రిజర్వ్ బ్యాంక్ ఆఫ్ ఇండియా

RBI/2015-16/418
DBS.CO/CISTE/BC.11/33.01.001/2015-16

జ్యేష్ఠ 12, 1938 (శక)

జూన్ 2, 2016

To

ఛైర్మన్/మేనేజింగ్ డైరెక్టర్ /చీఫ్ ఎగ్జిక్యూటివ్ ఆఫీసర్

అన్ని షెడ్యూల్డ్ కమర్షియల్ బ్యాంకులు (ప్రాంతీయ గ్రామీణ బ్యాంకులు తప్పించి)

డియర్ మేడమ్/సర్,

బ్యాంకులలో సైబర్ సెక్యూరిటీ ఫ్రేమ్ వర్క్

పరిచయం

1. ఇటీవలి కాలంలో బ్యాంకులు, వాటితో సంబంధమున్న ఇతర సంస్థలలో ఇన్ఫర్మేషన్ టెక్నాలజీ వినియోగం అతి వేగంగా పెరిగి, అది ఇప్పుడు వాటి కార్యకలాపాల నిర్వహణలో ఒక అంతర్భాగంగా మారింది. రిజర్వ్ బ్యాంక్ ఏప్రిల్ 29, 2011న జారీ చేసిన సర్క్యులర్ DBS.CO.ITC.BC.No.6/31.02.008/2010-11 ద్వారా ఇన్ఫర్మేషన్ టెక్నాలజీ, ఎలెక్ట్రానిక్ బ్యాంకింగ్, టెక్నాలజీ రిస్క్ మేనేజ్మెంట్ మరియు సైబర్ ఫ్రాడ్స్ (జి.గోపాలకృష్ణ కమిటీ) పై మార్గదర్శకాలను విడుదల చేసింది. వాటిలో బ్యాంకులు అమలు చేస్తున్న విధానాలు స్థిరంగా ఉండరాదనీ, మారుతున్న రోజువారీ పరిణామాలు, కొత్త సమస్యలను దృష్టిలో పెట్టుకుని నిరంతరం వాటిని మెరుగుపరచుకుంటూ, మార్పులు చేసుకోవాల్సి ఉంటుందనీ పేర్కొన్నారు.

2. నాటి నుంచి బ్యాంకులలో టెక్నాలజీని ఉపయోగించడం వేగం పుంజుకుంది. మరోవైపు, ఇటీవలి కాలంలో సైబర్ నేరాలు/అక్రమాల సంఖ్య, వాటి ప్రభావం, తీవ్రత బాగా పెరిగిపోయింది. మరీ ప్రత్యేకించి

బ్యాంకులతో పాటు ఇతర ఆర్థిక సంస్థలలో ఇది మరీ ఎక్కువైంది. దీని వల్ల బ్యాంకులలో ఒక గట్టి సైబర్ సెక్యూరిటీ వ్యవస్థను తయారు చేసుకుని, నిరంతరం జాగరూకతగా ఉండాల్సిన అవసరం ఏర్పడింది. బ్యాంకింగ్ రక్షణ వ్యవస్థ బలహీనంగా ఉండడం, బ్యాంకింగ్ వ్యవస్థలో ఇన్ఫర్మేషన్ టెక్నాలజీ ఇంకా అభివృద్ధి చెందే దశలో ఉండడం, పెరుగుతున్న పరిమాణం/వేగం వల్ల బ్యాంకింగ్ వ్యవస్థకు ఎదుర వుతున్న రిస్కులను తగ్గించడానికి దాని రక్షణ వ్యవస్థను మరింత పెంచుకోవాలి. ఇందుకోసం బ్యాంకులు ఏవైనా ప్రతికూల సంఘటనలు జరిగినపుడు వెంటనే ప్రతిస్పందించేలా మేనేజ్ మెంట్ అండ్ రిస్క్ ఫ్రేమ్ వర్క్ ను సిద్ధం చేసుకుని ఉండాలి.

బోర్డు ఆమోదించిన సైబర్ సెక్యూరిటీ పాలసీ యొక్క అవసరం

3. ప్రస్తుతం పెరిగిపోతున్న సైబర్ నేరాల దృష్ట్యా, వాటిని అరికట్టడానికి బ్యాంకులు వెంటనే తమ బోర్డు ఆమోదించిన సైబర్ సెక్యూరిటీ పాలసీని అమలు చేయాలి. ఇందుకోసం బ్యాంకులు తమ అంగీకారాన్ని వీలైనంత తొందరగా, సెప్టెంబర్ 30, 2016 లోపల రిజర్వ్ బ్యాంక్ యొక్క సైబర్ సెక్యూరిటీ అండ్ ఇన్ఫ ర్మేషన్ టెక్నాలజీ ఎగ్జామినేషన్ సెల్, డిపార్ట్‌మెంట్ ఆఫ్ బ్యాంకింగ్ సూపర్ విజన్, రిజర్వ్ బ్యాంక్ ఆఫ్ ఇండియా, సెంట్రల్ ఆఫీస్, వరల్డ్ ట్రేడ్ సెంటర్ -I, ఫోర్త్ ఫ్లోర్, కఫీ పెరేడ్, ముంబై - 400005 అన్న చిరునామాకు తెలియజేయాలి.

ఈ వ్యూహంలో ఈ క్రింది అంశాలపై స్థూలంగా చర్చించాలి.

సైబర్ సెక్యూరిటీ పాలసీ విస్తృత ఐటీ పాలసీ/ IS సెక్యూరిటీ పాలసీకి భిన్నంగా, ప్రత్యేకంగా ఉండాలి

4. బ్యాంకు మొత్తం ఒక సైబర్ సురక్షిత వాతావరణం ఏర్పాటయ్యేందుకు వీలుగా, వాటి సెక్యూరిటీ పాల సీ విస్తృత ఐటీ పాలసీ/ IS సెక్యూరిటీ పాలసీకి భిన్నంగా, ప్రత్యేకంగా ఉండాలి. తద్వారా అది సైబర్ నేరాల నుంచి రిస్కులను హైలైట్ చేస్తూ, ఆ సమస్యలను పరిష్కరించడం లేదా వాటి తీవ్రతను తగ్గించ డానికి వీలవుతుంది.

5. పరిమాణం, పద్ధతులు, సాంకేతిక క్లిష్టత, డిజిటల్ ఉత్పత్తులు, భాగస్వాములు, నేర దృక్పథం బ్యాంకు బ్యాంకుకూ మారుతుంటాయి. అందువల్ల అంతర్గతంగా ఉన్న ప్రమాదాలను పసిగట్టి సైబర్ సెక్యూరిటీ వ్యవస్థ కోసం తగిన భద్రతాపరమైన ఏర్పాట్లు చేసుకోవాలి. అంతర్గతంగా ఉన్న ప్రమాదాలను గుర్తించి, అంచనా వేసే క్రమంలో బ్యాంకులు తాము అనుసరిస్తున్న సాంకేతిక విజ్ఞానాన్ని, అవి వ్యాపార మరియు నియంత్రణ వ్యవస్థకు లోబడి ఉన్నాయా, అవి ఏర్పరుచుకున్న సంబంధాలు, డెలివరీ ఛానెల్స్, ఆన్ లైన్/మొబైల్ ఉత్పత్తులు, సాంకేతిక సేవలు, వ్యవస్థాపరమైన అలవాట్లు మరియు అంతర్గత, బాహ్య ప్రమాదాలను దృష్టిలో పెట్టుకోవాలి. అంతర్గత ప్రమాదాల తీవ్రతను బట్టి, బ్యాంకులు వాటిని తక్కువ, మధ్యరకం, ఎక్కువ, చాలా ఎక్కువ అన్న రకాలుగా వర్గీకరించడమో లేదా అలాంటివి మరో రకం వర్గీకరణ చేయడమో చేయాలి. అంతర్గత ప్రమాదాలను అంచనా వేసే క్రమంలో బిజినెస్ కాంపోనెంట్‌లో ఎంత మేరకు రిస్క్ ఉందన్న దానిని కూడా పేర్కొనవచ్చు. కంట్రోల్ లను అంచనా వేసే క్రమంలో బోర్డు చేసే తప్పులు, విధానాలు, పద్ధతులు, అనుభవపూర్వక మరియు అర్హత కలిగిన వన రులతో కూడిన సైబర్ రిస్క్ మేనేజ్ మెంట్ వ్యవస్థ, శిక్షణ మరియు పద్ధతులు, నేరం జరిగే అవకాశాల ను అంచనా వేసే వ్యవస్థ, పర్యవేక్షణ మరియు బ్యాంకుల ద్వారా సేకరించిన నేర ఇంటలిజెన్స్ స మాచారాన్ని విశ్లేషించడం, సమాచారాన్ని పంచుకునే ఏర్పాట్లు (తోటి బ్యాంకులు మరియు IDRBT/RBI/CERT-In వంటి వాటితో) నివారించగలిగే, కనిపెట్టగలిగే, సరిదిద్దగలిగే సైబర్ సెక్యూరిటీ నియంత్రణ, వెండర్ మేనేజ్ మెంట్, ఇన్సిడెంట్ మేనేజ్ మెంట్ మరియు ప్రతిస్పందలను రేఖామాత్రంగా పేర్కొనాలి.

