# केन्द्रीय विद्युत प्राधिकरण

## राजभाषा त्रैमासिक पत्रिका

# विद्युत वाहिनी

*द्वितीय अंक जनवरी 2023*

# साइबर सुरक्षा विशेषांक

जन-गण-मन अधिनायक जय हे,

भारत भाग्य विधाता .

पंजाब-सिन्धु-गुजरात-मराठा

द्राविड़-उत्कल-बंग

विंध्य हिमाचल यमुना गंगा

उच्छल जलधि तरंग

तब शुभ नामे जागे,

तब शुभ आशिष मांगे

गाहे तब जय-गाथा .

जन-गण-मंगलदायक जय हे

भारत भाग्य विधाता .

जय हे, जय हे, जय हे,

जय जय जय जय हे.

# संरक्षक की ओर से

**सम्मानित पाठकों,**

किसी भी मानव के लिए जीवन या जिन्दगी सबसे महत्वपूर्ण है. लेकिन जीवन को सुचारू रूप से चलाने के लिए कुछ आधारभूत तत्वों की आवश्यकता है. जिंदा रहने के लिए भोजन, पानी, हवा आदि प्रकृति प्रदत्त मूल तत्व हैं. लेकिन गरिमामय व गुणवता पूर्ण मानव जीवन जीने के लिए कुछ और आवश्यकताओं का पूर्ण होना भी महत्वपूर्ण हैं जैसे कि आवास, रोजगार, शिक्षा, स्वास्थ्य, वाहन, बिजली, संचार के साधन आदि. इन साधनों को मुहैया करवाने में विज्ञान का विशेष योगदान रहा है. विज्ञान के योगदान के रूप में डिजिटल माध्यमों यथा इन्टरनेट, स्मार्ट फोन, कम्प्यूटर, सर्वर, ऑन लाइन प्रणालियों का स्थान महत्वपूर्ण है. ये माध्यम जीवन में गति लाने के साथ विभिन्न दुष्कर कार्यों को सुगम बनाने में सक्षम हैं. लेकिन इस सम्बन्ध में एक बात हमेशा ध्यान रखनी होगी और वह है उपयुक्त साइबर सुरक्षा का पालन करना. आज बहुत से विध्नकारी तत्व संपूर्ण मानवता के खिलाफ खिलवाड़ करने से भी नहीं चूकते हैं और अपने स्वार्थ के लिए किसी भी हदतक गिरकर संपूर्ण व्यवस्था को चौपट करने के इरादे से सुरक्षा में सेंध लगाते रहते हैं. मैं उन कुशल हाथों की प्रशंसा करना चाहूँगा, जो इस प्रकार के कुत्सित प्रयासों को विफल करने में सदैव सक्रिय योगदान देते रहते हैं और सभी को साइबर सुरक्षा के मामले में सावधान करते रहते हैं.

इसी कड़ी में 'विद्युत वाहिनी पत्रिका' के इस अंक में संकलित समयपरिक लेखों के द्वारा संपूर्ण सभ्य समाज को "साइबर सुरक्षा" के विभिन्न आयामों से अवगत कराने व जागरूक बनाने का प्रयास किया गया है.

एक सुरक्षित नववर्ष की शुभकामनाओं सहित,

आपका,

(घनश्याम प्रसाद)
अध्यक्ष (के. वि. प्रा.)

# संपादक की कलम से

**आदरणीय पाठकगण,**

परिवर्तन समय की मांग है या यूँ कहें कि परिवर्तन शाश्वत सत्य है. इसी कड़ी में औद्योगिक क्रान्ति के बाद यदि किसी व्यवस्था ने हमारे जीवन को सबसे ज्यादा प्रभावित किया है तो वह है डिजिटल क्रान्ति. डिजिटल क्रान्ति का हमारे जीवन के प्रत्येक क्षेत्र और प्रत्येक गतिविधियों में समावेश परिलक्षित है. आज के युग में डिजिटल सुविधाओं के बिना हमारा जीवन ठहर सा जाता है, बहुत सी गतिविधियां बाधित हो जाती हैं.

यह डिजिटल माध्यम का ही प्रभाव है कि कम्प्यूटर, माउस या स्मार्ट फोन के कुछ गिने चुने कमांडस (निर्देशों) के द्वारा पूर्व में असंभव से लगने वाले कार्य अति सहजता से पूर्ण शुद्धि के साथ बहुत कम समय में पूरे हो जाते हैं. आज का समय ''ऑन लाईन' "Real Time Process" का है. इन्टरनेट के आगमन ने हमारे जीवन के विभिन्न क्रिया-कलापों को अति सुगम बना दिया है और हमारे कार्य महीनों व दिनों के मुकाबले क्षणभर में सम्पादित हो रहे हैं. लेकिन इस गतिशीलता के साथ साइबर सुरक्षा से संबन्धित सावधानियां बरतना जरुरी है. यह विघटनकारी तत्व ''साइबर सुरक्षा में सेंध लगाना'' के रुप में है. हमें अपनी सुविधा के साथ-साथ जागरूक व सुरक्षित भी रहना होगा.

इन्हीं कुछ तथ्यों तथा विभिन्न आयामों पर दृष्टिपात करते हुए विभिन्न विद्वानों के लेखों का संकलन 'विद्युत वाहिनी पत्रिका' के वर्तमान संस्करण में प्रस्तुत करने का प्रयास किया गया है. आशा ही नहीं पूर्ण विश्वास है कि पाठकगण पत्रिका में छपे लेखों से "साइबर सुरक्षा'' के क्षेत्र में और भी सजग बनेंगे तथा न केवल स्वंय की अपितु पूरे आर्थिक, सामाजिक व उद्योग जगत की डिजिटल सुरक्षा में बढ़ चढ़कर भागीदारी करेगें. इन सभी गंभीर बातों को ध्यान में रखते हुए पत्रिका का वर्तमान अंक पूर्ण जिम्मदारी से आपके सुरक्षित हाथों में सौंपते हुए गर्व महसूस कर रहा हूँ. नववर्ष की खुशियों, सुरक्षित व्यवस्था व आप सबकी सुरक्षा की कामनाओं सहित,

आपका,

(अशोक कुमार राजपूत)
सदस्य (विद्युत प्रणाली)
(के. वि. प्रा.)

# संदेश

प्रिय पाठकगण,

सर्वप्रथम आपको और आपके परिवार को नववर्ष 2023 की बहुत-बहुत बधाई. आशा है हमारा केंद्रीय विद्युत प्राधिकरण परिवार आप सभी की मेहनत और सहयोग से इस वर्ष में और अधिक उँचाईंयों को प्राप्त करेगा. आज हम तकनीकी युग में पूर्णतः प्रवेश कर चुके हैं या यूँ कहें कि कोरोना काल ने हमें एक बहुत बड़ी शिक्षा दी है कि हम अत्याधुनिक तकनीकी साधनों का प्रयोग करते हुए पूर्णतः तकनीक पर निर्भर हो जाएँ अर्थात इंटरनेट युक्त कंप्यूटर, मोबाईल, लैपटॉप इत्यादि हमारे दैनंदिन जीवन के अभिन्न आधार स्तंभ पर पूर्णतः जीवन यापन करें.

इन्हीं के साथ एक और नया क्षेत्र जिस पर केंद्रीय विद्युत प्राधिकरण बड़े पैमाने पर कार्य कर रहा है वह है "साईबर सुरक्षा", यानि कंप्यूटर सर्वर, मोबाइल डिवाइस, इलैक्ट्रॉनिक सिस्टम, नेटवर्क और डेटा को दुर्भावनापूर्ण हमलों से बचाने का अभ्यास. इसे दूसरे शब्दों में सूचना प्रौद्योगिकी सुरक्षा या इलेक्ट्रॉनिक सूचना सुरक्षा के रूप में भी जाना जाता है.

नेटवर्क सुरक्षा घुसपैठियों से कम्प्यूटर नेटवर्क को सुरक्षित करने का अभ्यास हो चाहे लक्षित हमलावर हों या अवसरवादी मैलवेयर.

साइबर सुरक्षा युक्तियों में किस तरह साइबर हमलों से स्वयं को सुरक्षित रखें अर्थात एंटीवाइरस सॉफ्टवेयर का उपयोग करें और मजबूत पासवर्ड का उपयोग करें. साथ ही अज्ञात अटैचमेंट का मैलवेयर न खोलें.

इसी तरह की अनेक सावधानियों को ध्यान में रखते हुए हमने विद्युत वाहिनी के द्वितीय अंक को साइबर सुरक्षा विशेषांक के रुप में तैयार कर आप सबको समर्पित किया है. इन्हीं शब्दों के साथ पुनः नववर्ष की शुभकामनाओं सहित,

आपका,

(एम.ए.के.पी.सिंह)
सदस्य, (जल विद्युत) के.वि.प्रा.
एवं
साइबर सूचना सुरक्षा अधिकारी
विद्युत् मंत्रालय, भारत सरकार

# विषेश आभार

मैं विद्युत वाहिनी के मुख्य सम्पादक के रूप में तथा विद्युत वाहिनी के सम्पादक मंडल की ओर से श्री एम. ए. के. पी. सिंह जी के प्रति विषेश आभार प्रकट करता हूँ जो कि विद्युत वाहिनी इस "साइबर सुरक्षा विशेषांक" के प्रणेता एवं प्रेरणा श्रोत रहे हैं. उन्ही की प्रेरणा एवं आशीर्वाद से हमारी टीम ने साइबर सुरक्षा जैसे जटिल किन्तु महतवपूर्ण विषय पर लेखनी चलाने का प्रयास किया और उन्हीं के मार्गदर्शन में यह कार्य संपादित हो सका. उनके प्रति धन्यवाद भर कहना एक छोटी चीज होगी, वह वास्तव में बड़े सम्मान के अधिकारी हैं.

मैं राजभाषा प्रभारी श्री उपेन्द्र कुमार जी का विशेष आभारी हूँ जिन्होनें इस उपक्रम में कोइ कोर कसर नहीं छोड़ी है. उनके योगदान के बिना विशेषांक को यह रूप प्रदान करना असंभव था.

मैं विद्युत वाहिनी के मुख्य सम्पादक के रूप में तथा विद्युत वाहिनी के सम्पादक मंडल की ओर से श्री सौमित्र मजुमदार, निदेशक (सूचना प्रोद्योगिकीय) का बहुत आभारी हूँ जिन्होंने साइबर सुरक्षा जो कि आज के समय के एक बड़ी आवश्यकता है एवं जिसके कारण ऑनलाइन धोखाधड़ी, ब्लैकमेलिंग, धमकी, स्पैमिंग, भड़काने वाले कमेंट्स, हैकिंग आदि बहुत ही आम समस्याएं हो गई हैं तथा इससे निपटने की सख्त से सख्त जरुरत है पर विशेषांक तैयार करने अपना बहुमूल्य योगदान दिया है. वे अत्यंत प्रशंसा एवम धन्वयद के पात्र हैं. हम आशा करते हैं कि राजभाषा के क्षेत्र में उनका योगदान सदैव मिलता रहेगा.

इस साइबर विशेषांक को बहुमूल्य रूप देने में सौमित्र जी का योगदान विभिन्न आयामों में प्रदर्शित होता है. इस दस्तावेज को कांसेप्ट से लेकर अंतिम रूप तक देने में उनका योगदान सर्वोपरि रहा है.

साथ ही मैं सभी लेखकों का हार्दिक धन्यवाद करता हूँ. हमारी टीम के सभी सदस्य प्रशंसा व धन्यवाद के पात्र हैं. विशेषांक को अंतिम रूप देने में लगे अन्य सहयोगियों के लिए सम्मान एवं धन्यवाद.

पाठकों के लिए अग्रिम रूप से धन्यवाद एवं शुभकामनाएँ प्रेषित हैं.

**जय हिंद**

# सूचना

**भारत सरकार**
**विद्युत मंत्रालय**
**केन्द्रीय विद्युत प्राधिकरण**
**राजभाषा अनुभाग**

****

**"के. वि. प्रा. की 'विद्युत वाहिनी' राजभाषा त्रैमासिक पत्रिका के लिए रचनाएं भेजने का अनुरोध"**

केन्द्रीय विद्युत प्राधिकरण की राजभाषा त्रैमासिक पत्रिका '**विद्युत वाहिनी**' का प्रथम अंक सुधी पाठकों को डिजिटल रूप में सौंप दिया गया है जो कि केविप्रा की वेबसाइट **cea.nic.in** के हिंदी खण्ड में **'नया क्या है'** के अन्तर्गत उपलब्ध है.

पत्रिका का द्वीतीय अंक साइबर सुरक्षा विशेषांक के रूप में आपके समक्ष प्रस्तुत है. आगामी अंकों के लिए आपका सहयोग प्रार्थनीय है. कृपया अपने स्वरचित लेख/रचनाएँ एवं कविताएँ आदि अन्य विधाएँ पत्रिका में छपवाने हेतु यथाशीघ्र vidyutvahini-cea@gov.in, एवं CE-RNDCEA@NIC.IN पर भेजने का कष्ट करें जिसके लिए केविप्रा के कार्मिकों के लिए निम्नलिखित प्रकार से मानदेय दिए जाने का भी प्रावधान है-

- तकनीकी लेख के लिए अधिकतम राशि रू0 3000/- मात्र तथा
- गैर- तकनीकी लेख आदि के लिए अधिकतम राशि रू0 1500/-मात्र

जैसा कि आपको विदित ही है की सामान्यत: पत्रिका में के.वि.प्रा. के कर्मचारी अपने लेख / कविता आदि दे सकते हैं. वर्तमान में गुणवत्ता के आधार पर हिंदी में लिखे लेख के लिए (अधिकतम) रु 3000/- तथा कविता के लिए रु 1000/-प्रोत्साहन राशि मान्य है. यूँ तो, राशि केवल सांकेतिक सम्मान का प्रतीक भर है, महत्वपूर्ण व प्रशंसा योग्य है आपका उल्लास भरा सकारात्मक योगदान. पत्रिका का संपादक मंडल पत्रिका का एक आकार निश्चित करता है, यदि प्राप्त लेखों की संख्या अधिक हो जाती है तो कुछ लेख आगामी अंक के लिए विचारार्थ रख लिए जाते हैं. आपसे अनुरोध है कि आप अपने संपर्क में आये व्यक्तियों / संस्थानों को भी हिंदी पत्रिका के लिये लेख लिखने को प्रोत्साहित करें. के.वि.प्रा. कर्मचारियों के अलावा प्राप्त लेख वर्तमान में प्रोत्साहन राशि के हकदार नहीं है, लेकिन इन लेखों का यथायोग्य सम्मान पत्रिका में प्रकाशित होने के रूप में प्राप्त होगा.

जैसा कि आप जानते ही हैं कि ऊर्जा, स्वछ पर्यावरण, ऊर्जा सुरक्षा, जलवायु संरक्षण, ऊर्जा का समुचित उपयोग, ऊर्जा संरक्षण आदि आज के ज्वलंत विषय हैं, और यही हमारी पत्रिका की मुख्य विषय वस्तु है. आपसे पुनः अनुरोध करता हूँ कि आप अपने उन्नत विचारों को लेख के रूप में कृपया हमें प्रेषित करें. लेख editable form मे होने चाहिए, साथ में लेखक / लेखकों का नाम , पासपोर्ट आकार का फोटो, पदनाम, प्रभाग, फ़ोन नंबर व ईमेल भी भेजें. लेखों के साथ आपका बैंक खाता संख्या, IFSC कोड और बैंक का नाम भी भेजा जाए, ताकि प्रकाशन के लिए लेख के चयन पर राशि की प्रतिपूर्ति की जा सके (Your bank account number, IFSC

code, and bank name also be sent along with the articles, so that the amount can be reimbursed upon selection of the article for publication).

सामग्री भेजने के लिए ईमेल: **vidyutvahini-cea@gov.in, ce-rndcea@nic.in**

केविप्रा के प्रभागों/अनुभागों के कार्यकलापों व उपलब्धियों, पावर सेक्टर से संबंधित समाचार/बैठकों के समाचार, फोटो सहित सम्मिलित करने के लिए पत्रिका के आगामी अंक में प्राकार्शनार्थ आमंत्रित किए जाते हैं.

कृपया अपनी रचनाएं शीघ्र प्रेषित करें.

(अशोक कुमार राजपूत)/ (A K Rajput)
सदस्य (विद्युत् प्रणाली)/ Member (Power Systems)
एवं मुख्य सम्पादक विद्युत वाहिनी

# संपादक मंडल

**पत्राचार का पता:** राजभाषा प्रभाग, एनआरपीसी काम्प्लेक्स, 18-A, सहीद जीत सिंह मार्ग, कटवारिया सराय, नई दिल्ली - 110016. दूरभाष: 011-26510183, ई-मेल: vidyutvahini-cea@gov.in

**मुख्यालय:** केंद्रीय विद्युत प्राधिकरण, सेवा भवन, आर के पुरम सेक्टर-1, नई दिल्ली - 110066



भाषा वह माध्यम है जिससे कोई भी समाज अपना ज्ञान, संस्कृति और संस्कार भावी पीढ़ियों तक पहुंचाता है.

\- श्री नरेंद्र मोदी (प्रधानमंत्री)

# अनुक्रमणिका

# 1. आम साइबर हमले

रोहित यादव, उपनिदेशक, टी.पी.आर.एम
*ईमेल-* rohit.cea316@gov.in

## प्रस्तावना

आज कंप्यूटर और इंटरनेट का युग है और इनके बिना किसी भी काम की कल्पना करना असंभव है. ऐसे में अपराधी भी तकनीक के साथ हाईटेक हो गए हैं और वे अपराध करने के लिये इनका इस्तेमाल करते हैं. साइबर अपराध ऐसे गैर-कानूनी कार्य हैं जिनमें कंप्यूटर, लैपटॉप, स्मार्टफोन तथा टेबलेट एवं इंटरनेट नेटवर्क का प्रयोग एक साधन अथवा लक्ष्य अथवा दोनों के रूप में किया जाता है. जिस तरह एक क्षेत्र पर कब्जा करने के लिए लड़ाई लड़ी जाती है, उसी तरह डिजिटल दुनिया में एक नेटवर्क तक पहुंच हासिल करने के लिए साइबर हमले किए जाते हैं. किसी सिस्टम का एक्सेस और डेटा पर कंट्रोल पाने के लिए हैकर्स अनैतिक साधनों का इस्तेमाल करते हैं. ये हमलावर एक कमजोर सिस्टम पर हमला करने और उस पर कंट्रोल पाने के लिए मैलिशियस कोड के कॉम्बिनेशन का इस्तेमाल करते हैं. साइबर सिक्योरिटी के ऊपर अटैक कई तरह के होते हैं. कुछ आम साइबर अटैक निम्नलिखित हैं:

## फ़िशिंग (Phishing)

ये हैकर्स द्वारा इस्तेमाल किए जाने वाले ऑनलाइन अटैक का सबसे आम तरीका है. फ़िशिंग में हमलावर खुद को एक विश्वसनीय सोर्स की तरह पेश करता है और एक मैलिशियस ईमेल भेजता है जो पहली नज़र में वैध लगता है. इस तरह का असली दिखने वाला ईमेल भेजने के पीछे हैकर का यूज़र्स का नाम, पासवर्ड, क्रेडिट कार्ड और बाकी बैंकिंग डिटेल हासिल करने का उद्देश्य होता है. उदाहरण के लिए आपके सोशल मीडिया अकाउंट के पासवर्ड की एक्सपायरी के बारे में एक ईमेल हो सकता है. ईमेल में एक लिंक शामिल होने की संभावना होती है जो पहली बार में वैध लगती है, लेकिन अगर ध्यान से देखा जाए, तो आपको इसकी स्पेलिंग में कुछ हेरफेर दिखाई दे सकता है. इस प्रकार की घटनाओं से सतर्क रहने की आवश्यकता है.

## स्मिशिंग (Smishing)

स्मिशिंग फ़िशिंग अटैक करने का एक ऐसा तरीका है जो कि आमतौर पर एक SMS के द्वारा किया जाता है. उस SMS में एक लिंक होता है अगर आप ऐसे लिंक पर क्लिक करते हैं, तो वेबसाइट (जो वैध भी दिख सकती है) आपकी सहमति के बिना आपकी निजी जानकारी को चुरा सकती है. उदाहरणतः आपके फ़ोन में एक SMS आता है, यह SMS दावा करता है कि यूज़र ने एक लॉटरी जीती है और उसे पाने के लिए यूज़र को अपने डिटेल देने की ज़रूरत है. आप जैसे ही लिंक पर क्लिक करते हैं, तो आपके बैंक खाते सम्बंधित निजी जानकारी पूछी जाती है. जैसे ही आपने अपनी जानकारी डाली और बैंक खाते से पैसे गायब. अतः यह ज़रूरी है कि आप ऐसे SMS को ध्यान से पढ़ें और सही प्रतीत होने वाले संदिग्ध URL पर क्लिक करने से बचें.

## मैलवेयर (Malware)

यह एक मैलिशियस सॉफ्टवेयर होता है, जो पीड़ित के डेटा तक एक्सेस पाने के लिए पेलोड का इस्तेमाल करता है. ये सॉफ्टवेयर एक प्रोग्राम इंस्टॉल करता है जिसमें कई तरह के मैलवेयर जैसे रैंसमवेयर, स्पाईवेयर, ट्रोजन, वर्म्स इत्यादि शामिल रहते हैं, जो कि सिस्टम या नेटवर्क को डैमेज करने या सिस्टम के डेटा को डिलीट और हाइजैक करने के लिए डिज़ाइन किये जाते हैं. रैनसमवेयर सबसे अधिक इस्तेमाल किया जाने वाला मैलवेयर है जो डेटा चोरी करने के लिए इस्तेमाल किया जाता है. एक बार मैलवेयर सिस्टम में इंस्टॉल हो जाने पर, ये संवेदनशील जानकारी की खोज करता है और इसे एन्क्रिप्ट करता है. फिर सिस्टम पर एक पॉप-अप मैसेज फिरौती के लिए कहता है. अगर पीड़ित फिरौती देने से मना कर देता है तो हैकर्स अक्सर डेटा डिलीट करने या उसे ऑनलाइन बेचने की धमकी देते हैं. इसके बाद अगर वह मांगी गई राशि दे दे तो पीड़ित के अपने डेटा का

फिर से एक्सेस करने की संभावना रहती है, हालांकि कोई गारंटी नहीं है कि हैकर आपका डेटा वापस कर दे या फिर उन्हें अपने सिस्टम से डिलीट कर दे.

### डॉस (DoS) अटैक

DoS अटैक एक ब्रूट फोर्स अटैक है जिसका उद्देश्य किसी सिस्टम या वेबसाइट के ट्रैफिक को कम करना और इसे ऑफलाइन करना है. हमलावर अत्यधिक ट्रैफ़िक के साथ एक सिस्टम या वेबसाइट पर बाढ़ ला सकते हैं या एक क्रैश को ट्रिगर करने वाली परिवर्तित जानकारी भेज सकते हैं, जिससे ये बाकी के एक्सेस से बाहर हो जाए.

