दि महाराष्ट्र अर्बन को-ऑपरेटिव्ह बँक्स् फेडरेशन लि., मुंबई

भारतीय क्रीडा मंदिर, ४था मजला, वडाळा, पी. बी. नं. ७१२०, मुंबई - ४०० ०३१.



नागरी बँक वार्तापत्र एप्रिल ते जून, २०२६

केंद्र सरकार, रिझर्व्ह बँक ऑफ इंडिया, राज्य सरकार यांचेकडे राज्यातील नागरी सहकारी बँकांचे प्रश्न उपस्थित करुन त्यांना न्याय मिळवून देण्यासाठी बांधिल असलेली राज्यस्तरीय संघीय संस्था

दि महाराष्ट्र अर्बन को-ऑप. बँक्स् फेडरेशन लि., मुंबई

नागरी बँक वार्तापत्र, एप्रिल ते जून २०२६

अनुक्रमणिका

अ.क्र.	लेखाचे शीर्षक	लेखक	पान क्र.
१.	RBI चे विलीनीकरण धोरण: बँकांचे विलीनीकरण नव्हे, तर बँका सक्षम करण्याचा संदेश	संपादक - सी. ए. अजय ब्रम्हेचा, अध्यक्ष, दि महाराष्ट्र अर्बन को-ऑप. बँक्स् फेडरेशन लि.	०३-०४
२.	डिजिटल व्यवहार - गोपनीयतेचा नवा रखवालदार	मा.श्री.गणेश निमकर - बँकिंग तज्ञ	०७-०९
३.	उच्च भांडवल – जोखीम-भारित मालमत्ता गुणोत्तर (CRAR/ CAR) चांगले की वाईट?	श्री. माधव प्रभूणे - बँकिंग तज्ञ	१०-११
४.	सहकारी बँक संचालक मंडळासाठी सखोल तांत्रिक दस्तऐवज रिझर्व्ह बँक सायबर सुरक्षा फ्रेमवर्क व डीपीडीपी कायदा, २०२३ - समस्या, परिणाम व उपाययोजना	श्री. निलय वानखडे - बँकिंग तज्ञ	१३-१८
५.	महिलांची संपत्ती : भारतातील सर्वात मोठी, पण अजूनही न वापरलेली आर्थिक संधी	श्रीमती प्रीती राठी गुप्ता - संस्थापक, LXME	२०-२२
६.	नागरी सहकारी बँकांची वाटचाल अनुपालन संस्कृती (Compliance Culture) च्या दिशेने व्हावी	श्री. उदय पेंडसे - संचालक, सहकार भारती प्रशिक्षण सहकारी संस्था, पुणे	२३
७.	माहे एप्रिल ते माहे जून २०२६ मधील रिझर्व्ह बँक ऑफ इंडियाचे परिपत्रके		२४-५५

डिस्क्लेमर:

या वार्तापत्रात प्रकाशित करण्यात आलेले लेख, मते व विचार हे संबंधित लेखकांचे वैयक्तिक मत असून, त्यांचा दि महाराष्ट्र अर्बन को-ऑप. बँक्स् फेडरेशन लि., मुंबई अथवा फेडरेशनच्या व्यवस्थापनाशी थेट किंवा अप्रत्यक्ष संबंध आहे असे समजू नये. या लेखांमधून व्यक्त केलेली मते ही फेडरेशनची अधिकृत भूमिका दर्शवत नाहीत, याची कृपया नोंद घ्यावी.

******

सहकारी बँक संचालक मंडळासाठी सखोल तांत्रिक दस्तऐवज रिझर्व्ह बँक सायबर सुरक्षा फ्रेमवर्क व डीपीडीपी कायदा, २०२३ - समस्या, परिणाम व उपाययोजना



श्री. निलय वानखडे
बँकिंग तज्ञ

प्रास्ताविक - एक थेट प्रश्न

पुढील संचालक मंडळ बैठकीत आपल्या – CISO ला एकच प्रश्न विचारा - ''उद्या एखाद्या शाखेतील संगणकातून ग्राहकांचा डेटा बाहेर गेल्यास, तो नेमका कुठून कुठे गेला, हे आपण ७२ तासांत अभियांत्रिकी पुराव्यांच्या आधारे सिद्ध करून शकतो का?'' जर उत्तर - ''होय, आपल्याकडे संचालक मंडळाने मंजूर केलेले सायबर सुरक्षा धोरण आहे'' - असे आले, तर समस्या अपेक्षेपेक्षा खूप मोठी आहे. कारण डिजिटल वैयक्तिक डेटा संरक्षण कायदा, २०२३ (डीपीडीपी ॲक्ट) धोरणांची मागणी करत नाही - तो अभियांत्रिकी पुराव्याची (Engineering Evidence) मागणी करतो. हा फरक सूक्ष्म वाटला तरी त्याचे आर्थिक व कायदेशीर परिणाम मोठे आहेत, आणि म्हणूनच हा दस्तऐवज संचालक मंडळासाठी विशेषत: तयार केला आहे.

१. समस्या काय आहे?

सहकारी बँकिंग क्षेत्रासमोरील मूलभूत समस्या तांत्रिक उपकरणांच्या अभावाची नसून, तांत्रिक मालकीच्या मूलभूत अनुपस्थितीची आहे. बहुतांश नागरी सहकारी बँका व जिल्हा मध्यवर्ती बँकांचे शाखा-नेटवर्क अद्यापही फ्लॅट लेअर-२ ब्रॉडकास्ट डोमेन स्वरूपात रचले गेले आहे. जिथे सीबीएस, थिन क्लायंट, एटीएम बॅकहॉल उपकरणे, सीसीटीव्ही रेकॉर्डर, प्रिंटर, स्कॅनर, व्हेंडर लॅपटॉप, गेस्ट वायफाय वापरकर्ते आणि सर्वात धोकादायक म्हणजे नेटवर्क उपकरणांचे मॅनेजमेंट इंटरफेस हे सर्व एकाच ब्रॉडकास्ट डोमेनमध्ये सहअस्तित्त्वात असतात. परिणामी, एका टोकाची तडजोड म्हणजे संपूर्ण नेटवर्कची तडजोड.

