دليل الاستجابة للحوادث

الإعداد

- تعاون مع القيادة العليا في مؤسستك والأفراد الآخرين ذوي الصلة لوضع خطة استجابة للحوادث واستمرارية الأعمال استنادًا إلى أكثر المخاطر إلحاحًا التي تم تحديدها في تقييم المخاطر السيبرانية لمؤسستك.
  - ضع سيناريوهات للتهديدات لأنواع الحوادث المرتبطة بالمخاطر السيبرانية ذات الأولوية القصوى لمؤسستك. ركز على بناء القدرة على الاستجابة لتلك السيناريوهات.
  - حدد داخل مؤسستك قائمة من نقاط الاتصال للاستجابة للحادث وسجلها واجعلها متاحة.
  - حدد وسجل معلومات الاتصال الخاصة بوكالات ومسؤولي إنفاذ القانون المحليين والاتحاديين ذوي الصلة.
  - ضع أحكامًا تحدد أنواع الحوادث التي يجب الإبلاغ عنها، ومتى يجب الإبلاغ عنها، ولمن.
  - ضع مبادئ توجيهية مكتوبة تحدد مدى سرعة استجابة الموظفين لحادث ما والإجراءات التي يجب تنفيذها، استنادًا إلى العوامل ذات الصلة مثل التأثير الوظيفي وآثار الحادث، وإمكانية الاسترداد المحتملة من الحادث.
  - أبلغ جميع الموظفين بالاتصال بالفريق الفني - سيتمثل على الأرجح في موظفي تكنولوجيا المعلومات و/أو مدير أمن المعلومات/المدير التنفيذي/مدير آخر مماثل - عند وقوع حادث.
  - انشر حلولاً لمراقبة إجراءات الموظفين ولتمكين تحديد التهديدات والحوادث الداخلية.
  - قم بتضمين خطط استمرارية الأعمال لتنسيق الطريقة التي ستعمل بها مؤسستك مع الموردين والعملاء الأساسيين في حالة الطوارئ التجارية، بما في ذلك كيفية إجراء عمليات يدوية أو بديلة إذا لزم الأمر.
  - قم بتضمين إجراءات مكتوبة لإيقاف تشغيل نظام الطوارئ وإعادة تشغيله.
  - طور طرق استرجاع البيانات الاحتياطية واستعادتها واختبرها، واختبر بيانات النسخ الاحتياطي بشكل دوري للتحقق من صلاحيتها.
  - ضع اتفاقيات وإجراءات لإجراء العمليات التجارية في منشأة/موقع بديل.
  - صمم قناة توزيع واضحة لجميع العملاء.

ممارسة التمارين الرياضية

- نظم تدريبات صغيرة على وضعية سطح الطاولة مع جميع الموظفين أو الممثلين من جميع مستويات الموظفين بما في ذلك المديرون التنفيذيون للمؤسسة، وموظفو العلاقات العامة/الاتصالات، وفرق الشؤون القانونية والامتثال.
- حدد تمارين وضعية سطح الطاولة على مستوى المجال وشارك فيها بصورة مثالية، وذلك في إطار ما يتعلق بمؤسستك.
- ضع عملية لضمان دمج الدروس المستفادة من التدريبات ومعالجتها في إستراتيجية الأمن السيبراني الخاصة بشركتك

الاستجابة

- نفذ إجراءات خطة الاستجابة للحوادث للحد من الأثر بما في ذلك ما يتعلق بإلحاق الضرر بالسمعة.
- حدد الأنظمة المتأثرة/المتضررة وقيم الضرر.
- حاول الحد من الضرر عن طريق إزالة (فصل) الأصول المتأثرة.
- ابدأ بتسجيل جميع المعلومات بمجرد اشتباه الفريق في وقوع حادث. حاول الحفاظ على دليل على الحادث أثناء فصل/عزل الأصول المحددة المتأثرة على سبيل المثال، جمع سجلات تكوين النظام والشبكة وسجلات كشف التسلل من الأصول المتضررة.
- قم بإخطار الأطراف الداخلية المناسبة والبائعين من جهات خارجية والسلطات، واطلب المساعدة إذا لزم الأمر.
- ابدأ أنشطة الإخطار والمساعدة الخاصة بالعملاء بما يتفق مع القوانين واللوائح التنظيمية والتوجيهات بين الوكالات.
- استخدم منصات مشاركة التهديدات مثل FS-ISAC أو MISP لإخطار المجال عن التهديد.
- وثّق جميع الخطوات التي تم اتخاذها أثناء الحادث لمراجعتها لاحقًا.

الاستعادة

- استعد الأصول المستردة إلى "نقاط الاسترداد" الدورية إذا كانت متاحة واستخدم بيانات النسخ الاحتياطي لاستعادة الأنظمة إلى حالة "جيدة" معروفة.
- قم بإنشاء نسخ احتياطية "نظيفة" محدثة من الأصول التي تمت استعادتها واضمن تخزين جميع النسخ الاحتياطية للأصول الحيوية في موقع آمن ماديًا وبيئيًا.
- تأكد من استعادة الأنظمة المصابة بالكامل واختبرها.تأكد من أن الأنظمة المتأثرة تعمل بشكل طبيعي.

المراجعة

- قم بإجراء مناقشة حول "الدروس المستفادة" بعد وقوع الحادث - اعقد اجتماعات مع كبار الموظفين، والمستشارين المعتمدين وبائع (بائعي) دعم الكمبيوتر لمراجعة نقاط الضعف المحتملة أو التوصية بخطوات جديدة ليتم تنفيذها.
- إذا أمكن، فحدد نقاط الضعف (سواء في البرامج أو الأجهزة أو العمليات التجارية أو سلوك الأفراد) التي أدت إلى الحادث وضع خطة للتخفيف منها.
- ضع خطة للمراقبة للكشف عن أي حوادث مماثلة أو أحداث أخرى تتعلق بالقضايا المحددة.
- شارك الدروس المستفادة والمعلومات حول الحادث في منصات مشاركة التهديدات مثل FS-ISAC.
- ادمج الدروس المستفادة في بروتوكولات الاستجابة لحوادث المؤسسة.

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®