ඩිජිටල් ප්‍රහාරවලින් අපේ රටේ අත්‍යවශ්‍ය සේවා ආරක්ෂා කරගැනීමේ වැදගත්කම

මහි කිරිඳිගොඩ (2/June/2025)
සම්බන්ධීකාරක - ඩිජිටල් හඬ්ල්
කළමණාකාර අධ්‍යක්ෂක - ෆලකේස් සොෆ්ට් ටෙක්නොලොජීස් පුද්. සමාගම

අද වන විට ලෝකය වේගයෙන් ඩිජිටල්කරණය වෙමින් පවතින අතර, ශ්‍රී ලංකාව ද ඩිජිටල් ආර්ථිකයක් ගොඩනැගීමේ අරමුණින් යුතුව මෙම ගමනට අවතීර්ණ වී සිටී. මෙම පරිවර්තනය මගින් සේවා කාර්යක්ෂමතාවය ඉහළ නංවන අතර, සමස්ත ආර්ථික වර්ධනයට ද සැලකිය යුතු දායකත්වයක් සපයනු ඇත.[1] කෙසේ වෙතත්, මෙම ඩිජිටල්කරණයත් සමඟම සයිබර් ප්‍රහාරවල තර්ජනය ද පෙර නොවූ විරූ ලෙස වැඩි වී තිබේ. මෙම තර්ජන ජාතියක ආරක්ෂාවට, ආර්ථික ස්ථාවරත්වයට සහ මහජන යහපැවැත්මට සෘජු තර්ජනයක් එල්ල කරයි.[1]

අත්‍යවශ්‍ය පද්ධති සහ වත්කම් ආරක්ෂා කිරීම අද වන විට ප්‍රමුඛතම සැලකිල්ලක් බවට පත්ව ඇත. මන්දයත්, විදුලිය, ජලය, සෞඛ්‍ය සේවා සහ ප්‍රවාහන ජාල වැනි අත්‍යවශ්‍ය සේවා මිලියන ගණනක් ජනතාවගේ දෛනික ජීවිතයේ කොඳු නාරටිය වන බැවිනි.[2] මෙම පද්ධතිවලට සිදුවන එක් බාධාවක් හෝ විනාශයක් ජාතික ආරක්ෂාව, මහජන සෞඛ්‍යය සහ ආර්ථික යහපැවැත්මට අතිශයින් හානිකර බලපෑම් ඇති කළ හැකිය.[2] ඩිජිටල් පරිවර්තනයේ වේගවත් ව්‍යාප්තිය, ශ්‍රී ලංකාවට විශාල ආර්ථික අවස්ථා ගෙන එන අතරම, ප්‍රමාණවත් සයිබර් ආරක්ෂණ ක්‍රියාමාර්ග නොමැති නම්, නව ප්‍රහාරක මාර්ග විවෘත කරන අතර පවතින අවදානම් උග්‍ර කරයි. ඩිජිටල්කරණයේ ප්‍රතිලාභ, ආරක්ෂාව පිළිබඳව ප්‍රමාණවත් අවධානයක් යොමු නොකළහොත්, අවදානම් සමඟ සෘජු සමානුපාතික වේ. මෙය සයිබර් ආරක්ෂාව යනු හුදු තොරතුරු තාක්ෂණ ගැටලුවක් නොව, ජාතික සංවර්ධනයේ සහ ආර්ථික අනාගතයේ මූලික කුළුණක් බවට පත් කරයි.

මෑතකාලීන සිදුවීම්: අවදි කිරීමේ ඇමතුමක්

මෑතකාලීනව වාර්තා වූ ජාතික ජල සම්පාදන හා ජලාපවහන මණ්ඩලයේ දත්ත දත්ත සොරකම *** (2025 ජූනි 1) [6], නම සඳහන් නොකරන** පුද්ගලික බැංකු දත්ත දත්ත සොරකම *** (2025 මාර්තු) [8], සහ විශ්‍රාම වැටුප් දෙපාර්තමේන්තුවේ සිදුවීම (2025 මැයි) [10] වැනි සිදුවීම්, අපගේ අත්‍යවශ්‍ය සේවා සහ මූල්‍ය ආයතන සයිබර් ප්‍රහාරවලට ගොදුරු විය හැකි ආකාරය පිළිබඳ කදිම නිදසුන් සපයයි. මෙම සිදුවීම් වියුක්ත තර්ජන නොව, පුරවැසියන්ට සෘජුවම බලපාන සැබෑ ලෝක සිදුවීම් වේ.

මෙම මෑතකාලීන දත්ත දත්ත සොරකම *** හා සිදුවූ සමීපත්වය සහ ඒවායේ මහජන දත්ත වල පුද්ගලිකත්වයේ ස්වභාවය, සාමාන්‍ය ජනතාව අතර අවදානම පිළිබඳ දැඩි, සංවේදී හැඟීමක් ඇති කරයි. ඒවා තුලින් මහජනතාව ඇතුළු සියලු පාර්ශ්වකරුවන්ගේ ක්ෂණික අවධානය අවශ්‍ය වන ප්‍රබල "අවදි කිරීමේ ඇමතුමක්" ලෙස ක්‍රියා කරයි. මෙම සිදුවීම් මගින් අපගේ ඩිජිටල් යටිතල පහසුකම්වල ආරක්ෂාව තවදුරටත් ශක්තිමත් කිරීමේ හදිසි අවශ්‍යතාව අවධාරණය කරයි.

සංවේදී යටිතල පහසුකම් යනු කුමක්ද? ඒවා ඉලක්ක වන්නේ ඇයි?

ශ්‍රී ලංකාවේ සංවේදී යටිතල පහසුකම්

සංවේදී යටිතල පහසුකම් (Critical Infrastructure - CI) යනු ජාතියක ආරක්ෂාවට, ආර්ථික ස්ථාවරත්වයට සහ මහජන යහපැවැත්මට අත්‍යවශ්‍ය වන පද්ධති, ජාල සහ වත්කම් (භෞතික හා අතථ්‍ය) වේ. ඒවායේ බිඳවැටීමෙන් ජාතික ආරක්ෂාවට, මහජන සෞඛ්‍යයට, ආරක්ෂාවට හෝ මේ සියල්ලටම විනාශකාරී බලපෑමක් ඇති විය හැක.[2] මෙම පද්ධති අපගේ දෛනික ජීවිතයේ කොඳු නාරටිය වන අතර, සමාජ සාමය පවත්වා ගැනීමට සහ විභව ව්‍යසනකාරී බිඳවැටීම් වළක්වා ගැනීමට ඒවා ආරක්ෂා කිරීම අත්‍යවශ්‍ය වේ.[2]

එක්සත් ජනපදයේ, සන්නිවේදනය, බලශක්තිය, මූල්‍ය සේවා, සෞඛ්‍ය සේවා, තොරතුරු තාක්ෂණය, ප්‍රවාහන පද්ධති සහ ජල හා අපජල පද්ධති ඇතුළු අංශ 16 ක් සංවේදී යටිතල පහසුකම් ලෙස හඳුනාගෙන ඇත.[2] ශ්‍රී ලංකාව සම්බන්ධයෙන්, පර්යේෂණ අධ්‍යයනයන් මගින් හදිසි සේවා, ජලය, බලශක්තිය, ප්‍රවාහනය, විදුලි සංදේශ සහ මූල්‍ය යන අංශ සංවේදී යටිතල පහසුකම් ලෙස විශේෂයෙන් හඳුනාගෙන ඇත.[11] හදිසි සේවා අංශය පූර්ව හා පශ්චාත් ආපදා තත්ත්වයන් දෙකෙහිම වඩාත්ම වැදගත් යටිතල පහසුකම ලෙස සැලකේ.[11] ගෝලීය වශයෙන් සංවේදී යටිතල පහසුකම් පිළිබඳ පුළුල් නිර්වචනයක් තිබුණද, ශ්‍රී ලංකාවට වඩාත් සංකේන්ද්‍රිත නිර්වචනයක් තිබීම වැදගත්ය. මෙම දේශීය ප්‍රමුඛතාවය මගින් ඉලක්කගත සම්පත් වෙන් කිරීම් සහ ප්‍රතිපත්ති සංවර්ධනය සඳහා ඉඩ සැලසේ, නමුත් ඒ සමඟම, හඳුනාගත් මෙම අංශවල සිදුවන ඕනෑම දත්ත දත්ත සොරකමක් *** ජාතික ස්ථාවරත්වයට සහ මහජන ජීවිතයට අසමානුපාතික ලෙස ඉහළ බලපෑමක් ඇති කරයි. විශේෂයෙන්ම හදිසි සේවා වැනි අංශයකට එල්ල වන සයිබර් ප්‍රහාරයක් දත්ත අහිමි වීමෙන් ඔබ්බට ගොස්, ආපදා ප්‍රතිචාර දැක්වීමේ හැකියාව අඩාල කර, මහජන සෞඛ්‍යයට සහ ආරක්ෂාවට සෘජු

තර්ජනයක් එල්ල කළ හැකිය.

