“Bulletproof” හොස්ටින් සේවා සපයන්නන්: සයිබර් අපරාධ යටිතල ව්‍යුහවලින් සන්නද්ධ අවකාශය තුළට ප්‍රවේශවීම

සාර්ථක සයිබර් අපරාධකරුවන් විශ්වාසය තබන්නේ ආරක්ෂිත, හඳුනාගත නොහැකි සහ ප්‍රත්‍යාස්ථ යටිතල ව්‍යුහ මතය. නෙට්වර්ක් තුලට නීතිවිරෝධීව පිවිසීම, විශ්වාසනීය දේ සොරා ගැනීම, රැන්සම්වෙයාර්, හෝ නීතිවිරෝධී සංසදවල දත්ත සොරකම් කිරීම යන සෑම අවස්ථාවක් පිටුපසම, සයිබර් අපරාධකරුවන් හට සැඟවී සිට ක්‍රියාත්මක විය හැකි ආරක්ෂිත යටිතල ව්‍යුහයක් ඇත.

කෙසේවුවද, සයිබර් අපරාධකරුවන් හට අනාවරණය කරගත නොහැකිව සහ සොයාගැනීමට අපසසුව සිටීම, ක්‍රමිකව වැඩිවන අභියෝගයකි. රාජ්‍යයන්, නීති ක්‍රියාත්මක කරන්නන්, සහ පුද්ගලික අංශය අතර ගෝලීයව සිදුවන සහයෝගීතාවය හේතුවෙන් තවදුරටත් ඔවුන්ට මාර්ගගතව නිර්ණාමිකව සිටීම අපහසුවී ඇත. තවද, තමා සතුවම තිබෙන ආරක්ෂිත යටිතල ව්‍යුහ පවත්වාගෙන යා හැකි නිපුණතාවය සහ විශේෂඥතාවය ඇත්තේ ඉතාම සුළු සයිබර් අපරාධකරුවන් හට පමණි. එම හේතුවෙන්, ඔවුන් වෙනුවෙන් මෙම සේවය සැපයිය හැකි නීතිවිරෝධී යටිතල ව්‍යුහ සපයන්නන් ඔවුන් සොයන අතර, ඒ මගින් සයිබර් අපරාධකරුවන් හට වින්දිතයන් සහ ලාභ වෙත සිය අවධානය යොමු කල හැකිය.

‘සේවාවක්-වශයෙන්-සයිබර්-අපරාධ’ (‘Cybercrime-as-a-service’) යනුවෙන් හැඳින්වෙන්නේ විවිධාකාර ද්වේෂසහගත සයිබර් ක්‍රියාකරුවන් හට උපකාර කිරීම සඳහා වර්ධනය කර ඇති ඇති පාතාල වෙළඳපොලකි. මෙම පාතාල වෙළඳපොල සමන්විත වී ඇත්තේ සයිබර් අපරාධකරුවන් හට මාර්ගගතව වින්දිතයන් ඉලක්ක කිරීමට උපකාර වන නිරන්තරයෙන් වැඩිවන සහ විකාශනයවන විවිධාකාර මිලට ගත හැකි මෙවලම්, සේවා සහ තොරතුරුවලින්. සයිබර් අපරාධකරුවන් විය හැකි අයට නෙට්වර්ක් වෙත ප්‍රවේශය මිලට ගැනීම, ආරක්ෂිත විධිවිධාන මඟ හැරීමට උපකාර වන මෙවලම් මෙන්ම වින්දිතයන්ට එරෙහිව භාවිතා කිරීමට මැල්වෙයාර් මිලට ගැනීම සහ පුද්ගලික තොරතුරු සොරකම් කිරීමද කල හැකිය. Bulletproof හොස්ටින් (BPH) සපයන්නන් මෙම පරිසර පද්ධතියේ කොටසක් වන අතර සයිබර් අපරාධකරුවන් හට ආරක්ෂිත යටිතල ව්‍යුහ ලබාදේ. වැදගත් කරුණ වන්නේ එක් BPH සැපයුම්කරුවෙකු විසින් ගෝලීයව වින්දිතයන් සිය ගණනක් කෙලින්ම ඉලක්ක කිරීමට සයිබර් අපරාධකරුවන් හට අවස්ථාව සලසා දීමයි.

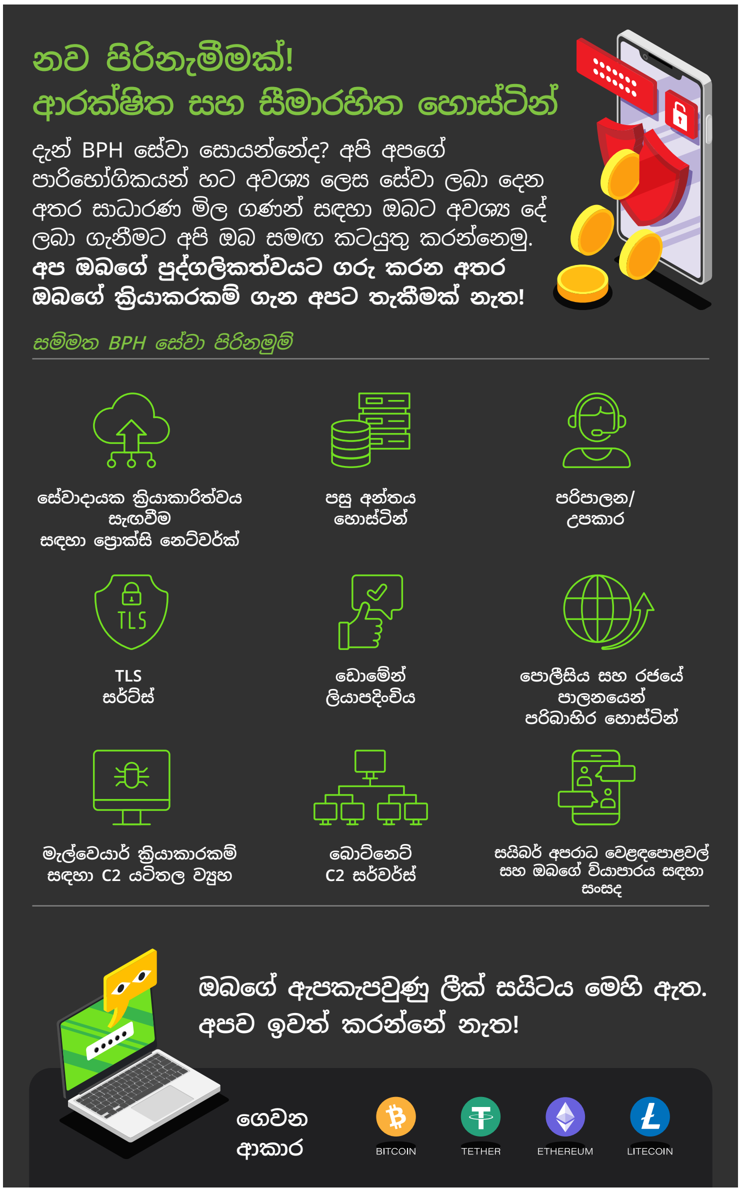
“Bulletproof” හොස්ටින් සපයන්නෙකු යන්නෙන් අදහස් වන්නේ කුමක්ද?

සරලව පැවසුවහොත්, සයිබර් අපරාධකරුවන් හට සත්‍යව පෙනී සිටින ලෙස සහ/හෝ භෞතිකව ක්‍රියාත්මක වීමට අවශ්‍ය යටිතල ව්‍යුහ BPH සපයන්නන් විසින් කුලියට ලබාදේ. BPH සපයන්නන් යනු විශේෂිත වර්ගයේ යටිතල ව්‍යුහ සේවාවක් වන අතර එමගින් ද්වේෂසහගත ක්‍රියාකරුවන් (සයිබර් අපරාධකරුවන් ඇතුළු) හට නීතිවිරෝධී දේ දැරීමට සහ අන්තර්ජාලයේ මෙහෙයුම් ක්‍රියාත්මක කිරීමට ඉඩකඩ සලසයි.

“Bulletproof” යන නාමය හුදු අළෙවි මෙවලමකි. සත්‍ය වශයෙන්, මෙම සේවාවන්ද වෙනත් යටිතල ව්‍යුහ සපයන්නන් මෙන්ම බාධාවීම්වලට භාජනය විය හැකිය. ඒ වෙනුවට, BPH සපයන්නන් නීති බලාත්මක කිරීම් වලට සහ වෙනත් අන්තර්ගත ඉවත් කිරීමට කරන ඉල්ලීම් ප්‍රතික්ෂේප කරන අතර වින්දිතයන් කරන අපචාර සම්බන්ධ පැමිණිලි සහ ග්‍රාහක ඉල්ලීම් දැන්වීම් නොසලකයි. මෙයින් අදහස් වන්නේ සයිබර් අපරාධකරුවන් හට සන්නිවේදනය කිරීම, නීතිවිරෝධී සංසද සහ වෙබ් අඩවි පවත්වා ගැනීම, මැල්වෙයාර් සහ ෆිෂිංග් කැම්පේන් (පුද්ගලික තොරතුරු සොරකම් කිරීම සඳහා ක්‍රියාත්මක වීම), සහ නීතිය ක්‍රියාත්මක කරන බලධාරීන් හෝ වෙනත් අයගේ ඉල්ලීම් හේතුවෙන් මෙහෙයවන්නාගේ බලපත්‍රය අවසානයට පත්වේය යන බියෙන් තොරව මුදල් විශුද්ධිකරණය කිරීම කළ හැකි බවයි.

BPH සපයන්නන් දැනුවත්වම සයිබර් අපරාධ පරිසර පද්ධතියේ සහභාගි වන අතර දරුණු ආකාරයේ මුදල් පදනම් වූ අරමුණු සහිත සයිබර් අපරාධවලට සහාය ලබාදෙයි. අපරාධකරුවන් විසින් BPH සපයන්නන්ට බලපෑම් කිරීමේ ප්‍රතිඵලයක් වශයෙන් ඕස්ට්‍රේලියානු සංවිධාන සහ ඒවායේ පාරිභෝගිකයන් හට බලපාන ප්‍රධාන ආකාරයේ සයිබර් අපරාධ සිදුවී ඇත. මෙම සිදුවීම්වල ප්‍රතිවිපාක අතර විනාශකාරී රැන්සම්වෙයාර් (පරිගනකයට ප්‍රවේශවීම වලක්වන මෘදුකාංග) ප්‍රහාර, දත්ත විකෘතිවීම් සහ සංවේදී තොරතුරු සොරකම් කිරීම් ඇතුළත් වේ.

පාතාල සංසදයන් තුළ bulletproof hosting සපයනන් පිළිබඳ වෙළඳ දැන්වීම්වල නියෝජනයක්:

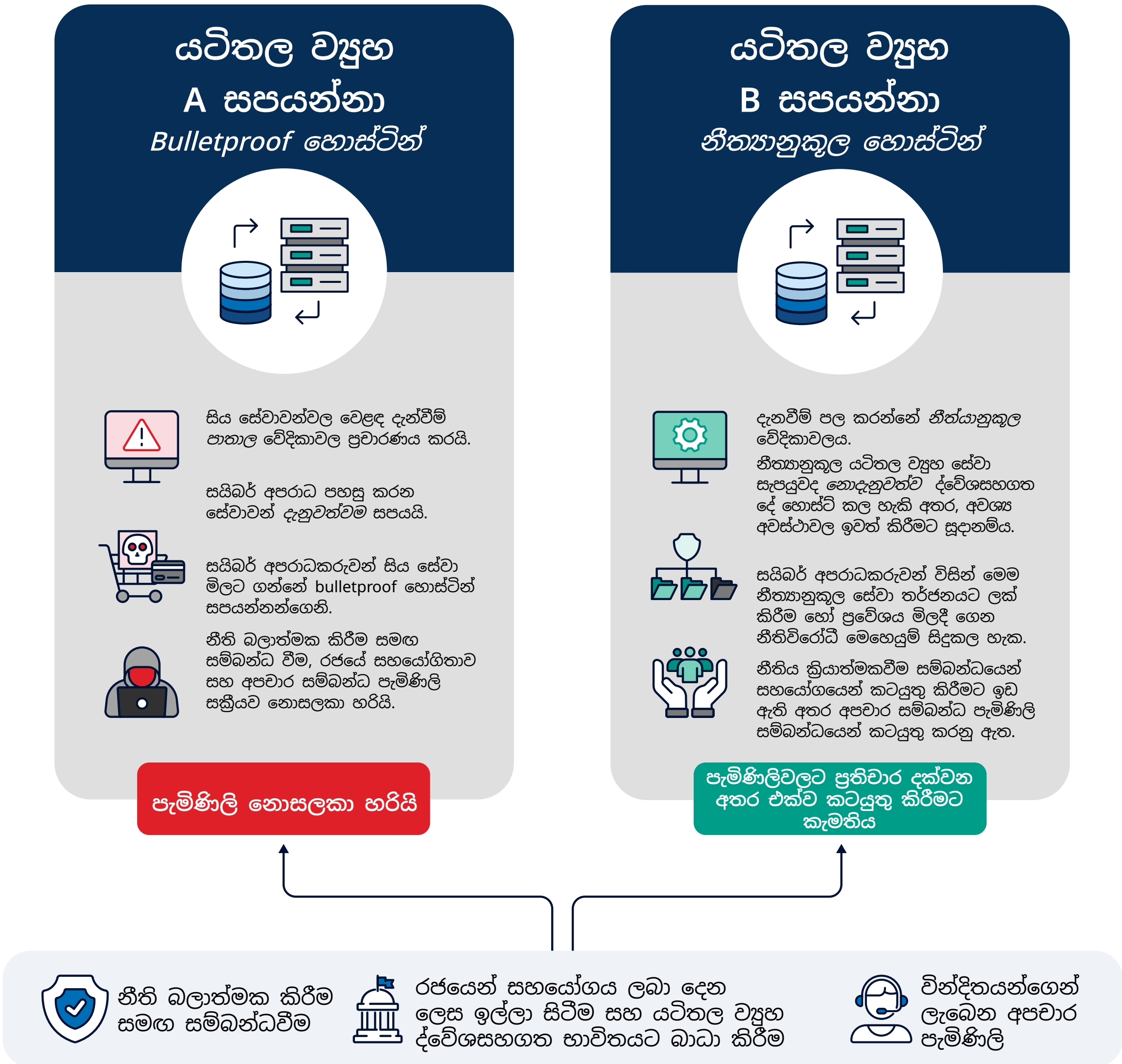


BPH සපයන්නන් ක්‍රියාත්මක වන ආකාරය කෙසේද?

BPH සපයන්නන් අනුව ව්‍යාපාර ආකෘතිය වෙනස් වේ. වඩාත්ම බහුල ක්‍රමය වන්නේ සයිබර් අපරාධකරුවන් හට IP ලිපින කුලියට දීම සහ ඔවුන්ගේ පිහිටි ස්ථාන, අනන්‍යතාව සහ ක්‍රියාකාරිත්වයන් අපැහැදිලි කිරීමට උපකාර වන සංකීර්ණ ලෙස ජාලයන් මාරු කිරීමේ ක්‍රම භාවිතා කිරීම වේ. බොහෝ අවස්ථාවලදී, BPH සපයන්නන් විසින් නීත්‍යානුකූල හොස්ටින් සේවා සපයනන්නන්ගෙන්, දත්ත මධ්‍යස්ථාන හෝ අන්තර්ජාල සේවා සපයනන්ගෙන් (ISPs) ලබා ගන්නා ලිපිනයන් සහ සේවාවන් නැවත අළෙවි කරයි. මෙම 'upstream' සපයන්නන් තමා විසින් යටිතල ව්‍යුහ සේවා ලබා දෙන්නේ BPH සපයන්නන් විසින් 'downstream' සේවා සපයන සයිබර් අපරාධකරුවන් හට බව නොදන්නවා විය හැකිය.

BPH සපයන්නන් විසින් සිය නෙට්වර්ක් සහ සිස්ටම් ආර්කිටෙක්චර් සිය පාරිභෝගිකයන් හඳුනා ගැනීම දුෂ්කර වන ආකාරයට හැඩගස්වා ගනී. උදාහරණයක් වශයෙන්, ඔවුන් විසින් පාරිභෝගිකගේ ක්‍රියාකාරකම සමඟ සම්බන්ධ අන්තර්ජාල මුහුණතට අදාල හඳුනා ගැනීම් - ඔවුන්ගේ IP ලිපිනයන් සහ ඩොමේන් නම් ආදිය, නිතර වෙනස් කරයි. මෙකී තාක්ෂණයන් මගින් ක්‍රියාකරුවෙකු හෝ පාරිභෝගිකයෙකු විසින් යම් අවස්ථාවක භාවිතා කරන IP ලිපිනයක් සමඟ යම් සිද්ධියක් සම්බන්ධ කිරීම දුෂ්කර කිරීම හේතුවෙන් පාරිභෝගිකයන් ආරක්ෂා කරන හෝ විමර්ශන කරන අයව අභියෝගයට ලක්වේ. තවද, BPH සපයන්නන් බොහෝ අවස්ථාවල භාවිතා කරන්නේ, ද්වේශසහගත සයිබර් ක්‍රියාකාරකම් විමර්ශනය කිරීම සහ වැළැක්වීම සඳහා විධිමත් ක්‍රමවේදයක් නොපවතින හෝ දැඩි නොවන සයිබර් පාලන තන්ත්‍රයන් ඇති රටවල යටිතල ව්‍යුහයන් වේ.

