй байдалтай холбоотой анхаарах зүйлс :

* Хулгай ба залилан
* Нууцлалын алдагдах
* Хувийн мэдээлэл алдагдах
* Бүрэн бүтэн байдал алдагдах
* Бэлэн байдал алдагдах

Эдгээр нөхцөл байдлууд нь хохирол болон гэмтэлд өртөх боломж буюу эрсдлийг буруулахыг байгуулагууд эрэлхийлэх хэрэгтэй тэр салбарууд өргөнөөр эзэлдэг байна. Зарим нөхцөл байдалд эдгээр салбарууд нь нэг салбарт хохирол учруулдаг нэг үйл ажилгаа нь магадгүй бусдад нь мөн хохирол учруулдаг тийм нарийн холбоотой юм. Үүнээс гадна залилан болон хувийн мэдээлэл алдагдал нь санаатай болон санамсаргүйгээр ч гарч болох үйлдэл бөгөөд мэдээллийн санд эсвэл систем гарсан өөрчлөлт хийгдэх бүрт заавал мэдээлэлж байна. Хулгай ба залилан нь зөвхөн мэдээллийн санд төдийгүй байгуулгад нөлөөлдөг. Ийм үйл ажилгааг хүмүүс үйлддэг учраас энэ боломжийг үүсгэхгүй байхад анхаарах хэрэгтэй. Хулгай болон залилангын мэдээллийг хэрэгцээгүйгээр өөрчлөх үйл ажилгааны үр дүн нууц эсвэл хувийн мэдээлэл алдагдана. Дутуу эсвэл гэмтсэн өгөгдлөөс өгөгдлийн бүрэн бүтэн байдал алдагдснаар байгуулгын ажилгаанд ноцтой нөлөөлж болно. Байгуулгууд 24/7 буюу тасралтгүй ажиллагааг эрилхийлж байна.(өдрийн 24 цаг , 7 хоногын 7 өдөр ) Өгөгдөл эсвэл системийн бэлэн байдал алдагдах нь байгуулгад санхүүд ноцтой нөлөөлж болно.Зарим тохиолдолд өгөгдлийн эвдрэл нь системийг ажилгааггүй болгож болно. Бэлэн байдал алдахдах гэдэг нь байгуулгын санхүүгийн гүйцэтгэлд ноцтойгоор нөлөөлж болох өгөгдөл , систем эсвэл хоёуланд хандаж чадахгүй байх явдал юм.Зарим тохиолдолд системийг ашиггүй байдалд хүргэдэг хэрэг явдлууд нь мөн магадгүй өгөгдлийг эвдрэлд хүргэж болох юм.Сүүлийн үед компьютерт суурилсан гэмт хэргийн үйл ажилгаа нэлээд өссөн ба дараагийн хэдэн жилүүдэд өсөлт нь үргэлжилэх урьдчилсан таамаг байна.

Аюул занал – Системд болон эцэст нь байгууллагад сөргөөр нөлөөлж болох ямар нэгэн санаатай болон санамсаргүй нөхцөл байдал буюу хэрэг явдал юм.

Байгууллагад хохирол учируулж болзошгүй хүн , үйл ажилгаа эсвэл нөхцөл байдалыг хамруулдаг хэрэг явдал нь аюул заналыг бий болгож болох юм. Хор хорхирол нь техник хангамж , програм хангамж өмн өгөгдлийн алдагдал гэх мэт мэдэгдэхүйц байж болно. Байгууллагын нүүр тулж буй асуудал нь бүх боломжит аюул заналыг илэрүүлэх юм.Тийм учраас наад зах нь тухайн байгууллага хамгийн ноцтой аюул заналыг тодорхойлоход цаг хугацаа , хүчин чармайлтаа гаргах хэрэгтэй .Өмнөх бүлэгт бид санаатай болон санамсаргүй үйл ажиллагаанаас үүдэлтэй алдагдалтай салбаруудыг тодорхойлсон. Зарим төрлийн аюул занал санаатай болон санамсаргүй байж болох ч үр дагавар нь хэвээрээ байна.Санаатай аюул заналхийлэл нь хүмүүстэй хамаатай ба байгууллагаас гадны хүн байж болох зөвшөөрөлгүй хэрэглэгчид болон эрх бүхий хэрэглэгчи аль аль нь үйлдэж болзошгүй юм.Ямар ч аюул заналыг хэрвээ амжиллттай болвол тодорхой нөлөө үзүүлэх аюулгүй байдлын болонжит цоорхой гэж үздэг. Хор нөлөө үзүүлж болох салбарын дор жагсаасан тул аюул заналын янз бүрийн төрлийн жишээг харуулж байна. Жишээ нь : Зөвшөөрөгдөөгүй өгөгдлийг аюул занал гэж үзээд илрүүлэх нь байгууллагын хувьд хувийн болон нууц хадгалах байдлын алдагдал , хулгай болон луйвард хүргэдэг байна.

Хариу арга хэмжээ /Компьютерт суурьласан хяналт/

Эрх олгох / authorization / : Тухайн зүйлийг олгох эрх буюу давуу эрх нь хууль ёсны хандах эрхтэй систем юм уу системийн обьеттэй байна.

Бататгал/ Authentication / : хэрэглэгч нь хэн болохыг тодорхойлох механизм

Хандалтыг хянах / access controls / : Өгөгдлийн сангийн системд хандалтын хяналтыг хангах нийтлэг арга зам нь эрх олгох , давуу эрхийг хүчингүй болгох юм.

Давуу эрх /privilege / : Давуу эрх нь үүсгэх эсвэл хандалт(унших , бичих , өөрчлөх) зарим өгөгдлийн санг(тухайлбал : холбоо , харагдац , индекс ) эсвэл DBMS-н тодорхой хэрэгслүүдийг ашиглах боломжийг олгодог.

Харагдац / views / : Харагдац бол нэг эсвэл олон харилцаан дээр оператор үйл ажилгагаа явуулж динамик үр дүн авдаг

Нөөц / backup / : Тогтмол хугацаанд өгөгдлийн сангийн хуулбар болон бүртгэлийн файлыг офлайн агуулахд хадгалах үйл явц юм.

Тэмдэглэл / Journaling / : Гэмтэл гарсан тохиолдолд өгөгдлийн сангийн бүх өөрчлөлтийг бүртгэлийн файлд (тэмдэглэлд) бичиж хадгалан , сэргээх үйл явц юм.

Бүрэн бүтэн байдал / integrity / :

Нууцлал / encryption / : Өгөгдлийг онцгой алгоритм ашиглан шифрлэлтийг буцаах түлхүүргүйгээр ямар ч програмд өгөдлийг уншигдахгүй болгоно

Майкрософт оффис ӨСМС хандалт болон Ораклийн ӨСМС (өгөгдлийн сангийн менежмент систем) нь системийн аюулгүй байдал болон өгөгдлийн аюулгүй байдал гэх аюулгүй байдлын хэмжигдэхүүний 2 хоёр төрлийг санал болгодог . Системийн аюулгүй байдал нь өгөгдлийн санг нээх нууц үгийн тохиргоог тааруулах мөн хэрэглэгч зөвхөн унших, өөрчлөх л боломжтой байх гэх мэтээр өгөгдлийн сангийн хэсгүүдэд тодорхой хязгаарлалтуудыг тавьж хэрэглэгчийн түвшинд өгөгдлийн аюулгүй байдлыг хангах.

Аюулгүй байдлын хэмжигдэхүүн нь Вэб дээрх ӨСМС-тэй уялдаатай байдаг энэ нь : итгэмжлэгдсэн серверүүд, галт хана, зурвас эмхэтгэх алгоритм болон тоон гарын үсэг, тоон сертификат, керберос, Аюулгүйн соккет давхарга (SSL) мөн Аюулгүйн HTTP (S-HTTP), Аюулгүйн Электрон Гүйлгээ (SET), Аюулгүйн Гүйлгээний Технологи (SST), Жава аюулгүй байдал болон АктивИкс аюулгүй байдал зэргийг багтаадаг

DBMS ба Вэбийн аюулгүй байдал

Интернэт холбооны үндсэн протокол гэж TCP / IP дээр тулгуурладаг. Гэсэн хэдий ч TCP / IP болон HTTP аюулгүй байдлыг хангах зорилготой зохиогдоогүй . Тусгай програм хангамжгүй бол интернэтийн урсгалыг хэнч уншиж бас хянаж чадна.

