الخليج

اقتصاد, تقنية وسيارات

30 نوفمبر 2022 14:26 مساء

نقاط هامة للتصدي لهجمات الفدية الخبيثة 10

مع تصاعد موجة هجمات الفدية الخبيثة، استعرضت شركة بالو ألتو نتوركس مجموعة من النقاط التي ينبغي للمؤسسات والأفراد التركيز عليها للتصدي لهذا النوع من الهجمات، وهي:

1. معرفة أحدث التطورات المرتبطة بمشهد التهديدات الإلكترونية المتطور والمتغير باستمرار لا شك أن هجمات برامج الفدية ستواصل نموها وتطورها مع اعتماد الجهات الخبيثة لتقنيات جديدة لاستهداف الأعمال التجارية. ويتعين على فريق الأمن والمسؤولين التنفيذيين البقاء على اطلاع ومعرفة بالتطورات الحالية المرتبطة بهجمات الفدية وتأثيرها المحتمل على الأعمال والخطوات التي على المؤسسات اتخاذها للتعامل مع هذه الهجمات ومنعها، وقد أشارت دراسة حديثة لشركة بالو ألتو نتوركس إلى أن نقص مستوى الوعي بأهمية الأمن الإلكتروني لدى الموظفين هو العامل الأول في حدوث الهجمات الإلكترونية في المؤسسات، إذ تأتي 55% من الهجمات نتيجة هذا النقص في الوعي.

2. معرفة النتائج والآثار لفقدان البيانات الهامة على الأعمال لفهم التأثيرات المختلفة لهجمات الفدية، يجب أولاً

الحصول على رؤية كاملة للأصول التجارية المختلفة، وفهم مكان وجود البيانات الحساسة وكيفية الوصول إليها واستخدامها عبر المؤسسة. ولتحقيق ذلك، يتعين استكمال عملية تخطيط البيانات، والتأكد من أن الوصول إلى المعلومات السرية يتم على أساس المعرفة الوافية، ومن ثم يجب إجراء دراسة تحليلية حول مخاطر عدم القدرة على الوصول إلى هذه البيانات.

3. تقييم مستوى الجاهزية على المستويين الداخلي والخارجي ترتفع مخاطر وقوع هجمات الفدية الكبيرة في حال عدم وجود تقييم منتظم لدفاعات الأمن الإلكتروني في الشركة. لذا، يجب إجراء تقييم للمخاطر التي تواجه الشركة وفقاً للمشهد الأمني المعتمد والقائم على الأشخاص والعمليات والتكنولوجيا وقدرات الحوكمة. كما يجب تحديد أي مخاطر يمكن أن تنجم عبر أطراف ثالثة خارجية. ويمكن إنشاء خطة رئيسية للتخفيف من حدة الهجمات توضح بالتفصيل متطلبات الوصول إلى مستهدفات الأمن المتوافقة مع أهداف العمل الإستراتيجية.

4. مراجعة واختبار خطة الاستجابة للحوادث من الهام جداً اختبار وتحديث خطة الاستجابة للحوادث بشكل منتظم، واستخدام أحدث المعلومات والبيانات المتعلقة بهجمات الفدية لإجراء التدريبات ومحاكاة الهجمات. يهدف هذا الاختبار لقياس مدى جاهزية الشركة للاستجابة والتعامل مع هجمات الفدية، كما يساهم في تحديد الثغرات وتقييم مستوى الدفاعات والقدرة على مواجهة التكتيكات والتقنيات والإجراءات التي تستخدمها المجموعات المعروفة في شن هجمات الفدية. وأشارت دراسة حديثة لشركة بالو ألتو نتوركس إلى أن 70% من المؤسسات في الإمارات لديها خطة لإدارة الطوارئ الأمنية، إلا أن 51% من المؤسسات فقط واثقة من فعالية هذه الخطط.

