डिनाएल-ऑफ-सर्विस हमलों के लिए तैयारी करना और उत्तर देना

पहली बार प्रकाशित: सितंबर 2011
पिछला अपडेट: मार्च 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

परिचय

यह प्रकाशन हमारे क्षेत्र में डिनाएल-ऑफ-सर्विस (डीओएस) हमलों में बढ़ते हुए रुझान के प्रत्युत्तर में इनके सहयोग से विकसित किया गया था: ऑस्ट्रेलियाई सिग्नल्स निदेशालय (एएसडी), न्यू ज़ीलैंड राष्ट्रीय साइबर सुरक्षा केंद्र (एनसीएससी-एनज़ेड), अकामाई टेक्नोलॉजीस लि. और क्लाउडफ्लेयर प्रो. लि। यह संगठनों को समकालीन थ्रेट ट्रेडक्राफ्ट के आधार पर सर्वोत्तम शमन कार्यप्रथाओं के बारे में मार्गदर्शन देता है, ताकि डीओएस हमलों के लिए तैयारी की जा सके और उनका जवाब दिया जा सके।

हम इस परामर्श को एएसडी के इंटरनेट ऑफ थिंग्स डिवाइस और सिक्योर यॉर वाई-फाई व राउटर प्रकाशनों के संयोजन में पढ़ने की सलाह देते हैं। ये प्रकाशन व्यक्तियों को अनजाने में डीओएस हमलों में योगदान करने से सुरक्षित रहने में सहायता देते हैं, जिससे अन्य लोग प्रभावित हो सकते हैं।

डीओएस हमले वैध उपयोगकर्ताओं को एक्सेस न देने के उद्देश्य से ऑनलाइन सेवाओं में हस्तक्षेप करने या बाधा डालने के लिए डिज़ाइन किए गए साइबर हमले होते हैं, जैसे वेबसाइटें, ईमेल और डोमेन नेम सिस्टम (डीएनएस) सेवाएँ। यह आमतौर पर किसी ऑनलाइन सेवा के प्रति अत्यधिक डेटा, कनेक्शन्स या रिक्वेस्ट्स भेजकर हासिल किया जाता है, ताकि वह सेवा अभिभूत हो जाए और उसकी कार्यात्मकता कम हो जाए।

डीओएस हमलों को सफल होने के लिए आमतौर पर बड़ी मात्रा में नेटवर्क ट्रैफ़िक की आवश्यकता होती है। ये तेजी से आम होते जा रहे हैं, आंशिक रूप से इसलिए क्योंकि आसानी से हस्तक्षेप किए जाने वाले इंटरनेट ऑफ थिंग्स (आईओटी) डिवाइसेज़ की संख्या में बढ़ौत्तरी हो रही है। आईओटी निर्माता अक्सर साइबरसिक्योरिटी की तुलना में उपयोगकर्ता के अनुभव को प्राथमिकता देते हैं, इसलिए अतिसंवेदनशील डिवाइसेज़ में इंटरनेट से कनेक्ट करने वाले नियमित घरेलू साजो-सामान शामिल हो सकते हैं, जैसे स्मार्ट टीवी, केतलियाँ, वैक्यूम क्लीनर्स और सुरक्षा प्रणालियाँ। दुर्भावनापूर्ण हमलावरों द्वारा अक्सर इन डिवाइसेज़ में डिवाइसेज़ का एक 'बॉटनेट' बनाने के लिए दूरस्थ रूप से हस्तक्षेप किया जा सकता है, ताकि यह नेटवर्क ट्रैफ़िक पैदा किया जा सके। इसके परिणामस्वरूप घरबारों और संगठनों से अनजाने में ही इन्फ्रास्ट्रक्चर में योगदान दिया जा सकता है, जिससे डीओएस हमले कर पाने की अनुमति मिलती है।

