बोर्ड स्तर गाइड: साइबर सुरक्षा नेतृत्व

निगरानी

संगठन के सर्वोच्च स्तर के नेतृत्व के नाते बोर्ड साइबर खतरे के अधिशासित करने के लिए सर्वोच्च जिम्मेदारी धारण करता है, इस कारण वह इस क्षेत्र में संगठन की रणनीति, नीति और गतिविधियों पर नजर रखता है। विशिष्ट रूप से बोर्ड को चाहिए कि:

- वह साइबर खतरे और लचीलेपन की अनंतिम जवाबदेही ले, चाहे वह पूर्ण बोर्ड के माध्यम से हो या बोर्ड की किसी विशिष्ट कमेटी ओवरसाइट के प्रतिनिधिमंडल के माध्यम से हो।
- वह एक कॉरपोरेट अधिकारी सामान्यतया सीआईएसओ कार्य सौंपे जो साइबर पुनर्स्थापन और साइबर पुनर्स्थापन लक्ष्य की प्रगति और साइबर पुनर्स्थापन को लेकर संगठन की क्षमता की रिपोर्टिंग के लिए जवाबदेह हो। सुनिश्चित करें कि इस अधिकारी के पास इन जिम्मेदारियों को पूरा करने के लिए बोर्ड तक नियमित पहुंच,पर्याप्त अधिकार, विषय वस्तु का नियंत्रण, अनुभव और संसाधन हैं।
- खतरा को बर्दाश्त करने की आपकी संगठन की क्षमता को वार्षिक आधार पर परिभाषित करे; आपकी कॉरपोरेट रणनीति और जोखिम उठाने की क्षमता के साथ अनुरूपता को सुनिश्चित करें।
- यह सुनिश्चित करें कि आपके संगठन का एक औपचारिक, स्वतंत्र साइबर पुनर्स्थापन समीक्षा वार्षिक रूप संचालित किया गया है।
- वह साइबर पुनर्स्थापन योजना का निर्माण, क्रियान्वयन, जांच और जारी बेहतरी का निरीक्षण करे और संगठन में संरेखन को सुनिश्चित करे और यह कि आपका सीआईएसओ या अन्य जवाबदेह अधिकारी नियमित रूप इस सब की रिपोर्ट बोर्ड को उपलब्ध करे।
- वह साइबर लचीलेपन और जोखिम आकलन को आपके संगठन की संपूर्ण व्यापार रणनीति, जोखिम प्रबंधन, बजट उपबंधन और संसाधन आवंटन के साथ जोड़े जिसके साथ संपूर्ण ऑपरेशनल जोखिम के साथ साइबर जोखिम को पूर्ण रूपेण शामिल करने का लक्ष्य हो। नियमित रूप से तीसरे पक्ष के जोखिमों की समीक्षा करें।
- वह उपरोक्त के संबंध में आपके प्रदर्शन को आवर्ती रूप से समीक्षा करे और सतत बेहतरी के लिए स्वतंत्र सलाह पर विचार करे।

सूचना से लैस रहना

बोर्ड द्वारा प्रभावी साइबर जोखिम निरीक्षण का कार्य विषय पर सदस्यों के नियंत्रण और अद्यतन सूचना पर निर्भर करता है।

- यह सुनिश्चित करें कि बोर्ड से जुड़ने वाले सभी व्यक्ति को साइबर खतरे से उत्पन्न जोखिम को समझने और उसके प्रबंधन का सटीक अद्यतन कौशल और ज्ञान है।
- प्रबंधन से आपके संगठन के वर्तमान और भविष्यगत जोखिम एक्सपोजर, प्रासंगिक नियामक आवश्यक-ताएं और जोखिम उठाने की क्षमता के औद्योगिक एवं सामाजिक मानदंडों के संबंध में नियमित सलाह लेते रहना। आगे, खतरे की पृष्ठभूमि और नियामक माहौल के मद्देनजर नवीनतम प्रगति के बारे में नियमित ब्रीफिंग में शामिल होना और संयुक्त योजना बनाना और श्रेष्ठ अभ्यासकर्ता साथी और साइबर सुरक्षा के नेताओं से मिलना और अधिशासन एवं रिपोर्टिंग के विषय में उच्च स्तरीय विचार आदान-प्रदान करना।
- बोर्ड की बैठकों के दौरान कार्यशील एजेंडा विषय के तौर पर प्रबंधन को साइबर जोखिम, खतरे और इवेंट के मात्रात्मक और समझने योग्य आकलन के लिए तैयार रखना।
- प्रणालीगत चुनौतियां जैसे कि आपूर्ति शृंखला समस्याएं, आम निर्भरताएं और सूचना साझाकरण में अंतराल के प्रति जागरूकता कायम रखना।

टोन को सेट करना

वरिष्ठ प्रबंधन के साथ-साथ बोर्ड आपके संगठन के केंद्रीय मूल्यों, जोखिम संस्कृति और साइबर पुनर्स्थापन के संबंध उम्मीदों को जरूर निर्धारित और संवर्धित करे।

- ऐसी संस्कृति को बढ़ावा दें जिसमें आपके संगठन के साइबर पुनर्स्थापन के कार्य हेतु कर्मी सभी स्तर पर अपनी महत्वपूर्ण जिम्मेदारियों को पहचाने। उदाहरण प्रस्तुत कर नेतृत्व करना।
- प्रबंधन की भूमिका का निरीक्षण करें जो आपके संगठन की जोखिम संस्कृति को मजबूत और बरकरार रखे। सुरक्षा पर संस्कृति के प्रभाव, मजबूती पर विचार करते हुए जोखिम संस्कृति को बढ़ावा देना उसकी निगरानी और आकलन करना एवं जहां आवश्यक हो वहां परिवर्तन करना।
- यह स्पष्ट कर दें कि आप संगठन के बाहर अथवा भीतर सभी कर्मियों से ईमानदारीपूर्वक कार्य करने और अवलोकन किए गए गैर-अनुपालन को प्रमुखता के साथ दूर करने की अपेक्षा रखते हैं।

साइबर जोखिम प्रशासन के मूल तत्व

पुष्टि करें कि आप सकारात्मक रूप में निम्नलिखित प्रश्नों के उत्तर दे सकते/सकती हैं:

1. क्या आपके संगठन ने **वैधानिक और नियामक संबंधी आवश्यकताओं को पूरा कर लिया है**?
2. क्या आपके संगठन ने **अपने साइबर एक्सपोजर की मात्रा का आकलन और वित्तीय पुनर्स्थापन की जांच कर लिया है**?
3. क्या आपके बोर्ड के पास इस बात की **कोई बेहतरी की योजना** है जिससे यह सुनिश्चित हो कि एक्सपोजर सहमत जोखिम बर्दास्त करने की क्षमता के अंदर है?
4. **संगठन के साइबर पुनर्स्थापन के संबंध में प्रबंधन के द्वारा उपलब्ध कराए गए सघन, स्पष्ट और कार्रवाई करने योग्य सूचना के बारे में क्या बोर्ड नियमित रूप से चर्चा करता है**?
5. क्या आपके बोर्ड के पास **घटना आधारित प्रत्युत्तर योजना मौजूद है जिसे हाल में बोर्ड स्तर समेत ड्राई-रन अभ्यास के द्वारा परखी गई हो**?
6. क्या साइबर खतरे के प्रबंधन के लिए जिम्मेदार महत्वपूर्ण लोगों की **भूमिका सुरक्षा तीन पंक्तियों के संबंध में** स्पष्ट और संरेखित हैं?
7. क्या आपने अपने संगठन के साइबर खतरा संरचना का **स्वतंत्र मान्यकरण और आश्वासन** प्राप्त किया है?