සයිබර් ප්‍රහාරකයන්ගේ ඉලක්ක බවට පත්වන හේතු

සංවේදී යටිතල පහසුකම් පද්ධතිවලට එල්ල වන සයිබර් ප්‍රහාර වැඩි වැඩියෙන් සංකීර්ණ, නිරන්තර සහ විභව බලපෑමෙන් යුක්ත වේ.[2] සයිබර් අපරාධකරුවන් විසින් කාර්මික පාලන පද්ධති (Industrial Control Systems - ICS) සහ SCADA පද්ධති (Supervisory Control and Data Acquisition) කඩාකප්පල් කළ හැකි Triton/TRISIS සහ Stuxnet වැනි අනිෂ්ට මෘදුකාංග සංවර්ධනය කර ඇත.[12] ජලය, බලශක්තිය සහ ප්‍රවාහන පද්ධති වැනි අත්‍යවශ්‍ය සේවා සඳහා අතිශයින් වැදගත් වන මෙම පද්ධතිවලට එල්ල වන ප්‍රහාර භෞතික ආරක්ෂාවට සෘජුවම බලපෑම් කළ හැකිය.[12] බොහෝ විට පැරණි තාක්ෂණයන් මත පදනම් වීම සහ හිමිකාරීත්වයෙන් යුතු ප්‍රොටෝකෝල භාවිත ICS/SCADA පද්ධතිවල ඇති සුවිශේෂී ස්වභාවය සයිබර් ප්‍රහාර විශේෂයෙන් ආකර්ශනීය ඉලක්ක බවට පත් කරයි. ඒවාට එල්ල වන සාර්ථක සයිබර් ප්‍රහාරයක් දත්ත දත්ත සොරකම්*** කිරීමෙන් ඔබ්බට ගොස්, සැබෑ ලෝකයේ බාධා කිරීම්, පාරිසරික හානි හෝ ජීවිත හානි පවා සිදු කළ හැකි අතර, සාමාන්‍ය තොරතුරු තාක්ෂණ දත්ත සොරකම්*** වලට වඩා අවදානම ඉහළ නංවයි.

ප්‍රහාරකයන්ගේ පොදු ඉලක්ක අතරට රාජ්‍ය ආයතන, මූල්‍ය ආයතන සහ නිෂ්පාදන සමාගම් ඇතුළත් වේ.[14] පොදු ප්‍රහාරක ක්‍රමවේදයන් වන්නේ අවදානමට ලක්විය හැකි පොදු යෙදුම් (public-facing applications) සහ සම්මුතිගත හෝ brute-forced credentials භාවිත කිරීමයි.[14] සැපයුම් දාම (supply chains) සහ විශ්වාසනීය සබඳතා (trusted relationships) හරහා සිදුවන ප්‍රහාර ද මෙවැනි තර්ජනයකි. මෙවැනි ප්‍රහාරවලින් අඩක් පමණ ප්‍රහාරය සාර්ථක වීමෙන් පසුව හඳුනාගැනේ.[14] සැපයුම් දාම දත්ත සොරකම් *** පිළිබඳ මෙම තොරතුරු ඉතා වැදගත්ය. එයින් පෙන්නුම් කරන්නේ සංවිධානයක සෘජු පද්ධති ආරක්ෂා කිරීම පමණක් ප්‍රමාණවත් නොවන බවයි; මෙම අවදානම් තෙවන පාර්ශවීය සැපයුම්කරුවන් හෝ හවුල්කරුවන්ගෙන් ද ආරම්භ විය හැකි බවයි. මෙය සංකීර්ණ යැපීම් ජාලයක් නිර්මාණය කරන අතර, ප්‍රාථමික සංවිධානයෙන් පිටත පවා දුර්වලම සම්බන්ධකය ප්‍රයෝජනයට ගත හැකිය. මෙම ප්‍රහාර බොහෝ විට සාර්ථක වීමෙන් පසුව හඳුනාගැනීම, සැලකිය යුතු හඳුනාගැනීමේ පරතරයක් සහ අභ්‍යන්තර පද්ධති පමණක් නොව සමස්ත ඩිජිටල් පරිසර පද්ධතියම වඩාත් ක්‍රියාකාරීව සහ අඛණ්ඩව අධීක්ෂණය කිරීමේ අවශ්‍යතාවය පෙන්නුම් කරයි.

කෘත්‍රිම බුද්ධිය (AI) භාවිතයෙන් සමාජ ඉංජිනේරු ප්‍රහාර (social engineering attacks), අනිෂ්ට මෘදුකාංග කේතීකරණය සහ මුරපද ප්‍රහාර වැඩි දියුණු කළ

හැක.[14] රාජ්‍ය අනුග්‍රහය ලබන සයිබර් අපරාධ සහ "ransomware-as-a-service" ගෝලීය වශයෙන් ඉහළ යමින් පවතී.[3]

ශ්‍රී ලංකාවේ මෑතකාලීන සයිබර් ප්‍රහාර: අපට ලැබුණු පාඩම්

ශ්‍රී ලංකාවට එල්ල වූ මෑතකාලීන ප්‍රධාන සයිබර් ප්‍රහාර කිහිපයක් පහත වගුවේ දැක්වේ. මෙම සිදුවීම් අපගේ ඩිජිටල් ආරක්ෂාවේ ඇති අඩුපාඩු සහ ඒවාට කඩිනමින් පිළියම් යෙදීමේ අවශ්‍යතාව පැහැදිලිව පෙන්වා දෙයි.

Table 1: මෑතකාලීන ශ්‍රී ලංකාවේ ප්‍රධාන සයිබර් සිදුවීම් (Recent Major Cyber Incidents in Sri Lanka)

සිදුවීම (Incident)	දිනය (Date)	බලපෑමට ලක් වූ ආයතනය/අංශය (Affected Entity/Sector)	ප්‍රහාරයේ වර්ගය (Type of Attack)	බලපෑම (Impact)
ජාතික ජල සම්පාදන හා ජලාපවහන මණ්ඩලය (NWSDB) SMS පද්ධති දත්ත සොරකම ***	2025 ජූනි 1	ජල සම්පාදන (Critical Infrastructure)	SMS Gateway Compromise / Ransom Demand	පාරිභෝගිකයින්ට Bitcoin කප්පම් ඉල්ලීම් සහිත පණිවිඩ නිල කෙටි කේතයෙන් ලැබීම [6]
නම සඳහන් නොකරන ** පුද්ගලික බැංකු දත්ත සොරකම ***	2025 මාර්තු	මූල්‍ය (Critical Infrastructure)	Ransomware / Data Exfiltration	දත්ත කාන්දු වීම (1.9 TB, පාරිභෝගික NIC ඡායාරූප, ගිණුම් අංක, කාර්ය මණ්ඩල දත්ත) [8]
ලංකා රජයේ ජාලය (LGN) ransomware ප්‍රහාරය	2023 අගෝස්තු 26	රජය (Critical Infrastructure)	Ransomware	5,000 කට අධික රජයේ ඊමේල් ගිණුම්වල දත්ත (මාස 3ක) නැතිවීම,

				ඔන්ලයින් උපස්ථ ද සංකේතනය වීම [15]
විශ්‍රාම වැටුප් දෙපාර්තමේන්තුව දත්ත සොරකම ***	2025 මැයි 26	රජය (Critical Infrastructure)	Ransomware / Data Exfiltration	617 GB දත්ත කාන්දු වීම (විශ්‍රාමිකයන්ගේ PII), අඳුරු වෙබ් අඩවිවලට දත්ත කාන්දු වීමේ අවදානම [10]

ජාතික ජල සම්පාදන හා ජලාපවහන මණ්ඩලයේ SMS පද්ධති දත්ත සොරකම * (National Water Supply and Drainage Board SMS System Breach)**

2025 ජූනි 1 වන දින, ජාතික ජල සම්පාදන හා ජලාපවහන මණ්ඩලයේ (NWSDB) නිල SMS gateway පද්ධතියට අනවසරයෙන් ඇතුළු වී ඇති බව වාර්තා විය.[6] මෙම ප්‍රහාරය හේතුවෙන්, පාරිභෝගිකයින්ට NWSDB හි නිල කෙටි කේතයෙන්ම "Your Waterboard account has been hacked by Alpha Team Your data can recover if we got 1.5 BTC" යනුවෙන් Bitcoin කප්පම් ඉල්ලා පණිවිඩ ලැබී ඇත.[6] මෙම පණිවිඩ නිල බිල්පත් සහ පැමිණිලි යාවත්කාලීන කිරීම් සඳහා සාමාන්‍යයෙන් භාවිතා කරන ලද port අංකයෙන්ම යවා තිබීම බරපතල තත්ත්වයකි.[6] කෙසේ වෙතත්, කුමන දත්ත ප්‍රමාණයක් අනවසරයෙන් ලබාගෙන හෝ කාන්දු වී ඇත්ද යන්න පැහැදිලි නැත.[6] මෙම සිදුවීම, මූලික මහජන උපයෝගිතා සේවාවක සන්නිවේදන පද්ධතිය ඉලක්ක කරගත් ප්‍රහාරයක් වන අතර, එයින් පෙන්නුම් කරන්නේ සුළු යැයි පෙනෙන දත්ත සොරකම් *** පවා මහජන විශ්වාසය බිඳ දමා පුළුල් ව්‍යාකූලත්වයක් ඇති කළ හැකි ආකාරයයි. විශේෂයෙන්ම, බලධාරීන් විසින් ක්ෂණිකව නිල ප්‍රකාශයක් නිකුත් නොකිරීම [6] මෙම ගැටලුව තවදුරටත් උග්‍ර කරයි.

නම සඳහන් නොකරන ** පුද්ගලික බැංකු දත්ත දත්ත සොරකම * (Anonymous ** Bank Data Breach)**

2025 මාර්තු 20 වන දින, Hunters International නම් ransomware කණ්ඩායමක් විසින් Anonymous ** Bank වෙත ප්‍රහාරයක් එල්ල කර ඇති බවට ප්‍රකාශ කරන ලදී.[8] බැංකුව පසුව ප්‍රහාරය තහවුරු කළ නමුත්, විස්තර ලබා දුන්නේ නැත.[8] දින කිහිපයකට පසු, ප්‍රහාරක කණ්ඩායම විසින් 1.9 terabytes (මිලියනයකට අධික ලිපිගොනු) දත්ත ප්‍රමාණයක් ප්‍රසිද්ධියට පත් කරන ලදී.[8] කාන්දු වූ

දත්ත අතර දහස් ගණනක් පාරිභෝගිකයන්ගේ ජාතික හැඳුනුම්පත් ඡායාරූප, දුරකථන අංක, ගිණුම් අංක, බැංකුවේ 500+ සේවක පිරිසගේ දත්ත මෙන්ම අනාගත සහ හිටපු සේවකයන්ගේ විස්තර ද අඩංගු විය.[8] මෙය ශ්‍රී ලංකාවේ මෙතෙක් වාර්තා වූ විශාලතම දත්ත දත්ත සොරකම ලෙස සලකයි *** .[8]

කාන්දු වූ ලේඛනවලට අනුව, බැංකුවට වසරකට පමණ පෙර ආරක්ෂක අඩුපාඩු පිළිබඳව අනතුරු අඟවා තිබී ඇත.[8] මෙම සිදුවීම හුදු තාක්ෂණික දත්ත සොරකමකට *** වඩා ගැඹුරු වන අතර, ආයතනික පාලනයේ බරපතල අඩුපාඩු සහ සැබෑ ආරක්ෂාව සහ අනුකූලතාවය අතර පවතින පරතරය මනාව පෙන්නුම් කරයි. බැංකුවට පෙර අවදානම් පිළිබඳව අනතුරු අඟවා තිබියදීත් ඒවා නොසලකා හැරීම, කළමනාකරණ මට්ටමේ නොසැලකිලිමත්කම සහ වගවීමක් නොමැතිකම පෙන්නුම් කරයි. ජාතික හැඳුනුම්පත් ඡායාරූප සහ අත්සන් වැනි අතිශය සංවේදී දත්ත විශාල වශයෙන් කාන්දු වීම, දහස් ගණනක් පුරවැසියන්ට අනන්‍යතා දත්ත සොරකම් *** සහ වංචා කිරීම් සඳහා දිගුකාලීන අවදානමක් ඇති කරයි.

බැංකුවේ ප්‍රතිචාරය මූලිකවම සේවා අඛණ්ඩතාවය පිළිබඳව අවධාරණය කළ අතර, බලපෑමට ලක් වූ පුද්ගලයන්ට ඇති අවදානම් පිළිබඳව පැහැදිලි සන්නිවේදනයක් නොතිබුණි.[8] මෙම සිදුවීම, පුද්ගලික දත්ත ආරක්ෂණ පනත (PDPA) සංශෝධන පිළිබඳව රජය අවධානය යොමු කරමින් සිටි අවස්ථාවක සිදුවීම, නීතිමය රාමුවල ක්‍රියාත්මක කිරීමේ සූදානම පිළිබඳව ප්‍රශ්න මතු කරයි.[8]

ලංකා රජයේ ජාලයට එල්ල වූ ransomware ප්‍රහාරය

2023 අගෝස්තු 26 වන දින, ශ්‍රී ලංකා රජයේ වලාකුළු යටිතල පහසුකම් (Lanka Government Network - LGN) වෙත ප්‍රධාන ransomware ප්‍රහාරයක් එල්ල විය.[15] මෙම ප්‍රහාරය රජයේ ර්මේල් ගිණුම් 5,000 ක් පමණ (ජනාධිපති කාර්යාලය, කැබිනට් කාර්යාලය, අධ්‍යාපන අමාත්‍යාංශය, සෞඛ්‍ය අමාත්‍යාංශය ඇතුළුව) අඩපණ කළ අතර, නොබැඳි උපස්ථ (offline backups) නොතිබූ බොහෝ ර්මේල් මැකී ගියේය.[15] සමහර සේවකයින්ට මාස තුනක ර්මේල් පණිවිඩ අහිමි විය.[15]

මෙම ප්‍රහාරයට ප්‍රධාන හේතුව වූයේ යම් මෘදුකාංගයක යල් පැන ගිය සංස්කරණයක් භාවිතා කිරීමයි. මෙම සංස්කරණය 2023 අප්‍රේල් මාසයේදී එහි සේවා කාලය අවසන් වී තිබුණි.[15] රජය 2021 සිට නවතම සංස්කරණයට යාවත්කාලීන කිරීමට උත්සාහ කළද, අරමුදල් සීමාවන් සහ පෙර පාලක මණ්ඩල තීරණ හේතුවෙන් එය සිදු කිරීමට නොහැකි විය.[15] ඔන්ලයින් උපස්ථ ද සංකේතනය වී තිබූ අතර, නොබැඳි උපස්ථ නිරන්තරයෙන් පවත්වාගෙන

ගොස් නොතිබීම, ආපසු හැරවිය නොහැකි දත්ත අහිමි වීමට හේතු විය.[15] ප්‍රහාරයෙන් පසු පැය 12ක් ඇතුළත LGN ප්‍රතිසාධනය කරන ලද අතර, දෛනික නොබැඳි උපස්ථ ක්‍රියාවලියක් ආරම්භ කරන ලදී.[15]

මෙම සිදුවීමෙන් පැහැදිලි වන්නේ, රජයේ ඩිජිටල් පද්ධති නඩත්තු කිරීමේදී ප්‍රමාණවත් ආයෝජනයක් නොමැති වීම සහ නිලධාරීවාදී මන්දගාමිත්වය කෙතරම් භයානක ප්‍රතිවිපාක ගෙන එන්නේද යන්නයි. යල් පැන ගිය පද්ධති මත යැපීම සහ මූලික උපස්ථ ක්‍රමවේදයන් (විශේෂයෙන් නොබැඳි උපස්ථ) ක්‍රියාත්මක කිරීමට අපොහොසත් වීම හේතුවෙන් රජයේ සන්නිවේදන දත්ත ස්ථිරවම අහිමි වීම, රජයේ කාර්යක්ෂමතාවයට, ඓතිහාසික වාර්තාකරණයට සහ ජාතික ආරක්ෂාවට සෘජුවම බලපාන ගැඹුරු ක්‍රමානුකූල අවදානමක් පෙන්නුම් කරයි. මෙය රාජ්‍ය අංශය තුළ සම්පත් වෙන් කිරීමේ සහ උපායමාර්ගික දැක්මේ පවතින ගැටලුකාරී තත්ත්වයක් මනාව කියාපායි.

විශ්‍රාම වැටුප් දෙපාර්තමේන්තුවේ සිදුවීම

2025 මැයි මාසයේදී විශ්‍රාම වැටුප් දෙපාර්තමේන්තුවට Cloak Ransomware ප්‍රහාරයක් එල්ල වූ බවට වාර්තා විය.[10] මෙම සිදුවීමෙන් 617 GB ක දත්ත ප්‍රමාණයක් සම්මුතිගත වූ බවට චෝදනා එල්ල වූ අතර, එය ශ්‍රී ලංකාවේ රාජ්‍ය අංශයේ මෙතෙක් සිදු වූ විශාලතම දත්ත දත්ත සොරකම *** විය හැකිය.[10] මෙම දත්ත අතර රටේ වඩාත්ම අවදානමට ලක්විය හැකි ජනගහනයෙන් කොටසක් වන විශ්‍රාමිකයන්ගේ පුද්ගලිකව හඳුනාගත හැකි තොරතුරු (PII) අඳුරු වෙබ් අඩවිවලට (dark web) කාන්දු වීමේ අධික අවදානමක් ඇත.[10] මෙම දත්ත මූල්‍ය වංචා, ඉලක්කගත තතුබෑම් ප්‍රහාර (phishing attacks) සහ වෙනත් අනිෂ්ට ක්‍රියාකාරකම් සඳහා සදාකාලිකවම භාවිතා විය හැකිය.[10]

විශ්‍රාම වැටුප් දෙපාර්තමේන්තුව ප්‍රකාශ කළේ සේවා කටයුතුවලට බාධාවක් නොවන බවයි.[10] කෙසේ වෙතත්, Anonymous ** Bank සිදුවීමට සමානව, බලපෑමට ලක් වූ පුද්ගලයන්ට ඔවුන්ගේ දත්තවලට ඇති අවදානම් පිළිබඳව පැහැදිලි, කාලෝචිත සහ සෘජු අනතුරු ඇඟවීමක් ලබා දීමට අපොහොසත් වීම විවේචනයට ලක් විය.[10] මෙම සිදුවීම විශේෂයෙන්ම භයානක වන්නේ එය ඉතා අවදානමට ලක්විය හැකි ජනගහනයක් ඉලක්ක කර ගැනීම හේතුවෙනි. රජයේ ආයතන, පුරවැසියන්ගේ සංවේදී දත්ත විශාල ප්‍රමාණයක් දරන බැවින්, ආදර්ශවත් සයිබර් ආරක්ෂාවක් සහ, තීරණාත්මක ලෙස, දත්ත දත්ත සොරකම් *** වලදී විනිවිදභාවයෙන් යුත් සහ සංවේදී සන්නිවේදන උපාය මාර්ග තිබිය යුතුය. සේවා අඛණ්ඩතාවය පිළිබඳව පමණක් අවධානය යොමු කරමින්, පුද්ගලික අවදානම් පිළිබඳව දැනුම් දීමට අපොහොසත් වීම, දත්ත සොරකම්වල *** මානව බලපෑම අවබෝධ කර

ගැනීමේ ක්‍රමානුකූල අඩුපාඩුවක් සහ සිදුවීම් සන්නිවේදනයේ හොඳම භාවිතයන්ට අනුකූල නොවීම පෙන්නුම් කරයි.

