सीआईएसओ- स्तरीय गाइड: अपने संगठन की रक्षा करना

मैलवेयर नुकसान को रोकना

- अपने फायरवाल को सक्रिय करें और अपने नेटवर्क एवं इंटरनेट के बीच बफर जोन के सृजन हेतु एक्सेस कंट्रोल लिस्ट्स (एससीएल'ज) सेट करें। एक्सेस को ह्वाइटलिस्टिंग सेटिंग का उपयोग कर प्रतिबंधित करें न कि किसी खास आईपी एड्रेस या सेवाओं को ब्लैकलिस्ट कर।
- सभी कंप्यूटर और लैपटॉप पर एंटीवायरस सॉफ़्टवेयर और एंटीस्पाइवेयर का उपयोग करें। वितरित कार्यबल की रक्षा के लिए यह सुनिश्चित करें कि सुरक्षा टूल्स 'वर्क फ्राम होम' माहौल में प्रभावी रूप से संचालित हों।
- निर्माता और वेडर के द्वारा उपलब्ध कराए गए अपडेटेड सॉफ्टवेयर को प्रमुखता से उपयोग करते हुए सभी सॉफ्टवेयर और फर्मवेयर को पैबंद करें। जहां उपलब्ध है वहां 'स्वतः अपडेट'।
- एडमिन अधिकारों के साथ आईटी कर्मचारियों के लिए नए प्रोग्रामों की स्थापना को प्रतिबंधित करें।
- सुरक्षा/पहचान हार्डवेयर या सॉफ्टवेयर द्वारा उत्पन्न गतिविधि लॉग को बनाए रखें और निगरानी करें। पासवर्ड सुरक्षा और एन्क्रिप्शन के साथ लॉग को सुरक्षित रखें।
- सभी होस्ट क्लॉक को सिंक्रोनाइज्ड कर रखें। अगर आपके संगठन के डिवाइस में अनियमित क्लॉक सेटिंग हो तो दुर्घटना होने पर इवेंट की कड़ियाँ मिलना कहीं अधिक कठिन हो जाएगा।
- एसडी कार्ड और यूएसबी स्टिक जैसे रिमूवेबल मीडिया तक पहुंच को नियंत्रित करें। इसके बजाय कर्मचारियों को ईमेल या क्लाउड स्टोरेज के माध्यम से फ़ाइलों को स्थानांतरित करने के लिए प्रोत्साहित करें। कर्मियों को बाहरी स्रोत से यूएसबी के उपयोग या अन्य को अपने यूएसबी देने के खतरों के बारे में शिक्षित करें।
- अपनी ईमेल सेवाओं पर ईमेल सुरक्षा और स्पैम फ़िल्टर सेट अप करें।
- एन्क्रिप्शन और अन्य उपलब्ध उपकरणों के साथ अपनी सार्वजनिक उपयोग वाली वेबसाइटों पर सभी पेजों को सुरक्षित करें।
- अपने परिसंपत्तियों और सिस्टम की सुरक्षा का आकलन करने के लिए पेनेट्रेशन टेस्टिंग की नियुक्ति पर विचार करें।

कर्मियों को प्रशिक्षण देना

- नए कर्मी को शामिल करते समय अनिवार्य साइबर सुरक्षा प्रशिक्षण अवश्य संचालित करें और यह कार्य नियमित अंतराल पर कम से कम वर्ष में एक बार अवश्य करें। कर्मचारियों से आवश्यकता:
    - सभी पेशेवर उपकरणों और खातों पर शक्तिशाली पासवर्ड का उपयोग करें और उन्हें व्यक्तिगत उपकरणों के लिए भी ऐसा करने और एक पासवर्ड मैनेजर का उपयोग करने के लिए प्रोत्साहित करें,
    - एट होम आईटी इन्फ्रास्ट्रक्चर सहित सभी उपकरणों पर ऑपरेटिंग सिस्टम, सॉफ्टवेयर और एप्लिकेशन अप टू डेट रखें,
    - सभी खातों पर दो-कारक वाला प्रमाणीकरण उपयोग करें,
    - खाते का विवरण और एक्सेस कार्ड्स को सुरक्षित रखें और उपयोग में ना होने पर उपकरणों को लॉक करें,
    - अनएन्क्रिप्टेड ईमेल या अन्य खुले संचार के माध्यम से खाते के विवरण या अन्य संवेदनशील डेटा को साझा करने से बचें,
    - अटैचमेंट को तुरंत खोलने या या अनापेक्षित या संदिग्ध ईमेल में लिंक को खोलने से बचें,
    - व्यक्तिगत जानकारी प्रदान करने से पहले एक संदिग्ध दिखने वाले ईमेल या एक पॉप-अप बॉक्स की वैधता की पुष्टि करें, और ईमेल अड्रेस पर पूरा ध्यान दें, और
    - अपने संगठन के तकनीकी कर्मियों और/या उच्च प्रबंधन को किसी भी संभावित आंतरिक या बाहरी सुरक्षा घटनाओं, खतरों, या डेटा या उपकरणों से छेड़छाड़ की सूचना दें।
- सिमुलेटेड मामले के माध्यम से जैसे कि किसी जाली खाते से फिशिंग शैली का ईमेल भेजकर नियमित रूप से कर्मियों की जागरूकता की जांच करें। किसी भी विफलता को सीखने के अवसर के रूप में लें न कि दंड देने के लिए।

