भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या 2537
जिसका उत्तर 11 दिसंबर, 2024 को दिया जाना है।
20अग्रहायण, 1946 (शक)

साइबर हमलों का बढ़ता खतरा

2537.श्री दीपक अधिकारी (देव):

क्या **इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री** यह बताने की कृपा करेंगे कि:

सरकार साइबर हमलों के बढ़ते खतरे से किस प्रकार निपट रही है तथा महत्वपूर्ण बुनियादी ढांचे, वित्तीय प्रणाली और व्यक्तिगत डेटा की साइबर सुरक्षा सुनिश्चित कर रही है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए एक स्वतंत्र, सुरक्षित, विश्वसनीय और जवाबदेह इंटरनेट सुनिश्चित करना है। सरकार विभिन्न साइबर खतरों और चुनौतियों के बारे में पूरी तरह से जागरूक और सजग है। देश की साइबर सुरक्षा स्थिति को मजबूत करने और महत्वपूर्ण बुनियादी ढांचे, वित्तीय प्रणाली और व्यक्तिगत डेटा की सुरक्षा सुनिश्चित करने के लिए सरकार ने कई प्रमुख पहल की हैं जिनमें अन्य बातों के साथ-साथ निम्नलिखित भी शामिल हैं:

i. भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) को सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ख के प्रावधानों के तहत साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है।

ii. सर्ट-इन द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) देश में साइबरस्पेस को स्कैन करने और साइबर सुरक्षा खतरों का पता लगाने के लिए नियंत्रण कक्ष के रूप में कार्य करता है। एनसीसीसी साइबर सुरक्षा खतरों को कम करने के लिए कार्रवाई करने के लिए साइबरस्पेस से मेटाडेटा साझा करके विभिन्न एजेंसियों के बीच समन्वय की सुविधा प्रदान करता है।

iii. साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना तैयार की है जिसका कार्यान्वयन केंद्र सरकार के सभी मंत्रालयों/विभागों, राज्य सरकारों और उनके संगठनों तथा महत्वपूर्ण क्षेत्रों द्वारा किया जाएगा।

iv. सरकार ने सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70क के प्रावधानों के तहत देश में महत्वपूर्ण सूचना बुनियादी ढांचे की सुरक्षा के लिए राष्ट्रीय महत्वपूर्ण सूचना बुनियादी ढांचा संरक्षण केंद्र (एनसीआईआईपीसी) की स्थापना की है।

v. एनसीआईआईपीसी साइबर हमलों और साइबर आतंकवाद से बचाव के उपाय करने के लिए महत्वपूर्ण सूचना अवसंरचना (सीआईआई)/संरक्षित प्रणालियों (पीएस) वाले संगठनों को खतरे की खुफिया जानकारी, स्थितिजन्य जागरूकता, अलर्ट और सलाह तथा कमजोरियों के बारे में जानकारी प्रदान करता है। यह इन संगठनों को मांगने परसाइबर सुरक्षा से संबंधित सलाह भी प्रदान करता है।

vi. कंप्यूटर सुरक्षा घटना प्रतिक्रिया दल-वित्त क्षेत्र (सीएसआईआरटी-फिन) की स्थापना सर्ट-इन के तत्वावधान और मार्गदर्शन में वित्तीय क्षेत्र से रिपोर्ट की गई साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने, उन्हें रोकने और कम करने के लिए की गई है।

vii. सर्ट-इन एक स्वचालित साइबर खतरा खुफिया आदान-प्रदान मंच संचालित करता हैजो सक्रिय रूप से विभिन्न क्षेत्रों के संगठनों के साथ अलर्ट एकत्रित करने, उनका विश्लेषण करने और साझा करने के लिए कार्य करता है ताकि वे सक्रिय रूप से खतरा न्यूनीकरण कार्रवाई कर सकें।

viii. साइबर स्वच्छता केंद्र (सीएसके) सर्ट-इन द्वारा प्रदान की जाने वाली एक नागरिक-केंद्रित सेवा हैजो स्वच्छ भारत के दृष्टिकोण को साइबर स्पेस तक विस्तारित करती है। साइबर स्वच्छता केंद्र बॉटनेट क्लीनिंग और मैलवेयर विश्लेषण केंद्र है और दुर्भावनापूर्ण प्रोग्रामों का पता लगाने में मदद करता है और उन्हें हटाने के लिए निःशुल्क उपकरण प्रदान करता है और नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और सर्वोत्तम अभ्यास भी प्रदान करता है ।

ix. सर्ट-इन कंप्यूटर, मोबाइल फोन, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/कमजोरियों और प्रतिउपायों के संबंध में निरंतर अलर्ट और सलाह जारी करता है।

x. सर्ट-इन ने अप्रैल 2022 में सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70खकी उपधारा (6) के तहत सुरक्षित एवं विश्वसनीय इंटरनेट के लिए सूचना सुरक्षा प्रथाओं, प्रक्रिया, रोकथाम, प्रतिक्रिया और साइबर घटनाओं की रिपोर्टिंग से संबंधित साइबर सुरक्षा निर्देश जारी किए।

xi. सर्ट-इन ने जून 2023 में सरकारी संस्थाओं के लिए सूचना सुरक्षा प्रथाओं पर दिशानिर्देश जारी किए, जिसमें डेटा सुरक्षा, नेटवर्क सुरक्षा, पहचान और पहुंच प्रबंधन, एप्लिकेशन सुरक्षा, तृतीय-पक्ष आउटसोर्सिंग, सख्त प्रक्रियाएं, सुरक्षा निगरानी, घटना प्रबंधन और सुरक्षा ऑडिटिंग जैसे डोमेन शामिल हैं।