अशा रचनेत मायक्रो-सेगमेंटेशन, ईस्ट-वेस्ट ट्रॅफिक एनफोर्समेंट, आयडेंटिटी-अवेअर पॉलिसी व इम्युटेबल ऑडिट लॉगिंग हे आधुनिक सायबर सुरक्षेचे चार मूलभूत आधारस्तंभ पूर्णपणे अनुपस्थित आहेत. हल्लेखोर एका असुरक्षित परिघीय बिंदूतून प्रवेश करून (उदा. व्हेंडरचा संक्रमित लॅपटॉप, अद्ययावत न केलेले वर्कस्टेशन किंवा असुरक्षित सीसीटीव्ही रेकॉर्डर) सीबीएस डेटाबेसपर्यंत पोहोचण्यासाठी आवश्यक मार्गावर कोणताही महत्त्वाचा आर्किटेक्चरल अडथळा अस्तित्त्वात नाही. संपूर्ण रचना एका अबोल गृहीतकावर उभी आहे ''धोके बाहेरून येतात, आत सुरक्षित आहे.'' २०२६ मध्ये हे गृहीतक संपूर्णत: कालबाह्य आहे.

समस्येचे मूळ - तीन स्तरीय अपयशाची साखळी

अ) नियामक स्तर: रिझर्व्ह बँकेच्या सीएसएफ आराखड्याने जाणीवपूर्वक ''नियामक प्रमाणबद्धता'' तत्त्व स्वीकारले — म्हणजे प्रशासकीय अपेक्षा निर्धारित केल्या, परंतू शाखेतील नेटवर्क प्रत्यक्षात कसे बांधले जावे, याचे तांत्रिक तपशील बँक व त्यांच्या तंत्रज्ञान भागीदारांच्या निर्णयावर सोपवले. सिद्धांतत: हा दृष्टीकोन योग्य आहे – मोठ्या व्यावसायिक बँकांकडे स्वत:च्या नेटवर्क आर्किटेक्ट टीम्स आहेत. परंतू सहकारी बँकिंगचे वास्तव वेगळे आहे.

ब) सिस्टिम इंटिग्रेटर स्तर:

नाबार्ड समर्थित एएसपी व्यवस्थेअंतर्गत डेटा सेंटर ऑपरेशन्स, डिझाइन, आयपी ॲड्रेस योजना व शाखेतील लॅन रचना हे सर्व सिस्टिम इंटिग्रेटर्सकडे (विप्रो, टीसीएस, इ.) सोपावण्यात आले. बँकेकडे केवळ शाखेतील हार्डवेअर व खुर्च्यांची मालकी राहिली. इंटिग्रेटर्सनी सर्वात स्वस्त, सोपा व कमी देखभाल खर्चिक 'फ्लॅट डिझाइन' स्वीकारला. कारण व्यावसायिकदृष्ट्या तो त्यांच्यासाठी सर्वाधिक फायदेशीर होता.

क) बँक स्तर:

हे तांत्रिक रचनात्मक प्रश्न विचारण्यासाठी आवश्यक असलेली अभियांत्रिकी क्षमता संचालक मंडळ व बँक व्यवस्थापनाकडे नव्हती आणि सीएसएफ ने ती क्षमता विकसित करण्याची गरजही अधोरेखित केली नाही. परिणामी, बँकेकडे सुंदर प्रशासकीय धोरणे आहेत, परंतू नेटवर्कची अभियांत्रिकी मालकी नाही. आणि डीपीडीपी च्या युगात ही दरी निर्णायक ठरते.

२. परिणाम काय?

डीपीडीपी कायदा हा रिझर्व्ह बँकेच्या सीएसएफ पेक्षा संरचनात्मकदृष्ट्या मूलत: वेगळा आहे. कारण तो धोरणात्मक दस्तऐवजीकरणाची नव्हे, तर अभियांत्रिकी पुराव्याची मागणी करतो. डिसेंबर, २०२५ मध्ये अधिसूचित नियमांची अंमलबजावणी टप्प्याटप्प्याने सुरू झाली असून,

सहकारी बँकिंगसाठी पूर्ण अनुपालनाची अपेक्षित मुदत २०२७ आहे. म्हणजे हाताशी फक्त दीडच वर्ष उरले आहे. परिणाम चार पातळ्यांवर एकाच वेळी उद्भवतात:

अ) कायदेशीर परिणाम - डेटा फिड्युशियरी म्हणून संपूर्ण उत्तरदायित्त्व बँकेवरच राहते, ही जबाबदारी कोणत्याही करारामार्फत सिस्टिम इंटिग्रेटर, एमएसपी किंवा व्हेंडरकडे हस्तांतरित करता येत नाही. कलम ३३(२) अंतर्गत, निष्काळजीपणामुळे झालेल्या उल्लंघनासाठी रु. २५० कोटींपर्यंत दंड आकारला जाऊ शकतो. दंडाची नेमकी रक्कम मनमानीपणे ठरत नाही. डेटा संरक्षण मंडळ खालील निकषांच्या महत्त्व आधारित मूल्यांकनाद्वारे ती निश्चित करते. उल्लंघनाचे स्वरूप व गांभीर्य, प्रभावित डेटा प्रिन्सिपल्सची संख्या, नुकसानीची व्याप्ती, उल्लंघन हेतू पुरस्सर होते की निष्काळजीपणामुळे, बँकेने यापूर्वी उचललेली प्रतिबंधात्मक पावले आणि उल्लंघन निदर्शनास आल्यानंतरचा प्रतिसाद.