నిరంతర నిఘా కొరకు ఏర్పాట్లు

6. నిర్ణీత కాలవ్యవధిలో నేరాలు జరిగే అవకాశాల కోసం అప్పుడప్పుడూ పరీక్షలు చాలా అవసరం. సైబర్ దాడులు ఎలాంటి సమయంలోనైనా జరగవచ్చు. మనం ఊహించని విధానంలో జరగవచ్చు. అందువల్ల వీలైనంత తొందరగా ఒక SOC (సెక్యూరిటీ ఆపరేషన్స్ సెంటర్ ను) ఏర్పాటు చేసుకోవడం చాలా అవసరం, ఇప్పటివరకు ఏర్పాటు చేసుకోనట్లయితే. అంతే కాకుండా ఈ సెంటర్ నిరంతరం

నిఘాతో ఉంటూ, ఎప్పటికప్పుడు తాజాగా ఉత్పన్నమయ్యే సైబర్ నేరాల గురించి తెలుసుకుంటూ ఉండాలి.

ఐటీ నిర్మాణ వ్యవస్థ భద్రతాపరమైన అనుకూలత కలిగి ఉండాలి.

7. భద్రతా ఏర్పాట్లు నిరంతరం అప్రమత్తతతో వ్యవహరించేలా ఐటీ వ్యవస్థను రూపొందించుకోవాలి. ఐటీ సబ్ కమిటీ ఈ ఐటీ వ్యవస్థను సమీక్షించి, అవసరమైతే దశలవారీగా రిస్క్ మేనేజ్ మెంట్‌కు అనుకూలంగా అప్ గ్రేడ్ చేసుకోవాలి. బ్యాంకు తీసుకునే రిస్క్ కాస్ట్ / పొటెన్షియల్ కాస్ట్ ట్రేడ్ ఆఫ్ నిర్ణ యాలు రాతపూర్వకంగా నమోదు చేయాలి. దీని వల్ల భవిష్యత్తులో ఎలాంటి సూపర్ విజన్ అవసరం అన్నదానిపై ఒక అవగాహన ఏర్పడుతుంది.

8. అనుంబంధం- I లో ఒక సూచనాత్మక, సంపూర్ణమైన కాకుండా, కనీస, ప్రాథమిక సైబర్ సెక్యూరిటీ మరియు నియంత్రతణ వ్యవస్థను పేర్కొనడం జరిగింది. బ్యాంకులు రోజువారీ కార్యకలాపాలలో ఎదుర య్యే సైబర్ నేరాలను ఎదుర్కొనడానికి, అరికట్టడానికి ఒక సెక్యూరిటీ ఆపరేషన్స్ సెంటర్ ను ఏర్పాటు చేసుకోవడంలో చురుకుగా వ్యవహరించాలి. SOC ఎలా ఉండాలన్నదానిపై అనుబంధం - 2లో కొన్ని సూచనలు చేయడం జరిగింది.

నెట్ వర్క్ మరియు డాటాబేస్ సెక్యూరిటీని ఎలాంటి లోటుపాట్లు లేకుండా సమగ్రంగా రూపొందించండి.

9. ఇటీవలి కాలంలో జరిగిన పరిణామాలు, అన్ని బ్యాంకులలో నెట్ వర్క్ సెక్యూరిటీని సమీక్షించాల్సిన అవసరాన్ని నొక్కి చెబుతున్నాయి. దీనికి తోడు, వ్యాపార కార్యకలాపాల కోసం చాలాసార్లు నెట్ వర్క్ /డాటాబేస్ కనెక్షన్లను ఒక నిర్ణీత సమయంలో అనుమతించడం జరుగుతోంది. అయితే నిర్లక్ష్యం కార ణంగా వాటిని మూసివేయడం మాత్రం జరగడం లేదు. దీని వల్ల సైబర్ దాడులు/నేరాలు జరిగే అవకాశం పెరుగుతోంది. అందువల్ నెట్‌వర్క్ మరియు డాటాబేస్లకు అనధికారికంగా యాక్సెస్ పొందడాన్ని నివారించాలి. ఒకవేళ అనుమతి ఇచ్చినా, ఒక క్రమబద్ధమైన పద్ధతిలో ఉండాలి. దానిని తూ.చ. తప్పకుండా పాటించాలి. అలాంటి నెట్‌వర్క్ మరియు డాటాబేస్ ల విషయంలో బాధ్యతలను స్పష్టంగా నిర్వచించాలి. ఆ బాధ్యత తప్పకుండా ఆ బ్యాంకు అధికారులకు అప్పగించాలి.

కస్టమర్ సమాచార పరిరక్షణ

10. బ్యాంకులు సాఫీగా పని చేయడానికి, తమ కస్టమర్లకు మెరుగైన డిజిటల్ ఉత్పత్తులను అందించ డానికి చాలా ఎక్కువగా సాంకేతిక పరిజ్ఞానంపై ఆధారపడతాయి. ఈ క్రమంలో అవి అనేక వ్యక్తిగత, సెన్సిటివ్ సమాచారాన్ని సేకరిస్తాయి. ఆ సమాచార యజమానులుగా బ్యాంకులు తమ వద్ద లేదా కస్ట మర్ల వద్ద లేదా థర్డ్ పార్టీ వెండర్ల వద్ద స్టోర్ చేసిన/లేదా చలనంలో ఉన్న సమాచార గోప్యతను, సమగ్ర తను పరిరక్షించాలి. తమ వద్ద ఉన్న సమాచార గోప్యతను ఎట్టి పరిస్థితులలోనూ బహిర్గతం చేయ రాదు. ఇందుకోసం బ్యాంకులు తమ డాటా/ఇన్ఫర్మేషన్ లైఫ్ సైకిల్‌లో అవసరమైన వ్యవస్థను, విధానాలను రూపొందించుకోవాలి.

సైబర్ క్రైసిస్ మేనేజ్ మెంట్ ప్లాన్

11. వెనువెంటనే ఒక సైబర్ క్రైసిస్ మేనేజ్ మెంట్ ప్లాన్ (CCMP)ను రూపొందించి, దానిని బోర్డు ఆమోదిత వ్యూహంగా అమలుపరచాలి. సైబర్ రిస్కులు ఇతర రిస్కులకన్నా భిన్నమైనవి. అందువల్ల సాంప్రదాయ BCP/DR ఏర్పాట్లు ఇక్కడ సరిపోవు. సైబర్ రిస్కులో ఉన్న సూక్ష్మమైన తేడాలను దృష్టిలో పెట్టుకుని ఎప్పటికప్పుడు జాగ్రత్తగా గమనిస్తుండాలి. ప్రభుత్వానికి చెందిన CERT-In (కంప్యూటర్ ఎమర్జెన్సీ రెస్పాన్స్ టీమ్ - ఇండియా, ఇది ప్రభుత్వ సంస్థ) సైబర్ సెక్యూరిటీ ఏర్పాటులో ముఖ్య పాత్రను పోషిస్తూ, ప్రోయాక్టివ్, రియాక్టివ్ సేవలు అందిస్తూ, మార్గదర్శకాలు రూపొందిస్తూ, ఆర్థిక రంగంతో పాటు అన్ని రంగాలలో నేర సమాచార వ్యవస్థను ఏర్పాటు చేసుకొనేలా చురుకైన పాత్ర ను నిర్వహిస్తోంది. CERT-In ఒక జాతీయ సైబర్ క్రైసిస్ మేనేజ్ మెంట్ ప్లాన్ మరియు సైబర్ సెక్యూరిటీ అసెస్ మెంట్ ఫ్రేమ్ వర్క్ ను కూడా రూపొందించింది. CCMPని రూపొందించే సమయంలో CERT-In మార్గదర్శకాలను రెఫర్ చేయవచ్చు.

12. CCMP ఈ క్రింది నాలుగు అంశాలను దృష్టిలో పెట్టుకోవాలి: (1) పరిశోధన (2) ప్రతిస్పందన (3) రికవరీ (4) నిలువరింపు. బ్యాంకులు సైబర్ దాడులను అరికట్టడానికి, వెంటనే సైబర్ చొరబాట్లను గుర్తించడానికి, తద్వారా ఫాలౌట్‌ను అరికట్టడానికి/నియంత్రించడానికి/ప్రతిస్పందించడానికి అవసర

మైన రక్షణ వ్యవస్థను ఏర్పాటు చేసుకోవాలి. బ్యాంకులు జీరో డే అటాక్స్, గుర్తు తెలియని ప్రదేశాల నుంచి జరిగే దాడులు, టార్గెట్ దాడులులాంటి వాటిని ఎదుర్కొనేందుకు సిద్ధంగా ఉండాలి. సేవల నిరాకరణ, అస్తవ్యస్థ సేవల నిరాకరణ (DDoS), ర్యాన్సమ్ వేర్ /క్రిప్టోవేర్, డిస్ట్రక్టివ్ మాల్ వేర్; స్పామ్, ఈమెయిల్ ఫిషింగ్, స్పియర్ ఫిషింగ్, వేలింగ్, విషింగ్ ఫ్రాడ్స్, డ్రైవ్-బై డౌన్‌లోడ్స్, బ్రౌజర్ గేట్ వే ఫ్రాడ్, ఘోస్ట్ అడ్మినిస్ట్రేటర్ ఎక్స్ ప్లాయిట్స్, ఐడెంటిటీ ఫ్రాడ్స్, మెమరీ అప్ డేట్ ఫ్రాడ్స్, పాస్ట్ వర్డ్ సంబంధిత ఫ్రాడ్స్, బిజినెస్ ఈమెయిల్ మోసాలలాంటి అనేక సైబర్ నేరాలను అరికట్టడానికి అవసరమైన చర్యలను బ్యాంకులు తీసుకోవాలి.

సైబర్ భద్రతా ఏర్పాట్ల సూచికలు

13. బ్యాంకుల వద్ద ఉన్న సైబర్ రక్షణ వ్యవస్థ ఎంత మేరకు సమర్థంగా పని చేస్తుంది? సైబర్ నేరాలను ఎదుర్కొనడానికి/అరిక్టడడానికి అవి సరిపోతాయా? అన్నది తెలుసుకోవడానికి బ్యాంకులు ప్రమాద/రిస్కు నివారణ సూచికలను తయారు చేసుకోవడం మేలు. ఈ సూచికలను అర్హత, సమర్థత కలిగిన స్వతంత్ర ప్రొఫెషనల్స్ ద్వారా సమగ్రంగా పరీక్షించాలి. ఉద్యోగులతో పాటు భాగస్వాముల అవగాహన పెంచడం కూడా దీనిలో భాగంగా చేపట్టాలి.

సైబర్ సెక్యూరిటీ సంఘటనల సమాచారాన్ని RBIతో పంచుకోవడం

14. బ్యాంకులు తమకెదురయ్యే సైబర్ సంఘటనలను పంచుకోవడానికి చాలా సందేహిస్తుంటాయని గుర్తించడం జరిగింది. అయితే, అంతర్జాతీయ అనుభవాల ప్రకారం, అలాంటి సంఘటలను, మేలైన పద్ధతులను తోటి బ్యాంకులతో పంచుకోవడం వల్ల సైబర్ నేరాలను కట్టడి చేయవచ్చు.

బ్యాంకులు తమకెదురయ్యే అన్ని సైబర్ సెక్యూరిటీ సంఘటనలను (అవి విజయవంతమై ఉండవచ్చు లేదా విఫల యత్నం కావచ్చు) రిజర్వ్ బ్యాంకుకు తెలియజేయాలని మళ్లీమళ్లీ చెప్పడం జరిగింది. బ్యాంకులు IDRBT సమన్వయంతో నిర్వహించే CSIOల ఫోరంలో చురుకుగా పాల్గొనేందుకు, తమ బ్యాంకులలో జరిగిన సంఘటనలను వెంటనే ఐడీఆరబీటీ ఏర్పాటు చేసిన ఇండియన్ బ్యాంక్స్ - సెంటర్ ఫర్ అనాలిసిస్ అండ్ రిస్క్స్ (IB-CARTకు) తెలియజేసేలా వాటిని ప్రోత్సహిస్తున్నారు. ఇలాంటి చర్య

ల వల్ల బ్యాంకులు ఒక సమిష్టి నేర నిరోధక వ్యవస్థను ఏర్పాటు చేసుకొని, సకాలంలో స్పందించే, మెరుగైన సైబర్ సెక్యూరిటీ వ్యవస్థను ఏర్పాటు చేసుకోవడానికి వీలవుతుంది.

సూపర్ వైజరీ రిపోర్టింగ్ ఫ్రేమ్ వర్క్

15. సైబర్ సంఘటనలతో పాటు ఇతర భద్రతా సంఘటనలకు చెందిన సంగ్రహ సమాచారాన్ని మరియు ఇతర వివరాలను సేకరించాలని నిర్ణయించడం జరిగింది. అనుబంధం-3లో ఇచ్చిన ఫార్మాట్ లో బ్యాంకులు వెంటనే అలాంటి సమాచారాన్ని నివేదించాలి.

సంసిద్ధతా లోటుపాట్లను వెంటనే RBI దృష్టికి తీసుకుపోవాలి

16. కంట్రోల్స్ లోని లోటుపాట్లను ముందుగానే గుర్తించి, ఐటీ సబ్ కమిటీ ఆఫ్ ద బోర్డ్ మరియు బోర్డ్ యొక్క మార్గదర్శకాలకు అనుగుణంగా వెంటనే పరిష్కార చర్యలు చేపట్టాలి. గుర్తించిన లోటుపాట్లను, వాటి నియంత్రణకు చేపట్టాల్సిన చర్యలు, వాటి ప్రభావం, ప్రతిపాదిత నియంత్రణలు/చర్యలు చేపట్టడానికి ఏర్పరచిన టైమ్ లైన్స్ తో కూడిన లక్ష్యాలు, అవి ఏ మేరకు ఆచరణ సాధ్యమన్నది తెలుసుకోవడానికి బ్యాంకులు తాము ఉపయోగించే/ప్రతిపాదించే ప్రమాణాలు తదితర వివరాలను సైబర్ సెక్యూరిటీ అండ్ ఇన్ఫర్మేషన్ టెక్నాలజీ ఎగ్జామినేషన్ (CSITE) సెల్ ఆఫ్ డిపార్ట్ మెంట్ ఆఫ్ బ్యాంకింగ్ సూపర్ విజన్, సెంట్రల్ ఆఫీస్ కు చీఫ్ సెక్యూరిటీ ఇన్ఫర్మేషన్ ఆఫీసర్ ద్వారా జులై 31, 2016లోపు పంపించాల్సి ఉంటుంది.

వ్యవస్థాపరమైన ఏర్పాట్లు

17. సెక్యూరిటీ లోటుపాట్లను గుర్తించి, వాటిపై తగిన శ్రద్ధ పెట్టి, వాటిని పై అధికారుల దృష్టికి తీసుకెళ్లి వేగంగా చర్యలు తీసుకునేలా బ్యాంకులు తమ సంస్థాగత ఏర్పాట్లను సమీక్షించుకోవాలి.

సైబర్ సెక్యూరిటీపై భాగస్వాములు/ పైస్థాయి మేనేజ్ మెంట్/ బోర్డు అవగాహన

18. ఒక సైబర్ - సురక్షిత వాతావరణాన్ని ఏర్పరచడానికి, సైబర్ నేరాలను నియంత్రించడానికి మొత్తం సంస్థలోని అందరికీ నిబద్ధత అవసరం. ఇందుకోసం అన్ని స్థాయిల సిబ్బందికీ ఒక ఉన్నతస్థాయి అవ

గాహన ఉండాలి. పైస్థాయి మేనేజ్ మెంట్ మరియు బోర్డుకు కూడా నేరాలలోని చిన్న చిన్న తేడాల గురించి అవగాహన ఉండాలి. బ్యాంకులు తమ కస్టమర్లు, వెండర్లు, సర్వీస్ ప్రొవైడర్లు, ఇతర భాగస్వాములకు బ్యాంకు యొక్క సైబర్ సెక్యూరిటీ వ్యవస్థ లక్ష్యాలను అర్థమయ్యేట్లు చేయడంలో చురుకైన పాత్ర పోషించాలి. వాటి అమలు లేదా పరీక్షలో వారు తగిన విధంగా ప్రతిస్పందిచేలా చూడాలి. సైబర్ దాడులపై భాగస్వాములకు (కస్టమర్లు, ఉద్యోగులు, వెండర్లు మొద.) తగిన అవగాహన ఉంటే, బ్యాంకులు సైబర్ దాడులను ఎదుర్కోనడం సులువవుతుంది. ఈ దిశగా బ్యాంకులు తగిన చర్యలు తీసుకోవాలని వాటికి సూచించడమైనది. అదే సమయంలో బ్యాంకులకు చెందిన బోర్డ్ ఆఫ్ డైరెక్టర్లు మరియు పైస్థాయి మేనేజ్ మెంట్ తమ సైబర్ సెక్యూరిటీ ఏర్పాట్లను మరింత వేగవంతం చేయాలి. బ్యాంకులు ఈ దిశగా వెంటనే చర్యలు తీసుకోవాలి.

ఈ సర్క్యులర్ కాపీని వచ్చే సమావేశంలో బోర్డ్ ఆఫ్ డైరెక్టర్లకు సమర్పించాలి.

