හැඳින්වීම

2020 වසර තුළ, කොවිඩ්19 වසංගතය ලොව පුරා ජනතාවගේ ජීවන රටාවේ පෙර නොවූ වෙනසක් ඇති කළේය. සාම්ප්‍රදායික භාණ්ඩ හා සේවා සඳහා ඇති ඉල්ලුම සැලකිය යුතු ලෙස වෙනස් වූ අතර තොරතුරු තාක්ෂණය හා සම්බන්ධ සේවාවන් සඳහා ඇති ඉල්ලුම ක්ෂණිකව වැඩි විය. මෙම නව ප්‍රවණතාවලට අනුගත වීම, ධනාත්මක හා ඍණාත්මක බලපෑම් ඇති කරන නව වෙළඳපොළ සහ අවස්ථාවන් නිර්මාණය කිරීමට හේතු විය. වර්තමාන තත්ත්වය තුළ ආයතන සහ පොදු ජනතාව අතර අවධානය දිනාගෙන ඇති එවැනි ප්‍රධාන මාතෘකා දෙකක් වන්නේ සයිබර් ආරක්ෂාව සහ සයිබර් අපරාධ ය.[1]

තොරතුරු තාක්ෂණය පදනම් කරගත් නව ආර්ථික ක්‍රියාකාරකම්

වසංගතය හේතුවෙන් රටවල් විසින් අනුගමනය කරන ලද සංචරණ සීමා කිරීම් නිසා සාම්ප්‍රදායික ආර්ථික ක්‍රියාකාරකම් හි නව ප්‍රවණතා මතු විය. තොරතුරු තාක්ෂණය හා අදාළ සේවාවන් මත බොහෝදුරට රඳා පවතින එවැනි ප්‍රධාන ප්‍රවණතා කිහිපයක් පහත ඉදිරිපත් කර ඇත.

අ) නිවසේ සිට රාජකාරි කිරීම

වසංගතයේ පළමු රැල්ල අතරතුර, බොහෝ රටවලට සැලකිය යුතු පූර්ව අත්දැකීම් හෝ වසංගතයෙන් පැන නගින නව තත්ත්වයන්ට මුහුණ දීමට සූදානමක් නොතිබුණි. වෛරසය පැතිරීම මැඩපැවැත්වීම සඳහා රටවල් පුරා ක්ෂණික ප්‍රතිචාරය වූයේ විවිධාකාරයේ සංචරණ සීමා පැනවීමයි. මෙම හදිසි වෙනස හේතුවෙන් භෞතික සේවා ස්ථානවල සිට සේවය කල සේවකයින්ට නිවසේ සිට රාජකාරි කිරීමේ ක්‍රමය වෙත කඩිනමින් මාරු වීමට සිදු විය. ඒ සඳහා සුදුසු යටිතල පහසුකම් සේවකයින්ට හෝ ආයතනවලට ප්‍රමාණවත්ව නොතිබුණි. මෙම ගැටලුව ලැප්ටොප් වැනි උපකරණ සම්බන්ධයෙන් පමණක් නොව, ආයතනික පද්ධති සහ ජාල වෙත ආරක්ෂිතව ප්‍රවේශ වීම සම්බන්ධයෙන් ද නිරීක්ෂණය විය. ඊමේල් සහ අන්තර්ජාල භාවිතය වැඩි වීමට අමතරව, බොහෝ ආයතන මේ සඳහා අතථ්‍ය පුද්ගලික ජාල (VPN)භාවිතා කළහ. තවද, මහා පරිමාණයෙන් රාජකාරි කටයුතු කිරීම සඳහා පුද්ගලික උපාංග භාවිතා කිරීම, ඉතා කෙටි කාලයක් තුළ ආරම්භ විය. පිළිගත් ප්‍රමිතීන්ට අනුකූලව මෙම පුද්ගලික උපාංග බොහොමයක් ප්‍රමාණවත් ලෙස සුරක්ෂිත කර නොතිබුණි.

ආ) මංගත ඉගෙනීම

අධ්‍යාපන ආයතන වරින් වර වසා දැමීමට සිදු වූ නිසා සියලුම අධ්‍යාපන කටයුතු සූම් (Zoom) සහ මයික්‍රොසොෆ්ට් ටීම්ස් (Microsoft Teams) වැනි අන්තර්ජාල ඉගෙනුම් මාධ්‍ය ඔස්සේ සිදු කිරීමට ගුරුවරු සහ කථිකාචාර්යවරු ඇතුළු ඉගැන්වීමේ කාර්ය මණ්ඩල යොමු වූහ. මෙහිදී සිසුන්ට සහභාගී වීමේ හැකියාව වර්ධනය කිරීම සඳහා අන්තර්ජාල ඉගෙනුම් මාධ්‍ය හෝ ඒ හා සමාන වට්ස්ඇප් (WhatsApp) වැනි වෙනත් මාධ්‍ය භාවිතා කරමින් පාඩම් සහ පැවරුම් බෙදා දෙන ලදී. පෙර පාසල් සිසුනු පවා අන්තර්ජාලය හරහා ගුරුවරුන් සමඟ විනාඩි 30 සිට පැය 1 දක්වා ඉගෙනුම් සැසි ආරම්භ කළහ. දෙමව්පියන්ගේ වැඩි පාලනයක් හෝ අවධානයක් නොමැතිව පෙරට වඩා දිගු කාලයක් අන්තර්ජාල පහසුකම් සහිත ජංගම උපාංග භාවිතා කිරීමට මෙහිදී සිසුන්ට අවස්ථාව හිමි විය.

ඇ) ඊ-වාණිජ්‍යය (E-commerce)

සාම්ප්‍රදායික ලෙස වෙළඳ සැල් හරහා භාණ්ඩ අළෙවි කිරීමේ යෙදුනු බොහෝ වෙළෙන්දෝ වේගයෙන් මංගත විකුණුම් ක්‍රම වෙත යොමු වූහ. ඒ අතරම, කොවිඩ්19 වේගයෙන් පැතිරීම වැළැක්වීම සඳහා පැන වූ සමාජ ආර්ථික කටයුතු සීමා කිරීම සහ සංචරණ සීමාවන් හේතුවෙන් ගනුදෙනුකරුවෝ ද වේගයෙන් අන්තර්ජාල මිලදී ගැනීම් වෙත යොමු වූහ. විකුණුම්කරුවන් සහ ගනුදෙනුකරුවන් ඉතා කෙටි කාලයක් තුළ මහා පරිමාණ වශයෙන් මංගත වේදිකාවලට යොමු වුවද, අදාළ පද්ධති ඊට සරිලන පරිදි සකස් වී නොතිබීමෙන් ඒවා බිඳවැටීම්වලට ලක්විය. වසංගතය සැලකිල්ලට ගනිමින් භෞතික මුදල් භාවිතය අඩු වීමක් සිදු වූ අතර මේ නිසා ද මංගත ගනුදෙනු ඉහළ යෑම සිදු විය.

ඈ) මංගත මූල්‍ය සේවා

බොහෝ බැංකු සහ මූල්‍ය ආයතන, තම ගනුදෙනුකරුවන්ට බැංකු ශාඛා වෙත යෑම අවම කිරීම සඳහා මංගත මූල්‍ය සේවා භාවිතා කිරීමට උනන්දු කළේය. මෙහි ප්‍රතිඵලයක් ලෙස අන්තර්ජාල බැංකු වෙබ් අඩවි සහ ජංගම යෙදුම් භාවිතය වැඩි විය. තොරතුරු සාක්ෂරතා මට්ටම අඩු පුද්ගලයින්ට දෛනික අවශ්‍යතා සඳහා මෙම මංගත මූල්‍ය සේවා භාවිතා කිරීමට සිදු වූ අතර මූල්‍ය සේවාවන්හි ප්‍රවේශය පුළුල් කිරීම සඳහා නොයෙකුත් සීමාවන් ලිහිල් කිරීමට ද සිදු විය.