ब) आर्थिक परिणाम - ५ ते १० लाख खातेदार असलेल्या मध्यम आकाराच्या नागरी सहकारी बँकांसाठी, गंभीर उल्लंघनापोटी रु. ५० ते १०० कोटींच्या दरम्यान दंड हा वाजवी मध्यम-श्रेणीतील अनुमान आहे. यात मात्र कायदेशीर सल्लागार खर्च, स्वतंत्र फॉरेन्सिक तपास, प्रभावित डेटा प्रिन्सिपल्सना द्यावी लागणारी नुकसारभरपाई, पर्यवेक्षकीय देखरेखीखाली राबवायच्या सुधारणा-योजनांचा खर्च आणि सर्वात विनाशकारी – ठेवीदारांच्या विश्वासातील घट व ठेवींचा बहिर्प्रवाह हे अंतर्भूत नाहीत. लहान व मध्यम सहकारी बँकांसाठी हा केवळ नियामक अनुपालनाचा प्रश्न नसून, त्यांच्या स्वत:च्या अस्तित्त्वाचाच प्रश्न आहे.

क) परिचालनात्मक परिणाम

फ्लॅट नेटवर्कवर डीपीडीपी च्या चार ठोस आवश्यकता पूर्ण करणे तांत्रिकदृष्ट्या व विश्वसनीयपणे अशक्य ठरते.

१) ७२ तास उल्लंघन सूचना (Breach Notification) : ईस्ट-वेस्ट दृश्मानताच (Visibility) नसल्याने ७२ दिवसांतही उत्तरे मिळणे कठीण.

२) हटवण्याचा अधिकार (Right to Erasure) : डेटाच्या प्रत्येक प्रतीचे नेमके स्थान बॅकअप, रेप्लिकेशन साईट्स, तृतीय पक्ष भांडारे - अज्ञात

३) उद्देशनिहाय वापर (Purpose Limitation) : डेटा मूळ संमतीच्या उद्देशापुरताच मर्यादित आहे हे तांत्रिक पुराव्यासह सिद्ध करण्याची क्षमता नाही.

४) कलम ६ अंतर्गत 'वाजवी सुरक्षा उपाययोजना' : केवळ उपाय अस्तित्त्वात आहेत, असे म्हणणे पुरेसे नाही. ते प्रत्यक्षात कार्यरत आहेत हे फॉरेन्सिक दर्जाच्या पुराव्यासह सिद्ध करता आले पाहिजे.

ड) वैयक्तिक उत्तरदायित्त्व: हा बहुधा सर्वात दुर्लक्षित परंतू सर्वाधिक धोकादायक परिणाम आहे. संचालक मंडळाच्या सदस्यांवर वैयक्तिक स्तरावरही कायदेशीर जबाबदारी येऊ शकते. उल्लंघनानंतर डेटा संरक्षण मंडळासमोर हजर राहताना, 'मला तांत्रिक तपशील माहित नव्हते' किंवा 'ती जबाबदारी सिस्टिम इंटिग्रेटरची होती', ही उत्तरे कायद्याच्या दृष्टीने अपूरी ठरतात, कारण डीपीडीपी कायद्यानुसार ती जबाबदारी मूलत: व पूर्णत: डेटा फिड्युशियरीकडे म्हणजे बँकेकडे असते.

३) उपाय काय?

उपाय कोणत्याही अत्याधुनिक उत्पादनात किंवा क्रांतिकारी तंत्रज्ञानात नाही, तर अभियांत्रिकी शिस्तीच्या पुनर्स्थापनेत आहे. आवश्यक तंत्रज्ञान दशकभरापासून परिपक्व व व्यापारीदृष्ट्या उपलब्ध आहे, खरी कमतरता तंत्रज्ञानाची नसून संस्थात्मक इच्छाशक्तीची व तांत्रिक मालकीच्या पून:प्रस्थापनेची आहे.

मध्यम आकाराच्या नागरी सहकारी बँकांसाठी (२०-५० शाखा, अंदाजे रु. १००० कोटी ठेवी) - एक वेळ भांडवली खर्च सुमारे रु. ३ ते ८ कोटी आणि वार्षिक परिचालन खर्च रु. १ ते २ कोटी - हा संभाव्य रु. ५० ते १०० कोटी दंडाच्या तुलनेत अंदाजे दहापट कमी आहे. आर्थिक दृष्टीने हा अतिरिक्त भार नसून, बँकेच्या स्वत:च्या अस्तित्त्व संरक्षणासाठीचा विमा हप्ता आहे आणि तो न भरण्याची खरी किंमत, मूळ धोका प्रत्यक्षात येतो त्या क्षणी, अत्यंत वेदनादायकपणे स्पष्ट होते. (टीप: हे आकडे ढोबळ आहेत, प्रत्यक्ष खर्च बँकेचा आकार, विद्यमान पायाभूत सुविधांची स्थिती व निवडलेल्या आर्किटेक्चरवर अवलंबून असेल - स्वतंत्र तांत्रिक मूल्यांकन अत्यावश्यक)

४. एक प्रांजळ टीप - व्हच्युअल सीआयएसओ व गॅप ॲनॅलिस्ट विषयी

गेल्या काही महिन्यांत बाजारात या सेवा देणाऱ्या अनेक संस्था पुढे आल्या आहे, यापैकी अनेकजण नि:संशय सद्हेतून काम करत आहेत आणि त्यांच्या योगदानाचे महत्त्व कोणत्याही प्रकारे कमी लेखता येणार नाही. ओळख व प्राथमिक जागरूकता निर्माण करण्याच्या कार्यात त्यांचे योगदान मोलाचे आहे. तथापि, संचालक मंडळाने एक मूलभूत बाब अत्यंत शांतपणे व व्यावहारिकदृष्ट्या लक्षात घ्यावी.