ඩිජිටල් ඔරොත්තු දීමේ හැකියාව: ඩිජිටල් පාලනය සහ පූර්ව ආරක්ෂාව (Pillars of Digital Resilience)

ඩිජිටල් පාලනයේ වැදගත්කම

- **පුද්ගලික දත්ත ආරක්ෂණ පනත (PDPA) සහ එහි භූමිකාව (Personal Data Protection Act (PDPA) and its Role)**
  ශ්‍රී ලංකාවේ පුද්ගලික දත්ත ආරක්ෂණ පනත (PDPA) අංක 9, 2022, ඩිජිටල් යුගයේ දත්ත ආරක්ෂණ අවශ්‍යතාවය සපුරාලීම සඳහා පනවන ලදී.[18] එය පුද්ගලික දත්ත ආරක්ෂා කිරීම සහ නීත්‍යානුකූල දත්ත සැකසීමට ඉඩ සැලසීම අරමුණු කරයි.[18] මෙම පනත ජාත්‍යන්තර ප්‍රමිතීන්ට අනුකූල වන අතර, දේශසීමා හරහා දත්ත ගලා ඒම සහ ඩිජිටල් වෙළඳාමට පහසුකම් සපයයි.[18] PDPA හි සම්පූර්ණ ක්‍රියාත්මක කිරීම අදියර කිහිපයකින් සිදු වන අතර, 2025 මාර්තු 18 දින සිට ක්‍රියාත්මක වීමට නියමිතව තිබූ ඇතැම් කොටස් (දත්ත විෂයයන්ගේ අයිතිවාසිකම්, පාලකයන් සහ සැකසුම්කරුවන්, දඬුවම්) අනුකූලතා සූදානම පිළිබඳ ගැටලු හේතුවෙන් ප්‍රමාදකර ඇත.[18] මෙම ප්‍රමාදය, රාජ්‍ය සහ පෞද්ගලික අංශවලට අනුකූලතාවය සඳහා වැඩි කාලයක් ලබා දීම, ධාරිතා වර්ධනය සහ යටිතල පහසුකම් වැඩිදියුණු කිරීම සඳහා වේ.[20]

  PDPA හි සම්පූර්ණ ක්‍රියාත්මක කිරීමේ ප්‍රමාදය, විශේෂයෙන්ම දත්ත විෂයයන්ගේ අයිතිවාසිකම් සහ දඬුවම් සම්බන්ධ කොටස්, නියාමන හිඩැසක් නිර්මාණය කරන අතර, එය අනිෂ්ට ක්‍රියාකරුවන්ට වාසිදායක විය හැකි අතර පුරවැසියන් අවදානමට ලක් කරයි. මෙම නීතිමය "අවිනිශ්චිතතාවය" මගින් ආයතන (රාජ්‍ය සහ පෞද්ගලික යන දෙඅංශයේම) දත්ත ආරක්ෂාව සඳහා ප්‍රමාණවත් ලෙස ආයෝජනය කිරීමේ ක්ෂණික අවශ්‍යතාවය අඩු කරයි. Anonymous ** Bank සහ විශ්‍රාම වැටුප් දෙපාර්තමේන්තුවේ සිදුවීම් මෙම ප්‍රමාදයන් අතරතුර සිදුවීම, මෙම ආරක්ෂාවන්හි හදිසි අවශ්‍යතාවය අවධාරණය කරයි. පනතට අනුකූල නොවීම සඳහා රුපියල් මිලියන 10 ක් දක්වා දඩ මුදල් පැනවීමට දත්ත ආරක්ෂණ අධිකාරියට (DPA) බලය ඇත.[18] කෙසේ වෙතත්, සම්පූර්ණ ක්‍රියාත්මක කිරීමේ ප්‍රමාදය හේතුවෙන් මෙම දඩ මුදල්වල සඵලතාවය අඩාල වී ඇත. මෙය පෙන්නුම් කරන්නේ ශක්තිමත් පාලනයක අවශ්‍යතාවය හඳුනාගෙන තිබුණද, එහි ප්‍රායෝගික ක්‍රියාත්මක කිරීම සැලකිය යුතු බාධාවන්ට මුහුණ දෙන බවයි.

- **දත්ත ආරක්ෂණ අධිකාරිය (DPA), SLCERT සහ ICTA හි කාර්යභාරය**

ශ්‍රී ලංකාවේ ඩිජිටල් පාලන රාමුව ශක්තිමත් කිරීම සඳහා ප්‍රධාන ආයතන කිහිපයක් ක්‍රියාත්මක වේ. **දත්ත ආරක්ෂණ අධිකාරිය (DPA)** PDPA යටතේ පිහිටුවා ඇති අතර, දත්ත ආරක්ෂණයේ වැදගත්කම අවධාරණය කරයි.[18] එය පෞද්ගලිකත්වය ආරක්ෂා කිරීම, අපරාධ වැළැක්වීම, නවෝත්පාදනයන් සක්‍රීය කිරීම, ඩිජිටල් සේවා කෙරෙහි විශ්වාසය ගොඩනැගීම සහ සාධාරණත්වය සහ විනිවිදභාවය සහතික කිරීම අරමුණු කරයි.[19] DPA හට විගණන සිදු කිරීමට, දත්ත දත්ත සොරකම්*** පැමිණිලිවලට ප්‍රතිචාර දැක්වීමට සහ බැඳීම් සහිත නියෝග නිකුත් කිරීමට බලය ඇත.[21]

ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර කණ්ඩායම (SLCERT) ශ්‍රී ලංකාවේ තොරතුරු ආරක්ෂාව සඳහා විශ්වාසනීය තනි සම්බන්ධතා ස්ථානය ලෙස ක්‍රියා කරයි.[22] එය මහජන සහ පෞද්ගලික අංශයේ සංවිධාන සහ සාමාන්‍ය මහජනතාව ආරක්ෂා කිරීම සඳහා තර්ජන සහ අවදානම් පිළිබඳ යාවත්කාලීන තොරතුරු සපයන අතර, පරිගණක හදිසි ප්‍රතිචාර හැසිරවීමේ සේවා සපයයි.[22] SLCERT, ICTA විසින් 2006 දී පිහිටුවන ලද අතර, දැන් තාක්ෂණ අමාත්‍යාංශය යටතේ ක්‍රියාත්මක වේ.[23] රාජ්‍ය ආයතන සඳහා වෙබ් අඩවි ආරක්ෂක මාර්ගෝපදේශ සහ අවම තොරතුරු ආරක්ෂක ප්‍රමිතීන් නිකුත් කර ඇත.[24] මෑතකාලීනව, රාජ්‍ය ආයතන ඔවුන්ගේ වෙබ් අඩවි සජීවී කිරීමට පෙර SLCERT හි ආරක්ෂක පරීක්ෂාවන් සහ නිර්දේශ දැඩි ලෙස ක්‍රියාත්මක කිරීම අනිවාර්ය කිරීමට රජය කටයුතු කරමින් සිටී.[24]

තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය (ICTA) ශ්‍රී ලංකාවේ ඩිජිටල් පරිවර්තනය මෙහෙයවන ප්‍රධාන ආයතනයයි.[26] එය ඩිජිටල් පාලනය වැඩි දියුණු කිරීම, ආරම්භක පරිසර පද්ධති පෝෂණය කිරීම සහ රටේ ඩිජිටල් හිඩැස් පිරවීම සඳහා කටයුතු කරයි.[26] ICTA, SLCERT සමඟ එක්ව රජයේ ර්මේල් ප්‍රහාරය විමර්ශනය කළේය.[15]

මෙම ආයතන (DPA, SLCERT, ICTA) සහ නීතිමය රාමු (PDPA, සයිබර් ආරක්ෂණ පනත) තිබියදීත්, මෑතකාලීන දත්ත දත්ත සොරකම් *** (LGN, Anonymous ** , විශ්‍රාම වැටුප් දෙපාර්තමේන්තුව) පෙන්නුම් කරන්නේ පවතින මාර්ගෝපදේශ ඵලදායී ලෙස සම්බන්ධීකරණය කිරීමේ සහ ක්‍රියාත්මක කිරීමේ සැලකිය යුතු පරතරයක් පවතින බවයි. SLCERT හි නිර්දේශ මෑතක් වන තුරුම අනිවාර්ය නොවීම [24] සහ යල් පැන ගිය පද්ධති පැවතීම [15] පෙන්නුම් කරන්නේ ප්‍රතිපත්ති සහ මාර්ගෝපදේශ

තිබුණද, ප්‍රායෝගික ක්‍රියාත්මක කිරීම සහ වගවීම ප්‍රමාණවත් නොවන බවයි. නව සයිබර් ආරක්ෂණ පනතක් සහ අධිකාරියක් ස්ථාපිත කිරීම [21] පාලනය කේන්ද්‍රගත කිරීමට සහ ශක්තිමත් කිරීමට කෙරෙන අඛණ්ඩ උත්සාහයක් වන අතර, පවතින ඛණ්ඩනය හඳුනා ගනී.

සූර්ව සයිබර් ආරක්ෂණ ක්‍රමවේද

- **අවදානම් තක්සේරු කිරීම සහ ආරක්ෂක ස්ථර**

  සංවේදී යටිතල පහසුකම් ආරක්ෂා කිරීම සඳහා නිතිපතා අවදානම් තක්සේරු කිරීම් සහ විශ්ලේෂණ අත්‍යවශ්‍ය වේ. මෙම ක්‍රියාවලිය මගින් ආරක්ෂක ක්‍රමවේදවල ඇති දුර්වලතා හඳුනා ගැනීමට සහ විවිධ තර්ජන මගින් ඇතිවන අවදානම් මට්ටම තීරණය කිරීමට උපකාරී වේ.[2] ශක්තිමත් "defense-in-depth" (ගැඹුරු ආරක්ෂක) උපාය මාර්ගයක් මගින් භෞතික බාධකවල සිට ඩිජිටල් ආරක්ෂාව දක්වා බහු ආරක්ෂක ස්ථර ඇතුළත් වේ. මෙයට ජාල කොටස්කරණය (network segmentation) මගින් ප්‍රහාරවල බලපෑම සීමා කිරීම, පුළුල් ප්‍රවේශ පාලන පද්ධති සහ සියලුම සම්බන්ධිත උපාංග සඳහා ශක්තිමත් endpoint ආරක්ෂාව ඇතුළත් වේ.[2] සංවේදී තොරතුරු සඳහා සංකේතන ප්‍රොටෝකෝල (encryption protocols) ක්‍රියාත්මක කිරීම අත්‍යවශ්‍ය වේ.[2]

  මෙම හොඳම භාවිතයන් පැහැදිලිව ලේඛනගත කර හඳුනාගෙන තිබුණද [2], Anonymous ** Bank සිදුවීම [8] මගින් පෙන්නුම් කරන්නේ ඒවා ප්‍රායෝගිකව ක්‍රියාත්මක කිරීමේ සැලකිය යුතු පරතරයක් පවතින බවයි. "සංවේදී පුද්ගලික දත්ත නිසි ලෙස සංකේතනය කර නොතිබීම" [8], "නිසි දත්ත රඳවා ගැනීමේ සහ මකාදැමීමේ ප්‍රතිපත්ති නොමැති වීම" [8], සහ "විගණන වාර්තා නොමැතිකම" [8] වැනි ගැටලු මගින් ආයතන මෙම මූලික ක්‍රියාමාර්ග ක්‍රියාත්මක කිරීමට අපොහොසත් වී ඇති බව පෙන්වයි. මෙය පෙන්නුම් කරන්නේ න්‍යායාත්මක හොඳම භාවිතයන් ප්‍රායෝගික, ශක්තිමත් ආරක්ෂක තත්ත්වයක් බවට පරිවර්තනය නොවන සැලකිය යුතු ක්‍රියාත්මක කිරීමේ පරතරයක් පවතින බවයි.

- **පද්ධති යාවත්කාලීන කිරීම් සහ ප්‍රවේශ පාලනය**

  නිරන්තර මෘදුකාංග යාවත්කාලීන කිරීම් සහ patch management (පද්ධතිවල ඇති ආරක්ෂක දුර්වලතා නිවැරදි කිරීම) අත්‍යවශ්‍ය සයිබර් සනීපාරක්ෂක පිළිවෙත් වේ.[2] යල් පැන ගිය පද්ධති (legacy systems) සයිබර් ආරක්ෂාවට සැලකිය යුතු අවදානමක් ඇති කරයි.[1] LGN ප්‍රහාරය [15] පැහැදිලිවම පෙන්නුම් කළේ යල් පැන ගිය මෘදුකාංගයක භාවිතය සහ අරමුදල් සීමාවන් හේතුවෙන් යාවත්කාලීන කිරීම් ප්‍රමාද වීම ප්‍රධාන

අවදානමක් වූ බවයි. රජයේ ආයතනවලට එල්ල වන සයිබර් ප්‍රහාරවලට ප්‍රධාන හේතු අතරට "යල් පැන ගිය යටිතල පහසුකම්" ද ඇතුළත් වේ.[1]

බහු සාධක සත්‍යාපනය (Multi-Factor Authentication - MFA) සහ ශක්තිමත් මුරපද ප්‍රතිපත්ති ක්‍රියාත්මක කිරීම මගින් අනවසර ප්‍රවේශය වළක්වා ගත හැක.[2] මෙය මුරපදයක් සම්මුතිගත වුවද ආරක්ෂාව තහවුරු කරයි. ආරක්ෂිත දුරස්ථ ප්‍රවේශය (Secure Remote Access) සඳහා Virtual Private Networks (VPNs) භාවිතය නිර්දේශ කෙරේ.[2] යල් පැන ගිය පද්ධති සහ මූලික සයිබර් සනීපාරක්ෂක පිළිවෙත්වල අඛණ්ඩ අභියෝගය ශ්‍රී ලංකාවේ රාජ්‍ය අංශය පුරා පවතින තීරණාත්මක සහ පුනරාවර්තන අවදානමකි. මෙය හුදු තාක්ෂණික අඩුපාඩුවක් නොව, උපායමාර්ගික සහ අයවැයකරණයේ අඩුපාඩුවකි. SLCERT හි පැහැදිලි මාර්ගෝපදේශ තිබියදීත් [25], මෙම මූලික අවදානම් අඛණ්ඩව පැවතීම, රජයේ ආයතන තුළ සම්පත් වෙන් කිරීම, තාක්ෂණික ධාරිතාව සහ සංවිධානාත්මක විනය පිළිබඳ ගැඹුරු අභියෝගයක් පෙන්නුම් කරයි.

- **සිදුවීම් ප්‍රතිචාර සැලසුම් (Incident Response Plans)**

ආරක්ෂක සිදුවීම් වලදී මෙහෙයුම් අඛණ්ඩතාව පවත්වා ගැනීම සඳහා හොඳින් ව්‍යුහගත සිදුවීම් ප්‍රතිචාර සැලැස්මක් අත්‍යවශ්‍ය වේ.[2] මෙම සැලසුම් මගින් සිදුවීම් හඳුනාගැනීම, ඒවා පාලනය කිරීමේ උපාය මාර්ග සහ ප්‍රතිසාධන ප්‍රොටෝකෝල විස්තර කළ යුතුය.[2] SLCERT ඩිජිටල් අධිකරණ වෛද්‍ය සේවා (digital forensics) සහ ප්‍රතිසාධන ක්‍රියාවලිය සඳහා සහාය සපයයි.[29]

LGN ප්‍රහාරය [15] මගින් මාස 3ක ර්මේල් දත්ත ස්ථිරවම නැතිවීම සහ Anonymous ** Bank හි "අකාර්යක්ෂම උපස්ථ ප්‍රතිසාධන ක්‍රියාවලිය" [8] පෙන්නුම් කරන්නේ, සිදුවීම් ප්‍රතිචාර සැලසුම් කඩදාසි මත තිබුණද, ඒවායේ සඵලතාවය සහ ක්‍රියාත්මක කිරීම බරපතල ලෙස අඩු බවයි. නිසි උපස්ථ උපාය මාර්ග (විශේෂයෙන් නොබැඳි, වෙනස් කළ නොහැකි උපස්ථ) නොමැතිකම, දත්ත සොරකමක් *** දත්ත නැතිවීමක් බවට පත් කරන අතර, එය වඩාත් බරපතල ප්‍රතිවිපාක ගෙන එයි. මෙය වත්මන් සිදුවීම් ප්‍රතිචාර සැලසුම් අසම්පූර්ණ, පරීක්ෂා නොකළ හෝ ප්‍රමාණවත් ලෙස සම්පත් නොමැති බවට ඇඟවුම් කරයි.

විනිවිදභාවය සහ මහජන විශ්වාසය: හවුල් වගකීමක්

- **දත්ත සොරකම් *** ප්‍රසිද්ධියේ පිළිගැනීමේ වැදගත්කම**

දත්ත දත්ත සොරකම්*** ප්‍රසිද්ධියේ පිළිගැනීම සහ විනිවිදභාවය, මහජන විශ්වාසය ගොඩනැගීමට සහ පවත්වා ගැනීමට අත්‍යවශ්‍ය වේ.[10] Anonymous ** Bank සහ විශ්‍රාම වැටුප් දෙපාර්තමේන්තුවේ සිදුවීම් වලදී, බලපෑමට ලක් වූ පුද්ගලයන්ට ඇති අවදානම් පිළිබඳව පැහැදිලි, ක්ෂණික සහ සෘජු අනතුරු ඇඟවීමක් ලබා නොදීම විවේචනයට ලක් විය.[8] ඒ වෙනුවට, සේවා අඛණ්ඩතාවය පිළිබඳව අවධාරණය කිරීමක් සිදු විය.[8] මෙමගින් පුද්ගලයන්ට වංචා සහ අනන්‍යතා දත්ත සොරකම් *** වලින් ආරක්ෂා වීමට අවශ්‍ය පූර්ව ආරක්ෂක ක්‍රියාමාර්ග ගැනීමට ඇති අවස්ථාව අහිමි වේ.[10]

ප්‍රධාන දත්ත දත්ත සොරකම් වලින් *** පසුව (Anonymous ** , විශ්‍රාම වැටුප් දෙපාර්තමේන්තුව, ජල මණ්ඩලය) ප්‍රමාද වූ, අපැහැදිලි හෝ සේවා-නැඹුරු මහජන දැනුම්දීම් පුනරාවර්තන රටාවක් දක්නට ලැබේ. මෙය සංවිධාන තුළ දත්ත අහිමි වීමේ ප්‍රමාණය සහ පුද්ගලික බලපෑම් සම්පූර්ණයෙන් හෙළිදරව් කිරීමට ඇති අකමැත්තක් හෝ සූදානම් නොවීමක් පෙන්නුම් කරයි. මෙම විනිවිදභාවය නොමැතිකම, භීතිය අවම කිරීමට අදහස් කළද, අවසානයේදී දිගුකාලීන මහජන විශ්වාසය සහ වගවීම බිඳ දමයි. එමගින් වගකිවයුතු සිදුවීම් කළමනාකරණයකට වඩා නොසැලකිලිමත්කම හෝ වසන් කිරීම පිළිබඳ හැඟීමක් ඇති කරයි. මෙයින් කෙනෙකුගේ පුද්ගලිකත්වය , ආරක්ෂාව යන කරුණු සඳහා කෙරෙන බලපෑම ඉතා ඉහල බැවින් පුද්ගලිකත්වය අයිතියක් ලෙස පිළි ගන්නා සමාජයක තොරතුරු අනවශ්‍ය පාර්ශවයක් අතට පත් වීම නීතිමය හා මානව අයිතිය වශයෙන් අභියෝගයට ලක් කල හැකිය.

- **විශ්වාසය ගොඩනැගීම සඳහා සන්නිවේදනය**

දත්ත ආරක්ෂණය මගින් ඩිජිටල් වේදිකා සහ ව්‍යාපාර කෙරෙහි මහජන විශ්වාසය වැඩි දියුණු කරයි. මෙය ඩිජිටල් සේවා සමඟ සම්බන්ධ වීමට මහජනතාව දිරිමත් කරන අතර ආර්ථික වර්ධනයට දායක වේ.[19] ආරක්ෂක සිදුවීම් පිළිබඳව මහජනතාවට නිවැරදි සහ කාලෝචිත තොරතුරු ලබා දීම අත්‍යවශ්‍ය වේ.[10] මෙය ව්‍යාජ තොරතුරු සහ වැරදි තොරතුරු පැතිරීම වළක්වා ගැනීමට උපකාරී වේ.[11]
මහජන විශ්වාසය යනු සමාජ යහපතක් පමණක් නොව, ශ්‍රී ලංකාවේ ඩිජිටල් ආර්ථික අභිලාෂයන් සඳහා තීරණාත්මක සාධකයකි. විශ්වාසය නොමැතිව, පුරවැසියන් ඩිජිටල් සේවා (උදා: ඩිජිටල්

හැඳුනුම්පත්, ඊ-ගෙවීම්) භාවිතා කිරීමට පසුබට වනු ඇත.[1] එමගින් රජය අත්කර ගැනීමට අපේක්ෂා කරන ප්‍රගතියට බාධා ඇති වේ. එබැවින්, අර්බුදකාරී අවස්ථාවන්හිදී ඵලදායී සන්නිවේදනයක් යනු හුදු මහජන සම්බන්ධතා අභ්‍යාසයක් නොව, ආර්ථික අවශ්‍යතාවයකි.

