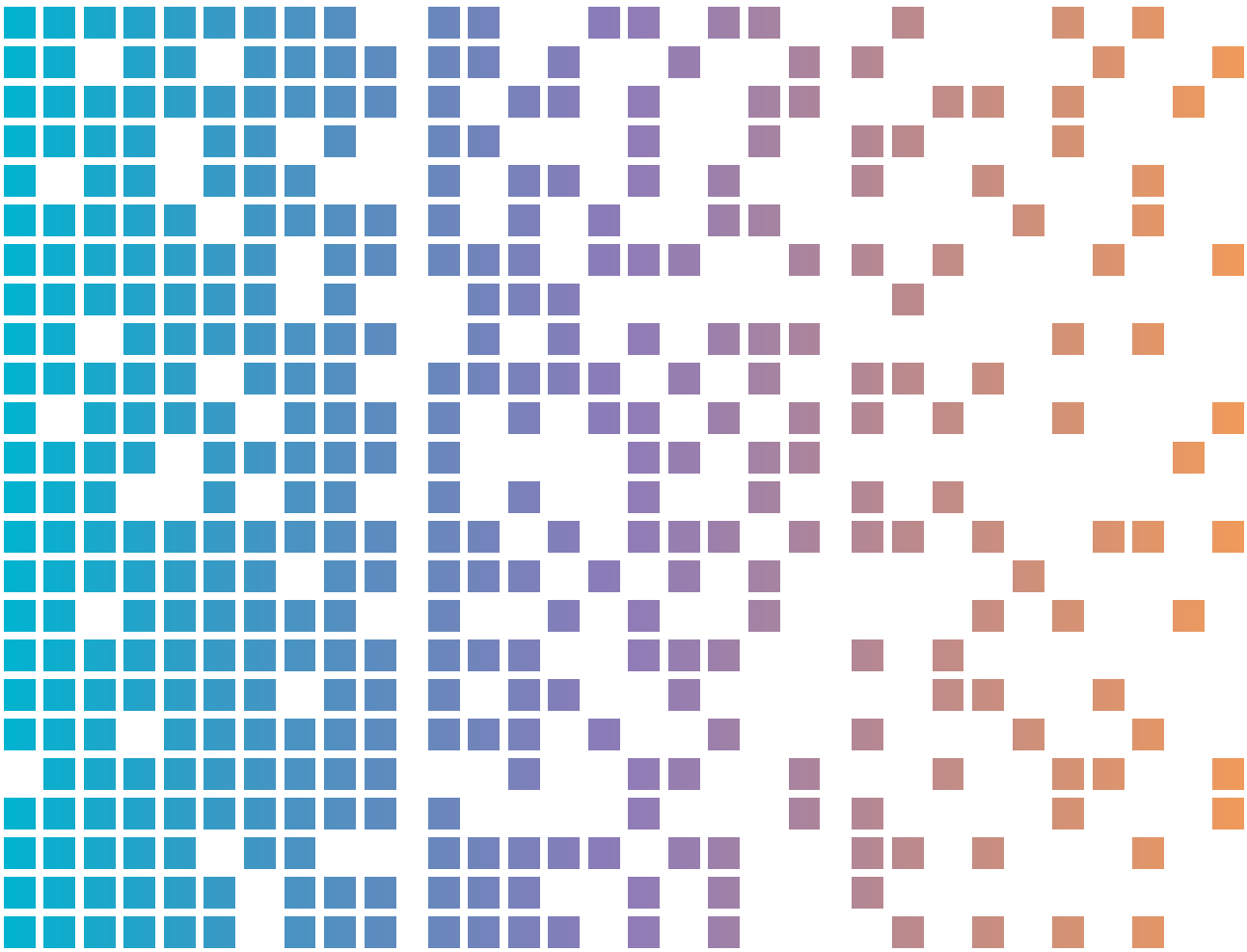
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

නිහඬ මංකොල්ලය: ආයතනික ජාලයන් අවදානමට ලක් කිරීම සඳහා සයිබර් අපරාධකරුවෝ තොරතුරු සොරා ගන්නා ද්වේශසහගත මෘදුකාංග භාවිතා කරති



අන්තර්ගත සංකීර්ණතාව
මධ්‍යස්ථ ● ● ○

පටුන

සංදර්භය

තොරතුරු සොරා ගන්නා ද්වේශසහගත මෘදුකාංග, සයිබර් අපරාධකරුවන් විසින් ප්‍රධාන වශයෙන් මුදල් ලබා ගැනීම සඳහා අයුතු ලෙස ප්‍රයෝජන ගන්නා පරිශීලක විශ්වාසනීය තොරතුරු සහ පද්ධති තොරතුරු සොරකම් කරයි. ඔස්ට්‍රේලියාව ඇතුළු ලොව පුරා විවිධ සංවිධානවලට සහ අංශවලට එරෙහි සයිබර් අපරාධ ප්‍රහාරවලදී තොරතුරු සොරකම් කරන්නන් නිරීක්ෂණය කර ඇත. මෙම ප්‍රකාශනය මගින් තොරතුරු සොරා ගන්නා ද්වේශසහගත මෘදුකාංග පිළිබඳ සයිබර් ආරක්ෂණ මාර්ගෝපදේශ පාඨකයින්ට සපයයි. එහි තර්ජන ක්‍රියාකාරකම් සහ ඒවා ලිහිල් කිරීම සඳහා සංවිධාන සහ ඒවායේ සේවකයින් වෙත ලබාදෙන උපදෙස් ඇතුළත් වේ.

