अर्थवेध

वेध नव्या शतकाचा...



महाराष्ट्र राज्य नागरी सहकारी बँक्स परिषद २०२३-२४
NUBA
२७ व २८ जानेवारी २०२४ नाशिक

दि नाशिक जिल्हा नागरी सहकारी बँक्स् असोसिएशन लि., नाशिक

* नागरी सहकारी बँकांचे नेतृत्त्व ६९
– अविनाश जोशी
* रिझर्व्ह बँकेचे नियंत्रण, करी ठेवीदारांचे संरक्षण ७१
– गणेश निमकर
* वैकुंठभाई मेहता यांचे सहकारातील योगदान ७५
– 'डॉ. हेमा यादव (वैकुंठभाई मेहता नॅशनल इन्स्टिट्युट ऑफ को-ऑप. मॅनेजमेंट)'
* सहकारातील 'विश्वास' ७९
– कैलास येवला
* भारतीय बँकिंगमधील डिजिटल प्रवासाचा वेध ८१
– माधव प्रभुणे
* सहकार बँकिंग सद्यस्थिती व भविष्यातील वाटचाल ८५
– सीए महेश धर्माधिकारी
* अडचणीतील बँकांच्या पुर्नजीवनाकरीता उपाययोजना ९१
– ॲड. महेश काबरा
* 'उमगुनी नव्या पाऊलखुणा (विलीनीकरण-एक नवीन वाट)' ९३
– मिलिंद काळे
* अस्तित्व टिकविण्यासाठी आपण हे करूया ९९
– विश्वास नित्सुरे
* सायबर फ्रॉड आणि सहकारी बँका १०३
– मिलिंद थोरात
* नागरी सहकारी बँकांचे संविधानिक लेखापरीक्षण १०७
– प्रकाश केशव वीरकर
* १) लोक अदालत संकल्पना' १११
२) थकीत एनपीए कर्जासाठी रिझर्व्ह बँकेचे तडजोड व बुडीत धोरण आणि कर्जदारांना मिळणाऱ्या सवलती ११५
– श्रीकांत एकनाथराव जाधव
* मानू कोणत्या रकमा खऱ्या (ऑडिटच्या व इन्स्पेक्शनच्या?) १२१
– सीए उदय कर्वे
* सहकारी बँकिंग व्यवस्थापन १२५
– वंदना धर्माधिकारी
* पद्मश्री डॉ. विठ्ठलराव विखे पाटील यांचे सहकारातील योगदान १२९
– डॉ. राजेंद्र लक्ष्मण सलालकर
* सायबर सुरक्षा संकटासाठी टायटॅनिक धडे १३५
– निलम वानखेडे
* केंद्रीय सहकार मंत्रालयाचा झंझावात १३७
– विद्याधर अनास्कर



सायबर सुरक्षा संकटासाठी

टायटॅनिक धडे

निलय वानखेडे

टायटॅनिकची दुःखद घटना आपल्याला सायबर सुरक्षा धोक्यांची पूर्वकल्पना देते. बुडलेले टायटॅनिक कॅनडाच्या न्यूफाउंडलँडच्या किनाऱ्यापासून काहीसे मैलांवर सापडले. जगभरात, सध्याच्या सायबर सुरक्षा धोक्यांची तुलना टायटॅनिकच्या दुःखद नशिबाशी करण्याचा प्रयत्न केला जात आहे. आज सायबर सुरक्षा दृष्टीकोनातून, सहकारी बँकांच्या मॅनेजमेंटने टायटॅनिक दुर्दैवी घटनेपासून धडा घेणे आवश्यक आहे.

वैयक्तिक गर्व आणि तंत्रज्ञानाबद्दल अहंकार :-

उत्तर अटलांटिकच्या भयंकर वादळांचा सामना करण्यासाठी टायटॅनिकची बांधणी त्या काळातील अत्याधुनिक तंत्रज्ञानाने करण्यात आली होती. त्या वेळी, हार्लंड अँड वुल्फ या जहाजबांधणी कंपनीने या जहाजाचे न बुडता येण्याजोगे म्हणून समज केला होता. या कंपनीला भ्रम होता की त्यांच्याकडे अत्याधुनिक आणि सर्वोत्तम तंत्रज्ञानावर आधारित प्रगत इंजीन आहे आणि कोणत्याही संकटाचा सामना करण्यास सक्षम आहे. अनसिंकेबल टायटॅनिकचा कंपनीचा दावा म्हणजे पोकळ बोलण्याशिवाय काहीच नव्हते, कारण, घर कितीही सुरक्षित असले तरी चोराला मार्ग सापडतो. मजबूत सुरक्षेसाठी सार्वजनिक जागरूकता, कार्यपद्धतींचे काटेकोर पालन आणि प्रगत तंत्रज्ञानाचा अवलंब आणि सर्वांत महत्त्वाचे म्हणजे संवेदनशीलता आणि काळजी घेण्याची वृत्ती आवश्यक आहे. त्यामुळे पूर्णपणे पारंपरिक तंत्रज्ञानाचे समर्थन करत राहणे म्हणजे सायबर सुरक्षा हिमखंडांच्या महासागराला बळी पडणे. एडवर्ड जे. स्मिथ, कॅप्टन, सर्व धोके दुर्लक्षित करून, कदाचित गर्विष्ठपणा आणि अभिमानामुळे, टायटॅनिक पूर्ण वेगाने पुढे नेत होता. टायटॅनिक बुडण्यातही त्याच्या या वृत्तीचासुद्धा मोठा वाटा होता.

