சேவை மறுப்பு தாக்குதல்களுக்குத் தயார்படுத்துதல் மற்றும் பதிலளித்தல்

முதல் வெளியீடு: செப்டம்பர் 2011
கடைசியாகப் புதுப்பிக்கப்பட்டது: மார்ச் 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

அறிமுகம்

நமது பிராந்தியத்தில் சேவை மறுப்பு (DoS) தாக்குதல்கள் அதிகரித்து வருவதால், அதற்குப் பதிலளிக்கும் விதமாக, ஆஸ்திரேலிய புலனாய்வு சமூகத்தின் ஒரு பகுதியாக இயங்கும் ஆஸ்திரேலிய சமிக்ஞைகள் இயக்குநரகத்தால் (ASD), நியூசிலாந்து அரசின் சைபர் பாதுகாப்பு மையம் (NCSC-NZ), Akamai Technologies Ltd மற்றும் Cloudflare Pty Ltd ஆகியவற்றுடன் இணைந்து இந்த ஆவணம் உருவாக்கப்பட்டது. DoS தாக்குதல்களுக்குத் தயாராகவும் பதிலளிக்கவும், தற்போது நடைமுறையிலுள்ள சிறந்த நடவடிக்கைகள் குறித்த வழிகாட்டுதலை இது வழங்குகிறது.

ASD வெளியிட்ட *Internet of Things devices* மற்றும் *Secure your Wi-Fi and router* என்ற வெளியீடுகளையும் இந்த ஆலோசனையுடன் இணைந்து படிக்கப் பரிந்துரைக்கிறோம். மற்றவர்களைப் பாதிக்கக்கூடிய DoS தாக்குதல்களுக்கு ஒருவர் தற்செயலாகப் பங்களிப்பதைத் தவிர்க்க இந்த வெளியீடுகள் உதவுகின்றன.

வலைத்தளங்கள், மின்னஞ்சல் மற்றும் Domain Name System என்ற தளங்களின் பெயர் அமைப்பு (DNS) சேவைகள் போன்ற ஆன்லைன் சேவைகளைச் சீர்குலைக்க அல்லது தரமிறக்க, மற்றும் முறையான பயனர்களுக்கான அணுகலை மறுக்க வடிவமைக்கப்பட்ட சைபர் தாக்குதல்கள் அனைத்துக்கும் கொடுக்கப்பட்டுள்ள பெயர், சேவை மறுப்பு தாக்குதல்கள் (DoS) ஆகும். ஒரு ஆன்லைன் சேவையை தரவு, இணைப்புகள் அல்லது கோரிக்கைகளால் நிரப்பி, சேவையை மூழ்கடித்து அதன் செயல்பாட்டைக் குறைக்கும் வகையில் பொதுவாக இது எட்டப்படுகிறது.

பொதுவாக, DoS தாக்குதல்கள் வெற்றிகரமாக நடைபெறுவதற்கு நெட்வொர்க் போக்குவரத்து அதிகளவு தேவைப்படுகிறது. எளிதில் பாதிக்கப்படக்கூடிய இணைய சாதனங்களின்(Internet of Things, சுருக்கமாக IoT) எண்ணிக்கை அதிகரிப்பதும், DoS தாக்குதல்கள் இப்போது அதிகமாகி வருவதற்கான ஒரு காரணமாக இருக்கிறது. சைபர் பாதுகாப்பை விட பயனர் அனுபவத்திற்கு IoT உற்பத்தியாளர்கள் பெரும்பாலும் முன்னுரிமை அளிப்பதால், வீட்டில் பயன்படும் தொலைக்காட்சிப் பெட்டிகள் (smart TVs), தண்ணீர் சூடாக்கிகள் (kettles), துப்புரவு கருவிகள் (vacuum cleaners) மற்றும் பாதுகாப்பு கமராக்கள் போன்ற இணையத்துடன் இணைக்கும் கருவிகள் பாதிக்கப்படக்கூடிய சாதனங்களில் அடங்கும். இந்த சாதனங்கள் பயன்படுத்தும் நெட்வொர்க்

போக்குவரத்திலிருந்து 'botnet' ஒன்றை உருவாக்கி, தீங்கிழைப்பவர்கள் பெரும்பாலும் தொலை தூரத்தில் இருந்து கொண்டு, DoS தாக்குதல்களை நடத்தலாம் என்பதால், அப்படி ஏற்பட அனுமதிக்கும் உள் கட்டமைப்பிற்கு வீடுகளும் நிறுவனங்களும் தற்செயலாகப் பங்களிக்கக்கூடும்.

தீங்கிழைப்பவர்கள் அதிக எண்ணிக்கையிலான IoT சாதனங்களை சமரசம் செய்த பின்னர் இந்த உள் கட்டமைப்பை, DoS தாக்குதல் நடத்த அதிகளவில் ஆர்வமாக உள்ள சைபர் குற்றவாளிகள் மற்றும் இணைய வழி தாக்குதல்களில் ஈடுபடுபவர்களுக்கு அவற்றை வாடகைக்கு விடக்கூடும் அல்லது விற்கக்கூடும் என்பதை சமீபத்திய செயல்பாடுகள் சுட்டிக் காட்டுகின்றன. பெரும்பாலான சந்தர்ப்பங்களில், DoS தாக்குதல்கள் ஒரு நிறுவனத்தின் உற்பத்தித் திறன் மற்றும் நிதி இழப்பை ஏற்படுத்துவதற்காக அல்லது ஒரு விடயத்தில் பொதுமக்களின் கவனத்தை ஈர்ப்பதற்காக நடத்தப்படுகின்றன. *சீன மக்கள் குடியரசுடன் தொடர்புடைய சிலர் ரவுட்டர்கள் மற்றும் IoT சாதனங்களைப் பயன்படுத்தி 'botnet' ஒன்றை உருவாக்குகிறார்கள்* என்ற எடுத்துக்காட்டு, ASD இன் ஆலோசனைக் கையேட்டில் விவரிக்கப்பட்டுள்ளது.

நமது பொருளாதாரம் மேலும் டிஜிட்டல் மயமாக்கப்படுவதாலும், இணையத்துடன் இணைக்கப்பட்ட, பாதுகாப்பு குறைவான IoT சாதனங்களின் எண்ணிக்கை அதிகரிப்பதாலும், DoS தாக்குதல்கள் தொடர்ந்து அதிகரிக்க வாய்ப்புள்ளது.

ஒரு நிறுவனத்தின் ஆன்லைன் சேவைகளை சீர்குலைக்க அல்லது தரமிறக்க, தீங்கிழைப்பவர்கள் பல அணுகுமுறைகளைப் பயன்படுத்துகின்றனர், அவற்றுள்:

- கிடைக்கக்கூடிய அனைத்து நெட்வொர்க் அலைவரிசையையும் பயன்படுத்தும் முயற்சியில், ஆன்லைன் சேவைகளில் நெட்வொர்க் போக்குவரத்தை அதிகளவில் தேவையில்லாமல் அதிகரித்தல்
- ஆன்லைன் சேவைகளில், அவற்றின் கணினி செயலாக்க வளங்களைத் திருடி நுகரும் முயற்சியில், மாற்றியமையக்கப்பட்ட நெட்வொர்க் போக்குவரத்தை இயக்குதல்
- பல கணினிகள் மற்றும், IoT சாதனங்கள் அல்லது பிற இணையத்துடன் இணைக்கப்பட்ட சாதனங்களைப் பயன்படுத்தி ஆன்லைன் சேவைகளில் நெட்வொர்க் போக்குவரத்தை பல திசைகளிலிருந்தும் மிகப் பெரிய அளவில் இயக்குதல் – இது பொதுவாக செய்யப்படும் DoS தாக்குதல் என்றாலும், இது விநியோகிக்கப்பட்ட DoS (distributed DoS - DDoS) தாக்குதல் என அழைக்கப்படுகிறது.
- ஒரு நிறுவனத்தின் ஆன்லைன் சேவைகளிலிருந்து முறையான பயனர்களைத் திருப்பிவிடும் முயற்சியில், ஒரு நிறுவனத்தின் இணைய தளங்களின் பெயர் அமைப்புப் பதிவு அல்லது DNS சேவையகங்களைக் கைப்பற்றுதல்

DoS தாக்குதல்களுக்கு இலக்காகாமல் நிறுவனங்கள் இருக்க முடியாது, ஆனால் அவற்றின் தாக்கத்திற்குத் தயாராகவும், சாத்தியமான வகையில் தாக்குதல்கள் நடப்பதைக் குறைக்கவும் நிறுவனங்கள் செயல்படுத்தக்கூடிய பல நடவடிக்கைகள் உள்ளன. DoS தாக்குதல்கள் நிகழும் முன் அவற்றுக்குத் தயாராவதே சிறந்த உத்தி, ஏனெனில் தயாரிப்பு இல்லாமல், DoS தாக்குதலின் போது அதற்குப் பதிலளிப்பது கடினம் மற்றும் அப்படி செய்யும் போது செயல்திறன் குறைவானதாக இருக்கும்.

DoS தாக்குதல்களிலிருந்து தங்களைப் பாதுகாத்துக் கொள்வதில் நிறுவனங்கள் முதன்மையாகக் கவனம் செலுத்தினாலும், மற்றவர்களை குறிவைத்துத் தீங்கிழைப்பவர்களால், தங்கள் ஆன்லைன் சேவைகள் மற்றும் இணையத்துடன் இணைக்கப்பட்ட சாதனங்கள் தகாத முறையில் பயன்படுத்தப்படுவதைத் தடுக்கவும் நடவடிக்கை எடுக்க வேண்டும்.

DoS தாக்குதல்களுக்குத் தயாராகுதல்

எங்கள் பிராந்தியம் முழுவதும் DoS தாக்குதல்கள் அதிகரித்து வரும் சூழலில், DoS தாக்குதல்களுக்குத் தயாராவதற்கான எந்தவொரு நடவடிக்கைகளையும் செயல்படுத்துவதற்கு முன்னர், உங்கள் நிறுவனம் அதன் வணிகத் தேவைகளை முதலில் மதிப்பிட வேண்டும், இதனால் உங்கள் ஒவ்வொரு ஆன்லைன் சேவையும் DoS தாக்குதல்களின் போது செயல்பாட்டில் இருக்க வேண்டுமா, அல்லது ஏற்படும் இடையூறுகளை தற்காலிக சேவை ஏற்கத்தக்கதா என்பதை நீங்கள் தீர்மானிக்க வேண்டும்.

உங்கள் நிறுவனம் DoS தாக்குதல்களைத் தாங்கும் திறனை அதிகரிக்க விரும்பினால், DoS தாக்குதல்கள் நிகழும் முன்னர், பொருத்தமான மற்றும் நடைமுறைக்கு ஏற்ற வகையில் பின்வரும் நடவடிக்கைகளை முன்கூட்டியே செயல்படுத்த வேண்டும்.

- உங்கள் நிறுவனம் உள்ளடக்க விநியோக வலையமைப்பை (CDN) பயன்படுத்தினால், பொருத்தமான மற்றும் நடைமுறைக்கு ஏற்ற வகையில், பின்வரும் கூடுதல் நடவடிக்கைகளை நீங்கள் செயல்படுத்த வேண்டும்.
  - பல்வேறு பயன்பாடுகள் மற்றும் நெட்வொர்க் அடுக்கு தாக்குதல்களிலிருந்து உங்கள் மூல இணைய சேவையகத்தைப் பாதுகாக்கக்கூடிய செயல்பாட்டை உள்ளடக்கிய ஒரு CDN ஐப் பயன்படுத்துவதைக் கருத்தில் கொள்ளுங்கள் - சில CDNகள் இவற்றை இணைய பயன்பாட்டு தீச்சுவரின் (firewallலின்) ஒரு பகுதியாக சேர்க்கக்கூடும்.
  - உங்கள் மூல இணைய சேவையகத்தின் இணைய நெறிமுறை (IP) முகவரியை தேவையற்ற முறையில் பொது தளங்களில் வெளியிடுவதைத் தவிர்க்கவும், மேலும் பொதுமக்கள் பார்க்கக்கூடிய எந்தவொரு இணைய நெறிமுறை முகவரியும் DoS தாக்குதல்களிலிருந்து பாதுகாக்கப்படுவதை உறுதி செய்யவும்.
  - தீங்கிழைப்பவர்கள் கணிக்கக்கூடிய இணைய நெறிமுறை (IP) முகவரியை உங்கள் மூல இணைய சேவையகத்திற்குப் பயன்படுத்துவதைத் தவிர்க்கவும், எடுத்துக்காட்டாக, பொதுமக்கள் பார்க்கக்கூடிய உங்கள் இணைய வழி சேவைகளின் இணைய நெறிமுறை (IP) முகவரியை அதே subnet முகவரியாகப் பயன்படுத்துவதை தவிர்க்கவும்.
  - CDN மற்றும் உங்கள் நிறுவனத்தின் அங்கீகரிக்கப்பட்ட மேலாண்மை நெட்வொர்க்குகள் மட்டுமே உங்கள் மூல இணைய சேவையகத்தை (origin web serverஐ) அணுக முடியும் என்பதை உறுதிப்படுத்த, அணுகல் கட்டுப்பாடுகளை (தீச்சுவர் - firewall போன்றவை) பயன்படுத்தவும்.
  - உங்கள் மூல இணைய சேவையகத்திற்கு அதிகளவு பாதுகாப்பு தேவைப்பட்டால், உங்கள் மூல இணைய சேவையகத்திற்கும் உங்கள் CDN வழங்குநருக்கும் இடையில் தனியார் நெட்வொர்க் இணைப்பை உள்ளடக்கிய நெகிழக்கூடிய பல்வேறு நெட்வொர்க் இணைப்பைப் பயன்படுத்துவதைக் கருத்தில் கொள்ளுங்கள்.
  - நினைவகப் பகுதியில் (cache) சேர்த்து வைக்கப்படும் அளவை மேம்படுத்த, CDN, மூல இணைய சேவையகம் மற்றும் நுகர்வோர் (client) HTTP தலைப்புகளை உள்ளமைக்கவும்.
  - உங்கள் இணைய சேவை அதிகளவு கிடைக்கும் தன்மை கொண்டதாக இருக்க விரும்பினால், மூல இணைய சேவையகங்களை பகிர்வதைக்

கருத்தில் கொள்ளுங்கள். இதனால் குறைந்த ஆபத்துள்ள இணைய நெறிமுறை (IP) முகவரிகளிலிருந்து வரும் கோரிக்கைகளும் அதிக ஆபத்துள்ள IP முகவரிகளிலிருந்து வரும் கோரிக்கைகளும் தனித்தனியாகக் கையாளப்படலாம்.

- உங்கள் ஆன்லைன் சேவைகளின் முறையான பயனர்களுக்கு என்ன செயல்பாடு தேவை மற்றும் எந்த அளவில் சேவையின் தரம் ஏற்றுக் கொள்ளத்தக்கது என்பதையும் அந்த செயல்பாட்டை எவ்வாறு பராமரிப்பது என்பதையும் DoS தாக்குதல்களின் போது என்ன செயல்பாடு தேவையில்லை என்பதையும் தீர்மானியுங்கள்.
- மேகக் கணிமை (cloud) அடிப்படையிலான DoS தாக்குதல் தணிப்பு சேவையை வாங்கிப் பயன்படுத்தவும்.
- உங்கள் நிறுவனத்தின் மீது தாக்குதல் நடக்கக்கூடிய வழிகளைக் குறைக்க முடியுமா என்று ஆராயுங்கள்:
  - DoS தாக்குதல்களைத் தாங்கக்கூடிய புகழ்பெற்ற சேவை வழங்குநர்களுக்கு (DNS போன்ற) அடிப்படை ஆன்லைன் சேவைகளை ஒப்பந்த சேவை அடிப்படையில் பெறுதல்
  - (மின்னஞ்சல் போன்ற) முக்கியமான ஆன்லைன் சேவைகளை, (இணைய வலைத்தளங்கள் போன்ற) இலக்கு வைக்க அதிக வாய்ப்புள்ள பிற ஆன்லைன் சேவைகளிலிருந்து பிரித்தல்
  - ஆன்லைன் சேவையின் network port(s) எனும் தொடர்பு முனைகளுடன் இணைய போக்குவரத்தை மட்டுமே DoS தாக்குதல் தணிப்பு சேவை அனுமதிக்கிறது என்பதை உறுதி செய்வது
- உங்கள் சேவை வழங்குநர்களுடன், அவர்களின் DoS தாக்குதல் தடுப்பு மற்றும் தணிப்பு உத்திகளின் விவரங்களைப் பற்றி கலந்துரையாடவும், குறிப்பாக அவர்களுடைய செய்முறை:
  - உலகின் எந்தப் பகுதியிலிருந்து DoS தாக்குதல் நடத்தப்பட்டாலும் அதனைத் தாங்கும் திறன் நிரூபிக்கப்பட்டுள்ளது
  - DoS தாக்குதல்கள் மற்றும் விரிவான அங்கீகரிக்கப்பட்ட DoS தாக்குதல் சோதனை இரண்டையும் கையாளும் வல்லமை நீண்ட காலமாகப் பயன்படுத்தப்பட்டது
  - இணைய தளத்தை அணுகுபவர்கள் யார் என்று ஆராய்வதற்கு மனித ஈடுபாடு இல்லாமல், பெரும்பாலான வகையான DoS தாக்குதல்களைத் தானாகவே குறைக்கும் திறன் உள்ளது
  - எவ்வளவு செலவாகும் என்பதன் அளவு நிர்ணயிக்கப்பட்டதா அல்லது இணையத் தளத்தை அணுகுபவர்கள் எண்ணிக்கை மற்றும் பயன்படுத்தப்படும் கணினி செயலாக்க வளங்களின் அளவின் அடிப்படையில் மாறுபடுமா என்பதும், அவர்கள் வசூலிக்கும் கட்டணம் உச்ச வரம்பு ஒன்றை மீறாமல் இருக்க முடியுமா என்பது போன்ற சேவைகளுக்கு விலை நிர்ணயம் செய்வதற்கான அவர்களின் அணுகுமுறை
  - DoS தாக்குதல்களின் போது, உங்களுக்கு அதனை எப்படி எப்போது தெரிவிப்பார்கள் மற்றும் அவர்களின் ஆன்லைன் சேவைகளை முடக்குவதற்கான வரம்புகள் எவை
  - DoS தாக்குதல்களின் போது மேற்கொள்ளக்கூடிய முன்-அங்கீகரிக்கப்பட்ட நடவடிக்கைகள்
  - உங்களது இணைய சேவைக்கு வேறு வழங்குநர்களுடன் DoS தாக்குதல் தடுப்பு ஏற்பாடுகள்

- நிகழ்நேர கண்காணிப்பு மற்றும் கணினி செயற்பாடு நின்றுவிட்டால் உடனே அறிவித்தல், நெட்வொர்க் போக்குவரத்து, கணினி செயலாக்க வளங்கள் மற்றும் தொடர்புடைய செலவுகள் போன்ற DoS தாக்குதல்களைக் கண்டறிவதற்கான நடவடிக்கைகளை செயல் படுத்தவும்.
- DoS தாக்குதல்களின் போது சேவையின் தொடர்ச்சியை எளிதாக்க உங்கள் இணையதளத்தின் குறைந்தபட்ச செயலாக்கம் மற்றும் அலைவரிசை தேவைப்படும் நிலையான ஒரு பதிப்பைத் தயாரிக்கவும்.
- பெரிய அலைவரிசை, போதுமான கணினி செயலாக்க வளங்கள், புவியியல் ரீதியாகப் பரவலாக்கப்பட்ட இருப்பிடங்களில் கணினிகள் மற்றும் விரும்பத்தகாத நெட்வொர்க் போக்குவரத்தை நிராகரிக்க மேகக் கணிமை (cloud) அடிப்படையிலான scrubbing என்ற பிழை திருத்தும் நுட்பம் ஆகியவற்றைக் கொண்ட மிகவும் நெகிழக்கூடிய ஆன்லைன் சேவைகளை வாங்கிப் பயன்படுத்தவும் - இது பொதுவாக நிலையான வலைத்தள உள்ளடக்கத்தை தேக்கப்படுத்த புகழ்பெற்ற CDNஐப் பயன்படுத்துவதைக் கொண்டிருக்கிறது மற்றும் தேவையற்ற நெட்வொர்க் போக்குவரத்திலிருந்து உங்கள் மூல இணைய சேவையகத்தைப் பாதுகாக்கிறது.
- தளங்களின் இணையப் பெயர்களைப் பதிவு செய்யும் பதிவாளருடன் தொடர்பு விவரங்கள் மற்றும் பிற தரவுகள் சரியானவை என்பதை உறுதிப்படுத்துவதுடன், இணைய முகவரிகளின் தொகுதியான டொமெய்ன் (domain) பதிவாளரால் registrar lock என்ற நிலைக் குறியீட்டை அமைக்கவும். இதற்கு டொமெய்ன் உரிமையாளர்களுக்காக, ASD வெளியிட்டுள்ள *Domain Name System security for domain owners* என்ற வெளியீட்டில் கூறப்பட்டுள்ள மேலதிக அறிவுரைகளையும் பார்க்கவும்.
- உங்கள் சேவை வழங்குநர்களின் தொடர்பு விவரங்களைப் புதுப்பித்த நிலையில் பராமரிப்பது மட்டுமன்றி, உங்கள் நிறுவனத்தின் தொடர்பு விவரங்களையும் அவர்களுடன் பகிர்ந்து கொள்ளுங்கள், உங்கள் நிறுவனத்தின் தேவைகளின் அடிப்படையில் அனைத்து தொடர்புகளும் (எடுத்துக்காட்டாக, ஒரு நாளில் 24 மணி நேரமும், வாரத்தில் 7 நாட்களும்) கிடைப்பதை உறுதி செய்யுங்கள்.
- சாதாரண தகவல்தொடர்பு வழிகள் செயல் படாமல் போகும் போது, நம்பகமான மாற்று தகவல்தொடர்பு வழிகளுக்கு உங்கள் நிறுவனத்தின் out-of-band எனும் நிலையில் பயன்படுத்தப்பட வேண்டிய தொடர்பு விவரங்களை உங்கள் சேவை வழங்குநர்களிடம் பகிரவும்.
- DoS தாக்குதல்களைத் தாங்குவதற்குத் தேவையான உங்கள் ஒவ்வொரு ஆன்லைன் சேவைகளுக்கும் எதிரான பல்வேறு வகையான DoS தாக்குதல்களை உள்ளடக்கிய சைபர் பாதுகாப்பு சம்பவங்களுக்குப் பதிலளிக்க, திட்டத்தை உருவாக்கி, செயல்படுத்திப் பராமரிக்கவும். இந்தத் திட்டம் செயல்படுமா என்பதை குறைந்தபட்சம் ஆண்டுக்கு ஒருமுறையாவது சோதித்துப் பார்க்கவும்.
- அதிகரித்த கணினி செயலாக்க வளங்களை நுகரும் அல்லது (குறுஞ்செய்திகளை அனுப்புவது போன்ற) கூடுதல் நிதி செலவுகளை ஏற்படுத்தும், பொதுவாகத் தவறான முறையில் பயன்படுத்தப்படும் செயல்பாடுகளிலிருந்து உங்களைப் பாதுகாக்கும் வகையில் செயலிகளை வடிவமையுங்கள்.
  - எத்தனை முறை கோரிக்கை வந்தது என்பதற்கான விகித வரம்பு மற்றும் கோரிக்கைகள் ஒரு மனிதனிடமிருந்து வந்தவை என்பதை சரி பார்ப்பது ஆகியவை பாதுகாப்பு செயல்முறையில் அடங்கும்.
  - செயலிகளின் செயல்பாட்டில் முறையற்ற கணினி குறியீடுகள் இருக்கின்றனவா, அவற்றை இலக்கு வைத்து DoS தாக்குதல் நடத்தப்படலாமா என்பது உட்பட சோதனையை மேற்கொள்ளவும்.
  - DoS திசையன்களை (vectors) அடையாளம் காணவும், சரி செய்யவும், அதிக கோரிக்கைகளை வைத்து load testing சோதனையை மேற்கொள்ளவும்.

DoS தாக்குதல்களுக்குப் பதிலளித்தல்

DoS தாக்குதல்களுக்கு உங்கள் நிறுவனம் தயாராக இல்லை என்றால், DoS தாக்குதல்களின் போது மேலே உள்ள சில நடவடிக்கைகளை செயல்படுத்த நீங்கள் முயற்சி செய்யலாம், இருப்பினும் அப்படி செய்யும் போது செயல்திறன் குறைவானதாக இருக்கும் மற்றும் செயல்படுத்த நேரம் எடுக்கும். அதனால், உங்கள் நிறுவனம் DoS தாக்குதலுக்கு சரியான வகையில் பதிலளிக்க முடியாமல் போகலாம்.

DoS தாக்குதல்களின் போது, பொருத்தமான மற்றும் நடைமுறைக்கு சாத்தியமான விதத்தில் பின்வரும் நடவடிக்கைகளை உங்கள் நிறுவனம் செயல்படுத்த வேண்டும்.

- உங்களது சைபர் பாதுகாப்பு, பதிலளிப்பு திட்டத்தை செயல்படுத்துங்கள்.
- பதிலளிக்கக்கூடிய நடவடிக்கைகளை உடனடியாக செயல்படுத்த முடியுமா என்று உங்கள் சேவை வழங்குநர்களிடம் கேளுங்கள். பதிலளிக்கும் திறனை அதற்கு முன்னர் நீங்கள் அவர்களுடன் கலந்துரையாடவில்லை என்றால், அவர்களால் பதிலளிக்க முடியாமல் போகலாம், அல்லது அவர்களுக்கு அதில் விருப்பமில்லாமல் இருக்கலாம் அல்லது அதற்காக, கூடுதல் கட்டணம் வசூலிக்க விரும்பலாம்.
- DoS தாக்குதலை நடத்த அனுமதிக்கக்கூடிய விடயங்களில் முக்கியமற்ற செயல்பாடுகளை உங்கள் ஆன்லைன் சேவைகளிலிருந்து முடக்கவும் அல்லது முக்கியமற்ற உள்ளடக்கத்தை அகற்றவும். எடுத்துக்காட்டாக, தேடல் செயல்பாடு, மாறும் உள்ளடக்கம் அல்லது பெரிய கோப்புகள் இல்லாமல் உங்கள் வலைத்தளத்தின் பதிப்பை வெளியிடவும்.
- உங்கள் DoS தாக்குதல் தணிப்பு சேவை வழங்குநர் உட்பட உங்கள் வாடிக்கையாளர்கள் மற்றும் உங்கள் சேவை வழங்குநர்களுடன் தொடர்பைப் பேணவும். உங்கள் ஆன்லைன் சேவைகள் செயலில் இருக்கின்றனவா என்று தொடர்ந்து கண்காணிக்கவும்.
- உங்கள் மூல இணைய சேவையகத்தின் IP முகவரியை நேரடியாகக் குறிவைத்து தாக்குதல் நடத்தப்பட்டிருந்தால் அதை மாற்றுவதற்குத் திட்டமிடுங்கள். மேலும் பாதுகாப்புகள் இல்லாமல் புதிய IP முகவரியை பொது வெளியில் பகிரங்கப்படுத்துவதைத் தவிர்க்கவும்.
- நடந்த DoS தாக்குதல் குறித்து ASD மற்றும் NCSC-NZ உள்ளிட்ட, மற்றைய தொடர்புடைய தரப்பினருக்கும் அறிவிக்கவும். அவர்களுடைய 'தொடர்பு விவரங்கள்' இந்த வெளியீட்டில் தரப்பட்டுள்ளன.

DoS தாக்குதல்களுக்குப் பங்களிப்பதைத் தவிர்த்தல்

மற்றவர்களைப் பாதிக்கக்கூடிய DoS தாக்குதல்களுக்குத் தற்செயலாகப் பங்களிப்பதைத் தவிர்ப்பதற்காக, உங்கள் நிறுவனம் பின்வரும் நடவடிக்கைகளை நடைமுறைப்படுத்த வேண்டும்.

- தேவையற்ற, பாதுகாப்பற்ற முறையில் கட்டமைக்கப்பட்ட அல்லது போதுமானளவு பராமரிக்கப்படாத சேவைகள், IoT சாதனங்கள் மற்றும் பிற இணையத்துடன் இணைக்கப்பட்ட சாதனங்களை இணையத்திற்கு அம்பலப்படுத்துவதைத் தவிர்க்கவும்.

- இணையத்தில் பகிரங்கமாக வெளிப்படும் சேவைகள், IoT சாதனங்கள் மற்றும் பிற இணையத்துடன் இணைக்கப்பட்ட சாதனங்களைப் பாதுகாப்பாக உள்ளமைக்கவும், பராமரிக்கவும் மற்றும் கண்காணிக்கவும்.
  - சிறு வணிக நிறுவனங்களுக்கான, கூடுதல் வழிகாட்டுதல்கள் ASD வெளியிட்டுள்ள *Internet of Things devices* மற்றும் *Secure your Wi-Fi and router* என்ற வெளியீடுகளில் பிரசுரிக்கப்பட்டுள்ளன.

உங்கள் நிறுவனம் ஆன்லைன் சேவைகளை நடத்தினால், பின்வரும் கூடுதல் நடவடிக்கைகளை நீங்கள் செயல்படுத்த வேண்டும்.

- அமெரிக்காவின் சைபர் பாதுகாப்பு அமைப்பான Cyber security and Infrastructure Security Agency (CISA) வெளியிட்டுள்ள *UDP-Based Amplification Attacks* ஆலோசனையில் கோடிட்டுக் காட்டப்பட்டுள்ள நெறிமுறைகளை மதிப்பாய்வு செய்வதற்கு முன்னுரிமை அளிக்கவும்.
- புதிய பெருக்க திசையன்கள் (amplification vectors) அடையாளம் காணப்படுவதால், அவற்றைக் கண்காணித்து, அவற்றுக்கு எதிராக உங்கள் ஆன்லைன் சேவைகளைப் பாதுகாக்கவும்.
- அங்கீகரிக்கப்பட்ட ஆன்லைன் சேவைகள் மற்றும் நிறுவனங்கள் மட்டும் உள்வரும் மற்றும் வெளிச்செல்லும் நெட்வொர்க் அணுகலைச் செய்யக் கூடியதாக கட்டுப்பாடுகளை உள்ளமைக்கவும்.
- தேவைப்பட்டால், அதிக கோரிக்கைகள் வந்தால் பாதிக்கப்படக்கூடிய ஆன்லைன் சேவைகளை, அடையாளம் காணப்படாத அநாமதேய பொது அணுகல் மூலம் பெறுவதை தடுக்கவும்.
- அணுகல் கட்டுப்பாடுகளைத் தடுப்பது அல்லது பயன்படுத்துவது சாத்தியமில்லை அல்லது பொருத்தமானதாக இல்லாவிட்டால், தவறான முறையில் அணுகுவதால் ஏற்படும் விளைவுகளைக் குறைக்க எத்தனை முறை கோரிக்கை வந்தது என்பதற்கான விகித-வரம்பு பொறிமுறையை செயல்படுத்துவதைக் கருத்தில் கொள்ளுங்கள்.

மேலும் தகவலுக்கு

நிறுவனங்கள் தங்கள் அமைப்புகள் மற்றும் தரவை சைபர் அச்சுறுத்தல்களிலிருந்து பாதுகாக்க, ASD வெளியிட்டுள்ள *Information security manual* என்ற பிரசுரத்தைப் பயன்படுத்தலாம். *Strategies to mitigate cyber security incidents* என்ற பிரசுரத்திலும், குறிப்பாக Essential Eight என்பதிலும் , கூறப்பட்டுள்ள ஆலோசனை பயனுள்ளவை.

நியூசிலாந்து அரசின் தகவல் உத்தரவாதம் மற்றும் தகவல் அமைப்புகள் பாதுகாப்பு பற்றிய கையேடு *New Zealand Information Security Manual*. தகவல் பாதுகாப்பு நிர்வாகிகள், விற்பனையாளர்கள், ஒப்பந்தக்காரர்கள் மற்றும் ஏஜென்சிகளுக்கு சேவைகளை வழங்கும் ஆலோசகர்களின் தேவைகளைப் பூர்த்தி செய்ய வடிவமைக்கப்பட்ட ஒரு பயிற்சியாளர் கையேடு இது.

பல்வேறு DoS தாக்குதல் வகைகள் பற்றிய கூடுதல் தகவல்கள் CISA வெளியிட்டுள்ள *DDoS Quick Guide* மற்றும் *Understanding and Responding to Distributed Denial-Of-Service Attacks* என்ற வெளியீடுகளில் கிடைக்கின்றன.

தொடர்பு விபரங்கள்

இந்த வழிகாட்டுதல் குறித்து, ஏதேனும் கேள்விகள் இருந்தால் *ASD* ற்கு எழுதவும் அல்லது ஆஸ்திரேலியாவில் 1300 CYBER1 (1300 292 371) என்ற இலக்கத்தை அழைக்கவும்.

சைபர் பாதுகாப்பு சம்பவம் குறித்து நியூசிலாந்தில் புகாரளிக்க incidents@ncsc.govt.nz ற்கு மின்னஞ்சல் அனுப்பவும் அல்லது NCSC-NZ இன் Report an incident இணையத் தளத்தைப் பார்க்கவும்.

பொறுப்புத் துறப்பு

இந்த வழிகாட்டியில் கூறப்பட்டுள்ள விடயங்கள் பொதுவானவை. அவை சட்ட ஆலோசனையாகக் கருதப்படக்கூடாது. மேலும், எந்தவொரு குறிப்பிட்ட சூழ்நிலையில் அல்லது அவசரகால சூழ்நிலையில் நேரடியாக உதவும் என்று நம்பக்கூடாது. எந்தவொரு முக்கியமான விடயத்திலும், உங்கள் சொந்த சூழ்நிலைகள் தொடர்பாக தகுந்த சுயாதீனமான தொழில்முறை ஆலோசனையை நீங்கள் நாட வேண்டும்.

இந்த வழிகாட்டியில் உள்ள தகவல்களை நம்பியதன் விளைவாக ஏற்படும் எந்தவொரு சேதம், இழப்பு அல்லது செலவுக்கும் ஆஸ்திரேலிய காமன்வெல்த் அரசு எந்த பொறுப்பையும் ஏற்காது.

பதிப்புரிமை

ஆஸ்திரேலிய அரசின் Coat of Arms வகை இலச்சினையின் பயன்பாடு

ஆஸ்திரேலிய அரசின் Coat of Arms வகை இலச்சினை எந்தெந்த விதிமுறைகளின் கீழ் பயன்படுத்தப்படலாம் என்பது, பிரதமர் துறை மற்றும் அமைச்சரவையின் Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au என்ற இணையதளத்தில் விரிவாக உள்ளது.

மேலும் தகவலுக்கு அல்லது இணைய பாதுகாப்பு முறியடிக்கப்பட்ட நிகழ்வு குறித்துப் புகாரளிக்க, எங்களைத் தொடர்பு கொள்ளவும்:

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

இந்த எண்ணை ஆஸ்திரேலியாவிற்குள் மட்டுமே பயன்படுத்த முடியும்.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre