विभाग 1
सायबर सुरक्षेची ओळख

जगभरात इंटरनेट वापरणारयांची संख्या 4 अब्जच्या वर गेलेली आहे. माहिती तंत्रज्ञान विकासां बरोबर इंटरनेट चा वापर आपल्या सर्वांसाठी अपरिहार्य ठरत आहे. इंटरनेट मुळे, आज सार्वजनिकपणे माहिती उपलब्ध करून देणे, माहिती इमेल द्वारे पाठविणे, सोशल नेटवर्किंग द्वारे आपल्या मित्रांशी जुडलेले असणे, चोवीस तास विविध सुविधा क्षणात पुरविणे, जगाच्या पाठीवर कुठूनही एकत्र काम करणे इत्यादी आपल्याला सहज पणे शक्य झाली आहे. लॉकडाउनच्या काळात मोबाइल, लॅपटाप्सचा वापर वाढला ज्याद्वारे अर्थव्यवस्था, शिक्षण आणि मनोरंजन या तिन्ही गोष्टी सायबर स्पेसमध्ये आपण आणल्या. या सर्व गोष्टीचा फायदा सायबर गुन्हेगार घेत असून, ते आपल्या सर्वांना 'लक्ष्य' करत आहेत. देशातील सायबर गुन्ह्यांमध्ये वाढ होऊनआर्थिक फसवणुकीला लहानापासून मोठ्यापर्यंत सर्व जण बळी पडण्याचं प्रमाणही वाढू लागलंय. हॅकर्स, हेर, अतिरेकी आणि गुन्हेगार संघटनांकडून, विविध सर्वर म्हणजेच कॉम्प्युटर्स वर आपली उपलब्ध महत्वाची वैयक्तिक माहिती हॅक म्हणजेच चोरली जाऊन त्याचा गैरवापर केला जाऊ शकतो. अलीकडेच मोठ्या प्रमाणात रेनसॅमवेअर नावाने प्रसिद्ध झालेल्या मालवेअरचा आर्थिक फटका मोठ्या प्रमाणात सर्व देशांनां झेलावा लागला, ज्या अटॅकमध्ये लोकांची महत्वाची वैयक्तिक माहिती ओलीस ठेवून हॅकर्स कडून खंडणी गोळा केली गेली.

“जर तुम्ही आपल्या शत्रूंना ओळखत असाल आणि स्वत:ला पण ओळखत असाल तर, तुम्ही शंभर युद्ध पण जिंकाल”. सायबर क्रिमिनल्स (सायबर स्पेस मधील गुन्हेगार) ह्यांचा हेतू आणि सायबर एटेकस (सायबर स्पेस मधील हल्ले) चे विविध प्रकार, आपण समजून घेतले तर, हे ज्ञान आपल्याला स्वतःचे प्रभावी संरक्षण करण्यास नक्कीच मदत करू शकेल. तर, ह्या विभागात सायबर सिक्युरीटीतील मूलभूत गोष्टी, सायबर थ्रेटस (सायबर स्पेस मधील धमक्या), सायबर एटेकस (सायबर स्पेस मधील हल्ले), सायबर क्रिमिनल्स (सायबर स्पेस मधील गुन्हेगार) ह्यांचा हेतू ह्या गोष्टी समजविल्या आहेत.

सायबर सिक्युरीटी क्षेत्रात वापरल्या जाणारी मूलभूत शब्दावली

सायबर क्राईम (सायबर गुन्हा)

गुन्हेगारी क्रिया जिथे लोक, सायबरस्पेसमधील माहिती, सेवा किंवा ॲप्लिकेशन्स लक्ष्य करण्यासाठी सायबरस्पेस वापरले जातात.

Asset (असेट/मालमत्ता)

एखाद्या संस्थेच्या दृष्टीने मूल्यवान असणारी कोणतीही वस्तू, मालमत्ता मूर्त (जे आपण प्रत्यक्षात पाहू शकतो असे) असू शकतात, जसे की नेटवर्क उपकरणे, सिस्टम इ. किंवा मालमत्ता अमूर्तही असू शकतात जसे की सॉफ्टवेअर किंवा बौद्धिक मालमत्ता. सायबरस्पेस मधील आपली उपलब्ध महत्वाची वैयक्तिक माहिती हे आपले असेट आहे.