कंप्यूटर नेटवर्क में अटैकर DoS अटैक के एक डिस्ट्रिब्यूटेड DoS (DDoS) नाम का इस्तेमाल कर सकते हैं. DoS की तरह, DDoS मुख्य सर्वर से जुड़े कई सिस्टम से अत्यधिक ट्रैफ़िक के साथ बैंडविड्थ को सैचुरेट करता है और इस प्रकार नेटवर्क की क्लॉगिंग करता है और फिर इसे ब्रेक डाउन की स्थिति तक लाता है. इस तरह के अटैक का लक्ष्य ये सुनिश्चित करना है कि पीड़ित नेटवर्क या वेबसाइट का ट्रैफ़िक कम हो जाए या इसे बाकी नेटवर्क को टारगेट करने के लिए उपयोग करें.

### मैन इन मिडिल अटैक (MI.T.M)

इसमें हमलावर दो पार्टी के बीच एक संचार को प्रकट करता है. ये पार्टियां दो यूज़र्स या एक यूज़र और एक एप्लिकेशन या एक सिस्टम के बीच हो सकती हैं. हमलावर खुद को दो संस्थाओं में से एक के रूप में प्रस्तुत करता है, जिससे यह प्रतीत होता है कि दोनों वैध पक्ष एक दूसरे के साथ संवाद कर रहे हैं. हमलावर दोनों के बीच कम्यूनिकेशन को ट्रैक करता है, इस प्रकार दोनों पक्षों के बीच शेयर की गई सभी जानकारियों का एक्सेस ले लिया जाता है. ऐसे हमलों का लक्ष्य पीड़ित से व्यक्तिगत और संवेदनशील जानकारी प्राप्त करना है, जिसमें आम तौर पर बैंकिंग और वित्त संबंधी जानकारी शामिल होती है.

इस तरह के हमलों से बचने के लिए, सुनिश्चित करें कि आप एक सुरक्षित इंटरनेट कनेक्शन से जुड़े हैं. HTTPS प्रोटोकॉल वाली वेबसाइट पर ही जाएं जो किसी भी तरह के स्पूफिंग हमलों से बचने के लिए विभिन्न एन्क्रिप्शन स्तरों का इस्तेमाल करते हैं.

### एसक्यूएल (SQL) इंजेक्शन और क्रॉस-साइट स्क्रिप्टिंग (XSS)

एक SQL इंजेक्शन हमले में, हैकर संवेदनशील जानकारी प्राप्त करने के लिए एक कमजोर वेबसाइट के डेटाबेस पर हमला करता है. हमलावर किसी भी डेटाबेस की SQL कमजोरियों को लक्षित करने के लिए मैलिशियस कोड का इस्तेमाल करता है, इस प्रकार सफल कार्यान्वयन के लिए डेटाबेस में संग्रहीत सभी डेटा तक पहुंच प्राप्त करता है.

XSS हमले के मामले में हमलावर वेब एप्लिकेशन को टारगेट करता है जो एक वेब ब्राउज़र को मैलिशियस कोड डिलीवर करता है. वेब ब्राउज़र एक्जीक्यूशन के लिए एक पुल के रूप में काम करता है और कोड सिर्फ तभी इंजेक्ट किया जाता है जब यूज़र हमले वाली वेबसाइट पर जाता है. इस तरह के हमलों के दौरान, संवेदनशील जानकारी जो उपयोगकर्ता के वेबसाइट पर प्रवेश करती है, उसे बिना किसी वेबसाइट या यूज़र्स के ज्ञान के हाईजैक कर लिया जा सकता है.

### विद्युत क्षेत्र में प्रमुख वैश्विक साइबर हमले

- **यू.एस. नॉर्थ ईस्ट ब्लैकआउट (2003):**
  **कारण:** कंट्रोल रूम में सॉफ्टवेयर की खराबी.
  **बहाली:** कुछ ग्राहक 6 घंटे के बाद, कुछ 2 दिन बाद, कुछ दूरस्थ स्थान लगभग एक सप्ताह के बाद.
  **परिणाम:** 8 अमेरिकी राज्यों में 45 मिलियन लोग, कनाडा में 10 मिलियन लोग, स्वास्थ्य सुविधाओं में $100M का नुकसान हुआ, 6 अस्पताल एक साल बाद दिवालिया.

- **न्यूयॉर्क में जलविद्युत उत्पादन पर साइबर हमला (2013):**
  हैकर्स ने एक सेलुलर मॉडेम के माध्यम से राई, न्यूयॉर्क के पास बोमन एवेन्यू बांध के बाढ़ नियंत्रण के लिए उपयोग की जाने वाली छोटी संरचना तक पहुंच प्राप्त की. ये सिस्टम पाइपलाइनों में प्रवाह, ड्रॉब्रिज की आवाजाही और बांधों से पानी छोड़ने

को नियंत्रित करते हैं. एक हैकर सैद्धांतिक रूप से विस्फोट, बाढ़ या ट्रैफिक जाम का कारण बन सकता है.

- **दक्षिण कोरियाई परमाणु और जलविद्युत कंपनी (2014):**
दक्षिण कोरियाई परमाणु और जलविद्युत कंपनी कोरिया हाइड्रो एंड न्यूक्लियर पावर (KHNP) को 2014 के अंत में हैक कर लिया गया था. हैकर्स ने दो परमाणु रिएक्टरों के लिए योजनाओं और मैनुअल के साथ-साथ 10,000 कर्मचारियों के डेटा को चुराकर ऑनलाइन पोस्ट कर दिया था.

- **यूक्रेनी बिजली कंपनी (2015):**
हैकर्स एक पश्चिमी यूक्रेनी बिजली कंपनी के सिस्टम में घुस गए, जिससे 2,25,000 घरों की बिजली कट गई. ब्लैकआउट में एक अमेरिकी रिपोर्ट ने निष्कर्ष निकाला कि एक वायरस को ईमेल के माध्यम से स्पीयर-फ़िशिंग के माध्यम से वितरित किया गया था. स्पीयर-फ़िशिंग एक तकनीक है जो प्रमुख कर्मचारियों को विस्तृत संदेश भेजती है, सोशल मीडिया से एकत्र की गई जानकारी का उपयोग करती है.

- **यूक्रेन (दिसंबर 2016):**
यूक्रेन पर 2016 का साइबर हमला एक साल से भी कम समय में दूसरा था. बिजली सबस्टेशन को अक्षम करने के बाद, हैकर्स ने कीव के कुछ हिस्सों में ग्राहकों को एक घंटे तक बिजली के बिना प्रभावित किया. बिजली की हानि उस रात कीव की बिजली खपत का पांचवां हिस्सा थी. हमले का श्रेय रूसी हैकरों को दिया गया, हमले का उद्देश्य पावर ग्रिड को भौतिक रूप से नुकसान पहुंचाना था.

- **ईएनटीएसओ-ई पर साइबर हमला (2020):**
ENTSO-E जो 35 देशों में 42 यूरोपीय ट्रांसमिशन सिस्टम ऑपरेटरों का प्रतिनिधित्व करता है. इसने मार्च, 2020 ही में अपने कार्यालय नेटवर्क में एक सफल साइबर घुसपैठ का सबूत पाया.

- इंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम (सीईआरटी-इन), जो साइबर सुरक्षा के मुद्दों पर प्रयासों का समन्वय करती है, ने पॉसोको के कुछ नियंत्रण केंद्रों पर शैडो पैड नामक मैलवेयर के खतरे पर 19 नवंबर 2020 को अलर्ट जारी किया. नेशनल क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (एनसीआईआईपीसी), जो महत्वपूर्ण क्षेत्रों में भारत के साइबर सुरक्षा संचालन की देखरेख करता है, ने फरवरी, 2021 को आरएलडीसी और एसएलडीसी को लक्षित करने वाले रेड इको के बारे में अलार्म किया.

- फरवरी 2021 में, शोधकर्ताओं ने बताया कि 2020 के मध्य से, चीनी उन्नत सतत खतरे (APT) Red Echo ने कम से कम 10 भारतीय बिजली क्षेत्र के संगठनों को प्रभावित किया है, जिसमें चार क्षेत्रीय लोड डिस्पैच केंद्र (RLDC) शामिल हैं, जो बिजली आपूर्ति को संतुलित करके पावर ग्रिड के संचालन के लिए जिम्मेदार हैं.

- **इलेट्रोब्रास, कोपेल ऊर्जा कंपनियों पर रैंसमवेयर हमलों का हमला (फ़रवरी, 2021):** रैंसमवेयर हमलों ने संचालन को बाधित कर दिया और कंपनियों को कम से कम अस्थायी रूप से अपने कुछ सिस्टम को बंद करने के लिए मजबूर किया.

- **डेल्टा-मोंट्रोस इलेक्ट्रिक एसोसिएशन (डीएमईए) (जनवरी, 2022)**: 25 साल के ऐतिहासिक डेटा को मिटा देने वाले दुर्भावनापूर्ण साइबरवेयर के कारण जनवरी, 2022 में कोलोराडो ऊर्जा कंपनी को अपने आंतरिक नियंत्रण के 90% सिस्टम को बंद करना पड़ा.

- **टाटा पावर पर साइबर हमला (अक्टूबर, 2022):** हमले ने टाटा पावर के कुछ आईटी सिस्टम को प्रभावित किया.

### साइबर हमलो से खुद को कैसे सुरक्षित रखें?

➢ साइबर सुरक्षा सभी की जिम्मेदारी है.

- फोरम या वेबसाइट्स पर अपनी संवेदनशील जानकारी जैसे ईमेल आईडी, पासवर्ड, क्रेडिट कार्ड की डिटेल आदि साझा न करें.
- सुनिश्चित करें कि आपका पासवर्ड कठिन हो और ऐसा कुछ न हो जिसका आसानी से अंदाज़ा लगाया जा सके.
- किसी भी लिंक पर क्लिक करने से पहले, सुनिश्चित करें कि वेबसाइट वैध है. मैसेज में या यु आर एल (URL) में किसी भी तरह की स्पेलिंग की गलतियों की जांच करें.
- अपने सिस्टम को लेटेस्ट सॉफ्टवेयर अपडेट के साथ अपडेट करें.
- भरोसेमंद एंटी-वायरस सॉफ्टेवेयर का इस्तेमाल करें और अपने सिस्टम को स्कैन करते रहें.
- स्पैम मैसेज और ईमेल को न खोलें और न ही उत्तर दें.
- अच्छे पासवर्ड प्रबंधन का अभ्यास करें.
- उपकरणों को कभी भी अप्राप्य न छोड़ें.
- अपने डेटा का बैकअप लें.
- ओपन वाई-फाई के इस्तेमाल से बचें. ये नेटवर्क सुरक्षित नहीं होते हैं और हैकर्स आसानी से आपके डेटा तक पहुंच प्राप्त करने के लिए एक मैलिशियस कोड इंजेक्ट कर सकते हैं.

*******

# 2. साइबर सुरक्षा की न्यूनतम अनिवार्यताएं

एन पटनायक (पूर्व सीईए, पूर्व सिक्योर मीटर, आई.टी. सलाहकार
*ईमेल- n.patnaik61@gmail.com*

## प्रस्तावना

"साइबर अटैक" के मौजूदा उदाहरण को उद्धृत करने के लिए मुझे यकीन है कि आप हाल ही में एम्स (AIIMS) आई.टी. सुरक्षा उल्लंघन के बारे में अच्छी तरह से अवगत होंगे, जिसके बाद पूरी प्रणाली अधर में है और एम्स ने पूरी तरह से मैनुअल मोड में काम करना शुरू कर दिया है.

बिजली उपयोगिताओं जैसे सार्वजनिक सेवा प्रदाताओं को इस तरह की बिजली क्षेत्र की समस्या के लिए और अधिक तैयार रहना चाहिए, जब तक कि यह हमला न करे और बहुत नुकसान न करे, आपको इसका पता नहीं चलेगा. विद्युत प्रणालियों को बिजली और स्विचिंग सर्जेज से काफी हद तक "बिजली बन्दी lightning arresters" के उपयोग से संरक्षित किया जाता है. उसी तरह साइबर अटैक से होने वाले बिजली के गंभीर हमलों से सुरक्षित रहने के लिए जागरूकता और ईमानदारी जरूरी है. साइबर घटनाओं से सुरक्षित रहने और महत्वपूर्ण बुनियादी ढांचे को बचाने के लिए सटीकता के साथ गंभीरता को अपनाना होगा. इसलिए हमें ऐसी किसी भी आपात स्थिति के लिए तैयार रहना चाहिए, कार्य करना चाहिए औरसाइबर साइबर हमले से सुरक्षा के लिये तैयार रहना चाहिए.

## बुनियादी बातों की आवश्यकता

जिन बुनियादी बातों को करने की आवश्यकता है वे निम्नानुसार हैं (निश्चित रूप से कई और सुरक्षा उपाय भी वांछनीय हैं):

### 1. कार्यों को प्राथमिकता दें

पारेतो नियम (Pereto Law) कहता है कि 20% कार्रवाई से 80% लाभ हो सकता है. उस पर पहले ध्यान दें. वह है स्टीफन कोवे की सात आदतें - एक आदत कहती है "पहली बात (चीज) पहले". चरणबद्ध कार्यान्वयन योजना को हमेशा प्राथमिकता दी जानी चाहिए.

**वे कौन से कार्य हैं** ? जिन्हें अब तक नहीं किए जाने पर प्राथमिकता के आधार पर किए जाने की आवश्यकता है:

**a) बैकअप**

टेप ड्राइव में सभी प्रणालियों का नियमित बैकअप रखें, जो एक बार लिखने वाले टेप हैं, जिन्हें सुरक्षा हमलों द्वारा संशोधित नहीं किया जा सकता है. यह

सिस्टम को पुनर्स्थापित करने में मदद कर सकता है क्योंकि रैंसमवेयर के हमले आपके भुगतान करने पर भी कम नहीं हो सकते हैं. इसलिए सुरक्षा हमलों से उबरने के लिए कभी भी फिरौती न दें. यह कार्रवाई बी.सी.डी.आर. (बिजनेस कंटीन्यूटी एंड डिजास्टर रिकवरी) आवश्यकता का हिस्सा है.

**b) सुरक्षा हमलों से पहले लंबी अवधि की कोशिशें और चेतावनी**

सुरक्षा हमला अक्सर लंबी अवधि में होता है - हमलावरों द्वारा दिनों से लेकर महीनों तक की कोशिशें. इसलिए, फ़ायरवॉल जैसे सुरक्षा उपकरणों के लॉग और सर्वर के अलर्ट की बारीकी से निगरानी करने की आवश्यकता है. एक सरल उदाहरण है, यदि किसी लॉग-इन प्रयास के लिए तीन बार पासवर्ड पुनः प्रयास किया जाता है, तो संबंधित उपयोगकर्ता से सत्यापन के साथ अलर्ट पर कार्रवाई की जानी चाहिए.

**c) एसओसी या सुरक्षा संचालन प्रणाली**

24x7 एसओसी स्वयं या तीसरे पक्ष द्वारा उपलब्ध सेवाओं को तैनात करने की आवश्यकता है. सुरक्षा चेतावनियों और संदेशों की उपेक्षा न करें. हालाँकि इन संदेशों को सुरक्षा सूचना और इवेंट मैनेजमेंट (SIEM) टूल का उपयोग करके सीमित किया जाना चाहिए, हालाँकि SIEM टूल दूसरा चरण हो सकता है पर प्राथमिकता वाली कार्रवाई नहीं.

**d) डिफ़ॉल्ट या आसानी से अनुमानित पासवर्ड**

पासवर्ड अक्सर डिफॉल्ट के रूप में या व्यवस्थापक के रूप में इंस्टॉल किए गए पासवर्ड के रूप में बनाए जाते हैं जैसे admin@123 या cea@123 or cea@123# आदि. किसी भी पासवर्ड का अनुमान लगाना आसान नहीं होना चाहिए, विशेष रूप से व्यवस्थापक के लॉग-इन के लिए स्ट्रिंग पासवर्ड का उपयोग करें. पासवर्ड अनिवार्य रूप से प्रत्येक 3 महीने में उपयोगकर्ता द्वारा सिस्टम सेटिंग्स के माध्यम से बदला जाना चाहिए और पिछले 3-4 पासवर्ड को नए पासवर्ड के रूप में स्वीकार नहीं किया जाना चाहिए. यहां तक कि डिफ़ॉल्ट कॉन्फ़िगरेशन जिन्हें स्थापना चरण में कॉन्फ़िगर किया जाना चाहिए, वे भी समस्या हैं.

**e) दो तरीकों से प्रमाणीकरण (द्विस्तरीय प्रमाणीकरण)**

विशेष रूप से व्यवस्थापक और पहली बार उपयोगकर्ता के लिए दो कारक प्रमाणीकरण आवश्यक है. यहां तक कि एस.बी.आई. (स्टेट बैंक ऑफ़ इंडिया) ने अब इसे सभी उपयोगकर्ता लॉग-इन के लिए अनिवार्य कर दिया है.

**f) फ़ायरवॉल कॉन्फ़िगरेशन**

नेटवर्किंग में फ़ायरवॉल सबसे महत्वपूर्ण उपकरण हैं. फ़ायरवॉल के लिए सार्वजनिक पोर्ट और एक्सेस नियम अच्छी तरह से कॉन्फ़िगर किए जाने चाहिए. फ़ायरवॉल के लॉग महत्वपूर्ण हैं और इनका नियमित रूप से विश्लेषण करने की आवश्यकता है. अक्सर फायरवॉल के कई पोर्ट खुले रखे जाते हैं. कहते हैं कि पोर्ट 80 या https के लिए 443 केवल बाहरी पहुंच के लिए खुला होना आवश्यक है. लेकिन अन्य पोर्ट्स प्रायः खुले रहते हैं. फ़ायरवॉल नियमों की समीक्षा करें और केवल आवश्यक बाहरी पहुँच प्रदान करें. हालांकि http को पूरी तरह से हतोत्साहित और समाप्त किया जाना चाहिए, केवल https की अनुमति दी जानी चाहिए.

**g) सर्वर अभिगम नियंत्रण**

अगला महत्वपूर्ण विन्यास सर्वरों के लिए है. सर्वर एक्सेस प्रबंधित करें और उपयोगकर्ताओं को केवल वांछित एक्सेस प्रदान करें.

**h) वी.ए.पी.टी. परीक्षण**

भेद्यता मूल्यांकन और प्रवेश परीक्षण किए जाने की आवश्यकता है.

**i) सी.ई.आर.टी./भारत सरकार एस.ओ.सी.**

यदि हम बिजली उपयोगिताओं को कार्य करने के लिए हजारों घटनाएं प्रदान करते हैं, तो वे कार्य नहीं करेंगे. इस प्रक्रिया को बहुत अधिक जोखिम वाली घटनाओं तक ही सीमित करना चाहिए.

**j) कोई टीएलएस 1.0 प्रोटोकॉल नहीं होना चाहिए**

सिस्टम में कोई टीएलएस 1.0 प्रोटोकॉल नहीं होना चाहिए, इसे युद्धस्तर पर खत्म करने के लिए तत्काल कार्रवाई की आवश्यकता है.

**k) USB ड्राइव प्रबंधन:** इस क्षेत्र में सावधानीपूर्वक विचार करने की आवश्यकता है.

**l) पैच प्रबंधन**

यह एक कमजोर क्षेत्र है, इसे एक सिस्टम में डालने के लिए प्राथमिकता में लिया जाना चाहिए.

**m) DDoS अटैक मैनेजमेंट**

विशेष विचार की आवश्यकता है.

**n) मैलवेयर और फ़िशिंग ईमेल**

एसओसी द्वारा निगरानी और फ़िल्टरिंग, सिस्टम से हटाना.

**o) सुरक्षा ज़ोनिंग और ज़ोन-आधारित पहुँच अधिकार**

कुछ DMZ ज़ोन बनाए जाने चाहिए, लेकिन कम से कम 3 ज़ोन जैसे DMZ, एप्लिकेशन ज़ोन और डेटाबेस एक्सेस ज़ोन बनाए जाते हैं. डेटा बेस अधिमानतः लिनक्स मशीनों पर होना चाहिए, न कि विंडोज़ मशीनों पर.

**p) डोमेन नियंत्रक**

वितरण प्रणालियों में अक्सर डोमेन-आधारित लॉग-इन (डोमेन नियंत्रक) नहीं होते हैं, वे कार्यसमूहों में या सर्वर से जुड़ी एकल मशीनों के रूप में काम करते हैं.

**q)** सख्ती से नियंत्रित वीपीएन कनेक्शन हमेशा दो फैक्टर एक्सेस के साथ.

### 1. सुरक्षा बजट और संसाधन

सुरक्षा के लिए बजट बनाना और लोगों का संसाधन करना महत्वपूर्ण है, जिन्हें अक्सर संगठनों के वार्षिक बजट में कम प्राथमिकता मिलती है. यह सुझाव दिया जाता है कि आने वाले वार्षिक बजट में उचित सिस्टम डिज़ाइन बजट के साथ इसका ध्यान रखा जाए और किसी भी सुरक्षा उल्लंघन के कारण बजट न दिया जाए.

### 2. व्यापारिक नेताओं और संचालन प्रमुखों के साथ सुरक्षा खतरों और खामियों की जवाबदेही

सुरक्षा खतरों और खामियों की जवाबदेही व्यावसायिक नेताओं के साथ होनी चाहिए न कि आई.टी. व्यक्तियों के साथ. आई.टी. व्यक्तियों को सक्षम, डिजाइनर और कार्यान्वयनकर्ता होने की आवश्यकता है और उन्हें जवाबदेही के दूसरे स्तर पर होना चाहिए और संगठन के पहले स्तर के जवाबदेही वाले व्यक्ति को रिपोर्ट करना चाहिए. जैसा कि कई मंचों में सही बताया गया है, यह आई.टी. संवर्ग उपयोगिताओं में स्थापित किया जाना चाहिए यदि नहीं है और सी.आई.एस.ओ. आई.टी. क्षेत्र से हो सकता है जो वरिष्ठ स्तर पर एक वरिष्ठ व्यापार नेता को रिपोर्ट करता है.

### 3. सुरक्षा मानक

विस्तृत कार्रवाई सबसे महत्वपूर्ण हैं. ये विस्तृत क्रियाएं मानकों के आधार पर उपलब्ध हैं. आईएसओ 27001 और संबंधित मानकों का पालन करना काफी महत्वपूर्ण है. यह उम्मीद है कि सभी प्रणालियों को प्रमाणित किया जाना चाहिए और प्रमाणपत्रों को आई.एस.ओ. आवश्यकता के अनुसार ऑडिट किया जाना चाहिए और साल दर साल लगातार सक्रिय रखा जाना चाहिए.

बहुत अधिक मानक नहीं थोपे जाने चाहियें, अन्यथा अनुपालन और स्पष्टता की कमी के मुद्दे होंगे. यदि आप 20 या 50 मानकों का पालन करने के लिए कहते हैं, तो क्या किया जा सकता है? कुछ मानकों में अतिव्यापी और कभी-कभी परस्पर विरोधी आवश्यकताएं भी होती हैं. बस एक सुझाव है, ओ.टी., आई.टी., फिर उसके उप-क्षेत्रों के आधार पर फोकस करने के लिए सभी क्षेत्रों को अलग करें और फिर बताएं कि किस क्षेत्र के लिए कौन सा मानक लागू है और संबंधित हितधारकों के साथ न्यूनतम से शुरू करें, यह सबसे पहले किया जाने वाला काम है. चरणबद्ध दृष्टिकोण अपनाना बेहतर है. महत्वपूर्ण

क्षेत्रों की पहचान करें और पहले उन पर ध्यान केंद्रित करें.

### 4. बाहरी देशों की धमकी

चीन और पाकिस्तान जैसे देश अक्सर भारत के खिलाफ होते हैं, ऐसे में उन देशों से हमारी सुरक्षा को खतरा हमेशा बना रहता है और हमें सतर्क रहना चाहिए.

### 5. सुरक्षा जोखिम उत्पत्ति की झलक

यहां उद्धृत समाचार आइटम काफी सामान्य हैं और समस्या की गंभीरता का संकेत देते हैं: "सुरक्षा जोखिम: यू.एस.ए. ने चीन के हुआवेई, जेड.टी.ई से गियर पर प्रतिबंध लगा दिया" जहां यू.एस.ए. ने इन दो कंपनियों और कई अन्य चीनी उपकरण कंपनियों पर प्रतिबंध लगा दिया है. आपने देखा होगा कि यूक्रेन युद्ध कैसे लड़ा जा रहा है, यह टैंकों और पैदल सेना पर नहीं बल्कि ड्रोन और मिसाइलों पर ज्यादा है. व्यावसायिक मोर्चों पर अन्य देशों के साथ भविष्य के जोखिम और प्रतियोगिता मुख्य रूप से आई.टी. पर हो सकती है इसलिए हमें तदनुसार तैयार रहना चाहिए. इसलिए सुरक्षा उपकरणों, और यहां तक कि सर्वरों का उपयोग करते समय मूल देशों को ध्यान में रखें. क्लाउड सर्विस प्रोवाइडर्स को भी सावधानी से चुनने की जरूरत है.

### 6. विद्युत क्षेत्र में सुरक्षा - विशाल और विविध आवश्यकताएं

बिजली क्षेत्र के प्रत्येक खंड के लिए साइबर सुरक्षा समान रूप से महत्वपूर्ण है, चाहे वह वितरण, उत्पादन और पारेषण प्रणालियों के लिए हो. हालांकि बहुत सारे नोड्स के साथ वितरण प्रणाली [जैसे कि उप-स्टेशन, वितरण ट्रांसफार्मर (डीटी)], व्यापक क्षेत्र (परिसर/पहुंच सुरक्षा) अधिक चुनौतीपूर्ण हो सकता है जबकि सुरक्षा के दृष्टिकोण से संचरण और उत्पादन अधिक महत्वपूर्ण हो सकता है. बिजली क्षेत्र को साइबर सुरक्षित बनाने के लिए विशिष्ट और मानक समाधानों को अपनाने की आवश्यकता है और सिस्टम को हर समय अपडेट रहना होगा. साइबर सुरक्षा के लिए उपकरण और उपकरणों के साथ-साथ सिस्टम को सुरक्षित बनाने का प्रशिक्षण और संस्कृति महत्वपूर्ण भूमिका निभाती है. लोगों को यह जानना चाहिए कि उद्देश्य क्या है और उन्हें क्या करना चाहिए. संबंधित कर्मचारियों के कर्तव्य में बुनियादी ढांचे और वित्तीय तंत्र की सुरक्षा सर्वोच्च प्राथमिकता होनी चाहिए. कुल मिलाकर लगातार चौकसी और कवायद भी जरूरी है.

*******

## 3. साइबर सूचना सुरक्षा अधिकारी के महत्व और भूमिका

सुमित कुमार सिन्हा, उपनिदेशक, सूचना प्रद्योगिकी एवं साइबर सुरक्षा
ईमेल- sumit.cea@gov.in

### प्रस्तावना

सरकारी संगठनों के कार्यों और प्रक्रियाओं के तेजी से डिजिटलीकरण के साथ, साइबर सुरक्षित आचरण को अपनाने की आवश्यकता अत्यंत महत्वपूर्ण होती जा रही है. साइबर सुरक्षा का उल्लंघन गंभीर क्षति का कारण बन सकता है एवं सरकारी संगठनो के कामकाज को बाधित कर सकता है. इसलिए यह अनिवार्य है कि सूचना प्रौद्योगिकी के उपयोग में शामिल प्रत्येक संगठन अपने कार्यों के निर्वहन में अपनी सूचना सुरक्षा (Information Security) आवश्यकताओं को पहचाने और उनका दस्तावेजीकरण करें. संगठनों को वैसी सूचना सुरक्षा प्रबंधन प्रणाली [Information Secuirty Management System(ISMS)] को लागू करना चाहिए जिसमें साइबर सुरक्षा के साथ-साथ भौतिक

और तार्किक सुरक्षा नियंत्रण शामिल हो, ताकि संगठन को सूचना सुरक्षा मुद्दों या साइबर संकटों से होने वाले नुकसान से बचाया जा सके. सर्वोत्तम सूचना सुरक्षा प्रणाली (ISMS) आचरण के अनुसार एक संरचित तंत्र सुनिश्चित करने के लिए इलेक्ट्रॉनिक्स एवं आई.टी. मंत्रालय (Meity) ने सभी मंत्रालयों/विभागों को एक मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ. /CISO) नामित करने की सलाह दी है. यह मंत्रालय/विभाग के सचिव (संगठनों के मामले में सीईओ/प्रमुख) की जिम्मेदारी है कि वे साइबर सुरक्षा कार्यक्रम स्थापित करें एवं सुरक्षा नीति अनुपालन का समन्वय करने के लिए वरिष्ठ प्रबंधन के एक सदस्य को 'मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ. /CISO)' के रूप में नामित करे. सूचना सुरक्षा कार्यक्रम स्थापित करने और संगठन में सुरक्षा नीति अनुपालन प्रयासों का समन्वय करने और सी.ई.आर.टी.-इन (CERT-In) जैसी नियामक एजेंसियों के साथ नियमित रूप से बातचीत करने के लिए मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ. ) को जनादेश और संसाधन दिए जाने चाहिए. सी.आई.एस.ओ. मंत्रालय/विभाग के सचिव (सीईओ/संगठनों के मामले में प्रमुख) को रिपोर्ट करेगा. यदि किसी कारण से, यह संभव नहीं है, तो सी.आई.एस.ओ. को सीधे मंत्रालय/विभाग (सीईओ/संगठनों के मामले में प्रमुख) में अगले वरिष्ठतम व्यक्ति को रिपोर्ट करना चाहिए.

अपने कर्तव्यों का प्रभावी ढंग से अनुपालन करने के लिए 'मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ.) को निम्नलिखित कौशल की आवश्यकता हैं:-

1. प्रबंधन क्षमताएं
2. रणनीतिक योजना क्षमता
3. साइबर कानूनों की जानकारी
4. सूचना सुरक्षा के क्षेत्र में एक्सपोजर
5. मौखिक और लेखन कौशल

## मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ.) की भूमिकाएं और जिम्मेदारियां

मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ.) की कुछ भूमिकाएँ और जिम्मेदारियाँ निम्नलिखित हैं:-

**(क) रणनीतिक योजना (Strategic Planning)**: इस भूमिका के तहत सी.आई.एस.ओ. की निम्न जिम्मेदारियां हैं:-

1. संगठन में सूचना सुरक्षा उपायों को लागू करने के लिए शीर्ष प्रबंधन के समर्थन के लिये प्रयासरत होना.
2. संगठन की आवश्यकता/उद्देश्यों के अनुरूप सूचना सुरक्षा लक्ष्यों और उद्देश्यों की पहचान करना.
3. सूचना सुरक्षा कार्यक्रम के दायरे और सीमाओं को परिभाषित करना.
4. कानूनी और नियामक आवश्यकताओं को समझना.
5. सूचना सुरक्षा कार्यान्वयन रणनीतियों को परिभाषित करना.
6. सूचना सुरक्षा कार्यक्रम के लिये बजट और संसाधनों की आवश्यकताओं का अनुमान लगाना.
7. संगठन के लिये सूचना सुरक्षा प्रबंधन की योजना बनाना और स्थापित करना.
8. साइबर खतरे के प्रबंधन ढांचे को परिभाषित करना.
9. सूचना सुरक्षा मापन मेट्रिक्स और अन्य प्रमुख प्रदर्शन संकेतकों को परिभाषित करना.
10. शीर्ष प्रबंधन से सूचना सुरक्षा योजना, बजट और संसाधनों के लिए अनुमोदन प्राप्त करना.

**(ख) नीति नियोजन (Policy Planning)**: इस भूमिका के तहत सुझाई गई जिम्मेदारियां निम्नलिखित हैं:-

1. सूचना सुरक्षा नीतियों, मानकों, प्रक्रियाओं, दिशानिर्देशों और प्रक्रियाओं की पहचान करना.

2. सुरक्षा नीतियों को बनाने, दस्तावेजीकरण, समीक्षा करने और लागू करने के लिए औपचारिक प्रक्रिया को परिभाषित करना.
3. सूचना सुरक्षा नीति को परिभाषित करना.
4. सूचना और सूचना एसेट के वर्गीकरण के लिए नीति को परिभाषित करना.
5. सूचना सुरक्षा नीतियों, प्रक्रियाओं, दिशानिर्देशों और प्रक्रियाओं का अनुमोदन प्राप्त करना.

**(ग) सूचना सुरक्षा प्रबंधन**: इस भूमिका के तहत मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ.) की निम्न जिम्मेदारियां हैं:-

1. रणनीतिक संगठन व्यापक सूचना सुरक्षा और जोखिम प्रबंधन योजना के विकास, रखरखाव, समीक्षा और सुधार में सहायता करना.
2. सभी संबंधितों को सूचना सुरक्षा नीतियों, प्रक्रियाओं और दिशानिर्देशों का प्रसार करना.
3. स्वीकृत सूचना सुरक्षा नीतियों, प्रक्रियाओं, दिशानिर्देशों और आई.एस.एम.एस. (ISMS) आदि के कार्यान्वयन को लागू करना.
4. संगठन की व्यावसायिक प्रक्रियाओं के साथ सूचना सुरक्षा प्रक्रियाओं को एकीकृत करना.
5. सुनिश्चित करना कि सूचना सुरक्षा विचार आई.टी. के साथ एकीकृत हैं.
6. सूचना सुरक्षा नीतियों, प्रक्रियाओं, मानकों, दिशानिर्देशों और प्रक्रियाओं, आई.एस.एम.एस. आदि की प्रभावशीलता का समय-समय पर मूल्यांकन और समीक्षा करना.
7. नई कमजोरियों/खतरों के संबंध में अलर्ट और सलाह जारी करना.
8. सूचना सुरक्षा घटनाओं और उल्लंघनों का रिकॉर्ड बनाए रखना.
9. सूचना सुरक्षा घटनाओं और उल्लंघनों के प्रभाव को कम करने के लिए उपचारात्मक कार्रवाई करना.
10. सूचना सुरक्षा और उल्लंघनों पर प्रबंधन अनुमोदन रिपोर्ट साझा करना.

## विद्युत क्षेत्र में साइबर सुरक्षा पर केंद्रीय विद्युत् प्राधिकरण दिशानिर्देशों के तहत प्रासंगिक प्रावधान

केंद्रीय विद्युत् प्राधिकरण साइबर सुरक्षा दिशानिर्देश, 2021 के अनुच्छेद 2 के अनुसार, विद्युत यूटिलिटीज को मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ. ) की नियुक्ति करना अनिवार्य है. उन्हें क्षेत्रीय-सी.ई.आर.टी. (Sectoral-CERT) और सूचना साझाकरण और विश्लेषण केंद्र-पावर पोर्टल (ISAC-Power) के साथ सी.आई.एस.ओ. और वैकल्पिक सी.आई.एस.ओ. के विवरण नियमित रूप से अपडेट करने होंगे. इस दिशानिर्देश के अनुसार साइबर एसेट्स (Cyber Assets) की साइबर सुरक्षा सुनिश्चित करने के लिए सी.आई.एस.ओ. की भूमिकाएं और जिम्मेदारी तय की जानी चाहिए. पावर यूटिलिटी के पास 24x7x365 आधार पर सूचना सुरक्षा प्रभाग (आई.एस.डी.) कार्यात्मक होना चाहिए, जिसका नेतृत्व सी.आई.एस.ओ. करता है. दिशानिर्देशों के तहत सी.आई.एस.ओ. को दी गई कुछ महत्वपूर्ण जिम्मेदारियां नीचे दी गई हैं:-

1. सी.आई.एस.ओ. आंतरिक और बाहरी प्रतिपुष्टि (Feedback) के आधार पर साइबर खतरों के मूल्यांकन और शमन योजनाओं के कार्यान्वयन और नियमित समीक्षा के लिए जिम्मेदार है.
2. सी.ई.आर.टी.-इन (CERT-In) द्वारा निर्धारित प्रारूपों में संगठन की सभी रिपोर्ट करने योग्य साइबर सुरक्षा घटनाओं की रिपोर्ट करना. सी.आई.एस.ओ. को यह सुनिश्चित करना है कि किसी भी साइबर सुरक्षा घटना के दौरान, आई.एस.डी. (ISD), आई.टी. (Information Technology) और ओ.टी. (Operational Technology) सिस्टम दोनों में साइबर सुरक्षा घटनाओं की निगरानी और घटनाओं के हर विवरण को सूक्ष्मता से रिकॉर्ड करता है.
3. सी.आई.एस.ओ. को यह सुनिश्चित करना चाहिए कि प्रत्येक साइबर घटना को निदेशक मंडल (Board of Directors) द्वारा अनुमोदित नवीनतम साइबर संकट प्रबंधन योजना [Cyber Crisis Management Plan (CCMP)] में

वर्णित साइबर सुरक्षा घटना प्रतिक्रिया योजना के अनुसार सख्ती से नियंत्रित किया जाता है.

4. सी.आई.एस.ओ. घटना का पता लगाने, घटना से निपटने, प्रत्येक घटना से सीखने और सी.ई.आर.टी.-इन (CERT-In) को रिपोर्ट करने के साथ-साथ आई.एस.ए.सी.-पावर (ISAC-Power) पोर्टल पर जानकारी अपलोड करने के विवरण को संकलित करने के लिए जिम्मेदार है.
5. सी.आई.एस.ओ. साइबर संकट प्रबंधन योजना (CCMP), रिस्क ट्रीटमेंट प्लान, नियामक की आवश्यकता के अनुपालन सहित सभी साइबर सुरक्षा संबंधी दस्तावेजों का संरक्षक है.

### निष्कर्ष

देश में साइबर सुरक्षा सुनिश्चित करने में मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ) एक महत्पूर्ण भूमिका अदा करता है. यह संगठनों के प्रमुख की जिम्मेदारी है कि वे साइबर सुरक्षा सुनिश्चित करने के लिए मुख्य सूचना सुरक्षा अधिकारी (सी.आई.एस.ओ.) नियुक्त करने का हरसंभव प्रयास करें.

*******

## 4. साइबर सुरक्षा में भारतीय विद्युत क्षेत्र की तैयारी

कु. स्वाति, सहायक निदेशक, सूचना प्रद्योगिकी एवं साइबर सुरक्षा
ईमेल- swati.cea @gov.in

### प्रस्तावना

डिजिटलीकरण में निरंतर प्रगति ने जहां एक तरफ जीवन की सुगमता के नए आयाम खोल दिए हैं, वहीं दूसरी ओर गंभीर जोखिम भी पेश किए हैं. वैश्विक दूरसंचार नेटवर्क में महत्वपूर्ण शक्ति संसाधनों के निरंतर एकीकरण के कारण सुरक्षा चुनौतियां उभर रही हैं. डिजिटलीकरण की सहायता से ऊर्जा को अधिक कुशल, सुलभ, नियंत्रित और किफायती बनाने की उम्मीद है. बड़े पैमाने पर साइबर हमलें अक्सर डिजिटल पद्धति पर निर्भर पावर ग्रिड के कामकाज को बधित करने की कुचेष्टा करते है, परिणामस्वरूप विद्युत् प्रणाली बाधित होने से राष्ट्रीय सुरक्षा, संचार, परिवहन और स्वास्थ्य सेवा को खतरा हो सकता है. भारतीय डेटा सुरक्षा परिषद (DSCI) द्वारा 2020 में राष्ट्रीय साइबर सुरक्षा रणनीति की अवधारणा की गई. DSCI की रिपोर्ट में भारत के लिए एक सुरक्षित, विश्वस्त, और जीवंत साइबर स्पेस सुनिश्चित करने के लिए 21 क्षेत्रों पर ध्यान केंद्रित किया गया है.

### साइबर सुरक्षा में ऊर्जा क्षेत्र की तैयारी

1. विदयुत क्षेत्र में साइबर सुरक्षा की तैयारियों के मद्देनजर सरकार ने तीन मुख्य उद्देश्य बनाए हैं जिसमें साइबर हमलों को रोकना, वल्नरबिलिटी को कम करना और साइबर हमलों से होने वाले नुकसान को कम करना शामिल हैं.
2. केंद्रीय विद्युत प्राधिकरण ने "केंद्रीय विद्युत प्राधिकरण (ग्रिड से कनेक्टिविटी के लिए तकनीकी मानक) (संशोधन) विनियम, 2019" में साइबर सुरक्षा पर धारा 3(10) के प्रावधान के तहत बिजली क्षेत्र में साइबर सुरक्षा पर दिशानिर्देश जारी किए हैं जिसके तहत साइबर-सुरक्षित इकोसिस्टम की स्थापना करने का उदेश्य है. साइबर सुरक्षा पर दिशानिर्देश की मदद से एक साइबर संरक्षित ढांचा निर्धारित करने, साइबर सुरक्षा खतरे की पूर्व चेतावनी, साइबर वल्नरबिलिटी प्रबंधन, जरूरी सेवाओं को सुरक्षित करने, साइबर आपूर्ति श्रृंखला जोखिमों को कम करने, ओपेन स्टैन्डर्ड के उपयोग को प्रोत्साहित करने, अनुसंधान और विकास को बढ़ावा देने, साइबर सुरक्षा के क्षेत्र में मानव संसाधन विकास इत्यादि को हासिल किया जा सकता हैं
3. भारत सरकार ने क्रिटिकल इंफ्रास्ट्रक्चर सेक्टर में साइबर सुरक्षा की जरूरतों की समीक्षा के बाद सेक्टर संबंधित सी.ई.आर.टी. (सर्ट- CERT) बनाए है. विद्युत मंत्रालय ने भारतीय विद्युत

क्षेत्र में साइबर सुरक्षा सुनिश्चित करने के लिए 6 क्षेत्रीय सी.ई.आर.टी. (थर्मल, हाइड्रो, ट्रांसमिशन, ग्रिड ऑपरेशन, नवीकरणीय ऊर्जा और विदयुत वितरण) स्थापित किये हैं.

4. भारत सरकार ने सूचना प्रौद्योगिकी अधिनियम-2000 के माध्यम से साइबर सुरक्षा मानकों, अनुपालनों, घटना प्रतिक्रिया और मार्गदर्शन के लिए समर्पित संगठन सी.ई.आर.टी-इन (CERT-In) की नींव रखी. सी.ई.आर.टी.- इन सभी हितधारकों (stakeholders) की साइबर जागरूकता बढ़ाने के लिए नियमित आधार पर कार्यशालाओं और प्रशिक्षण कार्यक्रमों का भी आयोजन करता है.
5. इसके अलावा भारत सरकार ने सूचना प्रौद्योगिकी अधिनियम, 2000 के प्रावधान के तहत राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC) को महत्वपूर्ण सूचना अवसंरचना संरक्षण के संबंध में एक राष्ट्रीय नोडल एजेंसी बनाया है. इसके कार्यों में से एक महत्वपूर्ण सूचना बुनियादी ढांचे के खिलाफ साइबर सुरक्षा के खतरों से बचाव के लिए सरकारी संस्थानों में रणनीतिक नेतृत्व और सुसंगतता प्रदान करना है.
6. साइबर सुरक्षा के क्षेत्र में सर्वोत्तम पद्धतियों का पालन करने, विद्युत क्षेत्र में विभिन्न साइबर सुरक्षा घटनाओं को साझा करने और उनका विश्लेषण करने के लिए आई.एस.ए.सी.-पावर (ISAC-Power) की कल्पना की गई थी. आई.एस.ए.सी.-पावर विद्युत मंत्रालय के तहत छह क्षेत्रीय सी.ई.आर.टी. के लिए साइबर सुरक्षा सम्बन्धित ज्ञान का साझा मंच हैं .
7. अनुसंधान, नवीनता, निर्माण-कौशल और प्रौद्योगिकी विकास के लिए सरकारी और महत्वपूर्ण क्षेत्रों में संगठनों की तैयारियों का आकलन करने के लिए साइबर सुरक्षा अभ्यास नियमित रूप से आयोजित किए जा रहे हैं. राष्ट्रीय सुरक्षा परिषद सचिवालय ने राष्ट्रीय साइबर सुरक्षा घटना प्रतिक्रिया अभ्यास (एन.सी.एक्स. - इंडिया) 2022 एक हाइब्रिड अभ्यास का आयोजन किया, जिसका उद्देश्य महत्व के "सूचना बुनियादी ढांचे" के खिलाफ साइबर सुरक्षा खतरों का जवाब देने के लिए सरकार में रणनीतिक नेतृत्व और सामंजस्य प्रदान करना था.
8. साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर): यह प्लेटफॉर्म इंटरनेट उपयोगकर्ताओं के लिए उपलब्ध है, जो बॉटनेट, मालवेयर इंफेक्शन और मालवेयर संक्रमण को रोकने और उनके कंप्यूटर/सिस्टम/उपकरणों को सुरक्षित करने के लिए किए जाने वाले उपायों के बारे में आम उपयोगकर्ताओं की जागरूकता बढ़ाता है.
9. राष्ट्रीय स्तर पर विभिन केंद्रीय एजेंसियां साइबर प्रभावित प्रणालियों को संचालन के लिए बहाल करने में सहायता, घटनाओं का विश्लेषण तथा इस तरह की घटनाओं की पुनरावृत्ति को रोकने के लिए सिस्टम प्रशासकों को अनुवर्ती कार्रवाई करने में सहायता प्रदान करती हैं.
10. केंद्रीय विद्युत प्राधिकरण द्वारा जारी दिशानिर्देशों के तहत, सी.ई.आर.टी.- आई.एन. (CERT-In) पैनलबद्ध ऑडिटर के माध्यम से विद्युत् प्रणालियों की नियमित ऑडिट अनिवार्य कर दी है.
11. साइबर सुरक्षा जागरूकता कार्यक्रम एक राष्ट्रीय जन जागरूकता प्रयास है जिसका उद्देश्य साइबर खतरों की समझ को बढ़ाना और नागरिकों को साइबर हमलों से बचाव के लिए सशक्त बनाना है. यह कार्यक्रम हर महीने के पहले बुधवार को आयोजित किया जाता है.

## चुनौतियाँ

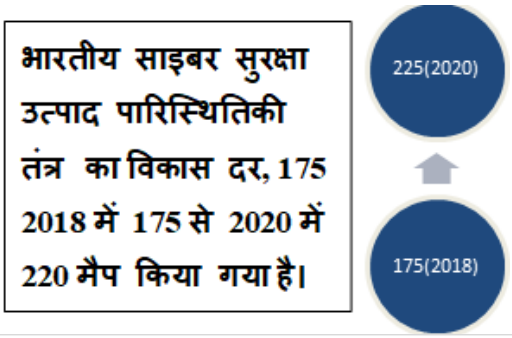
डिजिटल अर्थव्यवस्था को बढ़ावा देने के बीच भारत व्यापक डिजिटल निरक्षरता का सामना कर रहा है जो भारतीय नागरिकों को साइबर धोखाधड़ी, साइबर चोरी आदि के लिए अति-संवेदनशील बनाता है. आयातित इलेक्ट्रॉनिक उपकरणों के कठोर परीक्षण के लिए उपयुक्त परीक्षण प्रयोगशालाओं की तत्काल आवश्यकता है, ताकि यह सुनिश्चित किया जा सके

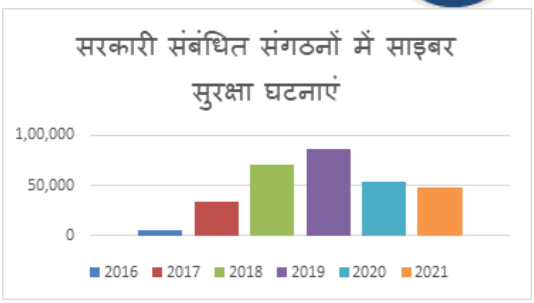
कि एम्बेडेड मैलवेयर (malware) फिट किए गए उपकरण पावरग्रिड सिस्टम का हिस्सा नहीं बन पायें.

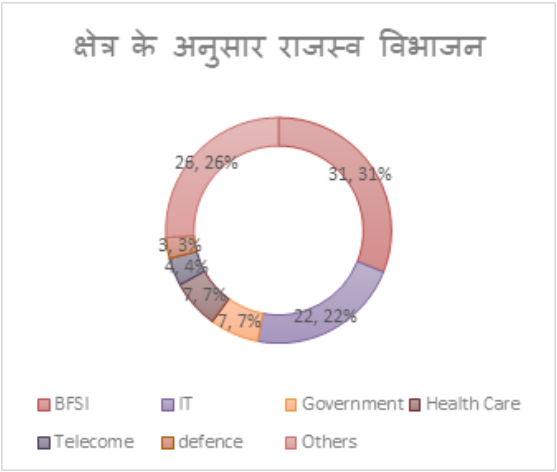
साइबर हमले को रोकने के हेतु सक्रिय प्रतिक्रिया के लिए केंद्रीय एजेंसियों के पास जो कर्मचारी हैं वह विश्व परिदृश्य के अनुसार बहुत कम संख्या होने के साथ-साथ अपेक्षाकृत कम कुशल भी हैं. गोपनीयता बढ़ाने वाली तकनीकों के बारे में कर्मचारियों में जागरूकता की कमी है. माना जाता है कि विश्व में अमेरिका, चीन, रूस, इज़राइल और यूनाइटेड किंगडम के पास सबसे विकसित साइबर युद्ध क्षमताएं हैं, जिन्होंने न केवल साइबर हमले के खिलाफ बचाव, बल्कि हानिकारक साइबर हमला करने की क्षमता विकसित करने में महत्वपूर्ण मात्रा में निवेश किया है. भारत का अपने पड़ोसी शत्रु देशों जैसे चीन के हैकर समूहों से खतरे दिन-प्रतिदिन बढ़ते जा रहे हैं. इन साइबर जोखिम से निपटने के लिए भारत को साइबर क्षेत्र में अपनी क्षमताओं को तेजी से बढ़ाने की आवश्यकता है.

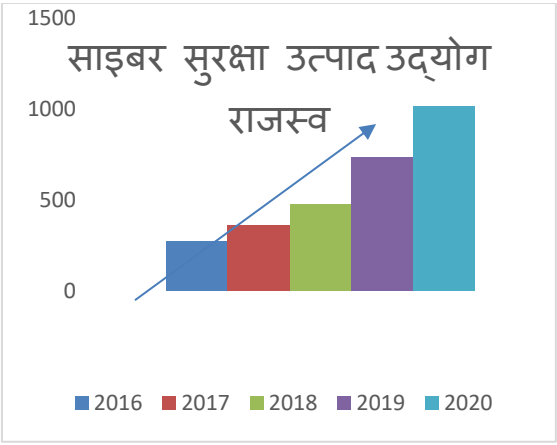
**प्रमुख उत्पाद**

| | |
|---|---|
| परिधि सुरक्षा | बहुकारक प्रमाणीकरण, उपयोगकर्ता इकाई व्यवहार विश्लेषणात्मक, वाइड एरिया नेटवर्क में सोफवेयर परिभाषित नेटवर्क. |
| गेटवे सुरक्षा | एंटी फ़िशिंग उपकरण, वेब अनुप्रयोग सुरक्षा, ईमेल सुरक्षा |
| संचालन सुरक्षा | समापन बिंदु का पता लगाने, प्रतिक्रिया प्रबंधित पहचान एवं प्रतिक्रिया और सुरक्षा व्यवस्था, स्वचालन और प्रतिक्रिया. |
| क्लाउड सुरक्षा | लंबी अवधि के लिए, व्यवसाय क्लाउड सुरक्षा और क्लाउड वर्कलोड सुरक्षा प्लेटफ़ॉर्म में निवेश को प्राथमिकता दे रहे हैं |
| साइबर सुरक्षा ढांचे | शून्य परीक्षण, सतत अनुकूल आशंका और विश्वास आकलन (CARTA) एवम सक्रिय रक्षा. |




*******

# 5. साइबर स्वच्छता केन्द्र

विनय वैष्णव,सहायक निदेशक, सूचना प्रद्योगिकी एवं साइबर सुरक्षा
ईमेल- vinay.vaishnav@nic.in

## प्रस्तावना

साइबर स्वच्छता केन्द्र (बॉटनेट शोधन और मालवेयर विश्लेषण केन्द्र), इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एम.ई.आई.टी.वाई) के तहत भारत सरकार की डिजिटल इंडिया पहल का एक हिस्सा है. जिसका लक्ष्य, भारत में बॉटनेट संक्रमणों का पता लगाकर एक सुरक्षित साइबर क्षेत्र बनाना तथा अंतिम प्रयोक्ताओं को सूचित करना, बॉटशोधन और सुरक्षा प्रणालियों को सक्षम करना है ताकि आगे संक्रमण से बचा जा सके. इसे "राष्ट्रीय साइबर सुरक्षा नीति" के उद्देश्यों के अनुसार स्थापित किया गया है, जो देश में एक सुरक्षित साइबर पारिस्थितिकी तंत्र बनाने की परिकल्पना करता है. यह केन्द्र इंटरनेट सेवा प्रदाताओं और उत्पाद/ कंपनियों / एंटीवायरस के साथ समन्वय और सहयोग से संचालित होता है. यह वेबसाइट उपयोगकर्ताओं / नागरिकों को उनके कंप्यूटर / उपकरणों को सुरक्षित करने के लिए सूचना और उपकरण प्रदान करती है. इस केन्द्र का संचालन भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (सर्ट-इन) द्वारा सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70 ख के प्रावधानों के तहत किया जा रहा है. यह बॉट्स द्वारा संक्रमित सिस्टम का पता लगाने के लिए उद्योग और शिक्षाविदों के साथ सहयोग करता है. इस केन्द्र का उद्देश्य इंटरनेट सेवा प्रदाताओं के सहयोग से नागरिकों / उपयोगकर्ताओं को उनके कंप्यूटर सिस्टम / मोबाइल डिवाइस की खराबी के बारे में सूचित करना और उन्हें अपने सिस्टम को ठीक करने में सहायता प्रदान करना है. यह केन्द्र आम नागरिकों / उपयोगकर्ताओं के बीच बॉटनेट, मालवेयर संक्रमण, उनके कंप्यूटर सिस्टम / मोबाइल डिवाइस / घरेलू राउटर जैसे उपकरणों को सुरक्षित करने और मालवेयर संक्रमण को रोकने के लिए किए जाने वाले उपायों के बारे में जागरूकता बढ़ाता है.

## मिशन

बॉटनेट/मालवेयर खतरों के बारे में सूचना सामग्री प्रदान करके और उपचारात्मक उपायों का सुझाव देकर डिजिटल इंडिया के सूचना प्रौद्योगिकी के बुनियादी ढांचे की साइबर सुरक्षा को बढ़ाना. निम्न सुरक्षा उपकरण साइबर स्वच्छता केन्द्र द्वारा उपलब्ध कराया जाता है:

**मुफ्त बॉट-निष्कासन उपकरण - (टूल) माइक्रोसॉफ्ट विंडोज हेतु:** नागरिक उपयोगकर्ता / अपने डिजिटल डिवाइस के लिए निम्नलिखित में से किसी भी बॉट निष्कासन उपकरण (टूल) का उपयोग मुफ्त में कर सकते हैं:

- क्विक हील
- ई-स्कैन एंटीवायरस
- के-7 सिक्योरिटी

**मुफ्त बॉट निष्कासन उपकरण (टूल) - एंड्रॉइड मोबाइल हेतु:**

- ई-स्कैन एंटीवायरस

**निःशुल्क मोबाइल सुरक्षा एप्लिकेशन - एंड्रॉइड मोबाइल हेतु:**

सी-डैक हैदराबाद ने इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय के सहयोग से एम-कवच 2 विकसित किया है. सी-डैक हैदराबाद एंड्रॉइड मोबाइल सुरक्षा एप्लिकेशन प्रदान कर रहा है.

**अन्य प्रासंगिक उपकरण:** यू.एस.बी. प्रतिरोध: यह उपकरण (टूल) एक डेस्कटॉप कंप्यूटर सुरक्षा समाधान है, जो पेन ड्राइव, बाहरी हार्ड ड्राइव, सेल फोन और अन्य समर्थित यू.एस.बी. मॉस स्टोरेज (विपुल भंडारण) उपकरण जैसे हटाने योग्य स्टोरेज मीडिया के उपयोग को नियंत्रित करता है.

**ऐप-संविद :** यह उपकरण ऐप-संविद (AppSamvid) विंडोज ऑपरेटिंग सिस्टम के लिए एक डेस्कटॉप आधारित एप्लीकेशन श्वेतसूचीकरण समाधान है. यह

केवल पूर्व-अनुमोदित निष्पादन योग्य फ़ाइल समूह के निष्पादन के लिए अनुमति देता है.

**ब्राउज़र :** यह उपकरण (टूल) एक ब्राउज़र विस्तार (एक्सटेंशन) है जो अनुमान और पूर्वाग्रह के आधार पर वेब ब्राउज़र के माध्यम से किए जाने वाले दुर्भावनापूर्ण एचटीएमएल (HTML) और जावास्क्रिप्ट (JavaScript attacks) हमलों का पता लगाता है और उन से बचाव करता है. यह उपयोगकर्ता को किसी भी दुर्भावनापूर्ण वेब पेज पर जाने पर चेतावनी देता है और वेब पेज की विस्तृत विश्लेषण कर खतरे की वर्णनात्मक प्रतिवेदन प्रदान करता है.

### उपसंहार

विद्युत क्षेत्र की लगभग सभी कंपनियां सीईआरटी-इन के साइबर स्वच्छता केन्द्र पर ऑन-बोर्ड हो गई हैं. नेटवर्क की सुरक्षा के लिए नवीनतम साइबर खतरों / कमजोरियों और प्रति-उपायों के संबंध में नियमित अलर्ट और सलाह नियमित आधार पर जारी की जाती हैं.

*******

## 6. भारत में साइबर कानून

विकास कुमार, उपनिदेशक, सूचना प्रद्योगिकी एवं साइबर सुरक्षा
ईमेल- kumar.vikash1105@gov.in

### प्रस्तावना

मनुष्यता के इतिहास में एक सभ्य समाज के साथ-साथ अपराध भी निरंतर बने रहे हैं. समय और परिस्थितियों के अनुसार अपराधों के प्रारूप में भी परिवर्तन होता रहा है. आज वर्तमान समय में साइबर अपराध जैसा शब्द सुनने मे आता है.

प्रौद्योगिकी और इलेक्ट्रॉनिक मीडिया के विकास के बाद कंप्यूटर से संबंधित अपराधों का जन्म हुआ है जिसे आमतौर पर "साइबर अपराध" कहा जाता है. इन अपराधों की व्यापक वृद्धि वैश्विक चिंता का विषय बन गई है तथा इस प्रकार के अपराध एक नई चुनौती के रूप में विश्व भर में सामने आये हैं. इन अपराधों में संचार सेवाओं की चोरी, औद्योगिक जासूसी, साइबर-स्पेस में अश्लील और आपत्तिजनक सामग्री का प्रसार, इलेक्ट्रॉनिक मनी लॉन्ड्रिंग और कर चोरी, इलेक्ट्रॉनिक क्रूरता, आतंकवाद और जबरन वसूली जैसी अवैध कंप्यूटर से संबंधित गतिविधियों की एक विस्तृत श्रृंखला शामिल है. इसके साथ ही इसमे टेली-मार्केटिंग धोखाधड़ी, टेली-संचार का अवैध अवरोधन भी शामिल है.

### साइबर अपराध

साइबर अपराध शब्द संसद द्वारा अधिनियमित किसी भी क़ानून या अधिनियम में कहीं भी परिभाषित नहीं है. एक मायने में, यह पारंपरिक अपराध की अवधारणा से मौलिक रूप से अलग नहीं है क्योंकि दोनों में सामान प्रकार के आचरण शामिल है, जो कानून के उल्लंघन का कारण बनता है और इसलिए यह राज्य द्वारा दंडनीय है. साइबर अपराध को किसी भी अवैध आपराधिक गतिविधि के रूप में परिभाषित किया जा सकता है जो कंप्यूटर का उपयोग या तो एक उपकरण, लक्ष्य या आगे अपराध करने के साधन के रूप में करता है. पारंपरिक अपराध शारीरिक रूप से उपस्थित होकर किए जाते हैं और उन्हीं अपराधों को जब दूर बैठकर कंप्यूटर के माध्यम से किया जाता है तब वह साइबर अपराध बन जाते हैं.

## भारत में साइबर कानून

विश्व के लगभग सभी देशों ने साइबर अपराध से निपटने हेतु कानून बनाए हैं. भारत में साइबर अपराधो को सूचना प्रौद्योगिकी अधिनियम, 2000 द्वारा सम्बोधित किया जाता है. साइबर अपराधों को नियंत्रित करने के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 (“आई.टी. अधिनियम”), 17 अक्टूबर, 2000 को प्रभावी हुआ. आगे समय की जरूरत के अनुसार सूचना प्रौद्योगिकी संशोधन विधेयक, 2008 द्वारा इस अधिनियम में संशोधन किया गया. अधिनियम का मुख्य उद्देश्य इलेक्ट्रॉनिक कॉमर्स को कानूनी मान्यता प्रदान करना और सरकार के साथ इलेक्ट्रॉनिक रिकॉर्ड दाखिल करने की सुविधा प्रदान करना है. निम्नलिखित अधिनियम, नियम और विनियम साइबर कानूनों के अंतर्गत आते हैं:

1. सूचना प्रौद्योगिकी अधिनियम, 2000
2. सूचना प्रौद्योगिकी (प्रमाणन प्राधिकारी) नियम, 2000
3. सूचना प्रौद्योगिकी (सुरक्षा प्रक्रिया) नियम, 2004
4. सूचना प्रौद्योगिकी (प्रमाणन प्राधिकारी) विनियम, 2001

## सूचना प्रौद्योगिकी अधिनियम, 2000 के साइबर सुरक्षा संबंधी महत्वपूर्ण प्रावधान

सूचना प्रौद्योगिकी अधिनियम, 2000, इंटरनेट और कंप्यूटर से जुड़ी हुई चीजों के लिए भारत में अधिनियमित एक महत्वपूर्ण अधिनियम है. भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 उन साइबर कार्यों का उल्लेख करते हैं जिन्हें भारत में अपराध बनाकर प्रतिबंधित किया गया है. विभिन्न अपराध और उनके लिए प्रदान की गई सजा सूचना प्रौद्योगिकी अधिनियम के अध्याय 11 और 11(ए) में निहित हैं. संक्षेप में यह अपराध निम्न है:-

1. **अनधिकृत पहुंच (धारा 43):**- यह खंड बताता है कि कोई भी व्यक्ति जो कंप्यूटर, कंप्यूटर सिस्टम या कंप्यूटर तक पहुंच प्राप्त करता है और उसे असुरक्षित करता है और यह कार्य उसके द्वारा कंप्यूटर के मालिक या उसके प्रभारी व्यक्ति की अनुमति के बिना किया जाता है तब पीड़ित व्यक्ति को एक करोड़ रुपये से अधिक के मुआवजे के रूप में नुकसान का भुगतान करने के लिए उत्तरदायी होगा.

   आई.टी. अधिनियम की धारा 2(1)(ए) में परिभाषित "एक्सेस" शब्द का अर्थ है "कंप्यूटर, कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क के तार्किक, अंकगणितीय या मौद्रिक कार्य संसाधनों में प्रवेश प्राप्त करना, निर्देश देना या संचार करना. "निम्नलिखित कृत्यों को शब्द के दायरे में लाने के लिए माना गया है: अधिनियम द्वारा परिकल्पित "पहुँच":- एक कंप्यूटर पर गैरकानूनी रूप से स्विच करना, कंप्यूटर पर स्थापित एक सॉफ्टवेयर प्रोग्राम का उपयोग करना, एक फ्लॉपी डिस्क की सामग्री को अवैध रूप से देखना, एक कंप्यूटर को अवैध रूप से बंद करना, अवैध रूप से कंप्यूटर प्रिंट-आउट लेना, इंटरनेट पर लॉगिंग; और कंप्यूटर को पिंग करना. अनधिकृत पहुंच का अपराध तब पूरा होता है जब डेटा, डेटा-बेस या जानकारी को एक कंप्यूटर से दूसरे कंप्यूटर में डाउनलोड, कॉपी या अवैध रूप से निकाला जाता है.

2. **सूचना, रिटर्न आदि प्रस्तुत करने में विफलता (धारा 44)**:- जहां किसी व्यक्ति को इस अधिनियम या इसके तहत बनाए गए किसी भी नियम के तहत नियंत्रक या प्रमाणन प्राधिकारी को कोई दस्तावेज, रिटर्न या रिपोर्ट प्रस्तुत करने की आवश्यकता होती है और वह उसे प्रस्तुत करने में विफल रहता है, वह प्रत्येक विफलता के लिए 1.5 लाख रुपये से अधिक का जुर्माना देने के लिए उत्तरदायी होगा और चूक के मामले में, प्रतिदिन के लिए 5,000/- रुपये का जुर्माना, जिसके दौरान ऐसी विफलता या चूक जारी रहती है. अधिनियम की धारा 45, अधिनियम के तहत बनाए गए किसी भी नियम के उल्लंघन के लिए दंड का प्रावधान करती है जिसके लिए

अधिनियम में विशेष रूप से कोई दंड प्रदान नहीं किया गया है. इस प्रकार, यह धारा अवशिष्ट दंड से संबंधित है और अधिनियम की कुछ धाराओं पर लागू होती है. अधिनियम की धारा 46 उल्लंघनकर्ता को उसके मामले में प्रतिनिधित्व करने का उचित अवसर देने के बाद उस पर लगाए जाने वाले दंड के न्याय-निर्णयन का प्रावधान करती है. न्याय-निर्णयन अधिकारी के पास उन मामलों का न्याय-निर्णयन करने की शक्ति होगी जिनमें चोट या क्षति का दावा पांच करोड़ रुपये से अधिक नहीं है. हालांकि, जहां दावा या क्षति इस सीमा से अधिक है, न्याय-निर्णयन का अधिकार क्षेत्र सक्षम न्यायालय में निहित होगा.

3. **कंप्यूटर स्रोत दस्तावेजों (कोड) के साथ छेड़छाड़ (धारा 65)**:- कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़ को धारा 65 के तहत दंडनीय बनाया गया है. धारा 65 के प्रयोजन के लिए, छेड़छाड़ का अर्थ है कंप्यूटर स्रोत दस्तावेज़ों (कोड) को जानबूझकर छुपाना, नष्ट करना, परिवर्तन करना, दूसरे को कंप्यूटर सोर्स कोड बदलने के लिए प्रेरित करना आदि.

4. **हैकिंग (धारा 66)**:- हैकिंग के आवश्यक तत्व किसी भी व्यक्ति को गैरकानूनी तरीके से नुकसान या क्षति पहुंचाने का इरादा है या इस बात का ज्ञान होना कि कंप्यूटर संसाधन दस्तावेज़ में रहने वाली जानकारी को छुपाने, नष्ट करने या बदलने से किसी भी व्यक्ति को नुकसान होगा. इस धारा के तहत यह अपराध तीन साल तक के कारावास या दो लाख रुपये तक के जुर्माने या दोनों से दंडनीय है. पहचान की चोरी हैकिंग का एक सामान्य रूप है जो तेजी से बढ़ता हुआ साइबर अपराध है जो तब होता है जब कोई व्यक्ति किसी धोखाधड़ी को जारी रखने के लिए दूसरे की व्यक्तिगत जानकारी को बिना उसकी जानकारी के विनियोजित करता है.
5. **एक निजी क्षेत्र की छवि (निजी प्रोफ़ाइल) को कैप्चर करना (धारा 66 ई)**:- इस धारा में कहा गया है, "जो कोई भी जानबूझकर किसी भी व्यक्ति की गोपनीयता का उल्लंघन करने वाली परिस्थितियों में उसकी सहमति के बिना किसी व्यक्ति के निजी क्षेत्र की छवि को कैप्चर, प्रकाशित या प्रसारित करता है, उसे कारावास से दंडित किया जाएगा, जिसे तीन साल तक बढ़ाया जा सकता है या 2 लाख रुपये से अधिक के जुर्माने या दोनों के साथ. अधिनियम की धारा 66 में धारा 66ए से 66एफ अश्लील संदेश भेजने, पहचान की चोरी, धोखा देने जैसे अपराधों के लिए कंप्यूटर संसाधनों का उपयोग कर प्रतिरूपण, इंटरनेट सुरक्षा का उल्लंघन करने के लिए सजा निर्धारित करता है.
6. **इलेक्ट्रॉनिक रूप में अश्लील सूचना का प्रकाशन (धारा 67)**:- इंटरनेट पर अश्लीलता, सूचना प्रौद्योगिकी अधिनियम की धारा 67 के तहत दंडनीय कार्य है. वेबसाइट पर अश्लील सामग्री का प्रसार एक अपराध है जिसमें तीन साल तक की कैद या जुर्माना हो सकता है. जो दो लाख रुपये तक या दोनों के साथ हो सकता है.
7. **नियंत्रक के निर्देशों का पालन करने में विफलता (धारा 68)**:- धारा 68 नियंत्रक या प्रमाणन प्राधिकरण को किसी भी कंप्यूटर संसाधन के माध्यम से प्रेषित किसी भी जानकारी को इंटरसेप्ट करने के लिए अधिकृत करता है, जब भी ऐसा करना उचित हो. इस तरह के आदेश का पालन करने में विफल रहने पर व्यक्ति को तीन साल तक की कैद या दो लाख रुपये तक का जुर्माना या दोनों हो सकता है. तथापि, यदि आई.टी. के किसी भी प्रावधान का अनुपालन सुनिश्चित करना आवश्यक हो तो नियंत्रक या प्रमाणन प्राधिकारी द्वारा आदेश पारित किया जाना चाहिए.
8. **किसी कंप्यूटर संसाधन के माध्यम से किसी सूचना के अवरोधन या निगरानी या डिक्रिप्शन के निर्देश जारी करने की शक्ति (धारा 69)**:- नियंत्रक या प्रमाणन प्राधिकारी या ऐसे प्राधिकरण का कोई कर्मचारी अधिकृत है. किसी भी कंप्यूटर संसाधन के माध्यम से प्रेषित किसी

भी जानकारी को इंटरसेप्ट करने के लिए जब भारत की संप्रभुता या अखंडता, राज्य की सुरक्षा, विदेशी राज्यों के साथ मैत्रीपूर्ण संबंधों या सार्वजनिक व्यवस्था के हित में या किसी संज्ञेय अपराध को करने के लिए उकसाने को रोकने के लिए ऐसा करना समीचीन है. 2008 के संशोधन अधिनियम द्वारा मूल अधिनियम में डाली गई नई धारा 69-ए केंद्र सरकार को भारत की संप्रभुता और अखंडता के हित में, किसी भी कंप्यूटर संसाधन के माध्यम से किसी भी जानकारी की सार्वजनिक पहुंच को अवरुद्ध करने के लिए निर्देश जारी करने का अधिकार देती है. हालाँकि, ऐसा करने के कारणों को उन्होंने लिखित रूप में दर्ज किया. मध्यस्थ जो इस धारा के तहत सरकार द्वारा जारी निर्देशों का पालन करने में विफल रहता है, उसे एक वर्ष की अवधि के लिए कारावास से दंडित किया जाएगा, जिसे सात साल तक बढ़ाया जा सकता है, और जुर्माना भी लगाया जा सकता है. 2008 के आई.टी. (संशोधन) अधिनियम द्वारा सम्मिलित की गई धारा 69-बी सरकार को साइबर सुरक्षा उद्देश्यों के लिए किसी भी कंप्यूटर संसाधन के माध्यम से ट्रैफिक डेटा या सूचना की निगरानी और संग्रह को अधिकृत करने का अधिकार देती है. मध्यस्थ द्वारा इस प्रावधान के उल्लंघन की सजा तीन साल तक की कैद और जुर्माना भी हो सकता है. इस खंड में संदर्भित जानकारी ई-मेल संदेशों पर लागू होगी.

9. **प्रोटेक्टेड सिस्टम तक पहुंच (धारा 70)**:- धारा 70 में निहित विशेष प्रावधान संरक्षित सिस्टम से संबंधित हैं. यह खंड प्रदान करता है कि उपयुक्त सरकार, आधिकारिक राजपत्र में अधिसूचना द्वारा, कभी भी घोषित कर सकती है. कंप्यूटर, कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क एक संरक्षित प्रणाली होने के लिए इस धारा के प्रावधानों के उल्लंघन में किसी भी प्रकार के कारावास के साथ सजा जो दस साल तक बढ़ाई जा सकती है और जुर्माने के लिए भी उत्तरदायी होगा. दो नए खंड, धारा 70-ए और 70-बी को सूचना प्रौद्योगिकी अधिनियम द्वारा मूल अधिनियम में सम्मिलित किया गया है. (संशोधन) अधिनियम, 2008 जो एक राष्ट्रीय नोडल एजेंसी की नियुक्ति का प्रावधान करता है जो केंद्रीय सूचना अवसंरचना के संरक्षण से संबंधित अनुसंधान और विकास सहित सभी उपायों के लिए जिम्मेदार होगी. सरकार का कोई भी संगठन इस उद्देश्य के लिए राष्ट्रीय नोडल एजेंसी के रूप में नामित किया जा सकता है. इस प्रकार नियुक्त राष्ट्रीय नोडल एजेंसी को भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In) (धारा 70-बी) कहा जाएगा.
10. **गलत बयानी (धारा 71)**:- नियंत्रक या प्रमाणन प्राधिकारी को डिजिटल हस्ताक्षर प्रमाणीकरण के लिए आवेदन करते समय किसी भी गलत बयानी को अधिनियम की धारा 71 के तहत अपराध बनाया गया है. दोनों, किसी भी भौतिक तथ्य की गलत बयानी और/या लाइसेंस या डिजिटल हस्ताक्षर प्रमाण पत्र प्राप्त करने के लिए नियंत्रक या प्रमाणन प्राधिकारी से किसी भी महत्वपूर्ण तथ्य को छुपाना एक अपराध होगा. लाइसेंस के लिए आवेदन करते समय एक व्यक्ति को आई.टी. (प्रमाणन प्राधिकारी) नियम के नियम 10 के अनुसार आवश्यक फॉर्म भरना होता है. डिजिटल हस्ताक्षर प्रमाण पत्र के लिए आवेदन करने के मामले में, एक व्यक्ति को अपने बारे में पूरी जानकारी के साथ नियम 23 द्वारा निर्धारित फॉर्म भरना होगा. यदि उपरोक्त में से किसी भी जानकारी/विवरण को गलत तरीके से प्रस्तुत किया जाता है या छुपाया जाता है, तो इस तरह के गलत बयानी के दोषी व्यक्ति को दो साल तक के कारावास या एक लाख रुपये तक के जुर्माने या दोनों से दंडित किया जा सकता है.
11. **गोपनीयता भंग करने के लिए दंड (धारा 72)**:- कोई भी व्यक्ति जो गलत तरीके से किसी इलेक्ट्रॉनिक रिकॉर्ड, पुस्तक, रजिस्टर तक पहुंच सुरक्षित करता है, पत्राचार, सूचना, दस्तावेज या

अन्य सामग्री आई.टी. अधिनियम या उसके तहत बनाए गए नियम के किसी भी प्रावधान के उल्लंघन में कारावास से दंडित किया जा सकता है जिसे दो साल तक बढ़ाया जा सकता है या एक लाख रुपये तक का जुर्माना या दोनों से दंडित किया जा सकता है. हालांकि, यह प्रावधान किसी व्यक्ति की व्यक्तिगत जानकारी को उसके ई-मेल सेवा प्रदाता द्वारा वेबसाइट द्वारा प्रकट किए जाने पर लागू नहीं होगा. सूचना प्रौद्योगिकी (संशोधन) अधिनियम द्वारा एक नई धारा 72-ए डाली गई है, कानूनी अनुबंध के उल्लंघन में सूचना के प्रकटीकरण के लिए दंड प्रदान करना और किसी व्यक्ति को गलत तरीके से नुकसान पहुंचाने या प्रकटीकरण द्वारा गलत लाभ प्राप्त करने के इरादे से व्यक्तिगत जानकारी वाली किसी भी सामग्री तक पहुंच प्राप्त करना. यह अपराध कारावास से, जिसकी अवधि तीन वर्ष तक हो सकती है, या जुर्माने से, जो पांच लाख तक हो सकता है, या दोनों से दंडनीय होगा.

12. **कुछ विवरणों में डिजिटल हस्ताक्षर प्रमाण पत्र का झूठा प्रकाशन (धारा 73)**:- अधिनियम की धारा 73 के तहत दंडनीय सायबर अपराध में दंड दो साल तक के कारावास या एक लाख तक के जुर्माने तक बढ़ाया जा सकता है. यह कहा जा सकता है कि ग्राहक द्वारा डिजिटल हस्ताक्षर प्रमाणपत्र की स्वीकृति से संबंधित प्रावधान आई. टी. अधिनियम की धारा 41 में निहित हैं जबकि डिजिटल हस्ताक्षर प्रमाणपत्र के निलंबन से संबंधित प्रावधान अधिनियम की धारा 37 में निहित हैं. आई.टी. अधिनियम के साथ एक डिजिटल हस्ताक्षर प्रमाणपत्र उपलब्ध कराने पर रोक लगाता है. यह ज्ञान कि (ए) प्रमाण पत्र में सूचीबद्ध प्रमाणीकरण प्राधिकारी ने इसे जारी नहीं किया है; या (बी) प्रमाण पत्र में सूचीबद्ध ग्राहक ने इसे स्वीकार नहीं किया है: या (सी) प्रमाण पत्र निरस्त या निलंबित कर दिया गया है

13. **कपटपूर्ण उद्देश्यों के लिए डिजिटल हस्ताक्षर प्रमाणपत्र का प्रकाशन (धारा 74)**:-

यह धारा प्रदान करती है कि जो कोई भी जानबूझकर किसी धोखाधड़ी या गैरकानूनी उद्देश्य के लिए डिजिटल हस्ताक्षर प्रमाणपत्र बनाता है, प्रकाशित करता है या अन्यथा उपलब्ध कराता है या जानबूझकर प्रकाशित करता है या किसी ऐसे उद्देश्य के लिए उपलब्ध कराता है, आई.टी. अधिनियम के तहत अपराध करता है और अपराधी को दंडित किया जा सकता है उस कारावास से, जिसकी अवधि दो वर्ष तक की हो सकेगी, या जुर्माने से, जो एक लाख रुपए तक का हो सकेगा, या दोनों से. अपराधों का शमन (समझौता) (धारा 77-ए):- आई.टी. (संशोधन) अधिनियम 2008 द्वारा मूल अधिनियम में नई धारा डाली गई. सक्षम क्षेत्राधिकार की अदालत द्वारा अधिनियम के तहत अपराधों की कंपाउंडिंग का प्रावधान करता है, बशर्ते वे आजीवन कारावास या तीन साल से अधिक की अवधि के कारावास से दंडनीय न हों. हालांकि, अदालत किसी भी अपराध को कम नहीं करेगी जहां आरोपी अपनी पिछली सजा के कारण बढ़ी हुई सजा के लिए उत्तरदायी है या आरोपी पर किसी सामाजिक-आर्थिक अपराध के लिए आरोप लगाया गया है या फिर अपराध अवयस्क या महिला के विरुद्ध किया गया है. इस अधिनियम के अंतर्गत तीन साल की सजा वाले अपराध जमानती होंगे (धारा 77-बी). 2008 के संशोधन अधिनियम द्वारा मूल अधिनियम में जोड़ा गया नया खंड उपबंध करता है कि अधिनियम के तहत तीन साल तक की सजा के अपराध संज्ञेय और जमानती होंगे, भले ही दंड प्रक्रिया संहिता, 1973 के उपबंध इस मामले में भिन्न हो. प्रारंभ में, अधिनियम के तहत अपराध की जांच करने की शक्ति एक पुलिस अधिकारी को अधिनियम की धारा 78 के तहत पुलिस उपाधीक्षक के पद से नीचे नहीं थी, लेकिन इस धारा में आई.टी. (संशोधन) अधिनियम, 2008 के बाद अब यह शक्ति पुलिस निरीक्षक में निहित है.

**उपसंहार**

हालाँकि, यह कहा जाना चाहिए कि सूचना प्रौद्योगिकी अधिनियम, 2000 का प्राथमिक उद्देश्य 2000 ई-कॉमर्स के लिए एक सक्षम वातावरण बनाना था परंतु इस अधिनियम मे साइबर सुरक्षा को भी सामान्य महत्व दिया गया है. तेजी से बदलते इंटरनेट और सूचनाओं से उत्पन्न चुनौतियों से निपटने में यह अधिनियम पर्याप्त रूप से सक्षम है.

*******

## 7. विद्युत क्षेत्र में सरकार द्वारा साइबर सुरक्षा सुनिश्चित करने की पहल

सुरभी अग्रवाल, सहायक निदेशक-1, सूचना प्रौद्योगिकी व साईबर सुरक्षा प्रभाग
ईमेल- surabhiagarwal.cea @gov.in

**1. केंद्रीय विद्युत प्राधिकरण (साइबर सुरक्षा के लिये दिशा-निर्देश):**

एक सुरक्षित साइबर पारिस्थितिकी तंत्र बनाने के लिए, विद्युत मंत्रालय एवं केंद्रीय विद्युत प्राधिकरण (के.वि.प्रा.) ने साइबर सुरक्षा के लिए दिशानिर्देश जारी किए हैं, जो विद्युत क्षेत्र के लिए साइबर सुरक्षा तैयारियों की स्तर को बढ़ाने के लिए आवश्यक कार्यों की रूपरेखा तैयार करते हैं. इन दिशा निर्देशों को हितधारकों के साथ विचार-विमर्श और साइबर सुरक्षा विशेषज्ञ एजेंसियों के इनपुट के पश्चात तैयार किया गया है. इनमें भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (सर्ट-इन), राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना केंद्र (एन.सी.आई.आई.पी.सी.), नेशनल सोसाइटी ऑफ कॉलेजिएट स्कॉलर्स (एन.एस.सी.एस) और अन्य संस्थान शामिल हैं.

**2. भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन):**

सर्ट-इन भारतीय साइबर स्पेस को सुरक्षित करने के उद्देश्य से भारत सरकार की इलेक्ट्रानिकी और सूचना प्रौद्योगिकी मंत्रालय का एक कार्यात्मक संगठन है. सूचना प्रौद्योगिकी संशोधन अधिनियम 2008 के अंतर्गत सर्ट-इन को राष्ट्रीय एजेंसी के रूप मे साइबर सुरक्षा संबंधित विभिन्न कार्यों के लिए नामित किया गया है. सर्ट-इन द्वारा विद्युत क्षेत्र मे निम्नलिखित योगदान प्रदान किया जाता है:

- साइबर घटनाओं पर जानकारी का संचयन, विश्लेषण और प्रसार
- साइबर सुरक्षा की घटनाओं का पूर्वनुमान और चेतावनियाँ
- साइबर सुरक्षा की घटनाओं से निपटने के लिए आपातकालीन उपाय
- साइबर घटनाओं की प्रतिक्रिया गतिविधियों का समन्वयीकरण
- दिशा-निर्देश, सलाह, भेद्यता नोट, सुरक्षा अभ्यास से संबंधित जानकारी के श्वेतपत्र, साइबर घटनाओं की प्रतिक्रियाओं, रोकथाम, प्रतिक्रिया और रिपोर्टिंग

**3. राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना केंद्र (एन.सी.आई.आई.पी.सी.):**

सूचना प्रौद्योगिकी संशोधन अधिनियम 2008 के द्वारा महत्वपूर्ण सूचना अवसंरचना की संरक्षण के लिए एन.सी.आई.आई.पी.सी. को स्थापित किया गया है. केंद्र सरकार द्वारा स्थापित एन.सी.आई.आई.पी.सी. हमारे देश की महत्वपूर्ण जानकारी की रक्षा के लिये गठित किया गया संस्थान है, जिसका राष्ट्रीय सुरक्षा, आर्थिक विकास एवं सार्वजनिक स्वास्थ्य देखभाल पर व्यापक प्रभाव पड़ता है.

एन.सी.आई.आई.पी.सी. ने मुख्य रूप से निम्नलिखित महत्वपूर्ण क्षेत्रों को चिन्हित किया है:

- विद्युत व ऊर्जा
- बैंकिंग, वित्तीय सेवाएं व बीमा
- दूरसंचार परिवहन
- सरकारी क्षेत्र
- सामरिक व सार्वजनिक उद्यम

विद्युत क्षेत्र के संगठनों / उपक्रमों / यूटिलिटियों द्वारा अपनी महत्वपूर्ण व्यावसायिक प्रक्रियाओं और अंतर्निहित सूचना बुनियादी ढांचे के विवरण को पहचान कर एन.सी.आई.आई.पी.सी. के परामर्श से सी.आई.आई. (क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर) घोषित किया जाता है तथा एन.सी.आई.आई.पी.सी. से जारी दिशा-निर्देशों के अनुरूप संगठनों / उपक्रमों / यूटिलिटियों में साइबर सुरक्षा नीति को लागू किया जाता है.

### 4. मुख्य सूचना सुरक्षा अधिकारियों (सी.आई.एस.ओ.) की नियुक्ति:

भारत सरकार ने सी.आई.एस.ओ. के लिए दिशानिर्देश प्रकाशित किए हैं, जिसमें सूचना प्रौद्योगिकी संबंधित बुनियादी ढांचे, वेबसाइट, पोर्टल, ऐप्स की सुरक्षा एवं उससे संबंधित अनुपालन के लिए सर्वोत्तम प्रथाओं को रेखांकित किया गया है. सी.आई.एस.ओ. द्वारा प्रत्येक तकनीकी नवाचार के साथ उत्पन्न होने वाली सुरक्षा आवश्यकताओं की पहचान और दस्तावेजीकरण किया जाता है. भारत सरकार के अंतर्गत सभी मंत्रालयों/विभागों/संगठनों में सी.आई.एस.ओ. की नियुक्ति की जाती है तथा मंत्रालयो/विभागो/संगठनो को अपनी सूचना सुरक्षा आवश्यकताओं की पहचान व प्रलेखन सी.आई.एस.ओ. के माध्यम से कराया जाता है. विद्युत क्षेत्र के सभी संगठनों / उपक्रमों / यूटिलिटियों में मुख्य सूचना सुरक्षा अधिकारी एवं वैकल्पिक मुख्य सूचना सुरक्षा अधिकारी की नियुक्ति पर विशेष जोर दिया जाता है.

### 5. साइबर स्वच्छता केंद्र (बॉटनेट शोधन और मालवेयर विश्लेषण केन्द्र):

साइबर स्वच्छता केन्द्र (बॉटनेट शोधन और मालवेयर विश्लेषण केन्द्र), इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एम.ई.आई.टी.वाई) के तहत भारत सरकार की डिजिटल इंडिया पहल का एक हिस्सा है. जिसका लक्ष्य, भारत में बॉटनेट संक्रमणों का पता लगाकर एक सुरक्षित साइबर क्षेत्र बनाना तथा अंतिम प्रयोक्ताओं को सूचित करना, बॉटशोधन और सुरक्षा प्रणालियों को सक्षम करना, ताकि आगे संक्रमण से बचा जा सके. साइबर स्वच्छता केन्द्र (बॉटनेट शोधन और मालवेयर विश्लेषण केन्द्र) "राष्ट्रीय साइबर सुरक्षा नीति" के उद्देश्यों के अनुसार स्थापित किया गया है, जो देश में एक सुरक्षित साइबर पारिस्थितिकी तंत्र बनाने की परिकल्पना करता है. यह केन्द्र इंटरनेट सेवा प्रदाताओं और उत्पाद/ कंपनियों / एंटीवायरस के साथ समन्वय और सहयोग से संचालित होता है. यह वेबसाइट उपयोगकर्ताओं / नागरिकों को उनके कंप्यूटर / उपकरणों को सुरक्षित करने के लिए सूचना और उपकरण प्रदान करती है. इस केन्द्र का संचालन सर्ट-इन द्वारा सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70 ख के प्रावधानों के तहत किया जा रहा है.

साइबर स्वच्छता केन्द्र बॉट्स द्वारा संक्रमित सिस्टम का पता लगाने के लिए उद्योग और शिक्षाविदों के साथ सहयोग करता है. यह केन्द्र इंटरनेट सेवा प्रदाताओं के सहयोग से नागरिकों / उपयोगकर्ताओं को उनके कंप्यूटर / सिस्टम / मोबाइल डिवाइस की खराबी के बारे में अवगत कराता है ताकि उन्हें अपने सिस्टम को ठीक करने में सहायता प्राप्त हो. यह केन्द्र आम नागरिकों / उपयोगकर्ताओं के बीच बॉटनेट, मालवेयर संक्रमण, उनके कंप्यूटर / सिस्टम / मोबाइल डिवाइस /घरेलू राउटर जैसे उपकरणों को सुरक्षित करने और मालवेयर संक्रमण को रोकने के लिए किए जाने वाले उपायों के बारे में जागरूकता बढ़ाता है.

6. **केंद्रीय विद्युत प्राधिकरण में कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल-विद्युत (सी.एस.आई.आर.टी.-पावर)** की स्थापना का निर्णय केंद्रीय विद्युत मंत्रालय द्वारा लिया गया है. विद्युत क्षेत्र के विभिन्न उपक्रमों तथा केंद्रीय विद्युत प्राधिकरण के अधिकारियों के समुह के माध्यम से **सी.एस.आई.आर.टी.**-पावर की गठन हेतु पहल की जा रही है, जिससे विद्युत क्षेत्र से संबंधित साइबर सुरक्षा घटनाओं पर त्वरित प्रतिक्रिया व समन्वय हो सके. इस सेट-अप के माध्यम से सदस्य घटकों को साइबर सुरक्षा घटनाओं को रोकने, पता लगाने, संभालने और प्रतिक्रिया देने के लिए सेवाएं एवं सहायता प्रदान की जाएगी.

7. **के.वि.प्रा. ने "केंद्रीय विद्युत प्राधिकरण (ग्रिड से संयोजन के लिए तकनीकी मानक) (संशोधन) विनियम, 2019"** में साइबर सुरक्षा पर विनियम 10 के प्रावधान के तहत विद्युत क्षेत्र में साइबर सुरक्षा पर दिशानिर्देश जारी किया जिनका पालन ग्रिड से संयोजन करने हेतु सभी अनुरोधकर्ता एवं ग्रिड के उपयोगकर्ता द्वारा किया जाना अनिवार्य है.

8. **के.वि.प्रा. (विद्युत क्षेत्र में साइबर सुरक्षा) दिशानिर्देश, 2021:**

भारत के विद्युत क्षेत्र में साइबर सुरक्षा सुनिश्चित करने के लिए, विद्युत मंत्रालय ने 6 (छह) क्षेत्रीय (तापीय, जल-विद्युत, पारेषण, ग्रिड प्रचालन, नवीकरणीय ऊर्जा एवं वितरण) सी.ई.आर.टी. का गठन किया गया है. प्रत्येक क्षेत्रीय सी.ई.आर.टी. ने साइबर हमलों और साइबर आतंकवाद से मुकाबला करने के लिए अपना विशिष्ट मॉडल साइबर संकट प्रबंधन योजना (सी.सी.एम.पी.) तैयार किया है. क्षेत्रीय मॉडल सी.सी.एम.पी. के अनुरूप उस क्षेत्र में कार्यरत संगठनों / उपक्रमों / यूटिलिटियों को अपना अनुमोदित सी.सी.एम.पी. तैयार कर परिचालित किया जाता है.

भारतीय विद्युत आपूर्ति प्रणाली के सभी जिम्मेदार संस्थाएं, सेवा प्रदाता, उपकरण आपूर्तिकर्ता / विक्रेता और विद्युत क्षेत्र में कार्यरत सलाहकार साइबर सुरक्षा सुनिश्चित करने के लिए समान रूप से जिम्मेदार हैं. दिशानिर्देश द्वारा विद्युत क्षेत्र के संगठनों / उपक्रमों / यूटिलिटियों में साइबर सुरक्षा तैयारियों के लिए आवश्यक कार्य योजना का निर्धारिण किया गया है ताकि विद्युत क्षेत्र में साइबर सुरक्षा तैयारियों के स्तर को बढ़ाया जा सके.

मुख्यत: इन दिशानिर्देशों के अनुसार निम्न बिंदुओं पर जोर दिया जाता है:

- संस्थाओं द्वारा एन.सी.आई.आई.पी.सी. से जारी दिशा-निर्देशों के अनुरूप साइबर सुरक्षा नीति को लागू किया जाए.
- संस्थाओं द्वारा योग्य सी.आई.एस.ओ. की नियुक्ति अवश्य हो.
- संस्थाओं द्वारा अपनी महत्वपूर्ण व्यावसायिक प्रक्रियाओं और अंतर्निहित सूचना बुनियादी ढांचे के विवरण की पहचान कर एन.सी.आई.आई.पी.सी. के परामर्श से सी.आई.आई. चिन्हित/घोषित किया जाए.
- संस्थाओं द्वारा इलेक्ट्रॉनिक सुरक्षा परिधि तथा परिधि के सभी एक्सेस पॉइंट्स की पहचान की जाए. संस्थाओं द्वारा सुनिश्चित किया जाए कि इलेक्ट्रॉनिक सुरक्षा परिधि के भीतर ही प्रत्येक क्रिटिकल सिस्टम कार्य करे.
- संस्थाओं द्वारा चौबिसो घंटे कार्यरत सूचना सुरक्षा प्रभाग (आई.एस.डी.) स्थापित किया जाए, जिसकी अध्यक्षता सी.आई.एस.ओ. करें.
- संस्थाओं द्वारा विद्युत क्षेत्र की सर्वोत्तम प्रथाओं के अनुरूप साइबर संकट मूल्यांकन एवं शमन योजनाएँ तैयार कर लागू की जाएं.

- संस्थाओं द्वारा पुराने पावर सिस्टम / सूचना प्रौद्योगिकी के उपकरण / प्रणाली को उचित चरणबद्ध तरीके से हटाया जाए.
- संस्थाओं द्वारा अपने कर्मियों (जिनके पास क्रिटिकल सिस्टम्स का अधिकृत साइबर या भौतिक एक्सेस अधिकार हो) के लिए वार्षिक साइबर सुरक्षा प्रशिक्षण कार्यक्रम कराया जाए.
- संस्थाओं द्वारा सभी कम्यूनिकेबल इंटेलिजेंट इक्विपमेंट का क्रय और उनके सर्विस लेवल एग्रीमेंट (एस.एल.ए.) को "विश्वसनीय स्रोतों" से किया जाए.
- संस्थाओं द्वारा साइबर सुरक्षा घटना रिपोर्टिंग एवं प्रतिक्रिया योजना का क्रियांवयन किया जाए.
- संस्थाओं द्वारा साइबर संकट प्रबंधन योजना तैयार कर उसकी समीक्षा क्षेत्रीय-सी.ई.आर.टी. द्वारा कराया जाए.
- संस्थाओं द्वारा ध्वंसन (सैबोटैज) संबंधित घटना को रिपोर्ट करने की प्रक्रिया का क्रियान्वयन कराया जाए.
- संस्थाओं द्वारा सभी इन-सर्विस तथा स्टैंडबाय साइबर संपत्तियों की सुरक्षा नियमित फर्मवेयर/सॉफ्टवेयर अपडेट और पैचिंग, भेद्यता प्रबंधन, प्रवेश परीक्षण, सुरक्षित कॉन्फ़िगरेशन एवं सुरक्षा नियंत्रणों के माध्यम से सुनिश्चित कराया जाए. संचारी उपकरणों का आई.एस.ओ./आई.ई.सी./आई.एस. मानकों के अनुसार संचार प्रोटोकॉल के लिए परीक्षण किया जाए.
- संस्थाओं को अपने क्रिटिकल सिस्टम्स के लिये सूचना सुरक्षा प्रबंधन प्रणाली को लागू कराया जाए तथा इसके लिये हर छह महीने के अंतराल में साइबर सुरक्षा लेखा-परीक्षा करवाया जाए.

### 9. आईएस-16335:2015 पावर कंट्रोल सिस्टम-सुरक्षा आवश्यकता:

बीआईएस द्वारा 'पॉवर कंट्रोल सिस्टम्स - सिक्योरिटी आवश्यकता' के लिये मानक जारी किया गया है, जिसमें विद्युत उत्पादन, पारेषण, वितरण एवं व्यापार में शामिल सभी महत्वपूर्ण संपत्तियों की पहचान व सुरक्षा के लिए आवश्यकताओं को निर्दिष्ट किया गया.

*******

# 8. विद्युत वितरण क्षेत्र में साइबर सुरक्षा

पवन कुमार गुप्ता, उपनिदेशक, डीपीएंडटी प्रभाग, के.वि.प्रा.
ई-मेल: pmisra.cea@cea.nic.in

### परिचय

साइबर सुरक्षा प्रौद्योगिकियों, प्रक्रियाओं और नियंत्रणों का उपयोग करके इलेक्ट्रॉनिक सिस्टम, सर्वर, नेटवर्क, डिवाइस, प्रोग्राम और डेटा को साइबर हमलों से रक्षा करने की प्रक्रिया है. चूंकि बिजली क्षेत्र किसी भी राष्ट्र के लिए महत्वपूर्ण क्षेत्रों में से एक है, इसलिए किसी भी साइबर हमले से बिजली व्यवस्था की रक्षा करना महत्वपूर्ण हो जाता है. बिजली क्षेत्र की वितरण प्रणाली ट्रांसफार्मर, सर्किट ब्रेकर, आइसोलेटर, रिले, विद्युत लाइनों और फीडर आदि का एक बड़ा और जटिल नेटवर्क है, जो सीधे अंतिम उपभोक्ता को बिजली की आपूर्ति करता है. बड़े नेटवर्क, दृश्यता और उपभोक्ताओं से सीधे कनेक्शन के कारण, वितरण क्षेत्र किसी भी साइबर हमले से बचाने के लिए महत्वपूर्ण हो जाता है.

## साइबर सुरक्षा की आवश्यकता

नियंत्रण और संचालन के लिए भारतीय वितरण क्षेत्र में आई.टी. की पैठ कुछ साल पहले अपेक्षाकृत कम थी, लेकिन अब सभी वितरण कंपनियां अपने दिन-प्रतिदिन के कार्यों में सूचना और संचार प्रौद्योगिकी को अपना रही हैं. स्मार्ट ग्रिड अनुप्रयोगों के आगमन के साथ, विद्युत क्षेत्र में साइबर स्पेस में वृद्धि हुई है. स्काडा / डी.एम.एस. पर साइबर हमले के प्रभाव से अस्पतालों, मेट्रो, हवाई अड्डों आदि जैसी महत्वपूर्ण सेवाओं के लिए बिजली की आपूर्ति बाधित हो सकती हैं, जो न केवल शामिल इकाइयों के लिए महत्वपूर्ण हो सकती हैं बल्कि साथ ही देश भर में प्रभाव डाल सकती हैं और एक बड़ी सार्वजनिक अशांति का कारण बन सकती हैं. उन्नत मीटरिंग इन्फ्रास्ट्रक्चर (ए.एम.आई.) के माध्यम से एकत्र किए गए डेटा में रुकावट/ गलत रिपोर्टिंग के परिणामस्वरूप गलत / गैर-परिचालन निर्णय हो सकता है और वितरण कंपनियों को मौद्रिक नुकसान हो सकता है और उपभोक्ता की गोपनीयता भंग हो सकती है.

## साइबर हमले के लिए अतिसंवेदनशील वितरण अवसंरचना

साइबर हमले के लिए अतिसंवेदनशील मुख्य अवसंरचना निम्नलिखित क्षेत्रों में हो सकती है:

- स्काडा सिस्टम
- उन्नत मीटरिंग इंफ्रास्ट्रक्चर (ए.एम.आई.)
- मीटरिंग, बिलिंग और संग्रह सॉफ्टवेयर
- वितरण स्वचालन प्रणाली
- डिस्कॉम/ई.आर.पी. की प्रक्रिया प्रबंधन प्रणाली
- उपभोक्ता वेब पोर्टल/पेमेंट गेटवे/एप्लिकेशन

स्काडा सिस्टम किसी भी डिस्कॉम में सबसे महत्वपूर्ण बुनियादी ढांचा प्रणाली है. स्काडा सिस्टम का उपयोग वितरण सब-स्टेशनों से उपभोक्ताओं तक बिजली के प्रवाह की निगरानी और नियंत्रण के लिए किया जाता है. सर्किट ब्रेकर, आइसोलेटर्स, ऑटो-रिक्लोजर, सेक्शनलाइज़र, ट्रांसफॉर्मर, कैपेसिटर बैंक आदि जैसे उपकरणों को मास्टर कंट्रोल सेंटर (एम.सी.सी.) और बैक-अप कंट्रोल सेंटर (बी.सी.सी.) से स्काडा सिस्टम के माध्यम से नियंत्रित किया जा सकता है. फील्ड उपकरणों और एम.सी.सी. के बीच संचार के उद्देश्य से सबस्टेशनों / फीडरों पर आर.टी.यू. और एफ.आर.टी.यू. को फील्ड में स्थापित किया जाता है. सब-स्टेशनों/फीडर में स्थापित आर.टी.यू./एफ.आर.टी.यू. आदि एम.पी.एल.एस. के माध्यम से या सेलुलर मोडेम का उपयोग करके एम.सी.सी. के साथ संचार करता है. बिजली आपूर्ति को बाधित करने के लिए उपरोक्त किसी भी उपकरण या संचार माध्यम को हैक किया जा सकता है.

## केंद्र सरकार द्वारा उठाए गए कदम

1. सूचना प्रौद्योगिकी संशोधन अधिनियम 2008 के अनुसार, भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन CERT-In) को देश में साइबर घटनाओं पर जानकारी एकत्र करने, विश्लेषण करने और प्रसारित करने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है. सर्ट-इन बिजली क्षेत्र सहित सभी क्षेत्रों के लिए नियमित आधार पर कंप्यूटर और नेटवर्क की सुरक्षा के लिए नवीनतम साइबर खतरों / कमजोरियों और प्रतिवादों के बारे में अलर्ट और सलाह जारी करता है.
2. सूचना प्रौद्योगिकी (आई.टी.) अधिनियम, 2000 की धारा 70ए के प्रावधानों के अनुसार, सरकार ने देश में महत्वपूर्ण सूचना बुनियादी ढांचे की सुरक्षा के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एन.सी.आई.आई.पी.सी.) की स्थापना की है. एन.सी.आई.आई.पी.सी. महत्वपूर्ण सूचना अवसंरचना (सी.आई.आई.) के लिए प्रारंभिक चेतावनी या अलर्ट के लिए नीति मार्गदर्शन, विशेषज्ञता साझा करने और स्थितिजन्य जागरूकता के लिए राष्ट्रीय स्तर के खतरे का समन्वय, साझा, निगरानी, संग्रह, विश्लेषण और पूर्वानुमान समन्वय करता है.
3. सरकार ने मुख्य सूचना सुरक्षा अधिकारियों (सी.आई.एस.ओ) के लिए आवेदन / बुनियादी

ढांचे और अनुपालन हासिल करने के लिए उनकी प्रमुख भूमिकाओं और जिम्मेदारियों के संबंध में दिशानिर्देश जारी किए हैं.

4. सभी सरकारी वेबसाइटों और अनुप्रयोगों को उनकी मेजबानी से पहले साइबर सुरक्षा के संबंध में ऑडिट किया जाना है. होस्टिंग के बाद भी वेबसाइटों और एप्लिकेशन का ऑडिट नियमित आधार पर किया जाएगा.
5. सरकार ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और लेखा परीक्षा करने के लिए सुरक्षा लेखा परीक्षा संगठनों को पैनलबद्ध किया है.
6. सरकार ने सी.ई.आर.टी.-इन, एन.सी.आई.आई.पी.सी. आदि जैसे विभिन्न संगठनों के माध्यम से आई.टी. बुनियादी ढांचे को सुरक्षित करने और साइबर हमलों को कम करने के संबंध में सरकार और महत्वपूर्ण क्षेत्र के संगठनों के नेटवर्क / सिस्टम प्रशासकों और मुख्य सूचना सुरक्षा अधिकारियों (सी.आई.एस.ओ.) के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित करता है.
7. सर्ट-इन साइबर स्वच्छता केंद्र (बॉटनेट सफाई और मैलवेयर विश्लेषण केंद्र) भी संचालित कर रहा है. केंद्र दोषपूर्ण सॉफ़्टवेयर का पता लगाने और उन्हें हटाने के लिए मुफ्त उपकरण प्रदान कर रहा है.

## विद्युत क्षेत्र में विशेष रूप से उठाए गए कदम

1. विद्युत मंत्रालय ने प्रत्येक क्षेत्र पर ध्यान केंद्रित करते हुए छह क्षेत्रीय सर्ट बनाए:
   - सर्ट - थर्मल - एनटीपीसी (नोडल एजेंसी)
   - सर्ट - हाइड्रो - एनएचपीसी (नोडल एजेंसी)
   - सर्ट - ट्रांसमिशन - पावरग्रिड (नोडल एजेंसी)
   - सर्ट - वितरण - सीईए (नोडल एजेंसी)
   - सर्ट - ग्रिड ऑपरेशन - ग्रिड-इंडिया (नोडल एजेंसी)
   - सर्ट - नवीकरणीय ऊर्जा - एमएनआरई/एसईसीआई (नोडल एजेंसी)
2. विद्युत क्षेत्र की साइबर सुरक्षा तैयारियों की समीक्षा के लिए विद्युत मंत्रालय ने सचिव (विद्युत) की अध्यक्षता में एक अधिकार प्राप्त समिति और अतिरिक्त सचिव (विद्युत) की अध्यक्षता में एक स्थायी समिति का गठन किया है.
3. विद्युत् मंत्रालय ने 2 जुलाई, 2020 के आदेश को अधिसूचित किया, जिसके द्वारा निम्नलिखित को अनिवार्य किया गया है:

   *"(1) बिजली आपूर्ति प्रणाली और नेटवर्क में उपयोग के लिए आयातित सभी उपकरणों, घटकों और भागों का देश में परीक्षण किया जाएगा ताकि किसी भी प्रकार के एम्बेडेड मैलवेयर/ट्रोजन/साइबर खतरे की जांच की जा सके और भारतीय मानकों का पालन किया जा सके.*

   *(2) ऐसे सभी परीक्षण प्रमाणित प्रयोगशालाओं में किए जाएंगे जिन्हें विद्युत मंत्रालय (एमओपी) द्वारा नामित किया जाएगा."*
4. सीईए ने अक्टूबर, 2021 के महीने में सीईए (बिजली क्षेत्र में साइबर सुरक्षा) दिशानिर्देश जारी किए. दिशानिर्देशों के मुख्य खंड साइबर सुरक्षा जागरूकता पैदा करने, एक सुरक्षित साइबर पारिस्थितिकी तंत्र बनाने, नियामक ढांचे को मजबूत करने, सुरक्षा खतरे के लिए तंत्र बनाने चेतावनी, भेद्यता प्रबंधन और सुरक्षा खतरों की प्रतिक्रिया, दूरस्थ संचालन और सेवाओं को सुरक्षित करना, महत्वपूर्ण सूचना बुनियादी ढांचे की सुरक्षा और लचीलापन, साइबर आपूर्ति श्रृंखला जोखिमों को कम करना, साइबर सुरक्षा में अनुसंधान और विकास को बढ़ावा देना, साइबर सुरक्षा के क्षेत्र में मानव संसाधन विकास, संचालन राष्ट्रीय साइबर सुरक्षा नीति आदि के बारे में हैं.

## सर्ट – वितरण की भूमिका

- सी.आई.एस.ओ. की नियुक्ति, सी.एस.के. में शामिल होने, सी.सी.एम.पी. की तैयारी, साइबर ऑडिट / मॉक ड्रिल के संचालन, सी.ई.आर.टी.-इन, एन.सी.आई.आई.पी.सी. आदि द्वारा

आयोजित विभिन्न प्रशिक्षण जैसे विभिन्न उपाय करने के लिए वितरण कंपनियों को सलाह देना.

- एम.ओ.पी./एन.सी.आई.आई.पी.सी./सी.ई.आर.टी.-इन/सी.आई.एस.ओ.-एम.ओ.पी. आदि से प्राप्त एडवाइजरी/अलर्ट/कमजोरियां/सूचना आदि सभी वितरण कंपनियों को प्रसारित करना और एम.ओ.पी./एन.सी.आई.आई.पी.सी./सी.ई.आर.टी.-इन/सी.आई.एस.ओ. को स्थिति रिपोर्ट/कार्रवाई रिपोर्ट प्रस्तुत करना.
- वितरण कंपनियों द्वारा उठाए जाने वाले विभिन्न कदमों के कार्यान्वयन में यूटिलिटीज को सलाह देना और नियमित रूप से स्थिति रिपोर्ट प्रस्तुत करना.
- विभिन्न खतरों, घटनाओं, अभ्यासों, आकलन, मैलवेयर, भेद्यता आदि पर की गई कार्रवाई के संबंध में सी.आई.एस.ओ. द्वारा प्रस्तुत आंकड़ों को संकलित करना.
- राज्यों/संघ राज्य क्षेत्रों में सी.आई.एस.ओ. द्वारा कार्यान्वयन के लिए समय-समय पर सर्ट-इन, और एन.सी.आई.आई.पी.सी. से प्राप्त अतिरिक्त उपायों का सुझाव देना.
- सर्ट-इन द्वारा विधिवत अनुमोदित एक मॉडल सी.सी.एम.पी. तैयार करना जिसका उपयोग यूटिलिटी द्वारा अपने स्वयं के सी.सी.एम.पी. तैयार करने के लिए किया जाना है.
- एम.ओ.पी./स्थायी समिति/अधिकार प्राप्त समिति/सी.आई.एस.ओ.-एम.ओ.पी. आदि द्वारा वांछित कोई अन्य कार्रवाई.

## साइबर सुरक्षा उपायों की स्थिति

कुछ प्रमुख साइबर सुरक्षा मानकों में सी.आई.एस.ओ. का नामांकन, सी.एस.के. में शामिल होना, सी.सी.एम.पी. की तैयारी, लेखा परीक्षा आयोजित करना, सी.आई.आई. की पहचान और आई.एस.ओ. 27001 का कार्यान्वयन शामिल हैं. सर्ट-डी इन मानकों में सुधार के लिए सभी डिस्कॉम के साथ नियमित रूप से बातचीत कर रहा है. देश के 82 प्रमुख डिस्कॉम के लिए इन मापदंडों की स्थिति (10.11.2022 को) इस प्रकार है:

| क्र. | कार्रवाई बिंदु | स्थिति |
|---|---|---|
| 1 | सी.आई.एस.ओ. का नामांकन | सभी डिस्कॉम ने सी.आई.एस.ओ. को नामित किया है. |
| 2 | ऑनबोर्डिंग साइबर स्वच्छता केंद्र (सी.एस.के.) | चंडीगढ़ को छोड़कर सभी डिस्कॉम ने सी.एस.के. को ऑनबोर्ड किया है. |
| 3 | साइबर संकट प्रबंधन योजना (सी.सी.एम.पी.) तैयार करना | 37 डिस्कॉम ने सी.सी.एम.पी. तैयार कर लिया है और शेष तैयारी में हैं. |
| 4 | साइबर सुरक्षा ऑडिट | 49 डिस्कॉम ऑडिट कर रहे हैं. अन्य डिस्कॉम को नियमित रूप से आई.टी. और ओ.टी. सिस्टम की ऑडिट करने की सलाह दी जा रही है. |
| 5 | महत्वपूर्ण सूचना अवसंरचना (सी.आई.आई.) की पहचान | 35 डिस्कॉम ने सी.आई.आई. के अपने विवरण की पहचान की है और अन्य प्रक्रिया में हैं. |
| 6 | आईएसओ 27001 का कार्यान्वयन | 25 डिस्कॉम ने कार्यान्वित किया है और अन्य डिस्कॉम कार्यान्वयन की प्रक्रिया में हैं. |

## निष्कर्ष

बिजली आपूर्ति में व्यवधान स्वास्थ्य, अर्थव्यवस्था, सुरक्षा और राष्ट्रीय सुरक्षा के संदर्भ में विनाशकारी प्रभाव डाल सकता है. सरकार ने सामान्य रूप से और विशेष रूप से बिजली क्षेत्र के लिए साइबर सुरक्षा में सुधार के लिए कई कदम उठाए हैं. यह देखा जा सकता है कि बिजली वितरण क्षेत्र में साइबर सुरक्षा के लिए जागरूकता भी बढ़ रही है, लेकिन सिस्टम को पूरी तरह से सुरक्षित करने के लिए अभी बहुत कुछ हासिल करना बाकी है.

*******

# 9. विद्युत यूटिलिटियों में साइबर सुरक्षा

इन्दर मोहन सूद [ई-मेल: sood@valiantcom.com], प्रबंध निदेशक & सीटीओ, वेलिएन्ट कोम्युनीकेशन लिमिटेड
& तनय राज [ई-मेल: tanay@tejasnetworks.com], सहयोगी उपाध्यक्ष, तेजस नेटवर्क्स लिमिटेड

## प्रस्तावना

जब विद्युत यूटिलिटी संचार प्रणालियां परंपरागत पद्धति से हटकर आधुनिक पद्धति, जैसे कि- टाइम-डिवीजन मल्टीप्लेक्सिंग (टी.डी.एम.) इंफ्रास्ट्रक्चर नेटवर्क से इंटरनेट प्रोटोकॉल (आई.पी.), पैकेट-आधारित नेटवर्क से एक वितरित ऊर्जा ग्रिड और मीटरिंग संसाधनों वाले अधिक उन्नत और कुशल संचार प्रणाली को अपनाने की ओर अग्रसर होती हैं, तो साइबर खतरों से उत्पन्न होने वाले संकट से निपटना और साइबर हमले तथा साइबर आतंकवाद के विरुद्ध प्रभावी रक्षा नीति अपनाना और भी अधिक महत्वपूर्ण हो जाता है.

फ़ायरवॉल को भेदकर, अथवा मोनोलिथिक नेटवर्क की किसी भी कमजोर कड़ी पर डाले गए ट्रोजन, मॉलवेयर आदि के कारण बिना पता चले की गई घुसपैठों और नेटवर्क में सेंध लगाकर परिचालन संबंधी संवेदनशील डेटा हासिल किया जा सकता है. ये खतरे राज्य प्रायोजित विरोधियों या साइबर हमलावरों को उकसाने के लिए स्वतंत्र रूप से कार्य करने वाले अपराधियों के कारण उत्पन्न हो सकते हैं. ट्रोजन, वायरस या मॉलवेयर की मौजूदगी फायरवॉल को भेदने के लिए "राह" खोलती है जिसके फलस्वरूप साइबर हमला होता है और कठिन समय में देश के विद्युत ढांचे को अपंग बना देता है, या राष्ट्रीय अपमान का कारण बनता है. इसे देखते हुए, यह जरूरी हो जाता है कि न केवल ऐसे हमलों को रोकने के लिए बल्कि ट्रोजन, वायरस या मॉलवेयर की मौजूदगी के कारण नेटवर्क के भीतर पहले से ही हो रही किसी भी गैरकानूनी और अनुचित गतिविधियों का पता लगाने के लिए प्रभावी तंत्र स्थापित किए जाएं.

## फायरवॉल

राष्ट्रीय पावर ग्रिड में विश्वसनीयता एवं सुरक्षा सुनिश्चित करने के लिए ताप विद्युत संयंत्रों, जल विद्युत उत्पादन एवं पारेषण परिसंपत्तियों, ग्रिड संचालन के साथ-साथ नवीकरणीय ऊर्जा और विद्युत वितरण व्यवस्था के ढांचे की सुरक्षा के लिए एक प्रभावी साइबर सुरक्षा और प्रतिरक्षा रणनीति अपनाना अत्यंत आवश्यक हो जाता है.

केवल फायरवॉल, साइबर सुरक्षा रणनीति का केंद्र-बिंदु नहीं बन सकती हैं, क्योंकि फ़ायरवॉल में न केवल बाहर से बल्कि (प्राय:) अंदर से ट्रोजन, वायरस या मॉलवेयर, जिन्हें नेटवर्क के सबसे कमजोर बिंदुओं पर लगाया या डाला गया हो, से सेंध लगाई जा सकती है.

आई.टी. और ओ.टी. प्रणालियों के बीच बनाई गई कृत्रिम पृथक्करण को किसी भी अंदरूनी या बाहरी व्यक्ति द्वारा आसानी से तोड़ा जा सकता है. संक्षेप में कहा जा सकता है कि साइबर सुरक्षा रणनीति के साधन के रूप में केवल फ़ायरवॉल का होना एक भ्रम मात्र है.

साइबर-हमले की शुरूआत, बाहरी हमलावरों या विश्वसनीय अंदरूनी सूत्रों, कमान और नियंत्रण द्वारा आरंभिक घुसपैठ, निष्पादन, दृढ़ता, विशेषाधिकार प्राप्त पहुंच, रक्षा परिहार, की तकनीकों के माध्यम से की जा सकती है.

किसी भी साइबर सुरक्षा रक्षा रणनीति का आधार उन साइबर हमलों और घुसपैठों को विफल करना होगा जो विद्युत आपूर्ति प्रणालियों को प्रभावित कर सकते हैं और ग्रिड संचालन को असुरक्षित और कमजोर बना सकते है.

### प्रभावी और निश्चित काउंटर-डिफेंस रणनीति का कार्यान्वयन

प्रभावी और निश्चित काउंटर-डिफेंस रणनीति के कार्यान्वयन के लिए कुछ आवश्यक बिंदुओं को नीचे सूचीबद्ध किया जा रहा है :

1. ऐसे साइबर हमलों के शमन हेतु साइबर सुरक्षा संबंधी घटनाओं का पता लगाने के लिए फायरवॉल के पीछे "पूर्व चेतावनी तथा प्रतिक्रिया प्रणाली" लगाना.
2. उपयुक्त ऑडियो-विजुअल चेतावनी तंत्र के माध्यम से शुरुआती साइबर हमले की चेतावनी और घुसपैठ का पता लगाने वाले उपकरणों का उपयोग करके कंप्यूटर सिस्टम की सुरक्षा करना.
3. एस.सी.ए.डी.ए. (स्काडा) और आई.सी.एस. प्रणाली पर साइबर हमलों का पता लगाना.
4. आई.टी. और ओ.टी. नेटवर्क में साइबर उल्लंघनों का पता लगाना और उपयुक्त चेतावनी तंत्र स्थापित करना.
5. महत्वपूर्ण संगठनात्मक डेटा की सुरक्षा के लिए डेटा लीक का पता लगाना.
6. उचित समय में फोरेंसिक विश्लेषण करने की क्षमता स्थापित करना.
7. आइसोलेटेबल ऑपरेशनल जोन बनाना, जिसमें निम्नलिखित शामिल हों:
   (क) स्वत: भौतिक वस्तु/उपकरण अलगाव की योग्यता (किसी विशिष्ट स्थान या दूरसंचार के किसी अकेले रैक को अलग करने की योग्यता, जो खतरे का स्रोत हो सकती है.)
   (ख) साइबर हमले का पता चलने की स्थिति में लैन नेटवर्क के भीतर महत्वपूर्ण क्षेत्रों को वैन नेटवर्क से तत्काल संपर्क हटाने के लिए नेटवर्क आइसोलेशन स्विच लगाना.
   (ग) यह सुनिश्चित करने के लिए कि बैक-अप संवेदनशील डेटा हमेशा सुरक्षित और संरक्षित रहे सभी बैक-अप ओ.टी. प्रणालियों [जैसे एन.ए.ए.एस. (नेटवर्क एज ए सर्विस)/एस.ए.एन. (स्टोरेज एरिया नेटवर्क), डेटा स्टोरेज सर्वर] के स्वचालित हार्ड आइसोलेशन को लागू करना.
   (घ) नेटवर्क उल्लंघन का पता चलने की स्थिति में सुरक्षा रिले, बे-कंट्रोल यूनिट और डेटा स्टोरेज डिवाइस जैसे सभी महत्वपूर्ण उपकरणों का ऑपरेशनल जोन आसोलेशन और आइलैंडिंग तंत्र बनाएं.
8. किसी खास नेटवर्क के लिए विशिष्ट और अनोखी नेटवर्क कमजोरी का पता लगाना और उनका यथोचित समाधान करना.
9. ऐसे ऑटोमैटिक फेलओवर स्विच लगाकर नेटवर्क विश्वसनीयता और नेटवर्क लचीलेपन को बनाए रखना, जो सभी महत्वपूर्ण क्षेत्रों और उपकरणों जैसे कि "आर.टी.यू", "पी.एम.यू." और उनसे संबंधित "प्रोटेक्शन एसेट्स" को वैकल्पिक ट्रांसमिशन उपकरण और वैकल्पिक ट्रांसमिशन मार्गों से भौतिक रूप से हटाते और पुन: संपर्क स्थापित करते हैं.
10. नियमित साइबर सुरक्षा ऑडिट करना.

### एकीकृत नेटवर्क प्रबंध प्रणाली

इसके अतिरिक्त, उपयोगकर्ता असाइनमेंट और सुदृढ़ अभिगम नियंत्रण वाले किसी केंद्रीय और एकाधिक दूरस्थ स्थानों से सभी नेटवर्क परिसंपत्तियों की निगरानी के लिए एक एकीकृत नेटवर्क प्रबंध प्रणाली भी अनिवार्य होती है.

- उदाहरण : नेटवर्क घुसपैठ, ट्रोजन या मैलवेयर गतिविधि का पता लगाने के लिए और रैंसमवेयर हमलों, डी.ओ.एस. हमलों आदि का मुकाबला करने के लिए फ़ायरवॉल और राउटरों की रियल-टाइम निगरानी.

- साइबर सुरक्षा स्थिति की निगरानी के लिए स्थानीय अतिरेक बनाना.

एकीकृत नेटवर्क प्रबंध प्रणाली सभी साइबर-सुरक्षा परिसंपत्तियों की परिचालन दृश्यता में और अधिक वृद्धि करेगी तथा बेहतर निगरानी और वास्तविक समय प्रबंधन और नियंत्रण के माध्यम से आई.टी. बुनियादी ढांचे को सुदृढ़ करेगी.

### निष्कर्ष

इस प्रकार जो समग्र व्यापक समाधान उभर कर सामने आएगा, उसके अंतर्गत विभिन्न बिंदुओं या नेटवर्क पर नेटवर्क-घुसपैठ का पता लगाना और पूर्व-चेतावनी प्रणाली स्थापित करना शामिल होगा और यह व्यापक रक्षा रणनीति के कार्यान्वयन में प्रभावी रूप से मदद करेगा जो किसी साइबर हमले या नेटवर्क उल्लंघन का पता लगने पर स्वचालित रूप से कार्य करेगा तथा सभी "महत्वपूर्ण विद्युत उत्पादन, पारेषण और वितरण परिसंपत्तियों" को सुरक्षित रखेगा.

*******

## 10. हैकिंग

अजय कुमार, सहायक निदेशक, सूचना प्रद्योगिकी एवं साइबर सुरक्षा
ईमेल- ajaysharma.jy@cea.nic.in

किसी ऐसी प्रणाली (सिस्टम) में सेंध लगाना जिसके लिए आप अधिकृत नहीं है, हैकिंग कही जाती है. उदाहरण के तौर पर किसी ऐसे ई-मेल अकाउंट में लॉग-इन करना, जो आपका नहीं है, अथवा किसी दूरस्थ कंप्यूटर में गतिविधियां संचालित करना, जिसमें कार्य करने के लिए आप अधिकृत नहीं हैं. किसी सिस्टम को हैक करने के अनेक तरीके होते हैं.

### हैकिंग के लाभ

हैकिंग के कई लाभ हैं:

1. इसका उपयोग खोई हुई जानकारी को दुबारा प्राप्त करने के लिए किया जाता है, खासकर जब आप अपना पासवर्ड भूल गए हों.
2. इसका उपयोग कंप्यूटर और नेटवर्क की सुरक्षा बढ़ाने के लिए पैठ परीक्षण करने के लिए किया जाता है.
3. इसका उपयोग यह जांचने के लिए किया जाता है कि आपके नेटवर्क पर सुरक्षा कितनी अच्छी है.

### हैकिंग के नुकसान

हैकिंग के कई नुकसान हैं:

1. यह किसी की निजता को नुकसान पहुंचा सकता है.
2. हैकिंग गैरकानूनी है.
3. अपराधी अपने लाभ के लिए हैकिंग का इस्तेमाल कर सकते हैं.
4. सिस्टम के संचालन में बाधा डालना.

### नैतिक हैकिंग

नैतिक हैकिंग को **व्हाइट हैट हैकिंग** के नाम से भी जाना जाता है. नैतिक हैकिंग में कंप्यूटर सिस्टम या डेटा तक अनधिकृत पहुंच प्राप्त करने का अधिकृत प्रयास शामिल है. नैतिक हैकिंग का उपयोग परीक्षण के दौरान पाई गई भेद्यता को ठीक करके सिस्टम और नेटवर्क की सुरक्षा में सुधार करने के लिए किया जाता है. नैतिक हैकर किसी संगठन की सुरक्षा व्यवस्था में सुधार करते हैं. नैतिक हैकर उन्हीं टूल्स, युक्तियों और तकनीकों का इस्तेमाल करते हैं जिनका इस्तेमाल दुर्भावनापूर्ण हैकर करते हैं, लेकिन ऐसा वे अधिकृत व्यक्ति की अनुमति से करते हैं. नैतिक हैकिंग का उद्देश्य सुरक्षा व्यवस्था में सुधार करना और दुर्भावनापूर्ण उपयोगकर्ताओं के हमलों से प्रणाली की रक्षा करना है.

नैतिक हैकिंग किसी एप्लिकेशन, सिस्टम, या संगठन के बुनियादी ढांचे में कमजोरियों का पता लगाने और नेटवर्क में संभावित डेटा उल्लंघनों और खतरों की पहचान करने के लिए सिस्टम सुरक्षा को अलग-थलग करने की एक अधिकृत प्रक्रिया है. सिस्टम या नेटवर्क का स्वामित्व रखने वाली कंपनी साइबर सुरक्षा इंजीनियरों को सिस्टम की सुरक्षा जांच करने के लिए ऐसी गतिविधियों को करने की अनुमति देती है. इस प्रकार, दुर्भावनापूर्ण हैकिंग के विपरीत, यह प्रक्रिया योजनाबद्ध और स्वीकृत है. नैतिक हैकरों

का लक्ष्य उन कमजोर बिंदुओं के लिए सिस्टम या नेटवर्क की जांच करना है जिनका लाभ दुर्भावनापूर्ण हैकर उठा सकते हैं या प्रणाली/ डेटा को नष्ट कर सकते हैं. वे सिस्टम/नेटवर्क/एप्लिकेशन की सुरक्षा को मजबूत करने के तरीकों का पता लगाने के लिए जानकारी एकत्र करते हैं और उसका विश्लेषण करते हैं. ऐसा करके, वे सुरक्षा पद्धति में सुधार कर सकते हैं ताकि यह बेहतर ढंग से हमलों का सामना कर सके या उन्हें टाल सके.

संगठनों द्वारा नैतिक हैकरों को अपने सिस्टम और नेटवर्क की कमजोरियों का ध्यान रखने और डेटा चोरी को रोकने के लिए समाधान विकसित करने के लिए काम पर रखा जाता है. इसे पुरानी कहावत "चोर को पकड़ने के लिए चोर की जरूरत होती है का हाई-टेक रूप माना जा सकता है."

### नैतिक हैकर की भूमिकाएं और जिम्मेदारियां क्या हैं?

कानूनी रूप से हैकिंग करने के लिए नैतिक हैकरों को कुछ दिशानिर्देशों का पालन करना चाहिए. एक अच्छा हैकर अपनी जिम्मेदारी जानता है और सभी नैतिक दिशानिर्देशों का पालन करता है. यहाँ नैतिक हैकिंग के सबसे महत्वपूर्ण नियम हैं:

- एक नैतिक हैकर को उस संगठन से प्राधिकार हासिल करना चाहिए जो सिस्टम का मालिक है. हैकरों को सिस्टम या नेटवर्क पर कोई सुरक्षा मूल्यांकन करने से पहले पूर्ण स्वीकृति प्राप्त करनी चाहिए.
- उनके मूल्यांकन का दायरा निर्धारित करना और संगठन को उनकी योजना से अवगत कराना.
- सिस्टम या नेटवर्क में पाए जाने वाले किसी भी सुरक्षा उल्लंघनों और कमजोरियों की जानकारी प्रदान करना.
- अपनी खोजों को गोपनीय रखना क्योंकि उनका उद्देश्य सिस्टम या नेटवर्क को सुरक्षित करना है. नैतिक हैकरों को अपने गैर-प्रकटीकरण समझौते से सहमत होना चाहिए और उसका सम्मान करना चाहिए.
- किसी भी भेद्यता के लिए सिस्टम की जाँच करने के बाद हैक के सभी निशान मिटा देना. यह दुर्भावनापूर्ण हैकरों को चिन्हित खामियों के माध्यम से सिस्टम में प्रवेश करने से रोकता है.

### नैतिक हैकिंग के प्रमुख लाभ

नैतिक हैकिंग सीखने में ब्लैक हैट हैकरों और परीक्षकों की मानसिकता और तकनीकों का अध्ययन करना शामिल है, ताकि यह सीखा जा सके कि नेटवर्क के भीतर कमजोरियों को कैसे पहचाना और ठीक किया जाए. नैतिक हैकिंग का अध्ययन उद्योगों और कई क्षेत्रों में सुरक्षा पेशेवरों द्वारा लागू किया जा सकता है. इनमें नेटवर्क रक्षक, जोखिम प्रबंध और गुणवत्ता आश्वासन परीक्षक शामिल हैं.

हालांकि नैतिक हैकिंग सीखने का सबसे स्पष्ट लाभ कॉर्पोरेट नेटवर्क को सूचित करने और सुधारने और बचाव करने की इसकी क्षमता है. हैकर किसी भी संगठन की सुरक्षा के लिए प्राथमिक खतरा होता है: हैकर कैसे काम करते हैं, यह सीखना, समझना और कार्यान्वित करना नेटवर्क रक्षकों को संभावित जोखिमों को प्राथमिकता देने में मदद कर सकता है और सीख सकता है कि उन्हें कैसे ठीक किया जाए. इसके अतिरिक्त, नैतिक हैकिंग का प्रशिक्षण या प्रमाण पत्र प्राप्त करने से उन लोगों को लाभ हो सकता है जो सुरक्षा क्षेत्र में एक नई भूमिका की तलाश कर रहे हैं या जो अपने संगठन में कौशल और गुणवत्ता का प्रदर्शन करना चाहते हैं.

### नैतिक हैकर बनने के लिए आवश्यक कौशल

एक नैतिक हैकर को कुशलता से हैकिंग करने के लिए सभी सिस्टम, नेटवर्क, प्रोग्राम कोड, सुरक्षा उपायों आदि के बारे में गहन जानकारी होनी चाहिए. इनमें से कुछ कौशलों में शामिल हैं:

- **प्रोग्रामिंग का ज्ञान** - एप्लिकेशन सुरक्षा और सॉफ्टवेयर विकास जीवन चक्र (एसडीएलसी) के क्षेत्र में काम करने वाले सुरक्षा पेशेवरों के लिए यह आवश्यक है.

- **स्क्रिप्टिंग ज्ञान** - नेटवर्क-आधारित हमलों और होस्ट-आधारित हमलों से निपटने वाले पेशेवरों के लिए यह आवश्यक है.
- **नेटवर्किंग कौशल** - यह कौशल महत्वपूर्ण है क्योंकि खतरे ज्यादातर नेटवर्क से उत्पन्न होते हैं. आपको नेटवर्क में मौजूद सभी उपकरणों के बारे में पता होना चाहिए, वे कैसे जुड़े हुए हैं, और कैसे पहचानें कि वे समझौता किए गए हैं.
- **डेटाबेस की समझ** - हमले ज्यादातर डेटाबेस को लक्ष्य कर किए जाते हैं. एस.क्यू.एल. जैसे डेटाबेस प्रबंधन प्रणालियों का ज्ञान आपको डेटाबेस में किए गए कार्यों का प्रभावी ढंग से निरीक्षण करने में मदद करेगा.
- **विंडोज, लिनक्स, यूनिक्स आदि जैसे विविध प्लेटफॉर्म का ज्ञान**.
- **बाजार में उपलब्ध विभिन्न हैकिंग टूल्स के साथ काम करने की क्षमता.**
- **सर्च इंजन और सर्वर का ज्ञान.**

*******

## 11. साइबर सुरक्षा जागरूकता की आवश्यकता

प्रेम चंद गुप्ता,सहायक निदेशक सूचना प्रद्योगिकी एवं साइबर सुरक्षा
ईमेल- gupta.prem @gov.in

### 1. जागरूक करना

सूचना एवं संचार प्रौद्योगिकी हमारे रोजमर्रा के जीवन का अभिन्न अंग बन चुकी है. सस्ते ब्रॉडबैंड और स्मार्ट फोन सुलभ होने से साइबर स्पेस में लगभग सबकी पैठ हो चुकी है, जो विश्व भर में लाखों उपभोगकर्ताओं को अप्रत्यक्ष रूप से जोड़े रखती है. साइबर स्पेस के व्यापक उपयोग से हमारे खिलाफ साइबर अपराध के जोखिम भी बढ़ गए हैं. डिजिटल दिनचर्या की एक छोटी सी गलती/लापरवाही भी साइबर अपराध को दावत दे सकती है और हमें आर्थिक हानि उठानी पड़ सकती है, हमारे सम्मान को ठेस पहुंच सकती है अथवा हमें उत्पीड़न का सामना करना पड़ सकता है. अत: बाहरी दुनिया से संपर्क साधते समय, चाहे वह वित्तीय लेन-देन हो, सोशल नेटवर्किंग हो, गेम खेलने हों या इंटरनेट पर कुछ तलाशना हो, हमें सतर्क और सावधान रहना चाहिए. साइबर हमले सूचना सुरक्षा के लिए गंभीर खतरा हैं. जैसे-जैसे डेटा उपयोग और इंटरनेट का उपभोग बढ़ता है, साइबर जागरूकता की जरूरत उतनी ही बढ़ती जाती है.

साइबर सुरक्षा जागरूकता का तात्पर्य है कि आखिरी उपभोक्ताओं को साइबर सुरक्षा के जोखिमों, उनके नेटवर्क फेस, उनसे उत्पन्न होने वाले खतरे, और व्यवहार को निर्देशित करने वाले सुरक्षा के सर्वोत्तम उपायों की कितनी जानकारी है. आखिरी उपभोक्ता को सबसे कमजोर कड़ी और किसी नेटवर्क में पहले जोखिम वाला माना जाता है. चूंकि आखिरी उपभोक्ता को सबसे अधिक जोखिम होता है, सुरक्षा बढ़ाने के तकनीकी साधन अपर्याप्त रहते हैं. संगठन मानवीय जोखिम को कम करने की कोशिश कर सकते हैं. इसे आखिरी उपभोक्ता के लिए साइबर सुरक्षा जागरूकता के लिए सुरक्षा संबंधी सर्वोत्तम दिशानिर्देश उपलब्ध कराकर पूरा किया जा सकता है. कर्मियों को आम खतरों और उनसे निपटने/कम करने के तरीकों के बारे में जागरूक किया जा सकता है.

साइबर सुरक्षा के मुद्दों पर रूचि अक्सर घटना होने के बाद उनसे निपटने के तरीकों पर केन्द्रित रहती है, जबकि उनकी रोकथाम और साइबर सुरक्षा की दिशा में योगदान बहुत कम रहा है. ऐसी दुनिया में जहां हैकरों और प्रणाली को सुरक्षित रखने के प्रयास करने वाले विभिन्न सामाजिक कार्यकताओं के बीच जंग लगातार जारी है, यह किसी अचम्भे से कम नही है. साइबर सुरक्षा को युद्ध का एक नया रूप कहा जाता है और आधुनिक युद्धनीति का भावी मंच माना जाता है. इतना महत्वपूर्ण होते हुए भी इसके बारे में जागरूकता इतनी कम क्यों है? और साइबर

स्पेस के बचाव और सुरक्षा के लिए हम कड़े उपाय क्यों नही कर रहे हैं?

घटनाओं को लापरवाह मानवीय व्यवहार और प्रशिक्षण के अभाव का परिणाम बताकर साइबर सुरक्षा जागरूकता के महत्व को कमतर आंका जाता है. छोटे-बड़े संगठनों द्वारा सूचना सुरक्षा सहयोगी समूह में कर्मियों की संख्या बढ़ाने तथा साइबर सुरक्षा प्रौद्यौगिकी बजट बढ़ाने जैसे किए जा रहे उपायों के बावजूद ये घटनाएं लगातार तेजी से बढ़ती जा रही हैं. कई संगठन या तो कर्मियों को जागरूक करने के प्रयासों को को कमतर आंकते हैं अथवा यह नही मानते कि उनके द्वारा दिया जा रहा साइबर सुरक्षा संबंधी मौजूदा प्रशिक्षण प्रभावशाली नही हैं.

### 2. जरूरतें

अधिकांश लोग समझते हैं कि वे संभावित खतरों से दूर हैं. हैकर अपना अगला शिकार किसे बनाएंगे यह पता नहीं होता, और संगठन या व्यक्ति यह मानते हैं कि वे किसी हमले का शिकार नहीं होंगे- ऐसा मेरे किसी पड़ोसी या किसी दूसरी कंपनी के साथ हो सकता है, लेकिन मेरे साथ नहीं होगा. इसके अलावा जब ऐसा किसी के साथ हो जाता है तो दूसरे यही सोचते हैं कि उनकी ही गलती रही होगी, और शायद वे सुरक्षा के जरूरी उपाय नहीं कर पाए. यह केवल एक भ्रम है, क्योंकि उनके सदाशय और सुरक्षा संबंधी सभी तरह के उपाय अपनाने के बावजूद हमेशा यह संभावना बनी रहती है कि किसी भी संगठन पर साइबर सुरक्षा संबंधी हमला हो सकता है. इसके अलावा यदि अधिकांश लोग यह नहीं मानते हैं कि साइबर सुरक्षा एक समस्या है, तो लोग इसे अनदेखा करते रहेंगे और इससे बचने के उचित उपाय नहीं करेंगे. अधिकांश लोगों में तत्काल उपाय नहीं करने की सोच के कारण कोई सामूहिक प्रयास नहीं हो पाता है.

जब साइबर सुरक्षा के बारे में तत्काल उपाय करने की जरूरत महसूस होगी तो किए जाने वाले उपायों पर चर्चा करने की जरूरत पड़ेगी. सुरक्षा बढ़ाने के बारे में किए जाने वाले उपायों के बारे में संगठनों की कोई निश्चित धारणा नहीं है. प्राय: हमलावर अज्ञात होते हैं और यह पता नहीं होता कि दुश्मन कौन है.

आखिरी उपभोक्ता के लिए साइबर सुरक्षा के जोखिम को कम करने वाले कार्यक्रम में साइबर सुरक्षा जागरूकता, साइबर सुरक्षा प्रशिक्षण, साइबर सुरक्षा संबंधी जानकारी प्रदान करना सहित विविध प्रयास शामिल किए जा सकते हैं.

साइबर सुरक्षा प्रशिक्षण, साइबर सुरक्षा संबंधी जानकारी के अंतर्गत निम्नलिखित विषयों को भी शामिल किया जा सकता है:

क. एंटी-मालवेयर का संरक्षण
ख. डेटा संरक्षण और गोपनीयता
ग. उपकरण प्रबंध
घ. घटना पर कार्रवाई
ङ. चीजों की सुरक्षा संबंधी इंटरनेट पासवर्ड प्रबंध
च. पैचिंग
छ. सुरक्षित वेब ब्राउजिंग
ज. सामाजिक इंजीनियरी

*******

## 12. नेटवर्क सुरक्षा

कु. स्वाति, सहायक निदेशक, सूचना प्रद्योगिकी एवं साइबर सुरक्षा
ईमेल- swati.cea @gov.in

नेटवर्क सुरक्षा में एक नेटवर्क व्यवस्थापक द्वारा अपनाए गए प्रावधान और नीतियां शामिल हैं, जो कंप्यूटर नेटवर्क और नेटवर्क-सुलभ संसाधनों में अनधिकृत प्रवेश, दुरुपयोग, संशोधन या सेवा में बाधा को रोकने और निगरानी करने के लिए किया जाता हैं. नेटवर्क को पहली बार 1969 में सैन्य उपयोग के

लिए और दुनिया भर के वैज्ञानिकों से जानकारी साझा करने के लिए ARPANET (उन्नत अनुसंधान परियोजना एजेंसी) के रूप में नामित किया गया था. वास्तव में, ARPANET के मूल लक्ष्यों में से एक लक्ष्य, ऐसा एक नेटवर्क बनाना था जो नेटवर्क के प्रमुख वर्गों के विफल होने या हमला होने पर भी कार्य करना जारी रखे.

ओपन सिस्टम इंटरकनेक्सन (ओ.एस.आई.) मॉडल सात लेयर्स का वर्णन है जिसे कंप्यूटर सिस्टमस नेटवर्क पर संचार करने के लिए उपयोग करते हैं. नेटवर्क लेयर्स विभिन्न नेटवर्क में स्थित एक होस्ट से दूसरे होस्ट में डेटा के प्रसारण के लिए काम करती है. यह पैकेट रूटिंग का भी ध्यान रखती है यानि पैकेट को प्रसारित करने के लिए उपलब्ध मार्गों की संख्या में से सबसे छोटा रास्ता चुनती है . नेटवर्क सुरक्षा प्रोटोकॉल एक प्रकार का नेटवर्क प्रोटोकॉल है जो नेटवर्क कनेक्शन पर पारगमन में डेटा की सुरक्षा और अखंडता सुनिश्चित करता है. नेटवर्क सुरक्षा प्रोटोकॉल्स, डेटा की सामग्री की समीक्षा या निकालने के किसी भी नाजायज प्रयास से नेटवर्क डेटा को सुरक्षित करने के लिए प्रक्रियाओं और कार्यप्रणाली को परिभाषित करते हैं. नेटवर्क सुरक्षा प्रोटोकॉल आमतौर पर डेटा को सुरक्षित करने के लिए क्रिप्टोग्राफी और एन्क्रिप्शन तकनीकों को लागू करते हैं. कुछ लोकप्रिय नेटवर्क सुरक्षा प्रोटोकॉल में सिक्योर फाइल ट्रांसफर प्रोटोकॉल (एस.एफ.टी.पी.), सिक्योर हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल (एच.टी.टी.पी.एस.) और सिक्योर सॉकेट लेयर (एस.एस.एल.) शामिल हैं.

नेटवर्क सुरक्षा उपकरण आमतौर पर भौतिक या वर्चुअलाइज्ड हार्डवेयर उपकरण होते हैं, जिसमें विक्रेता विशिष्ट सॉफ़्टवेयर स्थापित होता है. नेटवर्क सुरक्षा उपकरणों में बहुत से अलग-अलग कार्य होते हैं. कुछ नेटवर्क ट्रैफ़िक का प्रबंधन करते हैं, कुछ खतरों का पता लगाते हैं, और अन्य सुरक्षित रिमोट एक्सेस प्रदान करते हैं. कई सुरक्षा उपकरण कई अन्य उपकरणों से कार्यक्षमता को जोड़ते हैं, विशेष रूप से वे जो छोटे व्यवसायों के लिए अभिप्रेत हैं.

## हमें नेटवर्क सुरक्षा की आवश्यकता क्यों है?

इंटरनेट उपयोगकर्ता हैकर की चपेट में आसानी से आ सकते हैं क्योंकि कंप्यूटर सिस्टम पर अनधिकृत पहुंच से फ़ायरवॉल आसानी से टूट जाती है. हैकर्स न केवल हमारे कंप्यूटर से कुछ अनिवार्य जानकारी और डेटा चुरा सकते हैं, बल्कि हमारे कंप्यूटर से उन्हें जो संवेदनशील डेटा मिलता है, उससे वह पूरे कंप्यूटर सिस्टम को जोखिम में डाल सकते हैं. बहुत सी अन्य जानकारी जैसे कि हार्डवेयर और सॉफ़्टवेयर की कंपनी, सिस्टम कॉन्फ़िगरेशन तथा नेटवर्क कनेक्शन के प्रकार, फ़ोन नंबर और एक्सेस प्रमाणीकरण प्रक्रियाएं हैकर का ध्यान आकर्षित करती हैं अर्थात प्रलोभित करती हैं.

## बुनियादी सुरक्षा अवधारणाएं

सूचना सुरक्षा के मुख्यतः तीन स्तंभ हैं, पहला गोपनीयता, दूसरा अखंडता और तीसरा उपलब्धता. गोपनीयता का अर्थ है कि केवल प्रमाणित उपयोगकर्ता को ही बिना किसी असफलता के डेटा तक पहुंच प्राप्त हो, जैसे कि अनुसंधान डेटा, चिकित्सा और बीमा रिकॉर्ड, नए उत्पाद विनिर्देश और कॉर्पोरेट निवेश रणनीति उच्च स्तर के गोपनीय दस्तावेज होते है, अगर इन सभी फाइलों को पढ़ा या कॉपी किया जा रहा है तो कोई अनधिकृत व्यक्ति विशेष, कंपनी या लोगों को बड़ा नुकसान पहुंचा सकता है.

नेटवर्क सुरक्षा में अखंडता सभी डेटा की यथार्थता सुनिश्चित करती है जिससे अनधिकृत उपयोगकर्ताओं द्वारा डेटा को नहीं बदला जाना चाहिए. नेटवर्क सुरक्षा में उपलब्धता द्वारा सुनिश्चित किया जाता है कि हैकर्स द्वारा सिस्टम या पूरे नेटवर्क से छेड़छाड़ न किया जा सके जिससे सभी महत्वपूर्ण व्यवसायिक प्रक्रियाएं सुचारू रूप से उपलब्ध रहें. नेटवर्क सुरक्षा की उपलब्धता सेवा उन्मुख व्यवसायों में सबसे महत्वपूर्ण विशेषता होती है, जो उपयोगी और महत्वपूर्ण जानकारी पर निर्भर करती है. जानकारी और डेटा मिटाया जा सकता है या पहुंच से बाहर किया जा सकता है, जिसके परिणामस्वरूप

अनुपलब्धता के कारण वित्तीय और सामरिक नुकसान हो सकता है.

### नेटवर्क सुरक्षा की कमज़ोरी

नेटवर्क सुरक्षा जटिल और महंगी होती है. वास्तव में ऐसी प्रणाली बनाना या डिजाइन करना लगभग असंभव है जो अनधिकृत एक्सेस को पहचान कर हमेशा बिना चूक के पुर्णतः रक्षा करे. नेटवर्क सुरक्षा एक अथाह गड्ढे की तरह है जिसके लिए एक सशक्त रक्षा परिधि बनाने के लिए काफी कौशल और संसाधनों के निवेश, दर्जनों इंजीनियर और वर्षों की शोध की आवश्यकता होती है. अक्सर कहा जाता है कि नेटवर्क पर प्रतिरक्षित होने का एकमात्र 100% और सबसे अच्छा तरीका प्लग को खींचना है. सुरक्षा नीतियां बहुत जटिल, सटीक और कभी-कभी बहुत परस्पर विरोधी होती हैं. इंटरनेट भी एक सहकर्मी से सहकर्मी प्रणाली है, जिससे इंटरनेट को एक प्रणाली के रूप में ठप्प करना लगभग असंभव हो जाता है. विफलता का कोई एक बिंदु नहीं है जो इंटरनेट के सभी या बड़े हिस्से को प्रभावित कर सकता है. इसके अलावा, उपयोगकर्ता और सिस्टम डेवलपर के पास आज उत्पाद विकास पर खर्च करने के लिए सीमित संसाधन हैं.

हाल के वर्षों में, दुनिया भर में कई नेटवर्क सुरक्षा घटनाएं हुई हैं. इंटरनेट के तेजी से विकास करने वाले उपयोगकर्ता के कारण, सुरक्षा नेटवर्क पहले से कहीं अधिक असुरक्षित है. नेटवर्क पर अनेक प्रकार की सुरक्षा घटनाएँ होती हैं, जिन्हें मोटे तौर पर कई प्रकारों में वर्गीकृत किया जाता है: जांच, स्कैन, खाता समझौता, रूट समझौता, पैकेट खोजी, सेवा से इंकार, विश्वास का तोड़ना और दुर्भावनापूर्ण कोड आदि.

### निष्कर्ष

आज प्रत्येक कंपनी के नेटवर्क पर सूचना के महत्व के साथ, उपयुक्त नेटवर्क सुरक्षा उपकरणों का उपयोग न करना गैर-जिम्मेदाराना होगा. इन उपकरणों के इस्तेमाल से कंपनियां साइबर हमले को होने से पहले ही रोक सकती हैं. फायरवॉल नेटवर्क सुरक्षा उपकरण की सबसे पुरानी और सबसे अच्छी तरह से स्थापित किस्म हैं. घुसपैठ का पता लगाने और रोकथाम के उपकरण जैसे अन्य उपकरण फ़ायरवॉल की क्षमताओं को उभरते खतरों की एक विस्तृत श्रृंखला तक विस्तारित करते हैं. अन्य डिवाइस ईमेल संचार, स्थानीय नेटवर्क पर होस्ट किए गए वेब एप्लिकेशन और दूरस्थ वीपीएन कनेक्शन की सुरक्षा कर सकते हैं.

अंततः नेटवर्क सुरक्षा सबसे महत्वपूर्ण और हमेशा विकसित होने वाली तकनीकों में से एक के रूप में संक्षेपित किया जाता है और सुरक्षा मुद्दों से निपटने के लिए सर्वोत्तम पद्दतियों की भी आवश्यकता होती है और मानव संसाधनों को हमेशा नवीनतम कौशल के साथ प्रशिक्षण देते रहना चाहिए.

*******

## 13. साफ ऊर्जा संक्रमण पर सीईए प्रार्थना

सुरता राम, मुख्य अभियन्ता, आर.टी. ऐण्ड आई. प्रभाग, सीईए

श्रीCEA श्रीCEA नमोः नमोः,
ऊर्जा धम्मो सनातनो।

अभी तक जो ऊर्जा विकास रहा,
पर्यावरण प्रकृति पलट रहा।
बाढ, भूकम्प, भूस्खलन रहा,
साइक्लोन समुद्र बढाव रहा।
चरम सर्दी, गर्मी, वर्षा, अकाल रहा,
ऋतुओं में भारी बदलाव रहा।
श्रीCEA श्रीCEA नमोः नमोः,.....

आपदाओं के ढेर सहा,
मानव ही तो जड़ में रहा।
ग्रीन हाउस गैसों का जनक रहा.
जिससे ग्लोबल ऊष्मीकरण बढ़ा।
हर आई.ई.ए. इरेना रिपोर्ट कहे,
ऊर्जा व उद्योग,
मुख्य उत्सर्जक क्षेत्र रहे।
तुरन्त उपचारी कदम भरें हम,
दूरदृष्टि हमारे नेत्र रहें।.....
श्रीCEA श्रीCEA नमोः नमोः,.....

ऊर्जा संक्रमण कदम अचूक रहे,
किसी को न बिजली की भूख रहे।
पंचामृत लक्ष्य..., हम प्राप्त करें,
साफ हवा सबको नसीब रहे।।
श्रीCEA श्रीCEA नमोः नमोः,.....

हर बच्चा बूढा आशा करे,
श्री CEA, श्री CEA, क्या करें?
देश-विदेश सहयोग करें,
डेढ सेल्सिय ($1.5^0$C) मार्ग पर पांव धरें।
विद्युतिकरण व दक्षता दो बालक रहे,
ऊर्जा संक्रमण के चालक रहे।
संग अक्षय ऊर्जा व हाइड्रोजन रहे,
सतत बायोमास प्रयोजन रहे।
श्रीCEA श्रीCEA नमोः नमोः,.....

पंच प्रौद्योगिकी सतम्भ प्रयोग करें,
तय ऊर्जा का भविष्य हम करें।
विद्युतीकरण,व शक्तितंत्र लचक करें,
अक्षय ऊर्जा उपयोग अनवरत करें।
हरित हाईड्रोजन तैयार करें।
नाना नवाचार स्वीकार करें।
श्रीCEA श्रीCEA नमोः नमोः,.....

*******

# 14. केंद्रीय विद्युत प्राधिकरण के समाचार व उपलब्धियाँ

- केंद्रीय विद्युत प्राधिकरण के प्रभागों एवं अनुभागों द्वारा 30 सितम्बर, 2022 को समाप्त तिमाही में राजभाषा अधिनियम, 1963 की धारा 3(3) के अंतर्गत जारी कागजात, हिंदी में प्राप्त पत्रों के उत्तर, अंग्रेजी में प्राप्त पत्रों के उत्तर 'क', 'ख', 'ग' क्षेत्रों को भेजे गए मूल पत्रों तथा फाईलों पर हिंदी में कार्य की स्थिति के अनुसार मूल हिंदी पत्राचार का प्रतिशत क्रमशः 94.02, 92.09 तथा 89.80 प्रतिशत रहा है.
- दिनांक 14.09.2022 से 29.09.2022 तक हिंदी पखवाड़ा का आयोजन किया गया, पखवाडा की शुरूआत सूरत, गुजरात में आयोजित हिदी दिवस समारोह एवं द्वितीय अखिल भारतीय राजभाषा सम्मेलन में प्रतिभागिता से हुई. तदुपरांत, केविप्रा मुख्यालय में हिंदी की उत्तरोत्तर प्रगति व व्यावहारिक ज्ञान से संबंधित पाँच प्रतियोगिताओं का आयोजन किया गया. दिनांक 19.09.2022 के दिन 'हिंदी में काम करने के लिए प्रेरणा व प्रोत्साहन' विषय पर हिंदी कार्यशाला का आयोजन किया गया. समापन समारोह के दिन दिनांक 29.09.2022 को काव्य गोष्ठी का आयोजन किया गया व विभिन्न प्रतियोगिताओं के विजेता प्रतिभागियों एवं वार्षिक प्रोत्साहन योजना के प्रतिभागी विजेताओं को पुरस्कार एव प्रमाण पत्र प्रदान किए गए. हिंदी में सर्वाधिक कार्य करने वाले 2 प्रभागों को राजभाषा ट्रॉफी प्रदान की गई.
- दिनांक 31.10.2022 से 06.11.2022 तक के.वि.प्रा. में सतर्कता जागरूकता सप्ताह मनाया गया.
- के.वि.प्रा. में 19 से 25 नवंबर 2022 तक संप्रदायिक्ता सद्भावना सप्ताह और 25.11.2022 को झंडा दिवस मनाया गया.
- दिनांक 26.11.2022 को के.वि.प्रा. में संविधान दिवस मनाया गया.
- श्री प्रवीण गुप्ता, मुख्य अभियंता को सदस्य, (तापीय) तथा श्री अशोक कुमार राजपूत, मुख्य अभियंता को सदस्य, (विद्युत प्रणाली) बनाए जाने पर "विद्युत वाहिनी" परिवार द्वारा बहुत-बहुत बधाई दी जातीं हैं.
- के.वि.प्रा. के प्रांगण में 17.11.2022 को अध्यक्ष महोदय द्वारा जिम का उद्घाटन किया गया.
- मौ. अफजल, मुख्य अभियंता, के.वि.प्रा. को, संयुक्त सचिव, विद्युत मंत्रालय में प्रतिनियुक्ति के आधार पर नियुक्ति किए जाने के अनुसरण में उन्हें 04.10.2022 से के.वि.प्रा. से कार्यमुक्त किया गया.
- श्री अशोक कुमार ठाकुर, मुख्य अभियंता, के.वि.प्रा. को, नर्मदा नियंत्रण प्राधिकरण के कार्यकारी सदस्य के पद पर प्रतिनियुक्ति के आधार पर नियुक्ति किए जाने के अनुसरण में उन्हें 07.11.2022 से के.वि.प्रा. से कार्यमुक्त किया गया.
- 30.11.2022 को श्री सनत मंडल (कनिष्ठ सचिवालय सहायक) एवं श्री रमेश चन्दर (एम टी एस), के.वि.प्रा. की 30.11.2022 को अधिवर्षता की आयु पूर्ण होने पर कार्यालय से कार्यमुक्त किया गया. 31.10.2022 को श्री अजय कुमार गुप्ता (सहायक अनुभाग अधिकारी) एवं श्री राम नरेश सिंह (कनिष्ठ सचिवालय सहायक) के.वि.प्रा. की 31.10.2022 को अधिवर्षता की आयु पूर्ण होने पर कार्यालय से कार्यमुक्त किया गया. 30.09.2022 को श्री रवीन्द्र गुप्ता, मुख्य अभियंता, श्रीमती खोजम, अनुभाग अधिकारी, श्री रामपाल, (कनिष्ठ सचिवालय सहायक), श्री नरेश कुमार, (कनिष्ठ सचिवालय सहायक) एवं

श्रीमती जगमाली, (एम टी एस), के.वि.प्रा. की 30.09.2022 को अधिवर्षता की आयु पूर्ण होने पर कार्यालय से कार्यमुक्त किया गया. "विद्युत वाहिनी" परिवार द्वारा अपने सभी सेवा निवृत साथियों के आगामी भविष्य के लिए शुभकामनाएँ दी जातीं हैं.

- केंद्रीय मंत्री (विद्युत, नवीन एवं नवीकरणीय ऊर्जा) माननीय श्री आर के सिंह जी द्वारा दिनांक 07.12.2022 को केन्द्रीय विद्युत् प्राधिकरण की 2030 तक 500 GW से अधिक नवीकरणीय ऊर्जा क्षमता के एकीकरण के लिए पारेषण योजना की रिपोर्ट का विमोचन किया गया.
- भारत के बीसवीं विद्युत शक्ति सर्वेक्षण की रिपोर्ट (भाग - एक) दिनांक 21.11.2022 को प्रकाशित की गयी.
- केंद्रीय विद्युत प्राधिकरण (विद्युत संयंत्रों और विद्युत लाइनों के निर्माण, संचालन और रखरखाव के लिए सुरक्षा आवश्यकताएँ) (संशोधन) विनियम, 2022 को 15.11.2022 को अधिसूचित किया गया.
- श्री विजय मेंघाणी, मुख्य अभियंता (स्वच्छ ऊर्जा एवं ऊर्जा परिवर्तन), केविप्रा ने दिनांक 06.11.2022 से 19.11.2022 तक संयुक्त राष्ट्र के तत्त्वाधान में जलवायु परिवर्तन पर मिस्र में आयोजित अंतर्राष्ट्रीय बैठक (CoP 27) में भारत सरकार के प्रतिनिधि के रूप में भाग लिया व पर्यावरण के क्षेत्र में तकनीकी स्थानांतरण, वित्तीय सहयोग व ऊर्जा के संसाधनों के न्यायसंगत उपयोग पर विभिन्न नीतिगत विषयों पर वार्ता में भाग लिया व विकासशील देशों की आवश्यकताओं पर वैश्विक संस्थाओं का ध्यान आकर्षित किया.

## 15. फोटो फीचर

- 16.11.2022 को श्री घनश्याम प्रसाद, अध्यक्ष, केन्द्रीय विद्युत् प्राधिकरण, नव नियुक्त सदस्यों श्री अशोक कुमार राजपूत, सदस्य (विद्युत् प्रणाली) एवं श्री प्रवीन गुप्ता, सदस्य (तापीय) का स्वागत करते हुए.

श्री अशोक कुमार राजपूत
सदस्य (विद्युत् प्रणाली)

श्री प्रवीन गुप्ता
सदस्य (तापीय)

- सतर्कता जागरूकता सप्ताह - दिनांक 31.10.2022 से 06.11.2022 तक.



- एकता एवं सद्भावना दिवस की झलकी.


- केविप्रा राजभाषा त्रैमासिक पत्रिका "विद्युत् वाहिनी" के प्रथम अंक का अध्यक्ष महोदय एवं केविप्रा के माननीय सदस्यों द्वारा विमोचन: दिनांक-29.09.2022.

- हिंदी पखवाड़ा का समापन समारोह - दिनांक 29.09.2022.

- केविप्रा के प्रांगण में 17.11.2022 को अध्यक्ष महोदय द्वारा जिम का उद्घाटन.





- फरीदाबाद में एनएचपीसी द्वारा 8 व् 9 दिसम्बर 2022 आयोजित 12वीं अन्तर सीपीएसयू एथलेटिक्स चैंपियनशिप में सुश्री निधि चौहान द्वारा ऊँची कूद (1.05 मी.) में रजत पदक और 800 मी. दौड़ कांस्य पदक जीतने पर बधाई.

- शिलांग में उत्तर पूर्वी क्षेत्रीय भार प्रेषण केंद्र द्वारा आयोजित अन्तर सीपीएसयू शतरंज टूर्नामेंट में केन्द्रीय विद्युत प्राधिकरण की महिला टीम को जीतने की बधाई (तीसरा स्थान).



- इसी टूर्नामेंटने में केन्द्रीय विद्युत प्राधिकरण के श्री गुरजीत मेंधी, उपनिदेशक (आर.आई.ओ. - शिलांग ने व्यकिगत श्रेणी में दूसरा स्थान प्राप्त करने पर बधाई.

- श्री विजय मेंघाणी, मुख्य अभियंता (स्वच्छ ऊर्जा एवं ऊर्जा परिवर्तन), केविप्रा, संयुक्त राष्ट्र के तत्वाधान में जलवायु परिवर्तन पर मिस्र में आयोजित अंतर्राष्ट्रीय बैठक (CoP 27) में भारत सरकार के प्रतिनिधि के रूप में.


**********

एक बार पुनः नववर्ष 2023 की बहुत-बहुत शुभकामनायें.

**जय हिन्द.**

**********