* Интернэтээр мэдээлэл авах болон дамжуулахад дарааах сорилыг хангана :
* Илгээгч ба хүлээн авагчаас өөр хэнч халдашгүй (Хувийн нууц /privacy/ )
* Дамжуулах явцад өөрчлөгдөхгүй (Бүрэн бүтэн байдал /integrity/ )
* Хүлээн авагч илгээгчээс ирсэнд итгэлтэй байж чадна (Үнэн зөв байдал/authenticity/ )
* Илгээгч хүлээн авагчд итгэлтэй байж чадна (Дуураймал биш /non-fabrication/ )
* Илгээгч нь явуулчихсангаа үгүйсгэж чадахгүй байгаа (Татгалзалгүй/non-repudiation/)

Гэсэн хэдий ч , Гүйлгээг хамгаалах нь асуудлын хэсгийг шийдэх цор ганц шийдэл юм. Нэгэнт мэдээлэл вэб сэрвэрт хүрсэн бол хамгаалагдсан байх ёстой.Өнөөдөр ийм архитектурын ихэнх хэсэг нь баталгаажсан байдаг , гэхдээ энэ нь ерөнхийдөө янз бүрийн бүтээгдэхүүн, механизмыг шаарддаг. Вэб орчинд авч үзэх ёстой аюулгүй байдлын өөр нэг асуудал хэрэглэгчийн машинруу дамжуулагдаж мэдээлэлийн утга юм. Жишээ : HTML хуудас ActiveX хяналтыг агуулж болно , JavaScript / VBScript , эсвэл нэг буюу хэд хэдэн Java апплет. Дараах хортой үйлдэлийг хийх боломжтой ба урьдчилан сэргийлэх арга хэмжээ авах хэрэгтэй :

* + Бохир өгөгдөл эсвэл программын ажиллах бүтэц
  + Бүтэн дискнүүдийг дахин форматлах
  + Бүх системийг унтраах
  + Нууц үг , файл , нууц мэдээлэл татаж авах болон цуглуулах
  + Хэрэглэгчийн дүрд тоглон хэрэглэгчийн компьютерийн сүлжээгээр хууль бусаар эзлэх довтлох
  + Ялангуяа аюулгүй боловч гаралтын төхөөрөмжинд зохисгүй нөлөө үзүүлдэг

Прокси сервер / Proxy Servers /

Вэб орчинд нь прокси сервер нь Вэб браузер болон вэб серверийн хооронд суудаг компьютер юм. Энэ хүсэлтийг нь өөрөө биелүүлж чадах эсэхийг тодорхойлохын тулд вэб сервер нь бүх хүсэлтийг ялгадаг. Хэрэв тийм биш бол, энэ нь Вэб сервер рүү хүсэлтийг дамжуулдаг. Прокси сервер хоёр гол зорилготой юм : хүсэлт шүүх ба үйл ажилгааг сайжруулах

Галт хананууд / Firewalls /

Галт хана нь зөвшөөрөлгүй хандалт эсвэл хувийн сүлжээнээс сэргийлэх зорилготой. Галт хана тоног төхөөрөмж болон програм хангамж эсвэл аль алиныг нь хослуулан хэрэгжүүлж чадна. Интернэтэд холбогдсон хувийн сүлжээнд зөвшөөрөлгүй хэрэглэгчид нэвтрэхээс урьдчилан сэргийлэх тулд ашиглаж байна. Галт хана хэд хэдэн төрөл байдаг :

Пакет шүүлт / Packet filter / :

Програмын гарц / Application gateway / : Тодорхой програмууд FTP болон Telnet гэх мэт аюулгүй байдлын механизмыг хэрэглэнэ. Энэ нь маш үр дүнтэй боловч үйл ажилгааг бууруулдаг

Circuit түвшний гарц / Circuit-level gateway / : TCP эсвэл UDP холболт тогтоосон үед аюулгүй байдлын энэ арга замыг мөрдөнө. Холболт хийгдсэний дараа , пакетуудыг шалгалгүй хоструу урсгаж чадна.

Прокси сервер / Proxy server / : Сүлжээгээр орж , гарж буй бүх мэдээллийг ялгадаг. Прокси сервер нь үнэн сүлжээний хаягийг нуудаг.

Зурвас эмхэтгэл алгоритмууд ба дижитал гарын үсэг

Зурвас эмхэтгэл алгоримт эсвэл нэг мөр хэш функц : Дурын хэмжээтэй мөр (зурвас)авч тогтмол урттай мөр(хэш эсвэл эмхэтгэл) үүсгэдэг.Товч дараах шинжүүдтэй байна :

* Өөр зурвас олох тооцооллын хувьд биелэшгүү байх нэг эмхэтгэл бий болгоно
* Эмхэтгэлээс зурвасын талаар юу ч мэдэж чадахгүй.

Дижитал гарын үсэг нь хоёр хэсгээс бүрдэнэ : Хувь хүн болон байгууллагыг хувийн түлхүүр , гарын үсэгтэй нь хамт тооцоолол хийнэ. Гарын үсэг нь мэдээлэл хувь хүн эсвэл байгууллагаас ирсэн эсэхийг шалгаж чадна. Гараар бичсэн гарын үсэг шиг дижитал гарын үсэг нь олон ашигтай шинж чанартай байдаг :

* Жинхэнэ эсэхийг олон нийтийн түлхүүрээр харгалзах тооцооллыг ашиглан шалгаж чадна
* Энэ хуурамч байж чадахгүй
* Гарын үсэг зурсан мэдээлэл бол гарын үсэг нь цаашид хүчинтэй байх ба мэдээллийг шалгаж болно, өөрчилж чадахгүй.

Хамгаалалтын төрлүүд /Types of Security /:

Өгөгдлийн сангийн аюулгүй байдал нь олон асуудлуудыг тусгасан өргөн цар хүрээг хамардаг.

* Тодорхой мэдээлэл олж авах эрхийн тухай хууль эрх зүйн болон ёс зүйн янз бүрийн асуудлууд

Жишээ нь : АНУ-д мэдээллийн нууцлалыг зохицуулах олон хууль байдаг.

* Төрийн бодлого , аж ахуй байгуулгын түвшинд олон нийтэд хүргэж болохгүй мэдээл байдаг.

Жишээ нь : Зээлийн зэрэглэл, хувийн эрүүл мэндийн бүртгэл гэх мэт.

* Системтэй холбоотой асуудлыг системийн түвшинд төрөл бүрийн аюулгүй байдлын үйл ажилгааг хэрэгжүүлдэг байх ёстой.

Жишээ нь : Аюулгүй байдлын үйл ажиллагаа физик тоног төхөөрөмжийн түвшинд, үйлдлийн системийн түвшинд, эсвэл DBMS түвшинд шийдэх шаардлагатай эсэх.

* Зарим байгууллагад шаардлагатай аюулгүй байдлын түвшин , өгөгдөл болон хэрэглэгчид суурьласан хэд хэдэн ангилал тодорхойлж ангилдаг.

Жишээ нь : Маш нууц , нууц болон ангилагдаагүй. Мэдээллийн янз бүрийн ангилалд хандах хандалтыг зөвшөөрөхтөй холбоотой байгуулгын бодлого хэрэгжүүлдэг байх ёстой.

Хяналтын арга хэмжээ / Control Measures / :

Мэдээлэлийн сангийн аюулгүй байдлыг хангахад дөрвөн гол хяналтын арга хэмжээг ашигладаг.

* Хандалтыг хянах /Access control /
* Урсгалын хяналт / Flow control /
* Дүгнэлтийг хяналт / Inference control /
* Өгөгдлийн нууцлал / Data encryption /

Компьютерийн системүүдэд нийтлэг байдаг аюулгүй байдлын асуудал нь системд зөвшөөрөлгүй этгээд хандах , мэдээлэл олж авах эсвэл мэдээллийн санд хортой өөрчлөлт оруулхаас урьдчилан сэргийлэх юм.

Жишээ : Статик өгөгдлийн сангаас хүн амын насны бүлэг,орлогын түвшин , өрхийн тоо , боловсролын түвшин болон бусад шалгуурт үндэслэн статик мэдээлэл өгч болно. Ийм өгөгдлийн сангийн хэрэглэгчид нь засгийн газрын статикч эсвэл зах зээлийн судалгааны компаниуд нийт хүн амын тухай статик мэдээлэл авахын тулд өгөгдлийн санд хандах эрхтэй боловч тодорхой хувь хүмүүсийн дэлгэрэнгүй нууц мэдээллийг авч чадахгүй. Статик өгөгдлийн сангийн аюулгүй байдал нь хувь хүний мэдээлэл хандаж чадахгүй байна.!!!!. Энэ асуудал, статистикийн мэдээллийн сангийн аюулгүй байдал гэж нэрлэдэг. Холбогдох хяналтын арга хэмжээ дүгнэлт хяналтын арга гэж нэрлэдэг.

Өгөгдлийн сангийн аюулгүй байдал ба админ / Database security and DBA / :

Өгөгдлийн сангийн администратор (DBA) нь өгөгдлийн сангийн системийг удирдах гол мэргэжилтэн юм. DBA-ийн үүрэг, хариуцлага системийг ашиглах хэрэгтэй хэрэглэгчдэд давуу эрх олгох, байгууллагын бодлогын дагуу хэрэглэгчид болон мэдээллийг ангилах зэрэг юм. Админ нь өгөгдлийн санд админ бүртгэлтэй байна заримдаа супер хэрэглэгчийн бүртгэл гэж нэрлэдэг. Энэ нь ердийн мэдээллийн санд хэрэглэгчдэд хүртээмжтэй биш хүчирхэг боломжуудыг олгодог.

1. Бүртгэл үүсгэх / Account creation / : DBMS-д хандах эрхтэй хэрэглэгч эсвэл хэрэглэгчдийн бүлэгт шинэ бүртгэл , нууц үг үүсгэх үйлдэл юм .
2. Эрх олгох / Privilege granting / : Энэ арга хэмжээ нь тодорхой дансанд тодорхой давуу эрх олгохыг админ зөвшөөрөх үйлдэл юм.
3. Эрх цуцлах / Privilege revocation / : Урьд нь тодорхой дансанд өгсөн тодорхой давуу эрхийг цуцлах админ зөвшөөрөх үйлдэл юм.
4. Аюулгүй байдлын түвшин дэхь хэрэглээ / Security level assignment / :

Аюулгүй байдлын цэвэрлэгээний түвшинд хэрэглэгчийн бүртгэлийг зааж бүртгэх үйлдэл юм.

Админ нь өгөгдлийн сангийн системийн ерөнхий аюулгүй байдлыг хангах үүрэгтэй.

1-р үйлдэл : Жагсаалтыг бүхэлд нь DMBS-д хандах хандалтыг хянахад ашиглана. 2 ,3 -р үйлдэл : Өгөгдлийн санг дур зоргоороо ашиглахаас хянахад ашиглана.

4-р үйлдэл : Зөвшөөрөл хянахад ашиглана.

Андройд дээр mysql-тэй холбож insert ,update , delete , select хийсэн textlinked болгож үзсэн

**Аюулгүй байдал гэдэг нь хор хохирлоос хамгаалах эсвэл эсэргүүцэх чадварын чанар юм. Энэ нь хүн, орон гэр, эд зүйл, улс үндэстэн болон байгуулга гэх мэт эмзэг, үнэ цэнэтэй бүх зүйл дээр хэрэглэгддэг.**

Өгөгдлийн сангийн аюулгүй байдал :

Өгөгдлийн сангийн аюулгүй байдал нь хулгай, буруу хэрэглэх, хүсээгүй халдлага болон дайралтаас өгөгдлийг хамгаалдаг тогтсон журам, стандарт бодлого болон тоног төхөөрөмжийн цогц юм.Өгөдлийн сангийн аюулгүй байдал нь өгөгдлийн бүтэц байгууламж болон үүнд агуулагдаж байгаа өгөгдөлд нэвтрэх зөвшөөрлийг авч үздэг.Өгөгдлийн санг аюулгүй болгоход хэрэглэгдэх багаж хэрэгцэл нь ихэвчлэн өгөгдлийн сангийн програм хангамж дотор нь суулган тохируулагдсан байдаг ба үйлдвэрлэгчид нь Oracle, MySQL, Microsoft SQL Server гэх мэт өөр өөр байна. Өгөгдлийн сангийн програм хангамжыг үйлдвэрлэгчид өгөгдлийн сангийн аюулгүй байдлыг хангах зорилгоор хамгийн түгээмэл ашигладаг аргууд нь хандалтыг хянах, гэрчилгээ болон өгөгдлийн нууцлаж хадгалах юм.

Өгөгдлийн сангийн аюулгүй байдлын зорилго :

Үр ашигтай аюулгүй байдлын архитектүр нь нууцлал (confidentiality), бүрэн бүтэн байдал (integrity), бэлэн байдал(availability) тулгууралдаг.