అనుబంధం -1

బేస్ లైన్ సైబర్ సెక్యూరిటీకి అవసరమైన ముందస్తు ఏర్పాట్లు

బ్యాంకులు తమ బేస్ లైన్ సైబర్ సెక్యూరిటీ వ్యవస్థను మరింత కట్టుదిట్టం చేసుకొనేందుకు అవసరమైన సూచనాత్మక (సంపూర్ణం కాదు) ఏర్పాట్లను ఈ కింది జాబితాలో ఇవ్వడం జరిగింది. కాలక్రమంలో ఎదురయ్యే కొత్త సవాళ్లు, ఉత్పత్తులు, పద్ధతుల కారణంగా తలెత్తే సమస్యలను ఎప్పటికప్పుడు వీటిని ఉపయోగించుకుని పరీక్షించుకోవచ్చు. సమర్థమైన సైబర్ సెక్యూరిటీ కోసం CERT-In పేర్కొన్న ముఖ్యమైన సెక్యూరిటీ కంట్రోల్స్ ను కూడా చూడవచ్చు. మనం మన మెదడులో పెట్టుకోవాల్సిన కొన్ని ముఖ్యమైన అంశాలు :

ఎ) సాంకేతిక సమన్వయం, వాటితో పాటే ప్రమాదాలు పెరుగుతున్న నేపథ్యంలో, ఐటీ సబ్ కమిటీ పాత్రను పునఃసమీక్షించాలి. బోర్డు స్థాయి జోక్యం మరియు మార్గదర్శకాల వల్ల మేలు జరుగుతుంది.

బి) మనం శత్రువుల కన్నా ముందుండడానికి ప్రయత్నించడం మేలు చేస్తుంది.

సి) సైబర్ సెక్యూరిటీ ఆపరేషన్స్ సెంటర్ రియల్ టైమ్‌లో/రియల్ టైమ్ కు వీలైనంత దగ్గరగా వివిధ లాగ్‌లు/సంఘటనలను పర్యవేక్షించే సామర్థ్యాన్ని కలిగి ఉండాలి.

డి) జాగ్రత్తగా ఉండడం చాలా అవసరం. నిరంతరం అప్రమత్తంగా ఉండడం మేలు.

ఇ) హార్డ్ వేర్ డివైజ్ లు, సాఫ్ట్ వేర్ అప్లికేషన్లు భద్రతను కల్పించినా, వాటిని తగిన రూపు దిద్దడం చాలా అవసరం.

ఎఫ్) మానవ వనరులు చాలా ముఖ్యం. వారికి తగిన శిక్షణ అందే విధంగా చూడాలి. క్రమం తప్పకుండా వారికి బ్యాంకు యొక్క సెక్యూరిటీ పాలసీలను తెలియజేయండి.

బేస్ లైన్ కంట్రోల్స్

1) బిజినెస్ ఐటీ ఆస్తుల యొక్క జాబితా నిర్వహణ

1.1 ఏ రోజుకారోజు బిజినెస్ డాటా/ఇన్ఫర్మేషన్, కస్టమర్ డాటా/ఇన్ఫర్మేషన్, బిజినెస్ అప్లికేషన్స్, సపోర్టింగ్ ఐటీ ఇన్ ఫ్రాస్ట్రక్చర్ మరియు సదుపాయాలు - హార్డ్ వేర్ / సాఫ్ట్ వేర్ / నెట్ వర్క్ డివైజెస్, ముఖ్యమైన సిబ్బంది, సేవలు మొద. ఆస్తుల జాబితా నిర్వహణను చూసుకోండి. బిజినెస్ లో అవి ఏ మేరకు కీలకం అన్నదానిని పేర్కొనండి. ముఖ్యమైన ఆస్తులను గుర్తించడానికి బ్యాంకులకు వాటికంటూ ఒక వ్యవస్థ/ప్రమాణాలు ఉండవచ్చు.

1.2 బ్యాంకు యొక్క వర్గీకరణ/సెన్సిటివిటీ ప్రమాణాల ఆధారంగా డాటా/సమాచారాన్ని వర్గీకరించండి.

1.3 డాటా/సమాచారాన్ని ఏ విధంగా బ్యాంక్ వ్యవస్థ లోపల/బయట నిలువ చేస్తున్నారు, ట్రాన్స్ మిట్ చేస్తున్నారు, ప్రాసెస్ చేస్తున్నారు, యాక్సెస్ చేస్తున్నారు మరియు దానిని ఏ విధంగా ఉపయోగించుకుంటున్నారు; ఆ డాటా/సమాచారం సెన్సిటివిటీని బట్టి అవి ఏ మేరకు రిస్కులను ఎదుర్కొంటున్నాయి అన్న దానిని బట్టి సంస్థ నెట్ వర్క్ లోపల, బయట దానికి రక్షణ కల్పించండి.

2. అనధికార సాఫ్ట్ వేర్ ను ఉపయోగించడాన్ని నివారించడం

2.1 ఎప్పటికప్పుడు తాజా, వీలైతే కేంద్రీకృత అధికారిక/అనధికారిక సాఫ్ట్ వేర్ జాబితాను మెయిన్‌టెయిన్ చేయండి. విశ్వసనీయమైన అప్లికేషన్లు/సాఫ్ట్ వేర్లు/లైబ్రరీలను ఉపయోగించడానికి ప్రాధాన్యతనివ్వండి.

2.2 ఎండ్ యూజర్ పీసీలు, లాప్ ట్యాప్‌లు, వర్క్ స్టేషన్లు, సర్వర్లు, మొబైల్స్ మొదలైన వాటిలో సాఫ్ట్ వేర్/అప్లికేషన్ల ఇన్ స్టాలేషన్ విషయంలో సెంట్రలైజ్డ్ లేదా ఇతర విధంగా నియంత్రణ కలిగిన వ్యవస్థను ఏర్పాటు చేసుకోండి. అదే విధంగా అలాంటి సిస్టమ్స్/డివైజెస్‌లలో అనధికారిక సాఫ్ట్ వేర్లు/అప్లికేషన్లను గుర్తించి వాటిని పని చేయకుండా/బ్లాక్ చేసేందుకు ఒక వ్యవస్థను ఏర్పాటు చేసుకోవాలి.

2.3 వివిధ వెండర్లు /OEMల ద్వారా, మరియు సూచనల ద్వారా CERT-In మరియు ఇతర సంస్థలు విడుదల చేసే ప్యాచెస్ ను నిరంతరం పరిశీలిస్తూ ఉండండి. ఈ సెక్యూరిటీ ప్యాచ్ లను

బ్యాంక్ యొక్క ప్యాచ్ మేనేజ్ మెంట్ పాలసీకి అనుగుణంగా అమలు చేయండి. ఏదైనా OEM/ఉత్పత్తిదారు/వెండర్ బాగా తెలిసిన/ ప్రాచుర్యం పొందిన/వెల్లడైన దాడులకు రక్షణగా ఒక ప్యాచ్/ ప్యాచ్ ల సిరీస్ విడుదల చేస్తే బ్యాంకులు వెంటనే వాటిని ఒక ఎమర్జెన్సీ ప్యాచ్ మేనేజ్ మెంట్ విధానం ద్వారా అమలు చేసే వ్యవస్థ ఉండాలి.