सीईओ स्तरीय गाइड: साइबर सुरक्षा नेतृत्व

प्रशासन

आपके संगठन की साइबर सुरक्षा प्रबंधन के शीर्ष स्तर पर शुरू और समाप्त होती है। सीईओ बोर्ड के साथ मिलकर जोखिम की समझ को जरूर बरकरार रखें और संगठन की साइबर सुरक्षा से संबंधित गतिविधियां एवं कर्मियों के प्रति अनंतिम जवाबदेही और जिम्मेदारी धारण करें। आपको चाहिए कि:

- अगर पहले से मौजूद नहीं हो तो एक मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) की नियुक्ति करें अथवा संसाधन काफी सीमित हो तो संगठन के अंदर से ही किसी को सीआईएसओ के कार्यों के लिए नियुक्त करें।
- सीआईएसओ अथवा अन्य तकनीकी कर्मी के साथ साइबर सुरक्षा रणनीति फ्रेमवर्क की स्थापना और रखरखाव के लिए कार्य करें जो अंतरराष्ट्रीय, राष्ट्रीय और उद्योग मानदंडों एवं दिशा-निर्देशों का उपयोग करते हुए संगठन के विशिष्ट साइबर सुरक्षा की जरूरत को मुहैया कराए।
- संगठन की साइबर सुरक्षा को क्रियान्वित एवं प्रबंधन करने वाले कर्मी के सामने उसकी भूमिका और जिम्मेदारियों को स्पष्ट करें।
    - उपयुक्त साइबर सुरक्षा की भूमिका एवं सभी स्तर के कर्मियों के अधिकार एक्सेस की पहचान के लिए सीआईएसओ के साथ कार्य करें।
    - संचार और सहयोग का निरीक्षण करें ताकि यह सुनिश्चित हो सके साइबर सुरक्षा का प्रबंधन संपूर्णतया में हो रहा है, खासकर तब जब संगठन के अंदर साइबर सुरक्षा की जिम्मेदारियां एक से अधिक कर्मियों या प्रभागों (जैसे कि पृथक सूचना सुरक्षा, जोखिम और तकनीकी वर्टिकल्स का होना) के बीच साझाकृत हो।
- यह सुनिश्चित करें कि समय पर खतरे को जोड़ने के लिए आईएसओ के पास आपसे और बोर्ड से संचार के लिए स्पष्ट और सीधी लाइन हो।
- सीआईएसओ अथवा अन्य तकनीकी कर्मियों को वरिष्ठ प्रबंधन के सामने रूटीन तौर जानकारी प्रदान करने के लिए आमंत्रित करें।
- सुनिश्चित करें कि संगठन की सुरक्षा नीतियां, मानदंड, प्रवर्तन की युक्ति और प्रक्रिया सभी टीम और व्यापार की रेखाओं के आर-पार एक समान है।

जोखिम का आकलन और प्रबंधन

मजबूत साइबर सुरक्षा जागरूकता और तैयारी की मौजूदगी सतत जोखिम आधारित विश्लेषण पर निर्भर करता है। अपने संगठन की साइबर सुरक्षा को बेहतर करने के लिए:

- अपने संगठन के व्यापक जोखिम प्रबंधन और अधिशासन प्रक्रियाओं के अंदर साइबर सुरक्षा जोखिम आकलन और प्रबंधन को प्राथमिकता के रूप में स्थापित करें। अपने सीआईएसओ अथवा अन्य तकनीकी कर्मी के साथ एक ऐसा जोखिम आकलन योजना का संचालन करें जिसमें निम्न शामिल हो:
    - आपके संगठन की संपत्ति और उनके तकनीकी निर्भरता के विभिन्न स्तरों के बारे में वर्णन,
    - आपके संगठन की उसकी संपत्ति की तकनीकी निर्भरता से जुड़ी परिपक्वता और आंतरिक जोखिमों का आकलन करना,
    - आपके संगठन की परिपक्वता की वांछित स्थिति का निर्धारण,
    - इस बात को समझना कि साइबर सुरक्षा के खतरे आपके संगठन की जोखिम प्राथमिकता सूची में कहां पर रहते हैं,
    - साइबर सुरक्षा की आपकी मौजूदा स्थिति और इच्छित लक्षित स्थिति के अंतर को पहचानना,
    - परिपक्वता प्राप्त करने और बनाए रखने के लिए योजनाओं को लागू करना,
    - सुरक्षा और मौजूदा अंतर को दुर करने के लिए निवेश करने के लिए धन का मूल्यांकन और चिन्हित करना,
    - अपने संगठन की साइबर सुरक्षा की परिपक्वता, जोखिमों और लक्ष्यों का लगातार पुनर्मूल्यांकन करना, और
    - तीसरे पक्ष की पेनेट्रेशन-टेस्टिंग अथवा रेड-टीमिंग के उपयोग पर विचार करना,
    - सुरक्षात्मक उपायों पर विचार करें जैसे साइबर बीमा खरीदना।
- संस्थान भर से सामयिक प्रत्युत्तर प्राप्त हो इसकी व्यवस्थापना के लिए जोखिम आकलन प्रक्रिया के दौरान कर्मी के प्रयास का नेतृत्व करें।
- महत्वपूर्ण हितधारकों और बोर्ड समेत निरीक्षण एग्जिक्युटिव के लिए जोखिम आकलन का विश्लेषण करें और उनके सामने प्रस्तुत करें।
- आपके संगठन के इच्छित साइबर सुरक्षा तैयारी को बरकरार रखने या इसे बढ़ाने के लिए यथोचित बजट प्रबंध समेत अन्य किसी बदलाव का निरीक्षण करें जो इस बात को सुनिश्चित करता हो कि साइबर सुरक्षा के लिए उठाया गया कोई कदम जोखिम के मद्देनजर तर्कसंगत है या नहीं और आपके संगठन के लिए वहन करने योग्य है अथवा नहीं।
- उभरते साइबर जोखिम की समस्या से निपटने हेतु चल रहे निगरानी कार्य का प्रदर्शन तेज और स्फूर्त बना रहे इसका निरीक्षण करना।

सांगठनिक संस्कृति

आपके संगठन की साइबर सुरक्षा कोई एक बार की प्रक्रिया या कुछेक कर्मियों का कार्य नहीं है; यह हर व्यापार फैसले और ऑपरेशन का एक कारक है और एक अभ्यास है जिसका पालन हर कर्मी को आवश्यक रूप से करना होता है। आपके संगठन के अंदर सतत संपूर्ण साइबर सुरक्षा को प्रोत्साहन देने हेतु:

- टीम नेतृत्व के साथ साइबर सुरक्षा पर चर्चा आरंभ करें और नियमित रूप से साइबर जोखिम का प्रबंधन करने वाले कर्मी के साथ संचार करें।
- साइबर सुरक्षा प्रशिक्षण को सभी कर्मियों के लिए आनबोर्डिंग होने के एक हिस्सा के रूप शामिल करें जो इस बात को सुनिश्चित करे कि सभी कर्मी अद्यतन हैं और उन्होंने आपके संगठन की साइबर सुरक्षा नीतियों के समर्पित रहने के दस्तावेजों पर हस्ताक्षर कर दिया है और यह भी कि आपका आईटी विभाग या अन्य तकनीकी कर्मी ने उन्हें श्रेष्ठ कार्य अभ्यास के बारे में बता दिया है।
- संस्थान सभी कर्मियों को लघु और दीर्घकालीन सुरक्षा जिम्मेदारियों से अवगत कराने के लिए बारम्बार साइबर सुरक्षा प्रशिक्षण आयोजित करे।
- यह सुनिश्चित करें कि जब आपका संगठन संभावनाशील वेंडर का मूल्यांकन करता हो और तीसरे पक्ष के साथ डेटा साझा करता हो तो ऐसे मौकों पर हमेशा साइबर सुरक्षा पर विचार किया जाए।
- जब विलय या अधिग्रहण की बात हो तो संगठन की साइबर सुरक्षा के आकलन को इसमें शामिल करें।
- अपने संगठन की साइबर सुरक्षा नीतियों का वार्षिक रूप से समीक्षा करें।
- अपने संगठन के भीतर और भरोसामंद प्रतिस्पर्धी के साथ साइबर सुरक्षा के खतरे को लेकर स्वैच्छिक सूचना साझाकरण को बढ़ावा दें।
- सुरक्षा मसलों और आउटसेट से योजना निर्माण को शामिल करने वाले इनोवेशन को प्रोत्साहित करें।

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)।

सीआईएसओ- स्तरीय गाइड: अपने ग्राहकों की रक्षा करना

खातों का प्रशासन करना

- आपकी सेवाओं में लॉग करने के लिए आवश्यक है कि ग्राहक मजबूत यूजर आईडी और पासवर्ड का उपयोग करें। उन्हें सलाह दें कि वे उसी पासवर्ड का उपयोग न करें जिसका वे अन्य खातों के लिए उपयोग करते हैं।
- अविलम्ब सत्यापन, रीयल-टाइम सत्यापन, ट्रायल डिपॉजिट सत्यापन का इस्तेमाल करें, सत्यापन की पहचान करें और/अथवा आउट ऑफ वैलेट सवाल करें ताकि वास्तविक ग्राहकों का मान्यकरण हो सके और धोखाधड़ी के अवसर को कम किया जा सके।
- आपकी सेवा में लॉग करने के लिए दो-कारक सत्यापन की पेशकश करें जो आदर्श स्थिति के लिए आवश्यक होता है।
- धोखाधड़ी के किसी संकेत की जांच हेतु नियमित रूप यूजर खाते की जांच करते रहें।

डेटा की सुरक्षा करना

- इस बात पर विचार करें कि आपका संगठन किस ग्राहक डेटा को अपनी सेवा के लिए *अवश्य संग्रह* करता है और इससे इतर के ग्राहक डेटा के संग्रहण को लेकर सजग रहें।
- डेटा संधारण नीतियों का निर्धारण और वितरण करें। जब जरूरत ना हो तो ग्राहक के डेटा को नष्ट कर दें।
- पारगमन और स्थिर स्थिति में ग्राहक के डेटा को इन्क्रिप्ट करें।
- यह स्पष्ट करने के लिए कि प्रतिबंधित के विरुद्ध कौन सी डेटा स्थानांतरण नीति अनुमोदित है और यह विनिर्दिष्ट करने के लिए ग्राहकों डेटा से निपटते समय कर्मियों के हेतु क्या स्वीकार करने योग्य है, डेटा सुरक्षा की नीति को सामने रखें। यह सुनिश्चित करें कि ये नीतियां दस्तावेजित और संचारित है जोकि सभी कर्मियों के लिए प्रवर्तनीय है और आवर्ती रूप से समीक्षित एवं अपडेट किया हुआ है।

सार्वजनिक वेब एप्लिकेशन को सुरक्षित करना

- अपने संगठन के जन-मुखी वेब एप्लिकेशन (एप्लिकेशंस) पर HTTPS को लागू करें और सभी HTTP ट्रॉफिक को HTTPS पर पुनर्निर्देशित करें।
- अपनी वेबसाइट (वेबसाइटों) पर एक कंटेंट सुरक्षा नीति का उपयोग करें ताकि क्रॉस साइट स्क्रिप्टिंग हमले, क्लिकजैकिंग और अन्य कोड इंजेक्शन को रोका जा सके।
- अपनी वेबसाइट (वेबसाइटों) पर पब्लिक की पिनिंग को सक्षम करें ताकि हमलावर को हमला के बीच रोका जा सके।
- सुनिश्चित करें कि आपके जन-मुखी एप्लिकेशन (एप्लिकेशनों) कभी कूकी का उपयोग नहीं करे जिससे कि ग्राहकों की अतिसंवेदनशील या महत्वपूर्ण सूचना (जैसे कि पासवर्ड) भंडारित न हो, कूकी के लिए संरक्षित एक्सपायरेशन तिथियों का अनुपालन करें (बाद में नहीं बल्कि तुरंत) और आपके द्वारा उपयोग किए जाने वाले कूकीज में भंडारित सूचना हेतु इन्क्रिप्शन पर विचार करें।
- अपने जन-मुखी वेब एप्लिकेशन (एप्लिकेशनों) की सुरक्षा के आकलन हेतु साल में कम से कम एक बार पेनेट्रेशन टेस्टिंग सेवा नियुक्त करने पर विचार करें।

वित्तीय डेटा की रक्षा के लिए ग्राहकों और कर्मियों को व्यक्तिगत स्तर पर सलाह देना

अपने कर्मियों और ग्राहकों को सलाह दें कि वे अपने निजी आचरणों में निम्नलिखित दिशा-निर्देशों का पालन करें ताकि उनकी तैयारी बेहतर हो और साइबर हमले के विरुद्ध वे अपने वित्तीय डेटा की रक्षा कर सकें।

1. आधारभूत साइबर स्वच्छता के अभ्यास को सभी डिवाइसेज पर लागू करना।

- सभी व्यक्तिगत और पेशेवर डिवाइस पर मजबूत पासवर्ड का उपयोग करना और एक पासवर्ड मैनेजर के उपयोग पर विचार करना।
- अपने कंप्यूटर और मोबाइल डिवाइस पर सभी ऑपरेटिंग सिस्टम और अन्य सॉफ्टवेयर और एप्लिकेशंस को अद्यतन रखें।
- ऐसे एंटी-वायरस, एंटी-मैलवेयर और एंटी-रैंसमवेयर सॉफ्टवेयर इंस्टॉल करें जो दुर्भावनापूर्ण प्रोग्राम को रोक सकें, उसकी पहचान कर उन्हें हटा सकें।
- आपके कंप्यूटर का अनाधिकृत एक्सेस नहीं हो इसके लिए एक फायरवॉल प्रोग्राम का इस्तेमाल करें।
- केवल प्रतिष्ठित कंपनी के सुरक्षा प्रोडक्ट का इस्तेमाल करें। कंप्यूटर और उपभोक्ता प्रकाशनों से समीक्षाओं को पढ़ें और अपने कंप्यूटर या ऑपरेटिंग सिस्टम निर्माता के साथ परामर्श करने पर विचार करें।

2. संवेदनशील सूचना के प्रति सावधान रहें।

- अनक्रिप्टेड ईमेल के माध्यम से बैंक खातों का पासवर्ड या अन्य संवेदनशील वित्तीय खाता डेटा नहीं भेजें।
- इस बात को लेकर बुद्धिमता दिखाएं कि आप कहां और कैसे बैंकिंग या संवेदनशील सूचना से युक्त संचार के कार्य हेतु इंटरनेट से कनेक्ट होते/होती हैं। सार्वजनिक वाई-फाई नेटवर्क और पुस्तकालय या होटल व्यवसाय केंद्र जैसे स्थानों के कंप्यूटर जोखिमपूर्ण हो सकते हैं।

3. फिशिंग का प्रतिरोध करना।

- ईमेल अटैमेंट्स को तत्काल नहीं खोलें या ऐसे लिंकों पर क्लिक नहीं करें जो अविश्वसनीय या संदेहास्पद ईमेल हो। रूकें। सोचें। क्लिक करें।
- अगर कोई अप्रत्याशित रूप से ऑनलाइन या टेलीफोन के जरिए संपर्क करें और आपकी व्यक्तिगत सूचना की जानकारी मांगे तो संदेह करें। यहां तक कि ज्ञात पते के साथ संचार करते हुए ईमेल के जरिए व्यक्तिगत सूचना के साझाकरण को न्यूनतम रखें।
- याद रखें कि कोई भी वित्तीय संस्था आपसे ईमेल या फोन कर गोपनीय सूचना की मांग नहीं करती है जिसके बारे में उसे पहले से ही पता रहता है।
- मानकर चलें कि किसी ऐसे बैंक से अगर सूचना के लिए अनुरोध किया जाता है जहां आपका कभी कोई खाता नहीं रहा है तो यह स्कैम है।
- व्यक्तिगत सूचना प्रदान करने से पूर्व संदिग्ध नजर आने वाले ईमेल या किसी पॉप अप बाक्स की मान्यता का सत्यापन करें। ईमेल पते पर सावधानी से ध्यान दें।

कर्मियों को प्रशिक्षण देना

- मानवीय त्रुटि जोकि ग्राहकों के डेटा को असुरक्षित कर सकती है उसे कम से कम करने हेतु अपने कर्मियों को जवाबदेही और रणनीतियों के प्रति शिक्षित करें। इसका मतलब है कि उन्हें निम्नलिखित के लिए सुझाव दें:
  - ग्राहकों के डेटा तक उनकी पहुंच और प्रसारण के एक्सेस को सिर्फ वहीं तक सीमित करें जो उनके कार्य दायित्व के निर्वहन के लिए आवश्यक हो,
  - मजबूत पासवर्ड, टू-फैक्टर सत्यापन, सॉफ्टवेयर को अपडेट रखते हुए और संदिग्ध लिंक पर क्लिक नहीं करते हुए ग्राहकों के डेटा से निपटने वाले डिवाइस और खातों पर मजबूत सुरक्षा अभ्यास बरतें, और
  - अपने संगठन के तकनीकी कर्मी और/अथवा उच्च प्रबंधन को किसी वास्तविक आंतरिक या बाह्य खतरे या डेटा दुरुपयोग की रिपोर्ट करें।
- यह सुनिश्चित करें कि आपके कर्मी समझते हैं और उन्होंने आपके संगठन के डेटा सुरक्षा और सुरक्षा नीतियों के प्रति समर्पित रहने वाले दस्तावेज पर हस्ताक्षर कर रखा है ताकि वे इसका उल्लंघन नहीं करें और वे ग्राहकों से निपटते समय सहज रहें और उनसे असुरक्षित अंदाज में बातचीत नहीं करें।

ग्राहकों को अधिसूचित करना

- अपने संगठन के नियामक माहौल को समझे जब बात ग्राहकों के डेटा के उल्लंघन से निपटने की बात हो ताकि घटना होने पर आप अनुपालन के लिए तैयार रहें।
- जब आपके संगठन को पता चले कि ग्राहक की संवेदनशील सूचना के अनाधिकृत एक्सेस की घटना हुई है तो इसकी जांच कर प्रमुखता से तय करें इस घटना के कारण सूचना के अब तक दुरुपयोग होने और भविष्य में होने की संभावना क्या है। अधिसूचना के श्रेष्ठ अभ्यास का पालन करें और प्रभावित ग्राहक (ग्राहकों) को यथाशीघ्र इससे अधिसूचित करें:
  - जिस सूचना की सेंधमारी हुई उसकी सूचना और घटना का सामान्य विवरण,
  - सूचना और सहायता के लिए एक टेलीफोन नंबर,
  - अगले 12 से 24 महीने तक "सजग रहने का" रीमाइंडर,
  - इस बात की अनुशंसा कि संदिग्ध चोरी पहचान की घटना की प्रमुखता से रिपोर्ट करें,
  - सूचना का आगे और अनाधिकृत एक्सेस या उपयोग न हो इसके लिए वित्त संस्थान द्वारा उठाए कदमों के बारे में एक सामान्य विवरण,
  - क्रेडिट रिपोर्टिंग एजेंसियों की संपर्क सूचना और
  - आपके संगठन को जिन नियमों का पालन करना चाहिए, उनके लिए अन्य आवश्यक जानकारी।

सीआईएसओ- स्तरीय गाइड: तीसरे पक्ष के कनेक्शंस की सुरक्षा करना

तीसरे पक्षों के माध्यम से जोखिम की पहचान करना

- सभी वेंडर के संबंध की सूची और प्रत्येक मामले में सामने आने वाले डेटा की सूची बनाएं और इसे अद्यतन रखें।
- वेंडर अथवा तीसरे पक्ष द्वारा एक्सेस किए गए डेटा की समीक्षा करें। सुनिश्चित करें कि इस स्तर का एक्सेस 'न्यूनतम प्रेविलेज' के सिद्धांत का पालन करे।
- अपने वेंडर और तीसरे पक्ष के संबंधों को रैंक (निम्न, मध्यम, उच्च) करें जोकि इस आधार पर हो कि उसके सिस्टम का आपके संगठन पर उल्लंघन का असर क्या है।
- उच्चतम जोखिम के वेंडर से शुरू करते हुए प्रत्येक प्रदाता की साइबर सुरक्षा क्षमता का मूल्यांकन करें। प्रासंगिक मानदंडों का अनुपालन एक अच्छी शुरुआत बिंदु है। नियमित सुरक्षा मूल्यांकन के लिए एक योजना का विकास करें। उच्चतम जोखिम और/अथवा ग्राहक डेटा का सर्वाधिक एक्सेस वाले वेंडर का आप समय-समय पर ऑन-साइट आकलन कर सकते/सकती हैं।

तीसरे पक्ष की सुरक्षा का प्रबंधन करना

- सम्यक उद्यम के साथ प्रदर्शन करें। आपके संगठन के प्रस्ताव, अनुबंध, व्यापार निरंतरता, घटना प्रत्युत्तर के अनुरोध में और वेंडर के साथ सेवा स्तर के अनुबंधों में साइबर सुरक्षा उम्मीद को स्थापित करें। साइबर घटना के मामले में जिम्मेदारियों और उत्तरदायित्वों पर सहमति हों।
    - अन्य तीसरे पक्ष जैसे कि जिन वित्तीय संस्थानों के साथ आप लेनदेन करते हैं या डेटा साझा करते हैं, उनके साइबर सुरक्षा अभ्यास का निरीक्षण करें। ऐसी कोई भी साइबर सुरक्षा की आवश्यकताएं जिसकी साथ आपके संगठन को अवश्य प्रतिबद्ध होना चाहिए उसका अनुपालन आपके वेंडर और अन्य संगठन जिनके साथ आप डेटा साझा करते हैं या अपनी परिसंपत्ति को रखते हैं, को भी करना चाहिए।
- साइबर सुरक्षा मानकों के प्रति अपने वेंडर के अनुपालन की निगरानी के लिए स्थापित परस्पर सहमत उपायों का उपयोग करें।
- संवेदनशील डेटा हैंडल करने वाले आपके ऐसे वेंडर जिसके साथ आपके कोई खाता है उसके साथ यह जांच करें कि वे दो कारक प्रमाणीकरण, इन्क्रिप्शन या अन्य सुरक्षा उपाय प्रस्तुत करते या नहीं।
- सुनिश्चित करें कि आपने तीसरे पक्ष के जो सॉफ्टवेयर और हार्डवेयर इंस्टॉल किए हैं उसके साथ सुरक्षा हैंडशेक है या नहीं ताकि सत्यापन कोड के माध्यम से बूटिंग की प्रक्रियाएं सुरक्षित रहें और कोड की पहचान नहीं होने पर वे कार्यरत नहीं हो।
- अगर आपको कोई ऐसा वेंडर प्रोडक्ट प्राप्त होता है जो दोषपूर्ण है अथवा विन्यास से मेल नहीं खाता है तो किसी समाधान पर आने के लिए कार्य करें अथवा निकास रणनीति को चुनें।
- वार्षिक रूप से वेंडर के अनुबंध का मूल्यांकन करें और सुनिश्चित करें कि वे आपकी रणनीति की दिशा में और नियामक डेटा सुरक्षा आवश्यकताओं के लिए काम कर रहे हैं। अनुबंध समाप्त होने पर, आपने परिसंपत्तियों या डेटा वापस पाने के बारे में नियम को शामिल करें और पुष्टि करें कि वेंडर के पक्ष पर परिसंपत्ति या डेटा पूरी तरह से मिट दिये गए हैं, और आपके सिस्टम या सर्वर तक किसी भी पहुंच को अक्षम कर दिया गया है।

सूचना का साझाकरण

- यह सुनिश्चित करें कि आपके पास स्पष्ट संचार के चैनल हैं और अपने संगठन के वेंडर और सामने वाले पक्ष के साथ सुरक्षा मसलों पर संचार के लिए संपर्क के बिंदु मौजूद हैं।
- आंतरिक और बाह्य हितधारकों (वित्तीय प्रक्षेत्र के अधीन और बाहर के निकाय और सार्वजनिक प्राधिकार समेत) के साथ विश्वसनीय और कार्रवाई योग्य साइबर सुरक्षा की सूचना को समय पर साझा करने में शामिल रहें।
- अन्य संगठन खतरे, भेद्यता, घटनाएं के मामले में अपने वेंडर के साथ क्या अनुभव कर रहे हैं इसके प्रासंगिक अपडेट का पता करें और अपने संगठन की सुरक्षा के लिए प्रत्युत्तर तैयार करें और परिस्थिति-जन्य जागरूकता एवं शिक्षण को व्यापक करें। सूचना साझाकरण संगठन होने के नाते उदाहरण के लिए एफएस-आईएसएसी अप-टू डेट रहने की सुविधा प्रदान करेगा।

साइबर सुरक्षा को ध्यान में रखते हुए वेंडर का चयन कैसे करें

सक्षम वेंडर की साइबर तैयारी और जागरूकता और इसके परिणामस्वरूप उनसे आपके संगठन के जोखिम प्रोफ़ाइल पर पड़ने वाले प्रभाव को परखने के लिए निम्नलिखित प्रश्न उनसे पूछें:

1. **उनके क्या अनुभव रहे हैं?** वेंडर के क्लाइंट सेवा के इतिहास का पता करें। क्या इससे पहले उसने आपकी ही तरह के संगठन को सेवा दी है?
2. **क्या उन्होंने ज्ञात साइबर सुरक्षा मानदंड** जैसे कि एनआईएसटी फ्रेमवर्क या आईएसओ 27001 के साथ अपने अनुपालन को दस्तावेजीकृत किया है या क्या वे एसओसी2 रिपोर्ट उपलब्ध करा सकते हैं?
3. **अपनी सेवा देने के लिए आपके किस डेटा और/अथवा परिसंपत्ति को एक्सेस करने की उन्हें आवश्यकता होगी?** क्या वे स्पष्ट रूप से अनावश्यक एक्सेस का अनुरोध कर रहे हैं?
4. **उनके पास आपके संगठन के जो परिसंपत्तियाँ और डेटा हैं उसकी सुरक्षा की उनकी योजना क्या है?**
5. **वे स्वयं अपने तीसरे पक्ष साइबर जोखिम का प्रबंधन कैसे करते हैं?** क्या वे अपनी आपूर्ति श्रृंखला के बारे में सूचना उपलब्ध करा सकते हैं?
6. **आपके संगठन के परिसंपत्ति और/अथवा डेटा पर प्रभाव डालने वाली घटना होने की** स्थिति में आपदा से रिकवरी और व्यापार की निरंतरता के लिए उनकी योजना क्या है?
7. **वे आपके संगठन को किस प्रकार अद्यतन रखेंगे?** संचारी ट्रेंड्स, खतरे और संगठन के अंदर परिवर्तन के लिए उनकी योजना क्या है?

घटना प्रत्युत्तर गाइड

तैयारी

- अपने संगठन के वरिष्ठ नेतृत्व और अन्य प्रासंगिक कर्मी के साथ घटना प्रत्युत्तर और व्यापार निरंतरता के विकास हेतु कार्य करें जोकि सर्वाधिक दबाव मूलक जोखिम पर आधारित हो और जिसकी पहचान आपके संगठन के जोखिम आकलन में हुई हो।
  - आपके संगठन के सर्वोच्च-प्राथमिकता वाले साइबर जोखिमों से संबंधित घटनाओं के लिए खतरे के परिदृश्य विकसित करें। उन परिदृश्यों का जवाब देने के लिए क्षमता निर्माण पर ध्यान केंद्रित करें।
  - आपके संगठन के भीतर घटना की प्रतिक्रिया के लिए संपर्क के बिंदुओं की सूची को पहचानें, रिकॉर्ड करें और उपलब्ध कराएं।
  - उपयुक्त स्थानीय और संघीय कानून प्रवर्तन एजेंसियों और अधिकारियों के लिए संपर्क की जानकारी को पहचानें और रिकॉर्ड करें।
  - किस प्रकार की घटनाओं को सूचित किया जाना चाहिए, उन्हें कब और किसे सूचित किया जाना चाहिए, यह निर्दिष्ट करते हुए प्रावधान बनाएं।
  - लिखित दिशा-निर्देश तैयार करें जो इस बात को रेखांकित करे कि कर्मी कितनी तेजी से किसी घटना पर निश्चित तौर पर जवाब दें और उन्हें क्या कार्रवाई करनी चाहिए जोकि प्रासंगिक फैक्टर जैसे कि घटना के फंक्शनल और सूचनात्मक प्रभाव और घटना से बाहर निकलने की संभावना पर निर्भर हो।
  - सभी कर्मचारियों को अपनी तकनीकी टीम से संपर्क करने के लिए सूचित करें - आमतौर पर यह आईटी के कर्मचारी और/या सीआईएसओ/सीआईओ/ अन्य समतुल्य प्रबंधक होगा - जब कोई घटना होती है।
  - कर्मचारी की गतिविधियों पर नजर रखने और अंदरूनी खतरों और घटनाओं की पहचान को सक्षम करने के लिए समाधान लागू करें।
  - व्यापारिक आपातकाल के दौरान आपका संगठन प्राथमिक ग्राहकों और आपूर्तिकर्ताओं के साथ कैसे कार्य करेगा इस बात के समन्वयन के लिए व्यापार निरंतरता योजना को शामिल करें जिसमें यह भी शामिल हो कि अगर जरूरत हो तो आप मैनुअल या वैकल्पिक व्यापार प्रचालन का संचालन कैसे करेंगे।
  - आपातकालीन सिस्टम शट-डाउन और रीस्टार्ट के लिए लिखित प्रक्रियाओं को शामिल करें।
  - बैकअप डेटा की पुनर्प्राप्ति और पुनर्स्थापन के लिए, मान्यता के सत्यापन बैकअप डेटा की सामयिक जांच युक्तियों का विकास एंव जांच करना।
  - वैकल्पिक केंद्र/साइट पर व्यापार ऑपरेशन के प्रचालन हेतु स्थापित अनुबंध और प्रक्रियाओं का होना।
  - सभी ग्राहकों के लिए एक स्पष्ट प्रसार चैनल स्थापित करें।

अभ्यास करना

- सभी कर्मियों या कर्मियों के सभी स्तर के प्रतिनिधियों के साथ जिसमें संगठन के एग्जिक्यूटिव, पीआर/संचार कर्मी, और कानूनी और अनुपालन टीम शामिल हो, उन सबके साथ टेबलटॉप लघु अभ्यास का आयोजन करें।
- अपने संगठन के लिए प्रासंगिक उद्योग-दायरे के टेबलटॉप अभ्यासों की पहचान करें और आदर्श रूप से इसमें हिस्सेदारी करें।
- ऐसी प्रक्रियाओं की स्थापना कर यह सुनिश्चित करें कि अभ्यासों से मिली सीख को आत्मसात किया गया है और आपके संगठन की साइबर सुरक्षा रणनीति में इसकी चर्चा की गई है।

प्रत्युत्तर देना

- छवि संबंधी नुकसान के मद्देनजर प्रभाव को न्यूनतम करने के लिए घटना प्रत्युत्तर योजना की कार्रवाई का कार्यान्वयन करना।
- प्रभावित/समझौता हुए सिस्टम की पहचान करें और क्षति का आकलन करें।
- प्रभावित परिसंपत्ति को हटाकर (डिसकनेक्ट कर) क्षति को कम करें।
- जैसे ही टीम को संदेह हो कि कोई घटना घटी है यथाशीघ्र सभी सूचना की रिकॉर्डिंग आरम्भ कर दें। जब प्रभावित और चिह्नित परिसंपत्ति को डिसकनेक्ट/पृथक करते समय घटना के साक्ष्य को संरक्षित करने का प्रयास करें जैसे कि सिस्टम के कॉन्फ़िगरेशन, नेटवर्क का संग्रहण, और प्रभावित परिसंपत्ति से घुसपैठ डिटेक्शन लॉग का संग्रहण।
- यथोचित आंतरिक पक्षों, तीसरे पक्ष वेंडर और प्राधिकारों को अधिसूचित करें और अगर जरूरी हो तो सहायता का अनुरोध करें।
- ग्राहक अधिसूचना और सहायता गतिविधि शुरू करें जोकि कानून, नियमन और इंटर-एजेंसी गाइडेस के अनुरूप हों।
- खतरा साझाकरण प्लेटफार्म जैसे कि एफएस-आईएसएसी या एमआईएसपी का उपयोग उद्योग जगत को खतरे से अधिसूचित करने के लिए करें।
- बाद में समीक्षा हेतु घटना के दौरान उठाए गए सभी कदमों का दस्तावेजीकरण करें।

पुनर्बहाली

- अगर उपलब्ध हो तो आवर्ती "रिकवरी पॉइंट" में रिकवर किए गए परिसंपत्ति को पुन: भंडारित करें और सिस्टम के अंतिम "गुड" स्टेटस पर रीस्टोर करने के लिए बैकअप डेटा का उपयोग करें।
- रीस्टोर किए गए असेट से अपडेट किए हुए "स्वच्छ" बैकअप बनाएं और सुनिश्चित करें कि महत्वपूर्ण परिसंपत्ति के सभी बैकअप भौतिक रूप से और परिवेश के हिसाब से सुरक्षित लोकेशन में भंडारित किया गया है।
- इस बात की जांच और सत्यापन करें कि संक्रमित सिस्टम पूरी तरह रीस्टोर कर लिया गया है। पुष्टि करें कि प्रभावित सिस्टम सामान्य रूप से काम कर रहे हैं।

समीक्षा करना

- घटना घटने के बाद "सीखे गए सबक" चर्चा का संचालन करें- वरिष्ठ कर्मी, भरोसेमंद सलाहकार और कंप्यूटर सपोर्ट वेंडर(वेंडरों) के साथ बैठक करें और संभावित भेद्यता की समीक्षा कर लागू करने योग्य नए कदम की अनुशंसा प्राप्त करें।
- अगर संभव हो तो भेद्यता (चाहे वह सॉफ्टवेयर में हो या व्यापार प्रचालन या कर्मी के आचरण में हो) की पहचान करें जिसके कारण घटना घटी और इसके समाधान के लिए योजना का विकास करें।
- समान घटना या पहचाने गए मसले से संबंधित घटना से संबंधित आगे की किसी घटना की पहचान के लिए एक योजना का विकास करें।
- घटना के मद्देनजर सीखे गए सबक और सूचना को खतरा साझाकरण प्लेटफॉर्म जैसे कि एफएस-आईएसएसी पर साझा करें।
- अपने संगठन के घटना प्रत्युत्तर प्रोटोकॉल में सबक को जोड़ें।

रैंसमवेयर: रोकथाम और सुरक्षा

वास्तविक समय की सुरक्षा

रैंसमवेयर एक उभरता हुआ खतरा है क्योंकि दुर्भावनापूर्ण ढंग से कार्य करने वालों ने मैलवेयर से कंप्यूटर सिस्टम को बंधक बना कर मोनेटाइज़ करने का तरीका ढूंढ लिया है और उनकी रिहाई के लिए फिरौती का भुगतान करने की मांग करते हैं। अन्य मैलवेयर के विपरीत, जिन्हें अक्सर प्रभावी ढंग से काम करने के लिए लंबे समय तक छिपा रहना पड़ता है, रैंसमवेयर को स्पीयर-फ़िशिंग, गड़बड़ वेबसाइटों और करप्ट डाउनलोड के माध्यम से जल्दी निष्पादित करने के लिए बनाया जाता है। वित्तीय संस्थान विशेष रूप से रैंसमवेयर के प्रभाव की चपेट में आने के खतरे में रहते हैं, क्योंकि इससे धन को जल्दी और कुशलता से स्थानांतरित करने की क्षमता को खतरा हो सकता है और क्योंकि उन्हें लाभदायक लक्ष्य माना जाता है। हालांकि, बदमाश लोग कभी-कभी अपने वादे तोड़ते हैं: फिरौती का भुगतान करने के बाद भी, कुछ हमलावर मैलवेयर नहीं हटाते हैं या गोपनीय डेटा को नहीं छोड़ते हैं।

- ऐसी एंटी-मैलवेयर सुरक्षा प्रणालियों में निवेश करें जो वास्तविक समय में नए खतरे की खुफिया जानकारी के अनुकूल हैं।
- नेटवर्क से जुड़े सभी उपकरणों की सुरक्षा का मूल्यांकन करें जिसमें संवेदनशील या आवश्यक जानकारी रहती है। सभी सभी गैर-अनिवार्य प्रणालियों को एक अलग नेटवर्क में कनेक्ट करें।
  - अपने कार्यक्षेत्र में एलओटी या "स्मार्ट डिवाइसेस" को लाते समय विशेष रूप से सावधान रहें, क्योंकि इन प्रणालियों में अक्सर कमजोर या गैर-मौजूद सुरक्षा प्रणालियाँ होती हैं और इन्हें आवश्यक प्रणालियों तक पहुँच बिंदुओं के रूप में लक्षित किया जा सकता है।
  - रिपोट वर्क सेटअप की सुरक्षा पर विचार करें। सुनिश्चित करें कि सुरक्षा उपकरण सभी वेब ट्रैफ़िक की निगरानी के लिए ऑफ-नेटवर्क काम करते हैं।
- फ़िशिंग हमलों और शक्तिशाली पासवर्ड सुरक्षा की आवश्यकता पर कर्मचारी की शिक्षा को बढ़ावा दें।
- यदि संभव हो तो अपने संगठन में कई कारकों वाले प्रमाणीकरण को लागू करने पर विचार करें।
- सभी सिस्टम और सॉफ्टवेयर को नियमित रूप से अपडेट रखें। यदि संभव हो तो स्वचालित अपडेट की अनुमति के लिए सेटिंग्स बदलें।
- इस बात के लिए घटना की प्रतिक्रिया और संकट प्रबंधन योजना विकसित करें कि रैंसमवेयर हमले और मूल्यवान डेटा के नुकसान से कैसे निपटें।
- रैंसमवेयर हमले की स्थिति में एक बाहरी संचार योजना तैयार करें।

डेटा बैकअप

- सुरक्षित, नियमित रूप से अपडेटेड बैकअप सिस्टम में निवेश करें जो आपके डेटा को सुरक्षित रखे।
  - यदि यूएसपी या हार्ड ड्राइव का उपयोग करते हैं, तो बैकअप समाप्त होने के बाद नेटवर्क वाले कंप्यूटर से इन उपकरणों को भौतिक रूप से निकाल दें।
  - यदि क्लाउड स्टोरेज का उपयोग कर रहे हैं, तो सर्वर को उच्च-स्तर के एन्क्रिप्शन और कई कारकों वाले प्रमाणीकरण से लैस करें।
- सबसे खराब मामले में आपदा से उबरने के लिए सामान्य बही-खाता की केवल एक रीड-ओनली प्रतिलिपि बनाएं।
- ऐसी प्रणालियाँ विकसित करें जो स्वचालित डेटा रिकवरी और सुधार करती हैं।
- महत्वपूर्ण डेटा और व्यावसायिक सेवाओं को पुनर्प्राप्त करने में कितना समय लगेगा, इसका आकलन करने के लिए परिदृश्य बनाएं।

नियामक वातावरण

- अपने संचालन वातावरण में रैंसमवेयर के लिए उपयुक्त विनियामक और कानूनी मार्गदर्शन का मूल्यांकन करें।
  - देश-विशिष्ट मार्गदर्शन पर विचार करें। बदलते मार्गदर्शन के आवधिक मूल्यांकन के लिए एक योजना बनाएं।
  - वित्तीय-क्षेत्र के विशिष्ट मार्गदर्शन पर विचार करें।
  - अंतरराष्ट्रीय कानूनी और नियामक आवश्यकताओं पर विचार करें।
- फिरौती देने से जुड़े जोखिमों का आकलन करें। कुछ मामलों में, फिरौती का भुगतान करने से प्रतिरोधी सक्रियक के खिलाफ मौजूदा प्रतिबंधों का उल्लंघन हो सकता है।
- स्थानीय कानून प्रवर्तन के साथ संपर्क करें। हमले की स्थिति में त्वरित सूचना साझा करने के लिए संपर्क बनाएं।
- रैंसमवेयर के लिए साइबर बीमा पॉलिसियों के लाभों और कमियों का आकलन करें।

आपके संगठन की रैंसमवेयर की तैयारी को मापना

रैंसमवेयर की रोकथाम और सुरक्षा योजना बनाते समय निम्नलिखित प्रश्नों पर विचार करें।

1. क्या आपके संगठन के पास **नियमित रूप से निर्धारित बैकअप है**?
   - क्या ये बैकअप आपके नेटवर्क से हटे हुए हैं, या तो क्लाउड स्टोरेज सिस्टम या एयर-गैप्ड यूएसवी/हार्ड ड्राइव के माध्यम से?
2. क्या आपके संगठन के नेटवर्क से कोई भी **गैर अनिवार्य** उपकरण जुड़ा हुआ है?
   - क्या उन्हें अन्य नेटवर्क में स्थानांतरित किया जा सकता है जिनमें संवेदनशील डेटा नहीं रखा गया हैं?
3. क्या आपका संगठन फिरौती देने से जुड़े **विनियामक और कानूनी जोखिमों** को समझता है?
   - इस पर कानूनी मार्गदर्शन एक देश से दूसरे देश में भिन्न होता है और अक्सर अपडेट किया जाता है।
4. क्या आपका संगठन नियमित रूप से अपने सॉफ्टवेयर और सिस्टम को अपडेट करता है? क्या अपडेट्स**स्वचालित हैं**?
5. क्या आपके संगठन के पास एक योजना है **कि रैंसमवेयर के हमले और बहुमूल्य डेटा के नुकसान से कैसे निपटें?**
6. क्या आपके संगठन की **साइबर बीमा पॉलिसी** है? यदि है, तो यह योजना रैंसमवेयर हमलों को कैसे कवर करती है?
   - कुछ योजनाएं स्पष्ट रूप से फिरौती के भुगतान पर रोक लगाती हैं, जबकि अन्य इस तरह के भुगतान को नीति के हिस्से के रूप में शामिल करती हैं।

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
INTERNATIONAL MONETARY FUND
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA INDEPENDENT COMMUNITY BANKERS of AMERICA®

कार्यबल का विकास

आवश्यकताओं की पहचानना

- अपने काम के बोझ की आवश्यकताओं को पहचानें।
  - अपने संचालन की जटिलता और उस गति का मूल्यांकन करें जिसके साथ कार्यों को निष्पादित करने की आवश्यकता है।
  - बढ़ती क्षमता की जरूरतों पर विचार करें और विचार करें क्या उन्नत तकनीकें हमले के फ़लक को कम करने में मदद कर सकती हैं।
- अपने कार्यबल की आवश्यकताओं को पहचानें।
  - अपने संगठन में साइबर सुरक्षा कार्यबल की योग्यता, लचीलेपन और दक्षता पर विचार करें।
  - आदर्श रिपोर्टिंग संरचनाओं को पहचानें और वहां पर उजागर करें जहां बहु-कार्यक्षमता बेहतर है।
- उनके द्वारा ली गई भूमिकाओं और उनके द्वारा समर्थित व्यवसायिक कार्यों के आधार पर अपने कार्यबल के आवश्यक ज्ञान, कौशल, योग्यता और योग्यता को परिभाषित करें।
- अपने संगठन के मौजूदा साइबर सुरक्षा कार्यबल में महत्वपूर्ण कमी की पहचान करें।
  - भूमिकाओं और जिम्मेदारियों के आंतरिक आकलन के मार्गदर्शन के लिए एनआईसीई फ्रेमवर्क जैसे मौजूदा उपकरणों को लागू करें।

आंतरिक प्रशिक्षण और विकास को आगे बढ़ाना

- कैरियर मैप बनाएं जो आपके साइबर सुरक्षा कार्यबल के लिए उन्नति ट्रैक को प्रदर्शित करता है
- साइबर सुरक्षा भूमिकाओं में प्रतिभावान कर्मचारियों को बनाए रखने और पुन:स्थिति निर्धारण के लिए अपने संगठन के भीतर रास्ते को पहचानें।
  - रूचि और क्षमता के आधार पर साइबर सुरक्षा में गैर-पारंपरिक प्रवेश-बिंदुओं पर विचार करें।
  - अपने संगठन के भीतर अपस्किलिंग और पुनः- प्रशिक्षण कार्यक्रमों का विस्तार करें और पारगमन को प्रोत्साहित करें।
- आंतरिक प्रशिक्षण और स्वतंत्र रूप से सीखने को प्रोत्साहित करें।
  - निरंतर शिक्षा और कौशल प्रमाणन के लिए अवसर खोलें।
- कार्यबल को बनाए रखने के लिए डेटा की निगरानी करें।
  - यह पहचानने के लिए समय-समय पर अवधारित डेटा का मूल्यांकन करें कि क्या प्रशिक्षण और विकास कार्यक्रम कर्मचारी की जरूरतों को पूरा कर रहा है।

बाहरी भर्ती में सुधार

- स्पष्ट, आंतरिक रूप से सुसंगत नौकरी के विवरण लिखकर जॉब पोस्टिंग को मजबूत करें।
  - उपयुक्त कौशल सेट को उजागर करने के लिए एनआइसीई फ्रेमवर्क जैसे मौजूदा उपकरणों का उपयोग करें।
- आवेदन प्रक्रिया के माध्यम से भर्ती पर डेटा इकट्ठा करें, आवेदकों के प्रकार और पिछले कार्य अनुभवों को कैप्चर करें।
  - डेटा एकत्रण को व्यवस्थित करें और साइलो निर्माण को रोकने और टैलेंट उद्गम और विकास का समर्थन करने के लिए पूरी कंपनी में साझा करें।
  - पहुंच में कमी की पहचान करने के लिए समय-समय पर भर्ती डेटा का मूल्यांकन करें।
- उम्मीदवार की क्षमता का आकलन करने के लिए कई संकेतकों पर भरोसा करें।
  - व्यवस्थित हायरिंग के आकलन को लागू करने पर विचार करें।
  - उपयुक्त डिग्री, प्रमाणपत्र और कार्य अनुभव का मूल्यांकन करें।
  - हायर करने का निर्णय लेते समय एक विशिष्ट मीट्रिक (जैसे, इंजीनियरिंग में स्नातकोत्तर स्तर की डिग्री) पर भरोसा करने से बचें।

मूलभूत दृष्टिकोण

साइबर सुरक्षा कार्यबल बनाते समय निम्नलिखित रणनीतिक दृष्टिकोणों पर विचार करें।

1. नई प्रतिभाओं को पैदा करने वाली **आपूर्ति पाइपलाइन** का **विस्तार करें।**
   - क्या आपके विश्वविद्यालयों और तकनीकी कॉलेजों के साथ संबंध हैं?
   - क्या आप साइबर सुरक्षा इंटर्नशिप या अप्रेंटिसशिप प्रदान करते हैं?
2. **टैलेंट ओपनिंग के साथ मौजूदा आपूर्ति की पहचान और मिलान करें।**
   - क्या आपका मानव संसाधन विभाग आवश्यक कौशल को पोस्ट किए गए नौकरी विवरण में कुशलता से दिखला रहा है?
3. **मौजूदा कर्मचारियों** को साइबर कार्यबल का हिस्सा बनने के लिए **पुनः प्रशिक्षित** करें।
   - क्या आपका संगठन संसाधनों को अपने साइबर कार्यबल में स्थानांतरित करके मौजूदा प्रतिभा का लाभ उठा रहा है?
4. **तकनीकी नवाचार** के माध्यम से अपने साइबर कर्मचारियों **की मांगों को कम करें।**
   - क्या महत्वपूर्ण अवधि के दौरान क्षमता वृद्धि करने के लिए आपके तीसरे पक्ष के सेवा प्रदाताओं के साथ समझौते हैं?
5. वर्तमान कार्यबल के बने रहने में सुधार करें।
   - क्या आपका संगठन टीम के प्रतिभाशाली सदस्यों में निवेश कर रहा है?
   - क्या आपका संगठन इच्छुक व्यक्तियों को साइबर सुरक्षा में करियर तलाशने की अनुमति देता है?