हाल की गतिविधि इंगित करती है कि एक बार जब दुर्भावनापूर्ण हमलावर बड़ी संख्या में आईओटी डिवाइसेज़ में हस्तक्षेप कर लेते हैं, तो वे इस इन्फ्रास्ट्रक्चर को साइबर अपराधियों और हैकटिविस्टों को किराए पर दे सकते हैं या उन्हें बेच सकते हैं, जिनमें अपने चयनित लक्ष्यों के प्रति डीओएस हमले करने में रुचि बढ़ती जा रही है। अधिकांश मामलों में डीओएस हमले इसलिए किए जाते हैं, ताकि किसी संगठन की उत्पादकता में घटौती और आर्थिक नुकसान पैदा किया जा सके या किसी दृष्टिकोण के प्रति जनता का ध्यान आकर्षित किया जा सके। इस गतिविधि के एक उदाहरण का विवरण एएसडी की इस परामर्श-सूचना में दिया

गया है: पीपल्स रिपब्लिक ऑफ चाइना से जुड़े हमलावर बोटनेट ऑपरेशंस के लिए राउटर्स और आईओटी डिवाइसेज़ में हस्तक्षेप कर रहे हैं।

जैसे-जैसे हमारी अर्थव्यवस्था और भी अधिक डिजिटल बनती जा रही है और इंटरनेट से जुड़े कमतर सुरक्षा वाले आईओटी डिवाइसेज़ की संख्या बढ़ती जा रही है, वैसे-वैसे डीओएस हमलों में बढ़ौत्तरी जारी रहने की संभावना है।

किसी संगठन की ऑनलाइन सेवाओं को बाधित या कमतर करने के लिए दुर्भावनापूर्ण हमलावर कई तरीकों का उपयोग करते हैं, जिनमें शामिल हैं:

- उपलब्ध संपूर्ण नेटवर्क बैंडविड्थ का उपयोग करने के प्रयास में ऑनलाइन सेवाओं के प्रति बड़ी मात्रा में अवांछित नेटवर्क ट्रैफ़िक निर्देशित करना
- ऑनलाइन सेवाओं के कंप्यूटर प्रोसेसिंग संसाधनों का उपयोग करने के प्रयास में उनके प्रति अनुरूपित नेटवर्क ट्रैफ़िक निर्देशित करना
- एकाधिक कंप्यूटरों, आईओटी डिवाइसेज़ या इंटरनेट से जुड़े अन्य डिवाइसेज़ का उपयोग करके ऑनलाइन सेवाओं के प्रति एकाधिक दिशाओं से और बहुत बड़े पैमाने पर नेटवर्क ट्रैफ़िक निर्देशित करना, जोकि डिस्ट्रिब्यूटेड डीओएस (डीडीओएस) हमले के नाम से संदर्भित किया जाने वाला एक सामान्य प्रकार का डीओएस हमला है
- वैध उपयोगकर्ताओं को किसी संगठन की ऑनलाइन सेवाओं से दूर निर्देशित करने के प्रयास में संगठन के डोमेन रजिस्ट्रेशन या डीएनएस सर्वर को हाइजैक करना।

संगठन डीओएस हमलों का लक्ष्य बनने से बच नहीं सकते हैं, लेकिन तैयारी करने और संभावित रूप से हमलों का असर कम करने के लिए कई तरह के कदम उठा सकते हैं। डीओएस हमले किए जाने से पहले ही तैयारी करना सबसे अच्छी कार्यनीति है, क्योंकि तैयारी के बिना डीओएस हमले के दौरान प्रतिक्रिया करना कठिन और कम प्रभावी होता है।

संगठन मुख्यतः खुद को डीओएस हमलों से बचाने पर फोकस करते हैं, लेकिन दुर्भावनापूर्ण हमलावरों द्वारा उनकी ऑनलाइन सेवाओं और इंटरनेट से जुड़े डिवाइसेज़ को दूसरों को लक्ष्य बनाने के उद्देश्य से दुरुपयोग किए जाने से रोकने के लिए भी उन्हें कदम उठाने चाहिए।

