भारतातील सायबर सुरक्षा

EY च्या नवीनतम ग्लोबल इन्फॉर्मेशन सिक्युरिटी सर्व्हे (GISS) 2018-19 – भारत आवृत्तीनुसार, भारतामध्ये सायबर धोक्यांपैकी एक सर्वाधिक संख्या आढळून आली आहे आणि लक्षित हल्ल्यांच्या बाबतीत देश दुसऱ्या क्रमांकावर आहे. जरी बँकिंग आणि दूरसंचार हे सर्वाधिक आक्रमण झालेले क्षेत्र असले तरी मॅन्युफॅक्चरिंग, हेल्थकेअर आणि रिटेल यांनाही मोठ्या प्रमाणात सायबर हल्ल्यांचा सामना करावा लागला आहे.

सायबर धोक्याचे प्रकार/ Types of cyber threats

- **फिशिंग/Phishing**: भ्रामक ई-मेल आणि वेबसाइट्सचा वापर वैयक्तिक माहिती गोळा करण्यासाठी केला जातो.
- **मालवेअर/Malware**: हे दुर्भावनापूर्ण सॉफ्टवेअरचा संदर्भ देते ज्यामुळे सिंगल कॉम्प्युटर, सर्व्हर किंवा कॉम्प्युटर नेटवर्कचे नुकसान होते. मालवेअरचे विविध प्रकार म्हणजे रॅन्समवेअर, स्पायवेअर, व्हायरस, वर्म्स, ट्रोजन इ.
- **सेवा नाकारणे (DoS) हल्ले/Denial of Service (DoS) attacks**: एखादे मशीन किंवा नेटवर्क त्याच्या वापरकर्त्यांसाठी अगम्य बनवण्यासाठी बंद करण्यासाठी हा प्रकार घडतो. पूर वाहतूक(flooding traffic) किंवा क्रॅश होणारी माहिती पाठवून हे लक्ष्य केले जाते.
- **मॅन-इन-द-मिडल (MitM) हल्ले:** हे ऐकून होणारे (eavesdropping) हल्ले आहेत. हे दोन-पक्षीय व्यवहाराच्या बाबतीत घडते जेथे हल्लेखोर स्वत: ला त्यात ठेवतात. रहदारीमध्ये व्यत्यय आणून, ते डेटा फिल्टर करतात आणि चोरतात.
- **स्ट्रक्चर्ड क्वेरी लँग्वेज (SQL) इंजेक्शन:** डेटाबेसच्या संप्रेषणासाठी ही एक प्रोग्रामिंग भाषा आहे. वेबसाइट आणि सेवांसाठी गंभीर डेटा साठवणाऱ्या सर्व्हरवर हल्ला होतो. दुर्भावनापूर्ण (Malicious) कोडचा वापर सर्व्हरमधील माहिती प्रकट करण्यासाठी केला जातो जी सामान्यतः करत नाही.
- **क्रॉस-साइट स्क्रिप्टिंग (XSS):** हे SQL इंजेक्शन हल्ल्यासारखे आहे. हे वेबसाइटवरच हल्ला करत नाही परंतु वेबसाइटमध्ये दुर्भावनापूर्ण कोड इंजेक्ट केला जातो. जेव्हा एखादा वापरकर्ता वेबसाइटला भेट देतो तेव्हा ती थेट वापरकर्त्याच्या मागे जाते.
- **सामाजिक अभियांत्रिकी:** मानवी संवादाद्वारे हल्लेखोर संवेदनशील माहिती मिळवतात.
- **हार्डवेअर हल्ला:** मॅन्युफॅक्चरिंग बॅकडोअर मालवेअर किंवा इतर भेदक हेतूंसाठी तयार केले जाऊ शकते. मागील दरवाजे रेडिओ-फ्रिक्वेंसी आयडेंटिफिकेशन (RFID) चिप्स आणि आठवणींमध्ये एम्बेड केले जाऊ शकतात.

सायबर हल्ल्यामागील हेतू/ Motives behind cyber-attacks

- सायबर गुन्हे
- सायबर चोरी
- सायबर हेरगिरी
- सायबर घुसखोरी

भारतामध्ये सायबर हल्ला/ Cyber-attack in India

- EY चे 2018-19 चे ग्लोबल इन्फॉर्मेशन सिक्युरिटी सर्व्हे सूचित करते की लक्ष्यित हल्ल्यांमध्ये भारत दुसऱ्या क्रमांकावर आहे. बँकिंग, दूरसंचार, उत्पादन, आरोग्यसेवा, रिटेल आणि सरकारी वेबसाइट्स ही काही प्रभावित क्षेत्रे आहेत.
- इंडियन कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीम (CERT-In) च्या अहवालानुसार, अधिकृत भारतीय वेबसाइट्सवर सर्वाधिक सायबर हल्ले चीन, अमेरिका आणि रशियाकडून झाले आहेत.

अलीकडील हल्ल्याची काही उदाहरणे/ Some of the examples of the recent attack

- **StrandHogg Malware:** भारतीय सायबर गुन्हे समन्वय केंद्राने सर्व राज्ये आणि पोलीस विभागांना अलर्ट पाठवला आहे. हा हल्ला अँड्रॉइड ऑपरेटिंग सिस्टीमला मायक्रोफोन ऐकण्यास, एसएमएस, कॅमेरा, फोटो आणि इतर लॉगिन क्रेडेन्शियल्समध्ये प्रवेश करण्यास अनुमती देईल.
- **स्पायवेअर पेगासस:** सोशल मीडिया प्लॅटफॉर्म व्हाट्सएपचा वापर इस्रायली फर्म, एनएसओ ग्रुपने विकसित केलेले स्पायवेअर टूल 'पेगासस' वापरून पत्रकार आणि मानवाधिकार कार्यकर्त्यांची हेरगिरी करण्यासाठी केला गेला.
- **युनियन बँक ऑफ इंडिया:** जुलै 2016 मध्ये हॅकर्सनी कर्मचाऱ्यांना फिशिंग ईमेल पाठवला. त्यांनी क्रेडेन्शियल्समध्ये प्रवेश केला आणि निधी हस्तांतरित केला. यासाठी बँकेला $171 दशलक्ष खर्च आला. मात्र, तो परत वसूल करण्यात आला.
- **Wannacry Ransomware हल्ला**: मे 2017 मध्ये, खंडणीच्या मागणीसाठी भारतातील अनेक संगणक हॅकर्सनी लॉक केले. आंध्र प्रदेश पोलिस आणि पश्चिम बंगालच्या राज्य युटिलिटीच्या कार्यप्रणालीवरही परिणाम झाला.
- **पेट्या रॅन्समवेअर हल्ला:** हा जून २०१७ मध्ये झाला. हा जागतिक रॅन्समवेअर हल्ला होता. त्याचा परिणाम डॅनिश फर्म एपी मोलरवर झाला जो जेएनपीटी, मुंबई येथे कंटेनर हँडलर आहे.
- 2017 मध्ये CERT-In द्वारे GravityRAT (रिमोट ऍक्सेस ट्रोजन) मालवेअर हल्ला ईमेल संलग्नकाद्वारे विविध संगणकांमध्ये घुसखोरी करत असल्याचे आढळले.

- इतर मालवेअर हल्ले जसे मिराई, रीपर, सपोशी इ.

सायबर सुरक्षा फ्रेमवर्क/ Cyber Security Framework

- दृश्यमानता, विश्लेषणे आणि एकत्रीकरणाद्वारे वापरकर्ता, मालमत्ता आणि व्यवहारांच्या संरक्षणासाठी. शासन रचना खालीलप्रमाणे असू शकते:
- **ओळख आणि अधिकृतता:** गोपनीयता, किमान प्रकटीकरण आणि अनामिकता समर्थन.
- **डेटा सुरक्षा:** डेटा सार्वभौमत्व, डेटा लोकॅलायझेशन, इंटरऑपरेबिलिटी आणि सुरक्षित संप्रेषण.
- **धोक्याचे व्यवस्थापन:** प्रोफाइलिंग, संरक्षण, शोध आणि प्रतिसादाद्वारे.
- **लवचिकता निर्माण करणे:** जोखीम-आधारित निर्णय, डेटा प्रवाह आणि लोक-केंद्रित सुरक्षितता.

भारतातील कायदे

- माहिती तंत्रज्ञान कायदा, 2000- याने कायद्याच्या कलम 70(1) मध्ये महत्त्वपूर्ण माहिती पायाभूत सुविधा परिभाषित केल्या आहेत.
- राष्ट्रीय सायबर धोरण, 2013
- न्यायमूर्ती बी एन श्रीकृष्ण समितीच्या शिफारशीनुसार डेटा संरक्षण विधेयक.

सरकारी धोरण

- इंडियन कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीम (CERT-In) हे MeitY मधील एक कार्यालय आहे जे सायबर सुरक्षा धोक्यांना सामोरे जाणारी नोडल एजन्सी आहे.
- इंडियन सायबर क्राइम कोऑर्डिनेशन सेंटर (I4C) हे आर्थिक फसवणूक, पोर्नोग्राफिक आणि सांप्रदायिक सामग्री यासारख्या सायबर गुन्ह्यांचा सामना करण्यासाठी सर्वोच्च समन्वय केंद्र आहे.
- सायबर सुरक्षित भारत उपक्रम, 2018
- सायबर स्वच्छता केंद्र
- माहिती सुरक्षा शिक्षण आणि जागरूकता प्रकल्प
- डिजिटल अन्वेषण प्रशिक्षण आणि विश्लेषण केंद्र (DITAC)
- नॅशनल सायबर कोऑर्डिनेशन सेंटर: तंत्रज्ञान क्षमता शोधण्यासाठी भारताच्या डेटा सुरक्षा परिषदेच्या भागीदारीत टेकसागर प्लॅटफॉर्म सुरू केला आहे.
- राष्ट्रीय माहिती विज्ञान केंद्र
- सायबरस्पेसवर जागतिक परिषद आयोजित करण्यात आली होती. त्याची थीम 'सायबर 4 ऑल: शाश्वत विकासासाठी एक सुरक्षित आणि सर्वसमावेशक सायबरस्पेस' होती. आंतरराष्ट्रीय स्तरावर मान्यताप्राप्त 'रस्त्याचे नियम' आणि सर्व भागधारकांचा सहभाग स्थापित करणे हे त्याचे उद्दिष्ट होते.

