



चिकित्सा उपकरण और मैलवेयर

प्रलिस के लिये:

चिकित्सा उपकरण और मैलवेयर, रैनसमवेयर, साइबर हमले, दरोजन हॉर्स, साइबर सुरक्षति भारत, साइबर स्वच्छता केंद्र ।

मेन्स के लिये:

चिकित्सा उपकरणों पर मैलवेयर हमलों के प्रभाव और उपाय ।

चर्चा में क्यों?

हाल ही में कुछ विशेषज्ञों ने चेतावनी दी है कि ऑक्सीमीटर, हयिरिगि एड, ग्लूकोमीटर और पेसमेकर जैसे सामान्य चिकित्सा उपकरणों को [रैनसमवेयर](#) में बदला जा सकता है ।

- उद्योग विशेषज्ञ इस खतरे को पहचानते हुए किसी भी संभावित हानि को रोकने हेतु तत्काल प्रभाव से केंद्र सरकार के हस्तक्षेप की मांग कर रहे हैं ।
- यह चेतावनी **भारत के शीर्ष तृतीयक देखभाल अस्पतालों पर हुए रैनसमवेयर हमलों** के तुरंत बाद आई है, जिसके कारण दलिली के एम्स और सफदरजंग जैसे बड़े अस्पतालों के मेडिकल रिकॉर्ड को हैक कर लिया गया था ।

चिंताएँ:

- **डेटा उल्लंघन:**
 - चिकित्सा प्रौद्योगिकी उपकरणों के बढ़ते उपयोग और इन उपकरणों में पर्याप्त साइबर सुरक्षा के अभाव ने स्वास्थ्य सेवा उद्योग में डेटा उल्लंघनों तथा साइबर हमलों के संबंध में चिंताएँ बढ़ा दी हैं ।
 - ऐसे उपकरण आमतौर पर इंटरनेट, मोबाइल फोन, सर्वर और क्लाउड से जुड़े होने के कारण हमलों के प्रति संवेदनशील होते हैं ।
 - **सनफार्मा** (वर्ल्ड की चौथी सबसे बड़ी जेनरकि दवा कंपनी और एक भारतीय बहुराष्ट्रीय नगिम) को हाल के साइबर हमलों में **भारतीय चिकित्सा अनुसंधान परिषद (ICMR)** के साथ लक्षित किया गया था ।
- **सुभेद्य आबादी:**
 - भारत चिकित्सा उपकरणों हेतु वर्ल्ड के शीर्ष 20 बाजारों में से एक है , चिकित्सा उपकरण क्षेत्र के वर्ष 2025 तक 50 बिलियन अमेरिकी डॉलर तक पहुँचने का अनुमान है । हालाँकि, तेज़ आर्थिक विकास, बढ़ती मध्यम वर्ग की आय तथा चिकित्सा उपकरणों के बाजार में प्रवेश ने आबादी को साइबर खतरों के प्रति संवेदनशील बना दिया है ।
- **अपर्याप्त प्रणालियाँ:**
 - इसके अलावा भारतीय स्वास्थ्य सेवा उद्योग में एक केंद्रीकृत डेटा संग्रह तंत्र का अभाव है, जो डेटा भ्रष्टाचार की सटीक लागत निर्धारित करना चुनौतीपूर्ण बनाता है ।
 - इसके बावजूद यह स्पष्ट है कि डेटा न्यू ऑयल बन गया है और साइबर हमलों से एक महत्त्वपूर्ण खतरे से प्रभावित हो रहा है ।

ऐसे साइबर खतरों से निपटना:

- **वर्षेज्जों के साथ परामर्श:** सरकार को उन चुनौतियों की पहचान करने हेतु उद्योग विशेषज्ञों के साथ परामर्श करना चाहिये जो राष्ट्रीय सुरक्षा के लिये खतरा पैदा कर सकते हैं ।
- **कर्मचारी प्रशिक्षण:** कर्मचारियों को फिशिंग ईमेल को पहचानने एवं उससे बचने के तरीके हेतु प्रशिक्षित किया जाना चाहिये, जिसका उपयोग आमतौर पर रैनसमवेयर हमलों को शुरू करने हेतु किया जाता है ।
 - डेटा संरक्षण एक रॉकेटिंग साइंस नहीं है, लेकिन इसके लिये कानूनी एवं तकनीकी सक्षमता, पर्याप्त संसाधनों के आवंटन तथा व्यक्तिगत डेटा के प्रसंस्करण में शामिल सभी पेशेवरों के प्रशिक्षण की आवश्यकता होती है ।
- **नियमिती सॉफ्टवेयर अपडेट:** नियमिती सॉफ्टवेयर अपडेट उन कमजोरियों को दूर करने में मदद कर सकते हैं जिनका हैकर फायदा उठा सकते हैं ।
- **अभगिम नियंत्रण:** चिकित्सा उपकरणों तक केवल अधिकृत कर्मियों की पहुँच को सीमित करने से अनधिकृत व्यक्तियों को उपकरणों तक पहुँचने तथा

उन्हें मैलवेयर से संक्रमित करने से रोका जा सकता है।

- **एन्क्रिप्शन:** चकितिसा उपकरणों पर डेटा को अनधिकृत पहुँच से बचाने हेतु एन्क्रिप्शन का उपयोग किया जा सकता है।
- **नेटवर्क सेगमेंटेशन:** नेटवर्क को वभाजित करने से मैलवेयर को एक डविाइस से दूसरे डविाइस में प्रसारित होने से रोकने में मदद मलि सकती है।

साइबर खतरों के प्रमुख प्रकार:

- **रैंसमवेयर:** यह मैलवेयर का एक रूप है जहाँ पहले कंप्यूटर के डेटा को हाईजैक किया जाता है और फरि इसे पुनर्स्थापित करने के लिये पैसे की मांग (आमतौर पर बटिकॉइन के रूप में) संबंधी संदेश पोस्ट किया जाता है।
- **ट्रोजन हॉर्स :** कंप्यूटर प्रोग्राम के अंदर छुपा एक दुर्भावनापूर्ण सॉफ्टवेयर प्रोग्राम होता है। यह किसी वैध प्रोग्राम जैसे- किसी स्क्रीन सेवर के अंदर छुपकर कंप्यूटर में प्रवेश करता है।
 - जब उपयोगकर्ता संभवतः प्रोग्राम नषिपादति करता है, तो ट्रोजन के अंदर मैलवेयर का उपयोग ससि्टम में किसी और तरीके से प्रवेश करने के लिये किया जा सकता है जिसके माध्यम से हैकरस कंप्यूटर या नेटवर्क में प्रवेश कर सकते हैं।
- **क्लिकिज़ैकगि:** यह इंटरनेट उपयोगकर्ताओं को दुर्भावनापूर्ण सॉफ्टवेयर वाले लिंकि पर क्लिक करने या अनजाने में सोशल मीडिया साइटों पर नज़ि जानकारी साझा करने के लिये लुभाने का कृत्य है।
- **डनियल ऑफ सर्विस (DOS) अटैक:** किसी सेवा को बाधति करने के उद्देश्य से कई कंप्यूटरों और मार्गों से वेबसाइट जैसी किसी वशिष सेवा को ओवरलोड करने का जानबूझकर कर किया जाने वाला कृत्य।
- **मैन इन मडिलि अटैक:** इस तरह के हमले में दो पक्षों के बीच संदेशों को पारगमन के दौरान 'इंटरसेप्ट' किया जाता है।
- **क्रपिटो ज़ैकगि:** क्रपिटो ज़ैकगि शब्द क्रपिटोकैरेंसी से संबंधति है। क्रपिटो ज़ैकगि तब होता है जब हमलावर क्रपिटोकैरेंसी माइनगि के लिये किसी दुसरे के कंप्यूटर का उपयोग करते हैं।
- **ज़ीरो डे वलनेरेबलिटी :** ज़ीरो डे वलनेरेबलिटी मशीन/नेटवर्क के ऑपरेटगि ससि्टम या एप्लीकेशन सॉफ्टवेयर में व्याप्त ऐसा दोष है जिसे डेवलपर द्वारा ठीक नहीं किया गया है, ऐसे हैकर द्वारा इसका दुरुपयोग किया जा सकता है जो इसके बारे में जानता है।
- **ब्लूबगगि:** यह हैकगि का एक रूप है जो हैकरस को खोजे जा सकने योग्य चालू ब्लूटूथ कनेक्शन के माध्यम से डविाइस तक पहुँच प्रदान करता है। एक बार किसी डविाइस या फोन के ब्लूबग हो जाने के बाद, हैकर उसके कॉल सुन सकता है, संदेश पढ सकता है और संदेश भी भेज सकता है तथा संपर्कों के साथ छेड़छाड़ कर सकता है।

साइबर सुरक्षा से संबंधति पहलें:

- [भारतीय साइबर अपराध समन्वय केंद्र \(I4C\)](#)
- [भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल \(CERT-IN\)](#)
- [साइबर सुरक्षति भारत](#)
- [साइबर सवच्छता केंद्र](#)
- [राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र \(NCCC\)](#)

UPSC सविलि सेवा परीक्षा वगित वर्ष के प्रश्न

??????????:

प्रश्न. भारत में, किसी व्यक्तिके साइबर बीमा कराने पर, नधिकी हानिकी भरपाई एवं अन्य लाभों के अतिरिक्त नमिनलखिति में से कौन-कौन से लाभ दयि जाते हैं? (2020)

1. यदि कोई किसी मैलवेयर कंप्यूटर तक उसकी पहुँच को बाधति कर देता है तो कंप्यूटर प्रणाली को पुनः प्रचालति करने में लगने वाली लागत
2. यदि यह प्रमाणति हो जाता है कि किसी शरारती तत्त्व द्वारा जानबूझ कर कंप्यूटर को नुकसान पहुँचाया गया है तो एक नए कंप्यूटर की लागत
3. यदि साइबर बलात्-ग्रहण होता है तो इस हानिको न्यूनतम करने के लिये वशिष परामर्शदाता की की सेवाएँ पर लगने वाली लागत
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव करने में लगने वाली लागत

नीचे दयि गए कूट का प्रयोग कर सही उत्तर चुनयि:

- (a) केवल 1, 2 और 4
- (b) केवल 1, 3 और 4
- (c) केवल 2 और 3
- (d) 1, 2, 3 और 4

उत्तर: (b)

प्रश्न. भारत में साइबर सुरक्षा घटनाओं पर रिपोर्ट करना नमिनलखिति में से किसिके/कनिके लिये वधिति: अधदिशात्मक है? (2017)

1. सेवा प्रदाता
2. डेटा सेंटर
3. कॉर्पोरेट नकियाय

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

- (a) केवल 1
- (b) केवल 1 और 2
- (c) केवल 3
- (d) 1, 2 और 3

उत्तर: (d)

??????:

प्रश्न. साइबर सुरक्षा के विभिन्न तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिये कि भारत ने कसि हद तक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक विकसित की है। (2022)

स्रोत: द हट्टि

PDF Reference URL: <https://www.drishtias.com/hindi/printpdf/medical-device-and-malware>

