සේවා ප්‍රතික්ෂේපනය කිරීමේ ප්‍රහාර සඳහා සූදානම් වීම සහ ඒවාට ප්‍රතිචාර දැක්වීම

පළමු වරට ප්‍රකාශයට පත් කළේ: සැප්තැම්බර් 2011
අවසාන වරට යාවත්කාලීන කළේ: මාර්තු 2025

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

හැඳින්වීම

අපගේ කලාපයේ සේවා ප්‍රතික්ෂේපනය කිරීමේ (DoS) ප්‍රහාරයන් වැඩිවීමේ ප්‍රවණතාවයට ප්‍රතිචාර වශයෙන්, නවසීලන්තයේ National Cyber Security Centre (NCSC-NZ) (ජාතික සයිබර් ආරක්ෂක මධ්‍යස්ථානය), Akamai Technologies Ltd සහ Cloudflare Pty Ltd සමඟ සහයෝගයෙන්යුතුව Australian Signals Directorate (ASD) (ඔස්ට්‍රේලියානු සංඥා අධ්‍යක්ෂ මණ්ඩලය) විසින් මෙම ප්‍රකාශනය වර්ධනය කරන ලදී. එය DoS ප්‍රහාරයන් සඳහා සූදානම් වීමට සහ ඒවාට ප්‍රතිචාර දැක්වීමට, සමකාලීන තර්ජන ශිල්පීය ක්‍රම මත පදනම් වූ හොඳම ප්‍රායෝගික සැහැල්ලු කිරීම් පිළිබඳව සංවිධානවලට මග පෙන්වීමක් ලබා දෙයි.

ASD හි *Internet of Things උපාංග* සහ *ඔබේ Wi-Fi සහ router සුරක්ෂිත කරන* ප්‍රකාශන සමඟ ඒකාබද්ධව මෙම උපදෙස් කියවන ලෙස අපි නිර්දේශ කරමු. මෙම ප්‍රකාශන මගින් අන් අයට බලපෑම් කළ හැකි DoS ප්‍රහාරවලට නොදැනුවත්ව දායක වීම වළක්වා ගැනීම සඳහා පුද්ගලයන්ට උපකාරී වේ.

DoS ප්‍රහාර යනු නීත්‍යානුකූල පරිශීලකයින්ට ප්‍රවේශය ප්‍රතික්ෂේපනය කිරීම සඳහා වෙබ් අඩවි, ඊමේල් සහ වසම් නාම පද්ධති (Domain Name System (DNS)) සේවා වැනි මාර්ගගත සේවාවන් කඩාකප්පල් කිරීමට හෝ පහත හෙළීමට නිර්මාණය කර ඇති සයිබර් ප්‍රහාර වේ. මෙය සාමාන්‍යයෙන් සාක්ෂාත් කරගනු ලබන්නේ සේවාව යටපත් කර එහි කාර්යිකත්වය පහත හෙළීම සඳහා මාර්ගගත සේවාවක් දත්ත, සම්බන්ධතා හෝ ඉල්ලීම් වලින් පිටාර ගැලීමට සැලැස්වීම මගිනි.

මෙය සාමාන්‍යයෙන් සාක්ෂාත් කරගනු ලබන්නේ සේවාව යටපත් කර එහි කාර්යිකත්වය පහත හෙළීම සඳහා මාර්ගගත සේවාවක් දත්ත, සම්බන්ධතා හෝ ඉල්ලීම් වලින් පිටාර ගැලීමට සැලැස්වීම මගිනි. ඒවා වඩාත් සුලබ වෙමින් පවතින්නේ, පහසුවෙන් අවදානමට ලක්විය හැකි Internet of Things (IoT) උපාංග සංඛ්‍යාව වැඩිවීම හේතුවෙනි. IoT නිෂ්පාදකයින් බොහෝ විට සයිබර් ආරක්ෂාවට වඩා පරිශීලක අත්දැකීම් වලට ප්‍රමුඛත්වය දෙන බැවින්, අවදානමට ලක්විය හැකි උපාංගවලට ස්මාර්ට් රූපවාහිනී, කේතල, වැකියුම් ක්ලීනර්ස් සහ ආරක්ෂක පද්ධති වැනි අන්තර්ජාලයට සම්බන්ධ වන නිත්‍ය ගෘහ භාණ්ඩ ඇතුළත් විය හැකිය. ද්වේෂසහගත ක්‍රියාකාරීන් විසින් ‘ආසාදිත පරිගණක ජාලයක්’ නිර්මාණය කිරීම මගින් මෙම ජාල ගමනාගමනය ජනනය කිරීම සඳහා බොහෝ විට මෙම උපාංග දුරස්ථව අවදානමට ලක් කළ හැකිය. එමඟින් DoS ප්‍රහාර සිදුවීමට ඉඩ සලසන යටිතල ව්‍යුහයන් සඳහා නොදැනුවත්වම දායක වන නිවැසියෝ සහ සංවිධාන ඇති විය හැකිය.

මෑත කාලීන ක්‍රියාකාරීත්වයෙන් පෙනී යන්නේ ද්වේෂසහගත ක්‍රියාකාරීන් IoT උපාංග විශාල සංඛ්‍යාවක් අවදානමට ලක් කළ පසු, ඔවුන් මෙම යටිතල පහසුකම් සයිබර් අපරාධකරුවන්ට සහ දුෂකයින්ට කුලියට දීමට හෝ විකිණීමට හැකි බවය. ඔව්හු තමන් තෝරා ගන්නා ඉලක්කවලට එරෙහිව DoS ප්‍රහාර සිදු කිරීමට වැඩි වැඩියෙන් උනන්දු වෙති. බොහෝ අවස්ථාවන්හිදී, DoS ප්‍රහාර සිදු කරනු ලබන්නේ සංවිධානයක ඵලදායිතාව සහ මූල්‍යමය අලාභය ඇති කිරීමට, හෝ අභිප්‍රායක් සඳහා මහජන අවධානය ලබා ගැනීමට ය. මෙම ක්‍රියාකාරකම සඳහා උදාහරණයක් *මහජන චීන සමූහාණ්ඩුවට සම්බන්ධ ක්‍රියාකාරීන් ආසාදිත පරිගණක ජාල මෙහෙයුම් සඳහා රවුටර සහ IoT උපාංග අවදානමට ලක් කරයි* ASD හි උපදේශනයේ විස්තර කර ඇත.

අපගේ ආර්ථිකය තවදුරටත් ඩිජිටල්කරණය වන විට සහ අන්තර්ජාලයට සම්බන්ධ අඩු ආරක්ෂිත IoT උපාංග සංඛ්‍යාව වර්ධනය වන විට, DoS ප්‍රහාර දිගටම වැඩි වීමට ඉඩ ඇත.

සංවිධානයක මාර්ගගත සේවාවන් කඩාකප්පල් කිරීමට හෝ පහත් කිරීමට පහත හෙළීමට, ද්වේෂසහගත ක්‍රියාකාරීන් ප්‍රවේශයන් ගණනාවක් භාවිතා කරයි. ඒවාට ඇතුළත් වන්නේ:

- පවතින සියලුම ජාලවල සංඛ්‍යාත පරාසය පරිශීලනය කිරීමේ උත්සාහයක් ලෙස මාර්ගගත සේවාවන් වෙත අනවශ්‍ය ජාල ගමනාගමනය සන්නිවේදන විශාල ප්‍රමාණයක් යොමු කිරීම
- එහි පරිගණක සැකසුම් සම්පත් පරිශීලනය කිරීමේ උත්සාහයක් ලෙස මාර්ගගත සේවාවන් වෙත සකස් කරන ලද ජාල ගමනාගමනය සන්නිවේදන යොමු කිරීම
- බහු පරිගණක, IoT උපාංග හෝ වෙනත් අන්තර්ජාල සම්බන්ධිත උපාංග භාවිතා කරමින් බහු දිශාවන්ගෙන් සහ බොහෝ විශාල පරිමාණයෙන් මාර්ගගත සේවාවන් වෙත ජාල ගමනාගමනය යොමු කිරීම. මෙය ව්‍යප්ත කරන ලද DoS (DDoS) ප්‍රහාරයක් ලෙස හඳුන්වන පොදු DoS ප්‍රහාරයකි.
- සංවිධානයක අන්තර්ජාල සේවාවන්ගෙන් නීත්‍යානුකූල පරිශීලකයින් ඉවතට හරවා යැවීමේ උත්සාහයක් ලෙස සංවිධානයේ වසම් ලියාපදිංචිය හෝ DNS අනුග්‍රහ පරිගණකය පැහැර ගැනීම.

DoS ප්‍රහාර මගින් සංවිධානයන් ඉලක්කගත කිරීම වළක්වා ගත නොහැකි නමුත්, එම ප්‍රහාර වලට සූදානම් වීමට හා ඒවායේ බලපෑම අඩු කර ගැනීමට සංවිධානවලට ක්‍රියාත්මක කළ හැකි පියවර ගණනාවක් තිබේ. DoS ප්‍රහාර සිදු වීමට පෙර ඒවාට සූදානම් වීම හොඳම උපාය මාර්ගයයි. ඒ මන්ද යත් සූදානමකින් තොරව, DoS ප්‍රහාරයකදී ප්‍රතිචාර දැක්වීම දුෂ්කර හා අඩු ඵලදායී වීමය.

සංවිධාන ප්‍රධාන වශයෙන් අවධානය යොමු කරන්නේ DoS ප්‍රහාරවලින් තමන් ආරක්ෂා වීම සඳහා වුවද, අන් අය ඉලක්ක කර ගැනීම සඳහා ඔවුන්ගේ මාර්ගගත සේවාවන් සහ අන්තර්ජාලයට සම්බන්ධ උපාංග ද්වේෂසහගත ක්‍රියාකාරීන් විසින් අනිසි ලෙස භාවිතා කිරීම වැළැක්වීමට ද ඔවුන් පියවර ගත යුතුය.

DoS ප්‍රහාරවලට සූදානම් වීම

අපගේ කලාපය පුරා DoS ප්‍රහාරවල ප්‍රමාණය වැඩිවීමේ සන්දර්භය තුළ, DoS ප්‍රහාර සඳහා සූදානම් වීමට යම් පියවරක් ක්‍රියාත්මක කිරීමට පෙර, ඔබේ සංවිධානය මුලින්ම එහි ව්‍යාපාරික අවශ්‍යතා තක්සේරු කළ යුතුය. එමඟින් DoS ප්‍රහාර අතරතුර ඔබේ සංවිධානයේ සෑම මාර්ගගත සේවාවක්ම ක්‍රියාත්මක විය යුතුද, නැතහොත් තාවකාලික සේවා බාධා කිරීම් පිළිගත හැකිද යන්න තීරණය කළ හැකිය.

ඔබේ සංවිධානයට DoS ප්‍රහාරවලට ඔරොත්තු දීමේ හැකියාව වැඩිකර ගැනීමට අවශ්‍ය නම්, DoS ප්‍රහාර සිදුවීමට පෙර, සුදුසු සහ ප්‍රායෝගික ලෙස ඔබ පහත පියවරයන් සක්‍රීය ලෙස ක්‍රියාත්මක කළ යුතුය.

- ඔබේ සංවිධානය Content Delivery Network (CDN) (අන්තර්ගත බෙදාහැරීමේ ජාලයක්) ජාලයක් භාවිතා කරන්නේ නම්, සුදුසු සහ ප්‍රායෝගික ලෙස, ඔබ පහත අතිරේක පියවරයන් ක්‍රියාත්මක කළ යුතුය.
  - ඔබගේ ආරම්භක වෙබ් අනුග්‍රහ පරිගණකය විවිධ යෙදුම් සහ ජාල ස්ථර ප්‍රහාර වලින් ආරක්ෂා කිරීම සඳහා අවශ්‍ය කාර්යිකත්වය අඩංගු CDN එකක් භාවිතා කිරීම සලකා බලන්න - සමහර CDN වල මෙම විශේෂාංග වෙබ් යෙදුම් ෆයර්වෝලයක (ජාලය තුළට හෝ ඉන් පිටතට ගමනාගමනය නිරීක්ෂණය කරන ජාල ආරක්ෂණ උපාංගයක්) කොටසක් ලෙස ඇතුළත් විය හැකිය.
  - ඔබගේ ආරම්භක වෙබ් අනුග්‍රහ පරිගණකයේ අන්තර්ජාල ප්‍රොටෝකෝල (IP) ලිපිනය අනවශ්‍ය ලෙස ප්‍රසිද්ධියේ හෙළිදරව් කිරීමෙන් වළකින්න. එමෙන්ම ඕනෑම පොදු නිරාවරණයන් DoS ප්‍රහාර වලින් ආරක්ෂා කර ඇති බව සහතික කරන්න.
  - ඔබගේ ආරම්භක වෙබ් අනුග්‍රහ පරිගණකය සඳහා ද්වේෂසහගත ක්‍රියාකාරීන්ට පුරෝකථනය කළ හැකි IP ලිපිනයක් භාවිතා කිරීමෙන් වළකින්න. උදාහරණයක් ලෙස, ඔබේ මාර්ගගත සේවාවන්හි ප්‍රසිද්ධියේ හෙළිදරව් කරන ලද IP ලිපින අඩංගු ජාලයේ උපජාලයක ඇති IP ලිපිනයක්.
  - CDN සහ ඔබේ සංවිධානයේ අවසරය ලත් කළමනාකරණ ජාලවලට පමණක් ඔබේ ආරම්භක වෙබ් අනුග්‍රහ පරිගණකයට ප්‍රවේශ විය හැකි බව සහතික කිරීමට ජාල ප්‍රවේශ පාලන (ෆයර්වෝලයක් වැනි) භාවිතා කරන්න.
  - ඔබේ ආරම්භක වෙබ් අනුග්‍රහ පරිගණකයට ඉහළ මට්ටමේ ආරක්ෂාවක් අවශ්‍ය නම්, ඔබේ ආරම්භක වෙබ් අනුග්‍රහ පරිගණකය සහ ඔබේ CDN සපයන්නා අතර පුද්ගලික ජාල සම්බන්ධතාවයක් ඇතුළත් විය හැකි ඔරොත්තු දෙන විවිධ ජාල සම්බන්ධතාවයක් භාවිතා කිරීම සලකා බලන්න.
  - ග්‍රහණය කර ගන්නා ප්‍රමාණයෙන් උපරීම වාසි ලබා ගැනීම සඳහා CDN, ආරම්භක වෙබ් අනුග්‍රහ පරිගණකය සහ සේවාදායක HTTP ශීර්ෂයන් වින්‍යාස කරන්න.
  - ඔබට ඉහළ මට්ටමේ ලබා ගැනීමේ හැකියාවක් අවශ්‍ය නම්, අඩු අවදානම් IP ලිපින වලින් ලැබෙන ඉල්ලීම් ඉහළ අවදානම් IP ලිපින වලින් ලැබෙන ඉල්ලීම් වලින් වෙන්කර හැසිරවීමට හැකිවන පරිදි ආරම්භක වෙබ් අනුග්‍රහ පරිගණකය කොටස් කිරීම සලකා බලන්න.
- ඔබේ මාර්ගගත සේවාවන්හි නීත්‍යානුකූල පරිශීලකයින් සඳහා පිළිගත හැකි කාර්යිකත්වය සහ සේවාවේ ගුණාත්මකභාවය කුමක්ද, එම ක්‍රියාකාරීත්වය පවත්වා ගන්නේ කෙසේද, සහ DoS ප්‍රහාර අතරතුර කවර කාර්යිකත්වයක් අවශ්‍ය නොවන්නේද යන්න තීරණය කරන්න.
- Cloud-based (අන්තර්ජාලයේ තැන්පත් තොරතුරු මත පදනම් වූ) DoS ප්‍රහාර ලිහිල් කිරීමේ සේවාවක් ලබාගෙන භාවිතා කරන්න.
- ඔබේ සංවිධානයේ ප්‍රහාරක තලය අඩු කිරීමට පහත දේ සලකා බලන්න:
  - මූලික මාර්ගගත සේවා (DNS වැනි) DoS ප්‍රහාරවලට ඔරොත්තු දිය හැකි කීර්තිමත් බාහිර සේවා සපයන්නන් මගින් ලබා දීම
  - තීරණාත්මක මාර්ගගත සේවා (ඊමේල් වැනි) ඉලක්ක කිරීමට වැඩි ඉඩක් ඇති (වෙබ් අඩවි වැනි) වෙනත් මාර්ගගත සේවාවන්ගෙන් වෙන්කර තැබීම
  - DoS ප්‍රහාර ලිහිල් කිරීමේ සේවාව, මාර්ගගත සේවාවේ ජාල දොරටුව හා සම්බන්ධ ජාල ගමනාගමනයට පමණක් අවසර දෙන බව සහතික කිරීම.
- ඔබේ සේවා සපයන්නන් සමඟ ඔවුන්ගේ DoS ප්‍රහාර වැළැක්වීමේ සහ ලිහිල් කිරීමේ උපාය මාර්ග පිළිබඳ සාකච්ඡා කරන්න. විශේෂයෙන් ඔවුන්ගේ:
  - ලොව පුරා DoS ප්‍රහාරවලට ඔරොත්තු දීම සඳහා ඔප්පු කරන ලද හැකියාව
  - DoS ප්‍රහාර සහ සවිස්තරාත්මක අනුමත කළ DoS ප්‍රහාර පරීක්ෂණ යන දෙකම හැසිරවීම පෙන්නුම් කරන ඉතිහාසය
  - ජාල ගමනාගමනය කායිකව විශ්ලේෂණය කිරීම වැනි මානව සහභාගීත්වයෙන් තොරව බොහෝ වර්ගවල DoS ප්‍රහාර ස්වයංක්‍රීයව ලිහිල් කිරීමේ හැකියාව

  - මිල ස්ථාවරද නැතහොත් භාවිතා කරන ජාල ගමනාගමනය සහ පරිගණක සැකසුම් සම්පත් ප්‍රමාණය අනුව එය වෙනස් වේද යන්න, සහ ඔබට බිල්පත් සීමාවක් නියම කළ හැකිද යන්න වැනි ඔවුන් සපයන සේවාවන් සඳහා මිල නියම කිරීමේ ප්‍රවේශය
  - DoS ප්‍රහාර අතරතුර ඔබට දැනුම් දීම හෝ ඔවුන්ගේ මාර්ගගත සේවාවන් අක්‍රිය කිරීම සඳහා පර්යන්තයන්
  - DoS ප්‍රහාර අතරතුර ගත හැකි පූර්ව අනුමත ක්‍රියාමාර්ග
  - ඉහළ මට්ටමේ අන්තර් සම්බන්ධිත පද්ධති මෙහෙයවන සැපයුම්කරුවන් සමඟ DoS ප්‍රහාර වැළැක්වීමේ විධිවිධාන.
- පද්ධති ලබා ගැනීමේ හැකියාව, ජාල ගමනාගමනය, පරිගණක සැකසුම් සම්පත්, සහ ඒ ආශ්‍රිත පිරිවැය තත්‍ය කාලීනව නිරීක්ෂණය කිරීම හා අනතුරු ඇඟවීම වැනි DoS ප්‍රහාර අනාවරණය කර ගැනීමේ පියවර ක්‍රියාත්මක කරන්න.
- DoS ප්‍රහාර අතරතුර සේවාව අඛණ්ඩව පවත්වාගෙන යාමට පහසුකම් සැලසීම සඳහා අවම සැකසුම් සහ සංඛ්‍යාත පරාසයක් වශ්‍ය වන ලෙසින් ඔබේ වෙබ් අඩවියේ ස්ථිතික අනුවාදයක් සකස් කරන්න.
- විශාල සංඛ්‍යාත පරාසයක්, ප්‍රමාණවත් පරිගණක සැකසුම් සම්පත්, භූගෝලීය වශයෙන් විසිරී ඇති ධාරක ස්ථාන සහ අනවශ්‍ය ජාල ගමනාගමනය ඉවත දැමීම සඳහා cloud-based (අන්තර්ජාලයේ තැන්පත් තොරතුරු මත පදනම් වූ) ගමනාගමනය සහිත ඉහළ ඔරොත්තු දෙන මාර්ගගත සේවාවන් ලබාගෙන ඒවා භාවිතා කරන්න - මෙයට සාමාන්‍යයෙන් ස්ථිතික වෙබ් අඩවි අන්තර්ගතය ගබඩා කිරීමට සහ ඔබේ ආරම්භක වෙබ් අනුග්‍රහ පරිගණකය අනවශ්‍ය ජාල ගමනාගමනයෙන් ආරක්ෂා කිරීමට කීර්තිමත් CDN භාවිතා කිරීම ඇතුළත් වේ.
- රෙජිස්ට්‍රර් අගුළු දැමීම භාවිතා කරමින්, වසම් ලියාපදිංචි සම්බන්ධතා තොරතුරු සහ අනෙකුත් විස්තර නිවැරදි බව තහවුරු කරමින්, සහ ASD හි *වසම් හිමිකරුවන් සඳහා වසම් නාම පද්ධති ආරක්ෂාව* ප්‍රකාශනයේ දක්වා ඇති අතිරේක මාර්ගෝපදේශ අනුගමනය කිරීමෙන් ඔබේ සංවිධානයේ වසම් නාම ආරක්ෂා කර ගන්න.
- ඔබේ සංවිධානයේ අවශ්‍යතා මත පදනම්ව සියලුම සම්බන්ධතා ලබා ගත හැකි බව සහතික කරමින්, සේවා සපයන්නන් සඳහා යාවත්කාලීන සම්බන්ධතා තොරතුරු පවත්වා ගෙන, ඔබේ සංවිධානයේ සම්බන්ධතා තොරතුරු ඔවුන් සමඟ බෙදා ගන්න (උදාහරණයක් ලෙස, සතියේසෑම දිනකම පැය 24 පුරා).
- සාමාන්‍ය සන්නිවේදන නාලිකා අසාර්ථක වන විට, විශ්වාසදායක සන්නිවේදන නාලිකාවක් සඳහා ඔබේ සේවා සපයන්නන්ට ඔබේ සංවිධානයේ නිශ්චිත සංඛ්‍යාත කලාපයෙන් පිටත සම්බන්ධතා තොරතුරු ලබා දෙන්න.
- DoS ප්‍රහාරවලට ඔරොත්තු දීමට අවශ්‍ය ඔබේ එක් එක් මාර්ගගත සේවාවන්ට එරෙහි විවිධ ආකාරයේ DoS ප්‍රහාර ආවරණය කරන සයිබර් ආරක්ෂණ සිදුවීම් ප්‍රතිචාර සැලැස්මක් පිළියෙල කර, ක්‍රියාත්මක කර පවත්වාගෙන යන්න. එමෙන්ම එම සැලැස්ම අවම වශයෙන් වාර්ෂිකව පරිහරනය කරන්න.
- පරිගණක සැකසුම් සම්පත් වැඩියෙන් පරිභෝජනය කරන හෝ අමතර මූල්‍ය පිරිවැයක් දැරීමට සිදුවන (SMS පණිවිඩ යැවීම වැනි) බහුලව භාවිතා වන කාර්යිකත්වය ආරක්ෂා කිරීම සඳහා යෙදුම් නිර්මාණය කරන්න.
  - අනුපාත සීමා කිරීම සහ පුද්ගලයෙක් විසින් ඉල්ලීම් සිදු කරන බව සත්‍යාපනය කිරීම, මෙම ආරක්ෂණවලට ඇතුළත් වේ.
  - යෙදුම් කාර්යිකත්වයේ නුසුදුසු තාර්කික ප්‍රවාහ ඉලක්කගත කිරීම ඇතුළුව DoS ප්‍රහාර පරීක්ෂණ සිදු කරන්න.
  - DoS දෙශිකයන් හඳුනාගෙන ඒවා නිවැරදි කිරීම සඳහා load testing (පද්ධතියේ හැසිරීම පරීක්ෂා කිරීමේ ක්‍රියාවලිය) සිදු කරන්න.

DoS ප්‍රහාරවලට ප්‍රතිචාර දැක්වීම

ඔබේ සංවිධානය DoS ප්‍රහාර සඳහා සූදානම් වී නොමැති නම්, ඔබට ඉහත පියවරවලින් කිහිපයක් DoS ප්‍රහාර අතරතුරදී ක්‍රියාත්මක කිරීමට උත්සාහ කළ හැකිය. නමුත් ඒවා අඩු ඵලදායී සහ ක්‍රියාත්මක කිරීමට කාලයක් ගත විය හැකි අතර, එමඟින් ඔබේ සංවිධානයේ ප්‍රතිචාර දැක්වීමේ හැකියාව අඩු වේ.

DoS ප්‍රහාර අතරතුර, සුදුසු සහ ප්‍රායෝගික ලෙස, ඔබේ සංවිධානය පහත පියවර ක්‍රියාත්මක කළ යුතුය.

- ඔබේ සයිබර් ආරක්ෂණ සිදුවීම් ප්‍රතිචාර සැලැස්ම ක්‍රියාත්මක කරන්න.
- ඔබේ සේවා සපයන්නන්ට ප්‍රතිචාරාත්මක ක්‍රියාමාර්ග වහාම ක්‍රියාත්මක කළ හැකිදැයි ඔවුන්ගෙන් විමසන්න - ඔවුන්ගේ ප්‍රතිචාර දැක්වීමේ හැකියාව ඔබ මීට පෙර සාකච්ඡා කර නොමැති නම්, ඔවුන්ට ප්‍රතිචාර දැක්වීමට නොහැකි බව හෝ එයට අකමැති බව ඔබට සොයා ගත හැකිය, නැතහොත් ඔවුන් ඔවුන්ගෙන් ඒ සඳහා අමතර ගාස්තු අය කළ හැකිය.
- අත්‍යවශ්‍ය නොවන කාර්යිකතාවය අක්‍රීය කරන්න, නැතහොත් වත්මන් DoS ප්‍රහාරය ඵලදායී කරන ඔබේ මාර්ගගත සේවාවන්ගෙන් අත්‍යවශ්‍ය නොවන අන්තර්ගතයන් ඉවත් කරන්න. උදාහරණයක් ලෙස, සෙවුම් කාර්යිකත්වය, ගතික අන්තර්ගතය හෝ විශාල ගොනු නොමැතිව ඔබේ වෙබ් අඩවියේ අනුවාදයක් යොදවන්න.
- ඔබේ DoS ප්‍රහාර ලිහිල් කිරීමේ සේවා සපයන්නා ඇතුළු ඔබේ ගනුදෙනුකරුවන් සහ ඔබේ සේවා සපයන්නන් සමඟ සන්නිවේදනය පවත්වා ගනිමින්, ඔබේ මාර්ගගත සේවාවන්හි සුලභතාව දිගලම නිරීක්ෂණය කරන්න.
- ඔබගේ ආරම්භක වෙබ් අනුග්‍රහ පරිගණකය සෘජුවම ඉලක්ක කර ඇත්නම් එහි IP ලිපිනය වෙනස් කිරීම සලකා බලන්න. එමෙන්ම ආරක්ෂාවක්, නව IP ලිපිනය ප්‍රසිද්ධියේ හෙළිදරව් කිරීමෙන් වළකින්න.
- මෙම ප්‍රකාශනයේ ‘සම්බන්ධතා විස්තර’ කොටසට අනුව, DoS ප්‍රහාරය පිළිබඳව ASD සහ NCSC-NZ ඇතුළු අදාළ පාර්ශවයන්ට වාර්තා කරන්න.

DoS ප්‍රහාරවලට දායක වීමෙන් වැළකීම

අන් අයට බලපෑම් කළ හැකි DoS ප්‍රහාරවලට නොදැනුවත්වම දායක වීම වැළැක්වීම සඳහා ඔබේ සංවිධානය පහත පියවර ක්‍රියාත්මක කළ යුතුය.

- අනවශ්‍ය, අනාරක්ෂිත ලෙස වින්‍යාස කර ඇති හෝ ප්‍රමාණවත් ලෙස නඩත්තු කර නොමැති සේවාවන්, IoT උපාංග සහ අනෙකුත් අන්තර්ජාල සම්බන්ධිත උපාංග අන්තර්ජාලයට නිරාවරණය කිරීමෙන් වළකින්න.
- අන්තර්ජාලයට නිරාවරණය කර ඇති සේවාවන්, IoT උපාංග සහ අනෙකුත් අන්තර්ජාල සම්බන්ධිත උපාංග ආරක්ෂිතව වින්‍යාස කිරීම, නඩත්තු කිරීම සහ අධීක්ෂණය කරන්න.
  - කුඩා ව්‍යාපාර සඳහා අමතර මග පෙන්වීම ASD හි *Internet of Things උපාංග* සහ *ඔබේ Wi-Fi සහ රවුටරය සුරක්ෂිත කිරීම* සම්බන්ධ ප්‍රකාශන මගින් ලබාගත හැකිය.

ඔබේ සංවිධානය මාර්ගගත සේවා ක්‍රියාත්මක කරන්නේ නම්, ඔබ පහත දැක්වෙන අතිරේක පියවරයන් ක්‍රියාත්මක කළ යුතුය.

- එක්සත් ජනපදයේ සයිබර් ආරක්ෂණ සහ යටිතල ව්‍යුහ ආරක්ෂක ඒජන්සියේ (CISA) *UDP-පාදක විස්තාරණ ප්‍රහාර* උපදෙස් වල දක්වා ඇති ප්‍රොටෝකෝල සමාලෝචනය කිරීමට ප්‍රමුඛත්වය දෙන්න.
- නව විස්තාරණ දෛශික හඳුනාගෙන ඇති බැවින් සහ ඒවාට එරෙහිව ඔබේ මාර්ගගත සේවාවන් සුරක්ෂිත කරන බැවින්, ඒවා අධීක්ෂණය කරන්න.
- අනුමත කළ මාර්ගගත සේවාවන් සහ සංවිධාන වෙත ප්‍රවේශය සීමා කිරීමට ඇතුලට එන හා පිටතට යන ජාල ප්‍රවේශ පාලන දෙකම වින්‍යාස කරන්න.
- අවශ්‍ය නොවේ නම්, විස්තාරණ-නැඹුරුවක් ඇති මාර්ගගත සේවා සඳහා නිර්නාමික පොදු ප්‍රවේශය අවහිර කරන්න.
- ප්‍රවේශ පාලන අවහිර කිරීම හෝ යෙදීම කළ නොහැකි නම් හෝ එය සුදුසු නොවේ නම්, අපයෝජනයේ ප්‍රතිවිපාක අඩු කිරීම සඳහා අනුපාත-සීමා කිරීමේ යාන්ත්‍රණයක් ක්‍රියාත්මක කිරීම ගැන සලකා බලන්න.

වැඩිදුර තොරතුරු

ASD හි *තොරතුරු ආරක්ෂණ අත්පොත* යනු සංවිධානවලට සයිබර් තර්ජන වලින් තම පද්ධති සහ දත්ත ආරක්ෂා කර ගැනීම සඳහා යෙදිය හැකි සයිබර් ආරක්ෂණ රාමුවකි. *සයිබර් ආරක්ෂණ සිදුවීම් ලිහිල් කිරීමේ උපාය මාර්ගවල* ඇති උපදෙස්, *Essential Eight (අත්‍යවශ්‍ය අට) සමඟින්*, මෙම රාමුවට අනුපූරක වේ.

නවසීලන්ත තොරතුරු ආරක්ෂණ අත්පොත යනු තොරතුරු සහතික කිරීම සහ තොරතුරු පද්ධති ආරක්ෂාව පිළිබඳව නවසීලන්ත රජය නිකුත් කරන ලද අත්පොතයි. එය ඒජන්සි තොරතුරු ආරක්ෂණ විධායකයින්ගේ මෙන්ම ඒජන්සි වලට සේවා සපයන වෙළෙන්දන්, කොන්ත්‍රාත්කරුවන් සහ උපදේශකයින්ගේ අවශ්‍යතා සපුරාලීම සඳහා නිර්මාණය කර ඇති වෘත්තිකයින්ගේ අත්පොතකි. එය ඒජන්සි තොරතුරු ආරක්ෂණ විධායකයින්ගේ මෙන්ම ඒජන්සි වලට සේවා සපයන වෙළෙන්දන්, කොන්ත්‍රාත්කරුවන් සහ උපදේශකයින්ගේ අවශ්‍යතා සපුරාලීම සඳහා නිර්මාණය කර ඇති වෘත්තිකයින්ගේ අත්පොතකි.

විවිධ DoS ප්‍රහාර වර්ග පිළිබඳ වැඩිදුර තොරතුරු CISA හි *DDoS Quick Guide* සහ *Drived Denial-Of-Service Attacks අවබෝධය කර ගැනීම සහ ප්‍රතිචාර දැක්වීම* පිළිබඳ ප්‍රකාශනවල ඇත.

සම්බන්ධතා විස්තර

ඔස්ට්‍රේලියාව තුළ, මෙම මාර්ගෝපදේශය පිළිබඳව ඔබට යම් ප්‍රශ්න තිබේ නම් ASD වෙත ලියන්න, නැතහොත් 1300 CYBER1 (1300 292 371) අමතන්න.

නවසීලන්තය තුළ, සයිබර් ආරක්ෂක සිදුවීමක් වාර්තා කිරීමට, ඊමේල් මගින් incidents@ncsc.govt.nz දන්වන්න, නැතහොත් NCSC-NZ හි සිද්ධියක් වාර්තා කිරීම් වෙබ් පිටුවට පිවිසෙන්න.

හිමිකම් අතහැරීම

මෙම මාර්ගෝපදේශයේ අඩංගු කරුණු සාමාන්‍ය ස්වභාවයක් ගන්නා අතර එය නීති උපදෙසක් ලෙස හෝ යම් විශේෂිත අවස්ථාවකදී හෝ හදිසි අවස්ථාවකදී සහාය සඳහා විශ්වාසය තැබිය යුතු දෙයක් ලෙස සැලකිය යුතු නොවේ. ඕනෑම වැදගත් කාරණයකදී, ඔබේම තත්වයන් සම්බන්ධව සුදුසු ආකාරයේ ස්වාධීන වෘත්තීය උපදෙස් ලබා ගත යුතුය.

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

ප්‍රකාශන හිමිකම

රාජ්‍ය ලාංඡනය භාවිතා කිරීම

රාජ්‍ය ලාංඡනය භාවිතා කළ හැකි නියමයන් අග්‍රාමාත්‍ය සහ කැබිනට් දෙපාර්තමේන්තුවේ වෙබ් අඩවියේ Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au හි විස්තර කර ඇත.

වැඩිදුර තොරතුරු සඳහා, හෝ සයිබර් ආරක්ෂක සිදුවීමක් වාර්තා කිරීමට, අප සමඟ සම්බන්ධ වන්න:

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