برامج الفدية الضارة: الحماية والوقاية

قياس مدى استعداد المؤسسة لبرامج الفدية الضارة

تذكر الأسئلة التالية عند وضع خطة للوقاية والحماية من برامج الفدية الضارة.

1. هل تنشئ مؤسستك **نُسخًا احتياطية منتظمة مجدولة؟**
   - **هل تم فصل عمليات النسخ الاحتياطي هذه عن شبكتك، إما عبر أنظمة التخزين السحابي أو عبر وحدات USB/محركات الأقراص الثابتة غير المتصلة؟**
2. هل توجد أي **أجهزة غير أساسية** متصلة بشبكة مؤسستك؟
   - **هل يمكن نقلها إلى شبكات أخرى لا تحتوي على بيانات حساسة؟**
3. هل تدرك مؤسستك **المخاطر التنظيمية والقانونية** المتعلقة بدفع الفدية؟
   - **تختلف التوجيهات القانونية حول هذا الأمر من بلد إلى آخر ويتم تحديثها باستمرار.**
4. هل تقوم مؤسستك بتحديث برامجها وأنظمتها بانتظام؟ هل هذه التحديثات **تلقائية؟**
5. هل تمتلك مؤسستك **خطة لكيفية التعامل مع هجوم برامج الفدية الضارة** وفقدان البيانات المهمة؟
6. هل تمتلك مؤسستك **سياسة تأمين سيبراني؟** إذا كان الأمر كذلك، فكيف تغطي هذه الخطة هجمات برامج الفدية الضارة؟
   - **تحظر بعض الخطط بشكل صريح دفع الفدية، بينما تغطي خطط أخرى دفع الفدية باعتبارها جزءًا من السياسة.**

الحماية في الوقت الفعلي

تُمثل برامج الفدية الضارة تهديدًا متزايدًا منذ أن وجد أصحاب النوايا الخبيثة سبيلاً لجني المال من وراء البرامج الضارة عن طريق شلّ أنظمة الكمبيوتر والمطالبة بدفع فدية مقابل إطلاقها. على عكس البرامج الضارة الأخرى، التي غالبًا ما تظل مخفية لفترات طويلة لتعمل بشكل فعال، صُممت برامج الفدية الضارة لتنفيذ مهمتها بسرعة من خلال التصيد الاحتيالي ومواقع الويب المخترقة والتنزيلات التالفة. المؤسسات المالية معرضة بشكل خاص لتأثير برامج الفدية الضارة لأنها قد تهدد سرعة نقل الأموال وكفاءتها ولأنها تُعد أهدافًا مُربحة. ومع ذلك، قد يُخلف أصحاب النوايا الخبيثة وعودهم أحيانًا: حتى بعد دفع الفدية، بعض المهاجمين لا يقومون بإزالة البرامج الضارة وأحيانًا ينشرون بيانات سرية.

- استثمر في أنظمة الحماية من البرامج الضارة التي تتكيف مع التهديدات الإلكترونية الحديثة في الوقت الفعلي.
- قيّم أمان جميع الأجهزة المتصلة بالشبكات التي تحتوي على معلومات حساسة أو أساسية. قم بتوصيل جميع الأنظمة غير الأساسية بشبكة منفصلة.
  - كن حذرًا للغاية عند إدخال إنترنت الأشياء أو "الأجهزة الذكية" في مساحات العمل، إذ تحتوي هذه الأنظمة غالبًا على أنظمة أمان أضعف أو غير موجودة ويمكن استهدافها كنقاط وصول إلى الأنظمة الأساسية.
  - ضع في اعتبارك أمان إعدادات العمل عن بُعد. تأكد من عمل أدوات الأمان خارج الشبكة لمراقبة حركة الويب بأكملها.
- شجّع توعية الموظفين بهجمات التصيد الاحتيالي وضرورة إنشاء حماية قوية لكلمات المرور.
- انظر في تنفيذ مصادقة متعددة العوامل عبر مؤسستك إذا كان ذلك ممكنًا.
- حافظ على تحديث جميع البرامج والأنظمة بانتظام. غيّر الإعدادات للسماح بالتحديثات التلقائية إن أمكن.
- ضع خطة استجابة للحوادث وإدارة الأزمات تتناول كيفية التعامل مع هجوم برامج الفدية الضارة وفقدان البيانات المهمة.
- قم بإعداد خطة اتصال خارجية في حالة حدوث هجوم من أحد برامج الفدية الضارة.

النسخ الاحتياطي للبيانات

- استثمر في أنظمة النسخ الاحتياطي الآمنة التي يتم تحديثها بشكل منتظم والتي تحافظ على حماية بياناتك.
  - في حالة استخدام وحدات تخزين USB أو محركات أقراص ثابتة، افصل هذه الأجهزة فعليًا عن أجهزة الكمبيوتر المتصلة بالشبكة بعد استكمال إنشاء النُسخ الاحتياطية.
  - إذا كنت تستخدم التخزين السحابي، فزوّد الخادم بتشفير عالي المستوى ومصادقة متعددة العوامل.
- أنشئ نسخة للقراءة فقط من دفتر الأستاذ العام للتعافي من الكوارث في أسوأ الحالات.
- طوّر الأنظمة التي تقوم باسترداد البيانات ومعالجتها تلقائيًا.
- ضع سيناريوهات لتقييم المدة التي سيستغرقها استرداد البيانات المهمة وخدمات الأعمال.

البيئة التنظيمية

- قم بتقييم التوجيهات التنظيمية والقانونية المتعلقة ببرامج الفدية الضارة في البيئة التي تعمل فيها.
  - ضع في اعتبارك التوجيهات الخاصة بكل بلد. ضع خطة للتقييم الدوري للتوجيهات المتغيرة.
  - فكر في التوجيهات الخاصة بالقطاع المالي.
  - ضع في اعتبارك المتطلبات القانونية والتنظيمية الدولية.
- قم بتقييم المخاطر المرتبطة بدفع فدية. في بعض الحالات، قد يؤدي دفع فدية إلى انتهاك أنظمة العقوبات القائمة ضد الجهات المعادية.
- اتصل بجهة تنفيذ القانون المحلية. أنشئ اتصالات لتبادل المعلومات بسرعة في حالة حدوث هجوم.
- قم بتقييم مزايا وعيوب سياسات التأمين السيبراني الخاصة ببرامج الفدية الضارة.

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