Cyber Attack (सायबरअटॅक/हल्ला)

मालमत्ते/ असेट चा अनधिकृत वापर करणे, सायबरस्पेस मधील वैयक्तिक माहिती उघड करणे, माहिती मध्ये अनधिकृत रित्या बदल करणे, महत्वाची माहितीची चोरी करणे किंवा सायबरस्पेस मधील सिस्टम मध्ये अनधिकृत प्रवेश मिळवण्याचा प्रयत्न करणे.

Audit (ऑडिट)

पद्धतशीर, स्वतंत्र पुनरावलोकन(review/ रिव्हीव) प्रक्रिया ज्यामध्ये ठरविलेले मार्गदर्शक निकष किती प्रमाणात पूर्ण केले जातात हे निर्धारित करण्यासाठी मूल्यांकन केले जाते.

Access control (AC/ऍक्सेस कंट्रोल)

आपली माहिती/ असेट चा वापर अथवा आपल्या सिस्टिममध्ये प्रवेश अधिकृत वाआपल्या सुरक्षा आवश्यकता नुसार असल्याचे सुनिश्चित करण्यासाठी असणारे साधन.

Entity (एंटीटी/घटक)

वेगळे अथवा स्वतंत्र अस्तित्व असणारी व्यक्ती, सिस्टिम, प्रक्रिया इत्यादी.

Authentication (ऑथॉनटीकेशन /प्रमाणीकरण)

एखाद्या एंटीटी अथवा घटकाची सांगितलेली वैशिष्ट्ये बरोबर असल्याची दावा केल्यास ते खातर जमा करण्यासाठी सिस्टिम मध्ये असणारी तरतूद.

Availability (अवैलीबिलिटी /उपलब्धता)

अधिकृत एंटीटी अथवा घटकाद्वारे मागणी केल्यावर, त्यांच्या द्वारे आपल्या माहिती/ असेट चा वापर अथवा आपल्या सिस्टिममध्ये अधिकृत पणे प्रवेश करता येणे

Business Continuity (BC/बिझनेस कॉन्टीनुएटी)

एखादी विघटनकारी घटना जसे कि सायबर हल्ला झाल्यास एखाद्या संस्थेची पूर्वनिर्धारित स्तरावर उत्पादने आणि सेवांचे वितरण सुरू ठेवण्यासाठी क्षमता.

Business Impact Analysis (BIA/बिझनेस वर झालेले परिणामांचे विश्लेषण)

बिझनेस /व्यवसाया मध्ये एखाद्या विघटनकारी घटना मुळे व्यत्यय आल्यास, त्या घटनेचे व्यवसायातील प्रक्रिया आणि सेवां वर झालेले परिणामांचे विश्लेषण करण्याची प्रक्रिया

Confidentiality (कॉन्फिडेंटिऍलिटी /गोपनीयता)

कुठल्याही अनधिकृत व्यक्ती, संस्था किंवा प्रक्रिया ह्यांना आपल्या माहिती उपलब्ध करु ना देण्याचे सिस्टिम मधील वैशिष्ट्य.

Cyber theft (सायबर चोरी)

सायबरस्पेसवर चोरी अथवा सायबर स्पेसवर फसवणूक करणाऱ्या क्रिया.

Cyber terrorism (सायबर दहशतवाद)

देशातील राज्ये, व्यवसाय आणि अर्थव्यवस्था यांच्याविरूद्ध दहशतवाद्यांनी केलेले सायबर हल्ले. यात स्वत: च्या सरकारविरूद्ध लोकांना वळण देण्याचा प्रयत्न करणारे दहशतवादी गट किंवा सरकार असंतुलित करण्याचा प्रयत्न करणारे दुसरे राष्ट्र राज्य असू शकतात. हे सर्व दहशतवादाचे फक्त एक प्रकारचे मार्ग आहेत ज्यामुळे लोकां मध्ये भय निर्माण करण्यासाठी किंवा द्वेष उत्पन्न करण्यासाठी दहशतवाद्यांद्वारे योजिले जातात.

Hacking (हॅकिंग)

एखाद्या सिस्टिम अथवा प्रणाली वर अनधिकृत रित्या ताबा मिळविणे.

Cyber warfare (सायबर वॉरफेयर / सायबर युद्धनीती)

युद्ध प्रणाली अथवा युद्ध नीती ज्यामध्ये दुसऱ्या देशाच्या माहिती मालमत्ते वर किंवा पायाभूत सुविधांवर सायबर स्पेसद्वारे केलेले हल्ले.

Cyber espionage (सायबर एस्पियोनेज / सायबर हेरगिरी)

सायबर स्पेसवर गुप्त रित्या केलेली देखरेख अथवा हेरगिरी.

Vulnerability (असुरक्षितता)

सायबर सुरक्षा यंत्रणेतील कमकुवतपणा म्हणजेच असुरक्षितता, ज्याचा उपयोग संस्थेच्या असेटचे नुकसान करण्यासाठी केला जाऊ शकतो. उदाहरणार्थ, कोणतीही प्रमाणीकरण यंत्रणा नसलेली प्रणालीतील असुरक्षितता, ज्याचा उपयोग आपल्या वैयक्तिक माहितीचा अनधिकृत मार्गाने गैरवापर करण्यासाठी केला जाऊ शकतो, मालवेयर संक्रमणास कोणतेही अँटीव्हायरस प्रणाली नसलेली सिस्टम म्हणजेच असुरक्षितता.

Threat (थ्रेट/ संभाव्य धोका)

सायबर सुरक्षा यंत्रणेसाठी संभाव्य धोका ज्यामुळे संस्थात्मक मालमत्तेस हानी पोहोचू शकेल. उदाहरणार्थ हॅकर्स, गुन्हेगार, दहशतवादी, दुर्भावनायुक्त किंवा अप्रशिक्षित संस्थेतील व्यक्ती, नैसर्गिक आपत्ती, प्रतिस्पर्धी इत्यादींमुळे सायबर सुरक्षा यंत्रणेसाठी संभाव्य धोके ठरू शकतात. सिस्टममधील असुरक्षितता कमी करून संभाव्य धोक्याची तीव्रता नियंत्रित केली जाऊ शकते.

Phishing (फिशिंग)

फिशिंग हा गोपनीय माहिती मिळवण्या साठी हॅकर्स द्वारे एक प्रकारचे अटॅक आहे ज्या मध्ये फिशर्स म्हणजेच हॅकर्स आर्थिक फायद्यासाठी विशिष्ट व्यक्ती, गट किंवा संस्था ह्यांची नक्कल करून वापरकर्त्यांना फसवून त्यांच्याजवळील वैयक्तिक गोपनीय माहिती (बँकिंग प्रमाणपत्रे, क्रेडिट कार्ड नंबर इत्यादी) कडून घेण्याचा प्रयत्न करतात.

Social Engineering (सोशिअल इंजिनीरिंग)

सोशिअल इंजिनीरिंग एक प्रकारचे अटॅक आहे ज्या मध्ये बर्‌याचदा सुरक्षा प्रक्रियांचा भंग करण्यासाठी व्यक्ती किंवा संस्था ह्यांना फसविण्याचा समावेश असतो, मानवी संवाद साधून. यात हॅकर्स, वापरकर्ता असल्याचे भासवून व्यक्ती खात्याचे पासवर्ड रीसेट करण्यासाठी आणि सिस्टम खात्यांवरील अनधिकृत प्रवेश मिळविण्यासाठी हेल्पडेस्क विश्लेषकांना संपर्क करतो.

Risk (रिस्क/ जोखीम)

रिस्क म्हणजेच काही संभाव्य धोका/घटना घडून येण्याची शक्यता ज्यामध्ये सायबर सुरक्षा यंत्रणेतील असुरक्षितता हेरून मालमत्तेस हानी पोहोचवण्यासाठी वापरण्याची शक्यता निर्माण करते. सर्व **रिस्क** /जोखीम ओळखणे किंवा दूर करणे अवघड आहे. काही शिल्लक धोका/ **रिस्क** नेहमीच असतो ज्याला रेसिड्युअल **रिस्क** म्हणतात.

CIA Triad (सी आई ए ट्रायएड)

सी आई ए ट्रायएड, म्हणजेच वैयक्तिक माहितीची कॉन्फिडेंटिऍलिटी /गोपनीयता , इंटेग्रिटी/ विश्वसनियंता, अवैलबिलीटी /उपलब्धता . Confidentiality, integrity and availability. सी आई ए ट्रायएड हे एक मॉडेल आहे जे संस्थेमध्ये माहिती सुरक्षा व्यवस्थापनासाठी धोरणांच्या अंमलबजावणीसाठी मार्गदर्शित करते. कॉन्फिडेंटिऍलिटी मध्ये केवळ अधिकृत वापरकर्त्यांकडेच माहिती दिली जाणे. इंटेग्रिटी/ विश्वसनियंता मध्ये केवळ एखाद्या अधिकृत वापरकर्त्यां द्वारेच माहितीमध्ये बदल करता येणे. अवैलबिलीटी /उपलब्धता म्हणजे केवळ जेव्हा आवश्यक असेल तेव्हाच माहिती आणि सेवा अधिकृत वापरकर्त्यांसाठी वितरित केले जाणे.

Non-Repudiation (नॉन रेपुडीएशन)

ही सायबर सुरक्षा यंत्रणेतील एक वैशिट्य जी हमी देते की संदेश पाठविणारा नकार देऊ शकत नाही कि त्याने एखादा संदेश पाठविलेले नाही. तसेच हमी देते की संदेश प्राप्तकर्ता त्या संदेशास प्राप्त झाल्यास ते नाकारू शकत नाही.

Authorization (ऑथोरिझशन/ अधिकृतता)

ऑथोरिझशन म्हणजे प्रक्रिया जी निश्चित करते की दिलेल्या सिस्टमसाठी अधिकृत प्रवेश वापरकर्त्याचे कोणते अधिकार आहेत. **ऑथोरिझशन** प्रक्रिया हे अधिकृत वापरकर्त्या द्वारे कुठले अधिकार वापरण्याची परवानगी आहे किंवा त्याला कुठले सर्विसेस उपलबध आहेत ह्या धोरणांची अंमलबजावणी करते. सहसा, **ऑथॉनटीकेशन** नंतर **ऑथोरिझशन** किंवा अधिकृतता तपासण्याची प्रक्रिया केली जाते.

Accountability (अकाऊंटॅबिलिटी)

अकाऊंटॅबिलिटी प्रक्रिया जी अधिकृत वापरकर्त्याला, त्याने सायबरस्पेसमधील माहिती, सेवा किंवा ॲप्लिकेशन्स वर केलेल्या क्रियांसाठी जबाबदारी निश्चित करते. अधिकृत वापरकर्त्या द्वारे तयार झालेले ऑडिट ट्रेल्स आणि सिस्टम लॉग जबाबदारी व्यवस्थापित करण्यात मदत करतात.

Information Security Management (माहिती सुरक्षा व्यवस्थापन**)**

माहिती सुरक्षा व्यवस्थापन ही एक प्रक्रिया आहे ज्यात सायबरस्पेसमधील मालमत्तांचे संरक्षण करण्यासाठी संस्थेच्या मालमत्तांची ओळख, सुरक्षा धोरणे आणि प्रक्रियेचा विकास आणि अंमलबजावणी समाविष्ट असते. संस्थेच्या माहितीची गोपनीयता, अखंडता आणि उपलब्धता सुनिश्चित करणे हे त्याचे उद्दीष्ट आहे.

Information Security Policy (माहिती सुरक्षा धोरण)

माहिती सुरक्षा धोरण हि एक नियमावली ज्यामध्ये अधिकृत वापरकर्त्या माहिती, सेवा किंवा अँप्लिकेशन्स हाताळताना नियमांचे पालन करतात हे सुनिश्चित करते. सामान्यत: हि नियमावली योग्यरित्या दस्तऐवजीकरण केलेले असते, संस्थेच्या व्यवस्थापनाच्या मान्यतेने ते अधिकृत केले जाते आणि सर्व वापरकर्त्यांद्वारे वाचले जाईल याची खात्री केली जाते.

सायबर गुन्ह्यांचे विविध स्वरूप

बहुतांशी सरकारी संस्था आणि देशातील पायाभूत सुविधा हे सायबर हल्ल्यांच्या विविध प्रकारांचे लक्ष्य असतात, जे राष्ट्रीय सुरक्षेच्या दृष्टीने घातक असतात. शासकीय-संचालित वेब सर्व्हर विविध सेवा प्रदान करतात जसे कि सार्वजनिकपणे माहिती वेब साईट वर उपलब्ध करून देणे आणि ग्राहक सेवा प्रदान पोर्टल उपलब्ध करून देणे. काही वेब सर्व्हर सरकारी कर्मचार्‍यांना ऑनलाइन माध्यमातून दुर्गम स्थानां तील लोकांच्या रोजगाराशी संबंधित कार्ये करण्यास सक्षम देखील करतात. वेब सर्व्हर वर एखाद्या संस्थेच्या अंतर्गत नेटवर्कचे पोर्टल आणि डेटाबेस सिस्टम असू शकते. अश्या विस्तृत पणे वापरल्या जाणाऱ्या वेब सर्व्हर सायबर हल्लेखोरांचे लक्ष्य ठरू शकतात.

सायबर हल्लेखोर ग्राहकांच्या महत्वाची उपलब्ध वैयक्तिक माहिती हॅक म्हणजेच चोरून त्याचा गैरवापर करू शकतात. सरकारी कर्मचार्यांची ओळख आणि वित्तीय तपशील ह्यांचा गैरवापर करू शकतात. हल्लेखोर वेब सर्व्हर हॅक करून वेब पोर्टल वर असणारी अधिकृत माहितीत छेडछाड करू शकतात आणि दिशाभूल करणारी किंवा चुकीची माहिती वेब पोर्टल वर होस्ट करू शकतात. अश्या हल्लेखोरांना शोधण्यासाठी आणि खटला भरण्यासाठी प्रयत्न करण्यासाठी बराच वेळ आणि पैसा खर्च होऊ शकतो. ग्राहक सेवांमध्ये किंवा कर्मचार्‍यांच्या वेब पोर्टल वर अधिकृत प्रवेशात व्यत्यय आणल्याने उत्पादकता मध्ये नुकसान सोसावे लागते म्हणून बहुतांशी हल्ले रोखणे हाच चांगला उपाय ठरतो.

प्रत्येक गुन्हेगार नेहमीच मानवी दुर्बलता आणि लोभाचा फायदा घेण्यास उत्सुक असतात आणि नि:संशय ते कायम असेच करत राहतील. ह्याला सोप्पा उपाय म्हणजे त्यांच्या ह्या युक्त्याना आधीच समजणे आणि बळी न पडणे. त्यासाठी सायबर गुन्हेगार, त्यांच्या ह्या युक्त्या आणि त्यांच्या द्वारे करण्यात येणाऱ्या विविध गुन्ह्यांचे स्वरूप घेणे आवश्यक आहे.

पालकांची नजर चुकवून अनेक विद्यार्थी सोशल मीडिया जसे कि फेसबुक (FaceBook), लिंकेड इन (Linkdeln) वर जातात. तिथे आपली आवड, निवड, शाळा सर्व तपशील भरतात. याची कल्पना अनेकदा पालकांनाही नसते. याचाच फायदा घेत सायबर गुन्हेगार या विद्यार्थ्यांना लक्ष्य करतात. विद्यार्थ्यांनी प्रोफाइल तयार केलं की त्यांचा तपशील पाहिला जातो. तो हेरून त्याला अनुसरुन मेसेज त्यांना पाठवले जातात. हे विद्यार्थी सोशल मीडियावर अनोळखी व्यक्तींशी मैत्री करतात. सायबर गुन्हेगार अनेकदा तो मुलगा ज्या वयाचा आहे, त्या वयाचाच असल्याचं भासवतो आणि मुलं त्या जाळ्यात फसतात. मग गुन्हेगार त्यांना ब्लॅकमेल करू लागतो.

सर्च इंजिनवर अनेकदा कोणतीही माहिती शोधण्यासाठी विद्यार्थी लॉगइन करतात. त्यावेळेस अनेकदा गेम्स आणि पॉर्न वेब साइटचे पर्याय या मुलांसमोर येतात. त्यावर ते स्वाभाविकपणे क्लिक करतात आणि तिथून ते शिकार ठरण्यास सुरुवात होते.

क्रेडिट कार्ड किंवा डेबिट कार्डच्या मॅग्नेटिक स्ट्रिपमध्ये कार्डधारकाचं नाव, खातं क्रमांक, कार्डची एक्स्पायरी डेट, सीव्हीव्ही कोड आणि इतर माहिती साठवून ठेवलेली असते. मॉल किंवा दुकानातील कार्ड रीडर मशिनमध्ये कार्ड स्वाइप केल्यावर ही माहिती त्या मशिनद्वारं बँकेच्या सर्व्हरपर्यंत पाठवून पडताळून पाहिली जाते. ही माहिती चोरीला गेल्यास किंवा हॅक झाल्यास अशाच प्रकारचं बनावट कार्ड तयार करता येतं.

Author:
Dr Sunita Vikrant Dhavale
Defense Institute of Advanced Technology (DIAT), Pune, India.

लेखिका:

डॉ. सुनीता विक्रांत ढवळे

साहाय्य अध्यापिका,

डिफेन्स इन्स्टिटयूट ऑफ अड्वान्सड टेकनॉलॉजि, पुणे, इंडिया.