ප්‍රධාන කරුණු

- තොරතුරු සොරා ගන්නා ද්වේශසහගත මෘදුකාංග තොරතුරු සොරකම් කරන්නන් ලෙසද හැඳින්වෙන අතර එය වින්දිතයෙකුගේ උපාංගයෙන් තොරතුරු රැස් කිරීම සඳහා නිර්මාණය කර ඇති ද්වේශසහගත මෘදුකාංග වර්ගයකි. මෙයට පරිශීලක නාම සහ මුරපද, ණයපත් විස්තර, ක්‍රිප්ටෝ මුදල් පසුම්බි, දේශීය ලිපිගොනු, සහ කුකීස්, පරිශීලක ඉතිහාසය සහ ස්වයංක්‍රීයව පෝරම පිරවීමේ විස්තර ඇතුළු බ්‍රව්සර් දත්ත ඇතුළත් විය හැකිය.
- වින්දිතයාගේ සේවායෝජකයාගේ, ඔවුන්ගේ සේවාදායකයින්ගේ සහ වෙනත් ව්‍යවසාය පද්ධතිවල උපාංග වෙත මූලික ප්‍රවේශය ලබා ගැනීම සඳහා ආයතනික ගිණුම් හා සම්බන්ධ සොරකම් කරන ලද පරිශීලක විශ්වාසනීය තොරතුරු මිලදී ගැනීමට සහ භාවිතා කිරීමට සයිබර් අපරාධකරුවන් උත්සාහ කළ හැකිය. මෙම සංවිධානවලට පසුව ඇති වන බලපෑම් අතරට කප්පම් ගැනීමට යොදා ගන්නා මෘදුකාංග, කප්පම් ගැනීම, ව්‍යාපාරික විද්‍යුත් තැපැල් අවදානමට ලක් කිරීම සහ බුද්ධිමය දේපළ සොරකම් කිරීම ඇතුළත් විය හැකිය.
- ඔස්ට්‍රේලියානු සංඥා අධ්‍යක්ෂ මණ්ඩලයේ ඔස්ට්‍රේලියානු සයිබර් ආරක්ෂක මධ්‍යස්ථානය (ASD හි ACSC) විසින් ආයතනික ජාල කඩකිරීම් හඳුනාගෙන ඇති අතර, එය සේවකයින් විසින් අවදානමට ලක් වූ පුද්ගලික උපාංගවලින් රැකියා සම්පත් වෙත ප්‍රවේශ වීමෙන් ඇති වේ. බොහෝ අවස්ථාවන්හිදී, සයිබර් අපරාධකරුවෝ සොරකම් කරන ලද වලංගු පරිශීලක විශ්වාසනීය තොරතුරු භාවිතා කිරීම මගින් ආයතනික ජාල වෙත මූලික ප්‍රවේශය ලබා ගත්තෝය. සයිබර් අපරාධකරුවන් වරප්‍රසාද ලත් පරිශීලක ගිණුම් වෙත සාර්ථකව ප්‍රවේශ වීමෙන් පසුව පුළුල් ලෙස අවදානමට ලක්වීම් සාමාන්‍යයෙන් සිදු වූ බව අපගේ විමර්ශන මගින් පෙනී ගියේය.
- සේවකයින්ට, කොන්ත්‍රාත්කරුවන්ට, කළමනාකරණය කරන ලද සේවා සපයන්නන්ට හෝ වෙනත් ආයතනවලට දුරස්ථව තම ජාලයට ප්‍රවේශ වීමට පහසුකම් සපයන සංවිධාන, Bring Your Own Device (BYOD) දෘඪාංග ඇතුළුව, තොරතුරු සොරකම් කරන්නන්ගේ අවදානම් පිළිබඳව දැනුවත් විය යුතු අතර මෙම තර්ජනයෙන් තමන්ව ආරක්ෂා කර ගත යුතුය. සයිබර් අපරාධකරුවන් පුළුල් පරාසයක ශිල්පීය ක්‍රම භාවිතා කරමින් වින්දිත උපාංග වෙත තොරතුරු සොරකම් කරන්නන්ව යොදවයි. මේවාට වංචනිකව යවන (phishing) ඊමේල්, සොරකම් කරන ලද මෘදුකාංග බාගත කිරීම්, සෙවුම් යන්ත්‍ර ප්‍රශස්තිකරණ (SEO) ශිල්පීය ක්‍රම, ද්වේෂසහගත වෙළඳ දැන්වීම් හෝ සමාජ මාධ්‍ය වේදිකාවල පළ කරන ලද ද්වේෂසහගත සබැඳි ඇතුළත් වේ. සාමාන්‍යයෙන්, පරිශීලක හැසිරීම් සහ අඩු ආරක්ෂක පාලනයන් හේතුවෙන් රැකියා සහ පුද්ගලික අරමුණු සඳහා භාවිතා කරන උපාංගයන් මෙම ශිල්පීය ක්‍රම හරහා ආසාදනය වීමේ වැඩි අවදානමක් ඇත.
- තොරතුරු සොරකම් කරන්නන් විසින් සයිබර් අපරාධකරුවන්ට, විශේෂයෙන් ආරම්භක මට්ටමේ සහ සීමිත තාක්ෂණික ප්‍රවීණතාවයක් ඇති අයට, සයිබර් අපරාධ ක්‍රියාකාරකම් මගින් මුදල් ඉපයීමට ආකර්ශනීය ආකෘතියක් ලබා දෙයි.

පසුබිම

සයිබර් අපරාධකරුවන් විසින් තොරතුරු සොරකම් කරන්නන් භාවිතා කිරීම ඔස්ට්‍රේලියානු සංවිධානවල ආරක්ෂාවට සහ යහපැවැත්මට තර්ජනයක් වේ. සයිබර් අපරාධකරුවන් පරිශීලක විශ්වාසනීය තොරතුරු රැස් කිරීම සඳහා තොරතුරු සොරා ගන්නා ආසාදන භාවිතා කරන බැවින්, ඒවා සාමාන්‍යයෙන් ප්‍රධාන සයිබර් ආරක්ෂක සිදුවීම් සඳහා පූර්වගාමී ක්‍රියාකාරකම් වේ. මෙම පරිශීලක විශ්වාසනීය තොරතුරු, විශේෂයෙන් අන්තර්ජාලයට මුහුණලා ඇති දුරස්ථ සේවා හෝ වරප්‍රසාද ලත් ගිණුම් වෙත ප්‍රවේශය සපයන ඒවා, පසුව ආයතනික පද්ධති සහ දත්ත වෙත ආරම්භක ප්‍රවේශය සඳහා අයුතු ලෙස ප්‍රයෝජනයට ගනු ලැබේ.

සටහන: සොරකම් කරන ලද පරිශීලක විශ්වාසනීය තොරතුරු මිලදී ගැනීම සහ වලංගු කිරීම මගින් සයිබර් අපරාධ පරිසර පද්ධතිය තුළට ආරම්භක ප්‍රවේශය සඳහා තැරැව්කරුවෝ විශේෂිත කාර්යභාරයක් ඉටු කරයි.ඉන්පසු ඔවුන් ආයතනික පරිසරයන් සඳහා විශාල ඉල්ලුමක් ඇති උසස් තත්ත්වයේ පරිශීලක විශ්වාසනීය තොරතුරු, සංවිධානයේ ආයතනික ජාලය සූරාකෑම සඳහා පරිශීලක විශ්වාසනීය තොරතුරු භාවිතා කරන සයිබර් අපරාධකරුවන්ට වෙන්දේසි කරයි.

සොරකම් කරන ලද වලංගු පරිශීලක විශ්වාසනීය තොරතුරු සයිබර් අපරාධකරුවෝ ඉතා අගය කරති. ඒ මන්ද යත්, ඒවා මගින් ආයතනික ජාල සහ ව්‍යවසාය පද්ධති වෙත මූලික ප්‍රවේශය වේගවත් කරනු ලබයි. සොරකම් කරන ලද වලංගු පරිශීලක විශ්වාසනීය තොරතුරු සමඟින්, සයිබර් අපරාධකරුවන්ට සාමාන්‍ය උපක්‍රම සහ ශිල්පීය ක්‍රම කිහිපයක් මඟ හැරිය හැකිය. ඒවා අතරට ඇතුළත් වන්නේ:

- ඉලක්කයක් හඳුනා ගැනීම සහ ඒ ගැන සොයා බැලීම
- ඉලක්කයේ ජාලයන්ගේ අවදානම් ගණනය කිරීම
- ආරම්භක ප්‍රවේශය සඳහා දර්ශක වර්ධනය කිරීම, පහත දේ වැනි:
  - වංචනිකව යවනු ලබන දේවල්
  - මෘදුකාංගවල අවදානම් අයුතු ලෙස ප්‍රයෝජනයට ගැනීම
  - Remote Desktop Protocol (RDP) හෝ virtual private network (VPN) සේවාවන් ඇතුළුව දුරස්ථ සේවාවන් ඉලක්ක කර ගැනීම
  - පරිශීලක විශ්වාසනීය තොරතුරුවලට (මුරපද අනුමාන කිරීම) එරෙහිව එල්ල වන දරුණු බල ප්‍රහාර.

මෙම පියවරයන්ට කාලය ආයෝජනය කිරීම හා සමහර සයිබර් අපරාධකරුවන් බාධකයක් ඉදිරිපත් කෙරෙන තාක්ෂණික යෝග්‍යතා මට්ටමක් අවශ්‍ය වේ. විශේෂයෙන්ම, ආයතනික ජාල ආරක්ෂණය විනිවිද යාමට නොහැකි සයිබර් අපරාධකරුවන් හට තොරතුරු සොරා ගන්නා ආසාදනවලින් සෘජුවම ප්‍රතිලාභ ලැබිය හැකිය. ඒ මන්ද යත්, මෙම ආසාදන මගින් යෝග්‍ය ආයතනික ජාල වෙත ඉක්මන් සහ පහසු පරිශීලක අක්තපත්‍ර ප්‍රවේශයක් ලබා දිය හැකි බැවිනි. දුරස්ථව සේවයේ යෙදෙන අවස්ථා වලදී, සමහර සේවකයෝ රාජකාරි සහ පුද්ගලික අන්තර්ජාල බ්‍රවුසර් යන දෙකම සඳහා පුද්ගලික උපාංග භාවිතා කරති.

එසේ කිරීමෙන්, සේවකයින්ට ඔවුන්ගේ පරිශීලක විශ්වාසනීය තොරතුරු ඔවුන්ගේ වෙබ් බ්‍රවුසර මුරපද ගබඩාවල සහ දිගුවන්හි ගබඩා කිරීමට තෝරා ගත හැකිය. නැතහොත් ඔවුන් වෙබ් බ්‍රවුසර ස්වයංක්‍රීය පිරවුම් විශේෂාංග භාවිතා කළ හැකිය. තොරතුරු සොරකම් කරන්නන් මෙම මුරපද ගබඩා, සත්‍යාපන කුකීස් සහ වෙබ් බ්‍රවුසරය තුළ ඇති අනෙකුත් පුද්ගලික දත්ත සමඟින් ඉලක්කගත කරයි.

ආයතනික උපාංග මෙන් නොව, පුද්ගලික උපාංගවල සෑම විටම බලාත්මක කළ ව්‍යවසාය ආරක්ෂක ප්‍රතිපත්ති නොමැති අතර, එය සංවිධානවලට ඉහළ අවදානමක් ඇති කරයි. උදාහරණයක් ලෙස, සේවකයින් කොල්ලකන ලද මෘදුකාංග බාගත කිරීම සහ අධි අවදානම් සහිත මාර්ගගත බ්‍රවුසින් කිරීම වැනි ක්‍රියාකාරකම්වල නිරත විය හැකි අතර එමගින් සයිබර් තර්ජන සහ ද්වේශසහගත මෘදුකාංග ආසාදනවලට ඔවුන්ව නිරාවරණය වීම වැඩි කරයි.

තොරතුරු සොරකම් කරන්නන්, බෙදාහරින්නන්, ආරම්භක ප්‍රවේශ තැරැව්කරුවන් සහ කප්පම් මෘදුකාංග අනුබද්ධ සමාගම් දැන් මූල්‍ය ලාභය මගින් මෙහෙයවනු ලබන සයිබර් අපරාධ පරිසර පද්ධතියක මූලික කොටසක් නියෝජනය කරයි. සයිබර් අපරාධකරුවන් ප්‍රහාරයක නිශ්චිත අවධීන් ඉලක්ක කර ගනිමින් හැකියාවන්ට විශේෂත්වයක් දෙමින් සංවර්ධනය කර, පසුව එම හැකියාව අනෙකුත් අපරාධ අනුබද්ධ සමාගම්වලට සේවාවක් ලෙස විකුණන විට, පරිසර පද්ධතිය වඩාත් කාර්යක්ෂමව වර්ධනය වේ.

තර්ජනාත්මක ක්‍රියාකාරීත්වය

ASD හි ACSC ගෝලීය වශයෙන් තොරතුරු සොරකම් කරන්නන්ගේ ක්‍රියාකාරකම්වල වැඩිවීමක් නිරීක්සමින් සහ නිරීක්ෂණය කරමින් සිටින අතර එය ඔස්ට්‍රේලියානු ජාලවලට වැඩි තර්ජනයක් ඉදිරිපත් කරයි. 2023 පුරා සයිබර් අපරාධ ක්‍රියාකාරකම් හරහා වඩාත්ම ජනප්‍රිය ද්වේශසහගත මෘදුකාංග ප්‍රභේදය වූයේ තොරතුරු සොරකම් කරන්නන් බව කර්මාන්ත වාර්තාකරණයෙන් පෙන්නුම් කෙරේ. වංචනික වෙබ් වෙළඳපොළවල විකිණීමට ඇති සොරකම් කරන ලද දත්ත වැඩිවීමේ පරිමාව, සහ මෙම දත්ත උපයෝගී කර ගනිමින් ආරම්භක ප්‍රවේශ තැරැව්කාර ක්‍රියාකාරකම්වල වැඩිවීම, 2024 දක්වා වේගවත් වී ඇති මෙම ඉහළ යන ප්‍රවණතාවය පිළිබිඹු කරයි.

තොරතුරු සොරා ගන්නා පරිසර පද්ධති

පියවර 1: ද්වේශසහගත මෘදුකාංග ලබා ගැනීම

තොරතුරු සොරකම් කරන්නන්ව සාමාන්‍යයෙන් සයිබර් අපරාධ වෙළඳපොළෙහි MaaS හෝ Stealer-as-a-Service ලෙස පිරිනමනු ලැබේ. නැතහොත් මූලාශ්‍ර කේතයක් ලෙස විකුණනු ලැබේ. MaaS යනු ව්‍යාපාර ආකෘතියක් වන අතර එමඟින් ද්වේශසහගත මෘදුකාංග සංවර්ධකයෙකු තම ද්වේශසහගත මෘදුකාංග සඳහා දායකත්වයක් වෙබ් පාදක වේදිකාවක් හරහා පුද්ගලයන්ට විකුණන අතර එය නීත්‍යානුකූල Software-as-a-Service පිරිනැමීම් වලට සමාන වේ. MaaS ආකෘතිය මඟින් තාක්ෂණික කුසලතා නොමැති පුද්ගලයින්ට ද්වේශසහගත මෘදුකාංග බෙදා හැරීමට සහ සයිබර් ප්‍රහාර සඳහා භාවිතා කිරීම සඳහා සොරකම් කරන ලද තොරතුරු රැස් කිරීමට ඉඩ සලසන බැවින්, එය සයිබර් අපරාධකරුවන්ට ඇතුළුවීමට ඇති බාධකය අඩු කර ඇත.

MaaS ලෙස පිරිනමන තොරතුරු සොරකම් කරන්නන් සාමාන්‍යයෙන් සාපේක්ෂව අඩු මාසික ගාස්තුවකට වෙළඳ දැන්වීම් මඟින් ප්‍රචාරය කරනු ලබන අතර, එමඟින් සයිබර් අපරාධකරුවන්ට තොරතුරු සොරකම් කරන්නන්ගේ උපකරණ පුවරුවට ප්‍රවේශය ලබා දේ. උපකරණ පුවරුව තොරතුරු සොරා ගන්නා ද්වේශසහගත මෘදුකාංග නිර්මාණය කිරීමට, සොරකම් කරන ලද දත්ත සංවිධානය කිරීමට, සහ අවදානමට ලක් වූ පද්ධති ගණන සොයා ගැනීමට පහසුකම් සපයයි. MaAS ක්‍රියාකරුවෝ ප්‍රති-වයිරස මෘදුකාංග මඟින් සොයා ගැනීමෙන් වැළකී සිටීමට සහ ග්‍රාහකයින් ආකර්ෂණය කර ගැනීමට සහ රඳවා ගැනීමට විශේෂාංග යාවත්කාලීන කිරීම්, මෙවලම් සහ තාක්ෂණික සහාය ලබා දෙති. බොහෝ තොරතුරු සොරකම් කරන්නන්ට දත්ත මුදා හැරීමෙන් පසු වින්දිතයාගේ උපාංගයෙන් තමන්වම මකා දැමීමේ හැකියාව ඇත.

පියවර 2: බෙදා හැරීම

තොරතුරු සොරකම් කරන්නන් බෙදා හරින සහ අවදානමට ලක් වූ උපාංගවලින් තොරතුරු රැස් කරන සයිබර් අපරාධකරුවන් 'Traffers' (traffic distributors - අන්‍යෝන්‍ය සන්නිවේදන බෙදාහරින්නන්) ලෙස හැඳින්වේ. Traffers විසින් වින්දිතයින්ව ද්වේෂසහගත සබැඳි වෙත යොමු කර, පුළුල් සංවිධානාත්මක නිරතවීම්වල කොටසක් ලෙස තොරතුරු සොරකම් කරන්නන් පැතිරවීමට පහසුකම් සපයයි. බොහෝ සංවිධානාත්මක නිරතවීම් අවිචාරවත් වන අතර, ඒවා අවස්ථාවාදී ආසාදන මත රඳා පවතී. කෙසේ වෙතත්, සමහර සංවිධානාත්මක නිරතවීම් නිශ්චිත කර්මාන්තවලට ගැලපෙන අතර නිශ්චිත වින්දිතයින් ඉලක්කගත කරමින් වංචනිකව යවනු ලබන දේවල් ඇතුළත් වේ. Traffers මෙම වඩාත් ඉලක්කගත සංවිධානාත්මක නිරතවීම් සිදු කරන්නේ පාරිභෝගික ඉල්ලුමට ප්‍රතිචාර වශයෙනි; උදාහරණයක් ලෙස, ගැනුම්කරුවන් නිශ්චිත ඉහළ වටිනාකමක් ඇති සංවිධාන හෝ අංශ වෙත ප්‍රවේශය සෙවීම.

Traffers විසින් පුළුල් පරාසයක ශිල්පීය ක්‍රම භාවිතා කරමින් වින්දිත උපාංග වෙත තොරතුරු සොරකම් කරන්නන් යොදවනු ඇත. ඒවාට අයත් වන්නේ:

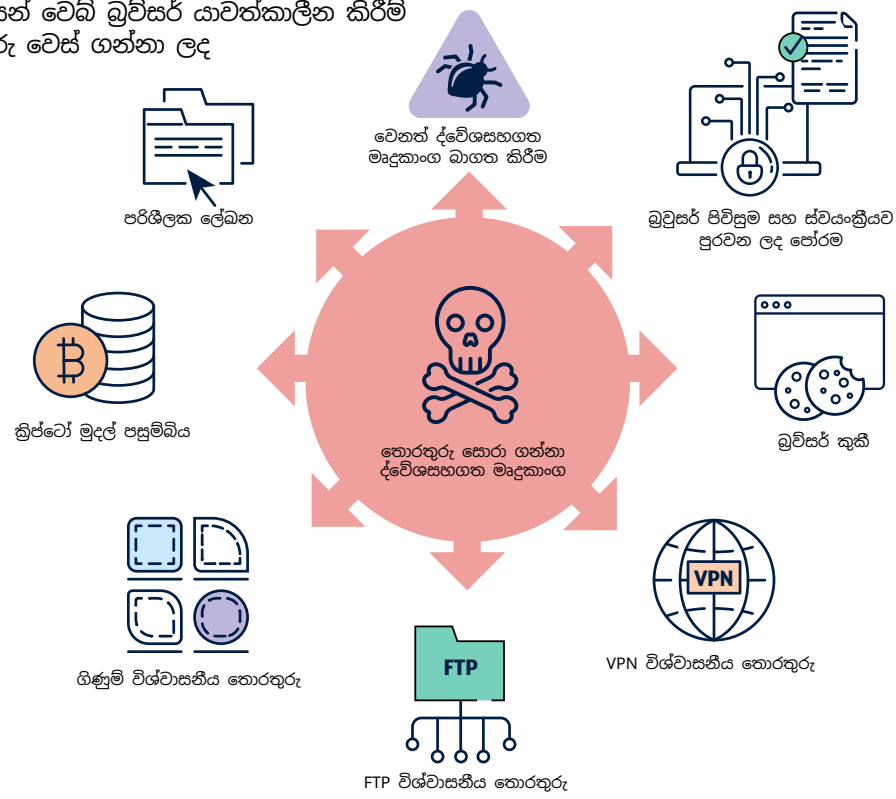
- **botnets (අවදානමට ලක් වූ පරිගණක ජාලයක්):** වංචනිකව යවන පණිවිඩ හෝ ද්වේශසහගත මෘදුකාංග ලබා දීම වැනි ද්වේෂසහගත ක්‍රියා සිදු කිරීම සඳහා සයිබර් අපරාධකරුවන් විසින් පාලනය කරනු ලබන අවදානමට ලක් වූ පරිගණක පද්ධති ජාල

- **වංචනිකව යවන දේ:** සමාජ මාධ්‍ය, සංසද සහ පණිවිඩ යෙදුම් මගින් යවන ඊමේල් හෝ සෘජු පණිවිඩ හරහා රැවටිලිකරී ලෙස සංවේදී තොරතුරු ලබා ගැනීමට උත්සාහ කිරීම. මේවා සයිබර් අපරාධකරුවන්ට ඇතුළුවීමට ඇති බාධකය අඩු කරන පොදු බෙදාහැරීමේ ක්‍රම වේ:
  - මෙම පණිවිඩවල සාමාන්‍යයෙන් අඩංගු වන්නේ ඊමේලයකට අමුණන ලද ද්වේෂසහගත ගොනු වෙනුවට ද්වේෂසහගත සබැඳියක් ය.
- **ද්වේෂසහගත සෙවුම් ප්‍රතිඵල:** ද්වේශසහගත මෘදුකාංග සපයන වෙබ් අඩවි වෙත ඉලක්ක යොමු කරන සෙවුම් යන්ත්‍ර ප්‍රශස්තිකරණ (SEO) ශිල්පීය ක්‍රම හරහා ලබා ලබාදෙන අතර ඒවා නීත්‍යානුකූල මෘදුකාංග හෝ වෙනත් අන්තර්ගතයන් ලෙසින් බොරු වෙස් ගනිමින් පෙනී සිටී
- **malvertising:** ද්වේශසහගත මෘදුකාංග බෙදා හැරීම සඳහා නීත්‍යානුකූල මාර්ගගත වෙළඳ දැන්වීම්වලට ඇතුල් කරන ලද හානිකර කේත භාවිතා කිරීම
- **පළඳු සහිත හෝ සොරකම් කරන කොල්ලකන ලද ලද මෘදුකාංග:** වීඩියෝ විස්තර හෝ අදහස් දැක්වීම් තුළට ඇතුල් කළ ද්වේශසහගත සබැඳි සමඟින්, හෝ විශ්වාස කළ නොහැකි බාගත කිරීමේ අඩවි මගින් YouTube වීඩියෝ හරහා බෙදා ගන්නා ලද වීඩියෝ ක්‍රීඩා ඇතුළුව බාගතකිරීම්
- **සමාජ මාධ්‍ය දැන්වීම් සහ පළ කිරීම්:** බොරු වෙස්ගත් ද්වේශසහගත මෘදුකාංග ගොනු වෙත ඉලක්ක යොමු කිරීම
- **ද්වේශසහගත මෘදුකාංග යාවත්කාලීන කිරීම්:** සාමාන්‍යයෙන් වෙබ් බ්‍රවුසර් යාවත්කාලීන කිරීම් ලෙස බොරු වෙස් ගන්නා ලද

අධ්‍යර 3: දත්ත රැස් කිරීම

තොරතුරු සොරකම් කරන්නෙකු විසින්දිතයාගේ උපාංගය ක්‍රියාත්මක කළ පසු, එය අවදානමට ලක් වූ යන්ත්‍රයෙන් සංවේදී දත්ත රැස් කිරීමට පටන් ගනී. තොරතුරු සොරකම් කරන්නන් අවදානමට ලක් වූ පරිගණක ජාලයක කොටසක් වන අවස්ථාවන්හිදී පරිශීලක විශ්වාසනීය තොරතුරු සොරකම් කිරීමට අමතරව, සයිබර් අපරාධකරුවන්ට අමතර හැකියාවන් සක්‍රිය කිරීමට හෝ වෙනත් ද්වේශසහගත මෘදුකාංග ලබා දීමට වින්‍යාස විධාන යැවීමෙන් අවදානමට ලක් වූ උපාංගය දුරස්ථව පාලනය කළ හැකිය. සාමාන්‍යයෙන්, තොරතුරු සොරකම් කරන්නන්ට සොරකම් කළ හැකි දේ:

- පරිශීලක නම් සහ මුරපද, විශේෂයෙන් වෙබ් බ්‍රවුසර්වල බහු-සාධක සත්‍යාපන (MFA) පරිශීලක සැසි / ටෝකනවල ගබඩා කර ඇති ඒවා
- කුකීස් සහතික කිරීම
- වෙබ් බ්‍රවුසර ස්වයංක්‍රීය පුරවන ලද පෝරම තොරතුරු
- ඊමේල් විශ්වාසනීය තොරතුරු, අන්තර්ගතයන් සහ සම්බන්ධතා
- වෙබ් බ්‍රවුසින් ඉතිහාසය
- පරිශීලක ලේඛන
- ණයපත් විස්තර
- ඩෙස්ක්ටොප් පණිවිඩ යෙදුම් මගින් චැට් ලොග්ස්
- පද්ධති තොරතුරු
- ක්‍රිප්ටෝ මුදල් පසුම්බි
- VPN හෝ or File Transfer Protocol (ගොනු හුවමාරු ප්‍රොටෝකෝලය) (FTP) විශ්වාසනීය තොරතුරු.



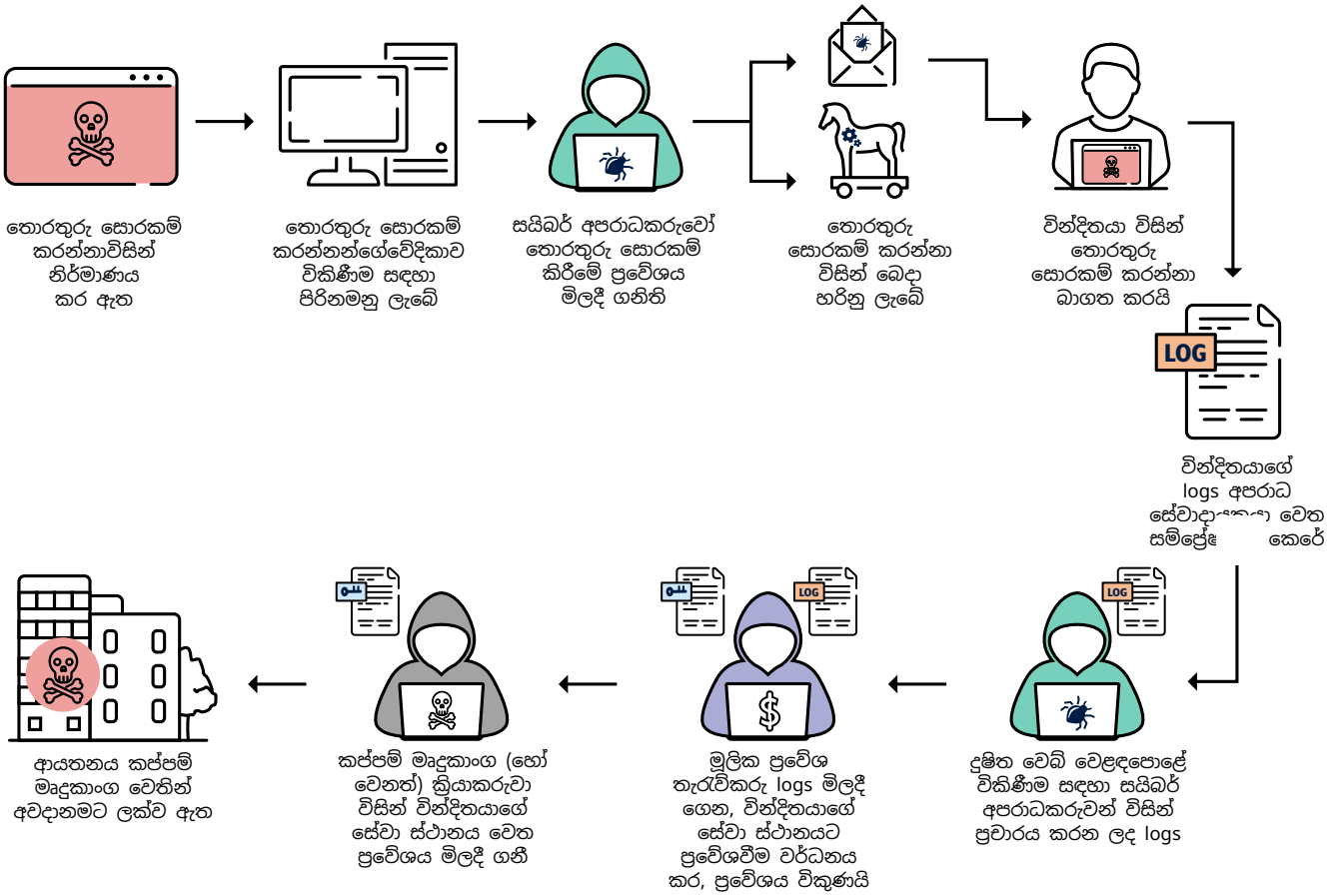
රූපසටහන 1. තොරතුරු සොරකම් කරන්නන්ගේ හැකියාව

සමහර වෙබ් බ්‍රව්සර් සහතික කරන කුකීස් මඟින් පරිශීලකයෙකු දින ගණනාවක් ගිණුමකට හෝ සේවාවකට ලොග් වී සිටීමට සලසන අතර එවිට පරිශීලකයින්ට නැවත සහතික කිරීමක් අවශ්‍ය නොවේ. සොරකම් කළහොත්, මෙම සහතික කරන ලද කුකීස් MFA අවශ්‍යතා ඵලදායී ලෙස මඟ හරවා, වින්දිත ගිණුම්, ආයතනික ජාල සහ ව්‍යවසාය පද්ධති වෙත සයිබර් අපරාධකරුවන්ට ප්‍රවේශය ලබා දිය හැකිය.

අධියර 4: දත්ත එක්රැස් කිරීම සහ මුදල් ඉපැයීම

සහ මුදල් ඉපැයීම තොරතුරු සොරකම් කරන්නන් වින්‍යාස කර ඇත්තේ ‘ logs’ ලෙස හඳුන්වන වින්දිතයාගේ තොරතුරු, ද්වේෂසහගත විධාන සහ පාලන සේවාදායකයන් වෙත මුදා හැරීමය. සාමාන්‍යයෙන්, තොරතුරු සොරකම් කරන්නෝ logs ගොදුරක් සයිබර් අපරාධකරුවන් සමඟ බෙදා ගැනීමට ටෙලිග්‍රෑම් සහ ඩිස්කෝඩ් වැනි ජනප්‍රිය පණිවිඩ යෙදුම් උපයෝගිකර ගනිති. Logs විකිණීම සහ වෙළඳාම සඳහා ටෙලිග්‍රෑම් සහ දුෂිත වෙබ් හරහා විශේෂිත වෙළඳපොළවල් පවතී. සයිබර් අපරාධකරුවෝ විවිධ ආකාරවලින් logs මගින් මුදල් උපයති. ඒවා අතරට ඇතුළත් වන්නේ:

- ආරම්භක ප්‍රවේශ තැරැව්කරුවන් ඇතුළු අපරාධ වෙළඳපොළවල logs විකිණීම
- අනන්‍යතා සොරකම් කිරීම සහ කප්පම් ගැනීම හරහා වින්දිතයාව සෘජුවම අයුතු ලෙස ප්‍රයෝජනයට ගැනීම
- කප්පම් මෘදුකාංග ක්‍රියාකාරකම් සඳහා ආයතනික ජාල වෙත මූලික ප්‍රවේශය ලබා ගැනීමට තොරතුරු උපයෝගී කර ගැනීම.



රූපසටහන 2. තොරතුරු සොරකම් කිරීමේ පරිසර පද්ධතිය සහ සංවිධානයකට ඇති විය හැකි බලපෑම

අනුමිති

තොරතුරු සොරකම් කරන්නන්ට පුද්ගලයන් සහ සංවිධාන වෙත දැඩි බලපෑම් ඇති කළ හැකිය. තොරතුරු සොරකම් කරන්නන් පරිශීලක විශ්වාසනීය තොරතුරු රැස් කරන විට, සයිබර් අපරාධකරුවන් වලංගු පරිශීලක ගිණුම් සහිත ආයතනික ජාල හෝ ව්‍යවසාය පද්ධති වෙත ප්‍රවේශ වීමට මෙම පරිශීලක විශ්වාසනීය තොරතුරු භාවිතා කළ හැකි අතර, බොහෝ විට පද්ධති හිමිකරුවන් විසින් එය සොයා ගැනීම ප්‍රමාද වේ.

තොරතුරු සොරකම් කරන්නන්ගේ බලපෑමට ලක් වූ **සංවිධාන** සඳහා, ප්‍රතිවිපාකවලට ඇතුළත් විය හැක්කේ:

- කප්පම් මෘදුකාංග
- දත්ත උල්ලංඝනය කිරීම
- ව්‍යාපාරික විද්‍යුත් තැපැල් අවදානමට ලක් වීම
- බුද්ධිමය දේපළ සොරකම් කිරීම
- සංවේදී තොරතුරු සොරකම් කිරීම.

තොරතුරු සොරකම් කරන්නන්ගෙන් බලපෑමට ලක් වූ **පුද්ගලයෙකු** සඳහා, ප්‍රතිවිපාකවලට ඇතුළත් විය හැක්කේ:

- පුද්ගලික ඊමේල් හෝ සමාජ මාධ්‍ය ගිණුම් වෙත අනවසරයෙන් පිවිසීම
- අනන්‍යතා සොරකම් කිරීමේ අවදානම වැඩි වීම
- වංචනිකව සිදු කෙරෙන ප්‍රහාරවල අවදානම වැඩි වීම
- මූල්‍ය අලාභය හෝ මූල්‍ය ගිණුම් වෙත අනවසරයෙන් ප්‍රවේශවීම
- පුද්ගලිකත්වය අහිමි වීම.

ප්‍රත්‍යෙක අධ්‍යයනය

මෙම ප්‍රත්‍යෙක අධ්‍යයනය ජනතාව අතර ප්‍රචාරණය සක්‍රීය කිරීම සඳහා නිර්නාමික කර ඇත. එය ASD හි ACSC වෙත වාර්තා කර ඇති ඔස්ට්‍රේලියානු ආයතනවලට බලපා ඇති බහුවිධ සයිබර් ආරක්ෂණ සිදුවීම් මත පදනම් වේ. මින් පසුව, බලපෑමට ලක් වූ ආයතනය 'සංවිධානය' ලෙස හැඳින්වේ. මෙම ප්‍රත්‍යෙක අධ්‍යයනයට අදාළ පුද්ගලයින්ගේ නම් මනඃකල්පිත වන අතර විඳිතයින්ගේ අනන්‍යතාවය ආරක්ෂා කිරීම සඳහා විස්තර ඉවත් කර ඇත.

මෙම සංවිධානය ඔස්ට්‍රේලියානු ව්‍යාපාරයක් වන අතර එහි කාර්ය මණ්ඩලයට තම පුද්ගලික උපාංගවලින් ආයතනික පද්ධති වෙත ප්‍රවේශ වීමට ඉඩ සලසයි. ඇලිස් යනු දුරස්ථව සේවය කරන සංවිධානයේ සේවිකාවකි. නිවසේ සිට වැඩ කරන විට, ඇලිස් ඇගේ පුද්ගලික ලැප්ටොප් පරිගණකය භාවිතයෙන් දුරස්ථව ඇගේ සංවිධානයේ ආයතනික ජාලයට ප්‍රවේශ වේ. ඇලිස් විසින් ඇය නීත්‍යානුකූල යැයි විශ්වාස කළ වෙබ් අඩවියකින් Notepad++ (එය සටහන් ගැනීමේ මෘදුකාංග වර්ගයකි) අනුවාදයක් ඇගේ **පුද්ගලික ලැප්ටොප් පරිගණකයට** බාගත කළේය. **තොරතුරු සොරකම් කරන්නෙකු** Notepad++ මෘදුකාංගය ස්ථාපනය කරන්නා ලෙස වෙස්වලා ගෙන ඇත. මෘදුකාංගය ස්ථාපනය කිරීමට ඇලිස් උත්සාහ කළ විට, තොරතුරු සොරකම් කරන්නා ක්‍රියාත්මක වී ඇගේ ලැප්ටොප් පරිගණකයෙන් **පරිශීලක විශ්වාසනීය ලබා ගැනීමට** පටන් ගත්තේය. මෙයට ඇය විසින් ඇයගේ වෙබ් බ්‍රවුසරයේ සුරකින ලද පිවිසුම් තොරතුරු වන අයගේ රාජකාරී පරිශීලක නාමය සහ මුරපදය ඇතුළත් විය. තොරතුරු සොරකම් කරන්නා පසුව එම පරිශීලක විශ්වාසනීය තොරතුරු සයිබර් අපරාධ කණ්ඩායමක් විසින් පාලනය කරන ලද දුරස්ථ විධාන සහ පාලන සේවාදායකයකට යැවිවේය. සොරකම් කරන ලද logs වෙනත් දේවල් සමඟ ඇසුරුම් කර **පසුව දුෂ්ට වෙබ් වෙළඳපොළක් හරහා සයිබර් අපරාධකරුවන්ට විකුණුවේය**. බොබ් නැමති සයිබර් අපරාධකරුවෙක් ඇලිස්ගේ පරිශීලක විශ්වාසනීය තොරතුරු මිලදී ගත් අතර, ඇගේ සංවිධානයේ ජාලයේ සේවාවන් සඳහා පරිශීලක විශ්වාසනීය තොරතුරු හඳුනා ගත්තේය. ඇලිස්ගේ සංවිධානය මෙම සේවාවන් සඳහා **MFA වින්‍යාස කර නොතිබුණි**. එයින් අදහස් කළේ ආයතනික ජාලය වෙත සාර්ථකව **සත්‍යාපනය කිරීමට සහ ප්‍රවේශ වීමට** බොබිට සොරකම් කරන ලද පරිශීලක විශ්වාසනීය තොරතුරු පමණක් භාවිතා කළ හැකි බවයි සොරකම් කරන ලද **වලංගු පරිශීලක විශ්වාසනීය තොරතුරු** භාවිතා කරමින් බොබ් ඇලිස්ගේ සංවිධානයේ ආයතනික ජාලයට සොයාගැනීමට නොහැකි වන පරිදි ප්‍රවේශ විය. සංවිධානයට අයත් සංවේදී දත්ත හඳුනාගෙන සමාගමෙන් කප්පම් ගැනීම සඳහා ඒවා මුදා හැරීමෙන් ආයතනික ජාලය හරහා පාර්ශ්වීයව හැරවීමට බොබිට හැකි විය. සංවේදී දත්ත සොරකම් කිරීමෙන් පසු, බොබ් සංවිධානයේ **දත්ත සමුදායන් සහ ගොනු පද්ධති** ප්‍රවේශ විය නොහැකි වන පරිදි **සංකේතනය කළේය**.

