छोटे संगठनों के लिए साइबर सुरक्षा

घटना की प्रतिक्रिया चेकलिस्ट

तैयारियां

- ☐ आपके संगठन के साइबर जोखिम मूल्यांकन में पहचाने गए सबसे अधिक गंभीर जोखिमों के आधार पर एक घटना प्रतिक्रिया और व्यवसायिक निरंतरता योजना को विकसित करने के लिए अपने संगठन के वरिष्ठ नेतृत्व और अन्य संबंधित कर्मचारियों के साथ काम करें।
- ☐ 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 बनाएं जो रूपरेखा बनाता है कि किसी घटना की प्रतिक्रिया कर्मियों को कितनी जल्दी देनी चाहिए और उपयुक्त कारकों के आधार पर कौन सी कार्यवाही की जानी चाहिए, जैसे घटना का कार्यात्मक और जानकारी का प्रभाव, और और घटना से वापस बहाली की संभावना।
- ☐ 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।
- ☐ यह समन्वय करने के लिए व्यवसायिक निरंतरता योजनाओं को शामिल करें कि आपकी संस्था व्यवसायिक आपातकाल के दौरान आपूर्तिकर्ताओं और प्राथमिक ग्राहकों के साथ कैसे काम करेगी, जिसमें शामिल है कि यदि आवश्यक हो तो आप मैनुअल और वैकल्पिक व्यवसायिक संचालन को कैसे करेंगे।
- ☐ इसमें आपातकालीन प्रणाली को बंद करने और दोबारा शुरू करने के लिए लिखित प्रक्रियाएं शामिल हैं।
- ☐ बैकअप डेटा को पुनः प्राप्त करने और पुनर्स्थापित करने; समय-समय पर इसकी वैधता को सत्यापित करने के लिए बैकअप डेटा का परीक्षण करने के लिए तरीकों का विकास और परीक्षण करें।
- ☐ एक वैकल्पिक सुविधा/साइट में व्यावसायिक संचालन करने के लिए समझौते और प्रक्रियाएं स्थापित की हुई है।
- ☐ सभी ग्राहकों के लिए एक स्पष्ट प्रसार चैनल स्थापित करें।
- ☐ बैकअप डेटा को पुनः प्राप्त करने और पुनर्स्थापित करने; समय-समय पर इसकी वैधता को सत्यापित करने के लिए बैकअप डेटा का परीक्षण करने के लिए तरीकों का विकास और परीक्षण करें।
- ☐ एक वैकल्पिक सुविधा/साइट में व्यावसायिक संचालन करने के लिए समझौते और प्रक्रियाएं स्थापित की हुई है।
- ☐ सभी ग्राहकों के लिए एक स्पष्ट प्रसार चैनल स्थापित करें।

अभ्यास

- ☐ सभी कर्मचारियों या कर्मचारियों के सभी स्तरों के प्रतिनिधियों के साथ छोटे टेबलटॉप अभ्यास आयोजित करें, जिसमें आपके संगठन के एक्सीक्यूटिव, पीआर/संचार कर्मचारी और कानूनी और अनुपालन टीमें शामिल हो।
- ☐ अपने संगठन के लिए प्रासंगिक उद्योग-व्यापी टेबलटॉप अभ्यास को पहचानें और आदर्श रूप से भाग लें।
- ☐ इस बात को सुनिश्चित करने के लिए एक प्रक्रिया स्थापित करें कि अभ्यास से सीखे गए पाठ को आपकी कंपनी की साइबर सुरक्षा रणनीति में शामिल और संबोधित किया गया है।

प्रतिक्रिया देना

- ☐ व्यवसाय संचालन पर प्रभाव को कम करने के लिए घटना प्रतिक्रिया योजना की कार्रवाइयों को लागू करें।
- ☐ प्रभावित हुई/ समझौता की गई प्रणालियों को पहचानें और नुकसान का आकलन करें।
- ☐ प्रभावित परिसंपत्तियों को हटाकर (डिस्कनेक्ट करके) नुकसान को कम करें।
- ☐ जैसे ही टीम को संदेह होता है कि कोई घटना हुई है, सभी सूचनाओं को रिकार्ड करना शुरू करें। प्रभावित चिन्हित संपत्तियों को पृथक/ अलग करते समय घटना के साक्ष्य को संरक्षित करने का प्रयास करें, जैसे प्रभावित परिसंपत्तियों से सिस्टम कॉन्फ़िगरेशन, नेटवर्क और घुसपैठ का पता लगाने वाले लॉग को एकत्र करें।
- ☐ उपयुक्त आंतरिक पक्षों, तीसरे पक्ष के वेंडर, और अधिकारियों को सूचित करें और यदि आवश्यक हो तो सहायता का अनुरोध करें।
- ☐ कानूनों, विनियमों और अंतर-एजेंसी मार्गदर्शन के अनुरूप ग्राहक को सूचित करने और सहायता की गतिविधियाँ शुरू करें।
- ☐ उद्योग को खतरे के बारे में सूचित करने के लिए एफएस-आईएसएसी या एमआईएसपी जैसे खतरों को साझा करने वाले प्लेटफार्मों का उपयोग करें।
- ☐ बाद में समीक्षा करने के लिए घटना के दौरान उठाए गए सभी चरणों को दस्तावेजीकृत करें।

समस्या से उबरना

- ☐ यदि उपलब्ध हो तो रिकवरी किये गए परिसंपत्तियों को समय-समय पर "रिकवरी पॉइंट" पर पुनर्स्थापित करें और सिस्टम को पिछली ज्ञात "अच्छी" स्थिति पर पुनर्स्थापित करने के लिए बैकअप डेटा का उपयोग करें।
- ☐ पुनर्स्थापित परिसंपत्तियों से अपडेट किया गया "नया" बैकअप बनाएं और सुनिश्चित करें कि सभी महत्वपूर्ण परिसंपत्तियों के बैकअप को भौतिक और पर्यावरणीय रूप से सुरक्षित स्थान पर संग्रहीत किये गए हैं।
- ☐ परीक्षण करें और सत्यापित करें कि संक्रमित सिस्टम पूरी तरह से बहाल हो गया हैं। पुष्टि करें कि प्रभावित सिस्टम सामान्य रूप से काम कर रहे हैं।

समीक्षा करना

- ☐ घटना घटित होने के बाद "सीखे गये सबक" चर्चा का आयोजन करें - संभावित कमजोरियों की समीक्षा करने या नए कदमों को लागू करने की सिफारिश करने के लिए वरिष्ठ कर्मचारियों, विश्वसनीय सलाहकारों और कंप्यूटर सपोर्ट वेंडर (वेंडर) से मिलें।
- ☐ संभव हो तो, उन कमजोरियों की पहचान करें (चाहे सॉफ्टवेयर, हार्डवेयर, व्यावसायिक संचालन, या कर्मचारियों के व्यवहार में) जिसके कारण घटना हुई और उनकी गंभीरता को कम करने की योजना बनाएं।
- ☐ पुष्टि करें कि प्रभावित सिस्टम सामान्य रूप से काम कर रहे हैं।
- ☐ पहचानी गई समस्याओं से संबंधित समान या आगे की घटनाओं का पता लगाने की निगरानी के लिए एक योजना बनाएं।
- ☐ खतरों को साझा करने वाले प्लेटफॉर्म जैसे एफएस-आईएसएसी पर सीखे गए सबक और घटना के बारे में जानकारी साझा करें।
- ☐ सीखे गए सबक को अपने संगठन की घटना प्रतिक्रिया प्रोटोकॉल में एकीकृत करें।