संगठन स्तरीय सुरक्षा नियंत्रण

1. ईमेल पहचान चुराने वाले फिशिंग हमलों को रोकने के लिए **मल्टी-फैक्टर सत्यापन(एमएफए)** लागू करें। यदि एम.एस. ऑफिस 365 का उपयोग किया जा रहा है तो एम.एफ.ए. सक्षम होना चाहिए। विंडोज लॉगिन के लिए भी एमएफए को सक्षम बनाया जाना चाहिए जो विशेष रूप से रिमोट डेस्क प्रोटोकॉल (आरडीपी) का उपयोग करके तीव्र हमलों के विरूद्ध प्रभावी होगा।

2. दुर्भावनापूर्ण गतिविधि को रोकने और मैलवेयर के सफल प्रसार को रोकने के लिए नेटवर्क पृथकता(बुनियादी ढांचे के महत्वपूर्ण हिस्सों को इंटरनेट और कम सुरक्षित आंतरिक नेटवर्क से दूर रखने के लिए नेटवर्क का विभाजन) को सक्षम करें। इससे उन प्रणालियों पर सीधे हमलों को रोका जा सकता है जो इंटरनेट फलक पर नहीं हैं। यह सुनिश्चित करने के लिए कि डेटा ट्रैक किया गया है, लॉग-इन की प्रभावी निगरानी और संवेदनशील डेटा की संपरीक्षा की जा सकती है।

3. एंटी-फिशिंग सॉफ्टवेयर संस्थापित करें जो मेल सर्वर पर चल सकता है और फिशिंग वेबसाइटों/मैलवेयर वाले किसी भी हाइपरलिंक के लिए ईमेल की जांच कर सकता है। यह फिशिंग के माध्यम से पहचान चोरी और दुर्भावनापूर्ण कोड क्रियान्वयन को रोक सकता है।

4. यह सुनिश्चित करें कि पैच प्रबंधन(नेटवर्क पर चल रहे सॉफ्टवेयर को पैच किया गया है और अद्यतन किया गया है) नियमित आधार पर किया जाता है, विशेष रूप से उन सर्वरों पर जहां अनपैच किए गए दूरस्थ डेस्कटॉप सॉफ्टवेयर मौजूद होने पर साइबर हमले हो सकते हैं। अन्यथा कंप्यूटर से अप्रयुक्त या अप्रकाशित सॉफ्टवेयर को हटा दें, विशेषकर दूरस्थ डेस्कटॉप सॉफ्टवेयर को। उन पोर्टस को बंद करें जिन्हें इंटरनेट से कनेक्ट करने की आवश्यकता नहीं है।

5. यह सुनिश्चित करने के लिए कि पूरे नेटवर्क में पासवर्ड की न्यूनतम स्ट्रैंथ का अनुपालन किया जाता है, संगठन में एक पासवर्ड नीति क्रियान्वित करें। इससे तीब हमलों को रोकने और हमलावरों को डिफॉल्ट पासवर्ड का लाभ उठाने से रोकने में मदद मिलेगी।

6. आईटी सिस्टम की समय-समय पर संपरीक्षा की जानी चाहिए।

7. पुराने कंप्यूटरों (विशेष रूप से इंटरनेट से जुड़े सर्वर) को हटा दिया जाना चाहिए ताकि साइबर हमले की संभावना को कम किया जा सके।

8. फिशिंग हमलों और ईमेल चोरी धोखाधड़ी के संबंध में कर्मचारियों को शिक्षित करें।

9. प्रयोक्ता मशीनों तक सीधे नेटवर्क पहुंच को प्रतिबंधित करने के लिए फायरवॉल एक्सेस कंट्रोल लिस्ट्स का उपयोग करें ताकि केवल स्वीकृत उपकरणों को ही उनसे कनेक्ट करने की अनुमति हो।

10. प्रभावित उपकरणों को त्वरित रूप से रूप से कामकाजी बनाने के लिए नियमित बैकअप रखें। सुनिश्चित करें कि बैकअप ऑफलाइन रखा गया है और सुनिश्चित करें कि एक पुनर्प्राप्ति योजना मौजूद है।

11. वेब अनुप्रयोग को सुरक्षित करने के लिए, सक्षम संपरीक्षकों और जांचकर्ताओं से संपूर्ण आईसीटी सिस्टम का नियमित रूप से भेद्यता मूल्यांकन और प्रवेश परीक्षण (वीएपीटी) किया जाए।