छोटे संगठनों के लिएसाइबर सुरक्षा

सीआईएसओ चेकलिस्ट: अपने संगठन की सुरक्षा करना

जोखिम-आधारित सूचना सुरक्षा कार्यक्रम विकसित करना

- ☐ **सभी प्रकार की जानकारी को पहचानें और सूची बनाएं जिसे आपका व्यवसाय संग्रहित और उपयोग करता है (जैसे ग्राहक का नाम और ईमेल)।**
- ☐ **प्रत्येक प्रकार की जानकारी के लिए पूछें और उत्तर रिकॉर्ड करें:**
  - यदि यह जानकारी सार्वजनिक कर दी जाती तो क्या होगा?
  - यदि यह जानकारी गलत हो, तो मेरे व्यवसाय का क्या होगा?
  - यदि मैं/मेरे ग्राहक इस जानकारी तक नहीं पहुँच सकते तो मेरे व्यवसाय का क्या होगा?
- ☐ **रिकार्ड करें कि आपके द्वारा पहचानी गई जानकारी के संपर्क में कौन सी तकनीक आती है। इसमें हार्डवेयर (जैसे कंप्यूटर) और सॉफ़्टवेयर एप्लिकेशन (जैसे ब्राउज़र ईमेल) शामिल हो सकते हैं।**
  - जहां लागू हो, अपने व्यवसाय के बाहर की प्रद्योगिकियों (जैसे"क्लाउड") और किन्हीं लागू सुरक्षा तकनीकों, जैसे फायरवॉल को शामिल करें।
  - उन तकनीकों को शामिल करें, जिनका उपयोग घर से काम करने की स्थिति में उपयोग किया जा सकता है।
  - 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।
- ☐ **अपने राष्ट्रीय सीईआरटी, एफएस-आईएसएसी, आपके स्थानीय इंफ्रागार्ड चैप्टर और अन्य से नियमित रूप से जानकारी की समीक्षा करें कि वित्तीय क्षेत्र किन खतरों और कमजोरियों का सामना कर सकता है और इसका अनुमान लगाएं कि आप कितना प्रभावित हो सकते हैं।**
- ☐ **महीने में कम से कम एक बार अतिसंवेदनशीलता स्कैन या विश्लेषण करें।**
- ☐ **अपने संगठन के लिए एक साइबर सुरक्षा नीति बनाएं, जिसमें 'घर से काम करने' का प्रोटोकॉल शामिल हो।**
- ☐ **सभी कर्मचारियों को नीति के विवरण पर प्रशिक्षित करें और उनसे दस्तावेज़ों पर हस्ताक्षर कराएं जो नीति का पालन करके आपके संगठन की साइबर सुरक्षा को बनाए रखने में उनकी भूमिका को स्वीकार करता है।**
- ☐ **आंतरिक खतरों के विरूद्ध एक सुरक्षा योजना बनाएं, जिसमें उद्योग-जोखिम मूल्यांकन और अभिगम नियंत्रण प्रबंधन शामिल हो।**

मैलवेयर से नुकसान को रोकना

- ☐ **अपने फ़ायरवॉल को सक्रिय करें और एक्सेस कंट्रोल सूची (एलसीएलएस) सेट करें। व्हाइटलिस्टिंग सेटिंग का उपयोग करके पहुंच को प्रतिबंधित करें।**
- ☐ **सभी कंप्यूटर और लैपटॉप पर एंटीवायरस सॉफ़्टवेयर और एंटीस्पाइवेयर का उपयोग करें।**
  - ☐ सुनिश्चित करें कि सुरक्षा उपकरण "घर से काम करने' के वातावरण में प्रभावी ढंग से काम कर सकते हैं।
- ☐ **निर्माताओं और वेंडर्स द्वारा प्रदान किए गए नवीनतम सॉफ़्टवेयर अपडेट लागू 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।**
- ☐ **सुनिश्चित करें कि सभी होस्ट क्लॉक्स सिंक्रनाइज़ हैं।**
- ☐ **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। बाहरी स्रोतों से यूएसबी का उपयोग करने या अपनी यूएसबी को दूसरों को देने के जोखिम पर कर्मचारियों को 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 संगठन की संपत्ति और प्रणालियों का मूल्यांकन करने के लिए एक पेनीट्रेसन टेस्टिंग सेवा को हायर करने रखने पर विचार करें।**

कर्मचारियों का प्रशिक्षण

- ☐ **सभी नए कर्मचारियों को ऑनबोर्डिंग करने के दौरान और वर्तमान कर्मचारियों के लिए साल में कम से कम एक बार नियमित अंतराल पर अनिवार्य साइबर सुरक्षा प्रशिक्षण चलाने की योजना बनाएं। 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।
- ☐ **नकली खातों से फ़िशिंग स्टाइल के ईमेल भेजने जैसे मिथ्याभास के माध्यम से कर्मचारी जागरूकता की नियमित परीक्षण करें। किसी भी कर्मचारी की असफलताओं का आकलन करें और उन्हें सीखने और सुधार के अवसरों के रूप में उपयोग करें।**