మీ విశ్వసనీయులు,

(ఆర్. రవి కుమార్)

చీఫ్ జనరల్ మేనేజర్

Encl: పైన పేర్కొన్నవి

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 అటాచబుల్స్ 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 నిర్దిష్టంగా అథరైజ్ చేసి, దాని వినియోగాన్ని పేర్కొని, ఎంత కాలం ఉపయోగిస్తార నే విష యాన్ని పేర్కొంటే తప్ప బ్యాంకింగ్ ఎన్విరాన్‌మెంట్‌లో తొలగించదగిన డివైజెస్ /మీడియాను అనుమ తించరాదన్న 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.), సర్వ ర్లు (ఆపరేటింగ్ సిస్టమ్స్, డాటా బేసెస్, అప్లికేషన్స్ మొద.), వెబ్/ఇంటర్నెట్ గేట్ వేస్, ఈమెయిల్ గేట్‌వేస్, వైర్‌లెస్ నెట్‌వర్క్స్, SMS సర్వర్లు మొదలైన వాటికి; సెంట్రలైజ్డ్ మేనేజ్ మెంట్ మరియు పర్యవేక్షణ కొరకు బిహేవియరల్ 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 పైనలైజ్ 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 పెనెట్రేషస్ 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 వ ర్క్‌ను 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

వివరించండి.

ఆపరేషనలైజింగ్ సైబర్ సెక్యూరిటీ ఆపరేషన్ సెంటర్ నెలకొల్పడం (C-SOC.)

పరిచయం

1- గత కొంతకాలంగా భారత బ్యాంకింగ్ పరిశ్రమ సాంకేతికపరంగా ఎంతో పరిణితి చెందుతూ, ప్రస్తుతం కస్టమర్లకు వినూత్నమైన సేవలను అందిస్తోంది. కస్టమర్లకు బ్యాంకింగ్ సేవలు అన్ని వేళలా, ఎలాంటి విరామం లేకుండా అందుతున్నాయి. కస్టమర్లు ఇంటర్నెట్, మొబైల్ కనెక్టివిటీ ద్వారా ఈ సేవలను పొందగలుగుతున్నారు. ఆర్థిక లావాదేవీల విషయంలో భద్రత అనేది అన్నిటికన్నా ముఖ్యమైనది. అందువల్ల RBI నిర్దిష్టమైన అప్లికేషన్లు, సేవలకు సంబంధించి సెక్యూరిటీ మరియు ఆపరేషన్స్‌పై ఎప్పటికప్పుడు మార్గదర్శకాలను జారీ చేస్తుంటుంది.

2 - బ్యాంకింగ్ పరిశ్రమలో ప్రత్యేకించి ఇంటర్నెట్‌ను ఉపయోగించుకుంటున్న అప్లికేషన్లు, ప్రస్తుతం అందుతున్న, భవిష్యత్తులో అందబోయే సేవల వైపు దృష్టి సారించాల్సిన అవసరం చాలా ఉంది. వాటి విషయంలో అన్ని అప్లికేషన్లు, సర్వీసుల కోసం సైబర్ సెక్యూరిటీ మార్గదర్శకాలను విడుదల చేయాలి.

3 - తగినటువంటి, తక్కువ ఖర్చయ్యే సమర్థమైన టెక్నాలజీ పరికరాలను ఉపయోగించుకుంటూ, ఉత్తమ పద్ధతులపై ఆధారపడిన పాలసీలు, నియమాలను అనుసరిస్తూ, సాంకేతికంగా సమర్థులైన, నిపుణులైన సిబ్బంది ద్వారా నిరంతర పర్యవేక్షణ కలిగిన వ్యవస్థను ఏర్పాటు చేసుకోవడం బ్యాంకింగ్ పరిశ్రమ ముందున్న తక్షణ కర్తవ్యం. సైబర్ సెక్యూరిటీ పాలసీపై ప్రభుత్వం ఎప్పటికప్పుడు జారీ చేసే మార్గదర్శకాలను అనుసరించడం, ముఖ్యమైన సమాచార రక్షణ, ఇన్ఫర్మేషన్ టెక్నాలజీ చట్టాన్ని అనుసరించడమన్నవి చాలా ముఖ్యమైనవి.

సైబర్ సెక్యూరిటీ ఆఫరేషన్స్ సెంటర్ ఏర్పాటు విషయంలో గవర్నెన్స్, టెక్నాలజీ, ఆపరేషనల్, ఔట్‌సోర్సింగ్, లీగల్ అంశాలను చెందిన సమస్యలను పరిష్కరించడం చాలా ముఖ్యం.

4 - C-SOC ఏర్పాటు చేసే సందర్భంలో ఈ క్రింది అంశాలను దృష్టిలో పెట్టుకోవడం అవసరం. ఇవి కేవలం సూచన మాత్రమే, సంపూర్ణం కాదు.

గవర్నెన్స్ అంశాలు:

- విపత్తు ఇంటలిజెన్స్‌పై టాప్ మేనేజ్‌మెంట్/బోర్డు వివరణ
- డాష్ బోర్డులు మరియు పైవిచారణ
- విధానాలు, వాటి పరిమాణం, వాటి అమలు (కీ మెట్రిక్స్, రిపోర్టింగ్ స్ట్రక్చర్, ఏది నివేదించాలో పేర్కొనండి)
- భాగస్వాములకు సమాచారం అందజేయండి, భాగస్వాములు పాల్గొనడం

సైబర్ SOC : గమనించాల్సిన అంశాలు:

1- గత కొన్నేళ్లుగా నివారక విధానాన్ని అనుసరిస్తూ వస్తున్న సాంప్రదాయ సెక్యూరిటీ వ్యవస్థలు ప్రతికూల స్వభావం కలిగినట్టివి. దాడుల గురించి ముందస్తు సమాచారం తెలిసినప్పుడు ఎదురయ్యే సమస్యలను అవి పరిష్కరించగలవు. అయితే గత కొంతకాలంగా విపత్తులు సంభవించే అవకాశాలు, పరిస్థితుల విస్తృతి చాలా పెరిగింది. అందువల్ల వాటిని పరిష్కరించే విషయంలో - సంఘటన జరిగిన తర్వాత ప్రతిస్పందించడం కన్నా సంఘటన జరగడానికి ముందే చర్యలు తీసుకునే దృక్పథం కలిగి ఉండడం ముఖ్యం. తెలియని విపత్తులను కూడా పరిష్కరించగలిగేలా ఉండాలి. ఉదాహరణకు జీరో డే దాడులు, ఎలాంటి సూచనలూ లేని దాడుల గురించి దృష్టిలో పెట్టుకోవడం అవసరం.

2- విపత్తులను వెంటనే గుర్తించడానికి; తగిన డాటా, పరికరాల ద్వారా విశ్లేషించడానికి, వేగంగా ప్రతిస్పందించడానికి సైబర్ SOC ముందస్తు పర్యవేక్షణ మరియు మేనేజ్‌మెంట్ సామర్థ్యాలను దృష్టిలో పెట్టుకోవడం అవసరం.

3- ప్రస్తుతం సెక్యూరిటీ ఆపరేషన్లను పర్యవేక్షిస్తున్న వ్యవస్థ ఏర్పాటు చేసిన ప్రొడక్ట్ యొక్క ప్రతి పాయింట్ నుంచి లాగ్‌లను సేకరిస్తుంది, లాగ్‌లను భద్రపరిచి ప్రాసెస్ చేస్తుంది, తగిన SIEM పరికరాల ద్వారా పరస్పర సంబంధాలను నిర్వచిస్తుంది, SIEM స్క్రీన్‌లను నిరంతరం పర్యవేక్షిస్తుంది. ఏదైనా అనుమానాస్పదంగా తోచినట్లయితే వెంటనే హెచ్చరికలు జారీ చేస్తుంది.

4. సైబర్ SOCలో భాగంగా అవసరమైన వ్యవస్థను ఏర్పాటు చేయడానికి ఈ క్రింది అంశాలను పరిశీలించాలి:

దాడులకు మూల కారణాలను కనుగొనే విధానాలు, వాటిని గుర్తించిన విభాగాల్లోకి వర్గీకరించడం, అదే విధమైన దాడులు జరగకుండా వాటికి పరిష్కారాలు కనుగొనడం.

ప్రైవసీని సాధించడానికి సంఘటనను పరిశోధించడం, ఫోరెన్సిక్స్, డీప్ పాకెట్ అనాలసిస్ అవసరం.