---

1 සයිබර් ආරක්ෂාව යනු පරිගණක පද්ධති, ජාල, වැඩසටහන්, උපාංග සහ දත්ත, සයිබර් ප්‍රහාර, හානි හෝ අනවසර ප්‍රවේශයන්ගෙන් ආරක්ෂා කිරීම සඳහා තාක්ෂණයන්, ක්‍රියාවලි සහ පාලනයන් යෙදීමයි. සයිබර් අපරාධ යනු පරිගණකයක්, ජාලගත උපාංගයක් හෝ ජාලයක් සම්බන්ධ ඕනෑම සාපරාධී ක්‍රියාවකි. බොහෝ සයිබර් අපරාධ සිදු කරනු ලබන්නේ සයිබර් අපරාධකරුවන්ට ලාභ උපයා ගැනීම සඳහා වන අතර, සමහර සයිබර් අපරාධ පරිගණක හෝ උපාංගවලට ඍජුවම හානි කිරීමට හෝ අක්‍රීය කිරීමට සිදු කරනු ලබන අතර අනිෂ්ට මෘදුකාංග, නීති විරෝධී තොරතුරු, රූප හෝ වෙනත් ද්‍රව්‍ය ව්‍යාප්ත කිරීම සඳහා පරිගණක හෝ ජාල භාවිතා කරයි.

ඉ) සංචරණ සීමා හේතුවෙන් මංගත රැස්වීම් සහ සම්මන්ත්‍රණ (virtual meetings and conferences) පැවැත්වීම

වසංගතය හේතුවෙන් පැනවුණු සංචරණ සීමා සහ සමාජ දුරස්ථ නිර්දේශයන් සමඟ පුද්ගල රැස්වීම් සහ සම්මන්ත්‍රණ, මංගත ක්‍රමවේද ඔස්සේ පැවැත්වීමට ආයතනවලට සිදු විය. මංගත රැස්වීම් මුළුමනින්ම නව සංකල්පයක් නොවුන ද, එය සැලකිය යුතු සේවක පිරිසකට, සාපේක්ෂව නව අත්දැකීමක් විය. විවිධ ආයතන මේ සඳහා විවිධ මෙවලම් භාවිතා කළ බැවින් එය දත්ත සුරක්ෂිතතාවයට අභියෝග කිහිපයක් එල්ල කළේය. බුද්ධිමය දේපළ සහ වෙළඳ රහස් ඇතුළු පුළුල් පරාසයක රහස්‍ය තොරතුරු අන්තර්ජාලය හරහා බෙදාගත යුතු වූ අතර රැස්වීම් කටයුතුවල රහස්‍යභාවය ආරක්ෂා කිරීම සඳහා අත්‍යවශ්‍ය ආරක්ෂක පියවරයන් පිළිබඳව බොහෝ රැස්වීම් සංවිධායකයන් සහ සහභාගිවන්නන් දැන සිටියේ නැත.

වසංගතය හේතුවෙන් ඉහළ ගිය අන්තර්ජාල භාවිතය නිසා වර්ධනය වූ සයිබර් අපරාධ

අ) තතුබාන (phishing) ඊමේල්

නිවසේ සිට රාජකාරි කිරීම, සයිබර් අපරාධකරුවන්ට විවිධ වර්ගයේ සයිබර් ප්‍රහාර දියත් කිරීමට කදිම අවස්ථාවක් නිර්මාණය කර දුනි. මෙම ප්‍රහාර වලින් බොහොමයක් ආරම්භ වූයේ අයාචිත තැපැල් / තතුබාන ඊමේල්වලින් (spam/phishing email) වන අතර එමඟින් ඊමේල් භාවිතා කරන්නන්ගේ සංවේදී හා රහස්‍ය තොරතුරු, ඔවුන්ගේ අනුදැනුමකින් තොරව නොදන්නා තෙවන පාර්ශවයකට හෙළි කිරීමට, ඊමේල් පරිශීලකයින්ව පොළඹවයි. සමහර තතුබෑම් ඊමේල් නිර්මාණය කරන ලද්දේ නිශ්චිත පුද්ගලයින් හෝ සංවිධානයක් ඉලක්ක කර ගනිමිනි. මෙම තතුබෑම් ඊමේල් ඉතා සංකීර්ණ ක්‍රම භාවිතා කරමින්, අයාචිත තැපැල් පෙරහන් (spam filter) මග හැර පරිශීලකයින්ගේ ඊමේල් පද්ධති වෙත ළඟා වේ. මෙම සියලු තොරතුරු එක්රැස් කිරීමෙන් පසුව සයිබර් අපරාධකරුවන්ට ව්‍යාපාරවල ඉතා තීරණාත්මක තොරතුරු පද්ධති වෙත සයිබර් ප්‍රහාර සැලසුම් කිරීමට සහ ක්‍රියාත්මක කිරීමට හැකි වූ අතර එමඟින් මූල්‍ය ප්‍රතිලාභ ලබා ගැනීමට ද හැකි විය.

ආ) උපාංග පොදුවේ භාවිතා කිරීම සහ අනවසර මෘදුකාංග භාවිතය.

බොහෝ සිසුන්ට ඔවුන්ගේ අධ්‍යයන කටයුතු සඳහා දෙමාපියන්ගේ උපාංග බෙදා ගැනීමට සිදු වන අතර සයිබර් ප්‍රහාරකයින් විසින් මෙම සිසුන් ඉලක්ක කර ගනිමින් සයිබර් ප්‍රහාර දියත් කරන ලදී. මෙහිදී අනිෂ්ට වෙබ් අඩවි වෙත පිවිස නොමිලේ ලැබෙන මෘදුකාංග සහ පරිගණක ක්‍රීඩා බාගත කර මෙම උපාංග වෙත ස්ථාපනය කිරීමට සිසුහු නැඹුරු වෙති. නොමිලේ ලැබෙන මෙම මෘදුකාංග බොහොමයක් සමඟ තොරතුරු සොරකම් කිරීම, යතුරු ලොගනය[2] (keylogging) සහ අන්තර්ජාලයට සම්බන්ධ වෙනත් උපාංගවලට සයිබර් ප්‍රහාර දියත් කරන බොට්ස්[3] (bot) ලෙස ක්‍රියා කිරීම වැනි විවිධ අරමුණු සඳහා භාවිතා කරන අනිෂ්ට මෘදුකාංග ක්‍රියාත්මක වේ.

ඇ) ව්‍යාජ වෙබ් අඩවි / යෙදුම්

ඊවාණිජ්‍යයේ උත්පාතය සමඟ සයිබර් අපරාධකරුවන්ට, තතුබාන ඊමේල් (spam email) යැවීමෙන් සහ අන්තර්ජාල වෙළඳසැලක්, බැංකු වෙබ් අඩවියක් ලෙස මවාපාමින් ව්‍යාජ වෙබ් අඩවි හෝ ජංගම යෙදුම් සැකසීම මගින්, ණයපත් (credit card) විස්තර වැනි ගනුදෙනුකරුවන්ගේ සංවේදී දත්ත සොරකම් කිරීම ඉතා පහසුවෙන් කර ගත හැකි විය. සමහර සංවිධානාත්මක අපරාධකරුවෝ වින්දිතයින්ගෙන් සංවේදී දත්ත සොරකම් කර වින්දිතයින්ට අයත් බැංකු ගිණුම් සඳහා මංගත බැංකු පැතිකඩ නිර්මාණය කර මෙම ගිණුම්වල මුදල් සොරකම් කරති.

ඈ) තොරතුරු ආරක්ෂණ අවධානය නැතිවීම

නිවසේ සිට රාජකාරි කිරීම, දුරස්ථ ප්‍රවේශය සහ වෙනත් අවශ්‍යතා සඳහා ඇති ඉල්ලුම වැඩිවීමත් සමඟ බොහෝ ආයතනවල තොරතුරු සුරක්ෂිතතාව කෙරෙහි තිබූ අවධානය ගිලිහී ගොස් ඇත. තොරතුරු ආරක්ෂණ වෘත්තිකයන් ද නිවසේ සිට වැඩ කරන විට සහ ඔවුන්ගේ අවධානය වෙනත් නව අභියෝගයන් වෙත යොමු වන විට, සයිබර් ආරක්ෂාව හා සම්බන්ධ පොදු කාර්යයන් (පද්ධති යාවත්කාලීන කිරීම්, පැච් කළමනාකරණය, ලොග් අධීක්ෂණය, ආරක්ෂක සිදුවීම් පිළිබඳ විමර්ශනය) අවධානයට ලක් නොවන අතර මෙම තත්ත්වයන් ද සයිබර් ප්‍රහාරකයින්ට හොඳ අවස්ථාවක් සපයයි.

ඉදිරි පියවර

වසංගතයේ පැවැත්ම කෙටි කලක් විය හැකි වුවද, එහි බලපෑම ඉදිරි වසර කිහිපය තුළ පවතිනු ඇත. එබැවින්, නව සම්මතයන්ට අනුකූලව ඉදිරියට යෑමට සහ සයිබර් ආරක්ෂණය සහ සයිබර් ප්‍රතිරෝධය වැඩිදියුණු කිරීමට ආයතනවලට කෙටිකාලීන, මධ්‍ය කාලීන හා දිගු කාලීන සැලසුම් තිබීම අත්‍යවශ්‍ය වේ.

අ) සයිබර් ප්‍රහාර සඳහා ඔරොත්තු දීමේ හැකියාව ශක්තිමත් කිරීම

සයිබර් අපරාධ පිළිබඳ නවීකරණය ඉතා වේගයෙන් ඉහළ යන නිසා ඉතා ඉහළ මට්ටමේ සයිබර් ආරක්ෂණ පියවරයන් අනුගමනය කළ ආයතනවලට පවා ඔවුන් සයිබර් ප්‍රහාරවලින් සම්පූර්ණයෙන්ම ආරක්ෂා වී ඇති බවට සහතික වීමට නොහැකි වී තිබේ. සමහර අනිෂ්ට මෘදුකාංග සැබෑ ප්‍රහාරයක් එල්ල කිරීමට පෙර දින 240 ක් වැනි දිගු කාලයක් ආයතනයක පරිගණක ජාලයක අනාවරණය නොවී සිටිය හැකි යැයි විශ්වාස කෙරේ. එමනිසා, බොහෝ ආයතන දැන් අවධානය යොමු කරන්නේ සයිබර් ප්‍රහාර

2 පරිගණක යතුරු ප්‍රවරුවක සියලුම යතුරු එබීම රහසිගතව නිරීක්ෂණ මෙවලමක් ලෙස හෝ ඔත්තු මෘදුකාංග ලෙස පටිගත කිරීම සඳහා මෘදුකාංග වැඩසටහනක් හෝ දෘඩාංග උපාංගයක් (යතුරු ප්‍රවරුව) භාවිතා කිරීම

3 ස්වයංක්‍රීය හෝ අවම මිනිස් මැදිහත්වීමකින් සබැඳි සෙවුම් ලෙස විධාන ක්‍රියාත්මක කිරීමට, පණිවිඩවලට පිළිතුරු දීමට හෝ සාමාන්‍ය කාර්යයන් කළ හැකි මෘදුකාංග වැඩසටහනකි

සඳහා ඔරොත්තු දීමේ හැකියාව ලබා ගැනීම සඳහා ය. එයින් අදහස් වන්නේ, සයිබර් ප්‍රහාරයක් මගින් තොරතුරු තාක්ෂණ පද්ධති අක්‍රීය කරනු ලැබුවහොත්, අවම බලපෑමකින් යුතුව ආයතනයට සිය සාමාන්‍ය ක්‍රියාකාරිත්වය නැවත ආරම්භ කළ හැකි බවයි. වලාකුළු පරිගණකකරණය (cloud computing) ඇතුළු තොරතුරු තාක්ෂණ යටිතල පහසුකම් කර්මාන්තයේ වර්ධනයන් මඟින් ව්‍යාපාරවලට අවශ්‍ය සයිබර් ඔරොත්තු දීමේ හැකියාව ළඟා කර ගැනීමට හැකි වී තිබේ.