अपने डेटा की सुरक्षा करना

- ☐ **अपने महत्वपूर्ण डेटा (जैसे दस्तावेज़, ईमेल, कैलेंडर) का नियमित बैकअप लें और परीक्षण करें कि उन्हें पुनर्स्थापित किया जा सकता है। क्लाउड पर बैकिंग अप करने पर विचार करें।**
- ☐ **सुनिश्चित करें कि आपके बैकअप वाले डिवाइस को मूल प्रतिलिपि वाली डिवाइस से स्थायी रूप से कनेक्ट नहीं किया गया है, न तो भौतिक रूप से और न ही स्थानीय नेटवर्क पर।**
- ☐ **सर्ज प्रोटेक्टर इंस्टॉल करें, जनरेटर का उपयोग करें, और सुनिश्चित करें कि आपके सभी कंप्यूटर और महत्वपूर्ण नेटवर्क उपकरण निर्बाध विद्युत आपूर्ति में प्लग किए गए हैं।**
- ☐ **मोबाइल डिवाइस प्रबंधन (एमडीएम) समाधान का उपयोग करें।**

अपने उपकरण को सुरक्षित रखें

- ☐ **मोबाइल उपकरणों के लिए पिन या पासवर्ड सुरक्षा को चालू करें। उपकरणों को कॉन्फ़िगर करें ताकि खो जाने या चोरी होने पर उन्हें ट्रैक किया जा सके, दूर से मिटाया या बंद किया जा सके।**
- ☐ **यदि उपलब्ध हो तो 'स्वचालित अपडेट' का उपयोग करके, अपने उपकरणों (सभी इंस्टॉल्ड ऐप्स) को अप टू डेट रखें।**
- ☐ **संवेदनशील डेटा भेजते समय, सार्वजनिक वाई-फाई हॉटस्पॉट से कनेक्ट न करें - सेलुलर कनेक्शन (टेथरिंग और वायरलेस डोंगल सहित) का उपयोग करें या वीपीएन का उपयोग करें।**
- ☐ **उन उपकरणों को अप-टू-डेट विकल्पों से बदलें जो अब निर्माताओं द्वारा समर्थित नहीं हैं।**
- ☐ **खोए हुए या चोरी हुए उपकरणों के लिए रिपोर्टिंग प्रक्रियाएं सेट करें।**

पासवर्ड का उपयोग करते हुए

- ☐ **सुनिश्चित करें कि सभी कंप्यूटर एन्क्रिप्शन उत्पादों का उपयोग करते हैं जिन्हें बूट करने के लिए 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।**

- ☐ जहाँ भी संभव हो दो-कारक वाले प्रमाणीकरण (2एफए) का उपयोग करें।
- ☐ स्टाफ को दिये जाने से पहले, नेटवर्क और आईओटी डिवाइस सहित सभी उपकरणों पर निर्माता द्वारा जारी किए गए डिफ़ॉल्ट पासवर्ड 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 कर्मचारियों के पास विशिष्ट पहचान वाले खाते हैं जिनको हर बार प्रमाणित किया जाता है जब जो आपके सिस्टम का उपयोग करते हैं।
- ☐ 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 संगठन के कंप्यूटर पर प्रत्येक कर्मचारी के लिए उपयोगकर्ता खाते बनाएं।
- ☐ दूरस्थ रूप से काम करने वाले कर्मचारियों और एडमिनिस्ट्रेटर्स के लिए स्पष्ट एक्सेस विकल्पों को परिभाषित करें।

अपने वाई-फाई को सुरक्षित 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। पासवर्ड राउटर के एक्सेस की सुरक्षा करता है, और सुनिश्चित करें कि पासवर्ड पूर्व-निर्धारित डिफ़ॉल्ट से अपडेट किया गया है। 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।
- ☐ अपने नेटवर्क पर मौजूद सभी उपकरणों की आसान ट्रैकिंग के लिए अपने नेटवर्किंग उपकरणों पर डायनामिक होस्ट कॉन्फ़िगरेशन प्रोटोकॉल (डीएचसीपी) लॉगिंग सक्षम करें।
- ☐ राउटर सेट करने के बाद एडमिनिस्ट्रेटर के रूप में लॉग आउट करें।
- ☐ अपने राउटर के सॉफ़्टवेयर को अपडेट रखें। निर्माता के साथ अपना राउटर पंजीकृत करें और अपडेट प्राप्त करने के लिए साइन अप करें।

फ़िशिंग हमले से बचें

- ☐ 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।
- ☐ कर्मचारियों को फ़िशिंग के स्पष्ट संकेतों की जाँच करना सिखाएं, जैसे खराब वर्तनी और व्याकरण, या पहचानने योग्य लोगो के निम्न-गुणवत्ता वाले संस्करण। 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)।

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America