డైనమిక్ బిహేవియర్ అనాలసిస్ - ప్రాథమిక స్టాటిక్ మరియు డైనమిక్ సమీక్ష, ఇండికేటర్స్ ఆఫ్ కాంప్రమైజ్ (IOC) సేకరణ

మంచి డ్యాష్ బోర్డ్‌తో విశ్లేషణ; ఐపీల భౌగోళిక ప్రదేశాన్ని చూపించడం

కౌంటర్ రెస్పాన్స్ మరియు హనీస్పాట్ సర్వీసులు

SOC నుంచి ఆశిస్తున్నవి:

- క్రిటికల్ బిజినెస్ మరియు కస్టమర్ డాటా/సమాచారను రక్షించే సామర్థ్యం; అంతర్గత మార్గ దర్శకాలు, దేశంలోని చట్టాలు, నియంత్రణకు లోబడి ఉండాలి.
- రియల్ టైమ్/నియర్ రియల్ టైమ్‌కు సంబంధించిన సమాచారాన్ని అందించగలిగే సామర్థ్యం; బ్యాంకు యొక్క భద్రతపై లోతుగా పరిశీలన
- సెక్యూరిటీ ఆపరేషన్లను సమర్థంగా నిర్వహించడం, సైబర్ రిస్కులు/విపత్తులను సమర్థంగా ఎదుర్కొనడం, కార్యకలాపాలలో నిరంతరాయత, రికవరీ ఉండేలా చూడడం
- విపత్తుల సమాచారాన్ని సేకరించడం, బ్యాంకులపై వాటి ప్రభావాలను ముందస్తుగా అంచనా వేయడం
- ఎవరు, ఎప్పుడు, ఏం చేశారన్న వివరాలు తెలుసుకునే సామర్థ్యం, సాక్ష్యాలను భద్రపరచడం
- వివిధ రకాల లాగ్‌లను, లాగింగ్ ఆప్షన్స్‌ను SIEM, టికెటింగ్/వర్క్ ఫ్లో/ కేస్ మేనేజ్‌మెంట్, అన్‌స్ట్రక్చర్డ్ డాటా/బిగ్ డాటా, రిపోర్టింగ్/డాష్ బోర్డ్, యూజ్ కేసెస్/రూల్ డిజైన్ (రిస్క్ అండ్ కాంప్లయెన్స్ అవసరాలు/డ్రైవర్లు మొద.వాటి ఆధారంగా తయారు చేసినవి) మొదలైన వాటిలోకి జోడించడం

SOC యొక్క ముఖ్యమైన బాధ్యతలలో ఈ క్రిందివి ఉండాలి:

- సెక్యూరిటీ సంఘటనల పర్యవేక్షణ, సమీక్ష మరియు పెంపు
- ప్రతిస్పందన మెరుగుపరచడం - రక్షణ, పరిశోధన, ప్రతిస్పందన, పూర్వస్థితి
- ఇన్సిడెంట్ మేనేజ్‌మెంట్, ఫోరెన్సిక్ సమీక్షను నిర్వహించండి
- బ్యాంకు లోపల మరియు బయటి సంస్థల కాంటాక్ట్ గ్రూపులతో సమన్వయం

5- సైబర్ SOC యొక్క ఇటుకరాళ్లు

సాంకేతిక సమస్యలు

బ్యాంకింగ్ టెక్నాలజీ రిస్క్ ప్రొఫైల్ మరియు వ్యాపార, రెగ్యులేటరీ అవసరాలకు అనుగుణంగా ముందస్తు పర్యవేక్షణ సామర్థ్యాలు కలిగిన తక్కువ ఖర్చయ్యే టెక్నాలజీ ఫ్రేమ్‌వర్క్‌ను రూపొందించి, దానిని అమలు చేయడం మొదటి అడుగు.

బ్యాంకులు కస్టమర్లకు అందించే వినూత్నమైన సేవల వ్యవస్థను స్పష్టంగా అర్థం చేసుకోవడం వలన సెన్సర్లు లొకేషన్‌ను గుర్తించి, సమీక్ష మరియు పరిశోధన చేపట్టడానికి అవసరమైన లాగ్‌లను సేకరించడానికి వీలవుతుంది. ప్రస్తుతం SIEM కొంతవరకు ఈ అవసరాలను తీరుస్తున్నా, అయితే సమస్య గుర్తింపు, పరిష్కారం కోసం ఒక సమగ్ర దృక్పథం అవసరం.

రెండో అడుగుగా - లాగ్‌లను అతి తక్కువ సమయంలో ప్రాసెస్ చేసి, తగిన ప్రతిపాదనలతో, మరింత లోతుగా పరిశోధించడానికి అవసరమైన ప్రత్యామ్నాయాలతో ముందుకు రావడానికి అవసరమైన సెక్యూరిటీ అనలిటిక్స్ ఇంజన్‌ను కలిగి ఉండడం.

మూడో అడుగు- ఆన్ ద ఫ్లై డీప్ ప్యాకెట్ ఇన్‌స్పెక్షన్ తో వైర్ స్పీడ్ పెర్ఫామన్స్‌ను డెలివరీ చేసే UTM పరిష్కారాలను ఉపయోగించుకుంటున్న ప్రస్తుతం అమలు చేస్తున్న డీప్ ప్యాకెట్ ఇన్‌స్పెక్షన్ విధానాలను పరిశీలించడం.

నాలుగో అడుగు - మాల్‌వేర్‌ను గుర్తించడానికి, సమీక్షించడానికి, ఫోరెన్సిక్ సమస్యల పరిష్కారం కోసం అవసరమైన పరికరాలు, సాంకేతిక పరిజ్ఞానం, డాటాను కలిగి ఉండడం.

పై సమస్యలను పరిష్కరించడానికి ఏర్పాటు చేసిన పరిష్కార వ్యవస్థ సులభంగా లభించడంతో పాటు మెరుగైన ప్రదర్శన, అవసరమైతే దాని పరిమాణాన్ని పెంచుకొనగలిగే అవకాశాలు కూడా ఉండాలి. తగిన విధంగా రూపొందించుకుని, ఈ క్రింది వాటిపై ఆలోచించాలి:

- SIEM ఆర్కిటెక్చర్ మరియు యూజ్ కేసెస్
- లాగ్ రకాలు, లాగింగ్ ప్రత్యామ్నాయాలు (డాటా సోర్సెస్, SIEMలోకి జోడించడం)
- వివిధ రకాల లాగ్‌లు, లాగింగ్ ప్రత్యామ్నాయాలను SIEMలోకి జోడించడం, టికెటింగ్/వర్క్ ఫ్లో/కేస్ మేనేజ్‌మెంట్, అన్‌స్ట్రక్చర్డ్ డాటా/బిగ్ డాటా, రిపోర్టింగ్/డ్యాష్ బోర్డ్, యూజ్ కేసెస్/రూల్ డిజైన్ (రిస్క్ మరియు కంప్లయన్స్ అవసరాలు/డ్రైవర్లకు అనుగుణంగా
- కస్టమైజేషన్) మొద.
- ప్రభావం, సామర్థ్యం పెంచడానికి సాంకేతిక పరిజ్ఞానం (ట్రాకింగ్ ఆఫ్ మెట్రిక్స్, అనలిటిక్స్, స్కోర్‌బోర్డులు, డాష్ బోర్డులు మొద.)

ప్రాసెస్ సంబంధిత అంశాలు:

CSCని డిజైన్ చేసే సమయంలో గుర్తు పెట్టుకోవాల్సిన ఒక ముఖ్యమైన విషయం ఒక భద్రతా లోపం యొక్క మూల కారణాన్ని తెలుసుకోవడానికి, భవిష్యత్తులో అలాంటి దాడులు తిరిగి జరక్కుండా చూడడానికి అనుసరించాల్సిన విధానాలను అర్థం చేసుకోవడం చాలా ముఖ్యం.

ఇన్సిడెంట్ మేనేజ్‌మెంట్

సెక్యూరిటీ ఆపరేషన్స్ నేపథ్యంలో ప్రాబ్లమ్ మేనేజ్‌మెంట్

సెక్యూరిటీ ఆపరేషన్స్‌కు పరిష్కారం కోసం వల్నరబిలిటీ అండ్ ప్యాచ్ మేనేజ్‌మెంట్ సెక్యూరిటీ రిస్క్ మేనేజ్‌మెంట్, అవైలబిలిటీ మేనేజ్‌మెంట్, కంప్యూటర్ ఫోరెన్సిక్ అండ్ రెస్పాన్స్ మేనేజ్‌మెంట్ లాంటి ముఖ్యమైన మెట్రిక్‌లను బాగా అర్థం చేసుకోవాలి.

ప్రజా సంబంధిత సమస్యలు

CSC 24 గంటలూ సమర్థమైన, తగిన అర్హత కలిగిన సిబ్బంది చేత నిర్వహించబడుతూ, పర్యవేక్షించబడుతూ ఉంటుంది. అందువల్ల దీని కోసం ఒక తగిన వ్యవస్థను రూపొందించుకోవడం అవసరం.

తగిన శిక్షణ పొందిన సిబ్బంది చేత 24 గంటల లెవల్ -1 పర్యవేక్షణ అన్నది మొదటి దశ. సమస్యల ను పరిష్కరించడానికి వారికి శిక్షణ, ప్రొడక్ట్/వెండర్ సర్టిఫికేషన్ అవసరం.

