المركز الوطني للأمن السيبراني
National Cyber Security Center

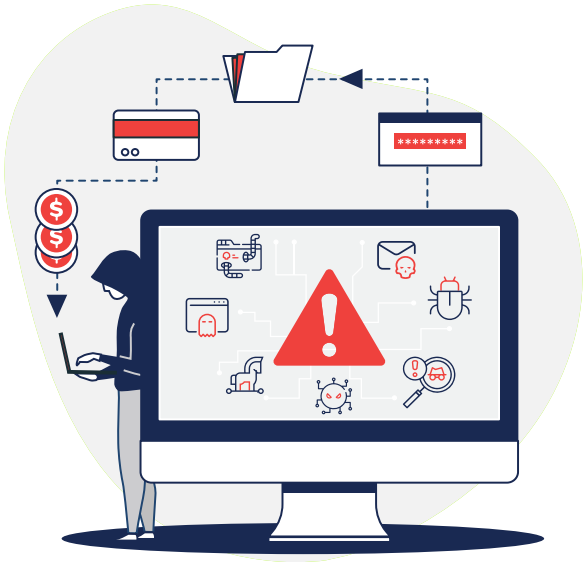
الأمن السيبراني 101
للمنظمات الأهلية

الفهرس

لماذا تحتاج المنظمات الأهلية إلى الأمن السيبراني

بدأت العديد من المؤسسات في جميع أنحاء العالم العمل مع المنظمات الأهلية لردع الهجمات السيبرانية والتصدي للتعطيل الناجم عنها، حيث نتج عن ذلك استجابةً للنداء العالمي للتصدي لتلك المخاطر السيبرانية على ذات المنظمات (NGOs).

لاحظ الباحثون في مجال الأمن السيبراني أن معظم الجهات الفاعلة من الدول أو غير الدول كالمجموعات الفاعلة، تواصل تركيز العمليات والهجمات السيبرانية على المنظمات الأهلية لأهداف مختلفة منها الاحتيال والذي عادةً ما يجمع بين التصيد وسرقة الهوية لخداع المنظمات غير الربحية لإتمام عمليات التحويلات المالية.

