घटना प्रत्युत्तर गाइड

तैयारी

- अपने संगठन के वरिष्ठ नेतृत्व और अन्य प्रासंगिक कर्मी के साथ घटना प्रत्युत्तर और व्यापार निरंतरता के विकास हेतु कार्य करें जोकि सर्वाधिक दबाव मूलक जोखिम पर आधारित हो और जिसकी पहचान आपके संगठन के जोखिम आकलन में हुई हो।
  - 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 तैयार करें जो इस बात को रेखांकित करे कि कर्मी कितनी तेजी से किसी घटना पर निश्चित तौर पर जवाब दें और उन्हें क्या कार्रवाई करनी चाहिए जोकि प्रासंगिक फैक्टर जैसे कि घटना के फंक्शनल और सूचनात्मक प्रभाव और घटना से बाहर निकलने की संभावना पर निर्भर हो।
  - 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।
  - व्यापारिक आपातकाल के दौरान आपका संगठन प्राथमिक ग्राहकों और आपूर्तिकर्ताओं के साथ कैसे कार्य करेगा इस बात के समन्वयन के लिए व्यापार निरंतरता योजना को शामिल करें जिसमें यह भी शामिल हो कि अगर जरूरत हो तो आप मैनुअल या वैकल्पिक व्यापार प्रचालन का संचालन कैसे करेंगे।
  - आपातकालीन सिस्टम शट-डाउन और रीस्टार्ट के लिए लिखित प्रक्रियाओं को शामिल करें।
  - बैकअप डेटा की पुनर्प्राप्ति और पुनर्स्थापन के लिए, मान्यता के सत्यापन बैकअप डेटा की सामयिक जांच युक्तियों का विकास एंव जांच करना।
  - वैकल्पिक केंद्र/साइट पर व्यापार ऑपरेशन के प्रचालन हेतु स्थापित अनुबंध और प्रक्रियाओं का होना।
  - सभी ग्राहकों के लिए एक स्पष्ट प्रसार चैनल स्थापित करें।

अभ्यास करना

- सभी कर्मियों या कर्मियों के सभी स्तर के प्रतिनिधियों के साथ जिसमें संगठन के एग्जिक्यूटिव, पीआर/संचार कर्मी, और कानूनी और अनुपालन टीम शामिल हो, उन सबके साथ टेबलटॉप लघु अभ्यास का आयोजन करें।
- अपने संगठन के लिए प्रासंगिक उद्योग-दायरे के टेबलटॉप अभ्यासों की पहचान करें और आदर्श रूप से इसमें हिस्सेदारी करें।
- ऐसी प्रक्रियाओं की स्थापना कर यह सुनिश्चित करें कि अभ्यासों से मिली सीख को आत्मसात किया गया है और आपके संगठन की साइबर सुरक्षा रणनीति में इसकी चर्चा की गई है।

प्रत्युत्तर देना

- छवि संबंधी नुकसान के मद्देनजर प्रभाव को न्यूनतम करने के लिए घटना प्रत्युत्तर योजना की कार्रवाई का कार्यान्वयन करना।
- प्रभावित/समझौता हुए सिस्टम की पहचान करें और क्षति का आकलन करें।
- प्रभावित परिसंपत्ति को हटाकर (डिसकनेक्ट कर) क्षति को कम करें।
- जैसे ही टीम को संदेह हो कि कोई घटना घटी है यथाशीघ्र सभी सूचना की रिकॉर्डिंग आरम्भ कर दें। जब प्रभावित और चिह्नित परिसंपत्ति को डिसकनेक्ट/पृथक करते समय घटना के साक्ष्य को संरक्षित करने का प्रयास करें जैसे कि सिस्टम के कॉन्फ़िगरेशन, नेटवर्क का संग्रहण, और प्रभावित परिसंपत्ति से घुसपैठ डिटेक्शन लॉग का संग्रहण।
- यथोचित आंतरिक पक्षों, तीसरे पक्ष वेंडर और प्राधिकारों को अधिसूचित करें और अगर जरूरी हो तो सहायता का अनुरोध करें।
- ग्राहक अधिसूचना और सहायता गतिविधि शुरू करें जोकि कानून, नियमन और इंटर-एजेंसी गाइडेस के अनुरूप हों।
- खतरा साझाकरण प्लेटफार्म जैसे कि एफएस-आईएसएसी या एमआईएसपी का उपयोग उद्योग जगत को खतरे से अधिसूचित करने के लिए करें।
- बाद में समीक्षा हेतु घटना के दौरान उठाए गए सभी कदमों का दस्तावेजीकरण करें।

पुनर्बहाली

- अगर उपलब्ध हो तो आवर्ती "रिकवरी पॉइंट" में रिकवर किए गए परिसंपत्ति को पुन: भंडारित करें और सिस्टम के अंतिम "गुड" स्टेटस पर रीस्टोर करने के लिए बैकअप डेटा का उपयोग करें।
- रीस्टोर किए गए असेट से अपडेट किए हुए "स्वच्छ" बैकअप बनाएं और सुनिश्चित करें कि महत्वपूर्ण परिसंपत्ति के सभी बैकअप भौतिक रूप से और परिवेश के हिसाब से सुरक्षित लोकेशन में भंडारित किया गया है।
- इस बात की जांच और सत्यापन करें कि संक्रमित सिस्टम पूरी तरह रीस्टोर कर लिया गया है। पुष्टि करें कि प्रभावित सिस्टम सामान्य रूप से काम कर रहे हैं।

समीक्षा करना

- घटना घटने के बाद "सीखे गए सबक" चर्चा का संचालन करें- वरिष्ठ कर्मी, भरोसेमंद सलाहकार और कंप्यूटर सपोर्ट वेंडर(वेंडरों) के साथ बैठक करें और संभावित भेद्यता की समीक्षा कर लागू करने योग्य नए कदम की अनुशंसा प्राप्त करें।
- अगर संभव हो तो भेद्यता (चाहे वह सॉफ्टवेयर में हो या व्यापार प्रचालन या कर्मी के आचरण में हो) की पहचान करें जिसके कारण घटना घटी और इसके समाधान के लिए योजना का विकास करें।
- समान घटना या पहचाने गए मसले से संबंधित घटना से संबंधित आगे की किसी घटना की पहचान के लिए एक योजना का विकास करें।
- घटना के मद्देनजर सीखे गए सबक और सूचना को खतरा साझाकरण प्लेटफॉर्म जैसे कि एफएस-आईएसएसी पर साझा करें।
- अपने संगठन के घटना प्रत्युत्तर प्रोटोकॉल में सबक को जोड़ें।