ලිහිල් කිරීම්

තම ආයතනික ජාලයට සම්බන්ධ වන උපාංග, විශේෂයෙන් දුරස්ථව සේවය කරන සේවකයින් භාවිතා කරන පුද්ගලික උපාංග, මත පාලනයන් ක්‍රියාත්මක කිරීමට සංවිධානවලට නොහැකි විය හැකිය. පරිශීලක විශ්වාසනීය තොරතුරු ඉලක්ක කරගත් තොරතුරු සොරකම් කරන්නන්ගේ අවදානමෙන් ආරක්ෂා වීමට පාලන ක්‍රියාත්මක කිරීම කෙරෙහි අවධානය යොමු කරන ලෙස ASD හි ACSC සංවිධාන නිර්දේශ කරයි. මෙම ලිහිල් කිරීම්වලට ඇතුළත් වන්නේ:

කාර්ය මණ්ඩලයට සයිබර් ආරක්ෂණ දැනුවත් කිරීමේ පුහුණුවක් ලබා දීම

- කාර්ය මණ්ඩලයට ඵලදායී පුහුණුවක් ලබා දීමෙන් සාර්ථක ඉලක්කගත සමාජ ඉංජිනේරු විද්‍යාව සහ ද්වේෂසහගතව ගොනු බාගත් කිරීම් වැළැක්වීම.
- තොරතුරු සොරකම් කරන්නන්, ඔවුන්ගේ බෙදාහැරීමේ ක්‍රම සහ ඔබේ සංවිධානයට ඇති වංචනිකව සිදු කෙරෙන තර්ජන පිළිබඳව දැනුවත්භාවය වැඩි කිරීම.

ආයතනික ගිණුම් සුරක්ෂිත කරන්න

- MFA ක්‍රියාත්මක කිරීම:
- බාහිර සහ අභ්‍යන්තර සේවා, පද්ධති සහ සංවේදී දත්ත ගබඩාවන් හරහා, විශේෂයෙන් වෙබ්මේල්, VPN සහ තීරණාත්මක පද්ධති වෙත ප්‍රවේශ වන වරප්‍රසාද ලත් පරිශීලක ගිණුම් සඳහා, MFA ක්‍රියාත්මක කරන්න. හොඳම පිළිවෙත වන්නේ සියලුම ගිණුම් මත වංචනිකව යවන දේවල් වලට ප්‍රතිරෝධය දක්වන MFA ක්‍රියාත්මක කිරීම ය.
- පරිශීලක ගිණුම් තවදුරටත් අවශ්‍ය නොවන විටඒවා අක්‍රීය කරන්න.
- පරිපාලක වරප්‍රසාද සීමා කරන්න:
- අගුළු දමා ඇති කැපවීමෙන් ක්‍රියා කරන වැඩපොළක පමණක් (එනම් ආරක්ෂිත පරිපාලක වැඩපොළක්) භාවිතා කරමින් ජාල පරිපාලනය සහ අනෙකුත් වරප්‍රසාද ලත් කාර්යයන් සිදු කරන්න.
- පද්ධති කළමනාකරණය සඳහා වරප්‍රසාද ලත් පරිශීලක ගිණුම් සහ පරිපාලන නොවන කාර්යයන් සඳහා සම්මත පරිශීලක ගිණුම් භාවිතා කරන ලෙස පරිපාලකයින්ගෙන් ඉල්ලා සිටීම මගින් අවම වරප්‍රසාද ලත් හොඳම පිළිවෙත අනුගමනය කරන්න.
- වරප්‍රසාද ලත් පරිශීලක ගිණුම් (මාර්ගගත සේවාවන් වෙත ප්‍රවේශ වීමට පැහැදිලිවම අවසර දී ඇති ඒවා හැර) අන්තර්ජාලය, ඊමේල් සහ වෙබ් සේවා වෙත ප්‍රවේශ වීම වළක්වන්න.
- පද්ධති සහ යෙදුම් සඳහා කාලෝචිත පරිපාලනය ක්‍රියාත්මක කිරීම සලකා බලන්න.
- වරප්‍රසාද ලත් පරිශීලක ගිණුම් සඳහා කළමනාකරණය සහ විගණනය ක්‍රියාත්මක කරන්න.
- මුරපද, විශේෂයෙන් බාහිර මුහුණත දුරස්ථ ප්‍රවේශ ගිණුම් සඳහා, විටින් විට යාවත්කාලීන කරන්න.
- සැසි ටෝකන සහ කුකීස් සඳහා ආයු කාලය අවසන් වන සහ නිශ්චිත දිනයකට පසු ස්වයංක්‍රීයව අවසන් වන ප්‍රතිපත්ති බලාත්මක කරන්න.

ව්‍යවසාය සංචලතාව දැඩි කරන්න

- ව්‍යවසාය සංචලතා අවදානම් තක්සේරුවක් සිදු කර ව්‍යවසාය සංචලතා දැඩි කිරීමේ මාර්ගෝපදේශ ක්‍රියාත්මක කරන්න.
- ආයතනිකව කළමනාකරණය කරන ලද උපාංග කළමනාකරණය නොකළ පුද්ගලික උපාංගවලට වඩා ආරක්ෂිත බැවින්, ඔබ සේවකයින්ට ඔවුන්ගේ වැඩ සඳහා පුද්ගලික උපාංග භාවිතා කිරීමට ඉඩ දෙන්නේ නම්, ඔබේම උපාංගය ගෙන ඒමේ (BYOD) ප්‍රතිපත්තියක් ක්‍රියාත්මක කරන්න.

Software-as-a-Service (Saas) විකුණුම්කරුවන් සහ කළමනාකරණය කරන ලද සේවා සපයන්නන් ඇතුළුව, ඔබේ ජාල වෙත විකුණුම්කරුවන් ප්‍රවේශ වීමෙන් ඇතිවන සැපයුම් දාම අවදානම් සමාලෝචනය කර තක්සේරු කරන්න.

කළමනාකරණය කරන ලද සේවා සපයන්නෙකු සම්බන්ධ කර ගැනීමේදී ඔබේ ආරක්ෂාව කළමනාකරණය කරන්නේ කෙසේද.

ඔබේ ආයතනික ජාලය ආරක්ෂා කර ගන්න

- යෙදුම් සහ මෙහෙයුම් පද්ධති යාවත්කාලීනව තබා ගන්න.
- දැඩි අවසර ලැයිස්තුවක් සමඟ යෙදුම් පාලනය බලාත්මක කිරීමට දේශීය ආරක්ෂක ප්‍රතිපත්ති යොදන්න.
- කාර්යභාරය සහ ක්‍රියාකාරීත්වය මත පදනම්ව ජාල කොටස් වෙන් කිරීම සඳහා ජාල කොටස් කිරීම ක්‍රියාත්මක කරන්න.
- පරිශීලක ක්‍රියාකාරකම්, විශේෂයෙන් දුරස්ථ සේවකයින් සඳහා, විගණනය කර නිරීක්ෂණය කරන්න.
- වරප්‍රසාද ලත් ගිණුම් අධීක්ෂණය කිරීමෙන් බාහිර ජාලයකට දත්ත විශාල ප්‍රමාණයක් උඩුගත කිරීම වැනි සංවේදී දත්ත වලට අනවසර ප්‍රවේශයක් හෝ අසාමාන්‍ය දත්ත හුවමාරු ක්‍රියාකාරකම් අනාවරණය කරගත හැකිය.
- අනවසර දත්ත හුවමාරු වැළැක්වීම සඳහා දත්ත අලාභ වැළැක්වීමේ ප්‍රතිපත්ති සහ මෙවලම් ක්‍රියාත්මක කරන්න.

ASD සයිබර් ආරක්ෂක ජාල හවුල්කරුවෙකු වී ASD හි සයිබර් තර්ජන බුද්ධි බෙදාගැනීමේ (CTIS) සේවාවට සම්බන්ධ වන්න

- CTIS යනු රජයේ සහ කර්මාන්ත හවුල්කරුවන්ට ද්වේෂසහගත සයිබර් ක්‍රියාකාරකම් පිළිබඳ තොරතුරු ලබා ගැනීමට සහ බෙදා ගැනීමට හැකි ද්විත්ව-මාර්ග බෙදාගැනීමේ වේදිකාවකි.
- ASD හි ACSC තොරතුරු සොරකම් කරන්නන්ගේ ක්‍රියාකාරකම් ගැන සොයා බලන අතර CTIS වේදිකාව හරහා ක්‍රියාකාරී විධාන සහ පාලන යටිතල පහසුකම් පිළිබඳ විස්තර බෙදා ගනී.
- හවුල්කරුවෙකු වීමට සහ ඔබේ සංවිධානය සහ පාරිභෝගික දත්ත සයිබර් අපරාධ තර්ජන වලින් ආරක්ෂා කිරීමට ලියාපදිංචි වන්න.

