Process Safety Beacon
उत्पादन क्षेत्र से जुडे व्यक्तियो के लिये संदेश
www.aiche.org/ccps/process-safety-beacon

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

इस अंक के प्रायोजक है
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

साइबर सुरक्षा और रसायनिक प्रचालन

जुलाई 2021

चित्र संख्या 1. ओल्ड मार , फलोरिडा जल उपचार सन्यंत्र

5 फरवरी , 2021 को , ओल्डमार , फलोरिडा में स्थित जल उपचार सन्यंत्र में एक कर्मचारी ने देखा कि उस के कम्पयूटर के पटल पर कर्सर (cursor) , शुरू में कोई चिंता का विषय नहीं था ; सन्यंत्र अपने कर्मचारियो के लिये कम्प्यूटर सांझा करने के लिये और आई टी से जुडे मुद्दो के हल के लिये सोफ्टवेयर प्रयोग में लाता था I

प्रयवेक्षक प्राय: अपना कम्पयूटर को सुविधा के प्रणालियो से जोडा करा करता था I परंतु कुछ घन्टे बाद , प्रचालक ने देखा कि जल उपचार सन्यंत्र के नियंत्रणो से कर्सर (cursor) गुजर रहा है और सन्यंत्र के नियंत्रणो में हस्तक्षेप कर रहा है I कुछ ही सेकेंडो के बाद ही , अतिक्रमी प्रणाली के सोडियम हाईड्रोक्साईड नियत बिंदु को 100 पी पी एम से 11, 100 पी पी एम ले गया I प्रचालक ने शीघ्रता से इस अतिक्रमण को देखा और सोडियम हाईड्रोक्साईड नियत बिन्दु को सामान्य कर दिया I सन्योग वश पानी की गुणवत्ता पर इस का कोई प्रभाव नहीं हुआ I

यू एस पूर्वी तटीय क्षेत्र को एक गैसोलिन की पूर्ति करने वाली पाईप लाईन कुछ समय पहले रेंसम्वेयर आक्रमण होने से काफी दिन बंद रही आपकी कम्पनी के अधिकतर प्रणालिया इंटरनेट से जुडी हुई है और इन को साइबर हमलो से बचाने के लिये सुरक्षा की आवश्यकता हैI संस्थान साइबर अतिक्रमण को रोकने के लिये बहुत प्रकार की कार्य नीतिया अपनाती है , जैसे कि फायरवाल , वाइरस विरोधी सोफ्ट वेयर और मालवेयर और कम्पयूटर को वाइरसो से बचाने के लिये नीतिया I

बहुत से लोग सुदूर से कार्य कर रहे है ; इस लिये इस ने साइबर अतिक्रमणो को बढाने में सहायता की है I

क्या आप जानते है ?

- **साइबर अपराधी अपने लक्ष्य को प्राप्त करने के लिये या बहुधा प्रकार की अति संवेदन शील विषयो का दुरुपयोग करने के लिये अति आधुनिक मालवेयर का प्रयोग करते है I**
- **.पैसा कमाने के उद्देश्य से संचालित अपराध करने वालो से रेंसम्वेयर आक्रमण बढते जा रहे है I**
- **एक गत अध्यन्न के अनुसार , साइबर आक्रमण प्रत्येक 39 सेकेंड के अंतर पर होता है (संदर्भ** https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- **कथित रूप से सम्मानीय संस्थानो को मेल भेजने को फिशिंग (Phising) कहते है , जो व्यक्तियो को अपनी व्यक्तिगत जानकारी देने के लिये उकसाते है I ये अतिक्रमण मालवेयर का प्रयोग करने के लिये प्राथमिक प्रवेश बिंदु है I**
- **ई मेल के द्वारा , संलग्न फाईलो से और भंडारण उपकरणो जैसे कि अंगूठे से चालित /प्रमाणित या अन्य भंडारण उपकरणो से कम्पनी की प्रणालियो में साईबर आक्रमण हो सकता है I**
- **साईबर सुरक्षा में पचानवे (95) प्रतिशत अतिक्रमण मानवीय गल्तियो के कारण होती है I (संदर्भ .** https://www.cybintsolutions.com/employee-education-reduces-risk/)

आप क्या कर सकते है ?

- **हमेशा सोफ्ट वेयर अपडेट करने की प्रार्थना करने से पहले आई टी (IT) से पुष्टि करते रहे, और समय बद्ध तरीके से अनुमोदित अपडेट ही संस्थापित करे I**
- **यह सुनिश्चित करे कि आप के फायरवाल (firewall) और अन्य नेटवर्क सोफ्ट वेयर बिल्कुल नये हैं और वो सही प्रकार से कार्य कर रहे हैं I**
- **यह सुनिश्चित करे कि आप ने अपने कम्पयूटर से डाटा (महत्त्वपूर्ण आंकडे) का बेक अप नियमित रूप से लेते रहे I**
- **सभी प्रकार के अभिगमनो के लिये मजबूत कूटशब्द (password) का प्रयोग करे I अपने कूटशब्द या अपने लेखा जोखे को किसी के साथ सांझा न करे और कूटशब्द आप नियमित रूप से परिवर्तित करते रहे I**
- **ब्राऊसर (browser) पर कूटशब्द (password) को सुरक्षित न करे I**
- **कोई भी जो आप को मेल अज्ञात सूत्रो से प्राप्त हुआ है , उसे आप न खोले या उस मेल के साथ संलग्नक को क्लिक न करे I**
- **कम्पनी के किसी भी कम्पयूटर पर अस्वीकृत सोफ्टवेयर संस्थापित न करे , यह सुनिश्चित करे कि अन्य प्रकार की वास्तविक सुरक्षा यंत्र सही प्रकार से सुरक्षित कर लिये गये है I**
- **यदि आप सुदूर अभिगम (remote access) प्रयोग कर रहे है , तो आप अपने कम्पनी की आवश्यकताओ का पालन कर रहे है I विशेष रूप से सतर्क रहे , जब आप सार्वजनिक इंटरनेट साइट प्रयोग कर रहे है I**
- **यदि आप अपने कम्पयूटर पर कुछ भिन्न देखते या अलग प्रकार का देखते है , तो आप सहायता की मांग करे ! ऐसा हो सकता है कि कोई घुस पैठिया (hacker)आप की कम्पयूटर प्रणाली पर पहुंचनने की कोशिश कर रहा है I**

साइबर आक्रमण वास्तव में होते है I आप इस की रक्षा करने के लिये बहुत महत्त्वपूर्ण है I

Translated into Hindi by Vivek Ranjan Gupta, Bharat Petroleum Corporation Limited, Mumbai, Maharashtra, India