ආ) වසංගත ආශ්‍රිත තත්ත්වයන් සඳහා ව්‍යාපාර අඛණ්ඩ සැලසුම්කරණය (Business Continuity Planning)

මූල්‍ය අංශය ඇතුළු බොහෝ කර්මාන්ත සඳහා ව්‍යාපාර අඛණ්ඩ වැඩසටහන් සැලසුම් කිරීම, පරීක්ෂා කිරීම සහ ක්‍රියාත්මක කිරීම අනිවාර්ය වේ. මෙම ව්‍යාපාර අඛණ්ඩ වැඩසටහන්වලින් බොහොමයක් ස්වාභාවික හෝ මිනිසා විසින් සාදන ලද ව්‍යසන, තාක්ෂණික අසමත්වීම් වැනි පරීක්ෂණ අවස්ථා ආවරණය කරයි. කෙසේ වෙතත්, වසංගත ආශ්‍රිත ව්‍යාපාර අඛණ්ඩ වැඩසටහන් බොහෝ සංවිධාන තුළ ක්‍රියාත්මක කර හෝ පරීක්ෂා කර නොමැති බව නිරීක්ෂණය විය. වසංගත අවස්ථාවක විශේෂත්වය නම් සමාජ ආර්ථික කටයුතු සීමා කිරීම හේතුවෙන් තොරතුරු පද්ධති සඳහා භෞතික ප්‍රවේශය ලබා ගත නොහැකි වීම සහ ඒවා හසුරුවන විශේෂ පුද්ගලයින් නොමැති වීමය. මෙවැනි අවස්ථාවක තොරතුරු ආරක්ෂක ව්‍යක්තිකයන් ගේ භූමිකාව ඉටු කල හැකි වෙනත් සේවකයන් සපයා ගැනීම ආයතනවලට දුෂ්කර විය හැකිය. මෙම සේවකයින්ට වසංගතය බලපාන්නේ නම්, එය එම විශේෂිත සේවා ක්ෂේත්‍රයේ රික්තයක් ඇති කරයි. එබැවින්, ආයතනවලට ඔවුන්ගේ ව්‍යාපාර අඛණ්ඩ සැලසුම්කරණය සඳහා දුරස්ථ වැඩ කිරීමේ විධිවිධාන සහ ප්‍රමාණවත් මානව සම්පත් ඇතුළත් කිරීම අත්‍යවශ්‍ය වේ.

ඇ) ප්‍රමාණවත් අයවැයක් වෙන් කිරීම

නිවසේ සිට වැඩ කිරීමේ නව සම්මතයන් සමඟ, සීමිත ප්‍රවේශයන් සහ වෙනත් දැඩි පාලනයන්ගෙන් ආරක්ෂා කළ තොරතුරු පද්ධති ආරක්ෂා කිරීම ආයතනවලට අතිශයින් දුෂ්කර වී ඇත. මෙම නව පහසුකම් සඳහා ඉඩ දෙන අතරම, ආයතන ඔවුන්ගේ තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කිරීම සඳහා කෙටි හා දිගු කාලීන සැලසුම් ක්‍රියාත්මක කළ යුතුය. සයිබර් ආරක්ෂාව සඳහා විශාල පිරිවැයක් දැරීමට සිදු වන අතර තොරතුරු සුරක්ෂිතතාව සඳහා අයවැයක් වෙන් කිරීම විශාල පරිමාණයේ ආයතනවලට පවා අපහසුය. තොරතුරු සුරක්ෂිතතාවයට අදාළ සම්පත් බෙදා හදා ගැනීම සඳහා විවිධ ක්ෂේත්‍ර තුළ ආයතන අතර සහයෝගිතාව දිගු කාලීනව සැමට ප්‍රයෝජනවත් වනු ඇත. කෙටිකාලීනව, ආයතන තම තොරතුරු තාක්ෂණ වත්කම් ආරක්ෂා කර ගැනීම සඳහා පවතින සයිබර් ආරක්ෂණ සම්පත් උපරිම ලෙස භාවිතා කිරීම කෙරෙහි වැඩි අවධානයක් යොමු කළ යුතුය.