2.4 మినహాయింపులు, వాటి కాలపరిమితి, ఆ మినహాయింపులు మంజూరు చేసే విధానం, దానిని ఏ విధంగా అప్రూవ్ చేయాలి, జారీ చేసిన మినహాయింపులను, బిజినెస్ ను, ఆ మినహాయింపుల నేప థ్యాన్ని సమగ్రంగా అర్థం చేసుకున్న అధికారులు (పైస్థాయిలోని వారైతే మేలు) ఒక నిర్ణీత కాలప రిమితిలో ఏ విధంగా సమీక్షించాలి అన్నదాని కోసం ఒక సమగ్రమైన వ్యవస్థను ఏర్పాటు చేసుకోవాలి.

3. ఎన్విరాన్ మెంటల్ కంట్రోల్

3.1 సహజంగా మరియు మనుషుల నుంచి ఎదురయ్యే ప్రమాదాల నుంచి కీలకమైన ఆస్తుల రక్షణ కొరకు తగిన ఎన్విరాన్ మెంటల్ కంట్రోల్స్‌ను వాటి స్థానంలో ఉంచాలి.

3.2 ఉష్ణోగ్రత, నీరు, పొగ, యాక్సెస్ అలారం, సేవకు సంబంధించిన అలర్ట్‌లు (విద్యుత్ సరఫ రా, టెలీకమ్యూనికేషన్, సర్వర్లు), యాక్సెస్ లాగ్‌లు మొద. ఎన్విరాన్ మెంటల్ కంట్రోల్స్ విష యంలో జరిగే ఉల్లంఘనలు/మినహాయింపులను నియంత్రించ డానికి అవసరమైన వ్యవస్థను ఏర్పాటు చేయాలి. బ్యాంకు యొక్క ముఖ్యమైన ఆస్తుల పరిరక్షణకు తగిన భద్రతాపరమైన చర్యలు తీసుకోవాలి.

4. నెట్ వర్క్ మేనేజ్‌మెంట్ మరియు సెక్యూరిటీ

4.1 ఎప్పటికప్పుడు సంస్థాగత స్థాయిలో వైర్డ్ మరియు వైర్‌లెస్ నెట్ వర్క్స్‌తో కూడిన ఒక నెట్ వర్క్ ఆర్కిటెక్చర్ చిత్రాన్ని తయారు చేసి, నిర్వహించండి.

4.2 బ్యాంక్ నెట్ వర్క్ (బ్యాంకు పరిసరాల లోపల/బయట)కు కనెక్ట్ చేయబడిన అధికారిక డివైజ్‌ల అప్ టు డేట్/సెంట్రలైజ్డ్ జాబితాను, బ్యాంక్ నెట్‌వర్క్‌ను నడిపిస్తున్న అధికారిక డివైజ్‌ల జాబితాను తయారు చేసి నిర్వహించుకోండి. బ్యాంకులు ఆటోమేట్ నెట్‌వర్క్ డిస్కవరీ అండ్ మేనేజ్ మెంట్‌ల సొల్యూషన్స్‌ను అమలు పరచడానికి పూనుకోవచ్చు.

4.3 అన్ని నెట్‌వర్క్ డివైజెస్ తగిన విధంగా కాన్ఫిగర్ చేయబడి ఉండేలా జాగ్రత్తలు తీసుకోండి. ఎప్పటికప్పుడు ఆ కాన్ఫిగరేషన్ తగిన స్థాయి నెట్ వర్క్ సెక్యూరిటీ ఉందేమో గమనిస్తూ ఉండండి.

4.4 వైర్‌లెస్ లోకల్ ఏరియా నెట్‌వర్క్‌లు, వైర్‌లెస్ యాక్సెస్ పాయింట్లు, వైర్‌లెస్ క్లయింట్ యాక్సెస్ సిస్టమ్‌ల భద్రత కొరకు తగిన కంట్రోల్స్ ఏర్పాటు చేయండి.

4.5 మొబైల్ డివైజ్‌లైన లాప్‌టాపులు, మొబైల్ ఫోన్లు, టాబ్లెట్లు మొదలైన వాటిలో అధికారిక హార్డ్‌వేర్ ఉపయోగిస్తున్నారో లేదో గుర్తించేందుకు తగిన వ్యవస్థను రూపొందించుకోండి. బ్యాంకు నిర్దేశించిన సెక్యూరిటీ ప్రమాణాలను అవి అందుకోగలిగినప్పుడే వాటికి కనెక్టివిటీ అందేలా చూసుకోండి.

4.6 బ్యాంక్ నెట్‌వర్క్‌తో అనధికారిక డివైజ్ కనెక్షన్లను వెంటనే గుర్తించి, వాటిని బ్లాక్ చేసేలా వ్యవస్థను ఏర్పాటు చేసుకోండి.

4.7 సిస్టమ్‌లు, సర్వర్‌లు, నెట్‌వర్క్ డివైజెస్, ఎండ్ పాయింట్స్‌లో ఏదైనా అసాధారణ సంఘుటన జరిగితే దానిని గుర్తించేందుకు, పరిష్కరించేందుకు అవసరమైన వ్యవస్థను ఏర్పాటు చేసుకోవాలి.

4. 8 నెట్‌వర్క్‌కు ఉన్న అన్ని కనెక్టింగ్ డివైజెస్‌తో పాటు అన్ని ప్రధానమైన ఐటీ కార్య కలాపాలకు స్టాండర్డ్ ఆపరేటింగ్ ప్రొసీజర్స్ (SOP) ను ఏర్పాటు చేసుకోండి.

4.9 వివిధ నెట్‌వర్క్ కార్యకలాపాల లాగ్‌లను సెక్యూరిటీ ఆపరేషన్స్ సెంటర్ పర్యవేక్షిస్తుంది. ఈ సెంటర్‌కు ఏవైనా అసాధారణ సంఘుటనలు జరిగితే వెంటనే పసిగట్టి, హెచ్చరికలు జారీ చేసే సామర్థ్యం ఉండాలి.

4.10 సమర్థంగా కాన్ఫిగర్ చేసిన ఫైర్ వాల్స్, ప్రాక్సీస్, DMZ పెరిమీటర్ నెట్ వర్క్స్, మరియు నెట్ వర్క్ బేస్డ్ ఐపీలు, ఐడీల ద్వారా బహుళ పొరల రక్షణ వ్యవస్థను ఏర్పరచుకోవాలి. లోపలికి వచ్చే, బయటికి వెళ్లే ట్రాఫిక్‌ను ఫిల్టర్ చేసేందుకు తగిన వ్యవస్థను ఏర్పాటు చేసుకోవాలి.

5. సెక్యూర్ కాన్ఫిగరేషన్

5.1 అన్ని రకాల డివైజెస్ (ఎండ్ పాయింట్స్/వర్క్ స్టేషన్స్, మొబైల్ డివైజెస్, ఆపరేటింగ్ సిస్టమ్స్, డాటా బేసెస్, అప్లికేషన్స్, నెట్ వర్క్ డివైజెస్, సెక్యూరిటీ డివైజెస్, సెక్యూరిటీ సిస్టమ్స్

(మొద.)వాటి లైఫ్ సైకిల్‌ను (సంకల్పించిన నాటి నుంచి అమలుచేసిన నాటి వరకు) అక్షరబద్ధం చేసి, వాటికి బేస్ లైన్ సెక్యూరిటీ ఏర్పాట్లు/ కాన్ఫిగరేష న్‌ను అమలు పరచాలి. క్రమం తప్పకుండా వాటిని సమీక్షించాలి.

5.2 ఇన్ డాటా సెంటర్లు, ఇన్ థర్డ్ పార్టీ హోస్టెడ్ సైట్లు, షేర్డ్ ఇన్‌ఫ్రాస్ట్రక్చర్ లొకేషన్లతో కూడిన బ్యాంక్ నెట్ వర్క్ యొక్క క్రిటికల్ డివైజెస్ (ఫైర్ వాల్, నెట్ వర్క్ స్విచెస్, సెక్యూరిటీ డివైజెస్ మొద.) కాన్ఫిగరేషన్ మరియు ప్యాచ్ లెవల్స్ ను క్రమం తప్పకుండా సమీక్షించండి.

6. అప్లికేషన్ సెక్యూరిటీ లైఫ్ సైకిల్ (ASLC)

6.1 అప్లికేషన్ లైఫ్ సైకిల్ యొక్క అన్ని దశలలోను ఇన్ఫర్మేషన్ సెక్యూరిటీ కొరకు జాగ్రత్తలు తీసుకోండి.

6.2 క్రిటికల్ బిజినెస్ అప్లికేషన్‌ల విషయానికి వస్తే, బ్యాంకులు ప్రొఫెషనల్ సామర్థ్యం కలిగిన సిబ్బంది/సర్వీస్ ప్రొవైడర్ల ద్వారా సోర్స్ కోడ్ ఆడిట్‌లు నిర్వహించేలా చూడొచ్చు. లేదా ఆ అప్లికేషన్‌లో ఎలాంటి అంతర్గత మాలీషియస్/ ఫ్రాడ్యులెంట్ కోడ్‌లు లేవని అప్లికేషన్ ప్రొవైడర్లు/ OEMల నుంచి గ్యారంటీ పొందవచ్చు.

6.3 అంతర్గతంగా/సహకారంతో అభివృద్ధి చేసిన అప్లికేషన్ల కోసం సెక్యూర్ కోడింగ్ ప్రాక్టీసెస్‌ను అమలు చేయవచ్చు.

6.4 బిజినెస్ ఫంక్షనాలిటీస్‌తో పాటు సిస్టమ్ యాక్సెస్ కంట్రోల్, అథెంటికేషన్, ట్రాన్సాక్షన్ అథరైజేషన్, డాటా ఇంటిగ్రిటీ, సిస్టమ్ యాక్టివిటీ లాగింగ్, ఆడిట్ ట్రయల్, సెషన్ మేనేజ్‌మెంట్, సెక్యూరిటీ ఈవెంట్ ట్రాకింగ్ మరియు ఈవెంట్ హ్యాండ్లింగ్‌లకు చెందిన సెక్యూరిటీ అవసరాలను సిస్టమ్ డెవలప్‌మెంట్/ అక్విజిషన్/ ఇంప్లిమెంటేషన్ యొక్క ప్రారంభ మరియు తర్వాత దశల్లో స్పష్టంగా పేర్కొనాల్సి ఉంటుంది.

6.5 డెవలప్‌మెంట్, టెస్ట్ మరియు ప్రొడక్షన్ ఎన్విరాన్‌మెంట్‌లను ఖచ్చితంగా వేరు చేయాలి.

6.6 సిస్టమ్/అప్లికేషన్ డెవలప్‌మెంట్ దృక్పథం థ్రెట్ మోడలింగ్ మీద ఆధారపడి ఉండాలి. దానిలో సెక్యూర్ కోడింగ్ ప్రిన్సిపల్స్ ఉండాలి. సెక్యూరిటీ పరీక్షలు అంతర్జాతీయ ప్రమాణాలకు, సెక్యూర్ రోల్ అవుట్‌కు అనుగుణంగా ఉండాలి.

6.7 సాఫ్ట్‌వేర్/అప్లికేషన్ డెవలప్‌మెంట్ ప్రాక్టీసులు ఓపెన్ వెబ్ అప్లికేషన్ సెక్యూరిటీ ప్రాజెక్ట్ (OWASP)లాంటి వాటి ఆధారంగా ఏదైనా విపత్తు జరిగే అవకాశాలను ఎదుర్కొనండి. లేయర్డ్ సెక్యూరిటీ మెకానిజం కొరకు డిఫెన్స్-ఇన్-డెప్త్ అన్న నియ మాన్ని అనుసరిచండి.

6.8 మొబైల్/ స్మార్ట్ ఫోన్‌లలో కేవలం వ్యాపార అవసరాల కొరకు ఎన్‌క్రిప్ట్ చేయబడిన, ఇతర స్మార్ట్ ఫోన్ డాటా/అప్లికేషన్ల నుంచి వేరు చేసిన కంటెయినరైజ్డ్ యాప్‌లను ఇన్‌స్టాల్ చేసే అవ కాశాలను పరిశీలించండి. అవసరమైతే ఆ కంటెయినరైజ్డ్ యాప్‌లో డాటాను చదివే వీలు లేకుండా ఒక రిమోట్ వైప్‌ను ఏర్పాటు చేసే అవకాశాలను కూడా పరిశీలించాలి.

6.9 ప్రస్తుతం ఎదురవుతున్న, కొత్తగా పుట్టుకొస్తున్న సెక్యూరిటీ ప్రమాదాలను అధిగమించ డానికి సరికొత్త టెక్నాలజీలను అనుసరించేలా జాగ్రత్తలు తీసుకోండి. బ్యాంకుకు చెందిన ఐటీ/సెక్యూరిటీ టీమ్ బ్యాంక్ క్రిటికల్ సిస్టమ్‌లో అలాంటి ప్రమాదాలకు నివారించే టెక్నాలజీని ప్రవేశ పెట్టే ముందు దానిపై తగిన పట్టు సాధించేలా జాగ్రత్త వహించండి.

7. ప్యాచ్/వల్నరబిలిటీ మరియు ఛేంజ్ మేనేజ్‌మెంట్

7.1 ప్యాచ్ చేయాల్సిన ఐటీ కాంపొనెంట్ల జాబితాను తయారు చేసేందుకు, ప్యాచెస్‌ను గుర్తించేందుకు, వల్నెరబుల్ సిస్టమ్స్ సంఖ్యను, అవి ప్రమాదాలకు గురి అయ్యే కాలాన్ని త గ్గించేందుకు ఒక క్రమబద్ధమైన, అక్షరబద్ధం చేసిన రిస్క్-బేస్డ్ వ్యూహాన్ని అనుసరించండి.

7.2 ఆపరేటింగ్ సిస్టమ్‌లు, ఇంటర్నెట్‌కు సరాసరి కనెక్ట్ చేయబడిన ఎండ్ యూజర్ డివైజెస్ లో నడుస్తున్న ఆపరేటింగ్ సాఫ్ట్‌వేర్, అప్లికేషన్ సాఫ్ట్‌వేర్‌లోను; సర్వర్ ఆపరేటింగ్ సిస్టమ్స్/ డాటా బేసెస్/అప్లికేషన్స్/మిడిల్‌వేర్ మొదలైన వాటిలో ఉన్న ప్యాచెస్‌ను గుర్తించేందుకు, ట్రాక్ చేసేందుకు, నిర్వహించేందుకు, పర్యవేక్షించేందుకు అవసరమైన వ్యవస్థను, పద్ధతులను ఏర్పాటు చేయండి.

7.3 బిజినెస్ అప్లికేషన్లు, సపోర్టింగ్ టెక్నాలజీ, సర్వీస్ కాంపొనెంట్లు మరియు ఫెసిలిటీస్‌కు చేసే మార్పులు సమర్థమైన కాన్ఫిగరేషన్ మేనేజ్‌మెంట్ ప్రాసెస్‌ల ద్వారా, కాన్ఫిగరేషన్ బేస్‌లైన్ ద్వారా నిర్వహించాలి.

7.4 ఇంటర్నెట్‌ను ఉపయోగించే వెబ్/మొబైల్ అప్లికేషన్లు, సర్వర్లు, నెట్ వర్క్ కాంపొనెంట్లకు అవి పని చేసినంత కాలం (ప్రీ-ఇంప్లిమెంటేషన్, పోస్ట్ ఇంప్లిమెంటేషన్, ఆఫ్టర్ ఛేంజెస్ మొద.) క్రమం తప్పకుండా VA/PT పరీక్షలు నిర్వహించాలి.

7.5 ఇంటర్నెట్‌ను ఉపయోగించే వెబ్/మొబైల్ అప్లికేషన్లు, సర్వర్లు, నెట్ వర్క్ కాంపొనెంట్లకు అవి పని చేసినంత కాలం (ప్రీ-ఇంప్లిమెంటేషన్, పోస్ట్ ఇంప్లిమెంటేషన్, ఆఫ్టర్ ఛేంజెస్ మొద.) ప్రొడక్షన్ ఎన్విరాన్‌మెంట్‌ను లేదా అలాంటి ఎన్విరాన్‌మెంట్‌ను పోలిన ప్రదేశంలోనే అప్లికేషన్ సెక్యూరిటీ టెస్టింగ్‌ను నిర్వహించాలి.

7.6 ప్రమాదాలను తగ్గించే వ్యూహంలో భాగంగా, ఆ సంఘటనకు మూల కారణాలను వెదికి, అవి ప్రమాదం బారిన పడే అవకాశాలను నివారించండి.

7.7 డాటా సెంటర్లలోని వివిధ (i) వీలాన్‌లు (ii) LAN/WAN ఇంటర్‌ఫేసుల మధ్య ఉన్న యాక్సెస్ పాయింట్లు, నోడ్‌లు (iii) ఎక్స్‌టర్నల్ నెట్‌వర్క్, భాగస్వాములు, వెండర్, సర్వీస్ ప్రొవైడర్ నెట్‌వర్క్‌తో బ్యాంక్ నెట్‌వర్క్ సంబంధాలను సెక్యూర్‌గా కాన్ఫిగర్ చేసేందుకు ఎప్పటికప్పుడు యాక్సెస్ డివైజ్ కాన్ఫిగరేషన్లు, ప్యాచ్ లెవల్స్‌ను సమీక్షిస్తుండండి.

8. యూజర్ యాక్సెస్ కంట్రోల్ / మేనేజ్‌మెంట్

8.1 బ్యాంకు పరిధిలో/పరిధి నిర్ధారణంగా ఉన్న (ఉదా. ఎన్‌క్రిప్షన్‌ను ఉపయోగించి, డివైజ్ అందుకు సహకరిస్తే), మారుతున్న (VPN లేదా ఇతర సెక్యూర్ వెబ్ ప్రొటోకాల్స్ లాంటి సాంకేతిక పరిజ్ఞానం ద్వారా) డాటా/సమాచారాన్ని పరిరక్షించడం ద్వారా బ్యాంకు ఆస్తులు/సేవలను సుర క్షితంగా పొందే అవకాశం కల్పించండి.

8.2 లాగ్ ఆన్ యూజర్ ఐడీ, విశ్వసనీయమైన సమాచారం, టోకెన్లు, యాక్సెస్ ప్రొఫైల్ మొదలైన కస్టమర్ యాక్సెస్ క్రెడెన్షియల్స్‌ను లీకేజీలు/దాడుల నుంచి కాపాడండి.

8.3 ఎండ్ యూజర్ వర్క్ స్టేషన్లు/పీసీలు/ల్యాప్‌టాపులు లాంటి వాటి విషయంలో అడ్మినిస్ట్రేటివ్ రైట్స్‌ను అనుమతించవద్దు. ఒకవేళ అవసరమైతే ఎందుకోసం అన్నది తెలుసుకునే హక్కు కలిగి ఉండేలా, అవసరమైనప్పుడు నిర్ణీత కాలపరిమితి కోసం మాత్రమే,నిర్దిష్టమైన విధానాల ద్వారా మాత్రమే అనుమతి జారీ చేయండి.

8.4 అప్లికేషన్లు, ఆపరేటింగ్ సిస్టమ్‌లు, డాటాబేస్, నెట్ వర్క్ అండ్ సెక్యూరిటీ డివైజెస్ /సిస్టమ్స్, పాయింట్ ఆఫ్ కనెక్టివిటీ (లోకల్/రిమోట్ మొద.) ల విషయంలో వాటి యాక్సెస్ పొందేందుకు, నిర్వహించేందుకు ఒక సెంట్రలైజ్డ్ అథెంటికేషన్ అండ్ అథరైజేషన్ వ్యవస్థను నెలకొల్పండి. దీనిలో బలమైన పాస్ వర్డ్ విధానం, రిస్క్ అసెస్‌మెంట్‌కు అనుగుణంగా 2-ఫ్యాక్టర్/మల్టీ ఫ్యాక్టర్ అథెంటికేషన్ ఉండాలి. అతి తక్కువ అధికారాలు, బాధ్యతలను స్పష్టంగా నిర్వచించడం మొదలైన నియమాలను కఠినంగా అమలుపరచాలి.

8. 5 క్రిటికల్ సిస్టమ్స్ (సర్వర్లు/ఆపరేటింగ్ సిస్టమ్/DB, అప్లికేషన్లు, నెట్‌వర్క్ డివైజెస్ మొద.) పై పని చేయడానికి, నిర్వహించడానికి, లాగ్ కావడానికి, పర్యవేక్షించ డానికి, ప్రివిలైజ్డ్ / సూపర్ యూజర్ /అడ్మినిస్ట్రేటివ్ యాక్సెస్ పొందడానికి తగిన (సెంట్రలైజ్డ్) వ్యవస్థను, కంట్రోల్స్‌ను కఠినంగా అమలు పరచడండి.

8.6 ఇన్‌వాలిడ్ లాగాన్ కౌంట్స్‌ను తగ్గించడానికి, డార్మాట్ అకౌంట్లను డీయాక్టివేట్ చేయడానికి కంట్రోల్స్‌ను అమలు చేయాలి.

8.7 లాగాన్ విధానంలో ఏవైనా అనూహ్యమైన మార్పులు వస్తాయేమో పరిశీలిస్తూ ఉండండి.

8.8 పీసీలు/లాప్‌ట్యాప్‌లు మొదలైన వాటిలో సాఫ్ట్ వేర్ ఇన్‌స్టాలేషన్‌లను నియంత్రించడానికి తగిన చర్యలు తీసుకోండి.

8.9 లాప్‌ట్యాప్‌లతో పాటు ఇతర మొబైల్ డివైజ్‌ల రిమోట్ మేనేజ్‌మెంట్/వైపింగ్/లాకింగ్ కోసం కంట్రోల్స్‌ను అమలు చేయండి.

8.10 ఆఫీస్ డాక్యుమెంట్స్‌లో VBA/మాక్రోస్ వినియోగాన్ని నియంత్రించడానికి, ఈమెయిల్ సిస్టమ్స్‌లో అటాచ్‌మెంట్స్ రకాలను నియంత్రించడానికి తగిన చర్యలు తీసుకోండి.

9. కస్టమర్లకు విశ్వసనీయమైన ఫ్రేమ్ వర్క్

9.1 కస్టమర్లు బ్యాంకు వద్ద ఒక పాజిటివ్ ఐడెంటిటీ వెరిఫికేషన్ చేసుకునేందుకు విశ్వస నీయ మైన ఫ్రేమ్ వర్క్/వ్యవస్థను అమలు పరచండి.

9.2 కస్టమర్ గుర్తింపు సమాచారాన్ని జాగ్రత్తగా భద్రపరచాలి.

9.3 బ్యాంకులు సెక్యూర్ అథెంటికేషన్ టెక్నాలజీలను ఉపయోగించుకోవడం ద్వారా పార్ట్‌నర్ సిస్టమ్స్ కస్టమర్ల ఐడెంటిఫికేషన్, అథెంటికేషన్ కు యాక్సెస్ పొందడంలో ఐడెంటిటీ ప్రొవైడర్‌గా వ్యవహరించాలి.

10. మెయిల్, మెసేజింగ్ సిస్టమ్‌ల భద్రత

10.1 బ్యాంకులు, వాటి భాగస్వాములు, వెండర్లు ఉపయోగించే మెయిల్, మెసేజింగ్ సిస్టమ్ లు సురక్షితంగా ఉండేలా జాగ్రత్తలు తీసుకోవాలి. దీనిలో భాగంగా ఈమెయిల్ స్పూఫింగ్, ఐడెంటికల్ మెయిల్ డొమైన్లను నివారించడం, అటాచ్‌మెంట్‌ల రక్షణ, హాని కలుగజేసే లింకులను దూరంగా ఉంచడం మొదలైన చర్యలు చేపట్టాలి.

10.2 ఈమెయిల్ సర్వర్ స్పెసిఫిక్ కంట్రోల్స్‌ను నమోదు చేసి, దానిని అమలుపరచాలి.

11 వెండర్ రిస్క్ మేనేజ్‌మెంట్

11.1 ఔట్‌సోర్స్‌డ్ మరియు పార్ట్‌నర్ ఏర్పాట్లలో బ్యాంకులు తగిన మేనేజ్‌మెంట్, సెక్యూరిటీ రిస్కుల విషయంలో భరోసా ఇచ్చేలా జవాబుదారీతనం వహించాలి.

11.2 బ్యాంకులు ముఖ్యమైన కార్యకలాపాలను ఔట్‌సోర్సింగ్ ఇవ్వాల్సిన అవసరాన్ని జాగ్రత్త గా పరిశీలించాలి. వెండర్/పార్ట్‌నర్ ఎంపిక విషయంలో సమగ్ర రిస్క్ అసెస్ మెంట్ ఆధారంగా వ్యవ హరించాలి.

11.3 థర్డ్ పార్టీ వెండర్లు/సర్వీస్ ప్రొవైడర్లు, భాగస్వాముల విషయంలో బ్యాంకులు నిరంతరం అప్రమత్తత, దూరదృష్టి కలిగి ఉంటూ వాటి నిర్వహణను పర్యవేక్షించాలి.

11.4 బ్యాంకులు అన్ని వెండర్/ఔట్సోర్సింగ్ కార్యకలాపాల రిస్కులను సమీక్షించ డానికి, ఆమోదించడానికి, పొందడానికి, నియంత్రించడానికి, పర్యవేక్షించడానికి బేస్ లైన్ సిస్టమ్ సెక్యూరిటీ కాన్ఫిగరేషన్ ప్రమాణాల సహకారం కలిగిన ఫ్రేమ్‌వర్క్, విధానాలు, పద్ధతులు రూపొందించాలి.

11.5 సర్వీస్ ప్రొవైడర్ (ఇతర బ్యాంకులతో సహా) దేశంలోని అన్ని నియంత్రణా, చట్టబద్ధమైన అవసరాలకు లోబడి ఉండేట్లుగా బ్యాంకులు జాగ్రత్తలు తీసుకోవాలి. ఇందుకోసం బ్యాంకులు ఆయా సర్వీస్ ప్రొవైడర్లతో వాటిపై ఆడిట్ హక్కులు, దేశంలోని రెగ్యులేటర్ల ద్వారా తనిఖీలు చేసే అధికారాన్ని కలిగి ఉండేలా ఒప్పందం కుదుర్చుకోవాలి.

11.6 బ్యాంకులు ఉపయోగించుకునే అన్ని సమాచార వనరులను (ఆన్‌లైన్/వ్యక్తిగత) రిజర్వ్ బ్యాంక్ చూడగలిగే/పొందగలిగే అవకాశం ఉండాలి. రిజర్వ్ బ్యాంక్ కోరినప్పుడు ఈ మౌలిక సదుపాయాలు/వనరులు భౌతికంగా బ్యాంకు పరిసరాలలో లేకున్నా, బ్యాంకులు ఆ సమాచారాన్ని అందజేయాలి.

11.7 బ్యాంకులు ఇన్‌ఫ్రాస్ట్రక్చర్ ఉన్న భౌగోళిక ప్రదేశం, డాటా సరిహద్దులు దాటి పోయే విష యంలో అవసరమైన అన్ని చట్టపరమైన నిబంధనలకు, నియంత్రణా సంస్థల పరిధికి లోబడి ఉండాలి.

11.8 బ్యాంకుల కీలక ఆస్తులపై యాక్సెస్ పొందే, నిర్వహించే వెండర్/థర్డ్ పార్టీ సిబ్బంది యొక్క అధికారిక ధృవపత్రాలను బ్యాంకులు స్వయంగా పరిశీంచి నిర్ధారించుకోవాలి.

11.9 థర్ట్ పార్టీ సర్వీస్ ప్రొవైడర్లందరికీ బ్యాక్ గ్రౌండ్ పరిశీలన, సమాచారాన్ని బయటికి వెల్ల డించరాదనే ఒప్పందాలు, సెక్యూరిటీ పాలసీకి లోబడి ఉంటామనే ఒప్పందాలు తప్పనిసరి.

12 తొలగించ వీలున్న మీడియా

12. 1 వర్క్ స్టేషన్లు/పీసీలు/ల్యాప్‌టాపులు/మొబైల్ డివైజ్‌లు/సర్వర్లు మొదలైన డివైజెస్లలో ఉపయోగించే - తొలగించే వీలున్న మీడియా/ BYOD నియంత్రణ, వాటిని సురక్షితంగా ఉపయోగించే విషయంలో అవసరమైన పాలసీలను పేర్కొని వాటిని ఖచ్చితంగా అమలుపరచాలి.

12.2 అలాంటి డివైజెస్‌కు/నుంచి ట్రాన్స్‌ఫర్/కాపీ చేసే మీడియా రకాలను, సమాచారాన్ని నియంత్రించండి.

12.3 అలాంటి తొలగించదగిన మీడియాకు రీడ్/రైట్ యాక్సెస్ ఇచ్చే ముందు వాటిని మాల్ వేర్/యాంటీ వైరస్ కొరకు స్కాన్ చేయండి.

12. 4 యాక్టివ్ డైరెక్టరీ లేదా ఎండ్ పాయింట్ మేనేజ్‌మెంట్ సిస్టమ్ ద్వారా తొలగించద గిన మీడియా వినియోగాన్ని బ్లాక్‌లిస్ట్/వైట్‌లిస్ట్/నియంత్రించేందుకు ఒక సెంట్రలైజ్డ్ పాలసీని అమలు చేసే విషయం గురించి ఆలోచించండి.

12.5 నిర్ధిష్టంగా అథరైజ్ చేసి, దాని వినియోగాన్ని పేర్కొని, ఎంత కాలం ఉపయోగిస్తార నే విషయాన్ని పేర్కొంటే తప్ప బ్యాంకింగ్ ఎన్విరాన్‌మెంట్‌లో తొలగించదగిన డివైజెస్ /మీడియాను అనుమతించరాదన్న నిబంధనను కఠినంగా అమలుచేయాలి.

13. అడ్వాన్స్‌డ్ రియల్ టైమ్ థ్రెట్ డిఫెన్స్ అండ్ మేనేజ్‌మెంట్

13.1 హాని కలుగజేసే కోడ్‌ను ఇన్‌స్టాల్ చేయడం, వ్యాప్తి చేయడం, అమలు చేయ డాన్ని అడ్డుకునే విధంగా సంస్థలోని మల్టిపుల్ పాయింట్స్ వద్ద ఒక బలమైన రక్షణ వ్యవస్థను నిర్మించాలి.

13.2 అన్ని రకాల డివైజెస్ (పీసీలు/ల్యాప్‌టాపులు/మొబైల్ డివైజెస్ మొద.), సర్వర్లు (ఆపరేటింగ్ సిస్టమ్స్, డాటా బేసెస్, అప్లికేషన్స్ మొద.), వెబ్/ఇంటర్నెట్ గేట్ వేస్, ఈమెయిల్ గేట్‌వేస్, వైర్‌లెస్ నెట్‌వర్క్స్, SMS సర్వర్లు మొదలైన వాటికి; సెంట్రలైజ్డ్ మేనేజ్‌మెంట్ మరియు పర్యవేక్షణ కొరకు బీహేవియరల్ డిటెక్షన్ సిస్టమ్స్‌తో పాటు యాంటీమాల్‌వేర్, యాంటీవైరస్‌ను ఉపయోగించండి.

13.3 విశ్వసనీయత కలిగిన ఇంటర్‌నెట్ వెబ్‌సైట్స్/సిస్టమ్స్‌నే ఉపయోగించే విధానాన్ని అమలుపరిచేందుకు ప్రయత్నించండి.

13.4 నెట్‌వర్క్ ప్యాకెట్స్‌ను సమగ్రంగా స్కాన్ చేసేందుకు, వెబ్/ఇంటర్నెట్ గేట్ వే ద్వారా వెళ్లే ట్రాఫిక్ భద్రంగా ఉండేందుకు సురక్షితమైన వెబ్ గేట్‌వేలను ఉపయోగించే విషయాన్ని పరిశీలించండి.

14. యాంటీ-ఫిషింగ్

14.1 ఫిషింగ్ వెబ్‌సైట్లు/రోగ్ అప్లికేషన్లను గుర్తించేందుకు వాటిని పని చేయకుండా చూసేందుకు బయటి సర్వీస్ ప్రొవైడర్ల నుంచి యాంటీ ఫిషింగ్/యాంటీ రోగ్ యాప్ సర్వీసులను తీసుకోండి.

15 డాటా లీక్ నివారణ వ్యూహం

15.1 ముఖ్యమైన (కాన్ఫిడెన్షియల్) బిజినెస్ మరియు కస్టమర్ డాటా/సమాచార రక్షణ కొరకు ఒక సమగ్ర డాటా లాస్/లీకేజీ నివారణ వ్యూహాన్ని తయారు చేసుకోండి.

15.2 ఎండ్‌పాయింట్ డివైజెస్‌లో ప్రాసెస్ చేసిన డాటాను రక్షించడం, ట్రాన్స్‌మిషన్‌లో ఉన్న డాటాతో పాటు సర్వర్లు, ఇతర డిజిటల్ స్టోర్లలో ఉన్న డాటాను, ఆన్‌లైన్ కానీ ఆఫ్‌లైన్ కానీ, రక్షించడం కూడా దీనిలో భాగంగా ఉంటుంది.

15.3 వెండర్ మేనేజ్‌డ్ డివైజెస్ విషయంలో కూడా ఇలాంటి ఏర్పాట్లు చేసుకోవాలి.

16 ఆడిట్ లాగ్‌ల నిర్వహణ, పర్యవేక్షణ మరియు సమీక్ష

16. 1 లాగ్ కలెక్షన్ స్కోప్, ఎంత తరచుగా చేయాలి, ఎక్కడ స్టోర్ చేయాలి అన్నదానిని ఫైనలైజ్ చేసే ముందు భాగస్వాములందరినీ సంప్రదించండి.

16.2 ఆడిట్ లాగ్స్‌ను ఒక క్రమబద్ధమైన పద్ధతిలో నిర్వహించి, సమీక్షించండి. దీని వల్ల ఏవైనా అటాక్‌ను కనుగొనడం, అర్థం చేసుకోవడం, రికవర్ కావడం సులభతరమౌతుంది.

16.3 ఒక సిస్టమ్‌లో యూజర్ యాక్షన్స్‌కు సంబంధించిన ఆడిట్ లాగ్స్‌ను క్యాప్చర్ చేయడంలో తగిన జాగ్రత్తలు తీసుకోవాలి. అవసరమైతే అలాంటి విషయాలలో ఫోరెన్సిక్ ఆడిటింగ్‌కు అవకాశం కల్పించాలి.

17 ఆడిట్ లాగ్ సెట్టింగ్స్

17.1 ప్రతి డివైజ్, సిస్టమ్స్ సాఫ్ట్‌వేర్, అప్లికేషన్ సాఫ్ట్‌వేర్ యొక్క లాగ్/ఆడిట్ ట్రయల్స్‌ను

క్యాప్చర్ చేసేందుకు సెట్టింగ్స్‌ను అమలు చేసి, ఎప్పటికప్పుడు వాటికి ఆమోదం తెలుపుతూ ఉండండి. లాగ్‌లను ప్రత్యేకంగా గుర్తించడానికి వాటిలో తేదీ, టైమ్ స్టాంప్, సోర్స్ అడ్రస్‌లు, డెస్టినేషన్ అడ్రస్‌లు, ప్రతి ప్యాకెట్ లేదా/మరియు ఈవెంట్ లేదా/మరియు ట్రాన్సాక్షన్‌లోని ఇతర ముఖ్యమైన సమాచారం ఉండేలా చూసుకోవాలి.

18. వల్నరబిలిటీ అసెస్‌మెంట్ మరియు పెనెట్రేషన్ టెస్ట్ మరియు రెడ్ టీమ్ ఎక్సర్‌సైజులు

18.1 క్రమం తప్పకుండా అన్ని క్రిటికల్ సిస్టమ్స్‌కు, మరీ ప్రత్యేకించి ఇంటర్నెట్‌ను ఉపయోగించుకునే సిస్టమ్స్‌కు వల్నరబిలిటీ అసెస్‌మెంట్ మరియు పెనెట్రేషన్ టెస్ట్ లను నిర్వహించండి.