डीपीडीपी कायद्याचे अनुपालन हे गॅप ओळखणे या टप्प्याटप्प्यापुरते मर्यादित नाही ते गॅप अभियांत्रिकी पद्धतीने भरून काढण्यापर्यंत पोहोचणे आवश्यक आहे.

चेकलिस्ट-आधारित अहवाल, स्कोअरकार्डस, मॅच्युरिटी असेसमेंट,

रिस्क हीटमॅप किंवा रंगबिंदू-दर्शक मॅट्रिक्स - ही सर्व साधने आहेत. ती परिस्थितीचे चित्र मांडण्यास उपयुक्त असली, तरी ती फॉरेन्सिक दर्जाचा पुरावा निर्माण करत नाहीत. डेटा संरक्षण मंडळासमोर हजर असताना 'आमचा मॅच्युरिटी स्कोअर ३.८ होता' किंवा 'आमच्या रिस्क हीटमॅपवर हा भाग पिवळा होता' ही विधाने कायदेशीर बचावाला निरुपयोगी ठरतात. मंडळ विचारते: 'व्हीएलएएन विभाजन कधी झाले? कोणी केले? लॉग्स कुठे आहेत? साक्षांकित डायग्राम सादर करा.'

कधीकधी, अनावधानाने का होईना, परिस्थिती गरजेपेक्षा अधिक भयानक स्वरूपात मांडली जाते - आकडे मोठे, इशारे तीव्र आणि कालमर्यादा कठोर सादर करून ज्यातून बँक व्यवस्थापन अनावश्यक भीतीचे वातावरण निर्माण होते. भीतीतून घेतलेले निर्णय हे क्वचितच चांगले अभियांत्रिकी निर्णय असतात, उलट, ते बहुधा घाईघाईत केलेल्या, अति खर्चिक व अपूर्ण उपाययोजनांकडेच नेतात.

म्हणूनच आमची नम्र विनंती ही, सल्लागार ओळख निर्माण करतात, अभियंते उपाय बांधतात. दोघांचेही स्थान वेगळे आहे. दोघांचेही महत्त्व आहे. परंतू त्यांची भूमिका अदलाबदल करता येत नाही. ज्या व्यक्तीने केवळ रिपोर्टस लिहिले आहेत, परंतू प्रत्यक्षात कधीही VLAN उभा केलेला नाही, बीजीपी कॉन्फिगर केलेला नाही किंवा फायरवॉल पॉलिसी ट्रबलशूट केलेली नाही. तिच्याकडून अभियांत्रिकी निर्णयांची अपेक्षा अवास्तव आहे.

संचालक मंडळाने आपल्या तांत्रिक भागीदाराची निवड करताना, त्यांनी काय शोधले यापेक्षा त्यांनी काय बांधले व ते किती दिवस टिकले हा निकष अधिक विश्वासार्ह ठरतो. शोधणारे बरेच आहेत. बांधणारे व त्यापुढे टिकवून ठेवणारे, हे फार कमी आहेत आणि डीपीडीपी च्या युगात ज्यांनी टिकवून ठेवले आहे, त्यांचाच पुरावा कायदेशीर दृष्टीने टिकेल.

५) उपायाची दिशा - सखोल तांत्रिक विश्लेषण

उपायांची दिशा सात परस्परावलंबी स्तंभांवर एकत्रितपणे काम करते. हे स्तंभ एकमेकांवर अवलंबून आहेत. एखादा वगळला तर इतरांची परिणामकारकता लक्षणीयरित्या कमी होते. उदा., उत्तम सेगमेंटेशन असूनही जर ऑडिट लॉगिंग नसेल, तर उल्लंघनाचा पुरावा सादर करता येणार नाही आणि उत्तम लॉगिंग असूनही जर मॅनेजमेंट प्लेन विलग नसेल, तर तेच लॉग्स हल्लेखोराकडून बदलले जाऊ शकतात.

५.१) नेटवर्क सेगमेंटेशन - मॅक्रो व मायक्रो दोन्ही पातळ्यांवर मॅक्रो-सेगमेंटेशन हे लेअर-३ स्तरावर VRF (Virtual Routing and Forwarding) तंत्रज्ञानाच्या आधारे केले जाते. प्रत्येक कार्यात्मक डोमेन - सीबीएस, एटीएम, सीसीटीव्ही, व्हेंडर ॲक्सेस, कॉर्पोरेट लॅन, गेस्ट वायफाय आणि मॅनेजमेंट प्लेन - स्वतंत्र व्हीआरएफ मध्ये असावा. प्रत्येक व्हीआरएफ हा स्वत:चा स्वतंत्र रूटिंग टेबल राखतो. व्हीआरएफ दरम्यान कोणताही ट्रॅफिक केवळ नियंत्रित इंटर-व्हीआरएफ लिकिंग पॉइंट्स वरूनच जायला हवा आणि तो प्रत्येक पॅकेट DPI सक्षम Next Generation Firewall मधून तपासणीसाठी जायला हवा. यामुळे एका डोमेनमधील उल्लंघन दुसऱ्या डोमेनमध्ये पसरवण्याची शक्यता मूलत:च रोखली जाते.

मायक्रो सेगमेंटेशन हे लेअर-४ व लेअर-७ पातळीवर काम करते. व्हीआरएफ च्या आत. इथे प्रत्येक वर्कलोड-टू-वर्कलोड संवाद ओळख-आधारित धोरणाने नियंत्रित होतो. स्त्रोत आयपी नव्हे तर स्त्रोत ओळख हा प्रमुख निकष ठरतो. उदा., सीबीएस ॲप्लिकेशन सर्व्हरला डेटाबेस सर्व्हरशी जोडण्यासाठी विशिष्ट सेवा-खाते, विशिष्ट टीसीपी पोर्ट व विशिष्ट प्रोटोकॉल यांचेच अधिकृत संयोजन वापरता येते. इतर कोणताही प्रयत्न तात्काळ नाकारला जाऊन SIEM मध्ये ॲलट म्हणून नोंदला जातो.

५.२) डेटा प्लेन व मॅनेजमेंट प्लेन यांचे संपूर्ण विलगीकरण

नेटवर्किंगमध्ये तीन लॉजिकल प्लेन अस्तित्त्वात असतात. डेटा प्लेन (ग्राहक व अनुप्रयोग ट्रॅफिक), कंट्रोल प्लेन (राउटिंग प्रोटोकॉल्स —OSPF, BGP, EIGRP) आणि मॅनेजमेंट प्लेन (SSH,SNMP, NETCONF/YANG, iLO/iDRAC, vCenter, RADIUS/TACACS+, सिरियल कन्सोल) यापैकी मॅनेजमेंट प्लेन हा प्रत्येक नेटवर्क उपकरणावर रूट-लेव्हल नियंत्रण देतो. त्यामुळे त्याची तडजोड म्हणजे एक उपकरण नव्हे, तर संपूर्ण नेटवर्कची तडजोड. म्हणून मॅनेजमेंट प्लेन हा पूर्णत: आऊट ऑफ बँड नेटवर्कवर स्वतंत्र भोतिक तारा, स्वतंत्र स्विचेस, स्वतंत्र आयपी स्पेस चालवला जायलाच हवा. डेटा प्लेनशी कोणताही भौतिक किंवा तार्किक मार्ग असता कामा नये.

५.३) व्हेंडर ॲक्सेस – Zero Standing Privilege तत्त्वावर

व्हेंडरना उत्पादन नेटवर्कमध्ये थेट, कायम प्रवेश कधीही असता कामा नये. प्रत्येक व्हेंडर ॲक्सेस हा पीएएम (Privileged Access Management) समाधानामार्फत, जेआयटी (Just-In-Time) तत्त्वावर मर्यादित कालावधीसाठी, एमएफए पडताळणीनंतर, बॅस्टियन/जंप सर्व्हरद्वारेच मिळायला हवा. प्रत्येक सत्राची व्हिडिओ रेकॉर्डिंग, प्रत्येक कीस्ट्रोकची नोंद आणि डेटाबेसवर चालवल्या जाणाऱ्या प्रत्येक एसक्यूएल क्वेरीचे लॉगिंग ही फॉरेन्सिक तपासणीसाठी किमान अपेक्षा आहे. व्हेंडरला विश्वास द्या पण पडताळणीचा प्रत्येक थर अबाधित ठेवा. हे या स्तंभाचे मूळ

तत्त्व.

५.४) देखरेख व टेलिमेट्री - बँकेच्या स्वत:च्या नियंत्रणाखाली

सायबर सुरक्षा देखरेखीची चार आधारस्तंभे SIEM (Security Information and Event Management) सर्व लॉग्सचे केंद्रीकरण व सहसंबंध विश्लेषण), NetFlow/IPFIX (ईस्ट-वेस्ट ट्रॅफिक प्रवाहाचे मेटाडेटा संकलन), IDS/IPS (सिग्नेचर व ॲनोमलीवर आधारित घुसखोरी ओळख व प्रतिबंध), EDR/XPR (एंडपॉइंट-स्तरीय वर्तन विश्लेषण व प्रतिसाद). हे चारही घटक बँकेच्या स्वत:च्या डेटा संटरमध्ये असावेत आणि त्यांच्यावरील प्रशासकीय नियंत्रण व्हेंडरकडे नव्हे तर बँकेच्या स्वत:च्या NetOps व SecOps टीमकडे असावे. व्हेंडर डॅशबोर्ड, मासिक पीडीएफ अहवाल किंवा स्क्रीनशॉट्सवर अवलंबून राहणे. हे प्रत्यक्ष देखरेख नाही. ती केवळ एक भ्रामक आश्वासन यंत्रणा आहे.

५.५) इम्युटेबल ऑडिट लॉगिंग व साक्षांकित पुरावा - साखळी

डीपीडीपी कायद्याअंतर्गत फॉरेन्सिक दर्जाचा पुरावा तेव्हाच कायदेशीरदृष्ट्या टिकतो जेव्हा लॉग्स टॅम्पर-रेझिस्टंट स्वरूपात साठवले जातात. म्हणजे WORM (Write-Once-Read-Many) स्टोरेज वर लिखाण, प्रत्येक लॉग-एंट्रीसाठी क्रिप्टोग्राफिक हॅश चेनिंग आणि स्वतंत्र, विश्वसनीय टाईम-स्टॅंपिंग ऑथॉरिटी कडून प्रत्येक नोंदीवर वेळ-शिक्का. केवळ बँकेच्या स्वत:च्या एनटीपी सर्व्हरने काम भागत नाही. कारण तो स्वत: तडजोडीचा विषय होऊ शकतो. किमान ३६५ दिवस हॉट रिटेंशन अधिक ७ वर्षे कोल्ड रिटेंशन हा बँकिंग क्षेत्रासाठी विवेकी मानदंड आहे.

५.६) ओळख-आधारित प्रवेश व वर्तन विश्लेषण – RBAC + UEBA

RBAC हे आधुनिक प्रवेश नियंत्रणाचे मूलभूत तत्त्व आहे. प्रत्येक प्रणालीसाठी (सीबीएस, एडी, ईमेल, फाईल सर्व्हर, नेटबँकिंग बॅकएंड) लीस्ट प्रिव्हिलेज तत्त्वावर भूमिका परिभाषित करणे आणि प्रत्येक वापरकर्त्याला त्याच्या भूमिकेपुरताच प्रवेश देणे. यासह टॉक्सिक कॉंबिनेशन उदा. व्यवहार निर्मिती अधिक व्यवहार मंजुरी एकाच भूमिकेत किंवा वापरकर्ता निर्माण अधिक पासवर्ड रिसेट एकाच हातात यांची सक्रीय ओळख व त्यांचे संरचनात्मक निर्मूलन अनिवार्य. त्रैमासिक ॲक्सेस रिव्ह्यू व Privilege Creep (वेळोवेळी जमा होत जाणारे अनावश्यक अधिकार) हे सर्व अधिकृत नियुक्त अधिकाऱ्याने स्वाक्षरीने प्रमाणित केले पाहिजे.

UEBA (User and Entity Behaviour Analytics) ही RBAC ची तार्किक पुढची पायरी आहे. कारण RBAC 'काय परवानगी आहे' हे सांगते, तर युईबीए प्रत्यक्षात काय घडत आहे आणि ते सामान्य आहे का हे सांगते. युईबीए प्रत्येक कर्मचारी, सेवा-खाते व उपकरण यांच्या नेहमीच्या वर्तनाचे यांत्रिक शिक्षण आधारित बेसलाईन तयार करते. कोण, कधी, कुठून, किती डेटा कोणत्या सिस्टीममधून. त्यानंतर असामान्य वर्तन तात्काळ ॲलर्ट म्हणून ओळखले जाते.

कार्यालयीन वेळेबाहेर बल्क डाऊनलोड, अनपेक्षित भौगोलिक स्थानावरून लॉगिन, सामान्यत: न वापरल्या जाणाऱ्या प्रणालींमध्ये अचानक प्रवेश किंवा खाते-तडजोडीची सूचक वर्तन श्रृंखला

विशेष महत्त्व सेवा खात्यांच्या देखरेखीला कारण ही खाती सहसा वाढीव अधिकारांची असतात, क्वचितच बदलली जातात, क्वचितच नियमित कर्मचाऱ्यांच्या निरीक्षणात येतात आणि म्हणूनच आधुनिक उल्लंघनांमध्ये ती सर्वाधिक गैरवापरली जातात. एकट्या सेवा-खात्यांची स्वतंत्र युईबीए देखरेख हे आज एक प्रगत एसओसीचे लक्षण मानले जाते.

५.७) बँकेची तांत्रिक मालकी - हस्तांतरणीय नसलेले कर्तव्य

आर्किटेक्चरल निर्णय, सुरक्षा-धोरणांची आखणी, बदल-व्यवस्थापन मंजुरी आणि घटना प्रतिसाद यांचे अंतिम अधिकार केवळ बँकेच्या स्वत:च्या तांत्रिक नेतृत्त्वाकडेच राहायलाच हवेत. सीआयएसओ आणि सिस्टिम इंटिग्रेटर हे सल्ला देऊ शकतात, अंमलबजावणी करू शकतात, साहाय्य पुरवू शकतात. परंतु ते निर्णयांचे मालक नाहीत. लहान मध्यम नागरी सहकारी बँकांसाठी पूर्णवेळ नेटवर्क आर्किटेक्ट परवडत नसल्यास, अनेक नागरी सहकारी बँका मिळून सामायिक सेवा मॉडेल अंतर्गत एकत्रित नेटवर्क अभियांत्रिकी संसाधन उभारणे हा सहकारी क्षेत्राच्या मूळ तत्त्वांशी पूर्णत: सुसंगत व आर्थिकदृष्ट्या व्यवहार्य पर्याय आहे.

६) संचालक मंडळासाठी थेट विचारण्याचे प्रश्न

खालील प्रश्न सीआयएसओ, सीटीओ व सीआयओ यांना थेट विचारावेत, लेखी उत्तरे, अद्ययाव आर्किटेक्चरल आकृत्या व प्रत्यक्ष लॉग-नमुने यांसह मागवावेत. केवळ होय/नाही स्वरूपातील उत्तरे अस्वीकार्य मानावीत. हे प्रश्न केवळ डीपीडीपी अनुपालनासाठीच नव्हेत. ते संचालक मंडळ सदस्यांच्या वैयक्तिक कायदेशीर दायित्वाच्या रक्षणासाठीही तितकेच महत्त्वाचे आहेत.

आर्किटेक्चर व सेगमेंटेशन

१) शाखेतील व्हेंडरचा लॅपटॉप सीबीएस डेटाबेस सर्व्हरपर्यंत किमान

किती नेटवर्क हॉप्स मध्ये व कोणत्या फायरवॉल नियमांना ओलांडून पोहोचू शकतो ? अद्ययावत लॉजिकल व फिजिकल नेटवर्क डायग्राम सादर करा.

२) शाखा स्तरावर एकूण किती व्हीएलएएन आहेत ? सीबीएस, एटीएम, सीसीटीव्ही, प्रिंटर/स्कॅनर, व्हेंडर ॲक्सेस, गेस्ट वायफाय व मॅनेजमेंट प्लेन हे प्रत्येक स्वतंत्र व्हीएलएएन मध्ये आहेत का ? इंटरव्ही एलएएन रूटिंग कोणत्या फायरवॉलमधून जाते ?

३) डेटा सेंटरचे मॅनेजमेंट इंटरफेस (SSH, iLO/iDRAC, Vcenter, स्विच कन्सोल) हे शाखेतील कोणत्याही सामान्य वर्कस्टेशनवरून थेट पोहोचण्यायोग्य आहेत का ? आऊट ऑफ बँड मॅनेजमेंट नेटवर्क स्वतंत्रपणे अस्तित्त्वात आहे का ?

ओळख व प्रवेश व्यवस्थापन

(४) RBAC: सीबीएस, एडी, ईमेल, फाईल सर्व्हर - या प्रत्येक प्रणालीसाठी लीस्ट प्रिव्हिलेज तत्त्वावर भूमिका परिभाषित आहेत का ? त्रैमासिक ॲक्सेस रिव्ह्यू व प्रिव्हिलेज क्रीप तपासणी कोण स्वाक्षरीने प्रमाणित करते ? टॉक्सिक कॉंबिनेशन (उदा. व्यवहार निर्मिती अधिक मंजुरी एकाच भूमिकेत) कशा प्रकारे ओळखून निर्मूलित केल्या जातात ?

५) UEBA: ही क्षमता बँकेकडे प्रत्यक्षात कार्यान्वित आहे का ? कर्मचारी, सेवा-खाती व उपकरणे यांच्या नेहमीच्या वर्तनाचे बेसलाईन तयार आहे का ? असामान्य वर्तन कार्यालयीन वेळेबाहेर बल्क डाऊनलोड, अनपेक्षित भौगोलिक लॉगिन, सामान्यत: न वापरल्या जाणाऱ्या सिस्टीममधील प्रवेश रिअल-टाईम ॲलर्ट म्हणून ओळखले जातात का ? विशेषत: सेवा-खात्यांची देखरेख कशी होते ?

देखरेख व घटना प्रतिसाद

६) ईस्ट-वेस्ट ट्रॅफिकवर देखरेख कोणत्या तंत्रांद्वारे केली जाते NetFlow, IPFIX, SPAN/RSPAN सत्रे किंवा इन-लाईन IDS ? या डेटाचे विश्लेषण बँकेच्या स्वत:च्या SOC/NOC टीमकडून होते, की बाह्य MSSP कडून ? आणि MSSP असेल, तर त्यांच्या SLM मध्ये मीन-टाईम - टू - डिटेक्ट व मीन - टाईम - टू - रिस्पाँड यांचे काय निकष आहेत ?

७) आज रात्री उल्लंघन झाले, तर ७२ तासांत संपूर्ण ॲटॅक पाथ (किल चैन) सिद्ध करण्यासाठी कोणते लॉग्स उपलब्ध आहेत. फायरवॉल, प्रॉक्सी, DNS, DHCP, AD, CBS ॲप्लिकेशन, डेटाबेस, ईडीआर ? हे लॉग्स वर्म स्टोरेजवर आहेत का ? रिटेंशन कालवधी किती ? टाईम-सिंक्रोनायझेशनसाठी एनटीपी स्त्रोत कोणता आहे आणि तो विश्वसनीय आहे का ?

संघटनात्मक रचना

८) बँकेत CISO व मुख्य नेटवर्क आर्किटेक्ट ही दोन स्वतंत्र, औपचारिकरीत्या नियुक्त केलेली पदे आहेत का ? CISO व NetOps हे दोन स्वतंत्र कार्यात्मक विभाग आहेत का ? प्रत्येकाकडे समर्पित बजेट, स्वतंत्र अहवाल रेषा व थेट निर्णय-अधिकार आहेत का ?

डीपीडीपी-विशिष्ट क्षमता

९) डीपीडीपी कलम १२ अंतर्गत डेटा प्रिन्सिपलकडून हटवण्याची विनंती आल्यास, सर्व प्रणाली, बॅकअप, रेप्लिकेशन साईट्स व तृतीय पक्ष भांडारांवरून डेटा हटवण्यास किती दिवस लागतील ?क्रिप्टोग्राफिक इरेजर ॲटेस्टेशन किंवा डिलीशन सर्टिफिकेट स्वरूपात पुरावा देता येतो का ?

१०) उद्देशनिहाय वापर - बँक हे तांत्रिक पुराव्यासह सिद्ध करू शकते का, की संकलित डेटाचा वापर मूळ संमतीच्या उद्देशापुरताच मर्यादित आहे ? डेटा वर्गीकरण व डेटा लिनिएज ट्रॅकिंग प्रत्यक्षात कार्यान्वित आहे का ?

व्हेंडर निर्भरता व गुंतवणूक पारदर्शकता

११) सिस्टिम इंटिग्रेटरच्या आर्किटेक्चरल निर्णयांचे शेवटचे स्वतंत्र त्रयस्थ-पक्ष पुनरावलोकन केव्हा झाले ? त्यातील किती शिफारशी प्रत्यक्षात अंमलात आणल्या गेल्या ?

१२) सिस्टिम इंटिग्रेटरच्या निष्काळजीपणामुळे उल्लंघन झाल्यास करारांतर्गत आर्थिक जबाबदारी कोणाची ? (टीप: डीपीडीपी कायद्यानुसार नियामक व कायदेशीर जबाबदारी कधीही हस्तांतरित होत नाही. ती बँकेकडेच राहते. परंतू इंटिग्रेटरकडून बँकेला आर्थिक भरपाई मिळवण्याचे करार-कलम अस्तित्त्वात आहे का ?

१३) २०२० पासूनच्या सायबर सुरक्षा खर्चाचे विभाजन - अ) परिषदा, ऑडिट, प्रमाणपत्रे व अनुपालन अहवाल विरुद्ध ब) प्रत्यक्ष नेटवर्क पुनर्रचना सेगमेंटेशन व आर्किटेक्चरल सुधारणा. या दोन्ही श्रेणींचे प्रमाणक काय ? जर पहिले प्रमाण दुसऱ्यापेक्षा कितीतरी जास्त असेल, तर आपण दिसण्यावर अधिक खर्च करत आहोत आणि असण्यावर कमी.

यापैकी बहुतांश प्रश्नांची समाधानकारक, पुराव्यासह उत्तरे मिळाली नाहीत. तर आपली बँक सध्या एका मोठ्या जोखमीच्या केंद्रस्थानी उभी

आहे, आणि हा धोका डीपीडीपी कायद्याची अंमलबजावणी पूर्ण क्षमतेने सुरू होताच कुठल्या ना कुठल्या स्वरूपात सार्वजनिकरीत्या उघडकीस येणे अटळ आहे.

७. संचालक मंडळासाठी अंतिम संदेश

रिझर्व्ह बँकेच्या सीएसएफ आराखड्याने गेल्या दशकात सहकारी बँकिंग क्षेत्रात अमूल्य प्रशासकीय शिस्त रुजवली. सुस्पष्ट संरचना, उत्तरदायित्त्वाची चौकट, औपचारिक अहवाल-प्रक्रिया आणि CISO सारख्या समर्पित पदाची मान्यता. ही कामगिरी कोणत्याही प्रकारे कमी लेखता येणार नाही. तथापि, या आराखड्याने एक मूलभूत प्रश्न मात्र पूर्णत: अनुत्तरित ठेवला. नेटवर्कची प्रत्यक्ष अभियांत्रिकी रचना नेमकी कशी असावी ? आणि याच मौनामुळे, सहकारी बँकिंग क्षेत्राची प्रशासकीय इमारत भक्कम असली, तरी तिचा अभियांत्रिकी पाया अद्यापही नाबार्ड-एएसपी युगाच्या पद्धतींमध्येच रुजलेला आहे.

डीपीडीपी कायदा हे मौन कदापि खपवून घेणार नाही. कारण तो प्रत्यक्ष तांत्रिक पुराव्यांवर आधारलेला आहे, धोरण दस्तऐवजांवर नव्हे.

संचालक मंडळासाठी पाच अंतिम सत्य

१) उत्तरदायित्त्व हस्तांतरणीय नाही -

डेटा फिड्युशियरी म्हणून कायदेशीर व आर्थिक जबाबदारी थेट बँकेवरच आहे, ती कोणत्याही कराराद्वारे, आऊटसोर्सिंग व्यवस्थेद्वारे किंवा सेवा-स्तरीय कराराद्वारे हस्तांतरित होत नाही. सिस्टिम इंटिग्रेटर, सल्लागार, vCISO, GAP analyst — कोणीही या जबाबदारीचा भार उचलू शकत नाही, अगदी सद्हेतून प्रयत्न करूनही नाही.

२) फ्लॅट नेटवर्कवर डीपीडीपी अनुपालन संरचनात्मकदृष्ट्या अशक्य -

कितीही उत्तम धोरणे, कितीही सखोल ऑडिट, कितीही व्यापक प्रशिक्षण कार्यक्रम हे फ्लॅट नेटवर्क आर्किटेक्चरमधील मूलभूत अभियांत्रिकी त्रुटी झाकू शकत नाहीत. हे केवळ 'अधिक काम' करण्याची बाब नाही - हे मूलत:च वेगळ्या प्रकारे बांधकाम करण्याची बाब आहे.

३) खर्च हा अतिरिक्त भार नसून विमा हप्ता -

आवश्यक तंत्रज्ञान दशकभरापासून परिपक्व व उपलब्ध आहे, कॅप-एक्स (रु. ३ ते ८ कोटी) हा संभाव्य दंडाच्या (रु. ५० ते १०० कोटी) तुलनेत विमा हप्ता आहे. अतिरिक्त भार नव्हे. २०२७ ची अंतिम मुदत येण्यापूर्वी निर्णय घेणे अत्यावश्यक.

४) हा निर्णय संचालक मंडळाचाच आहे -

हा निर्णय निव्वळ तांत्रिक नसून प्रशासकीय व कॅप-एक्स स्तरीय आहे. म्हणूनच तो CISO किंवा आयटी-प्रमुखावर सोपवून चालणार नाही. संचालक मंडळाच्याच स्तरावर घेणे आवश्यक. (आणि निर्णयानंतरही, अंमलबजावणीचा मागोवा घेणे - हेही मंडळाचेच कर्तव्य)

५) सल्लागार व अभियंता यांच्यातील भेद ओळखावा -

जो 'गॅप शोधतो' तो आवश्यकच आहे, परंतू 'गॅप भरून काढत नाही' काढत नाही आणि जो 'मॅच्युरिटी स्कोअर देतो' तो 'नेटवर्क सेगमेंट करत नाही.' डीपीडीपी च्या युगात केवळ ओळख पुरेशी नाही - अंमलबजावणी, साक्षांकन व दीर्घकालीन देखभाल हीच महत्त्वाची.

द्विमार्गी निवड स्पष्ट आहे.

मार्ग एक: पुढील दोन वर्षे ऑडिट अहवाल, धोरण-नूतनीकरण व 'सायबरसुरक्षा परिपक्वता परिषदां' मध्ये व्यस्त राहणे. अखेरीस एखाद्या मोठ्या उल्लंघनानंतर डेटा संरक्षण मंडळासमोर तांत्रिक पुराव्यांच्या अभावी उद्रारे देण्यासाठी हजर राहणे.

मार्ग दोन : आजच या तिमाहीतच काही कठीण, अप्रिय परंतू अत्यावश्यक प्रश्न स्वत:लाच विचारणे, बँकेच्या तांत्रिक मालकीची पुन:प्रस्थापना करणे आणि नेटवर्क अभियांत्रिकीमध्ये नियोजनबद्ध, मोजमापशील, टप्प्याटप्प्याने गुंतवणूक करणे.

म्हणूनच, पुढच्या वेळी जेव्हा संचालक मंडळासमोर सायबर सुरक्षा अहवाल सादर होईल, तेव्हा केवळ 'जोखीम स्वीकारार्ह पातळीवर आहे' या आश्वासनावर समाधान मानू नका. त्याऐवजी थेट हे दोन प्रश्न विचारा - ''या जोखमीचे मोजमाप तुम्ही नेमक्या कोणत्या पद्धतीने केले आहे ?'' आणि 'डीपीडीपी कायद्याच्या नव्या संदर्भचौकटीत, ते मोजमाप आजही वैध ठरते का ?' या दोन प्रश्नांची लेखी, पुराव्यासह उत्तरे मिळाली, तरच पुढची चर्चा सुरू व्हावी.

प्रशासन तुम्हाला वाचवणार नाही.

नेटवर्क अभियांत्रिकी वाचवेल किंवा त्याच्या अभावी, कोणीही वाचवू शकणार नाही.

*****