Компьютерын аюулгүй байдал

Компьютерын аюулгүй байдал (**Кибер аюулгүй байдал**, **Мэдээллийн технологийн (IT) аюулгүй байдал** ч гэдэг) нь систем, сүлжээ, өгөгдлийг кибер аюул заналхийллээс хамгаалахад зориулсан технологи, үйл явц, арга хэмжээ.

Эдгээр кибер аюул нь маш олон хэлбэртэй байдаг ба нарийн төвөгтэй халдлагууд нэмэгдсээр байгаа тул кибер аюулгүй байдлын стратеги болон үйл ажиллагаатай нягт уялдаатай байдал нь засгийн газар, аж ахуйн нэгжүүдэд маш чухал болсон. Өнөө үед кибер аюул занал нь улс үндэстэн, ард түмний нууц, улс төр, цэргийн эсвэл дэд бүтцийн хөрөнгөд чиглэх болсон ба үүнтэй уялдуулаад кибертерроризм (*cyberterrorism*), кибер дайн (*cyberwarfare*), кибер тагнуул (*cyberespionage*), кибер халдлага (*cyberattack*) гэх мэт ойлголтууд түгээмэл болсон.

Кибер халдлага нь ихэвчлэн хулгай (төлбөрийн картын өгөгдөл, хэрэглэгчийн мэдээлэл, компаний нууцлал эсвэл оюуны өмчийн), сүлжээнд зөвшөөрөлгүй нэвтрэх, албан тушаалтныг бүртгэл буюу санхүүгийн болон нэр хүндэд хохирол учруулах зорилгоор ашигладаг.

Компьютерын аюулгүй байдлыг хангах

Байгууллага, засгийн газрууд кибер аюул заналыг устгахад чиглэсэн "цэгийн бүтээгдэхүүн" хандлагыг авч, өөрсдийн аюулгүй байдлын технологиудыг нэг нэгнийхээ эсрэг холбож, өөрсдийн сүлжээг болон түүний дотор үнэ цэнэтэй өгөгдлийг хамгаалахын төлөө тэмцэж байна. Энэхүү арга нь үнэтэй, төвөгтэй боловч тодийгүй ихээхэн аюултай кибер зөрчлийн тухай мэдээлэл гарчигтай хэвээр байна. Үнэн хэрэгтээ, өгөгдлийн зөрчлийн тархалтаас шалтгаалан кибер аюулгүй байдлын сэдэв нь илүү эрсдэлтэй арга замыг эрэлхийлж байгаа захирлуудын зөвлөлийн хувьд тэргүүлэх ач холбогдол бүхий жагсаалтыг нээлээ.Үүний оронд байгууллага нь нэгдсэн, автоматжуулсан Дараагийн-үеийн аюулгүй байдлын платформыг байгуулж болох бөгөөд үүнд төгсгөлийн цэг, мэдээллийн төв, сүлжээ, нийтийн болон хувийн үүл, SaaS орчинд. Байгууллага нь урьдчилан сэргийлэлтийн асуудалд анхаарлаа хандуулах замаар сүлжээнд нөлөөлж, кибер аюулгүй байдлын ерөнхий эрсдэлийг удирдах түвшинд хүргэхээс сэргийлж чадна.

Яагаад кибер гэмт хэрэг нэмэгдэж байна вэ?

- **Кибер гэмт хэрэгтнүүдийг ялгаварлан гадуурхдаг**. Хэрэв сул тал байгаа бол түүнийг ашиглахыг хичээнэ.Санхүүгийн асар их орлого олсоны улмаас кибер гэмт хэрэг олон тэрбум фунт үйлдвэртэй болсон.
- **Кибер гэмт хэрэг байнга өөрчлөгдөж байдаг**. Кибер халдлагууд илүү төвөгтэй болж, байгууллагууд өөрчлөлтийн хурдыг дагахын төлөө тэмцэж байна.
- **Кибер халдлага нь** янз бүрийн хэлбэрээр хийгддэг бөгөөд зөвхөн технологийн сул талуудыг (жишээ нь хуучирсан програм хангамж) чиглүүлэхээс гадна хүмүүсийг (жишээлбэл, хортой холбоосууд дээр дардаггүй мэдээлэлгүй

ажилтнууд), зохион байгуулалтын үйл явц, процедурын дутагдалтай талыг ашиглах зорилготой юм.

Халдлага

Ач холбогдол

Кибер аюулгүй байдал нь өсөн нэмэгдэж буй технологийн хурдацтай хөгжил, мэдээллийн эрин зуунд үүсч буй зайлшгүй шаардлага болсноос гадна бизнесийн алдагдал хүлээх эрсдлийг бууруулах чухал ач холбогдолтой.

Кибер аюулгүй байдал нь засгийн газар, цэрэг, корпораци, санхүүгийн болон эмнэлгийн байгууллагууд компьютер болон бусад төхөөрөмжүүд дээр урьд өмнө байгаагүй хэмжээний мэдээллийг цуглуулж, боловсруулж, хадгалахад чухал ач холбогдолтой юм. Мэдээллийн ихээхэн хэсэг нь оюуны өмч, санхүүгийн мэдээлэл, хувийн мэдээлэл эсвэл зөвшөөрөлгүй хандалт, өртөгт сөрөг үр дагавартай байж болох өөр төрлийн өгөгдөл байж болох эмзэг мэдээлэл байж болно. Байгууллага нь аж ахуйн үйл ажиллагааны явцад сүлжээгээр болон бусад төхөөрөмжүүдийн хооронд эмзэг өгөгдлийг дамжуулдаг бөгөөд кибер аюулгүй байдал нь тухайн мэдээллийг хамгаалах, түүнийг боловсруулж ашиглахад зориулсан систем юм. Кибер довтолгооны тоо хэмжээ, нарийн төвөгтэй байдал өсөхийн хэрээр компаниуд, ялангуяа үндэсний аюулгүй байдал, эрүүл мэнд, санхүүгийн бүртгэлтэй холбоотой мэдээллийг хамгаалах үүрэг хүлээдэг компаниуд, тэдгээрийн эмзэг бизнесийн болон боловсон хүчний мэдээллийг хамгаалах алхмуудыг хийх хэрэгтэй байна.

Кибер аюулгүй байдлыг хэрхэн сайжруулах вэ?

- Кибер аюулгүй байдлын гурван үндсэн зүйл бол хүмүүс, үйл явц, технологи юм.
- 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.
- Эрсдлийг тодорхойлсоны 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.

Кибер аюулгүй байдлын сорилтууд

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

- Сүлжээний аюулгүй байдал
- Програмын аюулгүй байдал
- Endpoint аюулгүй байдал
- Өгөгдлийн аюулгүй байдал
- Өгөгдлийн аюулгүй байдал
- Cloud аюулгүй байдал
- Гар утасны аюулгүй байдал
- Гамшгийн сэргээх / бизнесийн тасралтгүй ажиллагааны төлөвлөлт
- Эцсийн хэрэглэгчийн боловсрол

Кибер аюулгүй байдлын хамгийн хэцүү сорилт нь аюулгүй байдлын байнгын өөрчлөгдөж байдаг шинж чанар юм. Уламжлал ёсоор бол байгууллага, засгийн газар кибер аюулгүй байдлын нөөцийг ихэнхдээ хамгаалалтанд байлгахын тулд хамгийн чухал системийн бүрдэл хэсгүүдийг хамгаалах, мэддэг эмчилгээнээс хамгаалж чаддаг. Өнөө үед энэ арга барил нь хангалтгүй байгаа бөгөөд байгууллагаас илүү аюул заналхийлж, түргэн өөрчлөгдөнө. Үүний үр дүнд зөвлөх байгууллагууд кибер аюулгүй байдлыг илүү идэвхтэй, дасан зохицох арга барилыг дэмжинэ. Үүний нэгэн адил, Үндэсний Стандарт Технологийн Хүрээлэн (NIST) нь уламжлалт периметрт суурилсан загвартай харьцуулахад аюулгүй байдлын өгөгдөлд чиглэсэн арга барилыг тасралтгүй хянах, бодит хугацааны үнэлгээнд шилжихийг зөвлөж байна.

Халдлагын чиглэл

Түүнчлэн кибер гэмт хэрэгтэнд халдаж болох хэд хэдэн векторууд байдаг бөгөөд тэдгээр нь хортой програмыг компьютерт халдварлах эсвэл хулгайлсан өгөгдлийг устгах боломжтой байдаг. Үүнд:

- **Social engineering /нийгмийн боловсруулалт/** - Хувь хүний сул талыг ашиглах, тэдгээрийг хортой холбоос дээр дарах, эсвэл хууран мэхлэх замаар компьютерт нэвтрэх эрхээ олж авдаг. Phishing болон pharming-д нийгмийн боловсруулалтын жишээ байдаг.
- **Phishing /өгөөш хаях замаар хохирогчоо удирддаг/** – Хэрэглэгчийн мэдээллийг олж авахыг оролдох нь хууль ёсны аж ахуйн нэгжийг хуурамчаар үйлдэх оролдлого юм.
- **Pharming /интернэт залилан/** – Вэбсайтын урсгалыг өөр өөрөөр дахин чиглүүлэх халдлага ба хуурамч вэбсайт болон хувь хүний мэдээллийг дараа нь эвддэг.
- **Drive-by /жолоодох/** - Систем доторх тодорхой сул талуудтай холбоотой оппортунист халдлага.
- **Man in the middle /дундын хүн/** - Дундын хүн бүр төгсгөлийн цэгийг дуурайдаг бөгөөд хохирогчид хоёуланг нь удирдах боломжтой халдлага.

Халдлага гарах орчин

- Хортой програмуудаар (Хортой код) дамжин халдах
- Цахим шуудан, мессежээр дамжин халдах
- Цахим хуудас (web page) нийтийн сүлжээгээр дамжин халдах
- Нууц үг эвдэх
- Төлбөртэй програмуудыг эвдэж ашиглах

Хортой код, програмууд

Кибер гэмт хэрэгтнүүд олон тооны хортой програмууд болон векторуудыг зорилгодоо хүрэхийн тулд ашигладаг:

- **Malware**
  - Malware нь гэмт хэрэгтнүүдийн зорилгодоо хүрэх боломжийг олгодог программ хангамжийн төрөл бөгөөд үүнийг дараах байдлаар ангилж болно.
- **Ransomware**
  - Ransomware нь компьютерийн систем дээр кибер халдлагыг эхлүүлсний дараа төлбөрийг шаарддаг хортой програмын төрөл юм. Энэ төрлийн хорт програм нь гэмт хэрэгтний дунд түгээмэл болж, жил бүр сая сая байгууллагыг зардаг.
- **Viruses (Вирус)**
  - Вирус нь нэг компьютерээс нөгөө компьютерт өөрөө өөрийгөө хуулбарлах боломжтой жижиг хэмжээний код юм.
- **Worms (Өт)**
  - Өтнүүд өөрсдийгөө хуулбарлах, өөрсдийгөө хавсаргах хөтөлбөр шаарддаггүй. Хулгайн эмгэгүүдийг байнга хайж, сул талыг олж илрүүлэх үед өтнүүд зохиогчдод мэдээлдэг.
- **Spyware/adware**
  - Хавсралтыг нээхдээ холбоос дээр дарах эсвэл халдвартай програмыг татаж авахдаа компьютер дээрээ Spyware / adware-г суулгаж болно.
- **Trojans**
  - Трояны вирус нь нэг функц (жишээлбэл, вирус арилгах) мэт харагддаг програм боловч яг үнэндээ үйлдэл хийх үед хортой үйлдлийг гүйцэтгэдэг.

Palo Alto Networks Next-Generation Security Platform

Palo Alto сүлжээний дараагийн үеийн аюулгүй байдлын платформ

Урьдчилан сэргийлэх

- Файлын эх сурвалжийг шалгах
- Antivirus-ны програм байнга ашиглах, тогтмол update хийх
- Флаш диск зэрэг зөөврийн хадгалах төхөөрөмжүүдийг компьютерт шалгахгүйгээр залгахгүй байх

- Гадны нээлттэй сүлжээнд аль болох холбогдохгүй байх (хувийн виртуал сүлжээ хэрэглэхээс бусад тохиолдолд)
- Laptop, зөөврийн төхөөрөмж дэх чухал мэдээллийг шифрлэх, хараа хяналтгүй үлдээхгүй байх
- Интернет хандалтын аюулгүй байдлыг хангах

ISO 27001 ба кибер аюулгүй байдал

- ISO 27001 нь мэдээллийн аюулгүй байдлын менежментийн олон улсын хэмжээнд хүлээн зөвшөөрөгдсөн шилдэг практик стандарт юм.
- ISO 27001-ийг хэрэгжүүлснээр таны бизнесийн мэдээллийг хамгаалах, мэдээллийн аюулгүй байдлыг хангахтай холбоотой зохицуулалтын үүргээ биелүүлж, кибер аюулгүй болгоход шаардлагатай арга хэмжээг авсан хэрэглэгч, сонирхогч талуудад баталгаа өгөх болно.

Кибер аюулгүй байдлын олон улсын стандарт

- Кибер аюулгүй байдлын тухай үндсэн ойлголтууд, тэдгээрийн мэдээллийн аюулгүй байдлын хүрээний бусад ойлголтуудтай хэрхэн уялдаатай байх зэргийг багтаасан ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity, олон улсын стандартыг эрх бүхий байгууллагаас 2012 оны 7 дугаар сараас батлан гаргасан байна.
- Энэ стандартад cybersecurity (кибер аюулгүй байдал) гэсэн нэр томьёо болон сүлжээний аюулгүй байдал, хэрэглээний аюулгүй байдал, интернетийн аюулгүй байдал, онц чухал дэд бүтцүүдийн аюулгүй байдал гэсэн нэр томьёонуудын ялгааг барууны мэргэжилтнүүдийн байр суурьнаас тодорхой зааж өгсөн гэж үзэж болохоор байна.