The Sameeksha Global: A Multidisciplinary Journal in Hindi
https://www.eurekajournals.com/Sameeksha.html
ISSN: 2581-401X

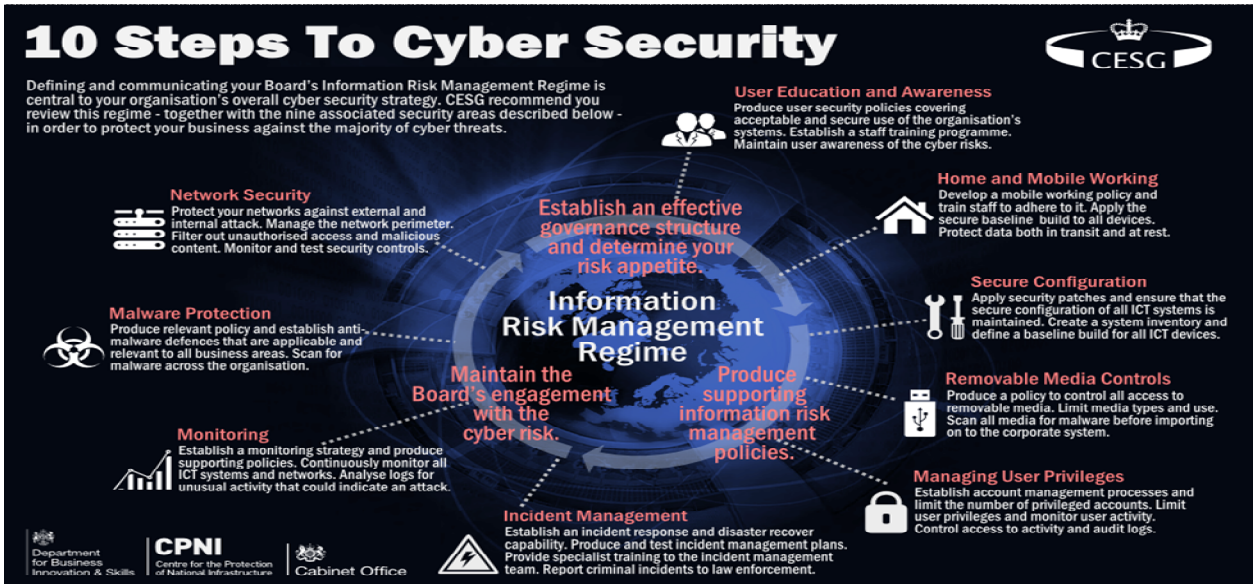
रणनीतिक साइबर सुरक्षा योजनाओं के लिए व्यापक जोखिम प्रबंधन पर विचारमंथन।

डॉ. अजय कृष्ण तिवारी[1]

[1]शिक्षाविद और अर्थशास्त्री और पीएच.डी. मार्गदर्शक

परिचय

यह शोध पत्र रणनीतिक साइबर सुरक्षा उपायों की योजना बनाने और बढ़ावा देने की आवश्यकता पर चर्चा करता है। मुझे आशा है कि आप समझ गए होंगे कि यदि ऐसा है तो पाठक को डिजिटल परिवर्तन की आवश्यकता के बारे में पता होना चाहिए। यह व्यवसाय मॉडल को डिजिटल तकनीक के साथ बदल देता है (DX) भी वित्तीय उद्योग में सक्रिय है, और इससे ग्राहकों के लिए सुविधा में सुधार होने की उम्मीद है। अन्य चूंकि ये नई सेवाएं और प्रौद्योगिकियां भी साइबर-हमलों द्वारा लक्षित हैं, इसलिए आज सेवा को साइबर सुरक्षा के लिए सोच-समझकर नियोजित और संचालित करने की आवश्यकता है।



हाल के साइबर हमलों का मुख्य उद्देश्य संगठनों की व्यक्तिगत जानकारी और गोपनीय जानकारी को चुराना, इंटरसेप्ट करना और छेड़छाड़ करना है। हमलों को व्यवस्थित रूप से चित्रित किया जाता है और बार-बार होने वाले हमलों की सूचना दी जाती है।

कीवर्ड: रणनीतिक साइबर सुरक्षा, डिजिटल परिवर्तन, व्यवसाय मॉडल, वित्तीय उद्योग, डिजिटल तकनीक, इंटरसेप्ट करना।

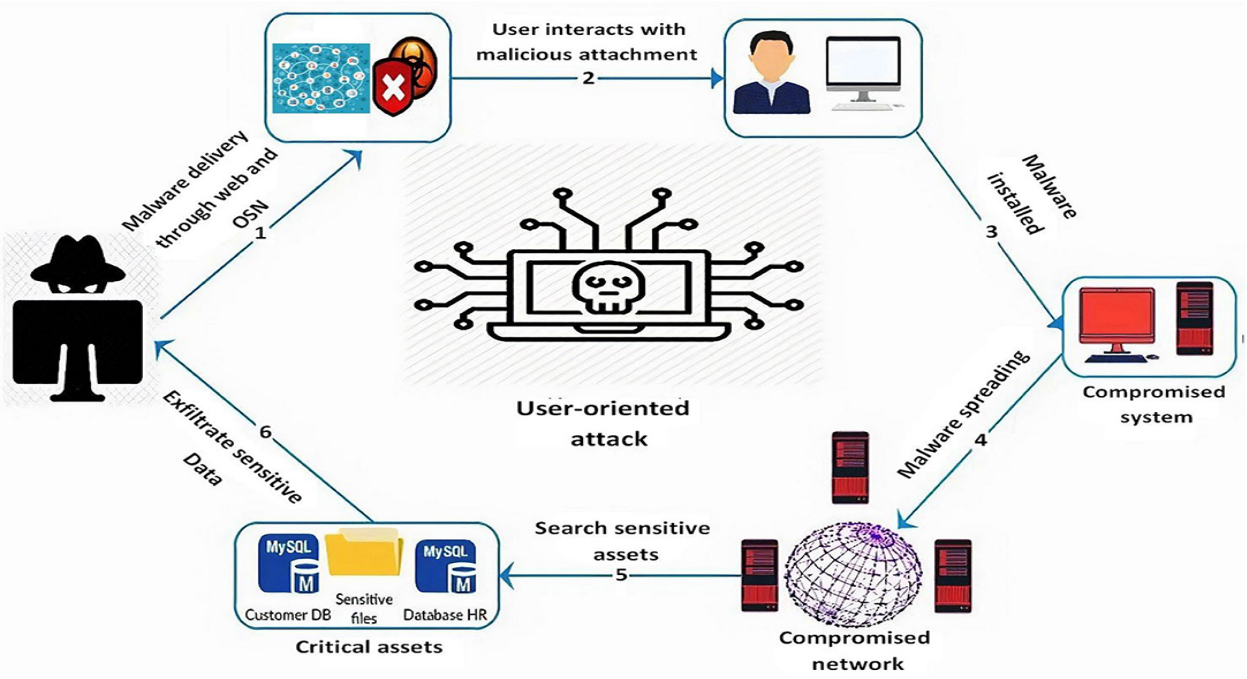
रणनीतिक साइबर सुरक्षा उपायों की योजना बनाने और उन्हें बढ़ावा देने की आवश्यकता

साइबर सुरक्षा के खतरे साल दर साल बढ़ते जा रहे हैं।हम साइबर सुरक्षा योजना के साथ बहुत सी व्यक्तिगत जानकारी और वित्तीय संपत्तियों की सुरक्षा करते हैं। हाल के दिनों में ऐसी घटनाएं हुई हैं जिनमें जानकारी रखने वाले और आईटी का उपयोग करने वाले वित्तीय संस्थानों को निशाना बनाया गया है। इसके अलावा, हाल के वर्षों में, लंबे समय तक सावधानीपूर्वक खोज और उन्नत प्रौद्योगिकी के उपयोग के कारण, जिसे राज्य-प्रायोजित माना जाता है, साइबर सुरक्षा खतरे साल-दर-साल बढ़ रहे हैं। किसी संगठन में समग्र जोखिम प्रबंधन के दृष्टिकोण से, व्यापक जोखिम प्रबंधन को एकीकृत करना महत्वपूर्ण है जो प्रगति में प्रबंधन प्रणालियों के व्यापक और रणनीतिक एकीकरण को पकड़ता है, उसका आकलन करता है और उसका अनुकूलन करता है। साइबर सुरक्षा में जोखिम प्रबंधन के लिए, भले ही कोई आईटी सेवा है जो किसी विशिष्ट व्यवसाय प्रभाग द्वारा उपयोग की जाती है, यह संगठन के आईटी विभाग या इसका उपयोग करने वाले विभाग तक सीमित होनी चाहिए।

This Photo by Unknown Author is licensed under CC BY-SA-NC

हमारा मकसद बढ़ते साइबर खतरों की सटीक पहचान और प्रबंधन करना है

एकल जिम्मेदारी के बजाय संगठनात्मक लक्ष्यों के साथ समग्र सुरक्षा और संरक्षण के लिए सुरक्षा का अनुकूलन करना नितांत आवश्यक है। इसे "साइबर रिस्क हैंडबुक फॉर डायरेक्टर्स, जापानी संस्करण" [1] में देखा जा सकता है, जिसके सिद्धांत 1 में कहा गया है कि "निदेशक सुरक्षा को उद्यम-व्यापी जोखिम प्रबंधन के मुद्दे के रूप में मानेंगे, न कि इससे निपटने की आवश्यकता है, केवल एक के रूप में आईटी मुद्दा। ", और साइबर जोखिम प्रबंधन नितांत आवश्यक है। मेरा मानना है कि यह सभी संगठनों से संबंधित महत्वपूर्ण विषयों में से एक है। इसलिए, इस शोध पत्र में, हमारा लक्ष्य बढ़ते साइबर खतरों की सटीक पहचान करना और उनका उचित प्रबंधन करना है।



This Photo by Unknown Author is licensed under CC BY

वित्तीय संस्थानों के लिए रणनीतिक साइबर सुरक्षा उपाय योजना

जैसा कि आप देख सकते हैं, साइबर घटनाओं की हालिया प्रवृत्ति और प्रत्येक वित्तीय संस्थान सुरक्षा उपायों की योजना और प्रचार कैसे करते हैं, इस पर उपयोगी साहित्य और प्रथाओं की खोज करें; मैंने विशिष्ट विधि का सारांश दिया। यदि प्रत्येक वित्तीय संस्थान रणनीतिक साइबर सुरक्षा उपायों को डिजाइन कर सकता है, तो यह करेगा। ऐसे सुरक्षा उत्पादों और सेवाओं के झांसे में न आएं जो खतरों के खिलाफ अस्पष्ट प्रभावशीलता के साथ मिनटों में किए गए प्रभावी उपायों के माध्यम से उच्च-सुरक्षा स्तर बनाए रखने की उम्मीद कर सकते हैं। फिर से, साइबर घटना की स्थिति में भी, हम सामान्य समय के दौरान प्रतिक्रिया और रिकवरी सिस्टम बनाए रखेंगे। यदि आप शुरू से ही ठीक से तैयार हैं, तो

आप आपात स्थिति में जल्दी और सटीक प्रतिक्रिया करके नुकसान को कम कर सकते हैं। मुझे लगता है कि हम यह कर सकते हैं। यह पेपर वित्तीय संस्थानों के लिए रणनीतिक साइबर सुरक्षा उपायों की योजना प्रदान करता है। मुझे उम्मीद है कि इससे आपको अपनी साइबर सुरक्षा की योजना बनाने में मदद मिलेगी।

This Photo by Unknown Author is licensed under CC BY-SA-NC

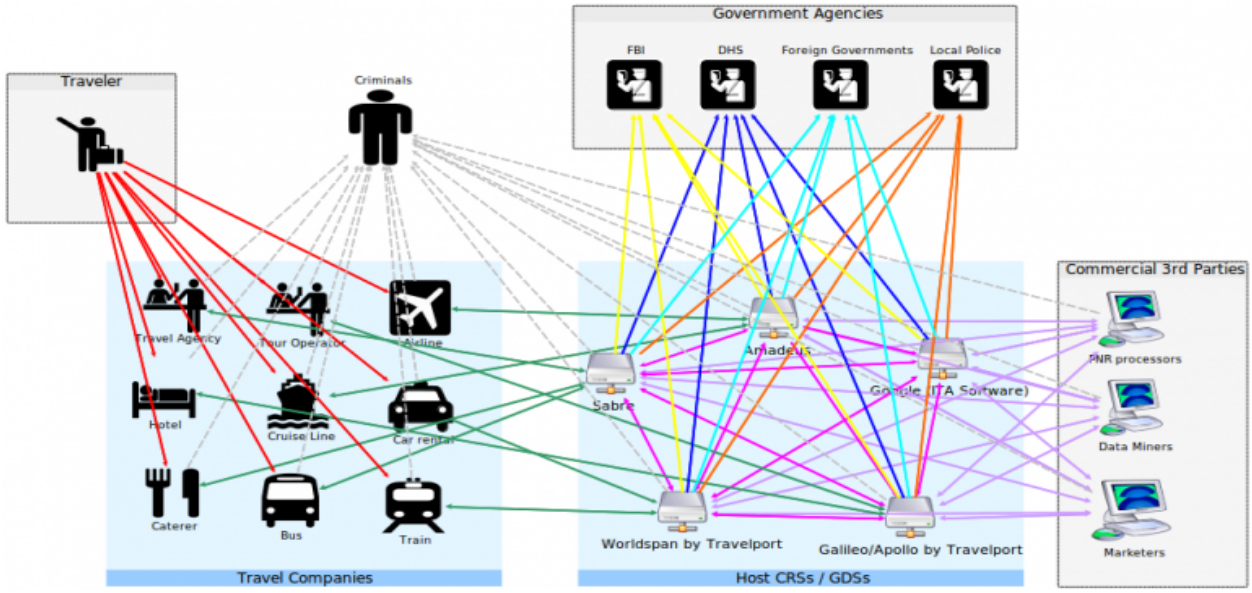
वित्तीय संस्थानों के लिए सामरिक साइबर सुरक्षा उपाय योजना

हम साइबर हमलों के इतिहास और हाल के रुझानों पर चर्चा करते हैं,यह पेपर निम्नानुसार व्यवस्थित है। हम साइबर हमलों के इतिहास और हाल के रुझानों पर चर्चा करते हैं, और प्रतिनिधि वित्तीय संस्थानों के लिए साइबर सुरक्षा पर चर्चा करते हैं। हम साइबर सुरक्षा आदि के लिए मानक और दिशानिर्देश पेश करते हैं और उनकी विशेषताओं के आधार पर उनका वर्गीकरण करते हैं। चल रहे साइबर प्लान की निगरानी पर भी चर्चा करता है और यह भविष्य के मुद्दों को दर्शाता है और साइबर हमलों के इतिहास और हाल के रुझानों को प्रस्तुत करता है, जैसा कि चित्र में दिखाया गया है, व्यक्तियों द्वारा सरल मज़ाक या मज़ाक साइबर हमलों का इस्तेमाल ऐसा करने की इच्छा को पूरा करने के लिए किया गया था। हालाँकि, हाल के वर्षों में, ऐसे हमले हुए हैं जो राज्य की भागीदारी के साथ-साथ समन्वित गतिविधियाँ प्रतीत होते हैं और उनके उद्देश्य अधिक नापाक हो गए हैं। हर संगठन इन साइबर हमलों का जवाब देने के लिए सुरक्षा उपाय भी करता है। हमलों का पता लगाने और बचाव में सुधार करके, सुरक्षा उत्पाद और सेवाएं हमलावरों का पता लगा सकते हैं।

सुरक्षा उत्पादों और सेवाओं द्वारा हमलावरों का पता लगाया जा सकता है

गोपनीय कॉर्पोरेट और राष्ट्रीय सूचना और सूचना को चुराने के लिए विभिन्न जासूसी गतिविधियाँ--

अधिक परिष्कारदर्ज किए गए लॉग फ़ाइलों को हटाने जैसे दर्ज किए गए हमलों को ज्ञान और सिस्टम ऑपरेशन इतिहास आदि से साइबर हमले की गतिविधियों के निशान को रोकने के लिए भी देखा गया है। इसके अलावा, व्यवसाय के पूर्ण डिजिटलीकरण के साथ, अगर कोई नुकसान होता है, तो इसे वैकल्पिक साधन जैसे मैनुअल काम। चूंकि प्रदर्शन किए जा सकने वाले कार्य की मात्रा की एक सीमा होती है, इसलिए कार्य अपने आप जारी नहीं रह पाएगा, और ग्राहकों और व्यावसायिक भागीदारों को परेशानी होगी। इससे हितधारकों पर भारी प्रभाव पड़ सकता है। इसका फायदा उठाकर जानकारी चुराने, किसी सिस्टम को बंद करने, उस सिस्टम को रिस्टोर करने या गोपनीय जानकारी जाहिर न करने के बदले में। ऐसे कई रैंसमवेयर अटैक हैं जो यूजर्स से पैसे की मांग करते हैं। इसके अलावा, गोपनीय कॉर्पोरेट और राष्ट्रीय जानकारी को चुराने के लिए कई जासूसी गतिविधियों को अंजाम दिया गया और जापान, संयुक्त राज्य अमेरिका, यूनाइटेड किंगडम, यूरोप और अन्य देशों ने संयुक्त रूप से इन गतिविधियों को अंजाम दिया।



This Photo by Unknown Author is licensed under CC BY-SA

यूक्रेन पर रूस के आक्रमण से देश में साइबर स्पेस को भी काफी नुकसान हुआ।

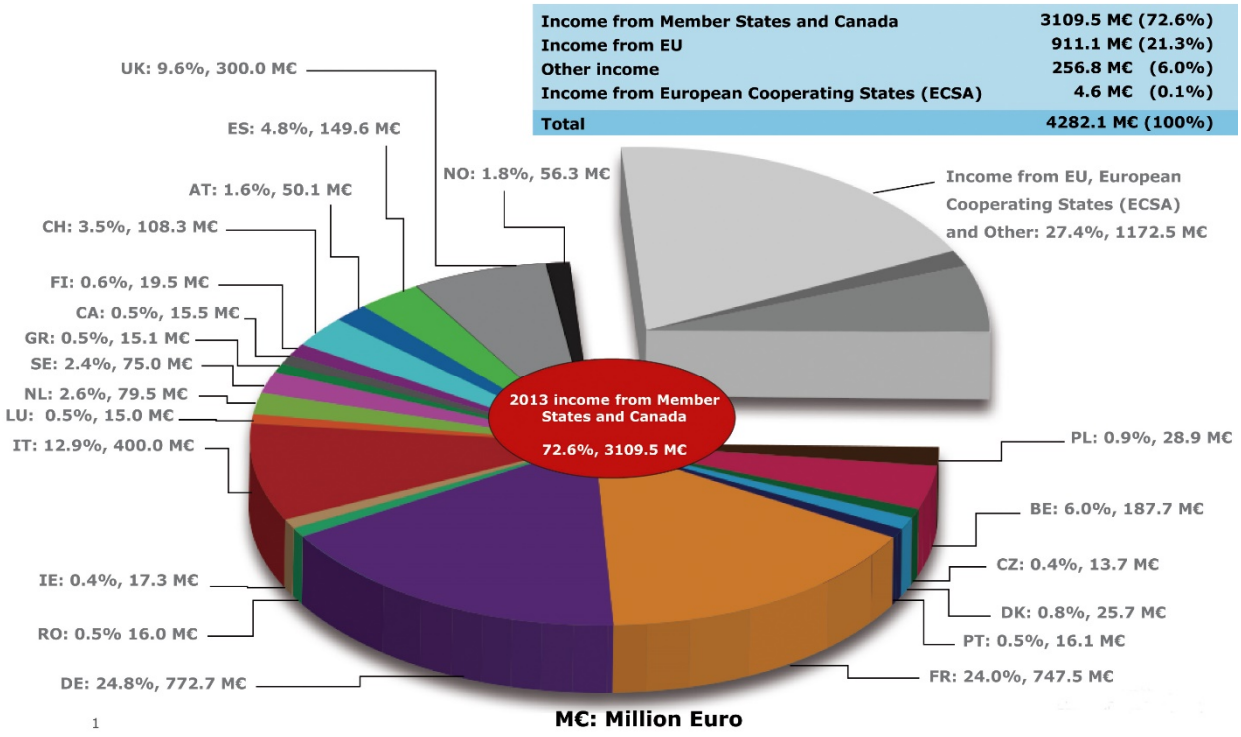
अभी हाल ही में, रूस द्वारा यूक्रेन पर मैलवेयर के आक्रमण का उद्देश्य यूक्रेनी सरकारी एजेंसियों के सिस्टम को लॉन्च करने से पहले और बाद में बाधित करना या नष्ट करना भी देश में साइबर स्पेस को महत्वपूर्ण नुकसान पहुंचाता है। और जवाबी कार्रवाई में रूस में भी इसी तरह के नुकसान की खबर

आई। दुनिया भर में दावोस बैठक के नाम से मशहूर वर्ल्ड इकोनॉमिक फोरम की वार्षिक बैठक में साइबर खतरों पर चर्चा की गई है। हाल के वर्षों में, अर्थव्यवस्था और समाज पर इसके भारी प्रभाव के कारण इसे तेजी से महत्वपूर्ण विषयों में से एक के रूप में लिया गया है। . और वैश्विक जोखिम रिपोर्ट जोखिमों और प्रभावों का भी विस्तार से वर्णन करती है। साइबर सुरक्षा के आसपास का वातावरण अधिक से अधिक गंभीर होता जा रहा है।

This Photo by Unknown Author is licensed under CC BY

2010 से सरकारों और वित्तीय संस्थानों के खिलाफ साइबर हमलों के उदाहरण

2010 के बाद से सरकारों और वित्तीय संस्थानों से संबंधित प्रमुख भाजक जब साइबर हमले अधिक गंभीर हो गए हैं। सुरक्षा घटनाओं को तालिका 7 में संक्षेपित किया गया है। जैसा कि तालिका में दिखाया गया है, न केवल मौद्रिक नुकसान, बल्कि व्यक्तिगत जानकारी और गोपनीय जानकारी की चोरी और सिस्टम शटडाउन जैसे नुकसान भी हुए हैं। और हाल के वर्षों में, लूप कंपनियों, व्यापार भागीदारों के माध्यम से लक्षित कंपनियों तक सीधे अनधिकृत पहुंच का प्रयास करने के अलावा, उपयोग किए गए सॉफ़्टवेयर और क्लाउड सेवाओं में भेद्यता, आदि। आपूर्ति श्रृंखला पर हमलों के कारण कई कंपनियों को गंभीर नुकसान हुआ है। एक विशेषता है जो वित्तीय संस्थानों के लिए विशिष्ट है। साइबर हमलों के मुख्य उद्देश्य प्रतिभूतियां, बीमा, धन उधार देना, धन हस्तांतरण आदि हैं। व्यक्तिगत जानकारी के अलावा, पंजीकृत खाते की जानकारी और उसकी प्रमाणीकरण जानकारी की चोरी शामिल है। चांदी उपरोक्त के अलावा, चोरी (धोखाधड़ी) नकदी के प्रेषण, आदि वित्तीय संस्थानों जैसे बैंकों और क्रेडिट यूनियनों में खातों में जमा किए जाते हैं जो जमा आदि को संभालते हैं।



This Photo by Unknown Author is licensed under CC BY-SA

टोक्यो 2020 ओलंपिक और पैरालंपिक खेलों से संबंधित साइबर सुरक्षा हमले

टोक्यो 2020 ओलंपिक और पैरालंपिक खेलों में विदेशों से दर्शक आएंगे। इसके अलावा, यह माना जाता है कि टोक्यो महानगरीय क्षेत्र में आयोजित प्रतियोगिताओं को भी दर्शकों के बिना आयोजित किया गया था। हालाँकि, जापान या विदेशों में साइबर हमले के कारण कोई बड़ा व्यवधान नहीं आया। आया। खेलों के बाद की आयोजन समिति और एनटीटी, जो खेलों के लिए साइबर सुरक्षा के प्रभारी थे, द्वारा संयुक्त रूप से आयोजित एक प्रेस कॉन्फ्रेंस में 450 मिलियन साइबर हमलों की पुष्टि की गई है कि संचालन पर कोई प्रभाव नहीं पड़ा। जापान और विदेशों में कंपनियों और व्यक्तियों को निशाना बनाने वाले साइबर हमलों के रूप में, एसएनएस, फ़िशिंग साइट्स, ओलंपिक से संबंधित मैलवेयर, आदि। प्रतियोगिता के पहले, दौरान और बाद में मोड़ देखे गए। हालाँकि, हाल के बड़े पैमाने के साइबर हमलों की तुलना में, हमले के तरीके के बारे में कुछ भी उल्लेखनीय नहीं था, और कोई ध्यान देने योग्य क्षति नहीं हुई थी।

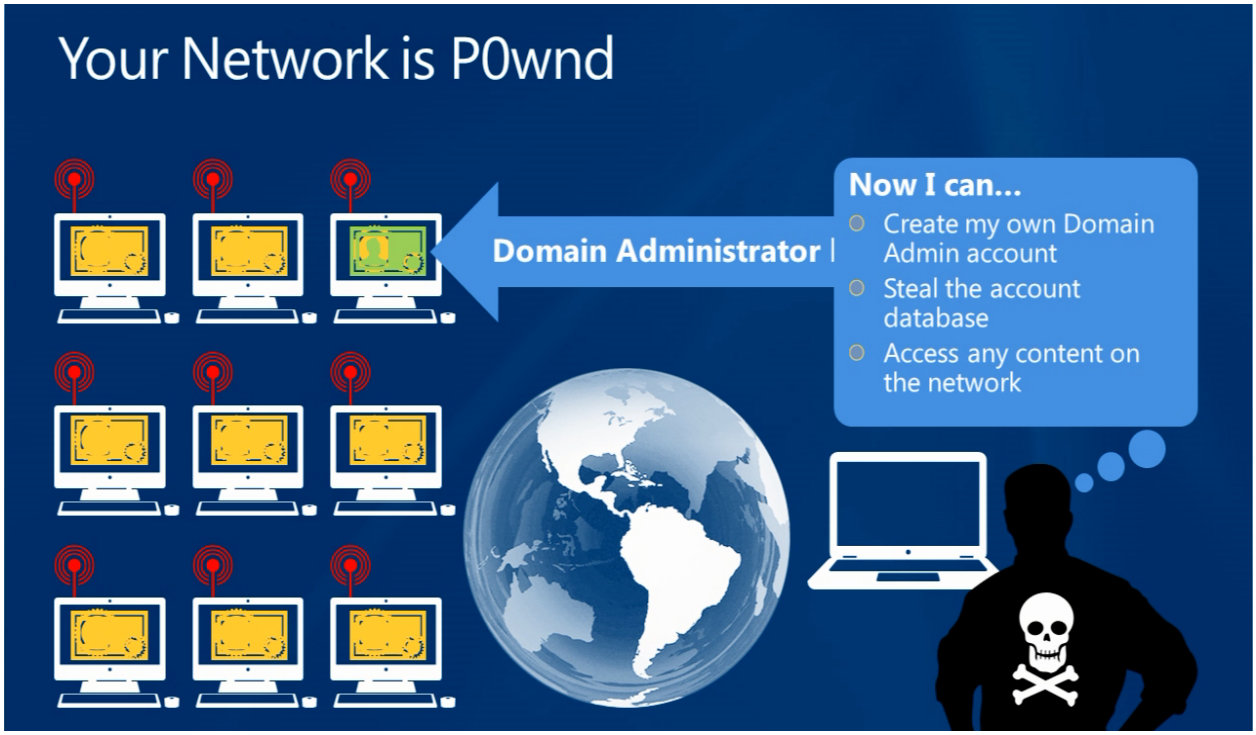
B

खेल-संबंधी कोई साइबर हमले नुकसान नहीं पहुँचाते

इसके अलावा, खेलों के दौरान DDoS हमलों में बढ़ती प्रवृत्ति देखी गई। कोई रिपोर्ट नहीं देखी है कि सिस्टम क्रैश हो गया है। ओलंपिक टिकटों पर खरीदार की जानकारी के बारे में लीक हुआ, लेकिन लगभग 10 लीक की सूचना ओलंपिक और पैरालंपिक खेलों की टोक्यो आयोजन समिति को दी गई। यह पता चला कि रिसाव तने के बाहर से था। उपायों को मजबूत करने के लिए एफएसए और अन्य सरकारी एजेंसियों के अनुरोधों के आधार पर, जापान में वित्तीय संस्थान हालांकि, टूर्नामेंट को एक साल के लिए बढ़ा दिया गया था और शुरुआत में अपेक्षा से अधिक लंबी अवधि के लिए सावधानीपूर्वक तैयारी की जा रही थी। खेलों से संबंधित किसी भी साइबर हमले से नुकसान नहीं हुआ। कोई ध्यान देने योग्य क्षति चेतावनियाँ और प्रतिउपाय के लिए अनुरोध प्राप्त नहीं हुए हैं, और वित्तीय संस्थानों के दृष्टिकोण से कोई प्रतिउपाय लागू नहीं किया गया है जिन्होंने अपेक्षाओं के विपरीत प्रतिक्रिया दी है।

साइबर हमलों की पहचान

साइबर हमलों की पहचान से पता चला हमले के तरीके और आईटी स्वयं विकसित होते रहते हैं इसलिए, वर्तमान साइबर सुरक्षाभविष्य में उपाय हमेशा प्रभावी नहीं हो सकते हैं। वर्तमान में, रैंसमवेयर से होने वाले नुकसान की कई रिपोर्टें आ रही हैं, और यह एक बार शांत हो गया है। यह भी फिर से बढ़ गया है, और इसका उपयोग ईमेल खातों को हाईजैक करने के लिए किया गया है और कुछ कंपनियों को नुकसान उठाना पड़ा है, जैसे कि सिस्टम में गड़बड़ी। इसके अलावा, वित्तीय समेत घरेलू दिग्गजों प्रमुख बुनियादी ढांचे ऑपरेटरों को लक्षित करने वाले हमलों का पता लगाया जा रहा है, कैबिनेट साइबर सुरक्षा केंद्र (एनआईएससी) और अन्य सरकारी मंत्रालयों और एजेंसियों से साइबर सुरक्षा उपायों को मजबूत करने का आग्रह किया गया है। सुरक्षा बनाए रखना जारी रखें और इसमें सुधार की आवश्यकता है।



This Photo by Unknown Author is licensed under CC BY-SA-NC

एनआईएसटी साइबर सुरक्षा ढांचा

NIST SP800-171

विशिष्ट विशेषताएं]

- अधिक तकनीकी और विस्तृत प्रक्रियाओं/आइटमों को शामिल करें।

- मैं सुरक्षित रहने के लिए क्या कर सकता हूं? इसे समझना आसान है, लेकिन इसमें बहुतसी बातें हैं।
- समय के साथ तालमेल बिठाने के लिए उन्हें बार-बार संशोधित किया जाता है।

वैचारिक [विशेषताएं]

- मुख्य रूप से अंतर्निहित अवधारणा का वर्णन करें।
- यह बहुतव्यापक है, लेकिन विशिष्ट क्या है यह पाठक पर निर्भर करता है कि वह प्रतिक्रिया दें या नहीं मुझे सोचना होगा।
- वर्णित सामग्री सार हैं

This Photo by Unknown Author is licensed under CC BY

साइबर सुरक्षा मानक और वित्तीय संस्थानों के लिए दिशानिर्देश

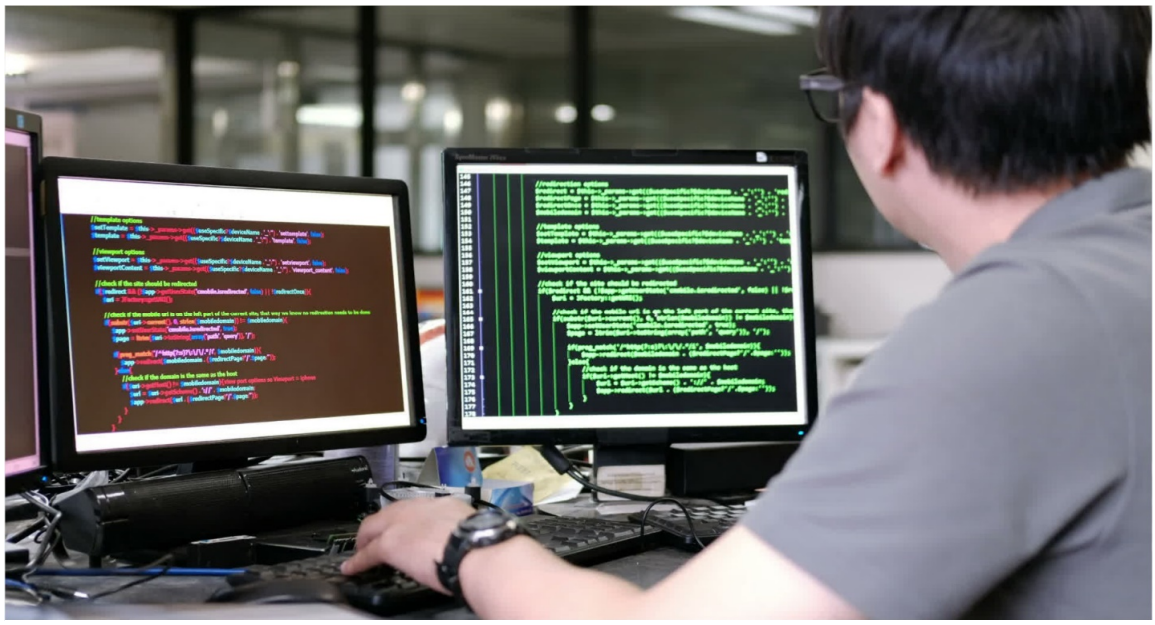
हमने साइबर हमलों के विकास के बारे में बताया और बताया कि कैसे वे अधिक परिष्कृत और दुर्भावनापूर्ण होते जा रहे हैं। और साइबर सुरक्षा को बनाए रखने और सुधारने की आवश्यकता के बारे में बताया। ये सेवाएं साइबर हमलों के खतरे के खिलाफ उपयुक्त प्रतिउपायों पर विचार करने के लिए

संदर्भ मानक और दिशानिर्देश यहां उपलब्ध हैं: जापान और विदेशों में पहले से ही कई हैं। हालाँकि, प्रत्येक संगठन द्वारा नियंत्रित की जाने वाली सूचना और प्रणालियाँ व्यवसाय के प्रकार और प्रकार पर निर्भर करती हैं, और विभिन्न आवश्यक साइबर सुरक्षा उपाय हैं। दूसरी ओर, वित्तीय उद्योग हालांकि व्यवसाय के पैमाने और स्थिति में भिन्न है, हालांकि पैमाने और प्रकार के व्यवसाय के आधार पर मतभेद हैं, साइबर सुरक्षा उपायों में आवश्यक समानताएं हैं। असंख्य हैं। इसलिए, वित्तीय संस्थानों को यह सुनिश्चित करना चाहिए कि वित्तीय उद्योग से संबंधित मानक, दिशानिर्देश आदि हैं। आपके संगठन के अनुकूल साइबर सुरक्षा उपायों की योजना बनाने और उन्हें लागू करने में आसान, उचित लक्ष्य निर्धारित करने में सक्षम हों, और साइबर के संबंध में अंतराल का विश्लेषण करें। आपके संगठन की सुरक्षा। घरेलू वित्तीय संस्थानों आदि द्वारा उपयोग किए जाने वाले विशिष्ट मानकों और दिशानिर्देशों का अवलोकन प्रदान करता है।

वित्तीय संस्थानों के कंप्यूटर सिस्टम के लिए सुरक्षा मानक और नियमावली

वित्तीय सूचना प्रणाली केंद्र, एक जनहित कॉर्पोरेट फाउंडेशन द्वारा प्रकाशित वित्तीय संस्थानों के लिए एक कंप्यूटर प्रणाली। सिस्टम सुरक्षा मानक/व्याख्यात्मक मैनुअल [3] 1985 में तैयार किया गया था और वित्तीय संस्थानों आदि की सूचना प्रणाली की सुरक्षा के लिए एक दिशानिर्देश है। यह काउंटरमेशर्स के लिए एक स्वैच्छिक मानक के रूप में प्रकाशित किया गया है और घरेलू वित्तीय संस्थानों के लिए वास्तविक मानक है। के रूप में व्यापक रूप से उपयोग किया जाता है। इस मानक को इस प्रकार से व्यवस्थित किया जाता है कि उद्देश्य और उपयोग की स्थिति के अनुसार इसका उपयोग सुविधापूर्वक किया जा सके। इसमें चार भाग होते हैं: "नियंत्रण मानक," "व्यावहारिक मानक," "साधन मानक,"

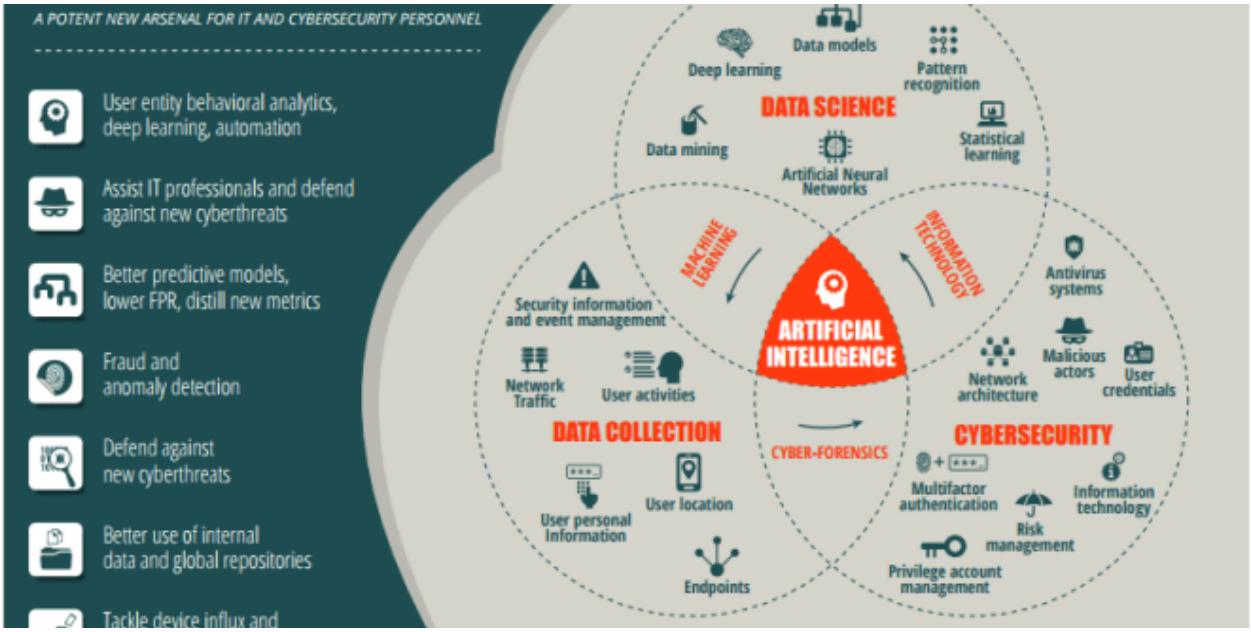
और "लेखा परीक्षा मानक।" बयान की सामग्री के विशिष्ट उदाहरणों में आईटी शासन, सिस्टम ऑडिट और साइबर सुरक्षा शामिल हैं।



This Photo by Unknown Author is licensed under CC BY

निष्कर्ष

साइबर सुरक्षा में तकनीकी तत्वों का एक उच्च अनुपात है, और पर्यावरण तेजी से बदलता है, इसलिए आईटी को साइबर सुरक्षा से परिचित लोगों को छोड़कर कई लोगों के लिए संभालना मुश्किल हो सकता है। यह पेपर रणनीतिक साइबर सुरक्षा उपायों की योजना बनाने और उन्हें बढ़ावा देने की आवश्यकता पर चर्चा करता है। मैं आशा करता हूँ कि तुम्हें समझ में आ गया होगा। यदि ऐसा है, तो पाठक को इस आवश्यकता के बारे में पता होना चाहिए कि मैं चाहूंगा कि आप यथास्थिति के साथ समाप्त होने के बजाय ठोस कार्रवाई करें। हालाँकि, साइबर सुरक्षा में भी, स्थितिजन्य जागरूकता प्रबंधन मान्यता और साझाकरण, समस्याओं का विश्लेषण), संचार (संदेश देना और पुष्टि करना), निर्णय लेना (समाधान नीति चयन, निर्णय लेना, समीक्षा करना), कार्यभार प्रबंधन (प्राथमिकता और संसाधन आवंटन), आदि। गैर-तकनीकी कौशल का लाभ उठाकर साइबर जिसमें कई वरिष्ठ अधिकारी और प्रबंधक अच्छे हैं - हमारा मानना है कि उच्च स्तर की सुरक्षा बनाए रखना और कुशलता से संचालन करना संभव है। इसलिए, साइबर सुरक्षा के साथ-साथ वित्तीय व्यवसाय में, जो कि हमारा मुख्य व्यवसाय है, मैं चाहूंगा कि आप अपने कौशल का उपयोग करें और इस पत्र में वर्णित प्रक्रियाओं के संदर्भ में एक रणनीतिक योजना तैयार करें।



This Photo by Unknown Author is licensed under CC BY-SA-NC

संदर्भ

जापान बिजनेस फेडरेशन (2019), निदेशकों के जापानी संस्करण के लिए साइबर रिस्क हैंडबुक, पीपी-65-69.

विश्व आर्थिक मंच (2022), वैश्विक जोखिम रिपोर्ट 2022, पीपी 43-45.

वित्तीय सूचना प्रणाली केंद्र (2021), वित्तीय संस्थानों के कंप्यूटर सिस्टम के लिए सुरक्षा मानक, आदि टिप्पणी (9वां संस्करण दिसंबर 2021 संस्करण).

वित्तीय सेवा एजेंसी (2016), साइबर सुरक्षा आकलन उपकरण पर एफएफआईईसी अनुसंधान, पीपी-65-67.

एनआईएसटी (2018), साइबर सुरक्षा फ्रेमवर्क संस्करण 1.1, पीपी-66-68.

आईपीए (2018), क्रिटिकल इन्फ्रास्ट्रक्चर वर्जन 1.1 की साइबर सुरक्षा में सुधार के लिए फ्रेमवर्क।

साइबर जोखिम संस्थान (2021), सीआरआई प्रोफाइल v1.2, पीपी-55-59.

फाइनेंशियल सर्विसेज एजेंसी (2016), साइबर सुरक्षा के लिए जी7 फंडामेंटल वित्तीय क्षेत्र, पीपी-76-79.

वित्तीय सेवा एजेंसी (2022) पर्यवेक्षण दिशानिर्देश।

कैबिनेट साइबर सुरक्षा केंद्र (2021), सरकारी एजेंसियों के लिए साइबर सुरक्षा उपाय, आदि मानदंडों का एकीकृत सेट।

एनआईएसटी (2020), एसपी800-53 संगठनों और सूचना प्रणाली नियंत्रण के लिए सुरक्षा और गोपनीयता (आईपीए द्वारा अनुवादित)