छोटे संगठनों के लिए साइबर सुरक्षा

रैंसमवेयर चेकलिस्ट

रैंसमवेयर की तैयारी

☐ **जब आप एक रैंसमवेयर की रोकथाम और संरक्षण योजना बनाते हैं, तो समय-समय पर निम्नलिखित का आकलन करें:**

- क्या आपके संगठन के पास नियमित रूप से निर्धारित बैकअप है?
- क्या आपके संगठन के नेटवर्क से कोई भी गैर-अनिवार्य उपकरण जुड़ा हुआ है?
- क्या आपका संगठन फिरौती देने से जुड़े विनियामक और कानूनी जोखिमों को समझता है?
- क्या आपका संगठन नियमित रूप से अपना सॉफ्टवेयर सिस्टम अपडेट करता है? क्या ये अपडेट स्वचालित हैं?
- क्या आपके संगठन के पास रैंसमवेयर के हमले और डेटा के नुकसान से निपटने की कोई योजना है?
- क्या आपके सिस्टम के पास साइबर बीमा पॉलिसी है? यदि है, तो यह योजना रैंसमवेयर हमलों को कैसे कवर करती है?

वास्तविक समय की सुरक्षा

☐ **उन एंटी-मैलवेयर सुरक्षा प्रणालियों में निवेश करें जो वास्तविक समय में नए खतरे की खुफिया जानकारी के अनुकूल हो।**

☐ **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।
- ☐ 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 सुरक्षाओं की आवश्यकता के बारे में कर्मचारी की शिक्षा को बढ़ावा देना।**

☐ **यदि संभव हो तो अपने संगठन में कई कारकों वाले प्रमाणीकरण को लागू करने पर विचार करें।**

☐ **सभी सॉफ्टवेयर और सिस्टम को नियमित रूप से अपडेट रखें।**

- ☐ यदि संभव हो तो स्वचालित अपडेट की अनुमति के लिए सेटिंग्स बदलें।

☐ **इसके लिए एक घटना की प्रतिक्रिया और संकट प्रबंधन योजना बनाएं कि रैंसमवेयर हमले और बहुमूल्य 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 सर्वर्स 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 बनाएं 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 पर्यावरण

- ☐ **अपने संचालन वातावरण में रैंसमवेयर के लिए उपयुक्त विनियामक और कानूनी मार्गदर्शन का मूल्यांकन करें।**
  - ☐ देश-विशिष्ट मार्गदर्शन पर विचार करें।
  - ☐ वित्तीय-क्षेत्र के विशिष्ट मार्गदर्शन पर विचार करें
  - ☐ अंतरराष्ट्रीय कानूनी और नियामक आवश्यकताओं पर विचार करें।
  - ☐ बदलते मार्गदर्शन के आवधिक मूल्यांकन के लिए एक योजना बनाएं।
- ☐ फिरौती देने से जुड़े जोखिमों का आकलन करें।
- ☐ 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।