මහජනතාව සවිබල ගැන්වීම: ඩිජිටල් සාක්ෂරතාවය සහ මූලික ආරක්ෂාව

- **ඩිජිටල් සාක්ෂරතා වැඩසටහන්වල අවශ්‍යතාවය (Need for Digital Literacy Programs)**

  ශ්‍රී ලංකාවේ ඩිජිටල් පරිවර්තනයත් සමඟ, ඩිජිටල් සාක්ෂරතා වැඩසටහන් අත්‍යවශ්‍ය වේ.[1] බොහෝ ශ්‍රී ලාංකිකයන්ට තම තොරතුරු ලබා ගන්නා ආකාරය, ගබඩා කරන ආකාරය සහ භාවිතා කරන ආකාරය පිළිබඳව අවබෝධයක් නොමැත.[31] මෙම දැනුමේ පරතරය, රහස්‍ය තොරතුරු කාන්දු වීම, වංචනික ක්‍රියාකාරකම් සහ ව්‍යාජ ලෙස පෙනී සිටීම හරහා ප්‍රහාරවලට ගොදුරු වීමේ අවදානම වැඩි කරයි.[31] ඩිජිටල් සාක්ෂරතාවය සහ ධාරිතා වර්ධන මුලපිරීම් මගින් පුරවැසියන්ට ඩිජිටල් පද්ධති භාවිත කිරීමට සහ ඒවායින් ප්‍රයෝජන ගැනීමට හැකි වේ.[30] පාසල් සහ විශ්වවිද්‍යාල විෂය මාලාවන්ට දත්ත ආරක්ෂණ මොඩියුල ඇතුළත් කිරීම නිර්දේශ කෙරේ.[1]

  ශ්‍රී ලංකාවේ සයිබර් ආරක්ෂක අවදානමෙන් සැලකිය යුතු කොටසක් පවතින්නේ තාක්ෂණික යටිතල පහසුකම්වල පමණක් නොව, මානව සාධකවල, විශේෂයෙන්ම අඩු ඩිජිටල් සාක්ෂරතාවය තුළය. මෙය සමාජ ඉංජිනේරු ප්‍රහාර (ෆිෂින් වැනි) සහ අනන්‍යතා දත්ත සොරකම්*** සඳහා පහසු බිමක් නිර්මාණය කරන අතර, පුද්ගලයන් දුර්වලම සම්බන්ධකය බවට පත් කරයි. පුළුල් ඩිජිටල් සාක්ෂරතාවය සඳහා ආයෝජනය කිරීම මූලික සයිබර් ආරක්ෂක ආරක්ෂාවක් වන අතර, පුරවැසියන් නොදැනුවත්ව ගොදුරු බවට පත්වීම වෙනුවට පළමු ආරක්ෂක වළල්ල බවට පත් කිරීමට එය උපකාරී වේ.

- **මහජනතාව සඳහා මූලික ඩිජිටල් ආරක්ෂක උපදෙස්**

  මහජනතාවට තම දත්ත ආරක්ෂා කර ගැනීමට සහ සයිබර් තර්ජනවලින් වැළකී සිටීමට උපකාර වන මූලික ඩිජිටල් ආරක්ෂක උපදෙස් පහත වගුවේ දැක්වේ.

Table 2: මහජනතාව සඳහා මූලික ඩිජිටල් ආරක්ෂක උපදෙස් (Basic Digital Safety Tips for the Public)

උපදෙස් (Tip)	විස්තරය (Description)	වැදගත්කම (Importance)
ශක්තිමත්, අද්විතීය මුරපද භාවිතා කරන්න	විවිධ ගිණුම් සඳහා සංකීර්ණ සහ වෙනස් මුරපද භාවිතා කරන්න. මුරපද කළමනාකරණ මෘදුකාංග භාවිතය සලකා බලන්න. [28]	දුර්වල හෝ නැවත භාවිතා කරන මුරපද සයිබර් ප්‍රහාරකයන්ට පහසු ඉලක්කයක් වේ. [14]
බහු සාධක සත්‍යාපනය (MFA) සක්‍රීය කරන්න	මුරපදයට අමතරව අමතර සත්‍යාපන ක්‍රමයක් (උදා: දුරකථනයට ලැබෙන කේතයක්) භාවිතා කරන්න. [28]	මුරපදයක් සම්මුතිගත වුවද අනවසර ප්‍රවේශය වළක්වයි. [28]
ෆිෂින් ප්‍රහාර හඳුනා ගන්න	සැක සහිත ඊමේල්, කෙටි පණිවිඩ හෝ වෙබ් අඩවි ගැන විමසිලිමත් වන්න. නොදන්නා සබැඳි (links) ක්ලික් කිරීමෙන් හෝ ඇමුණුම් විවෘත කිරීමෙන් වළකින්න. [28]	ෆිෂින් යනු දත්ත දත්ත සොරකම *** කිරීමේ ප්‍රධාන ක්‍රමවේදයකි. [15]
මෘදුකාංග යාවත්කාලීනව තබා ගන්න	ඔබගේ මෙහෙයුම් පද්ධතිය, යෙදුම් සහ ප්‍රති-වයිරස මෘදුකාංග නිරන්තරයෙන් යාවත්කාලීන කරන්න. [28]	යල් පැන ගිය මෘදුකාංගවල ආරක්ෂක දුර්වලතා පහසුවෙන් ප්‍රයෝජනයට ගත හැක. [1]
ආරක්ෂිත ජාල භාවිතා කරන්න	පොදු Wi-Fi ජාල භාවිත කරන විට ප්‍රවේශම් වන්න. සංවේදී තොරතුරු හුවමාරු කිරීමේදී VPN (Virtual Private Network) භාවිතය සලකා බලන්න. [28]	පොදු ජාල අනාරක්ෂිත විය හැකි අතර, දත්ත දත්ත සොරකම *** කිරීමට ඉඩ ඇත. [34]
ඔබගේ දත්තවලට	සමාජ මාධ්‍යවල පුද්ගලික තොරතුරු බෙදාගැනීමේදී	අධික ලෙස පුද්ගලික තොරතුරු බෙදාගැනීම

ප්‍රවේශය පාලනය කරන්න	ප්‍රවේශම් වන්න. ඔබගේ පෞද්ගලිකත්ව සැකසුම් (privacy settings) නිසි ලෙස සකසන්න. [31]	අනන්‍යතා දත්ත සොරකම ***ෙ අවදානම වැඩි කරයි. [31]
සැක සහිත ක්‍රියාකාරකම් වාර්තා කරන්න	යම් සයිබර් සිදුවීමක් හෝ සැක සහිත ක්‍රියාකාරකමක් දුටුවහොත් SLCERT වැනි අදාළ බලධාරීන්ට වාර්තා කරන්න. [32]	ක්ෂණික වාර්තා කිරීම මගින් සිදුවීම්වල බලපෑම අවම කර ගැනීමට සහ වැඩිදුර ප්‍රහාර වළක්වා ගැනීමට උපකාරී වේ. [29]
ළමුන්ගේ අන්තර්ජාල භාවිතය අධීක්ෂණය කරන්න	දෙමාපියන් ලෙස දරුවන්ගේ අන්තර්ජාල භාවිතය අධීක්ෂණය කර, ඔවුන්ට අන්තර්ජාල ආරක්ෂාව පිළිබඳව උගන්වන්න. [31]	ළමුන් අන්තර්ජාලයේ අවදානම්වලට පහසුවෙන් ගොදුරු විය හැක. [31]
දේශීය හෝ දේශපාලන සිදුවීම් පිළිබඳව සමාජ මාධ්‍යවල අදහස් දැක්වීමෙන් වළකින්න	ඇතැම් රටවල සමාජ මාධ්‍යවල අදහස් දැක්වීම් සම්බන්ධයෙන් නීතිමය ගැටලු ඇතිවිය හැක. [34]	සමාජ මාධ්‍ය භාවිතය අදාළ රටවල නීති හා රෙගුලාසිවලට යටත් වේ. [34]

දත්ත සොරකම්වල* බලපෑම:**

රටට, ආර්ථිකයට සහ පුරවැසියන්ට සංවේදී යටිතල පහසුකම් සහ රජයට බලපෑම (Impact on Critical Infrastructure and Government)

සංවේදී යටිතල පහසුකම්වලට එල්ල වන ප්‍රහාර, ජාතික ආරක්ෂාවට, මහජන සෞඛ්‍යයට සහ ආර්ථික ස්ථාවරත්වයට සෘජු බලපෑමක් ඇති කරයි.[2] රජයේ පද්ධතිවල දත්ත සොරකම්*** (උදා: LGN ප්‍රහාරය [15], විශ්‍රාම වැටුප් දෙපාර්තමේන්තුවේ සිදුවීම [10]), රජයේ සේවාවන් අඩාල කිරීමට, රහස්‍ය තොරතුරු නැතිවීමට සහ අභ්‍යන්තර සන්නිවේදනයට බාධා කිරීමට හේතු වේ.[1] මෙමගින් රජයේ කාර්යක්ෂමතාවය සහ විශ්වසනීයත්වය පිළිබඳව මහජනතාව තුළ සැකයක් ඇති වේ.[5]

සයිබර් ප්‍රහාර ජාතික ආරක්ෂාවට තර්ජනයක් වන අතර, අසත්‍ය ප්‍රවෘත්ති සහ වෛරී ප්‍රකාශ පැතිරවීමෙන් සමාජ නොසන්සුන්තාවයන් ඇති කළ හැක.[4] LGN සහ විශ්‍රාම වැටුප් දෙපාර්තමේන්තුවේ සිදුවීම් වැනි සංවේදී

යටිතල පහසුකම් සහ රජයේ පද්ධතිවල දත්ත සොරකම් ***, ක්ෂණික දත්ත අහිමි වීමෙන් ඔබ්බට ගොස් දෝලනය වන බලපෑමක් ඇති කරයි. ඒවා සංවේදී තොරතුරු නිරාවරණය කිරීමෙන් ජාතික ආරක්ෂාවට හානි කරයි, අත්‍යවශ්‍ය මෙහෙයුම් කඩාකප්පල් කිරීමෙන් මහජන සේවා සැපයීම අඩාල කරයි, සහ පාලනය කෙරෙහි පුරවැසියන්ගේ විශ්වාසය බිඳ දමයි. මෙම සමුච්චිත බලපෑම සමාජ සාමය අස්ථාවර කිරීමට සහ වෙනත් අර්බුදවලට ප්‍රතිචාර දැක්වීමට ජාතියක හැකියාවට බාධා කළ හැකි අතර, එය ගැඹුරු උපායමාර්ගික අවදානමක් පෙන්නුම් කරයි.

සාමාන්‍ය මහජනතාවට බලපෑම (Impact on the Common Public)

දත්ත සොරකම්*** පුද්ගලිකව හඳුනාගත හැකි තොරතුරු (PII) අඳුරු වෙබ් අඩවිවලට නිරාවරණය කරයි. මෙය අනන්‍යතා දත්ත සොරකම් ***, මූල්‍ය වංචා, ඉලක්කගත ෆිෂින් ප්‍රහාර සහ දිගුකාලීන පීඩාවක් වැනි අපරාධවලට හේතු විය හැක.[8] Anonymous ** Bank දත්ත දත්ත සොරකම තුලින් *** කාන්දු වූ ව්‍යාජ අත්සන්, ජාතික හැඳුනුම්පත් ඡායාරූප සහ පුද්ගලික විස්තර මගින් මෙවැනි අවදානම් උග්‍ර කරයි.[8] දත්ත හැසිරවීම පිළිබඳව මහජනතාවගේ දැනුවත්භාවය නොමැතිකම, පුද්ගලයන් වංචා සහ ව්‍යාජ ලෙස පෙනී සිටීම සඳහා පහසුවෙන් ගොදුරු වීමට හේතු වේ.[31]

පුද්ගලික දත්ත කාන්දු වීමෙන් පුරවැසියන්ට ඇති වන බලපෑම, පද්ධතියක් අක්‍රිය වීමෙන් සිදුවන ක්ෂණික අපහසුතාවයට වඩා බෙහෙවින් වැඩි ය. PII කාන්දු වීම දිගුකාලීන හානියක් ඇති කරයි. එහිදී පුද්ගලයන්ට ඉදිරි වසර ගණනාවක් පුරා වංචා සහ සූරාකෑම්වල අඛණ්ඩ තර්ජනවලට මුහුණ දීමට සිදු වේ.[10] මෙය "ඩිජිටල් වශයෙන් ඇතුළත් ශ්‍රී ලංකාවක්" Digitally Inclusive Sri Lanka [26] පිළිබඳ පොරොන්දුව යටපත් කරයි. මන්දයත්, එය බිය සහ අවිශ්වාසය ඇති කරන අතර, දැනටමත් අවදානමට ලක්ව ඇති හෝ අඩු ඩිජිටල් සාක්ෂරතාවයක් ඇති අය සඳහා ඩිජිටල් බැහැර කිරීමට හේතු විය හැකිය.[1]

අනාගත ඩිජිටල් ආර්ථිකයට බලපෑම (Impact on the Future Digital Economy)

ඩිජිටල් ආර්ථිකයක් ගොඩනැගීමේ ශ්‍රී ලංකාවේ අරමුණු, සයිබර් ප්‍රහාර සහ දත්ත දත්ත සොරකම් *** මගින් අඩාල විය හැක.[1] විශ්වාසය නොමැතිකම, ඩිජිටල් වේදිකා සහ ව්‍යාපාර සමඟ කටයුතු කිරීමට මහජනතාවගේ කැමැත්ත අඩු කරයි.[19] ඩිජිටල් හැඳුනුම්පත් පිළිබඳව පෞද්ගලිකත්ව සහ ආරක්ෂක ගැටලු හේතුවෙන් ඇති වන සැක සංකා සැබෑ අභියෝගයකි.[1]

ප්‍රධාන සයිබර් ප්‍රහාරයක් රටක සමස්ත ආර්ථික පද්ධති කඩාකප්පල් කර, මූල්‍ය අස්ථාවරත්වයක් ඇති කළ හැක.[1] ඩිජිටල් ආර්ථිකය, එහි

ස්වභාවයෙන්ම, ගනුදෙනු වල ආරක්ෂාව, දත්තවල පෞද්ගලිකත්වය සහ ඩිජිටල් වේදිකාවල ස්ථාවරත්වය පිළිබඳ විශ්වාසය මත දැඩි ලෙස රඳා පවතී. මූල්‍ය (Anonymous **) සහ රජය (LGN, විශ්‍රාම වැටුප් දෙපාර්තමේන්තුව) වැනි තීරණාත්මක අංශවල පුනරාවර්තන සහ සැලකිය යුතු දත්ත සොරකම් ***, මෙම විශ්වාසය මූලික වශයෙන් බිඳ දමයි.[19] මෙම විශ්වාසය බිඳ වැටීම, ඩිජිටල් සේවා මහජනතාව විසින් භාවිතා කිරීම අඩු කිරීමට, විදේශ ආයෝජන අධෛර්යමත් කිරීමට [26], සහ ජාත්‍යන්තර ඩිජිටල් වෙළඳාමට බාධා කිරීමට හේතු විය හැකි අතර, එමගින් අපේක්ෂිත ඩිජිටල් ආර්ථිකයේම අඩිතාලම අඩාල කරයි. ආර්ථික බලපෑම දත්ත සොරකම් *** වලින් සිදුවන සෘජු මූල්‍ය අලාභයට පමණක් සීමා නොවේ; විශ්වාසය නොමැතිකම හේතුවෙන් ඩිජිටල් පරිවර්තනය අඩාල වීමෙන් ඇති වන "අවස්ථාව අහිමි වීම" ද මෙයට ඇතුළත් වේ. ප්‍රධාන ප්‍රහාරයකින් "මූල්‍ය අස්ථාවරත්වයක්" ඇති කළ හැකි බවට වන අනතුරු ඇඟවීම [1] සයිබර් ආරක්ෂාව තාක්ෂණික ගැටලුවකින් සාර්ව ආර්ථික අවදානමක් දක්වා ඉහළ නංවයි.

සුරක්ෂිත ඩිජිටල් ශ්‍රී ලංකාවක් සඳහා කැඳවීමක්

සයිබර් ආරක්ෂාව යනු තනි ආයතනයකට හෝ අංශයකට පමණක් කළ හැකි දෙයක් නොවේ. එය රජය, පෞද්ගලික අංශය සහ මහජනතාව අතර සාමූහික වගකීමකි.[2] අනාගත ඩිජිටල් ශ්‍රී ලංකාවක් සඳහා, ශක්තිමත් ඩිජිටල් පාලනයක්, පූර්ව සයිබර් ආරක්ෂණ ක්‍රමවේදයන්, විනිවිදභාවය සහ මහජන විශ්වාසය ගොඩනැගීම, සහ පුළුල් ඩිජිටල් සාක්ෂරතාවය අත්‍යවශ්‍ය වේ.[2]

පුද්ගලික දත්ත ආරක්ෂණ පනතේ (PDPA) සම්පූර්ණ ක්‍රියාත්මක කිරීම සහ නව සයිබර් ආරක්ෂණ පනතක් හඳුන්වා දීම, නියාමන රාමුව ශක්තිමත් කිරීම සඳහා වැදගත් පියවර වේ.[18] SLCERT හි මාර්ගෝපදේශ අනිවාර්ය කිරීම සහ රාජ්‍ය ආයතනවල ධාරිතා වර්ධනය අත්‍යවශ්‍ය වේ.[5] පූර්ව ආරක්ෂක ක්‍රියාමාර්ග අතරට දේශීයකරණය වූ ආරක්ෂක පද්ධති, AI-බලැති තර්ජන හඳුනාගැනීමේ මෙවලම්, ජාත්‍යන්තර ප්‍රමිතීන් අනුගමනය කිරීම, ආරක්ෂිත සංවර්ධන පිළිවෙත්, තත්‍ය කාලීන තර්ජන බුද්ධි තොරතුරු බෙදාගැනීම සහ අඛණ්ඩව ආරක්ෂාව වලංගු කිරීම සහ අනුවර්තනය වීම ඇතුළත් වේ.[3] පුද්ගලයන් සඳහා, ඩිජිටල් සාක්ෂරතාවය වැඩි දියුණු කිරීම සහ මූලික ආරක්ෂක උපදෙස් අනුගමනය කිරීම වැදගත් වේ.[21]

පාලන අඩුපාඩු, තාක්ෂණික ණය, සන්නිවේදන ගැටලු සහ ඩිජිටල් සාක්ෂරතා පරතරයන් පිළිබඳ පුනරාවර්තන තේමා, ශ්‍රී ලංකාවේ සයිබර් ආරක්ෂක අභියෝගය මූලික වශයෙන් තාක්ෂණික එකක් නොව, සමාජීය එකක් බවට පත් කරයි. සැබෑ ඩිජිටල් ඔරොත්තු දීමේ හැකියාව සඳහා,

ප්‍රතිපත්ති සම්පාදකයන් ආරක්ෂක අයවැය සහ ක්‍රියාත්මක කිරීම් ප්‍රමුඛතාවය දීම, ආයතනික නායකයන් ආරක්ෂාවට ප්‍රමුඛත්වය දෙන සංස්කෘතියක් පෝෂණය කිරීම, සහ තනි පුරවැසියන් ආරක්ෂිත ඩිජිටල් පුරුදු අනුගමනය කිරීම යන සියලු මට්ටම් හරහා චින්තනයේ වෙනසක් අවශ්‍ය වේ. "ක්‍රියා කිරීමට කැඳවීම" යනු විශේෂිත ක්‍රියාමාර්ග සඳහා පමණක් නොව, ශ්‍රී ලංකාව සාමූහිකව සයිබර් ආරක්ෂාව වටහාගෙන ආමන්ත්‍රණය කරන ආකාරයෙහි මූලික වෙනසක් සඳහා ය.

