इंटरनेट सेवा प्रदाताओं हेतु साइबर अपराध रोकथाम सिद्धांत

कार्यकारी सारांश

- अधिक संख्या में उपभोक्ताओं को प्रभावित करने वाली ऑनलाइन दुर्भावनापूर्ण गतिविधियों को नियंत्रित करने हेतु इंटरनेट सेवा प्रदाताओं द्वारा क्रियान्वयन के लिये 4 प्रमुख सिद्धांतों को प्रस्तावित किया गया है। प्रत्येक सिद्धांत को कैसे लागू किया जा सकता है इसके तकनीकी विस्तार को संबंधित सिफारिश में शामिल किया गया है।
- इसमें मुख्यत: इस बात पर विचार किया गया कि किस प्रकार सरकार एवं सार्वजनिक क्षेत्र नीतिगत ढाँचे को स्थापित करने के लिये और अधिक कार्य कर सकते है जो इंटरनेट सेवा प्रदाताओं (Internet Service Providers- ISP) को दृढ़ता से कार्य करने के लिये सर्वोत्तम प्रोत्साहन उपलब्ध करा सकता है। कार्य के द्वितीय चरण में केंद्रित मुख्य क्षेत्रों में ऑनलाइन पारिस्थितिकी तंत्र की सुरक्षा के लिये उत्तरदायित्व एवं परिभाषित नियमों को शामिल करना है ताकि जवाबदेही का स्तर, कार्रवाइयों में पारदर्शिता तथा स्वतंत्र एवं खुले इंटरनेट को बनाए रखने से संबंधित सिद्धांतों की पुष्टि की जा सके और सामंजस्यपूर्ण ढंग से सर्वोत्तम प्रथाओं के अंगीकरण को प्रोत्साहित करने हेतु फ्रेमवर्क को निर्धारित करने का कार्य करना है।
- यह अनुशंसा की जाती है कि **इंटरनेट सेवा प्रदाताओं (ISP)** को निम्नलिखित प्रमुख सिद्धांतों को अपनाना चाहिये:
  1. व्यापक साइबर हमलों से उपभोक्ताओं की सुरक्षा करना एवं ज्ञात खतरों को पहचानने एवं वांछित प्रतिक्रिया देने हेतु समकक्षों के साथ मिलकर कार्य करना।
  2. खतरों से संबंधित जानकारी एवं जागरूकता फैलाने के लिये कार्यवाही करना एवं उपभोक्ताओं को उनके नेटवर्क एव स्वयं की सुरक्षा में सहयोग करना।
  3. सुरक्षा के न्यूनतम स्तर को बढ़ाने के लिये हार्डवेयर, सॉफ्टवेयर एवं अवसंरचना के विक्रेताओं तथा विनिर्माताओं के साथ मिलकर कार्य करना।
  4. राउटिंग और सिग्नलिंग/संकेतन (Signalling) की सुरक्षा को मजबूत करने हेतु आक्रमण के विरुद्ध रक्षा को प्रभावी तरीके से सुदृढ़ करने हेतु कार्यवाही करना।

यह सिद्धांतों का समूह ऐसी रणनीतिक कार्रवाइयों पर केंद्रित है जिन पर इंटरनेट सेवा प्रदाताओं का विश्वास है कि वे सामान्य ऑनलाइन अपराध से उपभोक्ताओं की सुरक्षा के प्रयोजन हेतु सक्षम है और इस प्रकार पूरे विश्व से इंटरनेट से संबंधित अपराधों के परिशोधन में सहायता मिलेगी।

अपेक्षित परिणामों एवं कार्य के लिये प्रोत्साहित करना

(Incentives for Action and Expected Outcomes)

- ऑनलाइन पारिस्थितिकी तंत्र में ऐसे कई विभिन्न कर्त्ता (Agents) है जो बड़े पैमाने पर होने वाले ऑनलाइन अपराध के विरुद्ध कार्रवाई कर सकते हैं। इंटरनेट ट्रैफिक वाहक के रूप में इंटरनेट सेवा प्रदाताओं की एक विशिष्ट एवं महत्त्वपूर्ण भूमिका है और साइबर अपराधियों द्वारा अपनाई जाने वाली कुछ रणनीतियों से निपटने में सक्षम होने के परिणामस्वरूप विशिष्ट स्थिति रखते हैं।
- ये चार सिद्धांत उन संगठनों पर भी निश्चित रूप से लागू हो सकते है जो स्वयं को इंटरनेट सेवा प्रदाताओं (ISPs) के रूप में मान्यता नहींदेते है। विश्व आर्थिक मंच और इन सिद्धांतों के विकास में शामिल साझीदार इन सिद्धांतों को लागू करने में सभी संगठनों को प्रोत्साहित करेंगे।
- ये सिद्धांत वैश्विक स्तर पर ISPs के अनुभव पर आधारित हैं जिन्होंने अपने ग्राहकों को ज्ञात दुर्भावनापूर्ण गतिविधियों से बचाने के लिये अपना ध्यान केंद्रित किया है और वे इससे प्राप्त होने वाले लाभों का प्रमाण देने में सक्षम हैं। अधिक जिम्मेदार व्यवहारों को अपनाने के व्यापक लाभों में निम्नलिखित शामिल हैं:
    - **ऑनलाइन सेवाओं मेंउपभोक्ताओं के विश्वास में वृद्धि ।**
    - नेटवर्क को दुर्भावनापूर्ण गतिविधियों से मुक्त कर सीमांत लाभों को बढ़ाया जा सकता है।
    - राष्ट्रीय ऑनलाइन पारितंत्र को स्वच्छ और सुरक्षित रखने में सहायक।
    - धोखाधड़ी एवं आपराधिक शिकायतों से संबंधित मामलों को कम करना एवं संबंधित मामलों की खोज एवं रिपोर्टिंग करना।
    - कंपनियों के कार्पोरेट सामाजिक उत्तरदायित्व (CSR) के अनुपालन में सहायक
    - प्रतिष्ठा एवं ब्रांड की बाज़ार में बेहतर छवि।

इंटरनेट सेवा प्रदाताओं एवं उपभोक्ताओं द्वारा सामना किये जा रहे कुछ सामान्य खतरे:

1. सोशल इंजीनियरिंग धोखाधड़ी (Social Engineering Fraud)

