Process Safety Beacon
Messages for Manufacturing Personnel
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

సైబర్ సెక్యూరిటీ మరియు కెమికల్ ఆపరేషన్స్

జూలై 2021

Figure 1. Oldsmar, Florida water treatment plant

ఫ్లోరిడాలోని ఓల్డ్స్మార్ నందు 5వ తేదీ ఫిబ్రవరి 2021న ఒక నీటి శుద్ధి కర్మాగారములో గల ఒక ఉద్యోగి కంప్యూటర్ స్క్రీన్‌పై గల కర్సర్ వింతగా తిరగడాన్ని గమనించాడు. తొలుత ఎటువంటి కంగారు పడలేదు. ఐ.టి.కు సంబంధించిన సమస్యలను పరిరక్షించుటకు కొరకు ప్లాంటులో ఉన్న స్టాఫ్‌కు రిమోట్ ఏక్సెస్ సాఫ్ట్‌వేర్ ద్వారా స్క్రీను పంచుకునే విధానాన్ని ప్లాంటు నందు వాడబడింది. సూపర్‌వైజర్ కూడా ఆపరేటర్ యొక్క కంప్యూటర్‌ను తరుచుగా అనుసంధానం చేసి చూసేవాడు. కొన్ని గంటల తర్వాత కర్సర్ జరిగి నీటి శుద్ధి నియంత్రణల వైపుగా కొట్టుకోవడం ఆపరేటర్ గమనించాడు. చొరబడినవాడు కొన్ని సెకన్లలోనే సిస్టమ్ యొక్క సోడియం హైడ్రాక్సైడ్ సెట్ పాయింట్‌ను 100 పార్ట్ పర్ మిలియన్ (పి.పి.ఎమ్.) నుండి 11,100 పి.పి.ఎమ్.కు మార్చేసాడు. ఆపరేటర్ తొందరగా చొరబాటును గమనించి సోడియమ్ హైడ్రాక్సైడ్ యొక్క స్థాయిలు సాధారణ స్థాయికి వచ్చేలాగా చేసాడు. అదృష్టవశాత్తూ నీటి యొక్క నాణ్యతపై ఎటువంటి ప్రభావము కనబడలేదు.

ఇటీవల కొలోనియల్ పైపుపై రాన్‌సమ్‌వేర్ సాఫ్ట్‌వేర్ దాడి వలన యు.ఎస్. ఈస్ట్‌కోస్ట్ గ్యాసోలిన్ లైను కొద్ది రోజుల పాటు మూసుకుపోయింది.

మీ కంపెనీ సిస్టమ్స్ అన్నీ ఇంటర్‌నెట్‌కు అనుసంధానమై ఉంటాయి. కావున వాటికి సైబర్ అటాక్స్ నుంచి రక్షణ అవసరము. కంపెనీ వివిధ రకములైన పధకాల ద్వారా ఈ సమస్యను ఎదుర్కోవాలి. ఉదా:- ఫైర్‌వాల్స్, యాంటీ వైరస్ సాఫ్ట్‌వేర్స్ మరియు పధకాలు.

చాలా మంది ప్రజలు దూర ప్రాంతాల నుండి పనిచేస్తున్నారు. ఇందువల్ల సైబర్ దాడులకు అవకాశములు పెరిగాయి.

మీకు తెలుసా?

- సైబర్ నేరగాళ్లు తప్పుడు సాఫ్ట్‌వేర్స్‌ను ఉపయోగించి వారికి కావలసిన గమ్యాన్ని సులభంగా చేరుకుంటున్నారు.
- రాన్‌సమ్‌వేర్ దాడులు గణనీయంగా కంపెనీలపై పెరుగుతున్నాయి. నిర్మాణాత్మకమైన దొంగలు దీనిని డబ్బు సంపాదించే సాధనముగా ఉపయోగిస్తున్నారు.
- ఇటీవల జరిపిన అధ్యయనం ప్రకారం - ప్రతీ 39 సెకన్లకు ఒక సైబర్ అటాక్ జరుగుతోంది (Ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- పిషింగ్ అంటే ఈ-మెయిల్స్ పంపడం, ముఖ్యంగా గౌరవప్రదమైన కంపెనీల పేరున పరిచయాలు పెంచుకుని, సమాచారాన్ని రాబట్టడం; ఈ పద్ధతి ద్వారా మాల్స్‌వేర్స్‌ను ప్రవేశపెడతారు.
- సైబర్ బెదిరింపులు - మీ కంపెనీ సిస్టమ్స్‌లోనికి ఈ-మెయిల్స్ ద్వారా ప్రవేశింపవచ్చు, అటాచ్‌మెంట్స్ ద్వారా గానీ, పోర్టబుల్ స్టోరేజ్ డివైస్ ద్వారా గానీ. ఉదా:- తంబ్ డ్రైవ్స్ మొదలగు పోర్టబుల్ డివైజ్‌లు.
- 95 శాతం సైబరు భద్రత పోవడానికి కారణాలు - మానవ తప్పిదాలే . (Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

మీరు ఏమి చెయ్యాలి?

- మీ సాఫ్ట్‌వేర్‌ను అప్‌డేట్ చేసేటప్పుడు మీ ఐ.టి. శాఖను సంప్రదించి, అనుమతి పొందిన వాటినే ఇన్‌స్టాల్ చేసుకోండి.
- మీ ఫైర్‌వాల్స్ ఇతర నెట్‌వర్క్ రక్షణ కవచాల తాజా వ్యవస్థలు సరిగా పనిచేస్తున్నాయా, ఆన్‌లో ఉన్నాయా గమనించండి.
- మీ సిస్టమ్‌ను డాటాను తరుచుగా బ్యాక్ అప్ చెయ్యండి.
- బలమైన పాస్‌వర్డ్‌లను వాడండి. ఎవ్వరికీ మీ పాస్‌వర్డ్‌లను చెప్పకండి. అక్కౌంట్సు గురించి చెప్పకండి. తరుచుగా పాస్‌వర్డ్‌లను మార్చండి.
- బ్రౌజర్స్‌పై పాస్‌వర్డ్‌లను సేవ్ చేయకండి.
- మీకు తెలియని వారు పంపిన లింక్‌లపై క్లిక్ కొట్టకండి.
- అనుమతి లేని సాఫ్ట్‌వేర్స్‌ను మీ కంపెనీ కంప్యూటర్‌లోనికి ఎక్కించకండి. అన్ని కీస్, ఇతర సెక్యూరిటీ డివైజ్‌లు భద్రంగా ఉన్నాయో లేదో చూసుకోండి.
- రిమోట్ యాక్సెస్ ఉంటే మీ కంపెనీ అవసరాలను అనుసరించండి, పబ్లిక్ ఇంటర్నెట్ సైట్లపై పనిచేసేటప్పుడు చాలా భద్రతతో ఉండండి.
- మీ కంప్యూటర్‌పై ఏమైనా క్రొత్త గుర్తులను గమనిస్తే, సహాయం అడగండి. అది హ్యాకర్స్ పని అని గుర్తెరగండి.

సైబర్ దాడులు నిజమైనవి. దానిని ఎదుర్కొనే భాగములో మీరు చాలా ముఖ్యమైనవారు.