ඈ) පරිශීලක දැනුවත්භාවය

සයිබර් ආරක්ෂණයේ වැදගත්ම අංගය ලෙස පරිශීලක දැනුවත්භාවය සැලකිය හැකිය, එයට හේතුව වන්නේ පද්ධති දුර්වලතා නිර්මාණය කර සයිබර් අපරාධකරුවන්ට ආයතනික පද්ධතිවලට ඇතුළුවීමට මග සලසන්නේ පරිශීලකයන් වන බැවිනි. රාජකාරී හා පෞද්ගලික කාර්යයන් අතර පැහැදිලි වෙනසක් නොපවතින අතර නිල කාර්යයන් සඳහා පුද්ගලික උපාංගත් පුද්ගලික කාර්යයන් සඳහා නිල උපාංගත් භාවිතා කිරීම නිතරම සිදු වේ. එබැවින්, අවශ්‍ය ආරක්ෂක අංග සමඟ එවැනි උපකරණ නිසි ලෙස නඩත්තු නොකෙරේ නම් මෙය ද සයිබර් ආරක්ෂාවට අවදානමක් වේ. පරිශීලකයෝ බොහෝවිට මෙම අවදානම් ගැන දැන නොසිටිති. එබැවින්, සයිබර් ආරක්ෂාව පිළිබඳව වඩාත් දැනුවත් වීම සහ ආරක්ෂිතව සිටීම සෑම අයෙකුගේම වගකීමකි. සේවකයින් අතර පරිශීලක දැනුවත්භාවය ඇති කිරීම කෙරෙහි ආයතන වැඩි අවධානයක් යොමු කළ යුතුය. පාසල් හා විශ්ව විද්‍යාල ද එය අනුගමනය කළ යුතුය.

ඉ) ජාතික පරිගණක සිදුවීම් ප්‍රතිචාර කණ්ඩායම් (CIRTs) සමඟ සම්පට කටයුතු කිරීම

රටක් තුළ සයිබර් ප්‍රහාරයන්ට, සයිබර් ආරක්ෂණ ප්‍රතිචාර සම්බන්ධීකරණය කිරීම සඳහා ජාතික මධ්‍යස්ථානය ලෙස සේවය කරන පරිගණක සිදුවීම් ප්‍රතිචාර කණ්ඩායම් බොහෝ රටවල පිහිටුවා ඇත. මේ සඳහා ශ්‍රී ලංකාවේ පිහිටුවා ඇති ආයතනය වන්නේ ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදයයි (Sri Lanka CERT). ඔවුන්ගේ මෙහෙවර වන්නේ රාජ්‍ය හා පෞද්ගලික අංශයේ ආයතනවල සහ සාමාන්‍ය ජනතාව අතර තොරතුරු තාක්ෂණ භාවිතා කරන්නන් ආරක්ෂා කිරීම ය. එබැවින්, ඕනෑම පුද්ගලයෙකුට හෝ සංවිධානයකට අවශ්‍ය විටෙක සයිබර් ආරක්ෂණය සම්බන්ධයෙන් ඔවුන්ගේ සේවාවන් සහ උපදේශනය ලබා ගත හැකිය.

සමාජ්තිය

වසංගත තත්ත්වයත් සමඟ උද්ගත වී ඇති සයිබර් තර්ජන සැලකිල්ලට ගනිමින් සයිබර් ආරක්ෂණය, ආයතන මණ්ඩල තුල විශේෂ අවධානයට ලක් වන මාතෘකාවක් බවට පත් විය යුතුය. වසංගතයේ දෙවන රැල්ල හරහා ගමන් කරන අතරතුර තුන්වන රැල්ලක් ඇති විය හැකි බවට සැලකිලිමත් වෙමින් සෑම ආයතනයක් ම සයිබර් ප්‍රහාර වැළැක්වීමේ පියවර ක්‍රියාත්මක කළ යුතු අතර සයිබර් ප්‍රහාර හඳුනා ගැනීම, ප්‍රතිචාර දැක්වීම සහ ප්‍රතිසාධන හැකියාවන් ශක්තිමත් කර ගත යුතුය. අද පවතින සම්බන්ධිත ලෝකයේ සයිබර් අපරාධ වලින් ආරක්ෂා වීම සෑම පුද්ගලයෙකුගේම වගකීමකි. ඒ අතරම, සයිබර් අපරාධවලට එරෙහිව සටන් කිරීමට සහ වර්තමාන සහ අනාගත පරම්පරාවන් සඳහා ආරක්ෂිත ලෝකයක් ගොඩනැගීමට ආයතනික, ආංශික, ජාතික සහ ජාත්‍යන්තර මට්ටමින් සාමූහික ප්‍රවේශයක් අවශ්‍ය වේ.