අවදානමට ලක් කිරීමක් සඳහා සූදානම් වන්න

- තොරතුරු සොරා ගැනීමේ අවදානමට ලක් කිරීමක් සිදු වුවහොත්, භාවිතා කිරීම සඳහා සයිබර් ආරක්ෂක සිදුවීම් ප්‍රතිචාර සැලැස්මක් සකස් කරන්න.සැක සහිත ගොනුවක් බාගත කර ඇති බවට සේවකයන් සැක කරන්නේ නම්, ඔවුන් විසින් කුමක් කළ යුතුද සහ කා සම්බන්ධ කර ගත යුතුද යන්න පිළිබඳව ඔවුන් දැනුවත් බව සහතික කර ගන්න.

ASD හි ACSC හි Essential Eight (අත්‍යවශ්‍ය දේවල් අට) ක්‍රියාත්මක කරන්න

- ඉහත සඳහන් කළ ලිහිල් කිරීම් වලට අමතරව, ASD හි ACSC හි අත්‍යවශ්‍යදේවල් අට හි ඉතිරි කොටස ක්‍රියාත්මක කිරීමට ASD හි ACSC දැඩි ලෙස නිර්දේශ කරයි.

දුරස්ථව වැඩ කරන විට ඔබේ සේවකයින්ට උපදෙස් ලබා දෙන්න

- ඔබගේ පුද්ගලික උපාංගවල ඔබගේ තොරතුරු ආරක්ෂා කර ගන්න
  - හොඳ සයිබර් හිතකර අවකාශයක් වර්ධනය කරගෙන සැක සහිත සබැඳි හෝ උත්පතන මත ක්ලික් නොකරන්න. නැතහොත් නොදන්නා හෝ විශ්වාස කළ නොහැකි මූලාශ්‍රවලින් ගොනු හෝ මෘදුකාංග බාගන්න එපා.
  - රාජකාරී සහ පුද්ගලික ගිණුම් සඳහා වෙනස් මුරපද භාවිතා කරන්න. හැකි සෑම තැනකම පුද්ගලික ගිණුම් සඳහා MFA භාවිතා කරන්න.
  - ඔබේ සේවායෝජකයා විසින් පැහැදිලිව අනුමත නොකළහොත් ඔබේ සේවා අක්තපත්‍ර පුද්ගලික මුරපද කළමනාකරුවෙකු තුළ ගබඩා නොකරන්න. මෙයට ඔබේ වෙබ් බ්‍රව්සරයේ මුරපද කළමනාකරු ඇතුළත් වේ. **සැකයක් ඇත්නම්, ආයතනිකව සහාය දක්වන මුරපද කළමනාකරුවෙකු ලබා දෙන ලෙස ඔබේ සේවායෝජකයාගෙන් ඉල්ලා සිටින්න.**
  - බෙදාගත් හෝ පොදු වැඩපොළවල් වලින් ඔබේ සේවා ගිණුම් වෙත ප්‍රවේශ නොවන්න.
  - ඔබගේ වෙබ් බ්‍රවුසරයේ ස්වයංක්‍රීය පිරවුම් විශේෂාංගයේ ගබඩා කර ඇති දේ පිළිබඳව දැනුවත් වන්න.තොරතුරු සොරකම් කරන්නන් බ්‍රවුසර ස්වයංක්‍රීයව පෝරම පිරවීම සඳහා සුරකින දත්ත ඉලක්ක කරයි. වෙබ් පෝරම පුරවන විට, ඔබේ වෙබ් බ්‍රවුසරයේ ස්වයංක්‍රීය පිරවුම් විශේෂාංගය සුරැකීමට වඩා, ක්‍රෙඩිට් කාඩ් අංක වැනි සංවේදී දත්ත අතින් ඇතුළත් කිරීම සලකා බලන්න.
  - තොරතුරු සොරකම් කරන්නන්ට ලබා ගත හැකි තොරතුරු අඩු කිරීම සඳහා බ්‍රවුසින් සැසියක් අවසන් කිරීමෙන් පසු සියලුම මාර්ගගත සේවාවන්ගෙන් ඉවත් වී වෙබ් බ්‍රවුසර කුකීස් ඉවත් කරන්න.
  - ඔබගේ මෙහෙයුම් පද්ධතියේ බිල්ට්-ඉන් ප්‍රති-වයිරස විසඳුම සක්‍රීය කර ඇති බවට වග බලා ගන්න. ඔබ තෙවන පාර්ශවීය ප්‍රති-වයිරස විසඳුමක් භාවිතා කරන්නේ නම්, එය යාවත්කාලීනව තබා ඇති බවත් කීර්තිමත් විකුනුම්කරුවෙකුගෙන් බවත් සහතික කර ගන්න.

සහාය

තොරතුරු සොරා ගැනීමේ අවදානමට ලක් කිරීමක් සම්බන්ධයෙන් බලපෑමට ලක්ව ඇති හෝ සහාය අවශ්‍ය ඔස්ට්‍රේලියානු සංවිධානවලට **1300 CYBER1 (1300 292 371)** හරහා හෝ cyber.gov.au/report හි වාර්තාවක් ඉදිරිපත් කිරීමෙන් ASD හි ACSC සම්බන්ධ කර ගත හැකිය.

ASD හි ACSC ආයතනයන්, යම් සිදුවීමක් සීමා කර ඇති බව සලකනු ලැබුවද, සැක සහිත ජාල ක්‍රියාකාරකම් සහ තොරතුරු සොරකම් කරන්නන් හා සම්බන්ධ අවදානමට ලක් වන දර්ශක වාර්තා කිරීමට දිරිමත් කරයි. සයිබර් තර්ජන ක්‍රියාකාරීන්ගේ උපක්‍රම, ශිල්පීය ක්‍රම සහ ක්‍රියා පටිපාටි පිළිබඳ අපගේ අවබෝධය වැඩිදියුණු කිරීම සඳහා ඔබ සපයන තොරතුරු අපි භාවිතා කරන අතර, එමඟින් එකම ආකාරයකින් ඉලක්ක කර ඇති අනෙකුත් ඔස්ට්‍රේලියානු සංවිධානවලට අනතුරු ඇඟවීමට අපට උපකාරී වේ.

හිමිකම් අත්හැරීම

මෙම මාර්ගෝපදේශයේ ඇති තොරතුරු සාමාන්‍ය ස්වභාවයක් ගන්නා අතර එය නීති උපදෙසක් ලෙස හෝ කිසියම් විශේෂිත අවස්ථාවකදී හෝ හදිසි අවස්ථාවකදී සහාය සඳහා විශ්වසනීය දෙයක් ලෙස නොසැලකිය යුතුය. ඕනෑම වැදගත් කාරණයකදී, ඔබ ඔබේම තත්වයන් සම්බන්ධව සුදුසු ස්වාධීන වෘත්තීය උපදෙස් ලබා ගත යුතුය.

මෙම මාර්ගෝපදේශයේ අඩංගු කරුණු මත විශ්වාසය තැබීමේ ප්‍රතිඵලයක් ලෙස සිදුවන ඕනෑම හානියක්, අලාභයක් හෝ වියදමක් සඳහා මධ්‍යම රජය කිසිදු වගකීමක් හෝ වගකීමක් භාර නොගනී.

වැඩි විස්තර සඳහා, හෝ සයිබර් ආරක්ෂණ සිදුවීමක් වාර්තා කිරීමට, අපව අමතන්න:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ඔස්ට්‍රේලියාව ඇතුලත පමණක් මෙම අංකය භාවිතා කිරීමේ හැකියාව පවතී.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre