Process Safety Beacon
Үйлдвэрийн ажилтнуудад зориулсан мэдээлэл
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

Дугаарыг ивээн тэтгэсэн
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Цахим орчны аюулгүй байдал ба химийн үйлдвэрлэл

2021оны 07-р сар

Зураг 1. Флорида мужийн Олдсмар хотын Бохир ус цэвэрлэх байгууламж

2021 оны 2-р сарын 5-ны өдөр Флорида мужийн Олдсмар хотод бохир ус цэвэрлэх байгууламжийн ажилтан хяналтын компьютерын дэлгэц дээрх сумны хөдөлгөөн хэвийн бус байгааг анзаарсан. Гэвч үйлдвэрийн алсын зайн программыг ашиглан ажилтнууд дэлгэцийн удирдлагыг хоорондоо шилжүүлж, IT-тай холбоотой асуудлыг шийдэх боломжтой байдаг тул тэрбээр эхэндээ санаа зовоогүй. Мөн ахлах ажилтан нь заримдаа операторын компьютертай холбогдож, байгууламжийн системүүдийг хянадаг байсан. Гэтэл хэдэн цагийн дараа дэлгэцийн сум хөдөлж, бохир ус цэвэрлэх байгууламжийн хяналтын удирдлагууд дээр дарж байгааг оператор ажигласан. Хэдхэн секундын дотор тухайн тус систем дэхь идэмхий натрийн тавилын цэгийг 100ppm-ээс 11,100ppm болгон өөрчлөхийг завдсан. Үүнийг түргэн анзаарсан оператор идэмхий натрийг хэвийн түвшинд нь буцааж тохируулсан. Азаар усны чанарт сөрөг нөлөө учраагүй.

Саяхан цахим халдлагаар шугам хоолойг хаасан тохиолдлын улмаас АНУ-ын Зүүн Эрэгт шатахууны хангамж хэдэн өдөр тасалджээ.

Танай компанийн системүүд интернэттэй холбогдсон байх магадлалтай бөгөөд цахим халдлагаас хамгаалах шаардлагатай. Компаниуд цахим халдлагаас сэргийлэх олон стратегийг ашигладаг. Үүнд: хамгаалалтын хана, вирусээс хамгаалах программ, халдлага болон вирусээс сэргийлэх бодлого зэрэг багтана.

Алсын зайнаас ажилладаг хүмүүсийн тоо өссөөр байгаа нь цахим халдлагад өртөх боломжийг улам нэмэгдүүлж байна.

Та мэдэх үү?

- Цахим гэмт хэрэгтнүүд зорилгодоо хүрэхийн тулд янз бүрийн сул талыг ашиглаж, маш нарийн арга заль хэрэглэдэг.
- Зохион байгуулалттай гэмт этгээдүүд цахим халдлагыг мөнгө олох хэрэгсэл болгон ашигладаг учир ийм гэмт хэргийн тоо өссөөр байна.
- Ойрын судалгаагаар 39 секунд тутамд нэг цахим халдлага тохиолддог гэсэн тооцоо гарчээ. (Эх сурвалж: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Ихэвчлэн нэр хүндтэй компанийн өмнөөс илгээдэг хуурамч и-мэйлүүд нь тухайн хүнийг хувийн мэдээлэл задруулахыг ятгадаг. Эдгээр үйлдэл бол цахим халдлагын үндсэн арга техник юм.
- Цахим халдлага нь и-мэйл, хавсралт, зөөврийн мэдээлэл хадгалах драйв зэргээр дамжин компанийн системд нэвтрэх боломжтой.
- Цахим орчны аюулгүй байдлыг зөрчсөн хэргийн 95% нь хүний алдаанаас шалтгаалдаг байна. (Эх сурвалж: https://www.cybintsolutions.com/employee-education-reduces-risk/)

Та юу хийж болох вэ?

- Компьютерын программ шинэчлэх хүсэлтийг ямагт IT-ийн хэлтэст мэдэгдэж, зөвшөөрөгдсөн шинэ хувилбарыг цаг алдалгүй суулгаж байх.
- Хамгаалах болон бусад сүлжээний программын шинэ хувилбарыг тогтмол суулгаж, идэвхжүүлж байх шаардлагатай.
- Өөрийн систем ба мэдээллийн нөөц хувилбарыг тогтмол хадгал.
- Бүх нэвтрэх эрхийг найдвартай нууц үгээр хамгаал. Нууц үг, хувийн нэвтрэх эрхийг бусадтай хуваалцахгүй, нууц үгийг ойрхон сольдог байх шаардлагатай.
- Нууц үгийг нэвтэрсэн хуудсанд хадгалан үлдээж болохгүй.
- Танихгүй хаягаас ирсэн линк ба и-мэйлийн хавсралтыг бүү нээ.
- Компанийн компьютер дээр зөвшөөрөлгүй программ хэзээ ч бүү суулга. Түлхүүр ба бусад аюулгүйн хэрэгслийг бүрэн хамгаал.
- Алсын зайнаас нэвтрэх эрхтэй бол компаниас заасан шаардлагыг мөрд. Нийтийн интернэт ашиглахдаа онцгой болгоомжтой бай.
- Хэрэв таны компьютерт хэвийн бус зүйл ажиглагдвал тусламж хүс! Гэмт этгээд нэвтрэхийг оролдож байж болзошгүй.

Цахим халдлага бодитоор оршдог. Та бол үүнтэй тэмцэх нэг чухал хүн юм.