ISSUE NO 03

OCTOBER 2023

Cyber Guardian

A Publication on Online Safety

SRI LANKA CERT CC
Sri Lanka Computer Emergency Readiness Team
Coordination Centre

SECURITY සයිබර් ආරක්ෂාවට දස ශික්ෂාවක්

1 අවදානම් කළමනාකරණ ක්‍රමවේදයක්.
(Risk Management)
ඔබේ ආයතනයේ මුල්‍ය හෝ මෙහෙයුම් තොරතුරුවලට ඇති අවදානම් හඳුනා ගැනීම සඳහා ජේෂ්ඨ කළමනාකරුවන්ගේ සහායෙන් අවදානම් තක්සේරු ක්‍රමවේදයක් සකස් කරන්න. ඒ අනුව තොරතුරු තාක්ෂණ පද්ධති සහ දත්ත සඳහා ඇති අවදානම තක්සේරුකර ඒවා සුරක්ෂිත කිරීමට සුදුසු ආරක්ෂක ක්‍රමවේද අනුගමනය කරන්න.

2 අනිෂ්ට මෘදුකාංග වැළැක්වීම.
(Prevention from Malware)
ඔබගේ ආයතනයට අනිෂ්ඨ මෘදුකාංග (Malware) මගින් වන හානි වැළැක්වීම සඳහා නිසි ප්‍රති අනිෂ්ඨ මෘදුකාංග ස්ථාපනය කරන්න.

3 ආරක්ෂිත වින්‍යාසයක්
(Secure Configuration)
ඔබගේ පරිඝනක මෘදුකාංග තොරතුරු පද්ධති සහ උපකරණ සැමවිටම නවතම Patch මගින් යාවත්කාලීන කරගන්න. තවද ඒවායේ ආරක්ෂාව තහවුරුවන පරිදි වින්‍යාසගත කරන්න.

4 පිටතින් සම්බන්ධ කරණ මෙවලම් භාවිතය සීමා කිරීම
(Removable Media)
සෑමවිටම පරිඝනක සඳහා පිටතින් සම්බන්ද කරණ මෙවලම් (උදා USB sticks, External Hard Disk) භාවිතය සීමාකරන්න. එම උපාංග සම්බන්ධ කිරීමේදී අනිවාර්යෙන්ම ප්‍රති අනිෂ්ඨ මෘදුකාංගයක් මගින් Scan කිරීම සඳහා ප්‍රතිපත්තියක් සකස් කරන්න. ඒවා සම්බන්ධකර ක්‍රියාත්මක කිරීමට පෙර ස්කෑන් කරන්න.

5 පරිශීලක අධ්‍යාපනය හා දැනුවත් භාවය
(User Education and Awareness)
සයිබර් ආරක්ෂණ තර්ජන බොහොමයක් සිදුවන්නේ නොදැනුවත්බව නිසාවෙනි. එම නිසා පරිශීලකයන් දැනුවත් කිරීම,අධ්‍යාපනය ලබාදීම , පුහුණුව ලබාදීම අත්‍යාවශ්‍යවේ.

6 අනන්‍යතා කළමනාකරණය
(Access Management System)
ආයතනය තුළ ඇති පරිඝණක සහ පද්ධති සඳහා පිවිසීම් සීමා කිරීමට අනන්‍යතා කළමනාකරණ ක්‍රියාදාමයක් පවත්වා ගත යුතු අතර එමගින් දත්ත සහ පද්ධති සඳහා වන අනවසර පිවිසුම් මගහරවා ගත හැක. තවද සෑමවිටම අක්ෂර, ඉලක්කම් සහ විශේෂ සංඛේත වලින් සමන්විත මුරපද භාවිතා කළ යුතු අතර අවම වශයෙන් එහි අක්ෂර 8 ක් හෝ ඊට වැඩි ප්‍රමාණයක් යොදා ගත යුතුවේ.