डीओएस हमलों के लिए तैयारी करना

हमारे क्षेत्र में डीओएस हमलों की बढ़ती हुई संख्या के संदर्भ में डीओएस हमलों के लिए तैयारी करने के किसी भी कदम को लागू करने से पूर्व आपके संगठन को पहले यह तय करने के लिए अपनी व्यावसायिक आवश्यकताओं का आकलन करना चाहिए कि क्या आपकी प्रत्येक ऑनलाइन सेवा को डीओएस हमलों के दौरान चालू रखना अनिवार्य है, या सेवा में अस्थायी रुकावटें स्वीकार्य हैं।

यदि आपका संगठन डीओएस हमलों का सामना करने की अपनी क्षमता बढ़ाना चाहता है, तो आपको डीओएस हमले किए जाने से पहले, जहां उपयुक्त और व्यावहारिक हो, निम्नलिखित कदमों को पूर्वक्रियात्मक रूप से लागू करना चाहिए।

- यदि आपका संगठन कन्टेंट डिलीवरी नेटवर्क (सीडीएन) का उपयोग कर रहा है, तो जहाँ उपयुक्त और व्यावहारिक हो, आपको निम्नलिखित अतिरिक्त कदम लागू करने चाहिए।
  - अपने ओरिजिन वेब सर्वर को अलग-अलग तरह के एप्लिकेशन और नेटवर्क लेयर हमलों से बचाने में कार्यक्षम सीडीएन का उपयोग करने पर विचार करें - कुछ सीडीएन इन सुविधाओं को वेब एप्लिकेशन फायरवॉल के किनारे पर उसके हिस्से के रूप में इसे शामिल कर सकते हैं।
  - अपने मूल वेब सर्वर के इंटरनेट प्रोटोकॉल (आईपी) एड्रेस का सार्वजनिक रूप से अनावश्यक खुलासा न होने का प्रयास करें, और डीओएस हमलों के खतरे से सभी सार्वजनिक खुलासों को सुरक्षित रखना सुनिश्चित करें।
  - अपने मूल वेब सर्वर के लिए किसी ऐसे आईपी एड्रेस का उपयोग न करने का प्रयास करें, जिसके लिए दुर्भावनापूर्ण हमलावर अनुमान लगा सकते हैं, उदाहरण के लिए, आपकी ऑनलाइन सेवाओं के सार्वजनिक रूप से प्रकट आईपी एड्रेस के एक ही नेटवर्क सबनेट में आईपी एड्रेस।
  - नेटवर्क एक्सेस कंट्रोल्स (जैसे फायरवॉल) का उपयोग करके सुनिश्चित करें कि केवल सीडीएन और आपके संगठन द्वारा प्राधिकृत मैनेजमेंट नेटवर्क ही आपके ओरिजिन वेब सर्वर को एक्सेस कर सकें।
  - यदि आपको अपने ओरिजिन वेब सर्वर के लिए ऊंचे स्तर की सुरक्षा की आवश्यकता है, तो लचीली और विविध नेटवर्क कनेक्टिविटी का उपयोग करने के बारे में सोचें, जिसमें आपके ओरिजिन वेब सर्वर और आपके सीडीएन प्रदाता के बीच प्राइवेट नेटवर्क कनेक्टिविटी शामिल हो सकती है।

  - कैशे में रखी जाने वाली मात्रा को ऑप्टिमाइज़ करने के लिए सीडीएन, ओरिजिन वेब सर्वर और क्लाइंट एचटीटीपी हेडर्स को कॉन्फिगर करें।
  - यदि आपको ऊंचे स्तर की उपलब्धता की आवश्यकता है, तो ओरिजिन वेब सर्वर्स को पार्टिशन करने के बारे में सोचें, ताकि कम खतरे वाले आईपी एड्रेसेज़ से आने वाली रिक्वेस्ट्स और ऊंचे खतरे वाले आईपी एड्रेसेज़ से आने वाली रिक्वेस्ट्स को अलग-अलग हैंडल किया जा सके।
- यह तय करें कि आपकी ऑनलाइन सेवाओं के वैध उपयोगकर्ताओं के लिए कौन सी फंक्शनैलिटी और सेवाओं की क्वॉलिटी स्वीकार्य है, उस फंक्शनैलिटी को कैसे बनाए रखा जाए, और डीओएस हमलों के दौरान कौन सी फंक्शनैलिटी आवश्यक नहीं है।
- एक क्लाउड-बेस्ड डीओएस एटैक मिटिगेशन सर्विस खरीदें और उसका इस्तेमाल करें।
- अपने संगठन में हमले की सतह को कम करने के लिए इन तरीकों पर विचार करें:
  - डीओएस हमलों का सामना करने में सक्षम प्रतिष्ठित सेवा प्रदाताओं को मूलभूत ऑनलाइन सेवाएं (जैसे डीएनएस) आउटसोर्स करना
  - महत्वपूर्ण ऑनलाइन सेवाओं (जैसे ईमेल) और लक्षित किए जाने की अधिक संभावना वाली अन्य ऑनलाइन सेवाओं (जैसे वेबसाइटों) के बीच पार्टिशन करना
  - यह सुनिश्चित करना कि डीओएस एटैक मिटिगेशन सर्विस केवल ऑनलाइन सेवा के नेटवर्क पोर्ट(र्ट्स) से जुड़े नेटवर्क ट्रैफ़िक को ही अनुमति दे।
- अपने सेवा प्रदाताओं के साथ डीओएस हमले की रोकथाम और मिटिगेशन के लिए उनके कदमों के विवरणों के बारे में चर्चा करें, विशेषकर उनकी:
  - दुनिया-भर से डीओएस हमलों का सामना करने की सिद्ध क्षमता
  - डीओएस हमलों और व्यापक प्राधिकृत डीओएस हमला टेस्टिंग, इन दोनों की हैंडलिंग करने का प्रदर्शित इतिहास
  - मानव भागीदारी के बिना अधिकांश प्रकार के डीओएस हमलों को स्वत: कम करने की क्षमता, जैसे उनकी सेवाओं के मूल्य-निर्धारण के लिए नेटवर्क ट्रैफ़िक एप्रोच का मैन्युल विश्लेषण
  - सेवाओं के लिए मूल्य निर्धारण एप्रोच, उदाहरण के लिए कि क्या शुल्क निश्चित हैं या क्या ये उपयोग किए गए नेटवर्क ट्रैफ़िक और कंप्यूटर प्रोसेसिंग संसाधनों की मात्रा के आधार पर परिवर्तनशील हो सकते हैं, और क्या आप बिलिंग सीमाएँ लागू कर सकते/ती हैं
  - क्या थ्रेसहोल्ड्स हैं, ताकि डीओएस हमलों के दौरान आपको सूचित किया जा सके या उनकी ऑनलाइन सेवाएं बंद की जा सकें
  - डीओएस हमलों के दौरान उठाए जा सकने वाले पूर्व-अनुमोदित कदम
  - अपस्ट्रीम प्रदाताओं के साथ डीओएस हमलों की रोकथाम के लिए व्यवस्थाएँ।
- डीओएस हमलों का पता लगाने के लिए कदम लागू करें, जैसे रियल टाइम में निगरानी और सिस्टम उपलब्धता, नेटवर्क ट्रैफ़िक, कंप्यूटर प्रोसेसिंग संसाधनों व संबद्ध शुल्कों के बारे में चेतावनी।
- अपनी वेबसाइट का एक अपरिवर्तनीय संस्करण तैयार करें, जिसमें डीओएस हमलों के दौरान सेवा की निरंतरता को सुविधाकृत करने के लिए न्यूनतम प्रोसेसिंग और बैंडविड्थ की आवश्यकता हो।
- अवांछनीय नेटवर्क ट्रैफ़िक को हटाने के लिए अत्यधिक बैंडविड्थ, पर्याप्त मात्रा में कंप्यूटर प्रोसेसिंग संसाधन, भौगोलिक रूप से बिखरे हुए होस्टिंग स्थल और क्लाउड-बेस्ड ट्रैफ़िक स्क्रबिंग वाली अत्यधिक लचीली ऑनलाइन सेवाएँ खरीदें और इस्तेमाल करें - आमतौर पर इसमें अपरिवर्तनशील वेबसाइट सामग्री को कैशे में रखने और अपने ओरिजिन वेब सर्वर को अवांछित नेटवर्क ट्रैफ़िक से बचाने के लिए किसी प्रतिष्ठित सीडीएन का उपयोग करना शामिल होता है।
- रजिस्ट्रार लॉकिंग के उपयोग, डोमेन रजिस्ट्रेशन संपर्क विवरणों की पुष्टि और अन्य विवरणों के सत्यापन, तथा एएसडी के डोमेन ओनर्स के लिए डोमेन नेम सिस्टम सुरक्षा प्रकाशन में दिए गए अतिरिक्त मार्गदर्शन का पालन करने के माध्यम से अपने संगठन के डोमेन नेम्स को संरक्षित बनाएं।
- अपने सेवा प्रदाताओं के अप-टु-डेट संपर्क विवरण बनाए रखें और उनके साथ अपने संगठन के संपर्क विवरणों को साझा करें तथा यह सुनिश्चित करें कि आपके संगठन की आवश्यकताओं के आधार पर सभी संपर्क उपलब्ध रहते हैं, उदाहरण के लिए, दिन में 24 घंटे, सप्ताह में 7 दिन।
- सामान्य संचार चैनलों के विफल होने की स्थिति में अपने सेवा प्रदाताओं को एक भरोसेमंद संचार चैनल उपलब्ध कराने के लिए उन्हें अपने संगठन के आउट-ऑफ-बैंड संपर्क विवरण दें।

- एक साइबर सुरक्षा घटना प्रतिक्रिया योजना को विकसित, लागू और बनाए रखें, जिसमें डीओएस हमलों का सामना करने की आवश्यकता वाली आपकी प्रत्येक ऑनलाइन सेवाओं के प्रति अलग-अलग तरह के डीओएस हमले शामिल किए गए हों, और कम से कम सालाना रूप से इस योजना का अभ्यास करें।
- सामान्य रूप से दुरुपयोग की जाने वाली ऐसी फंक्शनैलिटी के सरंक्षण के लिए एप्लिकेशन्स का आर्किटेक्चर बनाएँ, जो अधिक कंप्यूटर प्रोसेसिंग संसाधनों का उपयोग करती है या अतिरिक्त आर्थिक लागतें बढ़ाती है (जैसे एसएमएस मैसेजेस भेजना)।
  - इन संरक्षणों में दरों पर सीमाएँ लगाना और मानव की ओर से रिक्वेस्ट्स आने के लिए सत्यापन करना शामिल है।
  - डीओएस हमलों के लिए टेस्टिंग करें, जिसमें एप्लिकेशन्स फंक्शनैलिटी में अनुचित लॉजिक फ्लो को लक्षित करना भी शामिल है।
  - डीओएस वैक्टर्स की पहचान करने और उन्हें दुरुस्त करने के लिए अधिक व्यापक लोड टेस्टिंग करें।

डीओएस हमलों का उत्तर देना

यदि आपका संगठन डीओएस हमलों के लिए तैयार नहीं है, तो आप डीओएस हमलों के दौरान उपरोक्त कुछ कदम लागू करने का प्रयास कर सकते/ती हैं; लेकिन ये कम प्रभावी हो सकते हैं और लागू होने में समय ले सकते हैं, जिससे आपके संगठन की प्रतिक्रिया क्षमता कम हो सकती है।

जहाँ उपयुक्त और व्यावहारिक हो, आपके संगठन को डीओएस हमलों के दौरान निम्नलिखित कदम लागू करने चाहिए।

- अपनी साइबर सुरक्षा घटना प्रतिक्रिया योजना लागू करें।
- अपने सेवा प्रदाताओं से पूछें कि क्या वे उत्तर देने वाले कदमों को तुरंत लागू करने में सक्षम हैं - यदि आपने उत्तर देने की उनकी क्षमता पर पहले चर्चा नहीं की है, तो आपको पता चल सकता है कि क्या वे उत्तर देने में असमर्थ या अनिच्छुक हैं, या अतिरिक्त शुल्क लेते हैं।
- वर्तमान डीओएस हमले को प्रभावी बनाने वाली महत्वहीन फंक्शनैलिटी को अक्षम कर दें या अपनी ऑनलाइन सेवाओं से महत्वहीन सामग्री को हटा दें, उदाहरण के लिए, अपनी वेबसाइट का ऐसा संस्करण लागू करें, जो सर्च फंक्शनैलिटी, डायनैमिक कन्टेंट या बड़ी फाइलों से मुक्त हो।
- अपने ग्राहकों और अपने सेवा प्रदाताओं के साथ संचार बनाए रखें, जिसमें आपका डीओएस हमला मिटिगेशन सेवा प्रदाता भी शामिल है, और अपनी ऑनलाइन सेवाओं की उपलब्धता की निगरानी जारी रखें।
- यदि आपके ओरिजिन वेब सर्वर के आईपी एड्रेस को सीधे लक्षित किया जा रहा है, तो इसे बदलने के बारे में सोचें और सुरक्षात्मक कदमों को लागू किए बिना नए आईपी एड्रेस का सार्वजनिक रूप से प्रकट न होने का प्रयास करें।
- इस प्रकाशन के 'संपर्क विवरण' अनुभाग के निर्देशानुसार संगत पक्षों के पास डीओएस हमले की रिपोर्ट करें, जिसमें एएसडी और एनसीएससी-एनज़ेड शामिल हैं।

डीओएस हमलों में योगदान देने से बचें

अनजाने में दूसरों को प्रभावित कर सकने वाले डीओएस हमलों के प्रति योगदान देने से बचने के लिए आपके संगठन को निम्नलिखित कदम लागू करने चाहिए।

- अनावश्यक, असुरक्षित रूप से कॉन्फिगर की गई और अपर्याप्त रख-रखाव वाली सेवाओं, आईओटी डिवाइसेज़ और इंटरनेट से जुड़े अन्य डिवाइसेज़ का इंटरनेट पर खुलासा न होने का प्रयास करें।
- सेवाओं, आईओटी डिवाइसेज़ और इंटरनेट से जुड़े अन्य डिवाइसेज़ को सुरक्षित रूप से कॉन्फिगर करें और उनका रख-रखाव व निगरानी करें।
  - छोटे व्यवसायों के लिए अतिरिक्त मार्गदर्शन एएसडी के इंटरनेट ऑफ थिंग्स डिवाइसेज़ तथा अपने वाई-फाई और राउटर को सुरक्षित करें प्रकाशनों में उपलब्ध है।

यदि आपका संगठन ऑनलाइन सेवाएँ उपलब्ध करा रहा है, तो आपको निम्नलिखित अतिरिक्त कदम लागू करने चाहिए।

