

الأمن السيبراني للمؤسسات الأصغر حجمًا قائمة التدقيق الخاصة ببرامج الفدية الضارة

الاستعداد لمواجهة برامج الفدية الضارة

- عند وضع خطة للوقاية من برامج الفدية الضارة والحماية منها، قم بتقييم ما يلي بشكل دوري:
 - هل تنشئ مؤسستك نسخًا احتياطية منتظمة مجدولة؟
 - هل توجد أي أجهزة غير أساسية متصلة بشبكة مؤسستك؟
 - هل تدرك مؤسستك المخاطر التنظيمية والقانونية المتعلقة بدفع الفدية؟
- هل تقوم مؤسستك بتحديث أنظمة برامجها بانتظام؟ هل هذه التحديثات تلقائية؟
- هل تمتلك مؤسستك خطة للتعامل مع هجوم برامج الفدية الضارة وفقدان البيانات؟
- هل يمتلك نظامك سياسة تأمين سيبراني؟ إذا كان الأمر كذلك، فكيف تغطي هذه الخطة هجمات برامج الفدية الضارة؟

الحماية في الوقت الفعلي

- 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.
 - 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 للكلمات المرور.
- انظر في تنفيذ مصادقة متعددة العوامل عبر مؤسستك إذا كان ذلك ممكنًا.
- حافظ على تحديث جميع البرامج والأنظمة بانتظام.
 - غير 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 النسخ الاحتياطية.
 - إذا كنت تستخدم التخزين السحابي، فزود الخوادم 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

- اتصل بجهة تنفيذ القانون المحلية.
- إنشاء اتصالات لتبادل المعلومات بسرعة في حالة حدوث هجوم.
- قم بتقييم مزايا وعيوب سياسات التأمين السيبراني الخاصة ببرامج الفدية الضارة.
- قم بتقييم التوجيهات التنظيمية والقانونية المتعلقة ببرامج الفدية الضارة في البيئة التي تعمل فيها.
- ضع في اعتبارك التوجيهات الخاصة بكل بلد.
- ضع في اعتبارك التوجيهات الخاصة بالقطاع المالي.
- ضع في اعتبارك المتطلبات القانونية والتنظيمية الدولية.
- ضع خطة للتقييم الدوري للتوجيهات المتغيرة.
- قم بتقييم المخاطر المرتبطة بدفع فدية.