छोटे संगठनों के लिए साइबर सुरक्षा

सीआईएसओ चेकलिस्ट: तीसरे पक्ष से कनेक्शन की सुरक्षा करना

साइबर सुरक्षा को दिमाग में रखते हुए वेंडर चुनना

हर बार जब आप संभावित वेंडर का मूल्यांकन कर रहे हो तो निम्नलिखित प्रश्नों की जांच करें:

- ☐ उन्हें आपके संगठन की तरह ग्राहकों की सेवा करने का क्या अनुभव है?
- ☐ क्या उन्होंने ज्ञात साइबर सुरक्षा मानकों (जैसे NIST फ्रेमवर्क या आईएसओ 27001, या क्या वे एक एसओसी2 रिपोर्ट प्रदान कर सकते हैं) के साथ उनके अनुपालन का दस्तावेजीकरण किया है?
- ☐ उन्हें उनकी सेवाओं को देने के लिए आपके कौन से डेटा और/या परिसंपत्तियों के उपयोग करने की आवश्यकता होगी, और क्या वे किसी भी बिल्कुल अनावश्यक एक्सेस का अनुरोध कर रहे हैं?
- ☐ वे आपके संगठन की उन परिसंपत्तियों और डेटा की रक्षा करने की योजना कैसे बनाते हैं जो उनके अधिकार में हैं?
- ☐ वे अपने खुद के तीसरे पक्ष के साइबर जोखिम का प्रबंधन कैसे करते हैं, और क्या वे अपनी आपूर्ति श्रृंखला सुरक्षा के बारे में जानकारी प्रदान कर सकते हैं?
- ☐ यदि कोई घटना आपके संगठन को प्रभावित कर रही है तो आपदा से बहाली और व्यापार की निरंतरता के लिए उनकी क्या योजना है?
- ☐ वे आपके संगठन के भीतर के रुझानों, खतरों और परिवर्तनों का संचार करने के संदर्भ में आपके संगठन को कैसे अपडेट रखेंगे?

तीसरे पक्ष के द्वारा जोखिम को पहचानें

निम्नलिखित कदमों को शामिल करते हुए एक तीसरे पक्ष का साइबर जोखिम मूल्यांकन करें:

- ☐ सभी वेंडर संबंधों और परिसंपत्तियों और प्रत्येक में उजागर होने वाले डेटा की एक सूची बनाएं और लगातार अपडेट करें।
- ☐ उस डेटा की समीक्षा करें जिसकी प्रत्येक वेंडर या तीसरे पक्ष तक पहुंच है, ताकि सुनिश्चित किया जा सके कि पहुंच का प्रत्येक स्तर 'न्यूनतम विशेषाधिकार' के सिद्धांत का पालन करता है।
- ☐ उस प्रभाव के आधार पर अपने वेंडर्स और तीसरे पक्ष के संबंधों (निम्न, मध्यम, उच्च) को रैंक करें जो उनके सिस्टम के उल्लंघन के कारण आपके संगठन पर होगा।
- ☐ उच्चतम जोखिम वाले वेंडर्स के साथ शुरू करते हुए, प्रत्येक प्रदाता की साइबर सुरक्षा क्षमताओं और उपयुक्त मानकों के अनुपालन का मूल्यांकन करें।
- ☐ नियमित सुरक्षा मूल्यांकन के लिए एक योजना बनाएं, यह ध्यान में रखते हुए कि आप कभी-कभी सबसे अधिक जोखिम वाले और/या ग्राहक डेटा तक सबसे अधिक पहुंच वाले वेंडर्स के ऑन-साइट मूल्यांकन करना चाह सकते हैं।

तीसरे पक्ष की सुरक्षा को प्रबंधित करना

- ☐ सम्यक उद्यम के माध्यम से करें। वेंडरों के साथ प्रस्तावों, अनुबंधों, व्यापार निरंतरता, घटना की प्रतिक्रिया और सेवा स्तर के समझौतों के लिए सभी अनुरोधों में साइबर सुरक्षा की अपेक्षाएँ स्थापित करें। साइबर घटना के मामले में जिम्मेदारियों और उत्तरदायित्वों पर सहमति हों।
- ☐ वित्तीय संगठनों और अन्य संस्थाओं की साइबर सुरक्षा व्यवहार के बारे में पूछताछ करें, जिनके साथ आप लेनदेन करते हैं या डेटा साझा करते हैं, यह ध्यान में रखें कि आपके वेंडर और तीसरे पक्ष को किसी भी साइबर सुरक्षा आवश्यकताओं का पालन करना चाहिए जिसे आपके संगठन को पूरा करना चाहिए।

- ☐ साइबर सुरक्षा मानकों के साथ आपके वेंडर्स के अनुपालन की निगरानी करने के स्थापित और सहमत उपायों का उपयोग करें।
- ☐ यह देखने के लिए अपने वेंडर्स के साथ जांच करें जो संवेदनशील डेटा को संभालते हैं कि क्या वे आपके साथ उनके किसी भी खाते के लिए दो-कारक प्रमाणीकरण, एन्क्रिप्शन या अन्य सुरक्षा उपाय ऑफर करते हैं।
- ☐ सुनिश्चित करें कि आपके द्वारा इंस्टॉल किए गए सभी तीसरे पक्ष के सॉफ़्टवेयर और हार्डवेयर में एक सुरक्षा हैंडशेक है ताकि बूटिंग प्रक्रिया प्रमाणीकरण कोड के माध्यम से सुरक्षित हो और कोड मान्यता प्राप्त नहीं होने पर निष्पादित नहीं होगा।
- ☐ यदि आप ऐसे वेंडर उत्पादों का सामना करते हैं जो या तो नकली हैं या विनिर्देशों से मेल नहीं खाते हैं, तो एक प्रस्ताव पर बातचीत करने के लिए काम करें या एक बाहर निकलने की रणनीति बनाएं।
- ☐ वेंडर अनुबंधों का वार्षिक मूल्यांकन करें और सुनिश्चित करें कि वे आपके रणनीतिक दिशा-निर्देश और नियामक डेटा सुरक्षा आवश्यकताओं को निरंतर पूरा करते हैं। अनुबंध समाप्त होने पर, आपने परिसंपतियों 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।

जानकारी साझा करना

- ☐ सुनिश्चित करें कि आपके पास अपने संगठन के वेंडर और समकक्षों के साथ सुरक्षा कि मुद्दों के बारे में संचार करने के लिए स्पष्ट संचार चैनल और संपर्क के बिंदु हैं।
- ☐ जाँच करें कि आपने आंतरिक और बाह्य हितधारकों (वित्तीय क्षेत्र के भीतर और बाहर के संस्था और सार्वजनिक प्राधिकरण सहित) के साथ विश्वसनीय, कार्रवाई योग्य साइबर सुरक्षा जानकारी को समय पर साझा करने के लिए प्रक्रियाएं लागू की है।
- ☐ उसके बारे में उपयुक्त अपडेट्स को ट्रैक करें कि अन्य संगठन एफएस-आईएसएसी जैसी जानकारी को साझा करने वाले संगठनों और अन्य खतरों की जानकारी पाने वाले स्त्रोतों का हिस्सा बनकर खतरों, कमजोरियों, घटनाओं और प्रतिक्रियाओं के संदर्भ में उनके तीसरे पक्ष के साथ क्या अनुभव कर रहे हैं।