КИБЕР АЮУЛГҮЙ БАЙДАЛ

Ө.Энхчимэг /20B1NUM1389/

Удиртгал

Интернэтийн хөгжил, харилцаа холбооны сүлжээ улам бүр өргөжихийн хэрээр **кибер халдлагын**[1] тоо, хор хөнөөл илүү нэмэгдэж, аргачлал нь улам бүр нарийссаар байна. Улс орнууд кибер аюулгүй байдлыг хангах асуудалд ихээхэн анхаарал хандуулах болсон бөгөөд манай улсын хүн амын 68 хувь нь интернет хэрэглэж, төр хувийн хэвшлийн байгууллагуудын өдөр тутмын үйл ажиллагаа цахим хэлбэрт шилжих болсонтой холбоотойгоор кибер орчин дахь мэдээллийн хүртээмжтэй, бүрэн бүтэн байдлыг нь хангах шаардлага тавигдах болсон. Олон нийтийн мэдээллийн хэрэгслийг ашиглахдаа кибер аюулгүй байдлын ач холбогдол, мэдлэг, мэдээллийн нууцлал, хувийн болон бизнесийн хувьд мэдээллийн аюулгүй байдлын үнэ цэнийг таньж мэдэж хамгаалах хэрэгцээ шаардлага зайлшгүй тулгарч байгаа тул энэхүү сэдвийг сонгосон. Кибер ертөнцтэй холбогдохгүй хувь хүн, бизнесийн байгууллага, банк санхүү гэх мэт байгууллагууд байхгүй болсон цаг үе билээ. Байгууллагын үйл ажиллагаа түүний үе шат бүрт кибер аюулгүй байдал чухал нөлөө үзүүлнэ. Тухайлбал хүний нөөцийн алба нь хувь хүний регистрийн дугаар, банкны мэдээлэл, эрүүл мэндийн шинжилгээний хариу, гэр бүлийн мэдээлэл гэх мэт хувийн мэдээлэл дээр ажилладаг. Бизнес хөгжлийн алба нь хэрэглэгч үйлчлүүлэгчийн тухай мэдээлэл, бүтээгдэхүүн үйлдвэрлэл борлуулалттай холбоотой статистик мэдээ, санхүүжилт, стратегийн мэдээллийг ашигладаг. Хуулийн алба хэлтэс нь гэрээ, хэлэлцээр, зөвшөөрөл гэх мэт чухал нууцлал бүхий мэдээлэл дээр ажилладаг. Тиймээс кибер аюулгүй байдлын талаар мэдээллийг нийгэмд түлхүү хүргэх, бидний зайлшгүй анхааралдаа авах асуудлын нэг гэдгийг мэдээлэх шаардлага үүсэж байна.

Үндсэн ойлголт

Тодорхойлолт, Кибер халдлагын эсрэг авах арга хэмжээг кибер аюулгүй байдал гэж нэрлэнэ.[2] Кибер аюулгүй байдал гэдэг нь техник хангамж, програм хангамж, чухал өгөгдөл зэрэг интернетэд холбогдсон системийг халдлага, гэмтэл, зөвшөөрөлгүй хандалтаас хамгаалахыг хэлнэ. [3] Кибер гэмт хэрэг гэдэг нь компьютер, сүлжээнд холбогдсон төхөөрөмж, сүлжээтэй холбоотой аливаа гэмт хэргийн үйл ажиллагаа юм Харилцаа холбоонд интернетэд холбогдсон компьютер эсвэл бусад ухаалаг төхөөрөмжид аливаа аюулгүй байдлын зөрчилд өртөж болзошгүй. Үүнд:

- Имэйл, утас, мессеж гэх мэт харилцаа холбооны системүүд
- Замын хөдөлгөөний удирдлага, автомашины хөдөлгүүр, онгоцны навигацийн систем зэрэг тээврийн систем
- Засгийн газрын мэдээллийн сан, үүний Нийгмийн даатгалын дугаар, лиценз, татварын бүртгэл
- Банкны данс, зээл, цалингийн төлбөр зэрэг санхүүгийн систем
- Эмнэлгийн систем, үүний тоног төхөөрөмж, эмнэлгийн бүртгэл

[1] **Тайлбар:** Кибер халдлага гэж компьютерийн систем болон сүлжээнд эзэмшигчийн зөвшөөрөлгүй хандаж мэдээллийг хулгайлах, устгах, өөрчлөх болон системийг ашиглах боломжгүй болохыг хэлнэ.

[2] Мэдээллийн технологийн паспорт шалгалтад бэлтгэх гарын авлага 48 – р хуудас

[3] https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

- Боловсролын системийн тайлан карт, судалгааны мэдээлэл г.м

[4]Кибер аюулгүй байдлын аюулын цар хүрээ

Кибер хамгаалалтын тактикууд хөгжиж байгаа хэдий ч хортой программ хангамж болон бусад аюулууд шинэ хэлбэрт орж байгаа тул кибер аюулгүй байдлын аюул заналхийлж байна. Кибер аюулгүй байдлын заналхийлэл нь ялгаварлан гадуурхдаггүй гэдгийг санах нь ухаалаг хэрэг юм. Сүлжээг ашигладаг бүх хувь хүн, байгууллагууд боломжит зорилтот бүлэгт багтдаг. Кибер аюулаас өөрийгөө хамгаалахад туслахын тулд кибер аюулгүй байдлын гурван өөр төрлийн аюул заналыг мэдэх нь чухал:

- Кибер гэмт хэрэг
- Кибер халдлага
- Кибер терроризм.

Кибер гэмт хэрэг нь таны системийг сүйтгэх эсвэл санхүүгийн ашиг олох зорилгоор нэг буюу хэд хэдэн хүн үйлддэг.

Кибер халдлага нь ихэвчлэн улс төрийн шалтгаанаар хийгддэг бөгөөд таны нууц мэдээллийг цуглуулах, түгээх зорилготой байж болно.

Кибер терроризм нь хохирогчдод айдас, айдас төрүүлэхийн тулд цахим системийг зөрчих зорилготой юм.

[5]Кибер халдлага хэрхэн болдог вэ?

Кибер халдлага нь хувь хүн, бүлэг эсвэл зохион байгуулалттай бүлэглэл өөр хүн эсвэл байгууллагын аюулгүй байдлын системийг хорлонтойгоор зөрчихийг оролдсон үед үүсдэг. Хакерууд компани эсвэл байгууллагын аюулгүй байдлыг давж, нууц мэдээллийг хулгайлсан тохиолдолд өгөгдөл нөөц зөрчигддөг. Тэд энэ мэдээллийг хулгайлах, бусад залилан мэхлэх эсвэл Dark Web дээр зарах зорилгоор ашигладаг.

2022 онд мэдээллийн зөрчлийн тоо 68%-иар өссөн байна. Гэвч мэдээллийн зөрчлүүд нь кибер халдлагаас үүдэлтэй үр дагаврын зөвхөн нэг нь юм.

Халдлагыг хувийн мэдээлэл олж авах, кибер гэмт хэрэгтнүүдэд хувийн мэдээллийг хулгайлах боломжийг олгоход ашиглаж болно. Эсвэл тэднийг хорлонтой бүлэглэлүүд байгууллагын сүлжээг эвдэх зорилгоор ашиглаж болно

Кибер халдлагын 17 төрөл

1. Хортой програм дээр суурилсан халдлага (Ransomware, Trojans гэх мэт)
2. Фишинг халдлага (жадны фишинг, халим гэх мэт)
3. Man-in-the-middle attacks
4. Үйлчилгээнээс татгалзах халдлага (DOS ба DDoS)
5. SQL Injection халдлага
6. DNS туннел хийх
7. Тэг өдрийн мөлжлөг, халдлага
8. Нууц үгийн халдлага
9. Drive-by татаж авах халдлага

[4] What is cyber security? A definition + overview | Norton
[5] https://www.aura.com/learn/types-of-cyber-attacks

10. Сайт хоорондын скрипт (XSS) халдлага
11. Rootkits
12. DNS хуурамчаар үйлдэх эсвэл "хордуулах"
13. Интернэт зүйлсийн (IoT) халдлага
14. Сеанс хулгайлах
15. URL засвар
16. Cryptojacking
17. Дотоод аюул заналхийлэл

Кибер гэмт хэргийн тодорхойлолт

Хуулийн дагуу эсвэл өөр хэлбэрээр нууц мэдээллийг саатуулсан, задруулсан тохиолдолд кибер гэмт хэргийн талаар олон хувийн нууцтай холбоотой асуудлууд байдаг. Олон улсын хэмжээнд төрийн болон төрийн бус байгууллагууд тагнуул, санхүүгийн хулгай болон бусад хил дамнасан гэмт хэрэг зэрэг цахим гэмт хэрэг үйлддэг. Олон улсын хилийг давж, дор хаяж нэг үндэстэн улсын үйл ажиллагаатай холбоотой кибер гэмт хэргийг заримдаа кибер дайн гэж нэрлэдэг. Уоррен Баффет кибер гэмт хэргийг "хүн төрөлхтний нэг номерын асуудал" хэмээн тодорхойлж, кибер гэмт хэрэг нь "хүн төрөлхтөнд бодит эрсдэл учруулдаг" гэжээ.

[6]Кибер аюулгүй байдлын халдлагаас хэрхэн хамгаалах талаар:

Кибер аюулгүй байдлын мэдлэгийг нэмэгдүүлэхэд туслах үндсэн алхамууд байдаг.

1. Хувийн мэдээллээ өгөхдөө зөвхөн итгэмжлэгдсэн сайтуудыг ашиглах. Сайн дүрэм бол URL-г шалгах явдал юм. Хэрэв сайтад "https://" орсон бол энэ нь аюулгүй сайт болно. Хэрэв URL-д "http://" орсон бол - дутуу "s"-г тэмдэглэнэ үү - зээлийн картын мэдээлэл эсвэл Нийгмийн даатгалын дугаар гэх мэт нууц мэдээллийг оруулахаас зайлсхий.
2. Үл мэдэгдэх эх сурвалжаас ирсэн имэйлийн хавсралтыг нээх эсвэл холбоос дээр дарж болохгүй. Сүлжээ болон хэрэглэгчид хортой программ хангамж, вирус өртөх хамгийн түгээмэл арга замуудын нэг бол таны итгэдэг хүн илгээсэн мэт далдлагдсан имэйлүүд юм. Хамгийн чухал дүрэм бол вэбсайт руу орох имэйлийн холбоос дээр дарахаас илүүтэйгээр вэбсайт руугаа зочлох явдал юм.
3. Төхөөрөмжүүдээ үргэлж шинэчилж байгаарай. Программ хангамжийн шинэчлэлтүүд нь аюулгүй байдлын сул талыг засах чухал засваруудыг агуулдаг. Кибер халдагчид мөн хамгийн сүүлийн үеийн аюулгүй байдлын программ хангамжийг ажиллуулаагүй хуучирсан төхөөрөмжүүдийг онилж болно.
4. Кибер аюулгүй байдлын халдлагын үед нэмэлт хамгаалалт хийхийн тулд файлуудаа тогтмол нөөцлөөрэй. Хэрэв та кибер халдлагын улмаас төхөөрөмжөө цэвэрлэх шаардлагатай бол эсвэл ransomware халдлагад өртсөн тохиолдолд таны өгөгдөлд хандах боломжтой бол энэ нь таны файлуудыг аюулгүй, тусдаа газар хадгалахад тусална.

[6] What is cyber security? A definition + overview | Norton

Кибер аюулгүй байдлын хувьд байгууллагынхаа бүхий л мэдээллийн системийг бүхэлд нь зохицуулах хэрэгтэй. Кибер элементүүд нь дараах бүх зүйлсийг хамардаг:

- Сүлжээний аюулгүй байдал
- Программын аюулгүй байдал
- Endpoint аюулгүй байдал
- Өгөгдлийн аюулгүй байдал
- Cloud аюулгүй байдал
- Гар утасны аюулгүй байдал
- Бизнесийн тасралтгүй ажиллагааны төлөвлөлт
- Эцсийн хэрэглэгч

[7]**Кибер аюулгүй байдлын хяналт** нь кибер аюул, халдлагаас урьдчилан сэргийлэх, илрүүлэх, бууруулахад ашигладаг механизм юм. Механизмууд нь хамгаалалтын харуул, хяналтын камер зэрэг физик хяналтаас эхлээд галт хана, олон техникийн хяналтууд байдаг.

Захиргааны/удирдлагын хяналт нь шинэ программ хангамжийн удирдлага шиг "сайн" биш ч байгууллагын гишүүдэд бүтэц, зааварчилгаа өгч зөрчил гаргахгүй байхыг баталгаажуулдаг.

Физик хяналтууд нь системд хандах хандалтыг физик байдлаар хязгаарладаг. Fences, CCTV, Guard Dog г.м.

Техникийн/Логик хяналтууд нь шифрлэлт, хурууны хээ уншигч, баталгаажуулалт. Итгэмжлэгдсэн платформ модулиуд (TPMs) зэрэг техник хангамж эсвэл програм хангамжийн үндсэн дээр хандалтыг хязгаарладаг. Эдгээр нь физик удирдлагатай адил физик системд хандах хандалтыг хязгаарладаггүй, харин өгөгдөл эсвэл агуулгад хандах хандалт юм.

Үйл ажиллагааны хяналт гэдэг нь үйл явцыг өдөр тутмын түвшинд явуулж буй хүмүүсийг хамарсан хяналтууд юм. Жишээ нь, мэдлэг олгох сургалт, хөрөнгийн ангилал, бүртгэлийн файлуудыг шалгах зэрэг байж болно.