जोखिम आधारित सूचना सुरक्षा प्रोग्राम का विकास

1. **आपके व्यापार में जिस प्रकार की सूचना का भंडारण और उपयोग किया जाता है उसकी पहचान करना**
    - अपने व्यापार में उपयोग और भंडारित की जाने वाली सभी प्रकार की सूचनाओं (जैसे कि ग्राहक का नाम और ईमेल) की सूची बनाएं।
2. **अपनी सूचना के मूल्य को परिभाषित करें**
    - प्रत्येक प्रकार की सूचनाओं के लिए महत्वपूर्ण सवाल करें:
        - यदि यह जानकारी सार्वजनिक कर दी जाती तो क्या होगा?
        - अगर यह सूचना गलत होती तो मेरे व्यापार पर इसका क्या प्रभाव पड़ता जैसे कि डेटा की अखंडता में हेरफेर होता?
        - यदि मैं/मेरे ग्राहक इस जानकारी तक नहीं पहुँच सकते तो मेरे व्यवसाय का क्या होगा?
3. **एक इन्वेंट्री का विकास करें**
    - -पहचान करें कि आपके द्वारा चिह्नित की सूचना के साथ कौन सी तकनीक संपर्क में आई। इसमें हार्डवेयर (जैसे कंप्यूटर) और सॉफ़्टवेयर एप्लिकेशन (जैसे ब्राउज़र ईमेल) शामिल हो सकते हैं। मेक, मॉडल, सीरियल नंबर और अन्य पहचानकर्ता शामिल करें। निगरानी करें कि प्रत्येक उत्पाद कहां है। सॉफ़्टवेयर के लिए, पहचानें कि कौन सी मशीन(मशीनों) पर सॉफ़्टवेयर लोड किया गया है। इस बात की समझ विकसित करें कि तीव्र और/अथवा ब्रॉड वर्क फ्राम होम प्रतिनियुक्ति की स्थिति में वह इन्वेंट्री कैसे शिफ्ट कर सकती है।
    - जहां लागू होने योग्य हो वहां अपने व्यापार से बाहर की तकनीकों (जैसे कि "द क्लाउड") और आपके पास जो सुरक्षा तकनीक हो जैसे कि फायरवाल्स, को शामिल करें।
4. **अपने खतरे और भेद्यताओं को समझें**
    - नियमित रूप से समीक्षा करें कि वे किस तरह के खतरे और भेद्यताएँ हैं, जिससे वित्तीय प्रक्षेत्र का सामना हो सकता है और इस बात का आकलन करें कि आपके प्रभावित होने की संभावना क्या है। (आपके राष्ट्रीय सीईआरटी, एफएस-आईएसएसी और अन्य स्थानीय और क्षेत्रीय समूहों से सूचना प्राप्त की जा सकती है।)
    - कम से कम महीना में एक बार भेद्यता स्कैन या विश्लेषण का संचालन करें।
    - आंतरिक खतरे के विरुद्ध एक सुरक्षा योजना का विकास करें जिसमें एक उपक्रम वार जोखिम आकलन और एक्सेस कंट्रोल का कड़ा प्रबंधन शामिल हो।
5. **एक साइबर सुरक्षा नीति का सृजन करें**
    - अपने संगठन के वरिष्ठ प्रबंधन के साथ कार्य करें और एक ऐसी साइबर सुरक्षा रणनीति जो उपरोक्त जोखिम के लिए जरूरी उपाय करती हो और अंतरराष्ट्रीय, राष्ट्रीय और उद्योग मानदंड एवं दिशा-निर्देशों द्वारा सूचित हो, की स्थापना और रखरखाव करें। एनआईएसटी फ्रेमवर्क जैसे दिशा-निर्देश, एफएफआईईसी'ज साइबर सुरक्षा आकलन टूल और आईएसओ 27001 ऐसी नीतियों के लिए फाउंडेशन प्रदान करते हैं।
    - सभी कर्मियों को नीतियों के विवरण को लेकर प्रशिक्षित करें और उनसे ऐसे दस्तावेज पर हस्ताक्षर कराएं जिसमें स्वीकार किया जाए कि वे नीतियों का अनुपालन करते हुए आपके संगठन की साइबर सुरक्षा को बनाएं रखेंगे। इसमें एक स्पष्ट और अच्छी तरह जाना-पहचाना 'वर्क फ्राम होम' प्रोटोकॉल शामिल होना चाहिए।

अपने डेटा की सुरक्षा करना

- अपने महत्वपूर्ण डेटा (जैसे कि डॉक्युमेंट, ईमेल, कैलेंडर) का नियमित रूप से बैकअप लेते रहें और इस बात की जांच करें कि इन्हें फिर से भंडारित किया जा सकता है या नहीं। क्लाउड को बैकअप करने पर विचार करना।
- यह सुनिश्चित करें कि आपके बैकअप वाला डिवाइस मूल कॉपी धारण करने वाले डिवाइस स्थाई रूप से जुड़ा हुआ नहीं है और न तो भौतिक रूप से या किसी लोकल नेटवर्क पर जुड़ा है।
- सर्ज प्रोटेक्टर इंस्टॉल करें, जेनरेटर का उपयोग करें और यह सुनिश्चित करें कि आपके सभी कंप्यूटर और क्रिटिकल नेटवर्क डिवाइसेज अबाधित बिजली आपूर्ति के स्रोत से प्लग किया हुआ है।
- एक मोबाइल डिवाइस मैनेजमेंट (एमडीएम) साल्यूशन का उपयोग करें।

अपने डिवाइस को सुरक्षित रखें

- मोबाइल डिवाइसों के लिए पिन और पासवर्ड को सक्रिय करें। डिवाइस को इस तरह से कान्फिगर करें कि इसके गुम होने या चोरी होने की स्थिति में इन्हें ट्रैक किया जा सके, दूर से साफ किया जा सके या लॉक किया जा सके।
- अगर उपलब्ध हो तो 'स्वचालित अपडेट' विकल्प का उपयोग करते हुए अपने डिवाइस (और सभी इंस्टॉल किए हुए एप्स) को अद्यतन रखें।
- जब संवेदनशील डेटा भेज रहे हों तो सार्वजनिक वाई-फाई हॉटस्पॉट से कनेक्ट नहीं करें- सेलुलर कनेक्शन (टीथरिंग और वायरलेस डोंगल समेत) या वीपीएन का इस्तेमाल करें।
- ऐसे डिवाइस को बदल दें जो अब निर्माताओं के द्वारा समर्थित न हो और जिसके साथ अप-टू-डेट विकल्प नहीं हो।
- गुम या चोरी गए उपकरणों के लिए रिपोर्टिंग की प्रक्रिया निर्धारित करें।

पासवर्ड का उपयोग करना

- सुनिश्चित करें कि सभी कंप्यूटर इन्क्रिप्शन प्रोडक्ट का इस्तेमाल करते हैं जिसके लिए बूट हेतु पासवर्ड की आवश्यकता होती है। मोबाइल उपकरणों के लिए पासवर्ड या पिन सुरक्षा पर स्विच करें।
- शक्तिशाली पासवर्ड का उपयोग करें, अनुमान लगाने योग्य पासवर्ड (जैसे passw0rd) और व्यक्तिगत पहचानकर्ता(जैसे परिवार और पालतू जानवर का नाम) से बचें। सभी कर्मचारियों को ऐसा करने का निर्देश दें।
- जहां संभव हो वहां दोहरे कारक प्रमाणीकरण (2एफए) का उपयोग करें।
- कर्मियों में वितरण किए जाने से पूर्व नेटवर्क और आईओटी डिवाइस समेत सभी डिवाइसों से विनिर्माता द्वारा जारी किए गए डीफॉल्ट पासवर्ड को बदल दें।
- सुनिश्चित करें कि कर्मचारी अपने स्वयं के पासवर्ड को आसानी से रीसेट कर सकते हैं। यह यह भी चाह सकते हैं कि कर्मचारी नियमित अंतराल(जैसे तिमाही, छमाही, या सालाना) पर अपने पासवर्ड बदलें।
- पासवर्ड मैनेजर का उपयोग करने पर विचार करें। यदि आप एक का उपयोग करते हैं, तो सुनिश्चित करें कि मास्टर पासवर्ड (जो आपके सभी अन्य पासवर्ड तक पहुंच प्रदान करता है) शक्तिशाली है।

अनुमतियों को नियंत्रित करना

- सुनिश्चित करें कि सभी कर्मियों के पास अनूठे रूप से पहचाने जाने वाले खाते हैं जिसे उनके द्वारा आपके सिस्टम को एक्सेस करने के समय हर बार सत्यापित किया जा सके।
- केवल विश्वसनीय आईटी कर्मचारियों और प्रमुख कर्मचारियों को प्रशासनिक विशेषाधिकार दें और मानक उपयोगकर्ताओं के लिए कार्यस्थलों पर एडमिनिस्ट्रेटर विशेषाधिकार वापस लें।
- कर्मचारियों को केवल उन विशिष्ट डेटा प्रणालियों तक पहुंच प्रदान करें, जिनकी उन्हें अपनी नौकरियों के लिए आवश्यकता है और यह सुनिश्चित करें कि वे बिना अनुमति के कोई भी सॉफ़्टवेयर इंस्टॉल ना कर सकें।
- अपने कंप्यूटर के भौतिक एक्सेस पर नियंत्रण करें और प्रत्येक कर्मी के लिए उपयोगकर्ता खाता का सृजन करें।
- दूर से काम करने वाले कर्मी और व्यवस्थापक के लिए स्पष्ट एक्सेस विकल्प को परिभाषित करें।

अपने वाई-फाई नेटवर्क्स और डिवाइसेज को सुनिश्चित करना

- सुनिश्चित करें कि आपका कार्यस्थल का वाई-फाई सुरक्षित है और डब्ल्यूपीए2 के साथ एन्क्रिप्टेड है। राउटर अक्सर एन्क्रिप्शन बंद होने के साथ आते हैं, इसलिए इसे ऑन करना सुनिश्चित करें। राउटर का एक्सेस पासवर्ड से सुरक्षित हों और सुनिश्चित करें कि पासवर्ड प्रे-सेट डीफॉल्ट से अपडेट किया हुआ हो। किसी भी "दूरस्थ प्रबंधन" विशेषता को बंद करें।
- केवल कुछ मीडिया एक्सेस कंट्रोल अड्रेस वाले उपकरणों की अनुमति देकर अपने वाई-फाई नेटवर्क के एक्सेस को सीमित करें। यदि ग्राहकों को वाई-फाई की आवश्यकता है, तो एक अलग सार्वजनिक नेटवर्क इंस्टॉल करें।
- डायनेमिक होस्ट कन्फिगरेशन प्रोटोकाल (डीएचसीपी) लॉगिंग को अपने नेटवर्क डिवाइस पर सक्षम करें ताकि आपके नेटवर्क मौजूद सभी डिवाइसेज का आसानी से ट्रैकिंग हो सके।
- जब आप राउटर को स्थापित कर लें तो इसके बाद व्यवस्थापक के रूप में लॉग आउट कर लें।
- अपने राउटर सॉफ्टवेयर को अप टू डेट रखें। विनिर्माताओं के साथ निबंधन कर और अपडेट प्राप्त करने के लिए साइन अप कर अपडेट के बारे में जानें।

फिशिंग हमले से बचना

- सुनिश्चित करें कि कर्मचारी वेब पर ब्राउज़ न नहीं करते हैं या सर्वर पर या एडमिनिस्ट्रेट विशेषाधिकारों के साथ ईमेल नहीं चेक करते हैं।
- वेब और ईमेल फ़िल्टर सेट करें। कर्मचारियों को आमतौर पर साइबर सुरक्षा खतरों से जुड़ी वेबसाइटों पर जाने से प्रतिबंधित करने पर विचार करें।
- कर्मियों को इस बात का शिक्षण दें कि वे फिशिंग के स्पष्ट संकेत (जैसे कि खराब वर्तनी, व्याकरण या लोगो की निम्न स्तरीय गुणवत्ता जांच करें। क्या प्रेषक का ईमेल अड्रेस वैध लगता है?
- यदि आपको शंका होती है एक हमला हुआ है तो मैलवेयर के लिए स्कैन करें और जितनी जल्दी हो सके पासवर्ड बदलें। यदि स्टाफ फ़िशिंग हमले का शिकार हो जाता है तो कर्मचारी को दंडित ना करें (यह भविष्य में लोगों को रिपोर्टिंग से हतोत्साहित करता है)।