18.2 గుర్తించిన వల్నరబిలీటలను బ్యాంకు రిస్క్ మేనేజ్‌మెంట్/ ట్రీట్‌మెంట్ ఫ్రేమ్‌వర్క్‌కు అనుగుణంగా వెంటనే పరిష్కరించండి. దీని వల్ల అలాంటివి దుర్వినియోగం కాకుండా ఉంటాయి.

18.3 పబ్లిక్ ఫేసింగ్ సిస్టమ్స్ మరియు ఇతర క్రిటికల్ అప్లికేషన్లు ఎదుర్కొనే పెనెట్రేషన్ టెస్ట్ లను కేవలం ప్రొఫెషనల్లీ క్వాలిఫైడ్ టీమ్‌లు మాత్రమే చేపట్టాలి.

18.4 VA/PTలో వెల్లడైన అంశాలను మరియు ఫాలో అప్ చర్యలను ఇన్ఫర్మేషన్ సెక్యూరిటీ/ ఇన్ఫర్మేషన్ టెక్నాలజీ ఆడిట్ టీమ్‌తో పాటు, సీనియర్/ టాప్ మేనేజ్‌మెంట్‌లు కూడా పర్యవేక్షిస్తుండాలి.

18.5 దాడి జరిగే అవకాశాలను, బిజినెస్ రిస్క్‌ను గుర్తించడానికి, రక్షణ వ్యవస్థ సామర్థ్యాన్ని, దాడి చేసే వారి లక్ష్యాలను, చర్యలను ప్రతిబింబించే వాతావరణంలో అప్పటికే ఉన్న రక్షణ వ్యవస్థను పరీక్షించడానికి రెడ్ టీములను ఉపయోగించుకోవచ్చు.

18.6 CERT-In మరియు IDRBT మొదలైన సంస్థల ఆధ్వర్యంలో నిర్వహించే సైబర్ డ్రిల్స్‌లో క్రమం తప్పకుండా, చురుకుగా పాల్గొనండి.

19. ఇన్సిడెంట్ రెస్పాన్స్ మరియు మేనేజ్‌మెంట్

సైబర్ సంఘటనలకు ప్రతిస్పందించడం :

19.1 బోర్డు/టాప్ మేనేజ్‌మెంట్ ఆమోదం పొందిన పూర్తిస్థాయి సమర్థమైన ఇన్సిడెంట్ రెస్పాన్స్ కార్యక్రమాన్ని అమలు చేయండి.

19.2 ఇన్సిడెంట్ రెస్పాన్స్ ప్రొసీజర్ ఎలా ఉండాలన్న దానిని రాసి ఉంచుకోండి. దీనిలో అలాంటి సంఘటనలు ఎదురైనప్పుడు సిబ్బంది/ఔట్‌సోర్స్ సిబ్బంది పాత్రను పేర్కొనాలి. పరిస్థితిపై

అవగాహన, పొటెన్షియల్/పోస్ట్ ఇంపాక్ట్ పరిస్థితులపై ఆధారపడి ప్రతిస్పందన వ్యూహాన్ని రూపొందించుకుంటారు. ఇందుకోసం భాగస్వాములందరితో నిరంతరం కమ్యూనికేషన్, కోఆర్డినేషన్ కలిగి ఉండాలి.

19.3 ప్రతిస్పందన వ్యూహాలను నిరంతరం మెరుగుపరచుకొనేందుకు వీలుగా నేర్చుకున్న పాఠాలను అమలు పరచడానికి ఒక వ్యవస్థను ఏర్పాటు చేసుకోండి.

సైబర్ సంఘటనల నుంచి రికవరీ :

19.4 బ్యాంక్ BCP/DR సామర్థ్యాలు బ్యాంకు యొక్క సైబర్ రెసీలియన్స్ లక్ష్యాలకు తగినంత గా, సమర్థంగా సహకరిస్తాయి. బ్యాంకులు వెంటనే సైబర్ దాడులు/ఇతర సంఘటనల నుంచి కోలుకుని, రికవరీ టైమ్ లక్ష్యాలను అనుగుణంగా క్రిటికల్ ఆపరేషన్స్‌ను తిరిగి సురక్షితంగా ప్రారంభించేట్లుగా వాటిని తయారు చేసుకోవాలి. అదే సయమంలో అవి ఆయా కార్యకలాపాల సెక్యూరిటీ మరియు డాటాను కూడా పరిరక్షించాలి.

19.5 అన్ని ఇంటర్‌కనెక్టెడ్ సిస్టమ్స్ మరియు నెట్ వర్క్ (వెండర్లు, పార్ట్‌నర్‌లతో పాటు) సామర్థ్యాలు మరియు అవి ఏ మేరకు సిద్ధంగా ఉన్నాయన్న దానిని బ్యాంకు రికరవరీ టైమ్ లక్ష్యాలకు అనుగుణంగా పరస్పర సహకార, సమన్వయ రెసీలియన్స్ టెస్ట్ ద్వారా పరీక్షించుకోవాలి.

19.6 ఈ టెస్టింగ్‌లో కస్టమర్లు, ఇతర అంతర్గత, బయటి భాగస్వాములు, రెప్యుటేషన్ మేనేజ్‌మెంట్‌కు క్రైసిస్ సమాచారం అందుతోందా లేదా అన్న దానిని కూడా పరీక్షించడం జరుగుతుంది. ఈ నేపథ్యంలో తగిన సామర్థ్యాన్ని రూపొందించుకుని, దానిని అమలు చేయడం జరుగుతుంది. ఈ క్రింది వాటిని పరిశీలించవచ్చు:

ఎ) సంఘటనలను, ఏ విధంగా కనిపెట్టారన్నదానిని, ఉద్యోగులు/వెండర్లు/కస్టమర్లు ఏ పద్ధ తుల్లో రిపోర్ట్ చేశారన్న దానిని, ఎన్ని రోజులకోసారి పర్యవేక్షిస్తున్నారన్న దానిని, విపత్తు

సమాచార సేకరణ/పంచుకోవడం, ప్రతి పరిస్థితి/సంఘటన నేపథ్యంలో ఆశించే ప్రతిస్పంద ను పేర్కొనండి. అలాంటి సంఘటనలను ఎదుర్కొనే సిబ్బందికి స్పష్టమైన పాత్రను, బాధ్యతల ను అప్పగించి, వారికి తెలియజేయండి. అలాంటి సిబ్బందికి ప్రత్యేక శిక్షణను ఇప్పించండి. సంఘటన సమీక్షను పోస్ట్ చేయండి. ఇన్సిడెంట్ రెస్పాన్స్ ప్లాన్‌లను క్రమం తప్పకుండా పరీక్షించండి.

డి) రాన్సమ్‌వేర్/సైబర్ ఎక్స్‌టార్షన్, డాటా డిస్ట్రక్షన్, DDOS మొద. అడ్వాన్స్‌డ్ దాడులకు ప్రతిస్పందించేందుకు వ్యూహాలను తయారు చేసుకుని వాటిని కమ్యూనికేట్ చేయండి.

ఇ) విపత్తుకు గురి అయిన సిస్టమ్‌లు/డివైజ్‌ల కంట్రోల్స్‌కు రక్షణ కల్పించడం, వాటిని క్వారంటైన్‌లో పెట్టడం లాంటి చర్యల ద్వారా సైబర్ అటాక్‌ల స్థాయిని అదుపులో వుంచవచ్చు.

ఎఫ్) సెక్యూరిటీ ఆఫరేషన్ సెంటర్, ఇన్సిడెంటల్ రెస్పాన్స్, డిజిటల్ ఫోరెన్సిక్‌ను కలిసి పని చేస్తూ బిజినెస్ డౌన్ టైంను తగ్గించేందుకు/సాధారణ స్థితికి చేరేందుకు ఒక పాలసీని, ఫ్రేమ్ వర్క్‌ను నెలకొల్పాలి.

20) రిస్క్ బేస్డ్ ట్రాన్సాక్షన్ మానిటరింగ్

20.1 ఫ్రాడ్ రిస్క్ మేనేజ్‌మెంట్ సిస్టమ్‌లో భాగంగా అన్ని డెలివరీ ఛానెల్స్‌లోను రిస్క్ బేస్డ్ ట్రాన్సాక్షన్ మానిటరింగ్ లేదా సర్వైలెన్స్ కార్యక్రమాన్ని అమలు చేయడం జరుగుతుంది.

20.2 బ్యాంకులు ప్రత్యామ్నాయ కమ్యూనికేషన్ మార్గాల ద్వారా కస్టమర్‌లకు చెందిన అన్ని చెల్లింపులు, లేదా కస్టమర్ పేర్కొన్న విలువకన్నా అధికంగా ఉన్న ఫండ్ ట్రాన్స్‌ఫర్ ట్రాన్సాక్షన్ ల గురించి కస్టమర్‌లకు నోటిఫై చేయాలి.

21) మెట్రిక్స్

21.1 భవిష్యత్ మరియు గడిచిపోయిన కాలంలో చర్యల కోసం, ఒక సమగ్రమైన మెట్రిక్ సముదాయాన్ని, ఉదా: ముఖ్య ప్రదర్శనా సూచికలు, ముఖ్య రిస్క్ సూచికలను అభివృద్ధి చేయండి.

21.2 మెట్రిక్‌లలో యాంటీ మాల్‌వేర్ సాఫ్ట్‌వేర్, వాటి అప్‌గ్రేడేషన్ పర్సంటేజ్, ప్యాచ్ లేటెన్సీ, యూజర్ అవేర్‌నెస్ ట్రెయినింగ్ పరిధి, వల్నరబిలిటీ సంబంధిత మెట్రిక్స్ మొద. ఉంటాయి.

22) ఫోరెన్సిక్స్

22.1 నెట్ వర్క్ ఫోరెన్సిక్/ఫోరెన్సిక్ ఇన్వెస్టిగేషన్స్/ DDOS మిటిగేషన్ సర్వీసులు స్టాండ్ బైలో ఉండేలా సహకారం/ఏర్పాట్లు చేసుకోండి.

22.2 CERT-In మరియు IDRBT మొదలైన సంస్థల ఆధ్వర్యంలో నిర్వహించే సైబర్ డ్రిల్స్ లో క్రమం తప్పకుండా, చురుకుగా పాల్గొనండి.

23) యూజర్/ఉద్యోగి/మేనేజ్‌మెంట్ అవగాహన

23.1 యూజర్లు/ఉద్యోగులు, వెండర్లు, భాగస్వాములకు సెక్యూరిటీ పాలసీల గురించి; కస్టమర్ సమాచార/డాటాతో పాటు బ్యాంక్ నెట్‌వర్క్/ఆస్తుల ఆమోదపూర్వక వినియోగం గురించి వివరించండి. సైబర్ సెక్యూరిటీ ప్రమాదాల గురించి, వారి స్థాయిలో తీసుకుంటున్న రక్షణపరమైన చర్యల గురించి వారికి బోధించండి.

23.2 ఏవైనా అనుమానాస్పద సంఘటలు జరిగినట్లయితే వెంటనే వాటిని ఇన్సిడెంట్ మేనేజ్‌మెంట్ టీమ్‌కు తెలియజేసేలా వారిని ప్రోత్సహించండి.

23.3 ముఖ్యమైన సిబ్బందికి (ఎగ్జిక్యూటివ్, ఆపరేషన్స్, సెక్యూరిటీ సంబంధిత అడ్మినిస్ట్రేషన్ /ఆపరేషన్ మరియు మేనేజ్‌మెంట్ పాత్రలు మొద.) అవగాహన/శిక్షణ కార్యక్రమాలు ఏర్పాటు చేయండి.

23.4 అవగాహన స్థాయిని ఎప్పటికప్పుడు అంచనా వేస్తుండండి.

23.5 సమర్థమైన సైబర్ సెక్యూరిటీ నిర్వహణ కోసం ఒక సామర్థ్య నిర్మాణ వ్యవస్థను నెలకొల్పండి. కొత్తగా ఉద్యోగంలో చేరిన వారి కోసం సైబర్ సెక్యూరిటీ అవగాహనా కార్యక్రమాలు ఏర్పాటు చేయండి. ప్రతి సంవత్సరం కిందిస్థాయి, మధ్యస్థాయి, పైస్థాయి మేనేజ్‌మెంట్ కోసం వెబ్ బేస్డ్ క్విజ్, శిక్షణను ఏర్పాటు చేయండి. (ఇటీవలి, గతంలో జరిగిన సైబర్ దాడులను ప రిశీలిస్తే సైబర్ శత్రువులు బ్యాంకు ఉద్యోగులను కూడా లక్ష్యంగా చేసుకున్నారని తెలుస్తోంది.)

23.6 ఎప్పటికప్పుడు వివిధ సాంకేతిక అభివృద్ధి గురించి, సైబర్ సెక్యూరిటీ సంబంధిత అభివృద్ధి గురించి బోర్డు మెంబర్ల అవగాహన పెంచుతుండండి.

23.7 ఐటీ రిస్క్/ సైబర్ సెక్యూరిటీ విషయంలో ఇటీవలి కాలంలో మెరుగైన పద్ధతుల గురించి బోర్డు సభ్యులకు శిక్షణ ఇవ్వవచ్చు. బోర్డు సభ్యులందరికీ కనీసం ఏడాదిలో ఒకసారి ఇలాంటి శిక్షణ ఇవ్వాలి.

24) కస్టమర్ విద్య, అవగాహన

24.1 సైబర్ సెక్యూరిటీ విపత్తులపై కస్టమర్లకు అవగాహన కల్పించండి.

24.2 ఫిషింగ్ మెయిల్స్/ఫిషింగ్ సైట్స్ గురించి ఫిర్యాదు చేసేలా కస్టమర్లను ప్రోత్సహించండి. అలా ఫిర్యాదు చేసినప్పుడు వెంటనే దానిపై చర్య తీసుకోండి.

24.3 కస్టమర్లు తమ లాగాన్ వివరాలు, పాస్‌వర్డ్‌లు మొదలైన వాటిని థర్డ్ పార్టీ వెండర్లతో పంచుకోవడం వల్ల ఎదురయ్యే ప్రమాదాల గురించి, దాని దుష్పరిణామాల గురించి వారికి