xii. सर्ट-इन ने सितंबर 2023 में सुरक्षित एप्लिकेशन डिजाइन, विकास और कार्यान्वयन और संचालन के लिए दिशानिर्देश जारी किए। सर्ट-इन ने अक्टूबर 2024 में संस्थाओं, विशेष रूप से सार्वजनिक क्षेत्र, सरकार, आवश्यक सेवाओं, सॉफ्टवेयर निर्यात और सॉफ्टवेयर सेवा उद्योग में शामिल संगठनों के लिए सॉफ्टवेयर बिल ऑफ मैटेरियल्स (एसबीओएम) दिशानिर्देश भी जारी किए हैं ताकि संगठनों को यह जानने में मदद मिल सके कि उनके सॉफ्टवेयर या परिसंपत्तियों में कौन से घटक हैं जिससे कमजोरियों की पहचान करना और उन्हें ठीक करना आसान हो जाता है।

xiii. सर्ट-इन ने नवंबर 2023 में विभिन्न मंत्रालयों को एक परामर्श जारी किया जिसमें संवेदनशील व्यक्तिगत डेटा या सूचना सहित डिजिटल व्यक्तिगत डेटा या सूचना का प्रसंस्करण करने वाली सभी संस्थाओं द्वारा साइबर सुरक्षा को मजबूत करने के लिए उठाए जाने वाले उपायों की रूपरेखा बताई गई।

xiv. संगठनों की तैयारियों का आकलन करने तथा सरकारी और महत्वपूर्ण क्षेत्रों में लचीलापन बढ़ाने के लिए साइबर सुरक्षा मॉक ड्रिल नियमित रूप से आयोजित की जाती हैं ।

xv. राष्ट्रीय सूचना विज्ञान केन्द्र (एनआईसी) विभिन्न ई-गवर्नेंस समाधानों के लिए केन्द्र सरकार, राज्य सरकारों और जिला प्रशासकों के मंत्रालयों, विभागों और एजेंसियों को सूचना प्रौद्योगिकी (आईटी) सहायता प्रदान करता है और साइबर हमलों को रोकने और डेटा की सुरक्षा के उद्देश्य से उद्योग मानकों और प्रथाओं के अनुरूप सूचना सुरक्षा नीतियों और प्रथाओं का पालन करता है।

xvi. सर्ट-इन और भारतीय रिजर्व बैंक (आरबीआई) संयुक्त रूप से डिजिटल इंडिया प्लेटफॉर्म के माध्यम से 'वित्तीय धोखाधड़ी से सावधान और जागरूक रहें'पर साइबर सुरक्षा जागरूकता अभियान चला रहे हैं।

xvii. आरबीआई ने सभी भुगतान प्रणाली ऑपरेटरों को निर्देश दिया है कि वे अपने भुगतान प्रणाली का वार्षिक आधार पर सर्ट-इन के पैनलबद्ध लेखा परीक्षकों से ऑडिट कराएं और संबंधित वित्तीय वर्ष की समाप्ति के दो महीने के भीतर आरबीआई को रिपोर्ट प्रस्तुत करें।

xviii. सर्ट-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और लेखापरीक्षा करने के लिए 155 सुरक्षा लेखापरीक्षा संगठनों को सूचीबद्ध किया है।

xix. डेटा सुरक्षा सुनिश्चित करने के लिए सूचना प्रौद्योगिकी (उचित सुरक्षा अभ्यास और प्रक्रियाएँ तथा संवेदनशील व्यक्तिगत डेटा या सूचना) नियम, 2011 ('एसपीडीआई नियम') संवेदनशील व्यक्तिगत डेटा या सूचना को संभालने वाले अनुपालन करने वाले निकाय कॉर्पोरेट या उसकी ओर से किसी भी व्यक्ति के लिए उचित सुरक्षा अभ्यास और प्रक्रियाएँ अनिवार्य करता है। निकाय कॉर्पोरेट या उसकी ओर से किसी भी व्यक्ति को ऐसी जानकारी एकत्र करने से पहले उपयोग के वैध उद्देश्य के बारे में ऐसी जानकारी के प्रदाता से लिखित सहमति प्राप्त करनी होगी।

xx. इसके अलावा, व्यक्तियों के व्यक्तिगत डेटा की सुरक्षा करने और यह सुनिश्चित करने के लिए कि उनका डेटा केवल उनकी सहमति से ही साझा किया जाए, डिजिटलवैयक्तिक डेटा संरक्षण अधिनियम, 2023 (डीपीडीपी अधिनियम) लागू किया गया है। डीपीडीपीअधिनियम का उद्देश्य ई-कॉमर्स क्षेत्र में उपभोक्ताओं सहित व्यक्तियों के व्यक्तिगत डेटा की सुरक्षा करना और वैध उद्देश्यों के लिए व्यक्तिगत डेटा का प्रसंस्करण सुनिश्चित करना है। डीपीडीपी अधिनियम में उल्लेख किया गया है कि व्यक्तिगत डेटा के प्रसंस्करण के लिए उचित तकनीकी और संगठनात्मक उपायों को लागू किया जाना चाहिए और किसी भी व्यक्तिगत डेटा उल्लंघन को रोकने के लिए उचित सुरक्षा उपाय किए जाने चाहिए।

****