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?