

केंद्रीय रिज़र्व पुलिस बल

जून , 2026

साइबर बाइट



ज़ीरो ट्रस्ट सिक््योरिटी एक आसान सिद्धांत
का पालन करती है: "कभी भरोसा न करें,
हमेशा पुष्टि करें।

बॉस स्कैम: MHA ने साइबर अपराधियों के नए
तौर-तरीकों के बारे में नागरिकों को आगाह किया।

1. नवीनतम साइबर खतरा

BOSS घोटाला: गृह मंत्रालय ने साइबर अपराधियों के नए तौर-तरीकों के खिलाफ नागरिकों को चेतावनी दी:

'BOSS घोटाला', I4C - भारतीय साइबर अपराध समन्वय केंद्र, गृह मंत्रालय ने नागरिकों को धोखाधड़ी वाले ईमेल और WhatsApp संदेशों के बारे में चेतावनी देते हुए एक सलाह जारी की है जो आरबीआई अधिकारियों का रूप धारण कर सकते हैं और कंपनियों के CEO को लक्षित कर सकते हैं। CEO के माध्यम से, अधीनस्थ कर्मचारियों को उच्च मूल्य की वित्तीय धोखाधड़ी करने के लिए समझौता किया जा सकता है।



घोटाला कैसे संचालित होता है ?

साइबर अपराधी तत्काल विनियामक अनुपालन की आड़ में email या WhatsApp के माध्यम से दुर्भावनापूर्ण अभिलेख वितरित करके उच्च पदस्थ अधिकारियों और अधिकारियों को निशाना बना रहे हैं।

यही कार्यप्रणाली CRPF में भी देखी गई है। जालसाज पहले यूनिट, कार्यालय या प्रतिष्ठान के नियंत्रण कक्ष को कॉल करता है और खुद को एक आईटी अधिकारी या वरिष्ठ अधिकारी के रूप में गलत पहचान देता है। फिर वह DBA के मोबाइल नंबर का अनुरोध करता है। DBA का संपर्क नंबर प्राप्त करने के बाद, जालसाज DBA को कॉल करता है और उन्हें WhatsApp के माध्यम से भेजे गए एप्लिकेशन को इंस्टॉल करने का निर्देश देता है, जो संभावित रूप से आधिकारिक सिस्टम और संवेदनशील जानकारी से समझौता करता है।

कैसे बचें :-

सभी कर्मचारियों को साइबर स्वच्छता और साइबर सुरक्षा के बारे में जागरूक करें।

2. तृतीय-पक्ष विक्रेता हमले (आपूर्ति श्रृंखला हमले)

हाल के वर्षों में, साइबर अपराधियों ने संगठनों पर सीधे हमला करने के बजाय तीसरे पक्ष के विक्रेताओं और सेवा प्रदाताओं को तेजी से लक्षित किया है। एक अच्छी तरह से संरक्षित संगठन की सुरक्षा में सेंध लगाने की कोशिश करने के बजाय, हमलावर कमजोर विक्रेताओं की तलाश करते हैं जिनके पास पहले से ही संगठन के सिस्टम तक पहुंच है।

आज के संगठन कई बाहरी विक्रेताओं, क्लाउड सेवाओं, सॉफ्टवेयर एप्लिकेशन, एपीआई और ओपन-सोर्स सॉफ्टवेयर पर भरोसा करते हैं। यदि इनमें से किसी से भी समझौता किया जाता है, तो हमलावर इसे संगठन के नेटवर्क तक अनधिकृत पहुंच प्राप्त करने के लिए प्रवेश द्वार के रूप में उपयोग कर सकते हैं।



उदाहरण के लिए, यदि किसी कंप्यूटर रखरखाव कंपनी, सॉफ्टवेयर विक्रेता, या क्लाउड सेवा प्रदाता के पास किसी संगठन के सिस्टम तक पहुंच है और उनकी अपनी सुरक्षा कमजोर है, तो हमलावर बिना संदेह पैदा किए संगठन के नेटवर्क में प्रवेश करने के लिए उस पहुंच का दुरुपयोग कर सकते हैं।

हमारा संगठन कंप्यूटर, सर्वर, नेटवर्क डिवाइस और अन्य आईटी उपकरणों की मरम्मत और रखरखाव जैसी गतिविधियों के लिए तीसरे पक्ष के विक्रेताओं को भी नियुक्त करता है। ऐसे काम के दौरान, विक्रेताओं को सिस्टम, व्यवस्थापक खाते, पासवर्ड या अन्य संवेदनशील जानकारी तक पहुंच की आवश्यकता हो सकती है।

इसलिए, किसी तीसरे पक्ष के विक्रेता को कोई अनुबंध देने या काम सौंपने से पहले, यह सुनिश्चित करने के लिए एक तृतीय-पक्ष विक्रेता साइबर सुरक्षा नीति लागू की जानी चाहिए कि संगठन की जानकारी और आईटी संपत्तियां सुरक्षित रहें।

सभी विक्रेताओं को यह करना होगा:

- उनकी पहुंच का उपयोग केवल अधिकृत कार्यों के लिए करें।
- सभी आधिकारिक जानकारी गोपनीय रखें।
- संगठन के साइबर सुरक्षा दिशानिर्देशों और सुरक्षा प्रक्रियाओं का पालन।
- निर्धारित कार्य पूरा होने के बाद कोई भी आधिकारिक डेटा वापस करें या हटा दें।

संचार एवं सूचना प्रौद्योगिकी निदेशालय, के0रि0पु0बल

- यह सुनिश्चित करने के लिए कि संगठनात्मक डेटा और सिस्टम सुरक्षित रहें, पूरे कार्य के दौरान निगरानी रखें।

मूल संदेश:

भले ही किसी संगठन की अपनी सुरक्षा मजबूत हो, एक खराब सुरक्षा वाला विक्रेता सबसे कमजोर कड़ी बन सकता है, इसलिए, प्रत्येक तीसरे पक्ष के विक्रेता को संभावित साइबर सुरक्षा जोखिम के रूप में माना जाना चाहिए और उसे सौंपे गए कार्य को करने के लिए आवश्यक न्यूनतम पहुंच ही प्रदान की जानी चाहिए।

2. KNOWLEDGE बैंक

1. Agentic AI हमले

हैकर्स अब कंप्यूटर सिस्टम पर स्वचालित रूप से हमला करने के लिए आर्टिफिशियल इंटेलिजेंस (AI) का उपयोग कर रहे हैं, बजाय इसके कि कोई व्यक्ति कमजोर बिंदुओं को मैनुअल रूप से खोजे, AI जल्दी से नेटवर्क को स्कैन कर सकता है, सुरक्षा अंतराल ढूंढ सकता है, सिस्टम में सेंथ लगा सकता है और बहुत कम या बिना किसी मानवीय भागीदारी के एक कंप्यूटर से दूसरे कंप्यूटर पर जा सकता है। इससे साइबर हमले बहुत तेज हो जाते हैं और उन्हें रोकना अधिक कठिन हो जाता है।



2. Deepfakes और पहचान संबंधी धोखा

साइबर अपराधी नकली आवाज़ें और यथार्थवादी दिखने वाले वीडियो बनाने के लिए AI का उपयोग कर रहे हैं जो वास्तविक लोगों की नकल करते हैं। वे आपके बॉस, एक वरिष्ठ अधिकारी या एक विश्वसनीय सहयोगी होने का दिखावा कर सकते हैं और आपसे धन हस्तांतरित करने, गोपनीय जानकारी साझा करने या जरूरी कार्य करने के लिए कह सकते हैं। क्योंकि ये नकली ऑडियो और वीडियो संदेश वास्तविक दिखाई देते हैं, इसलिए किसी व्यक्ति की पहचान सत्यापित करना बहुत कठिन हो गया है।



3. मैलवेयर-मुक्त घुसपैठ:

आधुनिक हैकर हमेशा सिस्टम में सेंथ लगाने के लिए वायरस या मैलवेयर का उपयोग नहीं करते हैं, इसके बजाय, वे उपयोगकर्ता नाम और पासवर्ड चुराते हैं या ऑपरेटिंग सिस्टम में पहले से उपलब्ध वैध टूल (जैसे विंडोज प्रशासनिक उपयोगिताएँ) का दुरुपयोग करते हैं। चूंकि ये सिस्टम प्रशासकों द्वारा उपयोग किए जाने वाले वास्तविक उपकरण हैं,

इसलिए पारंपरिक एंटीवायरस सॉफ्टवेयर का उपयोग करके उनकी दुर्भावनापूर्ण गतिविधियों का पता लगाना बहुत कठिन है।



बेहतर सुरक्षा के लिए, किसी भी असामान्य या अनधिकृत गतिविधियों की पहचान करने के लिए प्रक्रिया विश्लेषण टूल का उपयोग करके नियमित रूप से अपने सिस्टम के व्यवहार की निगरानी करें। अपने एंटीवायरस सॉफ्टवेयर को अपडेट रखें और नियमित सिस्टम स्कैन करें। इसके अतिरिक्त, सत्यापित करें कि आपके सिस्टम को उचित प्राधिकरण के बिना बदला या संशोधित नहीं किया गया है।

3. आईटी बुनियादी ढांचे की सुरक्षा कैसे करें

शून्य विश्वास सुरक्षा (**Zero Trust Security**) - डिफ़ॉल्ट रूप से किसी पर भरोसा नहीं:

पहले, एक बार जब कोई उपयोगकर्ता किसी संगठन के नेटवर्क में लॉग इन करता था, तो उन पर आम तौर पर भरोसा किया जाता था और वे कई प्रणालियों तक पहुंच सकते थे, हालांकि, साइबर खतरे बहुत अधिक उन्नत हो गए हैं, और चोरी किए गए उपयोगकर्ता नाम और पासवर्ड का उपयोग अक्सर हमलावरों द्वारा अनधिकृत पहुंच प्राप्त करने के लिए किया जाता □□□



Zero Trust Security एक सरल सिद्धांत का पालन करती है: "कभी भरोसा न करें, हमेशा **Verify** करें" किसी भी सिस्टम या डेटा तक पहुंचने की अनुमति देने से पहले प्रत्येक उपयोगकर्ता, डिवाइस और एप्लिकेशन को सत्यापित किया जाना चाहिए, भले ही वे पहले से ही संगठन के नेटवर्क के अंदर हों।

इस दृष्टिकोण के तहत:

- उपयोगकर्ताओं को केवल उनके आधिकारिक कर्तव्यों के लिए आवश्यक सिस्टम और जानकारी तक पहुंच दी जाती है।
- नेटवर्क के अलग-अलग हिस्सों को अलग कर दिया जाता है ताकि, भले ही एक सिस्टम से समझौता हो जाए, हमलावर आसानी से दूसरे सिस्टम में नहीं जा सके।
- सभी उपयोगकर्ता गतिविधियों की लगातार निगरानी की जाती है, और संदिग्ध गतिविधियों, जैसे बार-बार विफल लॉगिन प्रयास या असामान्य स्थानों या उपकरणों से पहुंच की तुरंत जांच की जाती है।

यह दृष्टिकोण आज विशेष रूप से महत्वपूर्ण है क्योंकि कर्मचारी विभिन्न स्थानों, नेटवर्क और उपकरणों से आधिकारिक सिस्टम तक पहुंचते हैं इसलिए, सुरक्षा को केवल उपयोगकर्ता पर भरोसा करने के बजाय निरंतर सत्यापन पर निर्भर होना चाहिए क्योंकि वे संगठन के नेटवर्क से जुड़े हुए हैं।

कार्रवाई आवश्यक है:

यह देखा गया है कि कई इकाइयां/प्रतिष्ठान उचित पहुंच नियंत्रण के बिना उपयोगकर्ताओं को अप्रतिबंधित इंटरनेट पहुंच प्रदान कर रहे हैं, जिससे साइबर हमलों और अनधिकृत पहुंच का खतरा बढ़ जाता है।

तदनुसार, सभी डीबीए/तकनीकी अधिकारियों को यह सुनिश्चित करना चाहिए:

- प्रत्येक उपयोगकर्ता को भूमिका-आधारित एक्सेस कंट्रोल (**Role-Based Access Control**) प्रदान किया जाता है, जो केवल आधिकारिक कर्तव्यों के लिए आवश्यक सिस्टम और एप्लिकेशन तक पहुंच की अनुमति देता है।
- प्रशासनिक विशेषाधिकार केवल अधिकृत कर्मियों को ही दिए जाते हैं।
- पूरे संगठन में समान सुरक्षा निगरानी, फ़िल्टरिंग, लॉगिंग और साइबर सुरक्षा नीतियों को लागू करने में सक्षम करने के लिए सभी इंटरनेट ट्रैफ़िक को **centralized firewall** के माध्यम से रूट किया जाता है।

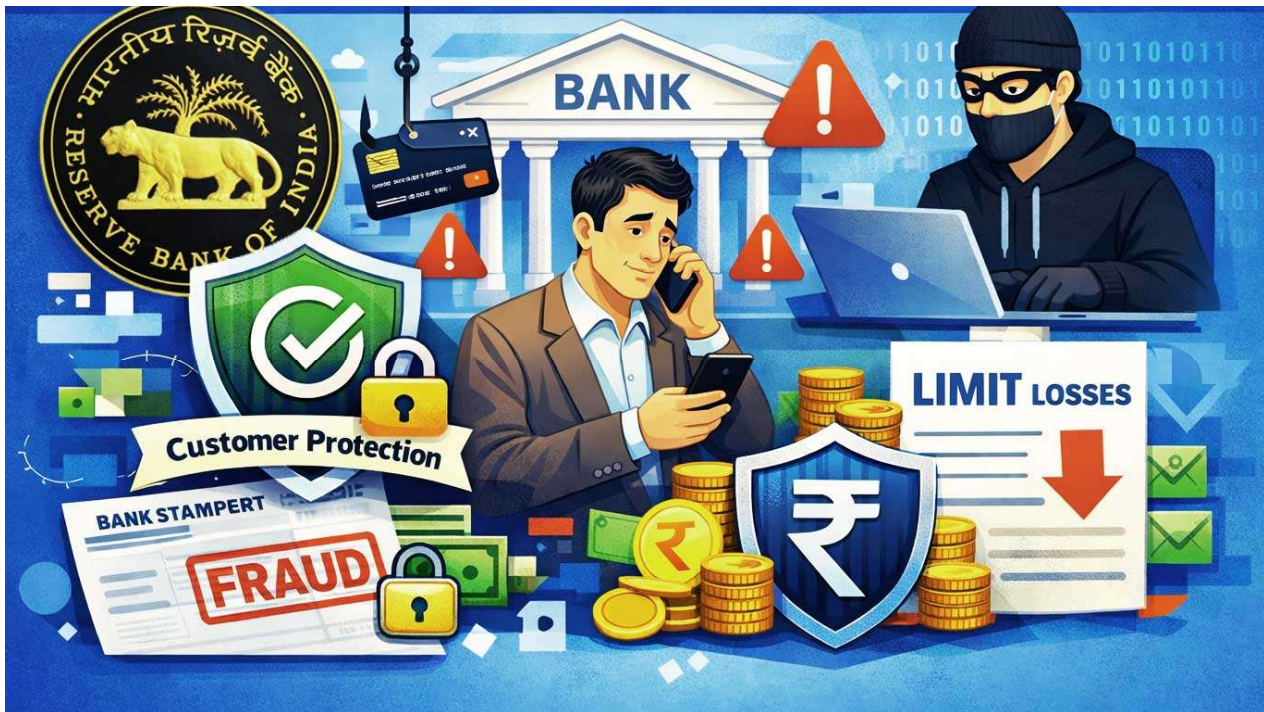
मूल संदेश:

किसी भी उपयोगकर्ता या डिवाइस पर भरोसा न करें, प्रत्येक एक्सेस अनुरोध को स्वचालित रूप से सत्यापित करें, केवल आवश्यक न्यूनतम अनुमतियाँ प्रदान करें, और साइबर खतरों के प्रभाव को कम करने के लिए सभी गतिविधियों की लगातार निगरानी करें।

4. साइबर गपशप

26 लाख रुपये की ऑनलाइन बैंकिंग धोखाधड़ी के आरोप में दिल्ली में 10 गिरफ्तार:

नई दिल्ली, पुलिस ने झारखंड के जामताड़ा और देवघर क्षेत्रों और दिल्ली-एनसीआर से संचालित एक अंतरराज्यीय साइबर धोखाधड़ी रैकेट के 10 लोगों को गिरफ्तार किया, जो कथित तौर पर 26 लाख रुपये से अधिक की ऑनलाइन बैंकिंग धोखाधड़ी में शामिल थे।



पुलिस के अनुसार, सिंडिकेट ने भोले-भाले पीड़ितों को निशाना बनाने के लिए परिष्कृत एपीके मैलवेयर, प्रतिरूपण घोटाले और रिमोट एक्सेस तकनीकों का इस्तेमाल किया। आरोपियों ने कथित तौर पर बैंक अधिकारियों के रूप में खुद को पेश किया, पीड़ितों को व्हाट्सएप के माध्यम से दुर्भावनापूर्ण एपीके फाइलें इंस्टॉल करने के लिए राजी किया, उनके मोबाइल फोन तक अनधिकृत पहुंच हासिल की, इंटरनेट बैंकिंग क्रेडेंशियल चुराए, OTP को इंटरसेप्ट किया और उनके बैंक खातों से पैसे उड़ाए।

2. 7.8 करोड़ रुपये की साइबर धोखाधड़ी: व्हाट्सएप 'बॉस' घोटाला:

पुलिस सूत्रों के अनुसार, आईएफएसओ इकाई, जो मामले की जांच कर रही है, ने पाया कि घोटालेबाजों ने शुरू में कंपनी के एक निदेशक को दुर्भावनापूर्ण संदेश भेजा था, इसे जरूरी मानते हुए, निदेशक ने इसे आगे की कार्रवाई के लिए अकाउंटेंट को भेज दिया। जैसे ही अकाउंटेंट ने ज़िप फ़ाइल पर क्लिक किया, उसके व्हाट्सएप खाते से कथित रूप से छेड़छाड़ की गई। इसके बाद कथित धोखेबाजों ने खाते पर नियंत्रण हासिल कर लिया, व्हाट्सएप पर कंपनी के संपर्क विवरण बदल दिए और उनकी नकल करके संदेश भेजना शुरू कर दिया। उन्होंने अकाउंटेंट को रियल-टाइम (RTGS), के माध्यम से धन हस्तांतरित करने का निर्देश दिया। तत्काल, उच्च-मूल्य वाले बैंक लेनदेन के लिए उपयोग की जाने वाली एक प्रणाली, सूत्रों ने कहा कि घोटालेबाज तत्काल नियामक अनुपालन आवश्यकताओं की आड़ में ईमेल या व्हाट्सएप के माध्यम से दुर्भावनापूर्ण ज़िप अभिलेखागार भेजकर उच्च-रैंकिंग अधिकारियों और कॉर्पोरेट अधिकारियों को लक्षित कर रहे हैं, कुछ मामलों में, वे भारतीय रिजर्व बैंक (RBI) के अधिकारियों का रूप धारण करते हैं। संदेश आम तौर पर अनुपालन के लिए केवल एक छोटी समय विंडो प्रदान करके तात्कालिकता की झूठी भावना पैदा करते हैं।

एक बार जब दुर्भावनापूर्ण फ़ाइल निष्पादित हो जाती है, तो मैलवेयर कार्यकारी के विंडोज डिवाइस और सक्रिय व्हाट्सएप वेब सत्रों को संक्रमित कर देता है। यह घोटालेबाजों को वरिष्ठ अधिकारियों के रूप में प्रस्तुत करते हुए अधीनस्थ कर्मचारियों के साथ संवाद करने और धोखाधड़ी वाले वित्तीय हस्तांतरण की योजना बनाने में सक्षम बनाता है।

5. साइबर स्वच्छता

- 1) सुनिश्चित करें कि आपका ऑपरेटिंग सिस्टम Windows 11 up to date है।
- 2) **Trellix** एंटीवायरस install और update किया गया।
- 3) छोटे लिंक पर क्लिक न करें।
- 4) अज्ञात स्रोतों से प्राप्त images, pdf files, zip files को न खोलें।
- 5) अज्ञात स्रोतों से प्राप्त ईमेल को न खोलें।
- 6) नेटवर्क में उपयोग करते समय USB ड्राइव को स्कैन करें।

6. IT DTE. में नया विकास

1 Sambhav

GMS को Sambhav ऐप में सफलतापूर्वक एकीकृत कर दिया गया है, CRPF कर्मों अब आसानी से Sambhav ऐप के माध्यम से शिकायत दर्ज कर सकते हैं।

2. E-bill

- i) Newspaper Bill Claim functionality को ई-बिल मॉड्यूल में उपलब्ध कराया गया है, जो उपयोगकर्ताओं को अपने समाचार पत्र बिल दावे इलेक्ट्रॉनिक रूप से प्रस्तुत करने में सक्षम बनाता है।
- ii) मोबाइल और टेलीफोन बिल दावा सुविधा को इलेक्ट्रॉनिक रूप से ई-बिल मॉड्यूल में पेश किया गया है।

3. Power BI Report

- i) सिग्नल स्टॉक स्थिति पावर बीआई रिपोर्ट में उपलब्ध कराई गई है।
- ii) सिग्नल कार्मिक Strength dashboard अब निगरानी और विश्लेषण के लिए Power BI में उपलब्ध है।
- iii) CRD OPS रिपोर्ट Power BI में उपलब्ध कराई गई है, जो सभी CRPF कर्मियों के working profiles का comprehensive view पेश करती है।



**Think Before
Click**



सीआरपीएफ के महानिदेशक श्री जी.पी. सिंह (आईपीएस) ने आरटीसी पेरिंगोम में प्रशिक्षकों, रंगरूटों तथा प्रशासनिक स्टाफ के साथ 'बड़ा खाना' कार्यक्रम में सहभागिता की।



सीआरपीएफ के महानिदेशक श्री जी.पी. सिंह (आईपीएस) ने आरटीसी पेरिंगोम में पौधारोपण कर पर्यावरण संरक्षण के प्रति बल की अटूट प्रतिबद्धता का संदेश दिया।



सीआरपीएफ के महानिदेशक श्री जी.पी. सिंह (आईपीएस) ने महानिदेशालय में आयोजित भव्य विदाई समारोह में सेवानिवृत्त हो रहे अधिकारियों को स्मृति-चिह्न प्रदान कर उन्हें सम्मानित किया।