අවසාන වශයෙන්, සයිබර් ආරක්ෂාව යනු තාක්ෂණික අභියෝගයක් පමණක් නොව, සමාජීය අභියෝගයකි.[19] ශ්‍රී ලංකාවේ ඩිජිටල් ආර්ථිකයේ සහ ජාතික ආරක්ෂාවේ අනාගතය රඳා පවතින්නේ සයිබර් ආරක්ෂාව සාමූහික, අඛණ්ඩ සහ විකාශනය වන වගකීමක් ලෙස අභ්‍යන්තරීකරණය කිරීමට ඇති හැකියාව මතය. මෙයට අඛණ්ඩ දේශපාලන කැමැත්ත, අංශ හරහා හවුල්කාරිත්වයන් සහ මානව ප්‍රාග්ධනය හා යටිතල පහසුකම් සඳහා දිගුකාලීන ආයෝජන අවශ්‍ය වේ. ඩිජිටල්කරණයේ ප්‍රතිලාභ සයිබර් තර්ජනවලින් යටපත් නොවී සම්පූර්ණයෙන් සාක්ෂාත් කර ගත හැකි "සුරක්ෂිත ඩිජිටල් ශ්‍රී ලංකාවක්" නිර්මාණය කිරීම මෙහි අවසාන ඉලක්කයයි.

** නම සඳහන් නොකරන පුද්ගලික බැංකුව (Anonymous ** Bank) නීතිමය වරණයට යටත්ව නම සඳහන් නොවේ.

*** දත්ත සොරකමක් ලෙස එය දත්තවල අනිසි භාවිතයක් හෝ අනවශ්‍ය පාර්ශවයක් අතට පත් වීම සරල තේරුම් ගැනීම සඳහා යොදා ඇත.

Works cited

1. A 'fully' digital economy: 'Susceptible to cyberattacks' | The Morning, accessed June 2, 2025, https://www.themorning.lk/articles/AMbL37YhVuDSThXYV8hn
2. What Is Critical Infrastructure Protection (CIP)? Definition | Proofpoint US, accessed June 2, 2025, https://www.proofpoint.com/us/threat-reference/critical-infrastructure-protection-cip
3. Securing Sri Lanka's critical infrastructure: Conversations on ..., accessed June 2, 2025,

https://www.ft.lk/it-telecom-tech/Securing-Sri-Lanka-s-critical-infrastructure-Conversations-on-building-resilience-in-evolving-threat-landscape/50-772108
4. Cyber Terrorism an Emerging Threat to Sri Lanka's National Security - Ministry of Defence, accessed June 2, 2025, https://www.defence.lk/upload/doc/Thusitha_Bulathgama_Cyber_Terrorism_an_Emerging_Threat_to.pdf
5. Threat of cyber attacks: Focus on securing SL's digital future | The Morning, accessed June 2, 2025, https://www.themorning.lk/articles/Q0gYmCOUBHGnWp7xEDl6
6. Water Board SMS Portal Hacked, Customers Receive Threat Messages - Newswire, accessed June 2, 2025, https://www.newswire.lk/2025/06/01/water-board-sms-portal-hacked-customers-receive-threat-messages/
7. NWSDB SMS System Hacked: Customers Receive Bitcoin Ransom Demands - DailyNews, accessed June 2, 2025, https://www.dailynews.lk/2025/06/01/admin-catagories/breaking-news/789134/nwsdb-sms-system-hacked-customers-receive-bitcoin-ransom-demands/
8. Anonymous ** data breach: Bank warned of security lapses in 2024 - ReadMe, accessed June 2, 2025, https://readme.lk/Anonymous **-data-breach-bank-warned-of-security-lapses-in-2024/
9. Anonymous ** Bank Issues Statement On Cybersecurity Incident - Newsfirst.lk, accessed June 2, 2025, https://www.newsfirst.lk/2025/04/02/Anonymous **-bank-issues-statement-on-cybersecurity-incident
10. Cybersecurity event mishandled: Researcher slams Pensions Dept response to data breach, accessed June 2, 2025, https://www.newswire.lk/2025/05/30/cybersecurity-event-mishandled-researcher-slams-pensions-dept-response-to-data-breach/
11. Defining critical infrastructure for Sri Lanka - UoM Repository, accessed June 2, 2025, https://dl.lib.uom.lk/items/7c46f36f-193c-4fb7-a456-a3d6d0d769cd
12. ICS/SCADA Cybersecurity - EC-Council, accessed June 2, 2025, https://www.eccouncil.org/train-certify/ics-scada-cybersecurity/
13. ICS/SCADA Cybersecurity Certification Course - Sri Lanka - The Knowledge Academy, accessed June 2, 2025, https://www.theknowledgeacademy.com/lk/courses/ec-council-certification-training/ics-scada-cybersecurity-certification-course/
14. Sri Lanka among top three APAC countries for cyber vulnerability - Daily Mirror, accessed June 2, 2025, https://www.dailymirror.lk/print/business-main/Sri-Lanka-among-top-three-APAC-countries-for-cyber-vulnerability/245-288839
15. Ransomware Attack Wipes Out Sri Lankan Government Emails, accessed June 2, 2025, https://www.bankinfosecurity.asia/ransomware-attack-wipes-out-sri-lankan-government-emails-a-23075
16. ICTA Cyber Attack: 5000 Email IDs Lost Due to Lack of Backup, accessed June 2, 2025,

https://thecyberexpress.com/icta-cyber-attack-no-backups-problems/amp/
17. September 2023: Major Cyber Attacks, Data Breaches, Ransomware Attacks, accessed June 2, 2025, https://www.cm-alliance.com/cybersecurity-blog/september-2023-major-cyber-attacks-data-breaches-ransomware-attacks
18. Personal Data Protection Act (Sri Lanka) - Wikipedia, accessed June 2, 2025, https://en.wikipedia.org/wiki/Personal_Data_Protection_Act_(Sri_Lanka)
19. Importance of data protection for organisations in Sri Lanka - Daily FT, accessed June 2, 2025, https://www.ft.lk/columns/Importance-of-data-protection-for-organisations-in-Sri-Lanka/4-776709
20. Sri Lanka Delays Enforcement of Data Protection Act to Strengthen Regulatory Readiness, accessed June 2, 2025, https://babl.ai/sri-lanka-delays-enforcement-of-data-protection-act-to-strengthen-regulatory-readiness/
21. Accountability and mitigation in addressing data breaches | The Morning - Themorning.lk, accessed June 2, 2025, https://www.themorning.lk/articles/ASp1MgDihjBN9jP0DBvD
22. About – Sri Lanka CERT, accessed June 2, 2025, https://www.cert.gov.lk/about
23. Sri Lanka Computer Emergency Readiness Team (SLCERT ..., accessed June 2, 2025, https://mode.gov.lk/docs/institutions/SLCERT
24. Mandatory SLCERT recommendations for state websites - The Sunday Times, Sri Lanka, accessed June 2, 2025, https://www.sundaytimes.lk/250105/news/mandatory-slcert-recommendations-for-state-websites-583837.html
25. Website Security Guidelines for Government Organizations - Sri Lanka CERT, accessed June 2, 2025, https://cert.gov.lk/wp-content/uploads/2023/07/Website-Security-Guidelines-for-Government-Organizations_2022.pdf
26. How the Ministry of Digital Economy and ICTA are powering Sri Lanka's digital transformation | e27, accessed June 2, 2025, https://e27.co/ministry-of-digital-economy-icta-are-powering-sri-lankas-digital-transformation-20250530/
27. Information and Communication Technology Agency of Sri Lanka - Wikipedia, accessed June 2, 2025, https://en.wikipedia.org/wiki/Information_and_Communication_Technology_Agency_of_Sri_Lanka
28. ICS Security Best Practices - Cybersecurity for Industry - NordLayer, accessed June 2, 2025, https://nordlayer.com/blog/ics-security-best-practices/
29. Sri Lanka CERT, accessed June 2, 2025, https://www.cert.gov.lk/
30. Charting Sri Lanka's Digital Future Through Inclusive Digital Public Infrastructure, accessed June 2, 2025, https://www.undp.org/srilanka/blog/charting-sri-lankas-digital-future-through-inclusive-digital-public-infrastructure
31. Sri Lanka's Digital Well-being - DailyNews, accessed June 2, 2025,

https://www.dailynews.lk/2025/03/24/featured/748051/sri-lankas-digital-well-being/
32. onlinesafety.lk Sri Lanka CERT|CC, accessed June 2, 2025, https://onlinesafety.lk/
33. Rising Cyber security Threats in Sri Lanka: Financial Phishing Attacks Surge, accessed June 2, 2025, https://lankanewsweb.net/archives/70819/rising-cyber-security-threats-in-sri-lanka-financial-phishing-attacks-surge/
34. Sri Lanka Travel Advice & Safety | Smartraveller, accessed June 2, 2025, https://www.smartraveller.gov.au/destinations/asia/sri-lanka
35. Critical infrastructure, Critical questions: Sri Lanka's cybersecurity considerations after the Anonymous ** Bank data breach – Sanjana Hattotuwa, accessed June 2, 2025, https://sanjanah.wordpress.com/2025/04/03/critical-infrastructure-critical-questions-sri-lankas-cybersecurity-considerations-after-the-Anonymous **-bank-data-breach/