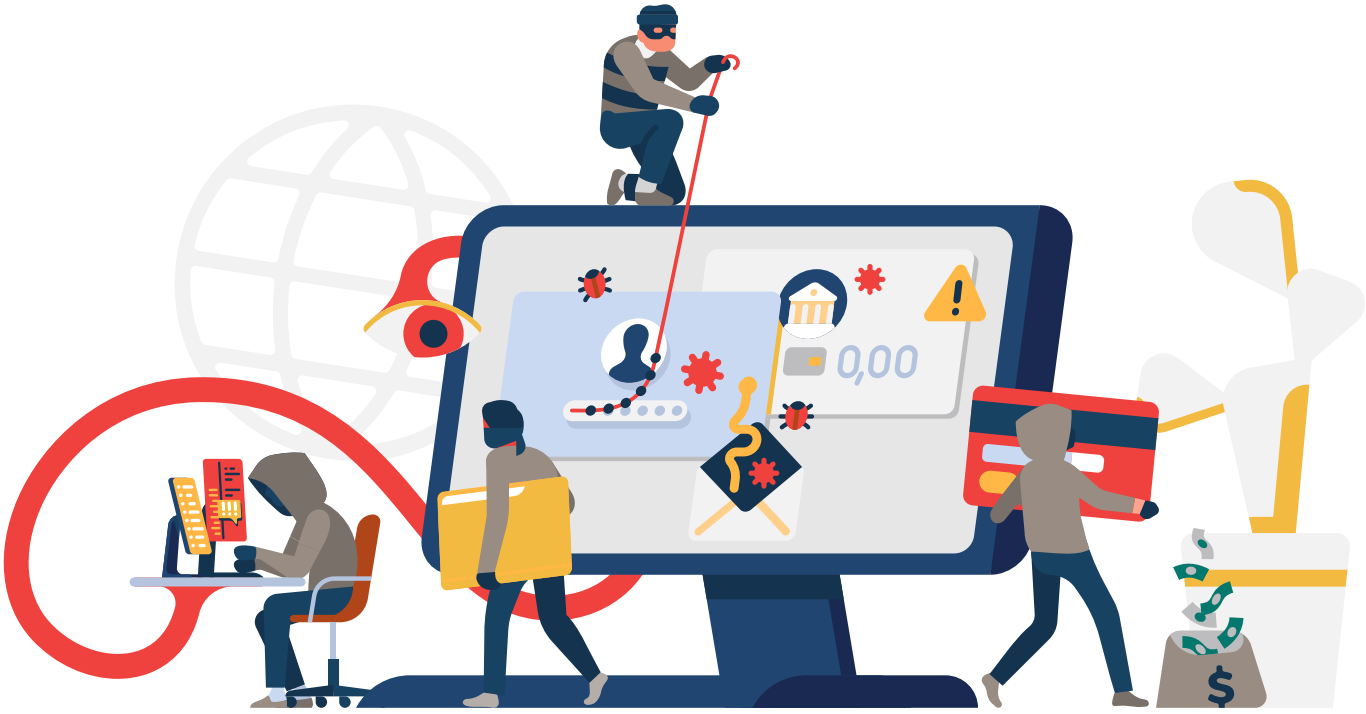


وكجزء من استراتيجية القرصنة المُتبعة والمعروفة باسم «احتيال الرئيس التنفيذي CEO Fraud» يقوم المحتالون بإنشاء عناوين بريد إلكترونية مزيفة وينتحلون هويات المدراء التنفيذيين أو الموظفين الموثوق بهم بقصد الخداع والاستغلال وذلك لتخويل تحويلات غير قانونية للأموال.

وكنوع آخر من الهجمات المتبعة هي هجمة فيروس الفدية أو Ransomware والذي يُنفذ بهدف تحقيق مكاسب مالية، حيث يقوم المهاجم بتشفير البيانات الهامة في أنظمة الكمبيوتر وينتج عن ذلك في بعض الأحيان تلف لتلك البيانات، الأمر الذي يدفع بالمؤسسات الخضوع لدفع الفدية لاسترجاع بياناتها.

وبشكل موجز، يتم تنفيذ الهجمات السيبرانية على المنظمات الأهلية للأسباب التالية:

1. منعهم من ممارسة أنشطتهم.
2. سرقة الأموال والبيانات والمعلومات الهامة.
3. الوصول إلى البيانات الخاصة بالمستفيدين وأصحاب المصلحة.
4. استخدام البيانات المسروقة في حملات التضليل.
5. استخدام البنية التحتية للمؤسسة لمهاجمة وتنفيذ الأنشطة الضارة و غير القانونية عبر الإنترنت.



إن من أسباب حدوث الهجمات السيبرانية هي استغلال المهاجمين لنقاط الضعف في الأنظمة أو بسبب خطأ بشري.

على الرغم من أن الهجمات تزداد تعقيدًا، إلا إنه ليس باستطاعة كل منظمة من المنظمات الأهلية تحمل تكاليف توظيف موظفين متخصصين في الأمن السيبراني لذا يجب على المنظمات الاستثمار في التوعية بالأمن السيبراني واتباع أفضل الممارسات بالإضافة إلى التدريب اللازم لجعل مؤسساتها أكثر مرونة في مواجهة الهجمات السيبرانية.

المخاطر

هجمات الفدية

اعتراض البيانات

هجوم تشويه موقع الويب

إساءة استخدام الهويات المسروقة

هجمات التصيد والاحتيال (ما يسمى بتصيد الحيتان الذي يستهدف البارزين من الرؤساء التنفيذيين)

قم بتعزيز جاهزية منظمتك الأمنية
ضد الهجمات السيبرانية

قم بنشر الوعي بالأمن السيبراني في مؤسستك

الأمن السيبراني مسؤولية مشتركة. قم بالاستثمار في برامج التوعية للموظفين وبالأخص لموظفي قسم تكنولوجيا المعلومات من خلال عقد دورات تدريبية وتوفير مواد توعوية من أجل تعزيز سلامة البيانات والأجهزة، وذلك بهدف جعل الأمن السيبراني جزءًا من ثقافة مؤسستك.

حماية البيانات الهامة

قم بتأمين بيانات الموظفين والمستفيدين ضد الأخطار المحتملة لسرقة البيانات، واتخذ تدابير إضافية لحماية البيانات المتعلقة بالأموال والمشاريع الخاصة بالمنظمة عن طريق تطبيق إحدى الطرق الأساسية مثل التشفير وإخفاء البيانات.

تأكد من وجود نسخ احتياطية للبيانات والأنظمة الهامة وبشكل دوري

النسخ الاحتياطي للبيانات الهامة هو عملية أساسية فقم بالتأكد من وجود السياسات الصحيحة والتدابير التقنية المناسبة لذلك، مثل وجود نسخ متعددة من البيانات الهامة المشفرة، وبهذه الطريقة يكون من الأسهل استعادتها في حالة حدوث هجوم سيبراني.
استفسر عن إجراءات النسخ الاحتياطي التي تستخدمها قواعد البيانات والخدمات التابعة لجهات خارجية يتم استخدامها في المؤسسة وتحقق من وثائق التعاقد والاشتراطات مع تلك الأطراف والمزودين لمعرفة إمكانية تحميل نسخة من بيانات المؤسسة بشكل دوري.

احرص على إنشاء كلمات المرور القوية واستخدم المصادقة متعددة العوامل

قم بإنشاء كلمات مرور على ولكل نظام تستخدمه ملتزماً بمعايير الأمان وأفضل الممارسات، واستخدم المصادقة متعددة العوامل (MFA) كطبقة ثانية من الأمان، حيثما أمكن ذلك. إذا كنت تواجه صعوبة في تذكر كلمات مرور متعددة، فاستخدم برنامج موثوق لإدارة كلمات المرور وتخزينها بشكل آمن.

قم بتثبيت برنامج مكافحة الفيروسات واحرص على تحديثه باستمرار

يجب تثبيت برنامج مكافحة الفيروسات من مصدر موثوق وتحديثه باستمرار على كل جهاز في المؤسسة، حيث إن تحديث برنامج مكافحة الفيروسات يساعد في منع البرامج الضارة من إصابة جهازك أو شبكتك في حال قيام أحد المستخدمين بالضغط على رابط ضار أو مشبوه.

كن حذرًا عند اختيار مزودي الخدمات

إذا قمت بالاستعانة بشركات خارجية للقيام بالأعمال المتعلقة بتكنولوجيا المعلومات الخاصة بك، فتأكد من أن مزود الخدمة يُطبق التدابير الأمنية لحماية البيانات والأنظمة الحساسة الخاصة بك. تَضمن الموظفين التابعين للشركات الخارجية أو مزود الخدمة في جلسات التوعية عند تعاملهم مع الأنظمة الخاصة بمؤسستك.

فكر في الحصول على بوليصة التأمين ضد المخاطر السيبرانية

فكر في الحصول على التأمين السيبراني حيث إنه وبحسب التغطية التي يقوم بها التأمين قد لا تكون التكاليف عالية ومن الممكن أن يغطي هذا التأمين تكاليف الإضرار بالسمعة والتعافي والعواقب المحتملة الأخرى من الهجوم السيبراني.

استخدم مواقع الويب المشفرة والآمنة

سهّلت التكنولوجيا على المؤسسات الخيرية والمنظمات غير الربحية قبول التبرعات عبر الإنترنت، ولكنها أيضًا أتاحت للمخترقين قابلية السرقة أثناء القيام بالمعاملات المالية والمصرفية الإلكترونية.
يساعد استخدام مواقع الويب الموثوقة والمشفرة والآمنة أثناء المعاملات المالية الالكترونية في الحفاظ على المعلومات آمنة لكلٍ من المستخدمين والمؤسسة، فلا تتجاهل الإشعارات التي تظهر من برنامج المتصفح على جهازك حول مواقع الويب غير الآمنة أو المحتوى الضار والمشبوه.

احذر مخاطر هجمات التصيد الاحتيالي وبرامج الفدية

من خصائص استخدام البريد الإلكتروني كطريقة للتواصل مع المتبرعين والعملاء هو السرعة والسهولة، حيث إنه من خلال رسائل البريد الإلكتروني والنشرات الإخبارية الآلية يتم إعلام الأطراف المهتمة بما يحدث في مؤسستك، ومع ذلك قد تكون عرضة للخطر إذا تم الضغط على رابط ضار، أو عند تحميل ملفات مشبوهة.
قم بالتحقق دائمًا من عنوان البريد الإلكتروني للمرسل، وإن كان مصدرهُ موثوقاً قم بالتحقق من الروابط أو الملفات المشبوهة في البريد الإلكتروني قبل الضغط عليها أو تحميلها.

تأكد أن اتصالات البريد الإلكتروني آمنة وموثوقة

هناك بعض المخاطر التي ينطوي عليها إرسال رسائل البريد الإلكتروني التي تحتوي على مستندات خاصة أو بيانات مالية، وذلك بسبب كون معظم رسائل البريد الإلكتروني المرسلة غير محمية بشكل جيد أثناء التنقل بين الخوادم. إن استخدام خادم بريد إلكتروني آمن وشبكة مشفرة يُمكن من جمع معلومات المتبرع وتنظيمها ونقلها بشكل آمن.

