Монгол дахь цахим мэдээллийн аюулгүй байдал

Эмзэг тал, эрсдэл бэрхшээл, шийдэх арга зам

М. Батсэргэлэн [*], О. Энхбат [**], Ч. Эрдэнэбат [***]
[*] МТ –ийн зөвлөх, [**] MCS Холдинг ХХК, [***] ШУТИС, КТМС, Компьютерийн ухааны салбар
enkhbat.18@gmail.com

***Хураангуй*—Монгол дахь цахим мэдээллийн аюулгүй байдал, түүний "хөндүүр цэг" (эмзэг сул тал, тодорхой зарим нүх цоорхой), тохиож буй болон болзошгүй аюул занал .. холбогдох жишээ баримт, шийдвэрлэх арга замын талаар энд товч өгүүлэв. Ялангуяа технологийн угшилтай эмзэг байдлыг хэрхэн оновчтой хамгаалах, эрсдлийг бууруулахад шаардлагатай тохируулга, арга техникийн талаар мөн дурдсан. Сэдвийн агуулгын хүрээнд, дотоодын мэдээлэл технологийн компаниудын сүлжээ, сервер, вэбүүдэд хийсэн шалгалт шинжлэлийн зарим үр дүнг тоймлон харуулсан болно.**

Түлхүүр үг—information security; mongolia; sql injection; xss; cisco; wireless; wep; ddos; ssl;

I. Удиртгал

Мэдээллийн аюулгүй байдал (МАБ) нь өнөө цагт өргөн хүрээнд .. өндөр түвшинд байнга яригддаг нийтлэг том сэдэв болж хувирсан техник технологийн дэвшлээс үүдэлтэй жам ёсны асуудал юм. Нэг хүнээс нөгөө хүнд очих цахим мэдээ мэдээлэл анхны агуулга шинжээ гээлгүй үнэн зөв дамжих ёстой. Гэвч .. мэдээллийн урсгалын зам зуурт дундын [хөндлөнгийн] хүчин зүйлс нөлөөлснөөр мэдээллийн анхны шинж тэмдэг алдагдах нь, уг мэдээллийг хүлээн авагч талын [сэтгэлзүйн] төлөв байдалд хүчтэй сөрөг нөлөө үзүүлэх, нэг ёсны "зэвсгийн зориулалтаар ашиглагдах" боломж бүхий нь нэгэнт нотлогджээ. Энэ байдал өөрөө, цахим мэдээлэл, чухамдаа хэр зэрэг үнэ цэнэтэй зүйл вэ, түүний үнэн зөв байх нь хэр чухал вэ гэдгийг илтгэн харуулдаг. Үүнийг ухаарсан америк, англи, герман тэргүүтэй өрнөдийн хөгжингүй орнууд цахим мэдээлэл үнэн зөв дамжигдах нөхцөлд анхаарч, ихээхэн хүч хөрөнгө зарсаар иржээ.

Эдүгээ хөгжиж буй орнууд ч тэдний нэгэн адил анхаарлаа мөн зүгрүү хандуулж байна. Хэдий тийм ч, хөгжингүй орнууд хүртэл мэдээлэл алдагдах аюулыг бүрэн хаах боломжгүй юм гэдгийг хүлээн зөвшөөрч, байдлыг улам улмаар сайжруулах, асуудлыг аль болох төгс шийдэхэд дөхүүлэх гэж оролдсоор тэмүүлсээр ажээ. Нэгэнт байдал ийм байгаа болохоор, үндэстэн дамнасан том корпорациуд ч мэдээллээ хамгаалж чадалгүй алдаж их хэмжээний эдийн засгийн хохирол амссаар буй аж. Гадны өндөр хөгжилтэй орнуудын хувьд байдал [нэг] иймэрхүү дүр төрхтэй байгаа бол Монгол Улсын хувьд байдал ямаршуухан байгааг ч хөндөж ярихгүй байхын аргагүй юм.

Монгол улсын мэдээлэл технологийн (МТ) салбарын хөгжил хурдцын хувьд мэдэгдэхүйц ахицтай байгаа боловч, монголын хэрэглэгчид гадаад орнуудад хийгдсэн тоног төхөөрөмжүүд дээр ажиллах, түүгээр сүлжээгээ байгуулах, мэдээллээ хамгаалах байдалтай явж ирсэн, энэ байдал өнөөдөр ч хэвээр байгаа юм. Гол нь гадны тоног төхөөрөмжүүдэд зохих ёсны хяналт шалгалт хийлгүй, тэдгээрийг чухал дэд бүтэцдээ ашиглах нь тийм ч их найдвар төрүүлэхээргүй үйлдэл бөгөөд цахим мэдээллийн аюулгүй байдлын талаасаа эрсдэлтэй алхам юм. Жишээ нь: Монгол Улсын засаг захиргааны үндсэн нэгж - 21 аймгийг холбосон шилэн кабелийн холболтын төхөөрөмжүүд бүгд (ZTE, Huawei г. м.) үндсэндээ өмнөд хөршийн компаниудых байгаа нь нэг эргэлзээ сэжиг .. их бага хардлага төрүүлэх үндэстэй [1]. Хэдэн жилийн өмнө Энэтхэг, Англий МТ –ийн салбарт ашиглаж байсан ZTE [2], Huawei [3] компаниудын төхөөрөмжүүдэд засгийн газраас нь мэргэжлийн баг томилон шалгалт тандалт хийж үзэхэд, тэдгээрт мэдээлэл дамжуулах нууц чип буйг илрүүлж, улмаар тэд дахиж ZTE, Huawei –ийн тоног төхөөрөмжийг авч ашиглахаас татгалзсан тохиолдлууд ч гарч байжээ [4], [5].

Нуугдмал чипийн хувьд, тэдгээр нь, төв серверээс өгөх команд хүлээх бөгөөд орж гарч буй сүлжээний урсгалд шилжилгээ боловсруулалт хийж төврүүгээ дамжуулах чадвартай байв. Гадаадын улс орнууд авч ашиглах ашиглах тоног төхөөрөмжүүддээ мэргэжлийн төвшний шалгалт хийх чадвартай мэргэжлийн багаа бодлогоор байнга хөгжүүлж байдаг нь, уг сэдэв хир зэрэг чухал вэ гэдгийг тодорхойлж буй хэрэг юм.

Манай орны хувьд иймэрхүү [чанарын] шалгалт хийх ашиглах тоног төхөөрөмж ч үгүй, шалгалт явуулах бэлтгэгдсэн мэргэжлийн баг ч үгүй явж ирсэн байдал төлөв өөрөө шууд эхний гэмээр эмзэг цэгийг үүсгэж байна гэлтэй. Байдал ийм байгаа нь монголд өнөөдөр, МАБ –ын тухай итгэл төгс ярих эрч хүчийг сааруулж байна гэж үзнэ. Өөр жишээ татья. Хэдэн жилийн өмнө БНХАУ –ын засаг төрийн системд хэрэглэгдэгч компьютер, сүлжээний тоноглол, үйлдлийн системүүд бүгд АНУ –ын Сиско [6], Майкрософт компанийн бүтээгдэхүүнүүд байв. Тухайн үед, АНУ Виндоус үйлдлийн системээ ашиглаж хятадын засаг төрийн нууц чухал мэдээллүүдийг хүссэн цагтаа авч бүрнээ чадна гэсэн болгоомжлол, хардлага БНХАУ –ын Үндэсний аюулгүй байдлын зөвлөлийн түвшинд яригдаж байсан ба улмаар тэд хариу арга хэмжээ авахад хүрсэн байдаг. БНХАУ мэдээллээ хамгаалахын тулд өөрсдийн

гэсэн үйлдлийн системийг бүтээж засгийн газрын системийн бүх компьютерууддаа ашигласнаар тухайн салбарт “үүсээд байсан” америкийн аюулыг бууруулж чадсан гэдэг [7].

Хятадын тал улмаар хариу арга хэмжээгээ бүх чиглэлд “хөгжүүлж” олон зуун өндөр төвшний мэргэжлийн хакераас бүрдсэн кибер-арми хүртэл үүсгэж дэлхийн улс орнуудын цахим нууц мэдээллийг гартаа оруулахыг санаархах болсоор удаж байна. Салбарын гаршууд мэргэжилтнүүдээс бүрдсэн өмнөд хөршийн хүчирхэг кибер-арми байнга шинэ шинэ вирус бүтээж, түүнийгээ гадагшаа үл дамжуулан, зөвхөн дотооддоо туршиж сайжруулсаар байдгийг аль ч талаас нь харлаа гэсэн бодлогын төвшний зохицуулалт гэдэг нь илт байдаг [8]. Хэрэв гадагшаа гаргахгүй хав дараастай тэр вирусын багцыг олон улсын “гүйлгээнд” оруулж гэмээнэ тэдгээрийг одоо ашиглаж байгаа аль ч анти-вирусын програмууд нэг хэсэгтээ илрүүлж чадахгүйд хүрнэ. Энэ хооронд тухайн вирусууд өөрийн байгаа ямарч саадгүй онилж, мэдээлэл хулгайлах, устгах, өөрчлөх .. гэх мэт үйлдлээ амжилттай гүйцэтгэх бололцоотой юм. Хятадын кибер-армийн зүгээс 2006 оноос хойш зохион байгуулсан удаа дараагийн олон довтолгоонд АНУ –ын томоохонд тооцогдох Гүүгл, Эппл тэргүүтэй 20 –иод компани өртөж хэдэн терабайт хэмжээтэй, олон арван тэрбум доллараар үнэлэгдэх мэдээллэл алдагдаж .. асуудал 2 улсын засгийн газрын түвшинд яригдатлаа хурцдаж байв.

Гадаадын өндөр хөгжилтэй орнуудад цахим сүлжээ нь өдөр тутмын хэрэглээ, бизнесийн үйл ажиллагааны салшгүй хэсэг болсон нь хувь хүн, пүүс компани бүрийн мэдээллийг нууцлах ажилд онцгой анхаарал хандуулахыг шаарддаг. Хэрэв хэн нэгний хувийн мэдээлэл алдагдвал учрах хохирол нь багагүй. Харин, одоохондоо монголын хувьд бүх зүйл цахим сүлжээнд хараахан холбогдоогүй, цахим сүлжээнээс хамааралтай бизнесийн үйл ажиллагаа явуулдаг компаниуд ч тийм олон биш байна. Энэ нь тухайн төрлийн аюул занал хол байна гэж үзэх үндэслэл болохгүй. Аюул бол дэргэд байна. Хуурмагаар тайвшруулах зарим аргументууд ч бий юм. Монголын банкуудын ихэнх нь онлайн төлбөр тооцооны системийг хэдийнэ нэвтрүүлсэн. Монголын банкууд онлайн төлбөр тооцооны системтэй болсон нь манай улсын хувьд МАБ -ын олон төрлийн хамгаалалт мониторингийн төвүүдтэйг “нотлон” илтгэмээр. Харамсалтай нь, манай бодит байдал энд эсрэгээрээ байгааг бид өмнө дурдсан билээ.

Монголд цахим мэдээллийн аюулгүй байдлаар идэвхтэй үйл ажиллагаа явуулдаг, гадны халдлагыг бүртгэж нэгдсэн тайлан гаргадаг CERT .. зэрэг мэргэжлийн байгууллагууд бий. Ажил асуудал эхлэлийн шатандаа .. хөгжих зүг идэвхтэй тэмүүлж байна. Манай улсын хувийн хэвшлийн Мобиком, улсын мэдлийн ҮДТ зэрэг нилээд хэдэн байгууллагуудад багагүй хүчин чадалтай IPS/IDS ашиглаж гадны халдлага, довтолгоо бүрийг тус бүрдээ чадах чинээгээрээ бүртгэдэг, мөн бусад МТ –ийн компаниуд, банкууд өөр өөрийн жижиг төхөөрөмж, галт хана .. зэргийг ашиглан холбогдох статистик, мэдээлэл гаргахаар чармайж ажилладаг [9]. Мөн Монгол улсад МАБ –тай холбоотой эрхзүйн орчин сайн бүрдээгүй, хууль тогтоомж боловсронгуй бус байдалдаа оршсоор байна. Товчхондоо төр засгийн хүчин чармайлт чамлагдсаар байна.

Өөр нэг бодит зүйл бол Монгол Улсын Засгийн газрын *.gov.mn [10] хаягтай вэб сайтууд цахим халдлагад өртөж байсан, байгааг эхэндээ сүрхий анхаардаг байсан ч, одоо бол болж л байдаг ердийн зүйл мэт сэтгэх хандлагатай болох шинж бүхий болов. Тэд давтамж ихтэйгээр хакдуулна тэглээ гээд хашрана гэж үгүй, дөжирсөн байдлаараа аанай л мөн хуучин ашигласан кодлол, технологи (Joomla [11]) дээрээ бушуухан дахин хийх, эсвэл яг ижил нөөцөлсөн кодоо сэргээгээд л байршуулчихна, мэдээж тэр нь, нэг их удалгүй мөнөөх халдлагадаа дахин өртөнө. Байдал ийм байхад бид шинэ зүйл тэр бүрий эрж хайхгүй байдаг нь эргэлзээтэй үйлдэл, хачирхалтай байр суурь юм. Үндэсний аюулгүй байдал гэж сүрхий ярих атлаа түүнд нийцсэн адекват арга хэмжээ авч хэрэгжүүлэх тал дээр шийдвэр гаргах дээд төвшиндөө тун сул анхаарч байна. Уг нь, цахим мэдээллийн аюулгүй байдал нь Монгол Улсын Үндэсний аюулгүй байдлын нэг үндсэн бүрэлдэхүүн хэсэг билээ. Энэ бүхэн юуг харуулаад байна гэхээр, цахим мэдээллийн аюулгүй байдлыг хангах эрхзүйн - үндсэн зарчимд тулгуурлан, цахим мэдээллийн аюулгүй байдлын соёлыг эрчимтэй хөгжүүлэх хүсэл зориг ялангуяа шийдвэр гаргах дээд түвшиндээ ихээхэн чамлагдаж байна гэлтэй.

Цахим мэдээлийн аюулгүй байдалд холбогдох буруу жишиг манайд элбэг, түгээмэл байна. МАБ гэж ярихаар зөвхөн технологи талын сэдэв гэж андуу ойлгох нь нэн төвөгтэй. Бодит амьдрал дээр технологи тал 20% ба тухайн хүний зан үйл, мэдлэгийн асуудлаас шалтгаалсан мэдээлэл алдалт 80% гэж гардаг нь хувь хүн бүр хичээх юм бол МАБ –ыг 80% хүртэл бууруулах боломжтой гэдгийг харуулна [12]. Үлдсэн [тэр] 20% -ийн тухайд, мэдээж хэрэг тэнд [өмнө дурдсан] өндөр чадвартай мэргэжлийн баг, өндөр хүчин чадлын тоног төхөөрөмжүүд шаардагдах нь тодорхой.

Мэдээллийн аюулгүй байдлын асуудлыг авч ярихдаа, монголын нөхцөлд, хүнийн зан үйл, мэдлэг чадварт түлхүү анхаарах цаг арга буюу тулж ирж байна. Энгийн жишээ татахад имэйл болон онлайн төлбөрийн хэрэглэгчийн нэр, нууц үг ижилхэн эсвэл нууц үг нь өөрийн төрсөн огноо, утасны дугаар .. гэх мэт хүн тодорхой чиглүүлэгтэйгээр таачих боломжтой зүйл их байгаа нь хэрэглэгчийг эрсдэлд оруулдаг. Мөн Виндоус үйлдлийн системийг албан ёсны лицензийн эрхгүй ашигладаг, түүний интернетэд байнга гардаг шинэчлэлтүүдийг огт суулгадаггүй, анти-вирусны сигнатурын шинэчлэлтийн татацуудыг суулгадаггүй .. гэхчилэнгийн асуудлууд ч нэмэгдэнэ. Бид хэн нэгтэй харилцаж байхдаа ямар мэдээллийг ярих эс ярих ёстойгоо ч мэдэхгүй сэтгэлийн хөөрөлд автах хандлагаасаа салж ангижрахгүй байна. МАБ –ын наад захын мэдлэг монголчуудад өнөө хир төлөвшиж өгөхгүй байна. Энэ нь монголчууд бидний хуулбарлах бэлэнчлэх сэтгэлгээнээс улбаатай байж болох ч, нийгэм дэх тухай салбарын .. хүний нөөцийн менежментийг бодлоготойгоор эрчимтэй зохион байгуулахгүйгээр үр дүнд төдийлэн хүрэхгүйг өмнө дурдсан 80% -ийн үзүүлэлт хэлээд байх шиг ээ.

Зураг 1. Мэдээлэлийн аюулгүй байдлын гурвалжин

Зураг 1 -т харуулснаар МАБ –ыг хамгийн сайн ойлгож дэмжих ёстой хүмүүс нь төрийн удирдах албан тушаалтан, хувийн хэвшлийн байгууллагуудын дарга нар .. мөн гэдэг нь харагдаж байна. Гэтэл, манай оронд эсрэгээрээ буюу МАБ –ын талаар ойлголтоор сайнгүй хүмүүс нь дээрх албан тушаалд тавигдчихаад байгаад оршино. Асуудалд ахиц гарахгүй байгаагийн бас нэгэн шалтгаан энэ буюу.

II. АЮУЛ ЗАНАЛЫН БОДИТ БАЙДАЛ

Дотоодын МТ -ийн компаниудын вэб хуудас, сүлжээ, утас зэргийг өөрсдийн боломжоор шалгахад гарсан үр дүнгээр, хамгийн их тохиолдсон эмзэг байдлыг бид тодорхойлох гэж оролдсон юм. Бид судалгаандаа SQL тарилга [13], XSS [13], Cisco свич, SNMP [14], SSL [15], акцес пойнтуудын нууц үгийн талаар анхаарвал зохих асуудлуудыг тухайлан авч үзлээ.

A. *SQL тарилга*

SQL тарилга (SQLi) гэж нэрлэгддэг энэ төрлийн халдлага нь хамгаалалтын сул талыг ашиглан тухайн програмын мэдээллийн санд хандах боломжийг олгодог довтолгооны арга техник (хэрэгсэл) юм.

Зураг 2. SQLi халдлагын жишээ

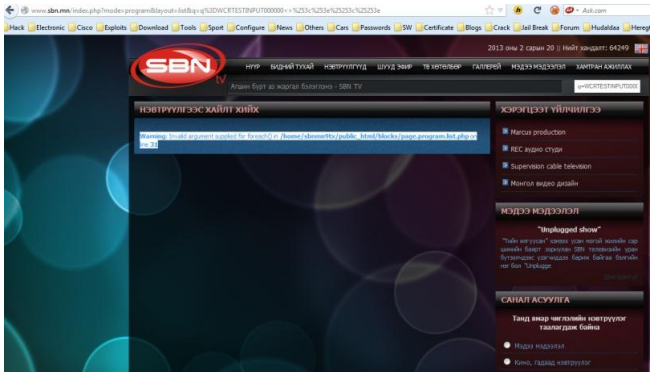
Төр засгийн байгууллага болон хувийн хэвшлийн компаниудын .. нийт 20 орчим вэб хуудаст шинжилгээ хийхэд тэдгээрийн дийлэнхэд (80% орчим хувьд) нь энэ алдаа илэрсэн болно. Тун сул үзүүлэлт. SQLi халдлагаас хамгаалах түгээмэл хэрэглээтэй 2 төрлийн арга байдаг бөгөөд энэ нь, оролтын өгөгдлийг нарийн шалгах, өгөгдлийн сантай ажиллахдаа сторед процедур ашиглах явдал байдаг.

Оролтын өгөгдлийг шалгах: Оролтын өгөгдлүүдийг зөвхөн ‘0-9’, ‘a-z’, ‘A-Z’ зэрэг тэмдэгтүүдээс тогтож байгаа эсэхийг шалгах функцийг зохион хэрэглэж болно.

Сторед процедур ашиглах: Өгөгдлийн сангаас мэдээлэл шүүж байгаа SQL илэрхийллээ програмын кодтой холихгүйгээр өгөгдлийн сангийн сервер дээрээ сторед процедур байдлаар бичиж хадгалан, өгөгдлүүдээ параметрээр дамжуулан дуудаж ажиллуулах нь SQLi халдлагын эрдслийг ихээхэн бууруулна.

B. *XSS*

Энэ нь хэрэглэгчийн хөтөч дээр ажиллах скрипт бүхий хорт код юм. Голдуу фишинг хийхэд, мөн зарим тохиолдолд хорт програм тараахад ашиглана.



Зураг 3. XSS халдлагын жишээ

Дээрх жишээний хувьд хэрэглэгчийн илгээсэн өгөгдлийг шалгалгүй шууд хэвлэснээр алдаа өгч вэбийн бүтэц, вэб аль хавтсанд байрлаж байгаа талаар дэлгэрэнгүй мэдээлэл үзүүлчихэж байна.

Хамгаалалт: Хэрэглэгчийн илгээсэн өгөгдлийг шууд хэвлэхгүй заавал HMTL хэлний онцгой тэмдэгтүүд рүү хувиргалт хийж байх нь зөв юм.

C. *Cisco свичүүдэд cdp*

Манай сүлжээний администраторууд нэг хэсэг Cisco төхөөрөмжүүдэд cdp тохиргоог анзааралгүй орхиод алдаа хийгээд байдаг байсан.

```
Cisco2621XM#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Cisco3550XL      Fas 0/1           124          T S       WS-C3548-XFas 0/1
Cisco2611        Fas 0/0           132           R        2621      Fas 0/0
Cisco2621XM#
```

Зураг 4. Cdp холболтын жишээ

Cisco төхөөрөмжийн интерфейсийн тохиргоонд no cdp коммандыг бичихгүй байх нь тухайн төхөөрөмжүүдийн талаарх мэдээллийг цуглуулах боломжийг олгодог. Үүнд:

Олж авсан мэдээллээ ашиглан сүлжээний бүтэцийн зураглал, замчлалын (routing) хүснэгт, хостуудын мэдээлэл (ARP хүснэгт) –ийг олж авах боломж бүхий юм.

D. Сүлжээний тоног төхөөрөмжүүдэд SNMP түлхүүр дефаулт байх

SNMP протокол нь тухайн сүлжээний тоног төхөөрөмжүүдийн сүлжээний урсгалыг хянахад хэрэглэдэг ба дундын холболтонд нууц үг ашигладаг [14].

Зураг 5. SNMP дефаулт түлхүүр үгээр шалгасан жишээ

Гэвч дефаулт нууц үг нь public, private гэх стандарт байдаг ба үүнийг солилгүй явуулснаас болж сүлжээний урсгалын талаарх мэдээлэл, сүлжээний зураглалаа бусдад алдах аюултай болдог. Бүр цаашилбал, хакерууд Cisco рүтер, свич, галт ханын тохиргоог шууд хуулж авах гэж оролдох болно.

E. е-Мэйл серверүүдэд SSL шифрлэлт ашиглахгүй байх

Ихэнх компаниуд е-мэйл сервертээ SSL [15] шифрлэлт ашиглахгүй байгаа нь ихээхэн эрсдлийг нөхцөлдүүлдэг. Үүнд: компанийн е-мэйл бүртгэл дэх нууц үгээ алдах, гадагш чиглэгдэж буй е-мэйлүүдээ алдах .. гэх мэт. Гэхдээ энэ төрлийн халдлагыг гадны сүлжээнээс шууд хийх нь ховор бөгөөд эхлээд олон төрлийн халдлагын аргууд ашиглаж дотоод сүлжээний аль нэг компьютерт нэвтэрсний дараа дээрх үйлдлүүдээ хийх боломж бүрдэнэ. Энэ аюулаас сэргийлэх гол арга бол сүлжээгээр дамжуулж буй мэдээллээ SSL шифрлэлт хийх, эсвэл өөр төрлийн шифрлэлтийн (жишээ нь: PGP [16]) технологи ашиглан дамжуулалт хийх явдал; гэж үзнэ.

F. Ачааллын тест буюу DDoS халдлагын хамгаалалт байхгүй байх

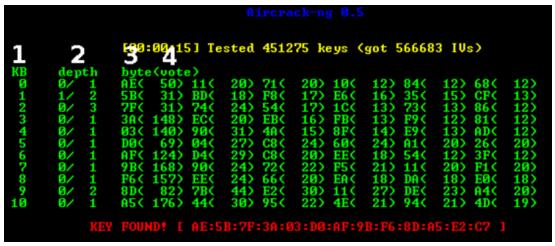
Энэ төрлийн халдлага нь гол төлөв хорлон сүйтгэх ажиллагаанд ашиглагддаг ба тухайн сүлжээ, вэб хуудасыг “жагсаалаас гаргах” зорилготой. Монголын зарим компаниудын вэб хуудасыг шинжлэхэд ихэнх нь энэ төрлийн халдлагын эсрэг ямар нэг тохиргоо буюу хамгаалах шийдэл байхгүй нь анзаарагдсан. Энэ чиглэлд бяцхан туршилт хийж гэмээнэ тэд зүгээр л үхлүүт сервер болон хувирах магадлал өндөртэй байв.

Зөвхөн нэг компьютерээс вэб ачааллын тест хийсэн бөгөөд шинжилгээнд хамруулсан 20 вэб серверийн 15 нь ачааллын тестийг тэсвэрлээгүй, хэрэв серверт 1 –ээс олон компьютерээр ачааллын тест хийсэнсэн бол үлдсэн 5 нь ч шалгуур давахгүй байдал .. шууд төсөөлөгдөж байсан болно.

Зураг 6. DDoS халдлагын жишээ

G. Утасгүй сүлжээний акцес пойнтын нууц үг шаардлага хангахгүй байх

Утасгүй сүлжээг байгууллага бүр л гол хэрэглээгээ болгож байгаа ч МАБ –даа үл анхааран, нууц үгийг WEP [17] технологиор өгөх эсвэл бүр нууц үггүй ч орхих явдал түгээмэл байдаг. Wi-Fi –ийн хувьд WPA2 256 бит кодлолыг ашиглах нь эрсдлийг бууруулах болно.



Зураг 7. Утасгүй сүлжээний халдлагын жишээ

Энэ мэтчилэнгийн олон төрлийн халдлага хийж болох энгийн эрсдлүүд монголын нөхцөлд түгээмэл байдалтай оршсоор байна. Сүүлийн үед шууд нэг-нүх цоорхой ашиглах замаар системд нэвтрэн ордог асуудал бараг үгүй болох шинжтэй байна. Үүний оронд олон шат дамжлага бүхий довтолгооны схем хэрэглэгддэг болж ирж байна. Жишээ нь: NFC [18] ашиглан хак хийе гэхэд, NFC –тэй тусдаа төхөөрөмж бэлдээд тэрийгээ програмчлаад NFC –тэй андройд утсанд ойртуулахад утасны NFC уншигч нь уншаад нөгөө төхөөрөмжөөс ирсэн URL хаягийг вэб броузер дээр дуудах ба броузерийн хувилбар алдаатай байвал түүнийг нь эксплойт хийгээд довтлогч этгээдийн компьютерлүү нь телнетээр эргэж хандаснаар довтлогч этгээд рүүт шеллтэй болж байх жишээтэй.

Бидний хэрэглэж байгаа IPv4 нөөц нь дууссан, МАБ талаасаа ч сайнгүй байгааг мэдэж байгаа ч IPv6 руу шилжих гэж ярахгүй байгаагийн учир юунд вэ?! 2011 онд болсон МТШХХГ -аас зохион байгуулсан хурал дээр IPv6 шилжих ажил явж байгаа гэсэн, 2012 оны бас нэгэн МТШХХГ -ийн хурал дээр аанай л мөн ажил явж байгаа .. гэсээр. Энэ байдлаараа 2013 оны ICTPA –ийн хурал дээр монголчууд бид дээрх хариултаа бас дахин давтахад дахиад бас ойрхон байх шиг ээ. Уг нь IPv6 –ийн сургалт 2011, 2012 онуудад монголд явагдсан. Азийн зарим улсын хувьд хаяглалтын дэд бүтцийн 80% орчимыг IPv6 руу

шилжүүлсэн гэсэн судалгааг 2011 онд БНСУ –ын Пусан хотноо болсон APNIC 32 конференцид танилцуулж байсныг энд дурдалтай.

III. Дүгнэлт

Өмнө өгүүлсэнчлэн .. цахим мэдээллийн тодорхой эмзэг байдлуудаас үүдэн учирч болох аюул занал монголын нөхцөлд амь бөхтэй оршисоор, бид хэзээ ч, хэнд ч өөрийн дансны нууц дугаар, е-мэйлын нууц дугаараа төвөггүй алдах боломж нээлттэй хэвээр байсаар байна.

Манай орны хувьд, мэдээллийн аюулгүй байдлын эмзэг байдлыг эрт мэдэх боломжийг олгодог аудитын шалгалт шинжилгээний компаниуд олшроогүй (SSS [19], PSSA [20] г. м), ба тэдний мэргэжлийн ур чадвар өндөр түвшинд хүрээгүй байгааг салбарын удирдлага анхааралдаа авмаар байна. Хэрэв ийм компаниудыг олшруулж төрөөс бодлогоор дэмжээд өгвөл ганц вэбээр тогтохгүй хувь хүн, байгууллага, бүр цаашилбал улс орны үндэсний аюулгүй байдалд чухал нөлөө үзүүлнэ. Тэгээд ч зогсохгүй хөгжингүй орнууд шиг хариу үйлдэл үзүүлэх чадвартай болох нь тийм ч биелэшгүй зорилт биш юм.

Ном зүй

[1] Х. Энхтуул, “21 аймгийг өндөр хурдны интернэттэй болгоно,” *iPost.mn*, 21-May-2012. [Online]. Available: http://ipost.mn/news/read/664. [Accessed: 10-Mar-2013].

[2] “ZTE Corporation,” *ZTE Corporation*. [Online]. Available: http://wwwen.zte.com.cn/en/. [Accessed: 10-Mar-2013].

[3] “Huawei - A leading global ICT solutions provider,” *Huawei*. [Online]. Available: http://www.huawei.com/en/. [Accessed: 10-Mar-2013].

[4] V. Mandalia, “India Bars ZTE, Huawei, Others from Sensitive Government Projects,” *Parity News*, 21-Jan-2013. [Online]. Available: http://paritynews.com/government/item/571-india-bars-zte-huawei-others-from-sensitive-government-projects. [Accessed: 10-Mar-2013].

[5] M. Rogers and D. Ruppersberger, “Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,” Washington DC, Oct. 2012.

[6] “Welcome to Cisco,” *CISCO*. [Online]. Available: http://www.cisco.com/. [Accessed: 10-Mar-2013].

[7] B. Gertz, “China blocks U.S. from cyber warfare,” *Washington Times*, 12-May-2009. [Online]. Available: http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/. [Accessed: 10-Mar-2013].

[8] “APT1: Exposing One of China’s Cyber Espionage Units,” *MandiantCorp*, 18-Feb-2013. [Online]. Available: https://www.youtube.com/watch?v=6p7FqSav6Ho. [Accessed: 10-Mar-2013].

[9] Tatar, “‘Мэдээллийн Аюулгүй Байдал 2012’ Өдөрлөг,” *Oin Manaach*, 25-Dec-2012. [Online]. Available: http://manaach.blogspot.com/2012/12/2012.html. [Accessed: 10-Mar-2013].

[10] “Defacements archive,” *Zone-H*, Mar-2013. [Online]. Available: http://zone-h.org/archive. [Accessed: 10-Mar-2013].

[11] “Joomla! The CMS Trusted By Millions for their Websites,” *Joomla.org*. [Online]. Available: http://www.joomla.org/. [Accessed: 10-Mar-2013].

[12] “The Human Factor in Data Protection,” Jan. 2012.

[13] M. Shema, *Seven Deadliest Web Application Attacks (Seven Deadliest Attacks)*. Syngress, 2010, p. 192.

[14] Tatar, “SNMP түлхүүр үгээ солиоч ээ□!!!,” *Oin Manaach*, 22-Nov-2012. [Online]. Available: http://manaach.blogspot.com/2012/11/snmp.html. [Accessed: 24-Nov-2012].

[15] С. Дөлмандах, “Тодруулга: SSL гэж юу вэ?,” *Технологи ба эрх чөлөө*, 31-Jul-2008. [Online]. Available: http://www.dulmandakh.com/2008/07/ssl.html. [Accessed: 15-Oct-2012].

[16] “The OpenPGP Alliance Home Page,” *OpenPGP.org*. [Online]. Available: http://www.openpgp.org/. [Accessed: 10-Mar-2013].

[17] “Wired Equivalent Privacy,” *Wikipedia*. [Online]. Available: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy. [Accessed: 10-Mar-2013].

[18] “Near field communication,” *Wikipedia*. [Online]. Available: http://en.wikipedia.org/wiki/Near_field_communication. [Accessed: 10-Mar-2013].

[19] “Бидний тухай | 3S LLC,” *3S LLC*. [Online]. Available: http://shop.sssmn.com/taxonomy/term/11. [Accessed: 10-Mar-2013].

[20] “Professional security service audit,” *pssa.mn*. [Online]. Available: http://pssa.mn/. [Accessed: 10-Mar-2013].