संघटनात्मक समन्वयाची गरज :-

टायटॅनिकच्या दुर्घटनेबाबत अनेक वेळा चौकशी झाली आणि त्या तपासाअंती एक निष्कर्ष असा निघाला की टायटॅनिकचे चालक दल (क्रू मेंबर्स) अनुभवी नव्हते आणि त्यांचे विविध गट (किंवा विभाग) एकत्रपणेसुद्धा काम करत नव्हते. समन्वयाचा अभाव एवढ्या मोठ्या आपत्तीला कारणीभूत ठरते. त्याचप्रमाणे, मजबूत सायबर सुरक्षा ही सुरक्षा व्यावसायिक, व्यवसाय व्यवस्थापन आणि विविध आयटी (IT) गट यांच्यातील समन्वय आणि सहयोग प्रयत्नांवर अवलंबून असते, उदाहरणार्थ, आयटी आणि नेटवर्क ऑपरेशन्स, ॲप्लिकेशन टीम, डेटा सेंटर इन्फ्रास्ट्रक्चर इत्यादी. कारण, सहयोग आणि सहकार्य यांचा अभावदेखील घातक परिणामांना कारणीभूत ठरू शकतात.

बिझनेस उद्दिष्टे आणि रिस्क मॅनेजमेंट यातील समतोलपणा :-

थॉमस अँड्र्यूज नावाच्या व्यक्तीकडे टायटॅनिकच्या संपूर्ण डिझाइन आणि बांधकामाची जबाबदारी सोपवण्यात आलेली होती. कोणत्याही आपत्कालीन परिस्थितीत जहाजावरील २४५३ प्रवासी आणि ८७४ चालक दल, असे एकूण ३३२७ प्रवासी वर्गांच्या वाहतुकीची हमी देण्यासाठी अँड्र्यूजला ६४ होड्या (लाईफबोट्स) हव्या होत्या. परंतु हार्लंड अँड वुल्फच्या मॅनेजमेंटला प्रोमेनेड डेक (ओपन-एअर अप्पर डेक) वरील किमती जागा वाया घालवायची नव्हती. त्यामुळे केवळ कायदेशीररित्या मान्य (स्वीकार्ह) असलेले केवळ १६ होड्या (लाईफबोट्स) आणि ४ मालवाहू बोटी (टेंडर बोट्स) देण्यात आले. ज्याची केवळ ११७८ प्रवासी वाहून नेण्याची क्षमता होती. या दुर्घटनेत फक्त ७०६ प्रवासी वाचले हा उर्वरित इतिहास आहे. त्याचप्रमाणे, बँक मॅनेजमेंट अनेकदा सायबर सुरक्षा धोक्यांचा विचार न करता बिझनेसला प्राधान्य देऊन पुढे जात असते. पर्यायाने, पुरेसे चांगले आहेत असे मानून सुरक्षेशी तडजोड करून मॅनेजमेंट सायबर सुरक्षेतील गुंतवणूक कमी करतात. इथे कोणता धडा शिकता येईल, तर मॅनेजमेंटने रिस्क फॅक्टर समजून न घेता आंधळेपणाने कोणताही निर्णय घेऊ नये आणि परिस्थितीला गृहीत धरू नये. अन्यथा, तुमची बँकसुद्धा अशाच एखाद्या हिमनगावर आदळू शकते तुमच्या कल्पनेपेक्षा खूप मोठे असेल.

टायटॅनिकवरील गहाळ दुर्बिणी – सायबर सुरक्षाबाबत उदासीनता :-

टायटॅनिकच्या दुःखद बुडण्यामागे अनेक घटक कारणीभूत

आहेत, त्यापैकी एक 'कावळ्याच्या घरट्यात दुर्बिणीचा अभाव' होता. डेव्हिड ब्लेअर प्रामुख्याने दुर्बिणीसाठी जबाबदार होते, परंतु टायटॅनिकच्या प्रवासापूर्वी शेवटच्या क्षणी त्यांना क्रू टीममधून वगळण्यात आले. अर्थात, वेळेत हिमखंड शोधण्याच्या लुकआउट (निरीक्षण) टीमची क्षमता दुर्बिणीअभावी प्रभावित झाली. त्याचप्रमाणे, सायबर सुरक्षेच्या जगातही, बँकेकडे त्यांच्या नेटवर्क ट्रॅफिकमध्ये सखोलपणे पाहण्याची अपुरी क्षमता असेल तर समुद्राच्या फसव्या पाण्यावर बेफिकीरपणे वाटचाल करण्यासारखे आहे, अयोग्य मार्गाने जाण्यासारखे आहे, त्यामुळे अनपेक्षित धोके निर्माण होतात. मी टायटॅनिकची हरवलेली दुर्बीण आणि आधुनिक सायबर सुरक्षेसाठी नेटवर्क ट्रॅफिक इंजिनीअरिंगच्या विश्लेषणाच्या आवश्यक गरजांमधील गांभीर्य यातील साधर्म्य शोधण्याचा प्रयत्न करतो.

प्राणघातक दुर्लक्षपणा टायटॅनिकची गहाळ दुर्बीण :-

त्या भयंकर रात्री, पाळत ठेवणाऱ्या टीमकडे दुर्बीण नव्हती, ज्यामुळे हिमनग शोधण्यात मदत झाली असती. या गंभीर नजरचुकीमुळे टायटॅनिकच्या हिमनगावर आदळण्यामध्ये काही प्रमाणात हातभार लागला.

समुद्राच्या अंधारात भ्रम - सायबर सिक्युरिटीमध्ये ट्रॅफिक ॲनालिटिक्स :-

समुद्रावर क्षितिजापलीकडे प्रभावीपणे नजर ठेवण्यासाठी पाळत ठेवणाऱ्या टीमला टायटॅनिकवर दुर्बिणीची गरज होती त्याप्रमाणे, नेटवर्क ट्रॅफिकच्या वर्तणुकीवर लक्ष ठेवण्यासाठी सायबर सुरक्षेला प्रगत विश्लेषणाची आवश्यक आहे. डिजिटल क्षेत्रात असे म्हणतात खूप उशीर होईपर्यंत धमक्यांकडे दुर्लक्ष करणे हे सर्व खूप सोपे आहे.

अपुरे दृश्यमानतेचे परिणाम - सायबर सुरक्षिततेचे अंधत्व :-

जेव्हा बँकेकडे मजबूत ट्रॅफिक विश्लेषण नसते, तेव्हा ती सायबर महासागरात मुळात आंधळी असते. नेटवर्कमध्ये धमक्या लपून राहू शकतात आणि त्याकडे दुर्लक्ष होऊ शकते, ज्यामुळे संवेदनशील डेटा, ऑपरेशन्स आणि प्रतिष्ठा धोक्यात येते.

धोका शोधणे आणि प्रतिसादात ट्रॅफिक विश्लेषणाची भूमिका :-

ट्रॅफिक विश्लेषणे नेटवर्क कार्यांचे एक विस्तृत दृष्टीकोन प्रदान करते, रिअल-टाइम धोका शोधणे आणि जलद प्रतिसाद देणे सक्षम करते. ही डिजिटल युगातील दुर्बिणीच्या समान सायबर सुरक्षा आहे.

स्पष्ट दृष्टीसह सायबर सुरक्षा धोरण तयार करणे :-

ज्याप्रमाणे टायटॅनिकच्या पाळत ठेवणाऱ्या टीमला दुर्बिणीचा फायदा होऊ शकतो, त्याचप्रमाणे बँकांनी धोके ओळखण्यासाठी आणि प्रभावीपणे प्रतिसाद देण्यासाठी प्रगत ट्रॅफिक विश्लेषणामध्ये गुंतवणूक केली पाहिजे. हे केवळ हिमनग शोधण्यापुरतेच मर्यादित नाही तर, संभावित आपत्ती टाळण्यासाठीसुद्धा आहे.

निष्कर्ष :-

टायटॅनिकची हरवलेली दुर्बीण, अपुरी तयारी आणि धोक्याचा शोध घेण्याच्या साधनांबद्दल आत्मसंतुष्टता धोक्याची एक धक्कादायक आठवण म्हणून काम करते. सायबर सुरक्षेच्या जगात, धडे स्पष्ट आहेत, नेटवर्क ट्रॅफिकच्या आकार आणि विश्लेषणाशिवाय, बँका अप्रत्यक्षपणे धोक्यांपासून सुरक्षित नसलेल्या आंधळेपणाने समुद्राच्या फसव्या पाण्यावर आर्थिक व्यवहार करत आहे. सतत विकसित होत असलेल्या सायबर सुरक्षा आव्हानांना बँकिंग क्षेत्र तोंड देत असल्याने, टायटॅनिक कथेने आम्हाला प्रगत नेटवर्क ट्रॅफिक शेपिंग आणि ॲनालिटिक्स, दुर्बिणीच्या बरोबरीने बँकिंग संरक्षण सुसज्ज करण्यावर लक्ष केंद्रित करण्यास प्रेरित केले पाहिजे. सायबर सुरक्षेच्या जटिल नेटवर्क लँडस्केपमध्ये बँकांना मार्गदर्शक दीपगृह असणे आवश्यक आहे, जे जहाज अंधारात जाणार नाही याची खात्री करते. बँकेने नेटवर्क मॉनिटरिंग आणि विश्लेषण यांच्या क्षमतांवर गुंतवणूक केली पाहिजे आणि डिजिटल महासागरात सुरक्षितपणे नेव्हिगेट करण्यासाठी सुसज्ज असल्याचे सुनिश्चित केले पाहिजे.

