MUNKH INSURANCE

КИБЕР ЭРСДЭЛИЙН ДААТГАЛЫН ТАНИЛЦУУЛГА

XX Anniversary

MUNKH INSURANCE

Anniversary

НЭГ. МОНГОЛ УЛСЫН ӨНӨӨГИЙН КИБЕР ЭРСДЭЛИЙН ТАЛААР

Монгол улс дахь кибер халдлагыг тоон үзүүлэлтээр авч үзвэл

7 ХОНОГТ ДУНДЖААР **8000** гаран удаагийн **ХАЛДЛАГА** бүртгэгддэг.

Үүнийг эрсдэлээр нь ангилж авч үзвэл:

- **71%** нь malware буюу компьютерт хор хөнөөл учруулдаг код
- **20%** нь кибер аюулгүй байдлын сул талыг хайх
- **4%** нь олсон сул талаа ашиглах
- **2%** нь нууц үг тайлах оролдлого
- **3%**-д нь бусад халдлагууд багтдаг байна.

Бүртгэгсэн кибер гэмт хэргүүдийг авч үзвэл
2024 оны байдлаар 5284 кибер гэмт хэрэг бүртгэгдсэнээс 193 нь
“Кибер аюулгүй байдлын эсрэг” буюу хамгаалалтын эсрэг гэмт хэрэг байна.

Кибер халдлагыг эрсдэлийн төрлөөр нь авч үзвэл:

Дотроос үүсэх кибер халдлагын эрсдэл

- Ажилтны санаатайгаар учруулах эрсдэл - Энэ нь компанийн дотоод мэдээллийг тухайн ажилтан санаатайгаар устгах, бусдад тараах, дамжуулан борлуулахыг хэлнэ.
- Мэдлэг, туршлага дутмаг ажилтны учруулах эрсдэл - Энэ нь тухайн ажилтан мэдлэг, туршлага дутмагаасаа болж компанийн дотоод мэдээлэл, датаг алдахыг хэлнэ.

Гаднаас үүсэх кибер халдлагын эрсдэл

- Гадаад болон дотоодын Хакерууд болон Хактивистуудын учруулах эрсдэл
- Кибер гэмт хэргийн байгууллагаас халдлага үйлдэх, Ransomware буюу өгөгдөл, мэдээлэл, болон дотоод програм хангамжийг барьцаалах
- Олон улсын нөлөөлөлөөс үүдэлтэй халдлагууд

Технологи болон үйл ажиллагааны дутагдлаас үүсэх эрсдэл

- Тодорхой бус эсвэл засварлагдаагүй програм хангамжийн сул талаас үүдэх эрсдэл
- Кибер аюулгүй байдал муу
- Системийн буруу тохиргоо
- Кибер аюулгүй байдлын талаарх мэдлэг дутмаг

Уламжлалт арга барилаар халдах кибер халдалгууд

- Зөөврийн компьютер эсвэл компьютер өгөгдөл хадгалах төхөөрөмж хулгайд өртөх
- Нууц үг, логин- ыг хүчээр тааруулах
- Social инженерчлэл буюу таны итгэдэг хэн нэгний дүрд хувирч халдах
- Фишинг буюу имэйл халдлага, залилан

MUNKH INSURANCE

Anniversary

Танай байгууллага Кибер эрсдлийн даатгалд бэлэн үү?

ГҮЙЦЭТГЭХ ЗАХИРЛЫН ХУВЬД:

Өөрийн байгууллагын кибер аюулгүй байдал ямар түвшинд байгааг мэдэхгүй?

САНХҮҮ ХАРИУЦСАН ЗАХИРЛЫН ХУВЬД:

Кибер халдлагад өртөхөд хэр хэмжээний санхүүгийн хохиролд учрахыг мэдэхгүй?

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЗАХИРЛЫН ХУВЬД:

Бидэнд хангалттай чадварлаг нөөц, шаардлагатай төсөв байгаа юу?

Дээрх бүх тодорхойгүй асуудлуудыг даатгалд хамрагдахаас өмнө "SELF ASSESSMENT TOOL" тодорхойлох ба эрсдэлийн үнэлгээ нь даатгалын хураамжид багтана.

ДААТГАЛЫН ҮНЭЛГЭЭ ХУРААМЖ

Кибер эрсдэлийн даатгалын үнэлгээ нь Даатгагч, Даатгуулагч талуудын харилцан тохиролцож тогтоосон мөнгөн дүн байна.

Даатгуулагчтай байгуулсан кибер эрсдэлийн даатгалын гэрээг олон улсын зах зээлд 100% давхар даатгуулж байршуулна.

Даатгалын гэрээ, андеррайтингийн нөхцөлийг давхар даатгалын зуучлагч, давхар даатгагчаас ирүүлсний

НӨХӨН ТӨЛБӨР

Бизнес тасалдал болон нэмэлт зардал	Бизнесийн эргэлтийн бууралт, ажлын өртөг нэмэгдэх (кибер халдлагын санхүүгийн нөлөөллийг бууруулахын тулд гэрээлэгч эсвэл тоног төхөөрөмж хөлслөх)
Кибер барьцааны төлбөр	Барьцааны төлбөрийг төлөх болон тухайн арга хэмжээний хувьд мэргэжлийн болон хуулийн зөвөлгөө авах мэргэжилтний төлбөр.
Халдлагын хариу арга хэмжээний зардал	Зохих мэргэжилтнүүдын зардал (Цахим шинжээч, ПР/Хямралын менежмент, breach coaches) болон кибер халдлагаас үүдэх хохирлын хэмжээг багасгах гуравдагч этгээд.
Мэдээлэлийн зөрчил удирдахад гарсан зардал	Хууль эрх зүйн болон мөрдөн байцаалтын зардал, мэдэгдлийн зардал, Зээлийн хяналт зэрэг хэрэглэгчийн дэмжлэгийн зардал
Цахим хөрөнгийн зардал	Цахим тоног төхөөрөмж / Дата бааз / Аппликэйшн / Софтвайр болон үйлдлийн системийг дахин суулгах, ачаалуулал нэмэт зардал
Гуравдагч этгээдийн өмнө хүлээх зардал	Кибер халдлагын үр дүнд гуравдагч этгээдийн нэхэмжлэл эсвэл зохицуулалтын үйл ажиллагааны улмаас үүссэн хамгаалалтын зардал ба/эсвэл хохирол
Зохицуулалт ба хууль эрх зүй	Мөрдөн байцаалтын зардал, хууль эрх зүйн дэмжлэг болон (хуулиар даатгуулсан бол), торгууль.
Нөхөн төлбөр бэлдэх зардал	Кибер халдлагын дараа хохирол үнэлэгч, шинжээч ба мэргэжилтэн томилох зардал.

НЭМЭЛТЭЭР ДААТГАХ БОЛОМЖТОЙ ЭРСДЭЛҮҮД

САЙЖРУУЛАХ
Кибер халдлагад өртсөн системыг засварлах, сайжруулах, солих зардал.

ОРЛУУЛАХ
Кибер халдлагын улмаас ашиглах боломжгүй болсон тоног төхөөрөмжийг шинээр худалдан авах болон суурьлуулах зардал.

НЭР ХҮНДЭД УЧРАХ ЗАРДАЛ
Кибер халдлагын улмаас компанийн брэнд болон нэр хүнд алдагдаж бизнес тасалдах зардал

MUNKH INSURANCE

Anniversary

КИБЕР ЭРСДЭЛИЙН ДААТГАЛЫН ДАВУУ ТАЛУУД

Кибер эрсдэлийн даатгал хийлгэхээс өмнө Олон улсын кибер аюулгүй байдлын стандарт, шаардлагыг хангасан байх шаардлагатай буюу холбогдох кибер аюулгүй байдлын үнэлгээг үнэ төлбөргүй хийж өгнө. Танай байгууллага уг үнэлгээг хийлгэснээр кибер аюулгүй байдын одоогийн нөхцөл байдлаа ойлгохоос гадна сайжруулах боломжтой.

Энэ даатгалд дагалдах нэмэлт үйлчилгээ болох Хакерын эсвэл аливаа кибер зөрчлийг сүлжээ болон системээс олж илрүүлэх, тусгаарлах, арилгах үүрэгтэй тусгай мэргэжлийн олон улсын баг хариуцан ажиллана.

Мөн энэ даатгалд дагалдах 2дахь нэмэлт үйлчилгээ нь Хуулийн зөвлөх үйлчилгээ
- Мэдээллийн зөрчилтэй холбоотой зохицуулалт, хариуцлагын асуудлаар зөвлөгөө өгнө.

3дахь нь Олон нийтийн харилцах зардлыг даатгалаар даана
- Зөрчлийг олон нийтэд мэдээллэх, ил болгох стратеги боловсруулах зардлыг хариуцна.

Харилцагч, хөрөнгө оруулагч, ажилчдын хувийн мэдээлэл задарсантай холбоотой аливаа залилан, мэхлэх үйлдэлээс хохирсон гурдагч этгээдүүдэд зориулан Credit monitoring буюу Зээлийн мэдээллийг хянах үйлчилгээг даатгалаас дааж гаргана.

24/7 халдлага , зөрчлийн үеийн сервис үйлчилгээ.
Бид кибер аюулгүй байдлын олон улсын мэргэжилтэнгүүдтэй хамтран ажилладаг бөгөөд эрсдэл, халдлага, зөрчил гарсан тохиолдолд танд туслах, эсрэг хариу үйлдэл үзүүлэх, удирдан чиглүүлэхэд хэзээд бэлэн байна.

Мөн Ransomware буюу мэдээлэл өгөгдлийг барьцаалсан тохиолдолд тохиролцоо хийх, төлбөр төлөх үйлчилгээ зэрэг давуу талууд багтана.

ХОЁР. “КИБЕР АЮУЛГҮЙ БАЙДЛЫН ТУХАЙ” хуулиас

"төрийн мэдээллийн нэгдсэн сүлжээ"	4.1.17."төрийн мэдээллийн нэгдсэн сүлжээ" гэж төрийн байгууллага хоорондын мэдээлэл солилцох, кибер аюулгүй байдлыг хангахад чиглэсэн нэгдсэн дэд бүтэц
"кибер орон зай"	4.1.2. "кибер орон зай" гэж интернэт болон бусад мэдээлэл, харилцаа холбооны сүлжээ, тэдгээрийн ажиллагааг хангах мэдээллийн дэд бүтцийн харилцан хамааралтай цогцоос бүрдсэн биет болон биет бус талбар;
"кибер орчин"	4.1.3. "кибер орчин" гэж мэдээлэлд хандах, нэвтрэх, цуглуулах, түүнийг боловсруулах, хадгалах, ашиглах боломж олгож байгаа мэдээллийн систем, мэдээллийн сүлжээний орчныг;
"бүрэн бүтэн байдал"	4.1.4."бүрэн бүтэн байдал" гэж мэдээллийг зөвшөөрөлгүй устгах, өөрчлөхөөс хамгаалсан байхыг;
"нууцлагдсан байдал"	4.1.5."нууцлагдсан байдал" гэж мэдээлэлд зөвшөөрөлгүй хандах, нэвтрэх боломжгүй байхыг;
"хүртээмжтэй байдал"	4.1.6."хүртээмжтэй байдал" гэж зөвшөөрөгдсөн хүрээнд мэдээлэлд хандах, нэвтрэх, цуглуулах, ашиглах боломжтой байхыг;
"мэдээллийн систем"	4.1.7."мэдээллийн систем" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.1-д заасныг;
"мэдээллийн сүлжээ"	4.1.8."мэдээллийн сүлжээ" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.2-т заасныг;
"кибер аюулгүй байдлын эрсдэлийн үнэлгээ"	4.1.9."кибер аюулгүй байдлын эрсдэлийн үнэлгээ" гэж 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 ажиллагааг;
"мэдээллийн аюулгүй байдлын аудит"	4.1.10."мэдээллийн аюулгүй байдлын аудит" гэж кибер аюулгүй байдлын хууль тогтоомж, холбогдох журам, стандартад нийцсэн эсэхэд дүгнэлт гаргах, зөвлөмж өгөх хараат бус хөндлөнгийн мэргэжлийн үйл ажиллагааг
"мэдээллийн системийн үйлдлийн бүртгэл"	4.1.11."мэдээллийн системийн үйлдлийн бүртгэл" гэж тухайн мэдээллийн системд хандсан, нэвтэрсэн, боловсруулсан, цуглуулсан, ашигласан үйлдэл, цаг хугацааг тодорхойлох бүртгэлийг;
"онц чухал мэдээллийн дэд бүтэцтэй байгууллага"	4.1.12."онц чухал мэдээллийн дэд бүтэцтэй байгууллага" гэж 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 байгууллагыг
"кибер аюулгүй байдлын зөрчил"	4.1.13."кибер аюулгүй байдлын зөрчил" гэж мэдээллийн системийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдалд заналхийлж байгаа аливаа үйлдэл, эс үйлдлийг;
"кибер халдлага"	4.1.14."кибер халдлага" гэж мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдлыг алдагдуулах зорилго бүхий үйлдлийг;
"үндэсний хэмжээний кибер халдлага"	4.1.15."үндэсний хэмжээний кибер халдлага" гэж 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 халдлагыг;
"кибер халдлага, зөрчилтэй тэмцэх төв"	4.1.16."кибер халдлага, зөрчилтэй тэмцэх төв" гэж 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 этгээдийг;

ХОЁР. “КИБЕР АЮУЛГҮЙ БАЙДЛЫН ТУХАЙ” хуулиас

"төрийн мэдээллийн нэгдсэн сүлжээ"

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

Кибер аюулгүй байдлыг хангах үйл ажиллагааны зарчим

1. “Үндэсний аюулгүй байдлын тухай” хуулийн 4 дүгээр зүйл-д заасан:
Үндэсний аюулгүй байдлыг хангах үйл ажиллагааны үндсэн зарчим
4.1.Үндэсний аюулгүй байдлыг хангах үйл ажиллагаанд дараахь үндсэн зарчмыг баримтална:
4.1.1.улс, үндэснийхээ язгуур ашиг сонирхлыг эрхэмлэх;
4.1.2.хүний эрх, эрх чөлөөг хамгаалах;
4.1.3.хууль дээдлэх;
4.1.4.нэгдмэл, харилцан уялдуулан зохицуулагдсан байх;
4.1.5.шуурхай, тасралтгүй байх;
4.1.6.бодит мэдээлэлд үндэслэх;
4.1.7.төрийн байгууллага, иргэд харилцан хариуцлага хүлээх;
4.1.8.үндэсний эв нэгдлийг эрхэмлэх;
4.1.9.нээлттэй байх. гэж зааснаас гадна

2. “Кибер аюулгүй байдлын тухай” хуулийн дараах зарчмыг баримтална:
5.1.1.нэгдмэл удирдлагатай байх;
5.1.2.шинжлэх ухаан, дэвшилтэт техник, технологи, инновацад тулгуурласан байх;
5.1.3.үндэсний бүтээгдэхүүн, үйлчилгээ, хүний нөөцийн чадавхыг дэмжих;
5.1.4.эрсдэлийн үнэлгээнд тулгуурлах;
5.1.5.төр, хувийн хэвшлийн түншлэлд тулгуурлах;
5.1.6.олон улсын хамтын ажиллагааг хөгжүүлэх.

Кибер аюулгүй байдлыг хангах үйл ажиллагааны чиглэл

6.1.Кибер аюулгүй байдлыг хангах үйл ажиллагааг дараах чиглэлээр хэрэгжүүлнэ:
6.1.1.кибер аюулгүй байдлын бодлого, удирдлага, зохион байгуулалт;
6.1.2.кибер аюулгүй байдлыг хангах техник, технологийн арга хэмжээ;
6.1.3.кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, соён гэгээрүүлэх арга хэмжээ;
6.1.4.кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, нөхөн сэргээх арга хэмжээ.

8 дугаар зүйл. Кибер аюулгүй байдлын эрсдэлийн үнэлгээ

8.1.Кибер аюулгүй байдлын эрсдэлийн үнэлгээг цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад бүртгүүлсэн хуулийн этгээд хийнэ.

8.2.Энэ хуулийн 8.1-д заасан хуулийн этгээд нь олон улсын мэргэжлийн холбоо, стандартын байгууллага, эсхүл түүнтэй дүйцэхүйц байгууллагаас олгосон хүчин төгөлдөр гэрчилгээ бүхий орон тооны ажилтантай байна.

8.3.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх журам, аргачлалыг цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага тагнуулын байгууллагатай хамтран батална.

8.4.Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон байгууллага болон онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээдийн кибер аюулгүй байдлын эрсдэлийн үнэлгээг тагнуулын байгууллага, эсхүл түүний зөвшөөрснөөр энэ хуулийн 8.1-д заасан хуулийн этгээд хийнэ.

8.5.Энэ хуулийн 8.1-д заасан хуулийн этгээд болон кибер аюулгүй байдлын эрсдэлийн үнэлгээний тайланг хүлээн авсан холбогдох байгууллага, албан тушаалтан нууцлалыг чандлан хадгалж, задруулахгүй байх үүрэг хүлээнэ.

ГУРАВ . “АЛСЫН ХАРАА-2050” МОНГОЛ УЛСЫН УРТ ХУГАЦААНЫ ХӨГЖЛИЙН БОДЛОГЫН ХҮРЭЭНД 2021-2030 ОНД ХЭРЭГЖҮҮЛЭХ ҮЙЛ АЖИЛЛАГАА-с

ДӨРӨВ.ЭДИЙН ЗАСАГ
Ухаалаг санхүүгийн зах зээл

АЛСЫН ХАРАА 2050

Зорилт 4.3.

Олон улсын санхүүгийн зах зээлтэй холбогдсон, олон тулгуурт, хүртээмжтэй санхүүгийн системийг хөгжүүлнэ.

4.3.5.Даатгалын зах зээлийн тогтвортой байдлыг хангах, системийн эрсдэлээс урьдчилан сэргийлэх тулгуур зарчмуудыг баримтална.

4.3.6.Даатгалын зах зээлийн тогтвортой байдлыг хангах, системийн эрсдэлээс урьдчилан сэргийлэх зорилгоор эрсдэлийн удирдлагын зохицуулалтын тогтолцоог сайжруулж төлбөрийн чадварын стандартыг бүрэн нэвтрүүлнэ.

4.3.9.Давхар даатгалын тогтолцоог боловсронгуй болгоно.

4.3.10.Технологид суурилсан даатгалын шинэ бүтээгдэхүүн, үйлчилгээний хууль, эрх зүйн орчныг боловсронгуй болгоно.

4.3.24.ДААТГАЛЫН ГЭРЭЭНИЙ СТАНДАРТЫГ ТОГТООЖ, БҮРТГЭЛИЙН ПРОЦЕССЫГ ХЯЛБАРШУУЛАХ, КИБЕР ДААТГАЛЫГ ХӨГЖҮҮЛНЭ.

4.3.25.Даатгалын зах зээлийн эрсдэлийг урьдчилан сануулах системийг бүрэн нэвтрүүлнэ.

4.3.26.Даатгуулагчдын кибер аюулгүй байдлыг хангах, хэрэглэгчийн эрх ашгийг хамгаалах эрх зүйн орчныг бүрдүүлнэ.