શુદ્ધિપત્રક

ધોરણ - 9

વિષય : કમ્પ્યુટર અધ્યયન

માધ્યમ : ગુજરાતી

ગુજરાત સરકાર તથા ગુજરાત માધ્યમિક અને ઉચ્ચતર માધ્યમિક શિક્ષણ બોર્ડની સૂચના અનુસાર વર્ષ 2021થી પ્રકાશિત થનાર પાઠ્યપુસ્તકની આવૃતિમાં પ્રકરણ-14 ના અંતે 'સાયબર સુરક્ષા, તેનાં જોખમો અને ઉકેલ' અંગે કેટલીક વધુ માહિતી મૂકવામાં આવી છે. હાલના સમયમાં ઈન્ટરનેટના વધેલા ઉપયોગોએ 'સાયબર હુમલા' નામે ઓળખાતા જોખમને જન્મ આપ્યો છે. તેનાથી સુરક્ષિત રહેવા માટેના ઉપાયો આમાં ચર્ચવામાં આવ્યા છે.

સાયબર સુરક્ષા, તેનાં જોખમો અને ઉકેલ (Cyber Security, its Threats and Solutions)

વર્તમાન સમયમાં આપણે અનેકવિધ કાર્યો માટે ઈન્ટરનેટનો ઉપયોગ કરીએ છીએ. આજે ઘર, કાર્યાલય, વાહનો અને ઘરનાં ઉપકરણો પણ ઈન્ટરનેટ સાથે જોડાવાં લાગ્યાં છે. ડેટાની વધુ પ્રમાણમાં વહેંચણી અને જુદા જુદા ઘટકોના આંતરજોડાણે સાયબર હુમલા (Cyber attack) નામે ઓળખાતા એક નવા જોખમને જન્મ આપ્યો છે. સાયબર હુમલો એક એવી પ્રવૃત્તિ છે જેમાં દુનિયામાં કોઈપણ સ્થાને બેઠેલ વ્યક્તિ ઈન્ટરનેટનો ઉપયોગ કરીને અન્ય કોઈ વ્યક્તિ કે સંસ્થાના IT માળખાંને નુકસાન પહોંચાડે છે અથવા તો માહિતીની ચોરી કરે છે. કોઈ વ્યક્તિ કે સંસ્થા દ્વારા અન્ય વ્યક્તિ કે સંસ્થાના માળખાંને તોડી પાડવાની આ એક સહેતુક અને દુષ્ટતાપૂર્ણ યોજના હોય છે. અહીં હુમલાખોરનો હેતુ ડેટાની ચોરી, માહિતીની ચોરી, આર્થિક લાભ, જાસુસી કે વિધ્વંસ હોઈ શકે છે. ઘણા પ્રકારના સાયબર હુમલા શક્ય છે જેમાંના કેટલાક નીચે જણાવ્યા છે.

ફિશિંગ (Phishing) : સામાન્ય રીતે આ હુમલા દ્વારા ખોટી વેબસાઈટ, પાનાં કે વેબ લિંક દ્વારા ભ્રમણા ઊભી કરી વ્યક્તિના ઈ-મેઈલના પ્રત્યુત્તર દ્વારા તેની સંવેદનશીલ માહિતી જાહેર કરવામાં આવે છે. ઉદાહરણ તરીકે, કોઈ વ્યક્તિ એવા સંદેશ સાથેનો ઈ-મેઈલ મેળવી શકે છે જેમાં તેને કોઈ વેબસાઈટ પર રમત રમ્યા બદલ લાખો રૂપિયાનું ઈનામ લાગ્યાની માહિતી આપવામાં આવે છે. ઈનામની રકમ મેળવવા માટે ઈ-મેઈલ મેળવનારે કોઈ લિંક પર ક્લિક કરીને પોતાની બેંકની માહિતી આપવાની હોય છે. આ પ્રકારના સંદેશના વિષય ઘણા આકર્ષક રાખવામાં આવે છે અને સ્પામ મેઈલ વિષે જાણનાર વ્યક્તિ પણ અહીં ફસાઈ જાય છે. ફિશિંગ હુમલા અને સ્પામ સામાન્ય રીતે શંકાસ્પદ ઈ-મેઈલ સિસ્ટમ દ્વારા રજૂ કરવામાં આવે છે.