قم بتثبيت حلول الأمان

تأكد من أن مؤسستك لديها حلول أمنية مثل جدران الحماية وبوابات البريد الإلكتروني وأنظمة الكشف عن التسلل والوقاية منها لحماية الموظفين والبيانات والأنظمة الحساسة.

أمِّن المنصات والمعاملات المالية

تستخدم المنظمات الأهلية العديد من المنصات المدمجة أو المطورة داخلياً لجمع التبرعات وجمع الأموال عبر الإنترنت.
إن منصات التبرع الجيدة تستخدم تقنيات التشفير مثل SSL أو TLS، مما يؤمن عمليات إتمام التبرعات والمعاملات الرقمية وتشفير المعلومات التي تم إدخالها. إن تفعيل واستخدام المصادقة الثنائية MFA والرموز الآمنة OTPضرورية للحفاظ على سلامة المتبرعين، فقم بالبحث عن نظام ومنصة توفر خاصية المصادقة متعددة العوامل لتأمين بيانات المتبرعين والمستخدمين.

مراقبة أنشطة المتطوعين

يمنح المتطوعون وقتهم لعدة أسباب وفي الغالب لرغبتهم في دعم المُجتمع وقد يمكنهم ذلك الوصول إلى بيانات من التصنيف الخاص في مؤسستك، وهذا يشكل خطراً إذا ما تقرب أحدهم باسم التطوع للوصول إلى البيانات الحساسة في المؤسسة.
تأكد من مراقبة أنشطة المتطوعين لأنه قد ينجح المتطوعون ذوو النوايا السيئة والمشبوهة في التسلل عبر الثغرات، مما يعرض مؤسستك لخطر حدوث هجوم إلكتروني.

إدارة المخاطر البشرية

إن الإدارة الفعالة للمخاطر البشرية تساعد على تقليل التكاليف وتوفير الوقت في الدفاع ضد الهجمات السيبرانية.

يمكن تحقيق ذلك من خلال تحديد المخاطر وتغيير السلوكيات في المؤسسة بدلاً من الاعتماد فقط على التقنيات والحلول الأمنية حيثُ إن التدريب والتوعية يُمكنان الموظفين من استشعار الخطر والعمل على حده بشكل استباقي مما يحسن مستوى الاستجابة و قدرات المرونة في التعافي لدى المؤسسة في حال وقوع هجمة سيبرانية.

ابق على اطلاع بأحدث إصدار من النظم والبرامج

قم بمواكبة التطورات والعمل على تثبيت التحديثات وتصحيحات الأمان لتقليل فرص العرضة للاختراق والاستغلال، حيث إن فعالية تلك التحديثات والرقع الأمنية (الإصلاح العاجل) جديرة بحمايتك من تهديد الهجوم الفوري (zero-day Attack)!

ارجع إلى الضوابط الأساسية للأمن السيبراني على موقعنا الإلكتروني للحصول على معلومات عن الضوابط الأساسية التي يجب على المؤسسات تنفيذها من أجل تلبية متطلبات إدارة المخاطر وحماية الأنظمة.

SCAN ME

نصائح سريعة:

- حماية البيانات الهامة بتفعيل النسخ الاحتياطي التلقائي وبشكل متعدد مشفر ومنتظم.
- تثبيت برامج مكافحة الفيروسات وتحديثها باستمرار.
- زيادة الوعي المؤسسي بالأمن السيبراني.
- عند القيام بأنشطة مالية عبر الإنترنت مثل التحويلات المصرفية، تأكد من استخدام مواقع ويب مشفرة وآمنة.
- احذر من برامج الفدية والخداع الاحتيالي.
- قم بإنشاء كلمات مرور فريدة وقوية واستخدام المصادقة متعددة العوامل الثنائية.
- قم بالنظر في خيارات التأمين السيبراني.
- كن حذرًا عند اختيار موفري خدمات تكنولوجيا المعلومات.
- تأمين اتصالات البريد الإلكتروني الخاصة بك عن طريق تشفير رسائل البريد الإلكتروني الحساسة.
- مراقبة أنشطة المتطوعين المشبوهة.
- تأكد من أن مؤسستك لديها حلول أمنية مثل جدران الحماية وبوابات البريد الإلكتروني وأنظمة منع وكشف التسلل IDS / IPS قبل وعند حدوث الهجمات الإلكترونية.
- قم بإدارة المخاطر البشرية من خلال الاستثمار في التوعية والتثقيف حول مخاطر الأمن السيبراني.

مع تحيات

المركز الوطني للأمن السيبراني

وزارة الداخلية

MINISTRY OF INTERIOR

www.ncsc.gov.bh

#الأمن_السيبراني