లెవల్-2లో ఉన్నత స్థాయి శిక్షణ పొందిన సిబ్బంది నిర్దిష్టమైన నెట్‌వర్క్, డాటా సెక్యూరిటీ, ఎండ్ పాయింట్ సెక్యూరిటీ మొద. వాటిపై దృష్టి కేంద్రీకరిస్తారు. వీరు సమస్య మూలకారణాన్ని సమీక్షించి, వాటికి పరిష్కారాలను కనుగొంటారు.

లెవల్-3 సిబ్బందిని SoC అనలిస్టులు అంటారు. వీరికి సెక్యూరిటీ మీద, డీప్ ప్యాకెట్ సమీక్ష, IOC సేకరణ, సాక్ష్యాల సేకరణ కోసం ఫోరెన్సిక్ నాలెడ్జి మీద, మాల్‌వేర్ రివర్స్ ఇంజనీరింగ్ మీద లోతైన అవగాహన ఉంటుంది. వీరు అవసరమైనప్పుడు కస్టమ్ స్క్రిప్ట్‌లు రాయగలిగిన వారై ఉంటారు.

పై కార్యక్రమాలను నిర్వహించే సిబ్బంది అందరికీ ఆయా బ్యాంకుల ఉత్పత్తుల గురించి, సేవల గురించి మంచి అవగాహన ఉండాలి.

- SOCకి అవసరమైన వ్యక్తులు/మేనేజింగ్ స్టాఫ్‌ను నియమించుకోవడంలో ఎదురయ్యే
- సమస్యల విషయంలో బ్యాంకులు ప్రాక్టికల్‌గా ఆలోచించాలి. ఇది బ్యాంకులోని ఇతర కార్యక లాపాల మాదిరి కాదు. ఇందుకోసం ఒక భిన్నమైన దృక్పథాన్ని అనుసరించాలి. ఎందుకంటే అలాంటి నైపుణ్యాలు కలిగిన వ్యక్తులను గుర్తించి, వారిని అట్టిపెట్టుకోవడం చాలా కష్టం.
- SOCలో సిబ్బంది - వారు 24X7X365, షిఫ్టులు, బిజినెస్ అవర్స్‌లో మాత్రమేనా అని వర్గీకరించారు.
- ఉపయోగించే నమూనా - తగిన నైపుణ్యాలు కలిగిన సిబ్బందిని/సర్వీస్ ప్రొవైడర్‌ను గుర్తించడం
- సొంత సిబ్బందికి శిక్షణ/సిబ్బందికి సర్వీస్ ప్రొవైడర్ ద్వారా శిక్షణ
- శిక్షణ పొందిన/తగిన నైపుణ్యాలు కలిగిన సిబ్బంది తమ వద్దే కొనసాగేందుకు తగిన పరిహారం/ ప్రోత్సాహకాలు
- SOC ఏ విధంగా పని చేస్తుందన్నది పరిశీలించేందుకు అవసరమైన కొలబద్దలు
- సామర్థ్య పెంపు కార్యక్రమాల ద్వారా సిబ్బంది సంఖ్యను పెంచుకుంటూ, వారు తమతోనే

కొనసాగేలా చేయడం

బయటి ఇంటిగ్రేషన్

బ్యాంకు కస్టమర్లకు సేవలు అందజేసే విషయంలో అనేక మంది భాగస్వాములు ప్రత్యక్షంగా లేదా పరోక్షంగా భాగం పంచుకుంటారు. వారికి ఉన్న అనుభవం చాలా ఉపయోగపడుతుంది. ఉదాహరణకు టెక్నాలజీ విషయంలో ప్రాడక్ట్ వెండర్లు, ఇతర ముఖ్య భాగస్వాములు వివిధ వనరుల నుంచి అందించే విపత్తు సమాచారాన్ని అందిస్తారు. ఇతర బ్యాంకుల నుంచి, ఫైనాన్షియల్ ఎకో సిస్టమ్ నుంచి అందే భద్రతాపరమైన సమాచారం చాలా ఉపయోగపడుతుంది.

బ్యాంకుకు చెందిన సైబర్ రెస్పాన్స్ సెల్స్ , CERT-In, ఇతర టెలికాం సర్వీస్ ప్రొవైడర్లు బ్యాంకింగ్ పరిశ్రమలో వస్తున్న మార్పులపై విలువైన సూచనలు అందిస్తారు.

అమలు చేయదగిన నమూనా గుర్తింపు

ముందుగా తీసుకోవాల్సిన నిర్ణయాలలో BOOను లేదా ఔట్ సోర్సింగ్ నమూనాను గమనించడం ముఖ్యమైనవి. ఒకసారి అమలు చేయడం ప్రారంభించిన తర్వాత ఆ నిర్ణయాన్ని వెనక్కి తీసుకోవడం కష్టం కావడం వల్ల ఇది చాలా ముఖ్యం.

- SOC ఇన్-హౌస్‌లోనే ఉండాలా లేదా ఔట్‌సోర్స్ చేయాలా?
- అది కేవలం ఇంటర్నెట్ ఎదుర్కొనే వాతావరణాన్ని మాత్రమే ఎదుర్కోవాలా లేక మొత్తం ఐటీ ఇన్‌ఫ్రాస్ట్రక్చర్‌నా?
- ప్రతి బ్యాంక్ తన సొంత విపత్తు నివారణ వ్యవస్థను ఏర్పాటు చేసుకోవాలా లేక అన్నీ కలిసి కన్సార్టియం విధానాన్ని ఏర్పాటు చేసుకోవాలా?
- బ్యాంక్ విపత్తులకు గురయ్యే అవకాశాలను దృష్టిలో పెట్టుకోవాలా?

SOC కోసం ప్రణాళికలు రూపొందించుకునే సమయంలో ఈ క్రింది వాటిని దృష్టిలో పెట్టుకోవాలి.

ఎ) SOC నిర్వహణ కోసం ప్రత్యేక నైపుణ్యాలు అవసరం

బి) అనుభవం కలిగిన సిబ్బందిని పొందడం కష్టం

సి) ఎక్కువ సమయం, శిక్షణ కోసం ఎక్కువ ఖర్చు

డి) తగిన పరిహార వ్యూహాల రూపకల్పన

ఇ) నిరంతరం అప్ టు డేట్ శిక్షణ పొందడం, తగిన కెరీర్ ప్రత్యామ్నాయాలు లేకపోవడం, తీవ్రమైన ఒత్తిడి ఉండడం తదితర కారణాల వల్ల సిబ్బందిని అట్టిపెట్టుకోవడం చాలా కష్టం.

ఎఫ్) ఇతర సహాయ సహకారాలకు సంబంధించి ఈ క్రింది వనరులు అవసరం (i) SIEM/ డ్యాష్ బోర్డ్/ రిపోర్టింగ్ వర్క్ ఫ్లో/కేస్ మేనేజ్‌మెంట్ సిస్టమ్స్ లాంటి SOC ఆపరేషన్స్‌ను నిర్వహించే సిస్టమ్‌ల అడ్మినిస్ట్రేషన్ (ii) విపత్తు ఇంటలిజెన్స్‌ను రిసీవ్ చేసుకోవడం, జోడించడం, ఉపయోగించడం (iii) కమ్యూనికేషన్ స్ట్రాటజీని అమలు చేయడం (iv) SOC సిబ్బంది సూపర్‌విజన్/మేనేజ్‌మెంట్ (v) రెగ్యులేటర్లు/చట్టాలు/నియంత్రణల ప్రమాణాలను అందుకోవడంలాంటి ఇతర సహాయక కార్యకలాపాల వనరులు అవసరం.

<u>సైబర్ సంఘటనలను రిపోర్ట్ చేయడానికి అవసరమైన టెంప్లేట్</u>

1. RBIకు సెక్యూరిటీ సంఘటన రిపోర్టింగ్ (SIR) (2 నుంచి 6 గంటలలోపు)

2. RBIకు తదనంతర అప్‌డేట్స్ (గత రిపోర్టింగ్ అసంపూర్తిగా ఉంటే అంటే ఇన్వెస్టిగేషన్ జరుగుతూ ఉంటే లేదా ఆ సంఘటనకు సంబంధించి కొత్త సమాచారం ఏమైనా తెలిస్తే లేదా RBI విజ్ఞప్తి మేరకు) అప్ డేట్ ఇవ్వాలి.

ప్రాథమిక సమాచారం

1. రిపోర్టింగ్ వివరాలు

* బ్యాంకు పేరు

* RBI, CERT-In, ఇరత సంస్థలకు
రిపోర్టింగ్ చేసే తేదీ, సమయం
(రిపోర్టింగ్ చేసే సమయంలో ప్రతి ఒక్కరికీ
వేర్వేరుగా సమయాన్ని పేర్కొనండి)

* రిపోర్ట్ చేస్తున్న వ్యక్తి పేరు

* హోదా/విభాగం

*కాంటాక్ట్ వివరాలు (ఉదా. అధికారిక
ఈమెయిల్ ఐడీ, టెలిఫోన్ నెంబర్,
మొబైల్ నెంబర్ మొద.)

2. సంఘటన వివరాలు

* సంఘటనను గుర్తించిన తేదీ, సమయం

* సంఘటనల రకాలు, ప్రభావితమైన సిస్టమ్స్

(i) **క్రిటికల్ ఐటీ సిస్టమ్స్ ఔటేజ్**

(ఉదా. CBS, ట్రెజరీ సిస్టమ్స్, ట్రేడ్ ఫైనాన్స్ సిస్టమ్స్, ఇంటర్నెట్ బ్యాంకింగ్ సిస్టమ్స్, ATMలు, SWIFT, RTGS, NEFT, NACH, IMPS లాంటి పేమెంట్ వ్యవస్థలు)

(ii) **సైబర్ సెక్యూరిటీ సంఘటన**

(ఉదా. DDOS, రాన్సమ్ వేర్/క్రిప్టోవేర్, డాటా బ్రీచ్, డాటా డిస్ట్రక్షన్, వెబ్ డిఫేస్‌మెంట్ మొద.) (దయచేసి అనుబంధాన్ని పూర్తి చేయండి)

(iii) **సమచార సంగ్రహం లేదా మాయం కావడం** (ఉదా. కస్టమర్ లేదా బిజినెస్‌కు చెందిన ముఖ్యమైన సమాచారం మాయం కావడం లేదా నాశనం లేదా కరప్ట్ కావడం)

(iv) **ఇన్‌ఫ్రాస్ట్రక్చర్ అందుబాటులో లేకుండా పోవడం** (ఉదా: డీసీ/సెంట్రల్ ప్రాసెసింగ్ యూనిట్లు, శాఖ మొద., పవర్/యుటిలిటీ సప్లై, టెలీకమ్యూనికేషన్ సప్లై)

(v) **ఆర్థికం** (ఉదా: లిక్విడిటీ, బ్యాంక్ రన్)?

(vi) **సిబ్బంది అందుబాటులో లేకపోవడం**

(ఉదా: ఎంత మంది, ఎంత శాతం సిబ్బంది

తక్కువగా ఉన్నారు/పని నుంచి ఆబ్సెంట్ అయ్యారు?)

(vii) **ఇతరములు** (ఉదా: ఔట్ సోర్స్డ్

సర్వీస్ ప్రొవైడర్లు, బిజినెస్ పార్ట్‌నర్లు,

ఐటీ చట్టం/ఇతర ఏవైనా చట్టాలు,

RBI/SEBI రెగ్యులేషన్ల ఉల్లంఘన మొద) ?

3. ప్రభావాన్ని అంచనా వేయడం (ఉదాహరణలు ఇవ్వడం జరిగింది కానీ అవి పూర్తిగా కాదు)

- సేవల అందుబాటుతో పాటు వ్యాపారంపై ప్రభావం - బ్యాంకింగ్ సేవలు, ఇంటర్నెట్ బ్యాంకింగ్, క్యాష్ మేనేజ్‌మెంట్, ట్రేడ్ ఫైనాన్స్, శాఖలు, ATMలు, క్లియరింగ్ మరియు సెటిల్‌మెంట్ కార్యకలాపాలు మొద.
- భాగస్వాములపై ప్రభావం - ప్రభావితమైన రిటైల్/కార్పొరేట్ కస్టమర్లు, ఆపరేటర్లు, సెటిల్‌మెంట్ సంస్థ(లు), బిజినెస్ పార్ట్‌నర్‌లు, సర్వీస్ ప్రొవైడర్లు మొద. ప్రభావితులైన భాగస్వాములు
- ఫైనాన్షియల్ మరియు మార్కెట్‌పై ప్రభావం – ట్రేడింగ్ కార్యకలాపాలపై ప్రభావం, ట్రాన్సాక్షన్ పరిమాణాలు, విలువలు, సొమ్ము నష్టం, లిక్విడిటీ ప్రభావం, బ్యాంక్ రన్, ఫండ్‌లను విత్‌డ్రా చేసుకోవడం మొద.
- రెగ్యులేటరీ మరియు చట్టాల ప్రభావం

4. ఆయా సంఘటనల కాలక్రమానుగతం:

- సంఘటన జరిగిన తేదీ, సమయం

  ఎంత కాలం పాటు?

- ఆ సంఘటన తీవ్రతను తగ్గించడానికి

  తీసుకున్న మధ్యంతర చర్యల కోసం

  తీసుకున్న అప్రూవల్‌లు, అలాంటి చర్యలు

  తీసుకోవడానికి గల కారణాలు

- సమాచారం ఇచ్చిన లేదా సంబంధం

  కలిగిన భాగస్వాములు

- ఉపయోగించిన కమ్యూనికేషన్ ఛానెల్స్

  (ఉదా: ఈమెయిల్, ఇంటర్నెట్, ఎస్సెమ్మెస్,

  ప్రెస్ రిలీజ్, వెబ్‌సైట్ నోటీస్ మొద.)

- BCP మరియు/లేదా DR నిర్ణయం/

  యాక్టివేషన్ చేయడానికి గల కారణాలు

5. మూల కారణ సమీక్ష (RCA)

- ఆ సమస్య ఎందువల్ల పుట్టింది/ఆ సంఘటన

  జరగడానికి కారణాలు, వాటి ప్రభావం.

- ఈ సమస్య పరిష్కారం/

  తీవ్రత తగ్గించేందుకు తీసుకున్న చర్యలు,

  ఆ చర్యలు తీసుకోవడానికి గల కారణాలు.

- దీర్ఘకాలంలో ఆ సమస్యను పరిష్కరించడానికి

  గుర్తించిన లేదా తీసుకున్న నివారణ

చర్యలు/ కరెక్షన్ల (ఒక్కసారి మాత్రమే) జాబితా

మరియు/లేదా అలాంటి సంఘటనలు

మళ్లీ భవిష్యత్తులో జరగకుండా

తీసుకున్న నివారణ చర్యలు

6. తేదీ/సమస్య పరిష్కారానికి నిర్దేశించుకున్న లక్ష్యం......

(DDMMYYYY)

-
-
-

గమనిక: వేరే విధంగా పేర్కొంటే తప్ప, అన్ని గళ్లనూ పూర్తి చేయాలి

<u>సైబర్ సెక్యూరిటీ ఇన్సిడెంట్ రిపోర్టింగ్ (CSIR) ఫామ్</u>

సాధారణ సమాచారం **రిపోర్ట్ నెం:**

1. కాంటాక్ట్ సమాచారం: (పైన పేర్కొన్న ప్రాథమిక సమాచారంలో ఉన్నదానికన్నా వేరేగా ఉంటే పేర్కొనండి)

బ్యాంక్ పేరు:

రిపోర్ట్ చేస్తున్న వ్యక్తి పేరు, హోదా:

విభాగం:

అధికారిక ఈమెయిల్:

టెలిఫోన్/మొబైల్:

2. ఇది ఒక కొత్త సంఘటనా? ☐ లేదా ఇప్పటికే రిపోర్ట్ చేసిన సంఘటనకు అప్ డేటా? ☐

* దయచేసి మొదటి అప్ డేట్ కు 1 ని సూచించండి. ఒకవేళ ఇది ఇప్పటికే జరిగిన సంఘటనకు అప్ డేట్ అయితే, ఈ అప్‌డేట్‌కు అప్‌డేట్ సంఖ్యను ఇవ్వండి. (X1, X2, X3 , X4 మొదలైనవి. ఇక్కడ X అంటే రిపోర్ట్ సంఖ్య.

అప్‌డేట్ సంఖ్య: టెక్స్ట్‌ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

3. తీవ్రతను బట్టి ఈ సంఘటనను దేని కింద వర్గీకరించబడింది?

తీవ్రత 1 ☐	తీవ్రత 2 ☐
క్రిటికల్ సిస్టమ్స్ ప్రభావితం/కస్టమర్ అప్లికేషన్ లేదా సిస్టమ్స్ సమస్యలను ఎదుర్కొంటున్నాడు. అంతర్గత నెట్‌వర్క్ దెబ్బ తినింది. లేదా వీటన్నిటి కలయిక.	సంఘటన బ్యాంక్ నెట్‌వర్క్/ క్రిటికల్ సిస్టమ్స్‌ను దెబ్బ తీసేంత తీవ్రం లేదా ఆ రెండింటి కలయిక

సంఘటన గురించి సమాచారం

4. RBIకు ఈ సంఘటన గురించి సమాచారం అందించిన తేదీ, సమయం సూచించండి. ఇతర సంస్థలు, (CERT-In, NCIIP), చట్ట అమలు సంస్థలకు కూడా దీని గురించి వెల్లడించినట్లయితే, ఆ తేదీ, సమయం కూడా సూచించండి.

(దయచేసి భారతీయ స్థానిక కాలమానంలో సూచించండి (+ 5.30 GMT))

RBIకి రిపోర్ట్ చేసిన తేదీ - తేదీ: తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి

CERT-In కి రిపోర్ట్ చేసిన తేదీ - తేదీ: తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి

NCIIPకి రిపోర్ట్ చేసిన తేదీ - తేదీ: తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి

.........కు రిపోర్ట్ చేసినది- సంస్థ పేరును పేర్కొనండి - తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి

5.ఎలాంటి విపత్తు/సంఘటన

(దయచేసి ఒకటికన్నా ఎక్కువ ఎంపిక చేయండి, అవసరమైతే)

☐ డెనియల్ ఆఫ్ సర్వీస్

☐ డిస్ట్రిబ్యూటెడ్ డెనియల్ ఆఫ్ సర్వీస్

☐ వైరస్/వామ్/ట్రోజన్/మాల్‌వేర్

☐ ఇంట్రూజన్/హ్యాక్/అనధరైజ్డ్ యాక్సెస్

వెబ్‌సైట్ డిఫేస్‌మెంట్

సిస్టమ్స్‌ను దుర్వినియోగం/ఇతర అవసరాలకు ఉపయోగించుకోవడం

☐ APT ఏపీటీ/జీరో డే అటాక్

☐ స్పియర్ ఫిషింగ్/వేలింగ్/ఫిషింగ్/విషింగ్/సోషల్ ఇంజనీరింగ్ అటాక్

☐ ఇతరములు: టెక్స్‌ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

6. ఈ సంఘటనకు, గతంలో జరిగిన సంఘటనలతో సంబంధం ఉందా?

ఒక దానిని ఎంచుకోండి:

- అవును అయితే, ఈ రెండు సంఘటనలూ ఎలా సంబంధాన్ని కలిగి ఉన్నాయో మరింత సమాచారాన్ని ఇవ్వండి

టెక్స్‌ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

- గతంలో రిపోర్ట్ చేసిన సంఘటన రెఫరెన్స్‌ను పేర్కొనండి.

టెక్స్‌ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

సంఘటన వివరాలు

7. సంఘటన వివరాలను ఈ క్రింది బాక్స్‌లో ఇవ్వండి.

- ఈ మొదటి సంఘటనను ఎప్పుడు కనుగొన్నారు/గుర్తించారు/చూశారు?

తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

- ఈ సంఘటనను ఎలా కనుగొన్నారు/గుర్తించారు/చూశారు?

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

* ఎవరు గుర్తించారు?

8. ఈ సంఘటన వల్ల ప్రభావితమైన క్రిటికల్ సిస్టమ్స్ లేదా నెట్‌వర్క్ ల వివరాలు ఇవ్వండి. దానిలో కనీసం ఈ క్రింది వివరాలు ఉండాలి:

ప్రదేశం, ఈ సిస్టమ్/నెట్‌వర్క్ పని, సిస్టమ్/నెట్‌వర్క్ లో నడుస్తున్న ప్రభావితమైన అప్లికేషన్లు(హార్డ్ వేర్ తయారీదారు, సాఫ్ట్ వేర్ డెవలపర్, మేక్/మోడల్ మొద) మొద.

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

ప్రస్తుతం సిస్టమ్‌లో ఎలాంటి సెక్యూరిటీ సాఫ్ట్ వేర్ ఇన్ స్టాల్ చేయబడి ఉంది?

ఈ సంఘటనలో ప్రమేయమున్న ఏవైనా TCP లేదా UDP పోర్టుల వివరాలు, ఒకవేళ తెలిసింటే.

ప్రభావితమైన సిస్టమ్ IP అడ్రస్, ఒకవేళ తెలిసి ఉంటే. ఒకవేళ తెలిస్తే అటాక్ చేసిన వారి IP అడ్రస్‌ను పేర్కొనండి.

అవసరం అనిపించన చోట, దయచేసి ప్రభావితమైన క్రిటికల్ సిస్టమ్ యొక్క OSను పేర్కొనండి: ఏదైనా ఒక దానిని ఎంచుకోండి :

- ఇతరములు అయినట్లయితే, OS పేరును పేర్కొనండి. :

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

9. ఆ దాడి యొక్క ప్రభావం ఏమిటి? (ప్రతి కాలమ్ కు ఒక బాక్స్‌లో టిక్ పెట్టండి)

కస్టమర్ సర్వీస్ డెలివరీ	సెన్సిటివ్ సమాచారం (నష్టం)	ప్రజల విశ్వాసం, సంస్థ ప్రతిష్ట
☐ ఎలాంటి ప్రభావం లేదు	☐ ఎలాంటి నష్టమూ లేదు	☐ ఎలాంటి ప్రభావం లేదు
☐ తక్కువ ప్రభావం	☐ తక్కువ నష్టం	☐ తక్కువ ప్రభావం
☐ ఎక్కువ ప్రభావం	☐ ఎక్కువ నష్టం	☐ ఎక్కువ ప్రభావం
☐ తీవ్రమైన ప్రభావం	☐ తీవ్రమైన నష్టం	☐ తీవ్రమైన ప్రభావం
☐ భారీ ప్రభావం	☐ భారీ నష్టం	☐ భారీ ప్రభావం

10. ప్రభావితమైన క్రిటికల్ సిస్టమ్స్/ నెట్ వర్కులు బ్యాంకు యొక్క ఇతర క్రిటికల్ సిస్టమ్స్/ క్రిటికల్ అసెట్స్ పై ప్రభావం చూపే అవకాశముందా?

ఒక దానిని ఎంచుకోండి :

అవును అయితే, మరిన్ని వివరాలు తెలియజేయండి.

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

సంఘటన స్థితి

11. ఆ సమయంలో తీసుకున్న ఫాలో అప్ చర్యలు ఏమి?

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

12. ప్రస్తుత పరిస్థితి లేదా ఈ సంఘటన అనంతర తీర్మానాలేమి?

ఒక దానిని ఎంచుకోండి:

ఒకవేళ అది పరిష్కారం కానట్లయతే, తర్వాత కార్యాచరణ ఏమిటి?

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

13. మీకు తెలిసి దాడి జరిగిన/కాంప్రమైజ్ అయిన మొదటి తేదీ ? (తెలియకుంటే చెక్ బాక్స్‌లో టిక్ చేయండి)

(దయచేసి భారతీయ స్థానిక కాలమానంలో సూచించండి (+ 5.30 GMT))

తేదీ: తేదీని ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి. తెలియదు : ☐

14. ఈ సంఘటనకు మూలం/కారణం ఏమిటి? (నిల్ లేదా తెలియకపోతే ఎన్ే)

టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

15. ఈ సంఘటనను CERT-In, NCIIP/ఏదైనా చట్ట అమలు సంస్థ/ IBCARTకు రిపోర్ట్ చేయడం జరిగిందా? ఒక దానిని ఎంచుకోండి.

  * అవును అయితే , రిపోర్ట్ చేసిన ఏజెన్సీని పేర్కొనండి.

  టెక్స్ ను ఎంటర్ చేయడానికి ఇక్కడ క్లిక్ చేయండి.

16. చెయిన్ ఆఫ్ కస్టడీని మెయిన్ టెయిన్ చేస్తున్నారా?

17. బ్యాంక్ చెయిన్ ఆఫ్ కస్టడీ ఫామ్‌ను నింపుతోందా?

18. ఈ సంఘటన అనంతరం సాక్ష్యాలను నమోదు చేయడానికి ఏ టూల్స్‌ను ఉపయోగించడం జరిగింది?

అటాక్ వెక్టర్స్

E1. బ్యాంకు ఈ సంఘటనకు సంబంధించిన IP అడ్రస్ లు, డొమైన్ పేర్లు గుర్తించిందా?

ఇండికేటర్స్ ఆఫ్ కాంప్రమైజ్, సంఘటనలో గుర్తించిన IP అడ్రస్‌లు, సంఘటనలో ప్రమేయం కలిగిన IP అడ్రస్‌లు (బాధితులు, మాల్ వేర్ కమాండ్ అండ్ కంట్రోల్ సర్వర్లు మొద.), పరిష్కరించిన డొమైన్ నేమ్స్, సంఘటనలో ప్రమేయం కలిగిన డొమైన్ నేమ్స్ (ఉదా: డ్రైవ్ బై డౌన్ లోడ్ సర్వర్లు, మాల్ వేర్ కంట్రోల్ అండ్ కమాండ్ సర్వర్లు, డీ ఫేస్డ్ వెబ్ సైట్లు), గుర్తించిన ఈమెయిల్ అడ్రస్‌లు వాటి ప్రమేయం, హానికారక ఫైల్స్/అటాచ్‌మెంట్స్ (ఫైల్ పేరు, సైజు, MD5/ IPSHA 1 హ్యాష్ మొద) మొదలైన వాటి గురించి IBCART, CERT-In, చట్టాన్ని అమలు చేసే సంస్థలకు రిపోర్ట్ చేయడం జరిగిందా?