भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 2310

जिसका उत्तर 21 दिसम्बर, 2022 को दिया जाना है।

30 अग्रहायण, 1944 (शक)

एम्स में साइबर हमला

2310. श्री अरुण साव :

श्री मोहन मंडावी :

श्री सुधाकर तुकाराम श्रंगारे :

श्री विजय बघेल :

श्री देवजी पटेल :

श्री सुनील कुमार सिंह :

श्री के. सुधाकरन :

श्री सुनील कुमार सोनी :

श्री राम मोहन नायडू किंजरापु :

श्री राकेश सिंह :

श्री वी.के. श्रीकंदन :

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

(क) क्या यह सच है कि अखिल भारतीय आयुर्विज्ञान संस्थान (एम्स) पर हाल ही में एक साहबर हमला हुआ है जिसमें हैकरों द्वारा उच्च रैंकिंग वाले सरकारी पदाधिकारियों और राजनयिकों सहित लाखों रोगियों का चिकित्सा डेटा चुरा लिया गया है;

(ख) यदि हां, तो तत्संबंधी ब्यौरा क्या है और ऐसे रोगियों की कुल संख्या कितनी है, जिनका डेटा चोरी हो गया है;

(ग) क्या जल शक्ति मंत्रालय के ट्विटर खाते की हैकिंग सहित हाल के दिनों में वाणिज्यिक और महत्वपूर्ण अवसंरचना को लक्षित करने वाले इसी प्रकार के रैंसमवेयर के मामलों का ब्यौरा क्या है;

(घ) क्या सरकार ने एम्स में साइबर हमले के दोषियों की पहचान की है और यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं;

(ड.) क्या सरकार ने ऐसे साइबर हमले को रोकने और भविष्य में बढ़ते साइबर अपराध को रोकने के लिए ठोस प्रयास और उपाय किए हैं; और

(च) यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं ?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क) और (ख): एम्स की सूचना और कंप्यूटर प्रणाली एम्स द्वारा प्रबंधित किए जाते हैं। एम्स से साइबर सुरक्षा घटना के घटित होने की सूचना मिलने पर भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) ने घटना का मूल्यांकन किया है। प्रारंभिक विश्लेषण के अनुसार, एम्स के सूचना प्रौद्योगिकी नेटवर्क में सर्वरों का अनुचित नेटवर्क विभाजन के कारण अज्ञात खतरे वाले कारकों द्वारा समझौता किया गया था, जिससे महत्वपूर्ण अनुप्रयोगों की गैर-कार्यक्षमता के कारण परिचालन में व्यवधान उत्पन्न हुआ। सीईआरटी-इन और अन्य हितधारक संस्थाओं ने आवश्यक उपचारात्मक उपायों की सलाह दी है। संबंधित हितधारकों द्वारा वर्तमान विश्लेषण के आधार पर, एम्स के पांच सर्वर प्रभावित हुए थे।

(ग) : जल मंत्रालय का ट्विटर अकाउंट से हाल ही में समझौता किया गया था और कपटपूर्ण क्रिप्टो संबंधित ट्वीट्स पोस्ट किए गए थे। सीईआरटी-इन ने मंत्रालय को अपने सोशल मीडिया एकाउंटो को सुरक्षित करने के लिए आवश्यक उपचारात्मक उपायों पर सलाह दी थी ।

रैंसमवेयर की घटनाएं समय के साथ वाणिज्यिक और महत्वपूर्ण बुनियादी ढांचे सहित कई क्षेत्रों में हमलों के साथ बढ़ी हैं। थ्रेट एक्टर्स ने अपने हमले के तरीकों का आधुनिकीकरण किया है, परिष्कृत रणनीति विकसित की है और हमले के अभियानों की एक विस्तृत श्रृंखला को अपनाया है। रैंसमवेयर कर्ता ज्ञात भेद्यताओं, दूरस्थ पहुँच सेवाओं की समझौता की गई साख का फायदा उठाते हैं और संगठनों के बुनियादी ढांचे में पहुँच प्राप्त करने के लिए फ़िशिंग अभियान चलाते हैं।

(घ): एम्स के अनुसार, भारतीय दंड संहिता की धारा 385 और सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 66 और 66एफ के तहत दिल्ली पुलिस के विशेष प्रकोष्ठ के साथ एक एफआई आर दर्ज की गई थी, और प्रभावित भौतिक सर्वरों को विशेष प्रकोष्ठ द्वारा जांच के लिए जब्त कर लिया गया था ।

(ङ) और (च): साइबर सुरक्षा स्थिति में वृद्धि करने और ऐसी घटनाओं पर अंकुश लगाने के लिए निम्नलिखित उपाय किए गए हैं :

(i) नवीनतम साइबर सुरक्षा खतरों के बारे में स्वास्थ्य क्षेत्र की संस्थाओं को संवेदनशील बनाने के लिए स्वास्थ्य और परिवार कल्याण मंत्रालय को सीईआरटी-इन द्वारा स्वास्थ्य क्षेत्र की संस्थाओं के लचीलेपन को बढ़ाने के लिए सुरक्षा प्रथाओं पर एक विशेष सलाह दी गई है। मंत्रालय से देश में सभी अधिकृत चिकित्सा देखभाल संस्थाओं/सेवा प्रदाताओं के बीच परामर्श का प्रसार करने का अनुरोध किया गया है। यह भी सुझाव दिया गया है कि वे प्राथमिकता के आधार पर सीईआरटी-इन-पैनलबद्ध लेखापरीक्षकों के माध्यम से विशेष लेखापरीक्षा करवायें , ऐसे लेखापरीक्षा के निष्कर्षों का अनुपालन करवाये और सुरक्षा के सर्वोत्तम प्रथाओं के कार्यान्वयन को सुनिश्चित करें ।

(ii) रैंसमवेयर घटना को देखने पर , सीईआरटी-इन प्रभावित संगठनों को की जाने वाली उपचारात्मक कार्रवाइयों के साथ सूचित करता है, और प्रभावित संगठनों, सेवा प्रदाताओं, संबंधित क्षेत्र के नियामकों और कानून प्रवर्तन एजेंसियों के साथ घटना की प्रतिक्रियात्मक उपायों का समन्वय करता है।

(iii) केंद्र सरकार के सभी मंत्रालयों और विभागों, राज्य सरकारों और उनके संगठनों और महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन के लिए सीईआरटी-इन द्वारा साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना तैयार की गई है।

(iv) सूचना प्रौद्योगिकी के बुनियादी ढांचे को सुरक्षित करने और साइबर हमलों को कम करने के लिए नेटवर्क और सिस्टम प्रशासकों और सरकार और महत्वपूर्ण क्षेत्र के संगठनों के मुख्य सूचना सुरक्षा अधिकारियों के लिए नियमित प्रशिक्षण कार्यक्रम सीईआरटी-इन द्वारा आयोजित किए जाते हैं। वर्ष 2021 और 2022 (नवंबर तक) के दौरान कुल 41 प्रशिक्षण कार्यक्रम आयोजित किए गए, जिनमें 11,377 प्रतिभागियों को शामिल किया गया।

(v) सीईआरटी-इन निरंतर आधार पर कंप्यूटर और नेटवर्क की सुरक्षा के लिए नवीनतम साइबर खतरों/भेद्यताओं और प्रतिउपायों के बारे में अलर्ट और परामर्श जारी करता रहा है। इसने अगस्त 2022 में "इंडिया रैंसमवेयर रिपोर्ट एच1 - 2022" भी प्रकाशित की है, जिसमें रैंसमवेयर हमलावरों की नवीनतम रणनीति और तकनीक और रैंसमवेयर - विशिष्ट घटना प्रतिक्रिया और शमन उपाय शामिल किये गए हैं।

(vi) साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) का संचालन सीईआरटी-इन द्वारा किया जाता है ताकि दुर्भावनापूर्ण प्रोग्रामों का पता लगाया जा सके और उन्हें हटाने के लिए मुफ्त उपकरण दिए जा सकें, और नागरिकों और संगठनों के लिए साइबर सुरक्षा टिप्स और सर्वोत्तम अभ्यास प्रदान किए जा सकें।

(vii) सीईआरटी-इन छोटे-छोटे अलर्ट को सक्रिय रूप से एकत्र करने, विश्लेषण करने और विभिन्न क्षेत्रों के संगठनों के साथ उनके द्वारा सक्रिय खतरे को कम करने के कार्यों के लिए उनके साथ साझा करने के लिए एक स्वचालित साइबर-खतरा विनिमय मंच संचालित करता है।

(viii) सरकार और महत्वपूर्ण क्षेत्रों में संगठनों की साइबर सुरक्षा मुद्रा और तैयारी के मूल्यांकन को सक्षम करने के लिए साइबर सुरक्षा मॉक ड्रिल आयोजित की जाती है। सीईआरटी-इन द्वारा अब तक 74 ऐसे ड्रिल किए गए हैं, जिनमें विभिन्न राज्यों और क्षेत्रों के 990 संगठनों ने भाग लिया।

(ix) मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में स्थितिजन्य जागरूकता पैदा करने के लिए राष्ट्रीय साइबर समन्वय केंद्र की स्थापना की गई है।

****