- सामाजिक इंजीनियरिंग धोखाधड़ी में वित्तीय लाभ के लिये अक्सर उपयोगकर्ता के व्यवहार को प्रभावित करने एवं गुप्त सूचनाओं के प्रकटन के लिये सामान्यत: ईमेल जैसी संचार प्रौद्योगिकी उपयोग की जाती हैं।
- वेरीजन डेटा उल्लंघन रिपोर्ट 2019 (Verizon Data Breach Report- 2019) के अनुसार वर्ष 2018 में डेटा उल्लंघन के मामलों में से 33% सोशल अटैक और 32% फिशिंग से संबंधित है।
- वर्तमान में 85% संगठनों द्वारा फिशिंग और सोशल इंजीनियरिंग अटैक जैसी समस्याओं का सामना किया जा रहा है।

2. विभिन्न उद्देश्यों विशेष रूप से बोटनेट्स (Botnets) के संचालन के लिये मेलवेयर का वितरण एवं उपयोग।

- लगभग 1000 साइबर हमलों के विश्लेषण से यह जानकारी मिली है कि इसमें मेलवेयर का प्रमुखता से प्रयोग हुआ है और कई देशों में इन्हें नियंत्रित करना अत्यधिक खर्चीला है।
- उदाहरण के लिये एक बैंकिंग बोटनेट का उपयोग 30,000 उपभोक्ताओं से 36 मिलियन यूरो से अधिक राशि को चुराने के लिये किया गया था।

3. विभिन्न तकनीकों का विस्तार नेमिंग एवं राउटिंग प्रोटोकॉल को कमजोर करने हेतु एवं बड़े पैमाने पर सेवा अवरोधन (Denial of Service-DoS) जैसे साइबर हमलों के लिये विभिन्न तकनीकों का उपयोग करना।

- किसी देश के कुल इंटरनेट यातायात में सेवा अवरोधन आक्रमण का हिस्सा लगभग 25% तक हो सकता है।
- अनुसंधान से ज्ञात होता है कि वेब आधारित हमले एवं सेवा अवरोधन आधारित हमले दोनों राजस्व में कमी लाने वाले प्रमुख कारक हैं।

सिद्धांत 1: व्यापक साइबर हमलों से उपभोक्ताओं की सुरक्षा करना एवं ज्ञात खतरों को पहचानने एवं वांछित प्रतिक्रिया देनेहेतुसमकक्षों के साथ मिलकर कार्य करना ।

यह सिद्धांत किन चुनौतियों का समाधान प्रस्तुत करता है?

- इंटरनेट सेवा प्रदाता (ISP) उपभोक्ताओं के पास पहुँचने से पहले ही व्यापक हमलों की पहचान करने एवं उनकी रोकथाम या शमन करने में सहयोग करके प्रथम श्रेणी की सुरक्षा के रूप में महत्त्वपूर्ण भूमिका निभा सकते है। इस संदर्भ में यदि ISPs कार्रवाई करते हैं तो संभावित हमलों के सफल होने की प्रायिकता को प्रभावी तरीके से कम किया जा सकता है। **BT साइबर सूचकांक** किसी आक्रमण के पैमाने को दर्शाता है जिसे प्रारंभिक स्तर पर इंटरनेट सेवा प्रदाताओं द्वारा की गई कार्रवाई की सहायता से रोका जा सकता है। इसके अतिरिक्त यदि कार्रवाई अपने स्वयं के नेटवर्क पर की जाती है तो समकक्षों के साथ सूचनाओं को साझा करके उपभोक्ताओं को उपलब्ध सुरक्षा को बढ़ा सकते है।
- ISP के स्तर पर मेलवेयर का अधिक सफलतापूर्वक निपटान किया जा सकता है जो प्राय: **सफल फिशिंग ईमेल** के परिणामस्वरूप डिवाइस में डाउनलोड हो जाते है तथा तंत्र को हानि पहुँचाने में इनका प्रयोग किया जा सकता है। सामान्यत: एक बार इंस्टाल हो जाने के बाद मेलवेयर **कमांड एवं कंट्रोल** सर्वर के माध्यम से नियंत्रित किये जाते हैं जिनका उपयोग सुभेद्य सिस्टम को कमांड देने एवं उससे डेटा चुराने हेतु किया जाता है। इन सर्वर का उपयोग उस कमांड को फैलाने के लिये किया जाता है जो डेटा चोरी, मेलवेयर को फैलाने और वेब सेवाओं को बाधित करने से संबंधित हो सकते हैं।
- बोटनेट्स का अपराधियों द्वारा कई तरीके से उपयोग एवं इनका मुद्रीकरण विभिन्न अपराधों जैसे - विभिन्न स्कैम्स या रैनसमवेयर को बढ़ावा देने एवं क्रिप्टोकरेंसीज की माइनिंग आदि में किया जा सकता है।
- बोटनेट्स की लागत मुख्य रूप से इंटरनेट सेवा प्रदाताओ (ISP) द्वारा वहन की जाती है और इसके प्रभाव उपभोक्ताओं एवं संपूर्ण समाज पर देखने को मिलते है।

यह सिद्धांत किस प्रकार प्रभावी है?

इस सिद्धांत के कार्यान्वयन से निम्नलिखित प्रभाव देखने को मिल सकते है:

- मेलवेयर को ग्राहकों के डिवाइसेज तक पहुँचने से रोक कर बोटनेट्स के विस्तार की रोकथाम की जा सकती है और ग्राहकों तथा इंटरनेट सेवा प्रदाताओ दोनों के लिये परिणामी लागत को कम किया जा सकता है।
- व्यापक जोखिमों और ISP द्वारा इनसे कैसे निपटा जाना चाहिये जैसी सूचनाओं के साझाकरण से यह अधिक व्यापक प्रतिक्रिया देने में सक्षम बनाएगा तथा अपराधियों के लिए हमलों में सफल होने को और अधिक कठिन बनाएगा।
- सामूहिक लचीलेपन का निर्माण करना तथा मेलवेयर के विस्तार तथा उपभोक्ताओं एवं अर्थव्यवस्था पर प्रभावों की रोकथाम की संभावना में वृद्धि।