7 උපස්ථ සැලැස්ම
(Backup Strategy)
ආයතනය තුළ ඇති දත්ත සහ ලොග් නිරතුරුව උපස්ථ ඊජනමව කලයුතු අතර ඒවා ආරක්ෂාකාරීව ප්‍රධාන පද්ධතියෙන් වෙන්ව ගබඩා කළ යුතුවේ.

8 සිද්ධි කළමනාකරණ සැලැස්ම
(Incident Management)
සිද්ධියකට ප්‍රතිචාර දැක්වීම සඳහා සුදුසු සිද්ධි කළමනාකරණ සැලැස්මක් ආයතනය සඳහා නිමානය කලයුතු අතර එහි ක්‍රියාකාරිත්වය නිරතුරුව ඇගයීමට ලක් කල යුතුවේ.

9 නිවසේ සිට රාජකාරි කටයුතුවල නිරතවීම
(Policy on Work from Distance)
දුරස්ථව කාර්යාලකටයුතු කිරීම සඳහා ප්‍රතිපත්තියක් සකස්කර ඊට අනුගතව කටයුතු කිරමට කාර්ය මණ්ඩලය පුහුණු කරන්න. දුරස්ථව කටයුතු කිරීමේදී දත්ත හා උපාංග ආරක්ෂා කරගැනීමේ මූලික ආරක්ෂිත ක්‍රමවේදයන් හදුන්වා දෙන්න.

10 ආරක්ෂණ විගණනයන්
(Security Assessments)
ආයතනය විසින් සිය පරිඝනක පද්ධති, දත්ත ආරක්ෂා කිරීමට ආරක්ෂණ විගණනයක් සිදුකලයුතු අතර එමගින් හදුනා ගන්නා ආරක්ෂිත දෝෂ නිවැරදි කලයුතු වේ. මෙම විගණනයන් පරිඝනක පද්ධතියේ ක්‍රියාත්මක කිරීමට පෙර හෝ දැනට ක්‍රියාත්මක වන පරිඝනක පද්ධතියක වෙනස් කිරීමක් සිදුකිරීමෙන් පසු හෝ එම පරිඝනක පද්ධතිය ස්ථාපනය කර ඇති මාධ්‍යයේ වෙනසක් සිදුකිරීමකින් පසු හෝ සයිබර් ප්‍රහාරයකින් පසු ආරක්ෂණ විගණනය කල යුතුය.

News

ශ්‍රී ලංකා සර්ට් ආයතනය විසින් රාජ්‍ය ආයතනවල තොරතුරු ආරක්ෂක නිලධාරීන් (ISO) සහකාර තොරතුරු ආරක්ෂක නිලධාරීන් (AISO) සහ අනෙකුත් නිලධාරීන් සඳහා නිර්මාණය කරන ලද සයිබර් වැඩසටහන් මල්ලවක් සංවිධානය කරනිඛේ. මේ අනුව 2000ක පමන නිලධාරීන්ට මෙම පුහුණුව ලබාදීමට සැලසුම් කර ඇත. මෙම සැසියේ මූලික පරමාර්ථය වන්නේ රාජ්‍ය ආයතනවල සංවේදී තොරතුරු වත්කම් ආරක්ෂා කිරීම සඳහා අවශ්‍ය දැනුම ලබාදීමයි.

Sri Lanka CERT විසින් අලුතින් පත් වූ ICT ගුරුවරුන් සඳහා පුහුණු සැසියක් පවත්වන ලදී. මෙම වැඩසටහන අධ්‍යාපන අමාත්‍යාංශය විසින් සංවිධානය කර තිබූ අතර මේ සඳහා සියලුම පළාත් නියෝජනය කරමින් තොරතුරු හා සන්නිවේදන තාක්ෂණ ගුරුවරුන් 130කට ආසන්න පිරිසක් සහභාගි වූහ.මෙම වැඩමුළුවේ දෙවන අදියර සඳහා ගුරුවරුන් 100 පමණ සහබාගි විය.

Hot Line -101
report@cert.gov.lk
www.cert.gov.lk
www.onlinesafety.lk

ශ්‍රී ලංකා සර්ට් ආයතනයේ කාර්යභාරය

ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය හෙවත් Sri Lanka CERT යනු සයිබර් තර්ජන වළින් සයිබර් අවකාශය ආරක්ෂා කිරීමේ ජාතික වගකීම දරන ආයතනය වේ. එය වාර්තමානයේ තාක්ෂණ අමාත්‍යංශය යටතේ ක්‍රියාත්මක වන අතර මනා පුහුණුවක් සහ සුදුසුකම් ලත් සයිබර් ආරක්ෂණ වෘත්තිකයන්ගෙන් සමන්විත වේ. ශ්‍රී ලංකා CERT අනෙකුත් විදේශීය පරිෂනක හදිසි ප්‍රතිචාර සංසද සමග සම්බන්ද වෙමින් කටයුතු කරණ අතර එය FIRST, Asia Pacific CERT යන අන්තර්ජාතික පරිෂනක හදිසි ප්‍රතිචාර සංසදයන්හි සාමාජිකත්වය දරයි.

ශ්‍රී ලංකාව තුළ සිදුවන සයිබර් ප්‍රහාර වලට ක්ෂණික ප්‍රතිචාර දක්වමින් එම ප්‍රහාර වැලැක්වීම ට හෝ ඒවායේ බලපෑම අවම කිරීමට ගෝලීය රාජ්‍ය ආයතනවලට සහාය වීමට ශ්‍රී ලංකා සර්ට් ආයතනය කටයුතු කරයි. තවද ගෝලීය හා දේශීය සයිබර් තර්ජන පිළිබඳව නිරන්තරව නිරීක්ෂණය කරමින් අදාළ පාර්ශවයන් දැනුවත් කිරීම හා තර්ජනවලින් මුදාගැනීම සඳහා තාක්ෂණික සහයද ලබාදේ. එමෙන්ම ජාතිකමය වශයෙන් සයිබර් ආරක්ෂාව පිළිබඳ ප්‍රතිපත්ති හා මාර්ගෝපදේෂ හදුන්වාදීම ද සිදුකරයි. ශ්‍රී ලංකා සර්ට් ක්‍රියාකාරිත්වය හේතුවෙන් ගෝලීය වශයෙන් එල්ලවන තර්ජන වලක්වාගැනීමට මෙන්ම අහිතකර බලපෑම් වලක්වා ගැනීමට ද හැකිවී තිබේ. විශේෂයෙන්ම රාජ්‍ය ආයතන සයිබර් ප්‍රහාර වලින් ආරක්ෂා කිරීමට සුදානම් කිරීම හා ප්‍රහාරයක් එල්ල වුවහොත් අවශ්‍ය ප්‍රතිචාර දැක්වීම සර්ට් ආයතනයේ මූලිකම වගකීමක් ලෙස හදුන්වා දිය හැකියි. එමෙන්ම සයිබර් ආරක්ෂාව පිළිබඳ රාජ්‍ය අංශයේ ශක්තිමත් ශ්‍රමබලකායක් ගොඩනැගීම, විවිධ සමාජ කොටස් දැනුවත් කිරීමත් සයිබර් තර්ජනවලට ලක්වන ආයතන හා පුද්ගලික ගැටළු විසඳාගැනීමට සහාය වීමත් සිදුකරයි.

Circular

රාජ්‍ය නිල කටයුතු සඳහා
gov.lk

සියලුම රාජ්‍ය ආයතන සිය නිල සන්නිවේදන කටයුතු සඳහා නිල විද්‍යුත් ලිපින භාවිතා කලයුතුවේ. පුද්ගලික කටයුතු සඳහා මෙම නිල ඊ මේල් භාවිතා නොකළ යුතු බවටත් රාජ්‍ය ආයතන සඳහා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය මගින් දක්වා ඇත. තවද ජනා ධිපති ලේකම් වරයා විසින් නිකුත් කළ SP/SB/10/13 චක්‍රලේකය මගින් ද මේ බව තහවුරු කොට තිබේ.

නිල විද්‍යුත් තැපැල් ලිපිනයක් යනු gov.lk යටතේ රජය විසින් නිකුත්කරන ලද්දකි. එය රජය සතු වත්කමක් වන අතර එය ආරක්ෂාකාරීව පරිහරණය කිරීම රාජ්‍ය නිලධාරීන්ගේ වගකීමකි. එම විද්‍යුත් ලිපින භාවිතා කිරමේදී අනුගමනය කලයුතු ආරක්ෂණ උපදෙස් ද මෙම ප්‍රතිපත්තියේ දක්වා ඇත.

Laws & policies

තොරතුරු, තොරතුරු තාක්ෂණ හා සයිබර් ආරක්ෂාව සම්බන්ධයෙන් වන අණ පනත්

- පරිගණක අපරාධ පනත, 2007 අංක 24.
- ගෙවීම් උපාංග වංචා පනත, 2006 අංක 30.
- පුද්ගලික දත්ත ආරක්ෂණය පනත, 2022 අංක 9.
- විද්‍යුත් ගනුදෙනු පනත 2006 අංක 19.
- රාජ්‍ය ආයතන සඳහා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය.

Gmail
පරිශීලකයන්ගේ ආරක්ෂාවට නව මාර්ගෝපදේශ

දත්ත සොරකම් කිරීම් හා අනිෂ්ඨ Malware මෘදුකාංග, email මගින් බෙදාහැරීමට එරෙහිව විද්‍යුත් තැපෑල ආරක්ෂාකොට ශක්තිමත් කිරීමට email යවන්නන් සඳහා නව මාර්ගෝපදේශ ලබන පෙබරවාරියේ සිට හඳුන්වා දීමට Google සමාගම සුදානම් වෙයි. මේ අනුව email වංචා කිරීම් සහ දත්ත පැහැර ගැනීම් වලට එරෙහිව ආරක්ෂාව ශක්තිමත් කිරීමට පරිශීලකයන්ගේ ගිණුම් සඳහා SPF/DKIM සහ DMARC සත්‍යාපන හඳුන්වාදෙනු ඇත. දත්ත සොරාගැනීම් පැහැරගැනීම් වලක්වාලීමටත් හානිකර මෘදුකාංග සංසරණය නිශ්චිතවම හඳුනාගැනීමටත් එමගින් හැකිවනු ඇත.

කරදරකාරී වෙළෙඳ email වලක්වා ගැනීම සඳහා එහි ඇති එක් අයිකනයක් click කිරීමෙන් එම සබඳතා unsubscribe කල හැකිය. ඊට අමතරව දින දෙකක් ඇතුලත සබඳතා වැලැක්වීම ක්‍රියාවට නැගීමට එම වාණිජ ව්‍යාපාරයන්ට සිදුවේ. මේ වන විටත් Gmail හි කෘතීම බුද්ධිය මත පදනම්වූ ආරක්ෂාව මගින් 99.9% කට වඩා දත්ත සොරකම් කිරීම් සහ අනිෂ්ඨ මෘදුකාංගemail සමග සම්බන්ධවීම සාර්ථක ලෙස වලක්වන බව Google සමාගම පවසයි. ඒ අනුව දිනකට අනවශ්‍ය email බිලියන 15 කට ආසන්න ප්‍රමාණයක් සාර්ථක ලෙස අවහිර කිරීමට හැකිවිතිබේ.

ඔබ email ආරක්ෂණ ප්‍රමිතීන්ගේ සංකීර්ණතා ගැන කරදර විය යුතු නැත. නමුත් ඔබට විද්‍යුත් තැපැලක් මුලාශ්‍රයක් ලෙස විශ්වාශය තැබිය හැකි විය යුතුය. කෙසේ වෙතත් මෙමගින් කිසියම් දුර්වලතාවකින් හෝ සිදුවිය හකි තර්ජන වලින් බේරීසිටීමට email භාවිතා කරන්නන්ට හැකිවනු ඇත.