- संयुक्त राज्य अमेरिका की साइबर सुरक्षा एवं इंफ्रास्ट्रक्चर सुरक्षा एजेंसी (सीआईएसए) की यूडीपी-बेस्ड एंप्लिफिकेशन अटैक्स परामर्श-सूचना में दी गई प्रोटोकॉल्स की समीक्षा को प्राथमिकता दें।
- जैसे-जैसे नए एंप्लिफिकेशन वेक्टर्स पहचाने जाते हैं, उनकी निगरानी करें और अपनी ऑनलाइन सेवाओं को संरक्षित करें।
- प्राधिकृत ऑनलाइन सेवाओं और संगठनों की एक्सेस को सीमित करने के लिए इनबाउंड और आउटबाउंड नेटवर्क एक्सेस नियंत्रणों, इन दोनों को कॉन्फिगर करें।
- एंप्लिफिकेशन-प्रोन ऑनलाइन सेवाओं की अनाम सार्वजनिक एक्सेस को रोकें, यदि ये आवश्यक न हों।
- यदि रोकना या एक्सेस नियंत्रण लागू करना संभव या उचित न हो, तो दुरुपयोग के परिणामों को कम करने के लिए दर-सीमित तंत्र लागू करने के बारे में सोचें।

आगे पढ़ें

एएसडी का जानकारी सुरक्षा मैनुअल एक साइबर सुरक्षा फ्रेमवर्क है, जिसे संगठन अपने सिस्टम और डेटा को साइबर खतरों से बचाने के लिए लागू कर सकते हैं। साइबर सुरक्षा घटनाओं को कम करने की कार्यनीतियाँ, और साथ ही आठ अनिवार्यताओं में दिया गया परामर्श इस फ्रेमवर्क का संपूरक है।

न्यू ज़ीलैंड जानकारी सुरक्षा मैनुअल इन्फोर्मेशन एश्योरेंस और इन्फोर्मेशन सिस्टम्स सुरक्षा के बारे में न्यू ज़ीलैंड सरकार का मैनुअल है। पेशेवरों के लिए इस मैनुअल को एजेंसी जानकारी संरक्षण कार्यकारियों के साथ-साथ एजेंसियों को सेवाएं प्रदान करने वाले विक्रेताओं, ठेकेदारों और सलाहकारों की आवश्यकताओं को पूरा करने के लिए भी डिज़ाइन किया गया है।

अलग-अलग प्रकार के डीओएस हमलों के बारे में और अधिक जानकारी सीआईएसए के डीडीओएस त्वरित संदर्शिका और डिस्ट्रिब्युटेड डिनाएल-ऑफ-सर्विस अटैक्स हमलों को समझना और उनका उत्तर देना प्रकाशनों में उपलब्ध है।

संपर्क विवरण

ऑस्ट्रेलिया में, यदि आपके पास इस मार्गदर्शन के बारे में कोई प्रश्न हैं, तो एएसडी को पत्र लिखें या 1300 CYBER1 (1300 292 371) पर कॉल करें।

न्यू ज़ीलैंड में, साइबर सुरक्षा घटना की रिपोर्ट करने के लिए incidents@ncsc.govt.nz पर ईमेल भेजें या या एनसीएससी-एनज़ेड घटना की रिपोर्ट करें वेबपेज पर जाएँ।

अस्वीकरण

इस संदर्शिका में दी गई सामग्री सामान्य प्रकृति की है और इसे कानूनी सलाह के रूप में नहीं लिया जाना जाना चाहिए अथवा किसी विशेष परिस्थिति या आपात स्थिति में इसपर सहायता के लिए भरोसा नहीं किया जाना चाहिए। किसी भी महत्वपूर्ण मामले में आपको अपनी परिस्थितियों के संबंध में उपयुक्त स्वतंत्र पेशेवर सलाह लेनी चाहिए।

इस संदर्शिका में निहित जानकारी पर निर्भरता के परिणामस्वरूप होने वाले किसी भी क्षति, हानि या खर्चे के लिए राष्ट्रमंडल कोई भी जिम्मेदारी या दायित्व स्वीकार नहीं करता है।

और अधिक जानकारी या किसी साइबर सुरक्षा की रिपोर्ट करने के लिए हमसे संपर्क करें:

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

यह नंबर केवल ऑस्ट्रेलिया में उपयोग के लिए उपलब्ध है।

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre