Process Safety Beacon
Boodskap aan bedryfspersoneel
www.aiche.org/ccps/process-safety-beacon

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

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Kuber sekuriteit in die chemiese bedryf

Julie 2021

Figure 1. Oldmar, Florida water behandelings aanleg.

Op 5 Februarie, 2021 het die operateur by 'n waterbehandelings aanleg in Oldsmar, Florida opgemerk dat die muis se pyltjie op die rekenaarskerm (cursor) self rond beweeg. Aanvanklik het dit niemand bekommer nie omdat ondersteuningspersoneel vanaf ander plekke toegang het om probleme op te los. Die toesighouer het soms toegang gekry om die aanleg se vordering te monitor. 'n Paar uur later het die operateur opgemerk dat die muis beweeg en aanleg veranderinge maak. Die kuber indringer het die set-punt vir natrium hidroksied verander van 100 dpm na 11000 dpm. Die operateur het vinnig gereageer en dit weer teruggestel na 100 dpm voordat waterkwaliteit geaffekteer is.

Na 'n onlangse kuber aanval by Colonial Pipeline moes hulle noodgedwonge die brandstof pyplyne na die VSA ooskus vir verskeie dae afsluit.

Jou maatskappye se beheer sisteme is waarskynlik ook aan die internet gekoppel en het daarom beskerming nodig. Daar is baie maniere wat maatskappye gebruik om kuber bedreigings af te weer, soos byvoorbeeld Internet "firewalls", teen-virus sagteware en prosedures om sisteme te beskerm teen kuber aanvalle en rekenaar virusse. Meer mense werk deesdae aanlyn. Dit verhoog die risiko van kuber aanvalle.

Het jy geweet?

- Kuber kriminele gebruik gesofistikeerde programme soms genoem "malware" om swak plekke uit te buit om hulle doel te bereik.
- Afpers aanvalle neem toe met georganiseerde kriminele wat dit as geldmaak plan gebruik.
- Volgens 'n onlangse studie is daar elke 39 sekondes 'n kuber aanval iewers. (Ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Sogenaamde "phising" gebruik e-posse, wat voorkom asof dit van gerespekteerde bronne kom, om individue om die bos te lei en sodoende persoonlike inligting in die hande te kry. Die aanvalle is skep ook geleenthede om "malware" te plant.
- Kuber dreigemente kom die maatskappy binne deur e-posse, aanhangsels en van draagbare geheue stokkies.
- Vyf-en-negentig persent van kuber sekuriteit-falings is as gevolg van menslike foute. (Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

Wat kan ek doen?

- EnsureBevestig altyd versoeke vir sagteware opgraderings met die maatskappy se spesialiste voordat jy dit toelaat. Installeer slegs goedgekeurde sagteware opgraderings.
- Maak seker beskermende sagte ware soos virusprogramme is op datum en in werking.
- Maak seker die rugsteun (back-up) word gereeld gedoen.
- Gebruik sterk wagwoorde vir alle toegang na programme. Moenie wagwoorde met ander deel nie en verander gereeld.
- Moenie wagwoorde op jou rekenaar se internet browser stoor nie.
- Moenie klik op links of aanhangsels van e-posse as jy nie weet van wie dit kom nie.
- Installeer slegs goedgekeurde sagteware op enige maatskappy rekenaar. Maak seker toegangsleutels is behoorlik geïnstalleer.
- As jy via die internet toegang het tot maatskappy sisteme, volg die maatskappy se vereistes noukeurig. Wees versigtig vir enige publieke internet web bladsye.
- As iets op jou rekenaar anders of ongewoon lyk, vra hulp. Dit kan dalk 'n kuberkraker wees wat probeer inkom.

Kuber aanvalle is werklik. Jy speel 'n sleutelrol in die verdediging.