Bulletproof හොස්ටින් සපයන්නන් නීත්‍යානුකූල යටිතල ව්‍යුහ සපයන්නන්ගෙන් වෙනස් වන්නේ කෙසේද?



BPH සපයන්නන් ඉලක්ක කර ගැනීම මගින් සයිබර් අපරාධ තර්ජනයට බලපෑම් ඇති වන්නේ කෙසේද?

BPH සපයන්නන් මගින් නියෝජනය වන්නේ සිය ගණනක සිට දහස් ගණනක් දක්වා සයිබර් අපරාධකරුවන්ට එක්වර බාධා කිරීමට හැකි අගනා අවස්ථාවකි. සයිබර් අපරාධකරුවන් සහ වෙනත් ද්වේශසහගත ක්‍රියාකරුවන් විශාල සංඛ්‍යාවක් මෙම සේවා සිය අපරාධ වැරදි පහසු කර ගැනීමට භාවිතා කරයි - ඉවත් කර ගැනීමට කරන ඉල්ලීම් හෝ අපචාර පැමිණිලි ඉදිරියේ සිය ක්‍රියාකාරකම් හඳුනා ගත නොහැකි සහ ක්‍රියාත්මකව පවතින බවට ඇති විශ්වාසය මත.

කෙසේ වුවද, නීතිය බලාත්මක කරන්නන්, රජයේ ආයතන, සහ පුද්ගලික අංශය මෙම නීති විරෝධී යටිතල ව්‍යුහ සපයන්නන් ඉලක්ක කර ගැනීමට සහ ඔවුන්ට බාධා කිරීමට සහයෝගීව කටයුතු කරයි. මේවා අතර හඳුනාගත් BPH සපයන්නන්ගේ අන්තර්ජාල ගමනාගමනය සක්‍රියව අවහිර කිරීම වැනි ආරක්ෂණ ක්‍රියාකාරකම් අඩංගු වේ. මෙම ක්‍රියාකාරකම් මගින් ඕස්ට්‍රේලියානු සහ සම්බන්ධ ජාල අතර අන්තර්ක්‍රියා අඩු කිරීමට උපකාර වන අතර, නීත්‍යානුකූල ‘upstream’ යටිතල ව්‍යුහ සපයනන් සහ ISPs සයිබර් අපරාධකරුවන් හට ආරක්ෂිත අන්තජාල සහ සයිබර් අපරාධකරුවන් හට ආරක්ෂිත යටිතල ව්‍යුහ ලබාදීම මගින් නොදැනුවත්ව BPH සපයන්නන් හට පහසුකම් සලසන අයව ඇතුලත් කරයි.

මෙම පරිසර පද්ධතියේ සයිබර්-අපරාධ-සේවාවක් වශයෙන් යටිතල ව්‍යුහ සපයන එකම කාණ්ඩය BPH සපයන්නන් පමණක් නොවේ. මෙම සේවා දිගින් දිගටම පවතින අතර සයිබර් අපරාධ ක්‍රියාවලියන්ට සක්‍රියව උපකාර කිරීම සහ නීත්‍යානුකූල විමර්ශන සහ ප්‍රතිචාරවලට හිතාමතාම බාධා සිදු කිරීම මගින් ඕස්ට්‍රේලියාවට සයිබර් අපරාධ තර්ජනය ඇති කරයි. BPH සපයන්නන්ට එරෙහිව ක්‍රියාමාර්ග ගැනීම මගින් මෙම සේවාවල සහ මෙම සේවා භාවිතා කරන ද්වේශසහගත සයිබර් ක්‍රියාකාරීන්ගේ දුර්වලබව ඉස්මතු වේ.