केस स्टडी

1.यूनाइटेड किंगडम (UK) में BT समूह ने **राष्ट्रीय साइबर सिक्योरिटी केंद्र (National Cybersecurity Centre-NCSC)** एवं **इंटरनेट सेवा प्रदाताओं (ISP)** के साथ मिलकर दुर्भावनापूर्ण मेलवेयर कनेक्शन को ब्लॉक करने के लिये कार्य किया है। यह न केवल ग्राहकों की सुरक्षा करता है बल्कि UK के ऑनलाइन स्पेस के बचाव एवं सुरक्षा को सुनिश्चित करने में भी सहायता करता है, जिसमें से बहुत से राष्ट्रीय बुनियादी ढाँचा के लिये महत्त्वपूर्ण है। वर्तमान में BT अपने साइबर इंडेक्स पर इस कार्यक्रम के सकारात्मक प्रभावों से संबंधित आँकड़े प्रकाशित कर रहा है।
2. KT दक्षिण कोरिया में वायरलाइन एवं वायरलेस दोनों प्रकार के नेटवर्क की सेवाओं में कार्यरत प्रमुख कंपनी है। अभी हाल ही में कंपनी ने **गीगा सिक्योर प्लेटफॉर्म (GiGA Secure Platform-GSP) नामक** एक प्लेटफॉर्म विकसित किया है जहाँ सार्वजनिक संगठन एवं कंपनियाँ दुर्भावनापूर्ण कोड एवं वेबसाइट से संबंधित जानकारी एवं इनसे निपटने हेतु आवश्यक रणनीतियाँ साझा करती हैं।

सिद्धांत के क्रियान्वयन हेतु अनुशंसाएँ

1. ज्ञात साइबर हमलों से उपभोक्ताओं को डिफॉल्ट रूप से सुरक्षा उपलब्ध कराना तथा यह सुनिश्चित करना कि उपभोक्ता को ऐसे प्रयासों से अवगत कराया जाए और उनके पास इससे बाहर रहने का अवसर उपलब्ध होना चाहिये।
2. उपभोक्ताओं को डिफॉल्ट रूप से सुरक्षा उपलब्ध कराने, सर्वाधिक उपयुक्त तौर-तरीकों के निर्धारण करने तथा निगरानी तंत्र एवं विनियामक ढाँचे को परिभाषित करने हेतु समकक्षों, राष्ट्रीय एवं अंतर्राष्ट्रीय समूहों के साथ सहयोग करना।

सिद्धांत 2: खतरों से संबंधित जानकारी एवं जागरूकता फैलाने के लिये कार्यवाही करना एवं उपभोक्ताओं को उनके नेटवर्क एवं स्वयं की सुरक्षा में सहयोग करना।

यह सिद्धांत किन चुनौतियों का समाधान प्रस्तुत करता है?

- मनुष्य, चाहे व्यावसायिक क्षेत्र में हो या निजी क्षेत्र में वे हमलावरों के प्राथमिक लक्षय होते हैं क्योंकि उनके सिस्टम और आँकड़ों तक पहुँच सबसे आसान होती हैं। हालाँकि उपभोक्ताओं को हमेशा डिफॉल्ट रूप से साइबर अपराधों से सुरक्षा उपलब्ध कराना संभव नहीं हो पाता है। इस प्रकार उपभोक्ताओं में जागरूकता का प्रसार करने और प्रत्यक्ष हमलों से बचाव के लिये 'सुरक्षा की दूसरी परत' (Second Layer of Defence) का निर्माण करना चाहिये।
- ऐसे कई तरीके हैं जिसमें मनुष्य की कमजोरियों या सुभेद्यता का लाभ उठाया जा सकता है लेकिन फिशिंग ये उपयोगकर्त्ताओं को अवांछनीय ईमेल भेजे जाते है और उन्हें अपनी सूचनाएँ देने के लिये अथवा फर्जी वेब लिंक पर क्लिक करने के लिये प्रोत्साहित किया जाता है। अपराधी इस प्रकार के हमलों का उपयोग निजी जानकारी जुटाने, अकाउंट को हैक करने, पहचान चुराने, अवैध भुगतानों या ऐसी किसी अन्य गतिविधि को शुरू करने के लिये कर सकते हैं जिससे उपयोगकर्त्ता की कोई महत्त्वपूर्ण जानकारी का पता लगाया जा सके। अपराधियों द्वारा इस प्रकार के लिंक्स का प्रयोग उपयोगकर्त्ताओं के सिस्टम्स पर मेलवेयर को इंस्टॉल करने के लिये भी किया जा सकता है। वर्तमान में लगभग 85% संगठन फिशिंग और सामाजिक इंजीनियरिंग हमलों से प्रभावित है। ऐसे हमलों मे प्राथमिक वाहक के रूप में ईमेल की बजाय फोन कॉल्स का उपयोग करने पर इसे विशिंग (Vishing) तथा SMS का उपयोग करने पर स्मिशिंग (SMiShing) कहा जाता है।

- यद्यपि फिशिंग हमले प्रायः पूरी तरह अव्यवस्थित रूप से लक्षित होते है लेकिन बिज़नेस ई-मेल कॉम्प्रमाइज (Business Email Compromise-BEC) जैसे अपराध अधिक लक्षित होते है। BEC के तहत कोई हमलावर किसी कॉर्पोरेट ई-मेल अकाउंट को हैक कर लेता है और धोखाधड़ी के लिये वास्तविक मालिक अथवा कंपनी के वरिष्ठ अधिकारी के नाम से ग्राहकों, भागीदारों और/या कर्मचारियों को मेल भेजकर अपने खाते में धन हस्तांतरण करने अथवा संवेदनशील जानकारी देने की मांग करता है। BEC को फिशिंग ई-मेल, डोमेन नेम स्पूफिग (Domain Name Spoofing) जैसी विभिन्न तकनीकों के माध्यम से अंजाम दिया जा सकता है।
- इस प्रकार के सभी सोशल इंजीनियरिंग हमलों का क्रियान्वयन अपेक्षाकृत आसान होता है और इस प्रकार के हमलों के लिये तकनीकी समझ या हमलावरों के उपकरण भाग पर महत्वपूर्ण व्यय की आवश्यकता नहीं होती है। यद्यपि उनका आर्थिक प्रभाव व्यापक हो सकता है। FBI के अनुसार, BEC धोखाधड़ी के कारण वर्ष 2018 में USA के व्यापारियों एवं व्यक्तियों को एक बिलियन डॉलर से भी अधिक का नुकसान हुआ।
- चूँकि इस प्रकार के अपराध मानव व्यवहार की कमियों के दोहन पर केंद्रित होते हैं, इसलिये इनका समाधान शिक्षा एवं जागरूकता के प्रसार पर आधारित होना चाहिये। यदि संभावित अवांछनीय ई-मेल को इनबॉक्स तक पहुँचने से रोकना संभव हो तो ऐसा किया जाना चाहिये। लेकिन ऐसे खतरों से निपटने के लिये उपभोक्ताओं को भी सशक्त किया जाना चाहिये।

यह सिद्धांत किस प्रकार प्रभावी है?

इस सिद्धांत के कार्यान्वयन से निम्नलिखित प्रभाव देखने को मिल सकते है:

- फिशिंग हमलों तथा इनके परिणामस्वरूप धोखाधड़ी एवं पहचान चोरी के कारण वित्तीय एवं प्रतिष्ठा संबंधी नुकसानों में कमी।
- अधिक-से-अधिक पारस्परिक विश्वास निर्माण एवं त्वरित प्रतिक्रिया तंत्र को सक्षम बनाने हेतु नागरिकों एवं उत्तरदायी साइबर प्राधिकरण के सदस्यों के बीच सूचना एवं जागरूकता के प्रसार में सुगमता।
- सर्वप्रथम भेजे गए अवांछनीय एवं फर्जी ईमेल की संख्या को कम करना ताकि हमलों की संभावना को कम कर, संचार प्रवाह को निर्बाध जारी रखा जा सके।

केस स्टडी

सऊदी अरब की सऊदी टेलीकॉम कंपनी (STC) समूह ने स्पैम एवं धोखाधड़ी समाधान के रूप में एक बहु-स्तरीय व्यवस्था लागू की है-

- प्रथम स्तर में किसी स्पैम शील्ड (Spam Shield) या स्मार्ट फिल्टर (Smart Filter) का उपयोग किया जाता है जो रियल टाइम मशीन लर्निंग एल्गोरिथ्म के आधार पर SMS फिल्टरिंग नियमों का मूल्यांकन एवं नवीकरण करता है।
- द्वितीय लेयर में SMS गेटवे एवं अत्याधुनिक जोखिम आसूचना प्लेटफॉर्म (Threat Intelligence Platform-TIP) का एकीकृत रूप से प्रयोग किया जाता है। यह प्लेटफॉर्म विभिन्न आंतरिक एवं बाहरी स्रोतों से सूचनाओं को प्राप्त करता है एवं ऐसे लिंक्स को जिनके दुर्भावनापूर्ण होने की संभावना है उन्हें SMS गेटवे को भेज दिया जाता है ताकि ऐसे SMS को ग्राहकों के पास पहुँचने से पहले ही बंद कर दिया जाता है।

- तृतीय स्तर में STC **डोमेन नेम सर्वर** (Domain Name Server-DNS) **सिस्टम** होता है,जो आगे TIP से जुड़ा हुआ है। यह TIP, DNS सिस्टम को किसी भी दुर्भावनापूर्ण डोमेन की पहचान करने एवं उसे ब्लॉक करने में सक्षम बनाता है।
- चतुर्थ स्तर में हैंडसेट की सुरक्षा को शामिल किया जाता है। STC ने प्रमुख हैंडसेट सुरक्षा भागीदारों के साथ सहयोग स्थापित किया है ताकि अपने ग्राहकों को हानिकारक लिंक एवं वायरस, मेलवेयर, स्पाइवेयर के विरुद्ध अतिरिक्त स्वचालित सुरक्षा प्रदान कराई जा सके।
- अंतिम सुरक्षा स्तर के अंतर्गत ग्राहक जागरूकता अभियानों का संचालन किया जाता है। किसी भी संदिग्ध SMS की सूचना देने के लिये ग्राहकों हेतु एक समर्पित फोन नंबर की व्यवस्था की गई है ताकि इसका परीक्षण हो सके और यदि आवश्यक हो तो ऐसे SMS को उनके स्रोत पर ही ब्लॉक किया जा सके।

इस पाँच स्तरीय सुरक्षा परतों के कारण STC की SMS सेवाओं के माध्यम से भेजे गए अवांछित एवं धोखाधड़ी संदेशों की संख्या को कम करने में काफी सहायता मिली है। STC के नेटवर्क पर प्रतिदिन 338 मिलियन SMS का पंजीकरण होता है, जिसमें से औसत 20 मिलियन SMS संदिग्ध या दुर्भावनापूर्ण विशेषताओं के कारण ब्लॉक कर दिये जाते है।

इस सिद्धांत के क्रियान्वयन हेतु अनुशंसाएँ

1. उपभोक्ताओं का निर्देशन

- ग्राहकों का सर्वोत्तम सुरक्षा अभ्यासों के बारे में एक न्यूनतम स्तर का मार्गदर्शन किया जाना चाहिये तथा जहाँ उचित हो संदिग्ध गतिविधियों की रिपोर्टिंग के तरीकों से भी अवगत कराना चाहिये। क्योंकि शिक्षा एवं जागरूकता का विस्तार ही सोशल इंजीनियरिंग अटैक के विरुद्ध सुरक्षा का प्रमुख उपकरण है।
- ग्राहकों की अपने सिस्टम पर पहचानी गई संदिग्ध गतिविधियों या सुभेद्यताओं की त्वरित सूचना देने के लिये तंत्र स्थापित करना और इनसे निपटने हेतु आवश्यक सहायता उपलब्ध कराना।

2. ई-मेल सुरक्षा

स्वयं के नेटवर्क डोमेन में **डोमेन आधारित संदेश प्रमाणीकरण, रिपोर्टिंग एवं अनुरूपता (**Domain-Based Message Authentication, Reporting and Conformance-DMARC) को लागू करना एवं ग्राहकों को भी अपने डोमेन में इसे लागू करने में सहयोग करना।

- DMARC एक तकनीकी मानक है जो इंटरनेट सेवा प्रदाताओं (ISP) के लिये दुर्भावनापूर्ण ई-मेल के प्रयासों जैसे- उपयोगकर्त्ता की व्यक्तिगत जानकारी की फिशिंग करने के लिये डोमेन स्पूफिंग, की रोकथाम करना आसान बनाता है।
- DMARC का क्रियान्वयन स्पूफिंग की पूरी तरह से रोकथाम नहीं करता है लेकिन यह हमलावरों के साइबर हमलों की लागत में महत्त्वपूर्ण वृद्धि कर देता है। इसके अतिरिक्त इसका प्रभावी क्रियान्वयन सार्वजनिक विश्वास के निर्माण एवं इसे सुदृढ़ करने में महत्त्वपूर्ण भूमिका निभाएगा, विशेष रुप से प्रसिद्ध ब्रांडों के संबंध में जिनके ईमेल डोमेन का उपयोग किसी दूसरे प्रकार से धोखाधड़ी के प्रयोजन से किया जा सकता है।
- यूनाइटेड किंगडम सरकार ने सरकारी डोमेन में DMARC के उपयोग की प्रभाविता को प्रमाणित किया है। नीदरलैंड एवं संयुक्त राज्य अमेरिका भी अपने डोमेन में DMARC क्रियान्वयन को अनिवार्य कर रहे है।

3. स्मिशिंग (Smishing) के प्रति सुरक्षा

नेटवर्क पर स्मिशिंग के जोखिमों को समझने के लिये ऑनलाइन पारितंत्र के सभी भागीदारों के साथ सहयोग करना और इन्हें कम करने एवं असामान्य व्यवहार की रिपोर्टिंग पर मानदंडों को लागू करने के लिये प्रयास करना।

स्मिशिंग का मुख्य कारण मोबाइल फोन एवं स्मार्ट फोन की तेजी से बढती संख्या हैं। SMS एवं इंस्टेंट संदेश संचार की सुलभ, प्रभावी एवं लोकप्रिय विधि है। कुछ देशों में इनके अन्य संचार रूपों की तुलना में अधिक खुले होने एवं पढ़ने की संभावना अधिक होने के कारण अवांछनीय ईमेल भेजने और फिशिंग हमले में इनके प्रयोग की संभावनाएँ अधिक हैं।

सिद्धांत 3: सुरक्षा के न्यूनतम स्तर को बढ़ाने के लिये हार्डवेयर, सॉफ्टवेयर एवं अवसंरचना के विक्रेताओं तथा विनिर्माताओं के साथ मिलकर कार्य करना।

यह सिद्धांत किन चुनौतियों का समाधान प्रस्तुत करता है?

- कुछ नेटवर्किंग हार्डवेयर, विशेष रूप से ग्राहकों को उपलब्ध कराए जाने वाले कम लागत वाले उपकरण प्रायः इस तथ्य के कारण आसान लक्षय के रूप में देखे जाते हैं क्योंकि ऐसे उपकरणों में सुविदित डिफॉल्ट प्रशासनिक पासवर्ड एवं उपयोगकर्त्ता ID युक्त फर्मवेयर एवं पासवर्ड होता है जिसका आसानी से दुरुपयोग किया जा सकता है और इनको आसानी से अपडेट भी नहीं किया जा सकता।
- नेटवर्क प्रदाता द्वारा प्रदत्त उपकरणों के साथ ही नेटवर्क से जुड़े हुए उपकरणों पर भी हमला हो सकता है। इंटरनेट से जुड़े हुए उपकरणों की बढ़ती संख्या से इन उपकरणों द्वारा ऑनलाइन पारिस्थितिकी तंत्र के लिये प्रस्तुत खतरों की मात्रा बढ़ रही है। मिराई बाटनेट एक ऐसा उदाहरण है कि कैसे असुरक्षित उपकरण वृहत् ऑनलाइन हमलों को बढ़ावा दे सकते है।
- वर्ष 2018 में FBI ने कहा की कुछ विशेष प्रकार के राउटर्स (Routers) के उपयोगकर्त्ताओं को इन्हें रीस्टार्ट करना चाहिये क्योंकि ये मेलवेयर से प्रभावित है। इस समस्या के कार्य-क्षेत्र के निर्धारण का एक अन्य तरीका 'इंटरनेट ऑफ थिंग्स' (IoT) उपकरणों के लिये डिजाइन किये गए मेलवेयर के प्रकारों का का पता लगाना है। एक अनुमान के मुताबिक़ वर्ष 2018 के प्रथमार्द्ध में इंटरनेट ऑफ थिंग्स उपकरणों पर हमले करने के लिये प्रयुक्त मेलवेयर्स की भिन्नताओं में तीन गुनी वृद्धि देखने को मिली है।
- हालाँकि ऐसे उपकरणों की सभी सुभेद्यताओं का निर्धारण करना कठिन है। लेकिन ऐसे सुभेद्य उपकरणों के कारण होने वाली हानि को कम करने के लिये कदम उठाए जा सकते है। ऐसा माना जाता है कि कोडिंग के समय सुरक्षित IoT उत्पाद की डिज़ाइन पर कम ध्यान दिया जाता है।
- वर्तमान में ऑनलाइन एवं भौतिक दुनिया की अंतर्संबद्धता में निरंतर वृद्धि हो रही है तो भविष्य में इंटरनेट से जुड़े हुए उपकरणों पर होने वाले ऑनलाइन हमले भौतिक दुनिया को गंभीर रूप से प्रभावित कर सकते हैं। जैसे- गृह सुरक्षा या जल आपूर्ति जैसी जीवन को प्रभावित करने वाली महत्त्वपूर्ण प्रणाली पर रैनसमवेयर आक्रमण से समुदायों एवं व्यक्तियों पर गंभीर प्रभाव पड़ सकता है।

यह सिद्धांत किस प्रकार प्रभावी है?

इस सिद्धांत के कार्यान्वयन से निम्नलिखित प्रभाव देखने को मिल सकते है:

- अपराधियों के लिये हमले हेतु उपलब्ध उपकरणों और अवसरों में कमी जिसके परिणामस्वरूप उपभोक्ताओं एवं इंटरनेट सेवा प्रदाताओं दोनों पर संभावित हमलों के प्रभाव में कमी लाना।
- उपभोक्ताओं में कुशल सुरक्षित कार्यप्रणालियों को बढ़ावा देना एवं समस्त आपूर्ति शृंखला में सुरक्षा मानकों तथा पारदर्शिता को प्रोत्साहित करना।
- परस्पर अंतर्संबद्ध पारितंत्र की सुरक्षा में वृद्धि एवं संचार अवसंरचना की स्थिरता को बढ़ाना।

केस स्टडी

1. STC विश्व भर में भिन्न-भिन्न आपूर्तिकर्ताओं एवं प्रबंधित सेवा प्रदाताओं (Managed Service Providers-MSP) के साथ कार्य करती है जो विशेष रूप से STC की साइबर सुरक्षा टीम के लिये चुनौती है। आपूर्ति शृंखला द्वारा प्रस्तुत खतरों से निपटने के लिये STC ने इसके समस्त स्तरों पर लागू होने वाले थर्ड पार्टी मानकों एवं नीतियों को परिभाषित किया। तीसरे पक्ष के सभी आपूर्तिकर्त्ताओं एवं MSP को इन मानको एवं नीतियों का अनुपालन करना अनिवार्य था। इन नियंत्रणों को लागू करने के परिणामस्वरूप STC अपने आपूर्तिकर्त्ताओं की सुरक्षा में वृद्धि करने में सक्षम हो चुकी है। इस प्रकार STC व्यापक ऑनलाइन पारिस्थितिकी तंत्र को सुगम बनाने के साथ ही स्वयं के उपभोक्ताओं को कई प्रकार के जोखिमों से संरक्षण प्रदान कर रही है।

2. यूरोपियन संचार मानक संस्थान (ETSI**) से संबंधित केस स्टडी**

ETSI ने इंटरनेट से जुड़े हुए किन्ही भी उपकरणों की खरीद के लिये तीन मुख्य मानदंड निर्दिष्ट किये है जिससे बड़ी संख्या में हमलों के विरुद्ध सुरक्षा में सहायता मिल सकती है-

1. यह सुनिश्चित करना कि उपकरण पूर्व-निर्धारित पासवर्ड के साथ न हो और उसे उपभोक्ता द्वारा परिवर्तित किया जाना अपेक्षित हो बल्कि वह विशिष्ट और अद्वितीय होना चाहिये। इससे मिराई आक्रमण को रोकने में सहायता मिली थी।
2. इंटरनेट-कनेक्टेड उपकरणों एवं सेवाओं का उत्पादन करने वाली कंपनियों को एक ऐसा संपर्क स्थल प्रदान कराना चाहिये जिसे मामलों को सीधे रिपोर्ट किया जा सके। यह कंपनियों को समय पर किसी मामले में प्रतिक्रिया देने एवं समाधान करने में सक्षम बनाता है।
3. इंटरनेट से जुड़े हुए उपकरणों में सॉफ्टवेयर का अद्यतन आसान और समयबद्ध होना चाहिये। यह सुनिश्चित करता है कि आक्रमण की सुभेद्यता बढ़ाने वाली किसी सॉफ्टवेयर की गड़बड़ी को ठीक किया जा सकता है ।

इस सिद्धांत के क्रियान्वयन हेतु अनुशंसाएँ

प्रबंधन प्रोटोकॉल का उपयोग एवं संवर्द्धित विक्रेता सुरक्षा

- सुभेद्य उपकरणों के कारण होने वाले नुकसान को कम करने के लिये उन प्रोटोकॉल को प्रतिबंधित करने पर विचार किया जाना चाहिये जिनकी सामान्यत: अधिकांश ग्राहकों को आवश्यकता नहीं है। जब तक ऐसा करने के लिये कोई उपयुक्त कारण न हो, ग्राहक परिसर उपकरण (Customer Premises Equipments-CPE) के प्रबंधन प्रोटोकॉल की उन नेटवर्क से बाह्य राउटिंग को ब्लॉक कर देना चाहिये तथा यह सुनिश्चित करना कि प्रबंधन की इंटरनेट के माध्यम से इन तक पहुँच न हो।
    CPE टेलीफोन या अन्य सेवा प्रदाता उपकरण हैं जो प्रदाता के परिसर की बजाय ग्राहक के परिसर (भौतिक अवस्थिति) पर स्थापित किये जाते हैं। टेलीफोन हैंडसेट, केबल टीवी सेट-टॉप बॉक्स और डिजिटल सब्सक्राइबर लाइन राउटर इसके उदाहरण हैं।

- समस्त आपूर्ति शृंखला में IoT उपकरणों के लिये स्वीकार्य न्यूनतम मानकों पर स्पष्टता सुनिश्चित करने हेतु पहलों और फ्रेमवर्क को प्रोत्साहन एवं समर्थन देना।
    - उपभोक्ताओं ने IoT उपकरणों की सुरक्षा कैसे की जाए इसके लिये हाल ही में यूरोपियन तकनीक मानक संस्थान द्वारा सिद्धांतों के एक समूह का समर्थन किया गया था।
    - इंटरनेट सोसायटी ने भी एक IoT ट्रस्ट फ्रेमवर्क स्थापित किया है, जो IoT उपकरणों के लिये सुरक्षा स्तर में वृद्धि करने का प्रयास करता है एवं उपभोक्ताओं से संबंधित सेवाओं तथा उनके डेटा गोपनीयता को और बेहतर तरीके से सुरक्षित करता है।

सिद्धांत 4: राउटिंग और सिग्नलिंग/संकेतन (Signalling) की सुरक्षा को मजबूत करने के लिये आक्रमण के विरुद्ध रक्षा को प्रभावी तरीके से सुदृढ़ करने हेतु कार्यवाही करना।

यह सिद्धांत किन चुनौतियों का समाधान प्रस्तुत करता है?

- कई अपराधी ऐसी रणनीतियों का उपयोग करते है जो हमले के लिये इंटरनेट पर ट्रैफिक के प्रवाह पर निर्भर करती हैं। ऐसे हमले का उद्देश्य बड़े पैमाने पर नेटवर्क एवं सेवाओं की उपलब्धता का अनुचित लाभ उठाना है। ऐसे कई हमले अपराधियों द्वारा पहचान के संबंध में अंतर्निहित धारणाओं का उल्लंघन करने का परिणाम होते है जो इंटरनेट पर राउटिंग, नेमिंग और एड्रेस प्रणालियों में निहित हैं। इस प्रकार के कई हमले DoS में होते हैं जिसका **संगठनों की प्रतिष्ठा**एवं **व्यापार संचालनों को आयोजित करने की उनकी क्षमता** दोनों पर प्रभाव पड़ सकता है।
- साथ ही सोशल इंजीनियरिंग अटैक के उद्देश्य से ईमेल एड्रेस की स्पूफिंग या मेलवेयर का प्रयोग करने के अलावा अपराधी नकल करने के लिये भी समान युक्तियों का उपयोग कर सकते हैं अर्थात् अपराधी आँकड़ों तक पहुँच प्राप्त करने के लिये इंटरनेट प्रोटोकॉल (IP) एड्रेस में हस्तक्षेप कर सकते है। इसी प्रकार अपराधी संपूर्ण एड्रेस ब्लॉक्स को चुरा सकते हैं, हालाँकि ऐसा आम तौर पर कम होता है लेकिन इससे IP एड्रेस की मैपिंग पर गंभीर प्रभाव पड़ सकता है।
- अपराधी समान उद्देश्य के लिये इंटरनेट ट्रैफिक की दिशा भी बदल सकते हैं अर्थात् अपराधी आक्रमण के विभिन्न तरीके अपना सकते है। ISP ने एक हालिया सर्वे में बताया कि उनमें 70% से अधिक ISP स्पूफिंग संबंधित आक्रमण से प्रभावित थे।
- IP सोर्स एड्रेस स्पूफिंग का एक आपराधिक उपयोग सेवा अवरोधन (DoS) का संचालन है जो ट्रैफिक को नकली एड्रेस की ओर निर्देशित कर देता है और नेटवर्क एवं सर्वर को नुकसान पहुँचा देता है।
- यह ISPs और उनके ग्राहकों दोनों को क्रमश: विकृत छवि और ब्रांड तथा सेवा अवरोधन द्वारा नकारात्मक रूप से प्रभावित कर सकता है। एक रिपोर्ट के अनुसार, वर्ष 2018 की तीसरी तिमाही में 65% DoS हमले संचार सेवा प्रदाताओ पर किये गए थे।
- इस प्रकार के राउटिंग हमलों के अतिरिक्त अपराधी डोमेन नेम सिस्टम (Domain Name System) से छेड़छाड़ की रणनीतियाँ अपना रहे है जिसमे इंटरनेट ट्रैफिक को फर्जी वेबसाइट की ओर मोड़कर उपभोक्ताओं से आँकड़े और उनकी जानकारी चुरा ली जाती है। डोमेन नेम सिस्टम मानव पठनीय वेब एड्रेस का मशीन पठनीय IP एड्रेस में परिवर्तन का प्रबंधन करता है।

यह सिद्धांत किस प्रकार प्रभावी है?

इस सिद्धांत को अपनाने से संपूर्ण रूप से ऑनलाइन पारितंत्र पर महत्त्वपूर्ण प्रभाव पड़ सकता है एवं ISPs की दक्षता में सुधार देखने को मिल सकता है जिससे अपने भागीदारों के साथ समकक्ष संबंधों (Peer Relations) में अधिक स्पष्टता आती है। इस सिद्धांत के कार्यान्वयन से निम्नलिखित प्रभाव देखने को मिल सकते है:

- भागीदारों के साथ समकक्ष संबंधों पर ISPs के बीच कार्य क्षमता और पारदर्शिता में वृद्धि करना।
- इंटरनेट संचार के कुछ मूल स्तंभों पर सशक्त रूप से होने वाले विनाशकारी आक्रमण की संभावनाओं को न्यून करना।
- ISPs को होने वाले राजस्व एवं मूल्य हानि को कम करना।

इस सिद्धांत के क्रियान्वयन हेतु अनुशंसाएँ

ISP के कार्यान्वयन को लागू करने के लिये प्रोटोकॉल संबंधित कई उपाय लागू कर सकता है जो अपराधियों के लिये ट्रैफिक राउटिंग का कुशलता पूर्वक उपयोग करना, सेवा अवरोधन अन्य आक्रमण करना अधिक कठिन बनाता है।

1. सिग्नलिंग/संकेतन और राउटिंग क्रियान्वयन हेतु प्रभावी आधारभूत प्रोटोकॉल्स को लागू करना।

वर्तमान BGP समकक्ष संबंधों को समझना और BGP हाईजैक की बेहतर तरीके से पहचान तथा प्रभावी प्रतिक्रिया सुनिश्चित करने हेतु समकक्षों के साथ सहयोग करना।

- इंटरनेट ट्रैफिक की राउटिंग के तरीकों से भी IP एड्रेस की स्पूफिंग जैसे सुरक्षात्मक मुद्दे संबद्ध है।
- सेवा प्रदाताओं (ISPs) एवं वाहकों (Carriers) द्वारा इंटरनेट नेटवर्क पर ट्रैफिक प्रवाह निर्धारित करने हेतु बॉर्डर गेटवे प्रोटोकॉल (Border Gateway Protocol-BGP) नामक प्रोटोकॉल का उपयोग किया जाता है। नेटवर्क इन रूट्स का 'विज्ञापन' करते हैं एवं एक राउटर इन रुट्स से पैकेट भेजने हेतु **न्यूनतम लागत वाला निर्णय** लेगा।
- अपराधी किसी विशेष गंतव्य के लिये न्यूनतम मूल्य वाले रूट की घोषणा कर सकते हैं जिसे स्वचालित रूप से चुन लिया जाएगा और ट्रैफिक संभावित रूप से अवांछित या फर्जी गंतव्य की ओर निर्दिष्ट हो सकता है। किसी धोखाधड़ी से संबंधित वेबसाइट की ओर पुनः निर्दिष्ट होने से अंतिम उपयोगकर्त्ता पर इसका नकारात्मक प्रभाव पड़ सकता है।
- कुछ देशों में वर्तमान BGP राउटिंग की निगरानी के लिये ISPs द्वारा सहयोग किया जा रहा है और इसने एक प्लेटफॉर्म विकसित किया है जिसके माध्यम से BGP हाईजैक के कुछ प्रकारों का स्वतः पता लगाया जा सकता है। जैसे BT ने सार्वजनिक एवं निजी क्षेत्रों में वैश्विक भागीदारों के साथ मिलकर कार्य किया है ताकि BGP संरक्षण के लिये औद्योगिक मानकों में सुधार करने तथा दुर्भावनापूर्ण मार्ग के परिवर्तन की बेहतर तरीके से पहचान करने के लिये प्रयास किये जा सके।

2. राउटिंग सुरक्षा हेतु पारस्परिक रूप से सहमत मानक (Mutually Agreed Norms for Routing Security-MANRS) प्रोजेक्ट से जुड़ने पर विचार करना एवं MANRS की आवश्यकताओं को लागू करना।

- **MANRS** इंटरनेट सोसायटी द्वारा समर्थित एक वैश्विक पहल है जो सबसे सामान्य राउटिंग जोखिमों के लिये अत्यंत महत्त्वपूर्ण समाधान उपलब्ध कराती है एवं ISPs द्वारा सामना की जा रही कई चुनौतियों के समाधान में भी सहायक है। इस प्रोजेक्ट के लाभों के बाह्य विश्लेषण से यह ज्ञात होता है कि ISPs द्वारा सहभागिता से ग्राहकों की दृष्टि में मूल्य में वृद्धि के माध्यम से उनके राजस्व में वृद्धि हो सकती है। MANRS निदेश इंटरनेट कम्युनिटी की सुरक्षा तथा संचालन दक्षता सुनिश्चित करने हेतु महत्त्वपूर्ण दस्तावेज़ है।
- GSMA-Led जैसी पहलों के माध्यम से BT समूह यूनाइटेड किंगडम में राउटिंग एवं सिग्नलिंग में सुधार करने के लिये कई उपायों पर कार्य कर रहा है ताकि ग्राहकों एवं UK तथा उससे बाहर भी व्यापक ऑनलाइन पारितंत्र की सुरक्षा करने में सहयोग किया जा सके।

3. इन्ग्रेस फ़िल्टरिंग (Ingress Filtering) का प्रयोग करना ताकि कुछ प्रकार के वितरित सेवा अवरोधन (DDoS) हमलों को कठिन बनाया जा सके और नेटवर्क पर दुर्भावनापूर्ण गतिविधियों की मात्रा को कम किया जा सके।

- कंप्यूटर नेटवर्किंग में इन्ग्रेस फिल्टरिंग एक ऐसी तकनीक है जिसका उपयोग यह सुनिश्चित करने के लिये किया जाता है कि नेटवर्क में प्रवेश करने वाला डेटा ट्रैफिक वास्तव में उन्हीं नेटवर्कों से संबंधित हैं, जहाँ से वे उत्पन्न होने का दावा करते हैं।
- इन्ग्रेस फ़िल्टरिंग का उपयोग उद्यमों और इंटरनेट सेवा प्रदाताओं (ISPs) द्वारा एक नेटवर्क में संदिग्ध आवागमन को रोकने के लिये किया जाता है।

4. DNS जैसे प्रोटोकॉल तक पहुँच और इनके उपयोग का उचित रूप से प्रबंधन किया जाना चाहिये जिनका DoS हमलों में प्रयोग किया जा सकता है।

5. SS7 प्रोटोकॉल की सुरक्षा संबंधी सुभेद्यताओं के बारे में जागरूकता का प्रसार करना एवं ग्राहकों की बेहतर सुरक्षा के लिये प्रासंगिक समाधानों को लागू करना और यह सुनिश्चित करना कि सिग्नलिंग की आगामी पीढ़ी अपेक्षाकृत अधिक सुरक्षित हो।

> टेलीकॉम ऑपरेटर्स सिग्नलिंग सिस्टम नंबर 7 (SS7) वह प्रोटोकॉल है जो अंतर्राष्ट्रीय टेलीकॉम नेटवर्कों को कॉल करने, SMS भेजने तथा रोमिंग की स्थिति में संचार करने की अनुमति देता है। इस प्रोटोकॉल में बहुत कम सुरक्षा अंतर्निहित है और इसलिये SS7 की सुभेद्यताओं का अपराधियों द्वारा लाभ उठाना आसान होता है।

निष्कर्ष

- इन सिद्धांतों के विकास में सहयोग करने वाले कार्य-दल ने इस बात पर सहमत व्यक्त की है कि सभी इंटरनेट सेवा प्रदाताओं को इन सिद्धांतों एवं अनुशंसाओं को लागू करने के लिये वचनबद्ध होना चाहिये क्योंकि वैश्विक ऑनलाइन पारितंत्र पर इनका व्यापक प्रभाव देखने को मिल सकता है।
- नवंबर 2019 में साइबर सुरक्षा पर वर्ल्ड इकोनामिक फोरम (WEF) के वार्षिक सम्मेलन में इन सिद्धांतों पर चर्चा की गई और कई भागीदारों द्वारा इनका समर्थन किया गया था।
- नीतिगत ढाँचा स्थापित करने एवं सुरक्षा को बढ़ाने के लिये इंटरनेट सेवा प्रदाताओं (ISPs) द्वारा उत्तरदायी व्यवहार को प्रोत्साहित करने हेतु विनियामक एवं सरकारों के बीच एक विचार-विमर्श शुरू करना प्राथमिकता होनी चाहिये।
    - **इस आलेख में प्रस्तावित अधिकांश गतिविधियों को सार्वजनिक-निजी क्षेत्र के व्यापक सहयोग से संपादित किया जा सकता है।**
    - साइबर अपराध रोकथाम पर संचार एवं जागरूकता वृद्धि में सरकार की भी महत्त्वपूर्ण भूमिका है। इसके अलावा सरकार और विनियामक विभिन्न भागीदारों द्वारा उत्तरदायी व्यवहार के लिये आवश्यक शर्तों का निर्धारण कर सकते है।
- ज्ञात खतरों एवं दुर्भावनापूर्ण वेबसाइटो पर विस्तृत सूचनाओं को साझा करना ताकि नवीन और उभरते खतरों से निपटने की रणनीति का विकास किया जा सके।
- इंटरनेट ऑफ थिंग्स (IoT) उपकरणों की सुरक्षा में सुधार करने के लिये सहयोग बढ़ाया जाना चाहिये क्योंकि इंटरनेट कनेक्टेड उपकरण साइबर हमलों के प्रति अधिक सुभेद्य होते है।

- सूचना साझाकरण जैसी पहलें और दुर्भावनापूर्ण गतिविधियों को आकर्षित एवं विश्लेषण करने वाले तथाकथित 'हनीपॉट्स' के माध्यम से साइबर हमलों से सुरक्षा करने एवं उचित प्रतिक्रिया देने की क्षमता में सुधार किया जा सकता है।
- ISPs के बीच प्रतिस्पर्द्धा को बढावा देने और ग्राहकों को सुरक्षित सेवाएँ उपलब्ध कराने के उद्देश्य से समकक्षों की तुलना और विश्लेषण प्रवृत्तियों को बढ़ावा दिया जाना चाहिये। इसके अतिरिक्त पहले से उठाए जा रहे कदमों के प्रभावों का मापन भी वांछित है।