रैंसमवेयर: रोकथाम और सुरक्षा

वास्तविक समय की सुरक्षा

रैंसमवेयर एक उभरता हुआ खतरा है क्योंकि दुर्भावनापूर्ण ढंग से कार्य करने वालों ने मैलवेयर से कंप्यूटर सिस्टम को बंधक बना कर मोनेटाइज़ करने का तरीका ढूंढ लिया है और उनकी रिहाई के लिए फिरौती का भुगतान करने की मांग करते हैं। अन्य मैलवेयर के विपरीत, जिन्हें अक्सर प्रभावी ढंग से काम करने के लिए लंबे समय तक छिपा रहना पड़ता है, रैंसमवेयर को स्पीयर-फ़िशिंग, गड़बड़ वेबसाइटों और करप्ट डाउनलोड के माध्यम से जल्दी निष्पादित करने के लिए बनाया जाता है। वित्तीय संस्थान विशेष रूप से रैंसमवेयर के प्रभाव की चपेट में आने के खतरे में रहते हैं, क्योंकि इससे धन को जल्दी और कुशलता से स्थानांतरित करने की क्षमता को खतरा हो सकता है और क्योंकि उन्हें लाभदायक लक्ष्य माना जाता है। हालांकि, बदमाश लोग कभी-कभी अपने वादे तोड़ते हैं: फिरौती का भुगतान करने के बाद भी, कुछ हमलावर मैलवेयर नहीं हटाते हैं या गोपनीय डेटा को नहीं छोड़ते हैं।

- ऐसी एंटी-मैलवेयर सुरक्षा प्रणालियों में निवेश करें जो वास्तविक समय में नए खतरे की खुफिया जानकारी के अनुकूल हैं।
- 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।
  - अपने कार्यक्षेत्र में एलओटी या "स्मार्ट डिवाइसेस" को लाते समय विशेष रूप से सावधान रहें, क्योंकि इन प्रणालियों में अक्सर कमजोर या गैर-मौजूद सुरक्षा प्रणालियाँ होती हैं और इन्हें आवश्यक प्रणालियों तक पहुँच बिंदुओं के रूप में लक्षित किया जा सकता है।
  - 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 सुरक्षा की आवश्यकता पर कर्मचारी की शिक्षा को बढ़ावा दें।
- यदि संभव हो तो अपने संगठन में कई कारकों वाले प्रमाणीकरण को लागू करने पर विचार करें।
- सभी सिस्टम और सॉफ्टवेयर को नियमित रूप से अपडेट रखें। यदि संभव हो तो स्वचालित अपडेट की अनुमति के लिए सेटिंग्स बदलें।
- इस बात के लिए घटना की प्रतिक्रिया और संकट प्रबंधन योजना विकसित करें कि रैंसमवेयर हमले और मूल्यवान 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 सर्वर 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 विकसित करें 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 वातावरण

- अपने संचालन वातावरण में रैंसमवेयर के लिए उपयुक्त विनियामक और कानूनी मार्गदर्शन का मूल्यांकन करें।
  - देश-विशिष्ट मार्गदर्शन पर विचार करें। बदलते मार्गदर्शन के आवधिक मूल्यांकन के लिए एक योजना बनाएं।
  - वित्तीय-क्षेत्र के विशिष्ट मार्गदर्शन पर विचार करें।
  - अंतरराष्ट्रीय कानूनी और नियामक आवश्यकताओं पर विचार करें।
- फिरौती देने से जुड़े जोखिमों का आकलन करें। कुछ मामलों में, फिरौती का भुगतान करने से प्रतिरोधी सक्रियक के खिलाफ मौजूदा प्रतिबंधों का उल्लंघन हो सकता है।
- 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।

आपके संगठन की रैंसमवेयर की तैयारी को मापना

रैंसमवेयर की रोकथाम और सुरक्षा योजना बनाते समय निम्नलिखित प्रश्नों पर विचार करें।

1. क्या आपके संगठन के पास **नियमित रूप से निर्धारित बैकअप है**?
   - क्या ये बैकअप आपके नेटवर्क से हटे हुए हैं, या तो क्लाउड स्टोरेज सिस्टम या एयर-गैप्ड यूएसवी/हार्ड ड्राइव के माध्यम से?
2. क्या आपके संगठन के नेटवर्क से कोई भी **गैर अनिवार्य** उपकरण जुड़ा हुआ है?
   - क्या उन्हें अन्य नेटवर्क में स्थानांतरित किया जा सकता है जिनमें संवेदनशील डेटा नहीं रखा गया हैं?
3. क्या आपका संगठन फिरौती देने से जुड़े **विनियामक और कानूनी जोखिमों** को समझता है?
   - इस पर कानूनी मार्गदर्शन एक देश से दूसरे देश में भिन्न होता है और अक्सर अपडेट किया जाता है।
4. क्या आपका संगठन नियमित रूप से अपने सॉफ्टवेयर और सिस्टम को अपडेट करता है? क्या अपडेट्स**स्वचालित हैं**?
5. क्या आपके संगठन के पास एक योजना है **कि रैंसमवेयर के हमले और बहुमूल्य डेटा के नुकसान से कैसे निपटें?**
6. क्या आपके संगठन की **साइबर बीमा पॉलिसी** है? यदि है, तो यह योजना रैंसमवेयर हमलों को कैसे कवर करती है?
   - कुछ योजनाएं स्पष्ट रूप से फिरौती के भुगतान पर रोक लगाती हैं, जबकि अन्य इस तरह के भुगतान को नीति के हिस्से के रूप में शामिल करती हैं।

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
INTERNATIONAL MONETARY FUND
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA INDEPENDENT COMMUNITY BANKERS of AMERICA®