મલવેર (Malware) : Malware એટલે "malicious software" જેમાં વાયરસ (Virus), વોર્મ (Worm), ટ્રોજન હોર્સ (Trojan Horse) અને સ્પાયવેર (Spyware)નો સમાવેશ થાય છે.આ સોફ્ટવેર આઈ.ટી. માળખામાં પાયમાલી સર્જી મશીન પર નિયંત્રણ મેળવે છે, માહિતીનો દુરુપયોગ કરે છે, પ્રવૃત્તિઓ પર ધ્યાન રાખે છે, માહિતીની નોંધ કરે છે અને અન્ય અનિચ્છિત કાર્યોનો અમલ કરે છે. હુમલાખોર ઈ-મેઈલ વ્યવસ્થાનો ઉપયોગ કરીને સરળતાથી એક સિસ્ટમ પરથી અન્ય સિસ્ટમ પર મલવેર મોકલે છે. જોકે, હુમલાખોર દરવખતે સફળ થતા નથી પરંતુ જો સફળ થાય તો તે આપણા ઈ-મેઈલ એકાઉન્ટ, મશીન, વિગતો અને અન્ય સંવેદનશીલ માહિતી પર નિયંત્રણ મેળવી લે છે.

રેન્સમવેર (Ransomware) : આ પ્રકારના હુમલામાં ભોગ બનનારના કમ્પ્યૂટર કે ફાઈલોને હેકર દ્વારા લોક કરી દેવામાં આવે છે. આ કિસ્સામાં હુમલાખોર ખંડણી માંગવા માટે માહિતી મેળવે છે. પોતાની આ માહિતી પાછી મેળવવા માટે ભોગ બનનારે હુમલાખોરને ચૂકવણી કરવી પડે છે. રેન્સમવેર ફિશિંગ ઈ-મેઈલ દ્વારા અથવા અજાણતા ચેપગ્રસ્ત વેબસાઈટની મુલાકાત લેવાથી ફેલાય છે.

ડેટા એક્સપોઝર (Data Exposer) : સાયબર સુરક્ષા અંગે હાલમાં આ એક વ્યાપક જોખમ બની રહ્યું છે. અહીં હુમલાખોર બેન્કિંગ, સોશિયલ મીડિયા, યુનિવર્સિટી અથવા ડેટાનો સંગ્રહ કરતા અન્ય કોઈ વિનિયોગનો ઉપયોગ કરવાનો પ્રયત્ન કરે છે. ડેટા એક્સપોઝર જુદી જુદી રીતે જોવા મળે છે. ડેટા સુધી પહોંચવા માટે હેકર ઉપયોગકર્તાની લોગિન વિગતોને સોશિયલ એન્જિનિયરિંગ દ્વારા અથવા તો મલવેરનો ઉપયોગ કરીને ચોરી લે છે. ડેટાની અકસ્માતે થયેલ વહેંચણી પણ ઘણીવાર ડેટા એક્સપોઝરમાં પરિણમે છે.ડેટાની અકસ્માતે થયેલ વહેંચણી એ માનવીય ભૂલ હોય છે. ઈ-મેઈલ દ્વારા "Reply All" જેવી કરવામાં આવેલી સરળ પ્રક્રિયા ડેટા એક્સપોઝરનું જોખમ ઊભું કરે છે.

આ હુમલાઓને કારણે ''સાયબર સુરક્ષા'' (Cyber security) નામનું એક પદ અસ્તિત્વમાં આવ્યું છે. સાયબર સુરક્ષા એ કેટલીક કાર્યપદ્ધતિઓનો સમૂહ છે જેનો ઉપયોગ કમ્પ્યૂટરના હાર્ડવેર, સોફ્ટવેર કે ઈલેક્ટ્રોનિક ડેટાની ચોરી કે નુકસાન સામે કમ્પ્યૂટર સિસ્ટમના રક્ષણ માટે કરવામાં આવે છે. તેનો એક હેતુ કમ્પ્યૂટર સિસ્ટમ દ્વારા પૂરી પાડવામાં આવતી સેવાઓની સુરક્ષા પણ છે. ઈન્ટરનેટનો ઉપયોગ કરીને આભાસી રીતે જોડવામાં આવેલા તમામ ઘટકો માટે પણ સાયબર સુરક્ષા ખૂબ મહત્વની બની છે.

અહીં આપવામાં આવેલાં કેટલાંક પગલાં કોઈપણ સંસ્થા કે વ્યક્તિને તેમના ડેટા અને માહિતીને વધુ સારી સુરક્ષા માટે મદદરૂપ બનશે. જો આ પગલાંનો યોગ્ય અમલ કરવામાં આવે તો સાયબર હુમલા સામેની સુરક્ષામાં તે મદદરૂપ બનશે.

- સર્વર, અંગત કમ્પ્યૂટર, લેપટોપ કે મોબાઈલ સાધન જેવી કમ્પ્યૂટર સિસ્ટમનો ઉપયોગ કરતી વખતે સક્ષમ એન્ટી-વાયરસ કે એન્ટી-મલવેર સોફ્ટવેર સ્થાપિત કરવું.
- સિસ્ટમમાં સ્થાપિત કરેલું એન્ટી-વાયરસ કે એન્ટી-મલવેર સોફ્ટવેર અદ્યતન (updated) છે તેની ખાતરી કરવી. રોજેરોજ વાયરસ અને મલવેરના નવા સમૂહ આવતા રહે છે. માટે, વ્યક્તિ કે સંસ્થા માટે આ વાયરસથી સુરક્ષા મેળવવી જરૂરી બને છે.
- નેટવર્કની સુરક્ષા માટે ફાયરવોલનો ઉપયોગ કરવો. ઈ-મેઈલ સિવાય પણ અન્ય ઘણા સ્રોત દ્વારા મલવેર ફેલાતા હોવાને કારણે નેટવર્કમાં ડેટાના સ્થાનાંતરણ પર નિયંત્રણ હોવું જરૂરી છે. ફાયરવોલ નેટવર્કમાં પ્રવેશ કરતા અને નેટવર્ક છોડી જતા ડેટાનું ધ્યાન રાખે છે. આ જ રીતે, ઘરના અંગત કમ્પ્યૂટર કે લેપટોપ જેવા ઉપયોગકર્તાના કમ્પ્યૂટર પર અંગત ફાયરવોલની સ્થાપના કરી કમ્પ્યૂટર સુરક્ષિત છે તેની ખાતરી કરી લેવી જોઈએ.
- ઉપયોગકર્તા દ્વારા મોકલવામાં અને મેળવવામાં આવનાર દરેક ઈ-મેઈલને કમ્પ્યૂટર વાયરસ માટે તપાસવા જોઈએ. આ માટેના ફિલ્ટર (Filter) આદર્શ રીતે રાઉટર (Router) કે એક્સેસ પોઈન્ટ (Access point) જેવા નેટવર્કના પ્રવેશ-સ્થાન પર સ્થાપિત કરવા જોઈએ.
- તમામ ઉપયોગકર્તાને કમ્પ્યૂટરનો શ્રેષ્ઠ ઉપયોગ કરવા માટેની તાલીમ આપવી જોઈએ. ઉદાહરણ તરીકે, કોઈએ ક્યારેય ઈ-મેઈલના અનપેક્ષિત જોડાણ (Attachment) ખોલવાં જોઈએ નહિ તથા અજ્ઞાત સ્રોત પરથી આવેલ લિંક પર ક્લિક કરવી જોઈએ નહિ.
- ડાઉનલોડ સ્રોત અંગેની યોગ્ય માહિતી મેળવ્યા વગર અજાણ્યા ઉદ્‌ગમસ્થાનેથી મેળવેલા પ્રોગ્રામને ડાઉનલોડ ન કરવા જોઈએ તથા અમલમાં ન મૂકવા જોઈએ.

- અગત્યની ફાઈલ અને ફોલ્ડરનો નિયમિત રીતે બેકઅપ (backup) લેવાતો હોય તેની ખાતરી કરવી જોઈએ. બેકઅપને પોર્ટેબલ ડ્રાઈવ (Portable drives) કે રિમૂવેબલ મિડિયા (Removable media) દ્વારા સાચવવો જોઈએ. વધુ સલામતી માટે બેકઅપનો અન્ય સ્થાન પર પણ સંગ્રહ કરવો જોઈએ.
- અંતિમ ઉપયોગકર્તાઓને શક્ય હોય ત્યાં પ્રવેશ નિયંત્રણો (access controls)ની પ્રક્રિયાનો ઉપયોગ કરીને મર્યાદિત પરવાનગીઓ આપવી.
- સંસ્થામાં નેટવર્ક સુરક્ષાની પ્રણાલી નક્કી કરવી અને તેને તમામ ઉપયોગકર્તાઓ સુધી પહોંચાડવી.

ઈ-મેઈલ પદ્ધતિના ઉપયોગ દરમ્યાન સામાન્ય જોખમો (Common threats while using an Email system)

કોઈપણ સંસ્થામાં આજે ઈ-મેઈલ સિસ્ટમ સંચારણના એક મહત્વના ભાગ તરીકે ઉપયોગમાં લેવામાં આવે છે. માહિતી મેળવવા તથા મોકલવા માટેની પ્રક્રિયાને સરળ બનાવવા માટે ઈ-મેઈલનો ઉપયોગ કરવામાં આવે છે. સામાન્ય રીતે ઈ-મેઈલ પદ્ધતિમાં બે ઘટકોનો સમાવેશ થાય છે : સર્વર (Server) અને ક્લાયન્ટ (Client). આ ઘટકોને મેઈલ સર્વર (Mail Server) અને મેઈલ ક્લાયન્ટ (Mail Client) તરીકે ઓળખવામાં આવે છે. મેઈલ ક્લાયન્ટની મદદથી ઉપયોગકર્તા ઈ-મેઈલ વાંચી શકે છે; ઈ-મેઈલ લખી શકે છે; ઈ-મેઈલ મોકલી શકે છે તથા ઈ-મેઈલનો સંગ્રહ કરી શકે છે. માટે, ઈ-મેઈલના કાર્ય સાથે સંકળાયેલા આ તમામ ઘટકોની યોગ્ય સુરક્ષા જરૂરી બને છે. મેઈલ ક્લાયન્ટ, સર્વર તથા ઈ-મેઈલ સિસ્ટમના ભાગરૂપે આવેલ તમામ માળખાં અને સાધનોની સુરક્ષા મહત્વની છે.

હુમલાખોર ઈ-મેઈલ સિસ્ટમના ઉપયોગનો ગેરલાભ લઈ સંસ્થાકીય કે વ્યક્તિગત પ્રવૃત્તિમાં અડચણ ઊભી કરે છે. તે ખાનગી માહિતીનો ઉપયોગ કરવાનો પ્રયત્ન કરે છે, સ્રોત માટેનો IT ઉપયોગ ખોરવી નાખે છે અથવા તો સંસ્થા પર નિયંત્રણ મેળવી લે છે. જ્યારે લોકો ઈ-મેઈલનો ઉપયોગ કરતા હોય ત્યારે સામાન્ય રીતે જોવા મળતા જોખમોમાં મલવેર, સ્પામ, ફિશિંગ, સોશિયલ એન્જિનિયરિંગ, સ્રોતનો અનધિકૃત ઉપયોગ અને અંગત માહિતી જાહેર કરી દેવાનો સમાવેશ થાય છે. આ જોખમો કોઈ વ્યક્તિ કે સંસ્થાને કેવી રીતે અસર કરશે તેના વિષે વિસ્તૃત સમજૂતી મેળવીએ.

સ્પામ (Spam) : આપણા મેઈલબોક્સમાં મળતા વણમાગ્યા વ્યાવસાયિક કે અવ્યાવસાયિક ઈ-મેઈલને સામાન્ય રીતે સ્પામ તરીકે ઓળખવામાં આવે છે. સ્પામનું વલણ કમ્પ્યૂટરમાં આવેલ ડિસ્કની જગ્યા, મેમરી કે પ્રોસેસર જેવા સ્રોતનો ઉપયોગ કરી ઉપયોગકર્તાની કાર્યક્ષમતા ખોરવી નાખવાનું હોય છે. વધુમાં, મલવેરના ફેલાવા માટે પણ તેનો ઉપયોગ કરવામાં આવે છે. હાલમાં ઈ-મેઈલ સિસ્ટમમાં ''સ્પામ'' નામનું એક સ્વતંત્ર ફોલ્ડર આપવામાં આવે છે અને તે આ પ્રકારના ઈ-મેઈલની સ્પામ તરીકે નોંધ કરે છે.

સોશિયલ એન્જિનિયરિંગ(Social Engineering) : વ્યક્તિની કે સંસ્થાની સંવેદનશીલ માહિતીને કબજે કરી લેવાની પ્રક્રિયાને સોશિયલ એન્જિનિયરિંગ કહે છે. ઈ-મેઈલ સ્પૂફિંગ (E–mail spoofing) એ એક સામાન્ય સોશિયલ એન્જિનિયરિંગ હુમલો છે, જેમાં વિગતોની ગેર-રજૂઆત દ્વારા વ્યક્તિ કે પ્રોગ્રામ મોકલનાર દ્વારા અધિકૃત ઉપયોગકર્તા હોવાનો સફળતાપૂર્વક દેખાવ કરવામાં આવે છે. ઉદાહરણ તરીકે,સંસ્થાના આઈ.ટી. વિભાગને તેના એકાઉન્ટ ઓફિસર તરફથી એક સંદેશ મળી શકે છે. (અહીં હુમલાખોર એકાઉન્ટ ઓફિસરના ઓળખપત્રનો ઉપયોગ કરી રહ્યો છે) તેમાં દર્શાવ્યા અનુસાર એકાઉન્ટ ઓફિસર કોઈ અત્યંત મહત્વની માહિતી માટેનો પાસવર્ડ ભૂલી ગયા છે અને તેને રીસેટ કરવાની માંગણી કરે છે.

સ્રોતનો અનધિકૃત ઉપયોગ (Unauthorized access to resources) : દુષ્ટ હેતુ ધરાવતા હેકર કે અતિક્રમણ કરનાર વ્યક્તિ સ્રોતનો અનધિકૃત ઉપયોગ કરવા માટે મેઈલ સર્વર પર સફળ હુમલો કરીને ઈ-મેઈલ સિસ્ટમનો ઉપયોગ કરી શકે છે.

માહિતી જાહેર થઈ જવી(Information leak) : લોકો જુદી જુદી જગ્યાએ જુદાં જુદાં સાધનોની મદદથી ઈ-મેઈલ સેવાનો ઉપયોગ કરે છે. એકથી વધુ જગ્યા પરથી ઈ-મેઈલનો ઉપયોગ કરવાની રીત ક્યારેક કોઈ હેતુ વગર પણ માહિતીને જાહેર કરી દે છે.

અહીં એ નોંધ લેવી પણ જરૂરી છે કે આગળના મુદ્દામાં ચર્ચેલ મલવેર અને ફિશિંગ હુમલાઓ પણ ઈ-મેઈલ દ્વારા સરળતાથી પ્રયોજી શકાય છે.

ઈ-મેઈલના રોજેરોજ વધતા ઉપયોગને કારણે સંચારણ માટે ઈ-મેઈલ સેવાના ઉપયોગ સમયે અગમચેતી રાખવી એ ખૂબ જરૂરી બન્યું છે. સંસ્થા અને ઉપયોગકર્તાને ઈ-મેઈલ સેવાનો ઉપયોગ કરતી વખતે રાખવી પડતી અગમચેતી વિષે દિશાસૂચન મળે તે માટે અહીં કેટલાંક પગલાં આપવામાં આવ્યાં છે.

- સંસ્થાનો મેઈલ-સર્વર માટેનો વિનિયોગ સુરક્ષિત છે તેની ખાતરી કરો.
- તમે જે મેઈલ ક્લાયન્ટનો ઉપયોગ કરો છો તે સુરક્ષિત છે તેની ખાતરી કરો.
- મેઈલના વહન માટે ઉપયોગમાં લેવામાં આવેલ પ્રસારણ માધ્યમ સુરક્ષિત છે તેની ખાતરી કરો.
- સહાયક હાર્ડવેર અને સંચાલક ઘટકોને સુરક્ષિત બનાવો.
- અવિશ્વસનીય સ્રોત પરથી મેળવેલા ઈ-મેઈલને ખોલશો નહિ.
- ઈ-મેઈલના અનપેક્ષિત જોડાણને સ્કેન કર્યા વગર ક્યારેય ખોલશો નહિ.
- તમારા મેઈલ એકાઉન્ટ માટે મજબૂત પાસવર્ડની પસંદગી કરો.
- તમે જે સાધન પર ઈ-મેઈલ સેવાનો ઉપયોગ કરતા હો તેમાં અદ્યતન એન્ટી-વાયરસ સોફ્ટવેરનો ઉપયોગ કરો.
- કોઈ ભોજનાલય, મોલ કે તેના જેવા અન્ય જાહેર સ્થળોના વાઈ-ફાઈની મદદથી ઈ-મેઈલનો ઉપયોગ ન કરો.
- અન્ય વ્યક્તિ ઉપયોગ કરી શકે તે રીતે તમારા મશીનને રેઢું મૂકીને તેનાથી દૂર ન જાઓ.

સ્વાધ્યાય

1. સાયબર સુરક્ષા એટલે શું?

2. ઈ-મેઈલનો ઉપયોગ કરતી વખતે ઉદ્‌ભવતા જોખમોની યાદી બનાવી સમજાવો.

3. ડેટા એક્સપોઝર એટલે શું? શેના દ્વારા સંસ્થાને તેનાથી બચાવી શકાય?

4. નીચેના પદની વ્યાખ્યા આપો:

(a) Spam (b) Ransomware (c) Malware (d) Phishing

5. **આપેલ વિકલ્પોમાંથી યોગ્ય વિકલ્પ પસંદ કરો :**

(1) નીચેનામાંથી શેના દ્વારા ખોટી વેબસાઈટ, પાનાં કે વેબ લિંક દ્વારા ભ્રમણા ઊભી કરી વ્યક્તિના ઈ-મેઈલના પ્રત્યુત્તર દ્વારા તેની સંવેદનશીલ માહિતી જાહેર કરી દેવામાં આવે છે?

(a) Cyber Bullying (b) Cyber Grooming (c) Phishing (d) Spam

(2) હેકર નીચેનામાંથી શેના દ્વારા ભોગ બનેલા ઉપયોગકર્તાના કમ્પ્યૂટર કે ફાઈલને લોક કરી દે છે?

(a) Malware (b) Spam (c) Phishing (d) Ransomware

(3) ઈ-મેઈલ સેવાનો ઉપયોગ કરતી વખતે નીચેનામાંથી કયું જોખમ ઉદભવી શકે છે ?

(a) Social Engineeing (b) Phishing (c) Spam (d) આપેલ તમામ