5. اعتماد نهج الأمن الإلكتروني القائم على انعدام الثقة في حال اعتماده بالشكل الأمثل، يساهم نهج الأمن الإلكتروني في تبسيط إدارة المخاطر وتوحيدها من خلال اعتماد حالة (Zero Trust) الاستراتيجي القائم على انعدام الثقة أمان واحدة للمستخدمين أو الأجهزة أو مصادر الاتصال أو طرق الوصول إلى المعلومات. يعمل نهج الأمن القائم على انعدام الثقة على التعامل مع مخاطر هجمات الفدية من خلال إزالة عامل الثقة ومتابعة عملية التحقق والمصادقة في كل مرحلة من مراحل التفاعل الرقمي.

6. تحديد الأصول المعرضة للخطر وصد هجمات الفدية الشائعة يتعين على الشركات اعتماد نظام لتتبع مختلف الأصول والأنظمة والخدمات التي تمتلكها الشركة على شبكة الإنترنت العامة، بما يشمل تتبع الأصول عبر جميع مزودي الخدمات السحابية ومزوي خدمة الإنترنت، وذلك باستخدام فهرسة شاملة تمتد عبر المنافذ والبروتوكولات الشائعة، والتي غالبًا ما يتم تهيئتها بشكل غير صحيح. فعلى سبيل المثال، يتسبب بروتوكول سطح المكتب البعيد (RDP) بغالبية إصابات هجمات الفدية، إذ يمكن للمهاجمين اكتشاف بروتوكول سطح المكتب البعيد بسهولة نظراً للتوجهات المتزايدة والشائعة للعمل من المنزل.

7. منع التهديدات المعروفة وغير المعروفة يجب البقاء على اطلاع بتطورات هجمات الفدية والتسلح بالمعرفة التقنية اللازمة لتقديم حماية جديدة بمعدل أسرع من استجابة المهاجمين. وبهدف منع التهديدات الإلكترونية المعروفة، تحتاج لإيقاف ومنع عمليات الاستغلال والبرامج الضارة وحركة مرور الأوامر والتحكم من الوصول إلى الشبكة، حيث إن حظر هذه العمليات يؤدي إلى زيادة تكلفة تنفيذ هجمات الفدية بشكل يمكن أن يردع المهاجمين.

8. اعتماد الاتمتة قدر الإمكان عند وقوع هجمات الفدية، يتم إنفاق ساعات عديدة من العمل اليدوي في محاولة

تجميع مصادر المعلومات المختلفة من أدوات متعددة. لذا من المهم اعتماد الأدوات المناسبة التي تدعم الإصلاح التلقائي لهجمات الفدية باستخدام موارد التشغيل المعدة مسبقًا للاستجابة لمثل هذه الهجمات على أتمتة العملية بأكملها بشكل (SOAR) واسترجاع البيانات. تعمل منتجات تنسيق الأمان والأتمتة والاستجابة يمكن فرق الاستجابة من إيقاف هجمات الفدية بسرعة وتقليل فقدان البيانات والحد من التأثير المالي المرتبط .بهذه الهجمات

9. تأمين الأعمال السحابية لتأمين الأعمال الموجودة على السحابة وتحصينها ضد هجمات الفدية، يجب التأكد من إعداد وتهيئة مختلف موارد البنية التحتية السحابية وخدمات كيوبرنتس وصور حاويات البيانات بشكل آمن، واتخاذ الخطوات اللازمة للتخلص من الثغرات الأمنية، والتأكد من عدم توقف أي من مميزات الأمان بشكل افتراضي. تحقق من الباقات والمكتبات مفتوحة المصدر بحثًا عن نقاط الضعف التي يمكن تصحيحها. كما .يجب تحديد وإزالة مميزات إدارة الهوية والوصول غير المستحقة أو غير المستخدمة

10. تقليل وقت الاستجابة من خلال اعتماد اتفاقية للحصول على الدعم الخارجي من المهم جداً اتخاذ الإجراءات السريعة بمجرد تحديد وقوع خرق إلكتروني محتمل. كما إن وجود اتفاقية خاصة بالحصول على الدعم التقني الخارجي للاستجابة للحوادث يعتبر من المسائل الهامة للحفاظ على مستوى عال من الأمن، حيث يمثل خبراء الاستجابة للحوادث جزء من فريق العمل لدى الشركة ويتمتع بالقدرات والتقنيات اللازمة لتقديم المساعدة عند .الحاجة