Аюул заналхийлэл, босоо чиглэлээс хамааран эрсдэлийг бууруулах зорилгоор ангилж, хэрэглэх боломжтой хяналтын төрлүүд:

- Урьдчилан сэргийлэх хяналтууд нь ямар нэг үйлдэл хийхийг зөвшөөрөхгүй байх ба firewalls, fences хандалтын зөвшөөрлийг агуулдаг.
- Мөрдөгчийн хяналтыг зөвхөн видео тандалт, халдлага илрүүлэх систем гэх мэт үйл явдлын үеэр эсвэл дараа нь идэвхжүүлдэг.
- "Guard Dog" эмзэг байдлыг ашиглахыг хориглодог.
- Залруулагч хяналт нь нэг төлөвөөс нөгөө төлөвт үйлдэл хийх боломжтой.
- Сэргээх хяналт нь хатуу дискийг сэргээх гэх мэт алдагдлаас ямар нэг зүйлийг буцааж авдаг.
- Хандалтын бүртгэлийг тогтмол хянаж байх г.м бусад хяналтын дутагдлыг нөхөхийг оролддог хяналтуудыг нөхөх хяналтууд гэнэ.

[7] https://www.techtarget.com/searchsecurity/feature/Types-of-cybersecurity-controls-and-how-to-place-them

Кибер аюулгүй байдлын үр дүнтэй арга бол байгууллагад тулгарах аюул занал, эмзэг байдал, эрсдэлийг тодорхойлж иймэрхүү эрсдэлийг үүсгэж болзошгүй нөлөөлөл, магадлалыг урьдчилан тодорхойлох явдал юм. Эрсдэл тодорхойлогдсоны дараа байгууллага нь эдгээр эрсдлийг бууруулахын тулд зохих арга хэмжээг хэрэгжүүлж, тэдгээрийн бизнесийн зорилгыг тэнцвэржүүлж, эдгээр арга хэмжээний өртөг, гарч болох эрсдэл, магадлалыг даван туулах ёстой.

Монгол Улс Кибер аюулгүй байдлыг хангах ажлын хүрээнд ОУ-ын "MITRE" байгууллагатай хамтран сургалт зохион байгуулсан. Уг сургалт нь Кибер аюулгүй байдлыг ханган ажиллах хүний нөөцийн ур чадварыг нэмэгдүүлэхэд чухал ач холбогдолтой юм.

[8]Кибер халдлагад өртөх эрсдлийг багасгахын тулд кибер аюулгүй байдлын үндсэн туршлагаас:

- Програм хангамжийг шинэчилэх.
- Антивирусын хамгийн сүүлийн үеийн програм хангамж суулгах.
- Хүчтэй нууц үг ашиглах.
- Хэрэглэгчийн нэр нууц үг солих.
- Олон хүчин зүйлийн гэрчлэл (MFA) хэрэгжүүлэх. Гэрчлэлт гэдэг нь хэрэглэгчийн таних мэдээллийг баталгаажуулахад хэрэглэгддэг процесс юм.
- Галт хана суулгах.
- Сэжигтэй имэйлд сэрэмжтэй хандах.

Кибер аюулгүй байдлыг хангах үйл ажиллагааны чиглэл:

- Кибер аюулгүй байдлын бодлого, удирдлага, зохион байгуулалт
- Кибер аюулгүй байдлыг хангах техник, технологийн арга хэмжээ.
- Кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, соён гэгээрүүлэх арга хэмжээ.
- Кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, нөхөн сэргээх.

Монгол Улсын Эрх зүйн зохицуулалт

[9]Монгол Улсын Засгийн газраас 2021 оны 06 дугаар сарын 30-ны өдөр өргөн мэдүүлсэн Кибер аюулгүй байдлын тухай хуулийн төсөл болон хамт өргөн мэдүүлсэн хуулийн төслүүдийг Улсын Их Хурлын 2021 оны 12 дугаар сарын 17-ны өдрийн чуулганы нэгдсэн хуралдаанаар хэлэлцэн баталж, кибер аюулгүй байдлыг хангах эрх зүйн үндсийг бүрдүүлсэн.

Кибер аюулгүй байдлын тухай хуулийг 2022 оны 05 дугаар сарын 01-ний өдрөөс эхлэн дагаж мөрдсөн.

Аж үйлдвэрийн дөрөвдүгээр хувьсгалд манай улс үндэсний кибер аюулгүй байдлыг хангах эрх зүйн тогтолцоо, улс орны хөгжил, аюулгүй байдалд түлхэц болох, цаашлаад үндэсний аюулгүй байдлын бүрэлдэхүүн хэсэг болох мэдээллийн аюулгүй байдлаа хангах нөхцөлийг бүрдүүлж байгаа амин чухал хуультай болж байна

Монгол Улсын хувьд Үндэсний аюулгүй байдлын тухай хууль, “Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал”-д мэдээллийн аюулгүй байдлыг үндэсний аюулгүй

[8] https://us.norton.com/blog/malware/what-is-cybersecurity-what-you-need-to-know
[9] https://gratanet.com/laravel-filemanager/files/3/MN-%20Cybersecurity%20Law.pdf

байдлын нэг бүрэлдэхүүн хэмээн тодорхойлсон байдаг ч кибер аюулгүй байдлын индексийн гол үзүүлэлт болох хууль, эрх зүйн орчин бүрдээгүй, үндэсний кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах чиг үүрэг бүхий байгууллага байхгүй, хамтын ажиллагаа сул явж ирсэн байна. Иймхүү хууль батлагдсанаар кибер аюулгүй байдлыг хангах тогтолцоо, эрх зүйн орчин бүрдэж, иргэн, хуулийн этгээд, төрийн байгууллагын кибер аюулгүй байдлыг хангах талаарх эрх, үүрэг нь тодорхой болж, кибер аюулгүй байдлыг хангах үйл ажиллагааг хэрэгжүүлэх, кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийх, хяналт тавих, нэгдсэн удирдлага зохион байгуулалтаар хангах боломж бүрдсэн.

Мөн Зэвсэгт хүчний кибер командлал тайван цагт батлан хамгаалах салбарын хэмжээнд кибер аюулгүй байдлыг хэрхэн хамгаалах зохицуулалтыг хуульд тусгасан.

Эрүүгийн хуулийн 26 дугаар бүлгийн нэр томьёо, гэмт хэргийн бүрэлдэхүүн, ойлголтыг Кибер аюулгүй байдлын тухай хууль, НҮБ-ын Будапештийн конвенцод нийцүүлэн Эрүүгийн хуульд нэмэлт, өөрчлөлт оруулсан.

Түүнчлэн Кибер аюулгүй байдлын тухай хууль батлагдсантай холбогдуулан Зөрчлийн тухай, Харилцаа, холбооны тухай, Зөрчил шалган шийдвэрлэх тухай, Эрүүгийн хэрэг хянан шийдвэрлэх тухай хуульд холбогдох нэмэлт, өөрчлөлтийг тус тус оруулсан болно.

Кибер аюулгүй байдлын тухай хууль 5 бүлэг, 25 зүйлтэй.

Нэгдүгээр бүлэгт

Кибер аюулгүй байдлын тухай хуулийн зорилт, хууль тогтоомжийн бүрдэл, үйлчлэх хүрээ, нэр томъёоны тодорхойлолт, үйл ажиллагааны зарчмыг тусгасан.

Хоёрдугаар бүлэгт

Кибер аюулгүй байдлыг хангах нийтлэг журам, үйл ажиллагааны чиглэл, эрсдлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийлгэх талаар тусгасан.

Гуравдугаар бүлэгт

Кибер аюулгүй байдлыг хангахтай холбоотой төрийн байгууллага, хуулийн этгээд, иргэний эрх, үүргийг тусгасан.

Дөрөвдүгээр бүлэгт

Кибер халдлага, зөрчилтэй тэмцэх төвийн бүтэц, тэдгээрийн чиг үүргийг тусгасан.

Тавдугаар бүлэгт

Кибер аюулгүй байдлын тухай хууль тогтоомж зөрчигчдөд хүлээлгэх хариуцлага, шилжилтийн үеийн зохицуулалт, хууль хүчин төгөлдөр болох талаар тусгасан.

[10]Хуулийн зорилт

1.1.Энэ хуулийн зорилт нь кибер аюулгүй байдлыг хангах үйл ажиллагааны тогтолцоо, зарчим, эрх зүйн үндсийг тогтоох, кибер орон зай, кибер орчин дахь мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг хангахтай холбогдсон харилцааг зохицуулахад оршино.

[10]https://legalinfo.mn/mn/detail?lawId=16390365491061

Хуулийн үйлчлэх хүрээ

Кибер аюулгүй байдлыг хангахтай холбоотой төр, хүн, хуулийн этгээдийн хооронд үүсэх харилцааг уялдуулах зохицуулах, зохион байгуулах, хяналтыг хэрэгжүүлэх харилцаанд үйлчилнэ.

Хуульд өөрөөр заагаагүй бол Монгол Улсын мэдээллийн систем, мэдээллийн сүлжээгээр дамжуулан үйл ажиллагаа явуулж байгаа гадаадын иргэн, харьяалалгүй хүн, гадаадын болон гадаадын хөрөнгө оруулалттай хуулийн этгээдэд энэ хууль нэгэн адил үйлчилнэ.

Хуулийн нэр томьёоны тодорхойлолт

“Кибер аюулгүй байдал”- кибер орчинд мэдээллийн бүрэн бүтэн, нууцлагдсан хүртээмжтэй байдал хангагдсан байхыг хэлнэ.

“Кибер орон зай”- интернет болон бусад мэдээлэл, харилцаа холбооны сүлжээ, тэдгээрийн ажиллагааг хангах мэдээллийн дэд бүтцийн харилцан хамааралтай цогцоос бүрдсэн биет болон биет бус талбар.

“Кибер орчин”- мэдээлэлд хандах, нэвтрэх, цуглуулах, түүнийг боловсруулах, хадгалах, ашиглах боломж олгож байгаа мэдээллийн систем, мэдээллийн сүлжээний орчин.

“Кибер халдлага”- мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдлыг алдагдуулах зорилго бүхий үйлдэл.

"Кибер аюулгүй байдлын зөрчил" - мэдээллийн системийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдалд заналхийлж байгаа аливаа үйлдэл, эс үйлдэх.

“Кибер халдлага, зөрчилтэй тэмцэх төв”- кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, мэдээллийн системийг нөхөн сэргээх үйл ажиллагааг зохицуулж, мэргэжлийн удирдлагаар хангах үндсэн чиг үүрэг бүхий этгээд.

"Кибер аюулгүй байдлын эрсдэлийн үнэлгээ" - цахим мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдал алдагдах, аюул занал тохиолдох магадлал, эмзэг байдлын түвшин, түүнээс үүсэх үр дагавар, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээг тодорхойлох мэргэшсэн үйл ажиллагаа.

“Онц чухал мэдээллийн дэд бүтэцтэй байгууллага”- кибер аюулгүй байдал алдагдсанаар хэвийн үйл ажиллагаа нь доголдож Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулж болох мэдээллийн систем, мэдээллийн сүлжээ бүхий байгууллага.

"Үндэсний хэмжээний кибер халдлага"- онц чухал мэдээллийн дэд бүтэцтэй байгууллагын мэдээллийн систем, мэдээллийн сүлжээнд халдсаны улмаас тухайн байгууллагын хэвийн үйл ажиллагааг алдагдуулж, Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулахуйц кибер халдлаг.

"Төрийн мэдээллийн нэгдсэн сүлжээ"- төрийн байгууллага хоорондын мэдээлэл солилцох, кибер аюулгүй байдлыг хангахад чиглэсэн нэгдсэн дэд бүтэц бүхий төрийн интернэт хэрэглээ, албан болон тусгай хэрэглээний сүлжээний цогц.

[11]Японы Кибер аюулгүй байдлын үндсэн хууль

Япон улсад тус улсын Парламентаас 2014 онд баталсан Цахим аюулгүй байдлын суурь хууль /The Basic Act on Cybersecurity/-аар цахим мэдээллийн аюулгүй байдлын асуудлыг зохицуулсан байдаг.

Тус хуульд төв Засгийн газар болон мужийн захиргаа цахим мэдээллийн аюулгүй байдлыг хангах асуудлаар арга хэмжээнүүд /бодлого/ боловсруулж, хэрэгжүүлэх үүрэг хүлээдэг. Тухайлбал Засгийн газраас Дараах асуудлыг хамарсан үндэсний стратегийг баталж, хэрэгжүүлнэ:

1. Цахим мэдээллийн аюулгүй байдлыг хангах үндсэн зорилтууд;
2. Төрийн байгууллагуудын цахим мэдээллийн аюулгүй байдлыг хангах арга хэмжээнүүд;
3. Онц чухал дэд бүтэцтэй байгууллагууд, тэдгээрийн мэргэжлийн холбоодын цахим аюулгүй байдлыг хангах асуудлыг дамжих арга хэмжээнүүд;
4. Холбогдох бусад бодлогын асуудлууд

Кибер аюулгүй байдлын тухай хууль 4 бүлэг 25 зүйлтэй.

- I бүлэг Ерөнхий заалтууд(1-11 дүгээр зүйл)
- II бүлэг Кибер аюулгүй байдлын стратеги(12-р зүйл)
- III бүлэг Үндсэн бодлого(13-23 дугаар зүйл)
- IV бүлэг Кибер аюулгүй байдлын стратегийн төв байр(24-35 дугаар зүйл)
- Нэмэлт заалтууд

Хуулийн зорилт

Японы кибер аюулгүй байдлын үндсэн бодлогыг тодорхойлох, үндэсний болон орон нутгийн засаг захиргааны хариуцлага зэрэг зүйлийг тодорхой болгох, кибер аюулгүй байдлын стратеги боловсруулах кибер аюулгүй байдлын санаачилгын үндэс болох бусад зүйлсийг хангахад оршино. Мөн түүнчлэн кибер аюулгүй байдлын санаачилгыг Мэдээлэл, харилцаа холбооны дэвшилтэт сүлжээний нийгмийг бүрдүүлэх үндсэн хууль (2000 оны 144-р хууль)-тай уялдуулан Кибер аюулгүй байдлын стратегийн төв байрыг байгуулах зэрэг арга замаар иж бүрэн, үр дүнтэй ахиулах, ингэснээрээ, эдийн засаг, нийгмийн эрч хүчийг нэмэгдүүлж, тогтвортой хөгжилд хүрэх, ард иргэд нь аюулгүй, аюулгүй байдлын мэдрэмжтэй амьдрах нийгмийг бий болгох, түүнчлэн олон улсын хамтын нийгэмлэгийн энх тайван, аюулгүй байдлыг хангахад хувь нэмэр оруулах, Японы үндэсний аюулгүй байдалд хувь нэмэр оруулах. Интернэт болон бусад дэвшилтэт мэдээллийн хөгжлийн чиг үүрэг болгон дэлхийн хэмжээнд үүсч буй дотоод болон гадаад нөхцөл байдлын өөрчлөлт, кибер аюулгүй байдалд заналхийллийн ноцтой байдал нэмэгдэж байгаатай холбогдуулан мэдээллийн чөлөөт урсгалыг хангахын зэрэгцээ аюулгүй байдлыг хангах харилцаа холбооны сүлжээ, мэдээлэл, харилцаа холбооны технологийн хэрэглээ нэмэгдсэн.

[11]https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en#:~:text=Article%2021The%20national%20government,core%20technologies%3B%20the%20development%20of

Кибер аюулгүй байдлын өнөөгийн байдал

Дэлхийн улсууд цахим халдлага, цахим гэмт хэргээс үүдэн 2017 онд 600 тэрбум америк долларын хохирол амсаж байсан бол. 2020 онд ойролцоогоор 10.5 их наяд америк долларын хохирол амссан нь дэлхийн нийт эдийн засгийн 1 хувьтай тэнцэх хэмжээний дүн юм'. Түүнчлэн АНУ-д байрлах Ponemon хүрээлэнгийн судалгаагаар цахим халдлага, цахим гэмт хэргээс үүдэн нэг байгууллага 2017 онд дунджаар 130 цахим халдлагад өртөж 11.7 сая америк долларын, 2020 онд дунджаар 524 цахим халдлагад өртөн 3.86 сая америк долларын алдагдал хүлээжээ.

Тохиолдол

1. [12]Twitter

2020 оны 7-р сарын дундуур Твиттерт spear phishing халдлага гарсан. Кибер гэмт хэрэгтнүүд олон нийтийн сүлжээний админ самбарыг эвдэж, хувийн болон компанийн алдартай Twitter хэрэглэгчдийн дансыг хянаж, тэдний өмнөөс хуурамч биткойны бэлэг тараажээ.

Хакерууд тус компанийн мэдээллийн технологийн хэлтсийн мэргэжилтнүүдээр өөрийгөө таниулж, Twitter-ийн алслагдсан хэд хэдэн ажилчидтай холбогдож, тэдний ажлын дансны итгэмжлэлийг асуусан байна. Эдгээр итгэмжлэлүүд нь халдагчдад нийгмийн сүлжээний администраторын хэрэгсэлд нэвтрэх, олон арван хүмүүсийн Twitter хаягийг шинэчлэх, залилан мэхлэх мессеж нийтлэхэд тусалсан.

Халдлагын төрөл: Phishing attacks (spear phishing)

Энэхүү халдлага нь тодорхой хүмүүст чиглэсэн. Ажилтнуудын хувийн мэдээллийг илүү үнэмшилтэй болгож, биткойн бэлэглэнэ гэх холбоос үүсгэж харилцагчдын дансны мэдээлэл болон хувийн мэдээллийг хулгайлсан.

Хэрхэн урьдчилан сэргийлэх вэ ?

Тодорхой зааварчилгаа бүхий кибер аюулгүй байдлын бодлогыг бий болгох нь чухал. Байгууллагууд ажилтнуудаа уг бодлогын үндсэн дүрмийг бүрэн ойлгож, кибер аюулгүй байдлын талаарх ерөнхий ойлголтыг нэмэгдүүлэхийн тулд тогтмол сургалт явуулж байх ёстой. Ажилтнууд нууц үгээ хэрхэн, ямар нөхцөлд шинэчилж болохыг мэддэг бол луйварчдын урхинд орох магадлал бага байх болно.

Хэрэглэгчид нь ихэвчлэн хамгийн чухал систем, өгөгдөлд хандах эрхтэй байдаг тул давуу эрхтэй бүртгэлүүд нэмэлт хамгаалалт шаарддаг. Хэрэв хакерууд ийм данс руу нэвтэрч орвол тухайн байгууллагын аюулгүй байдал, нэр хүндэд үзүүлэх үр дагавар нь аймшигтай.

2. Microsoft Word

Хамгийн анхны бөгөөд хамгийн том кибер аюулын нэг нь 1999 онд программист Дэвид Ли Смитийн Мелисса вирусаас үүдэлтэй юм. Тэрээр вирус агуулсан Microsoft Word-ээр дамжуулан хэрэглэгчдэд нээх файл илгээсэн. Вирус нээгдсэний дараа идэвхжиж, Microsoft зэрэг олон зуун компаниудад ноцтой хохирол учруулсан. Нөлөөлөлд өртсөн системийг засварлахад 80 сая доллар зарцуулсан гэсэн тооцоо бий.

[12] https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches

Халдлагын нэр : The Melissa Virus

Вирус нь ихэвчлэн "[хэрэглэгчийн нэр]-ээс ирсэн чухал мессеж" гэсэн гарчигтай, хүлээн авагчийг хавсаргасан баримт бичгийг нээхийг уриалсан мессеж бүхий цахим шуудангаар тараагддаг.

Хэрхэн урьдчилан сэргийлэх вэ ?

Үл мэдэгдэх эсвэл сэжигтэй эх сурвалжаас имэйл хавсралт нээх эрсдэлийн талаар хэрэглэгчдэд сургах. Гэнэтийн эсвэл хүсээгүй имэйлүүд, ялангуяа хавсралттай имэйлүүдэд үл тоох .

Дүгнэлт

Орчин үеийн кибер болон мэдээлийн аюулгүй байдал нь дээрхи хэдэн чиглэлийн халдлагуудаар хязгаарлагдахгүй бөгөөд цаашид улам бүр арга, хэрэгсэл нь нарийн болж өсөн нэмэгдэх хандлагатай байна. Тиймээс бид интернэт ашиглах, харилцаа холбооны сүлжээнд холбогдохдоо өөрийн хувийн болон бусад чухал мэдээллийг хамгаалахын тулд нэн түрүүнд энгийн логикоор тайлагдахгүй нууц үг хийх, бусад шаардлагатай лицензтэй программ хангамж ашиглах хэрэгтэй. Кибер ертөнцөд өөрийгөө болон бизнесээ хамгаалах нэг чухал зүйл нь няхуур, болгоомжтой байх. Кибер халдлагын талаар мэдлэг мэдээлэлтэй байх нь халдлагад өртөх эрсдлийг бууруулж чадна. Кибер аюулгүй байдал нь кибер бүх халдлагаас 100 хувь хамгаалахгүй ч олон төрлийн аюулаас хамгаалж чадна, түүнд хариу арга хэмжээг үзүүлэх болно. Кибер халдлага өсөн нэмэгдэхийн хэрээр кибер аюулгүй байдал ч мөн адил өөрчлөгдөж байна.

Ямар ч тохиолдолд эрсдэл байх болно. Эрсдэл учирч хэвийн үйл ажиллагаа алдагдсан тохиолдолд хурдан сэргээх боломжит нөхцөлийг бүрдүүлэх, хариу арга хэмжээг авч байх шаардлагатай. Бизнесийн байгууллага нь үйл ажиллагааны шат бүрдээ эрсдэлийн үнэлгээ хийж кибер аюулгүй байдлыг дээр дурдсан алхмуудын дагуу хэрэгжүүлэх нь халдлагаас урьдчилан сэргийлэх, учирч болзошгүй эрсдэлийг бууруулна.

Монгол Улсад кибер аюулгүй байдлын тухай хууль жилийн өмнө батлагдаж, хэрэгжиж эхлээд жил ч болоогүй байгаа тул харьялагдаагүй талбар ихтэй.

Хувь хүн бүр кибер аюулгүй байдлын тухай мэдлэг, мэдээлэлтэй байх. Байгууллага бүр кибер аюулгүй байдал болон мэдээллийн аюулгүй байдлын тогтолцоог хэрэгжүүлэх шаардлагатай.

Ашигласан эх сурвалж

https://old.legalinfo.mn/law/details/17088?lawid=17088

https://www.paloaltonetworks.com/cyberpedia/cyber-security

https://www.aura.com/learn/types-of-cyber-attacks

https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

https://www.britannica.com/topic/cybercrime

https://en.wikipedia.org/wiki/Cybercrime

https://www.parliament.mn/nn/16476/

https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches

https://www.japaneselawtranslation.go.jp/en/laws/view/3677/en#:~:text=Article%2021The%20national%20government,core%20technologies%3B%20the%20development%20of