- इंटरनेट वापरकर्त्यांना अधिक जलद आणि सुरक्षित ब्राउझिंग अनुभव देण्यासाठी सरकारने स्वतःचे सार्वजनिक डोमेन नेम सर्व्हर (DNS) सुरू करण्याची योजना आखली आहे.
- नरेश चंद्र टास्क फोर्स आणि चीफ ऑफ स्टाफ कमिटीच्या शिफारशींवर राष्ट्रीय सुरक्षेसमोरील आव्हानांना तोंड देण्यासाठी सरकार संरक्षण सायबर एजन्सी स्थापन करणार आहे.
- MHA ने सरकारला सुरक्षित करण्यासाठी राष्ट्रीय माहिती सुरक्षा धोरण आणि मार्गदर्शक तत्त्वे (NISPG) जारी केली आहेत

भारतातील सायबर सुरक्षा पदानुक्रम

PM OFFICE/CAB INET SECY (PMO/CAB SEC)	MINISTERY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Security COuncil (NSC)	National Cyber Corrd Centre (NCCC)	Ambassadors & Ministers	Tri Service Cyber Commad	Department Of Information Technology (DIT)	Cyber Security And Anti Hacking Organisation (CSAHO)
National Technical Research Org (NTRO)	Directorate of Forensic Science (DFS)	Defence Attaches	Army (MI)	Department of Telecom (DoT)	Cyber Society of India (CySI)
National Critical Info Infrastructure Protection Centre (NCIIPC)	National Disaster Mgt Authority (NDMA)	Joint Secretary (IT)	Navy (NI)	Indian Computer Emergency Response Team CERT-IN	Centre of Excellence for Cyber Security Research & Development in India (CECSRDI)
Joint Intelligence	Central Forensic Science Lab (CFSLs)		Air Force (AFI)	Educational Research Network (ERNET)	Cyber Security of India (CSI)

PM OFFICE/CABINET SECY (PMO/CAB SEC)	MINISTERY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Crisis Management Committee (NCMC)	Intelligence Bureau (IB)		Def Info Assurance & Research Agency (DIARA)	Informatics Center (NIC)	National Cyber Security of India (NCS)
Research & Analysis Wing (RAW)			Defence Intelligence Agency (DIA)	Centre for Development of Advanced Computing C-DAC	Cyber Attacks Crisis Management Plan of India (CACMP)
Multi Agency Center			Defence Research Dev Authority (DRDO)	Standardisation, Testing and Quality Certification (STQC)	
National Information Board (NIB)					

आंतरराष्ट्रीय यंत्रणा:

- यूएन ग्रुप ऑफ गव्हर्नमेंट अँड एक्सपर्ट्स (यूएनजीजीई) ने 2013 मध्ये 11 नियम सुचवले होते.
- बुडापेस्ट कन्व्हेन्शन ऑन सायबर-सुरक्षा 2001 मध्ये युरोप कौन्सिलने काढले, जे 1 जुलै 2004 रोजी लागू झाले. भारताने परदेशी कायद्याची अंमलबजावणी करणाऱ्या एजन्सींसोबत डेटा सामायिकरणाच्या मुद्द्यावर त्याचा स्वीकार केलेला नाही. ऑगस्ट 2020 मध्ये, नवीन कराराची स्थापना करण्यासाठी समिती बोलावली जाणार आहे.
- CERT-In ने मलेशिया, सिंगापूर आणि जपान या तीन राष्ट्रांसोबत सहकार्य करारावर स्वाक्षरी केली आहे.

निष्कर्ष:

P-P-P मॉडेलद्वारे सायबर-सुरक्षा फ्रेमवर्कची कल्पना केली जाऊ शकते. आंतरराष्ट्रीय मानकांचे पालन करणारे सिक्युरिटी ऑडिट सर्व सरकारी वेबसाइट्सना लागू असावे. राज्य-सीईआरटीच्या मदतीने सायबर-सुरक्षा कवायती केल्या जाऊ शकतात. आयटी प्रकल्प राबवणाऱ्या सरकारी संस्थांनी आयटी कायदा, 2000 आणि राज्य सायबर सुरक्षा धोरणाच्या सुरक्षा आवश्यकतांचे पालन करण्यासाठी योग्य वाटप केले पाहिजे. सायबर सुरक्षेसाठी नागरिक आणि लहान व्यवसायांमध्ये क्षमता वाढवणे आणि जागरूकता निर्माण करणे आवश्यक आहे.