لضعف منظومتها الأمنية..

الشركات الصغيرة الأكثر تعرضا للحوادث السيبرانية

٨٨٪ منها تعرضت للاختراق مرة على الأقل خلال العامين الماضيين

في عالم اليوم المترابط، أصبحت الشركات الصغيرة أهدافا للهجمات الإلكترونية بشكل متزايد. ومع محدودية الموارد والخبرة، غالباً ما تعاني هذه الشركات لتتمكن من الدفاع عن نفسها ضد التهديدات المعقدة.

ومع ذلك، يمكن للشركات الصغيرة تعزيز وضعها الأمني بشكل كبير وحماية بياناتها الحساسة عبر تبين تدابير قوية لحماية كلمات المرور. وبمناسبة اليوم العالمي لكلمات المرور، كشفت كاسبرسكي عن تدابير أمن سيبراني بسيطة ولكنها مهمة لحماية كلمات المرور في بيئة الشركات الصغيرة.

وجدت دراسة أجرتها كاسبرسكي نهاية عام ٢٠٢٣ أن ٧٦% من الشركات الصغيرة حول العالم، و٨٨% منها في منطقة الشرق الأوسط وتركيا وإفريقيا، قد تعرضت لحادث سيبراني واحد على الأقل في العامين الماضيين.

وكانت عواقب تلك الهجمات وخيمة، إذ أسفرت عن تسرب بيانات سرية (٣٤% على مستوى العالم، و٢٩% في منطقة الشرق الأوسط وتركيا وإفريقيا)، وإلحاق الضرر بالسمعة (٢٣% على مستوى العالم، ٢٠% في منطقة الشرق الأوسط وتركيا وإفريقيا)، وفقدان ثقة العملاء (٢٠% على مستوى العالم، و٩% في منطقة الشرق الأوسط وتركيا وإفريقيا)، وسواها.

كما اضطرت حوالي ٩% من الشركات الصغيرة العالمية أو في منطقة الشرق الأوسط وتركيا وإفريقيا إلى إيقاف أجزاء معينة من عملياتها التجارية. وبفحص أسباب هذه الحوادث السيبرانية، اتضح أن استخدام كلمات مرور ضعيفة أو الفشل في إجراء تحديثات منتظمة لكلمات المرور هو سبب أساسي للحوادث. حيث كان هذا السبب مسؤولاً عن قرابة ربع الحوادث (٢٤% عالمياً و٢٠% في الشرق الأوسط وتركيا وإفريقيا)، وهو السبب الثاني بعد تحميل برمجية خبيثة. ولمعالجة هذه المشكلة العالمية، تقدم كاسبرسكي النصائح التالية للمساعدة في تعزيز سياسات كلمات المرور للشركات الصغيرة.

أنشئ كلمات مرور قوية

على الرغم من أهميته، غالباً ما يتم إهمال هذا الإجراء الواضح من قبل الموظفين الذين كثيراً ما يتعين عليهم التوفيق بين العديد من كلمات المرور لمجموعة متنوعة من التطبيقات التي يستخدمونها. لذا وبالإضافة إلى إنشاء كلمة مرور قوية، تأكد من أن كل كلمة مرور مختلفة لكل واحدة من خدمات الشركة. إذ تعد كلمات المرور الضعيفة والمعاد استخدامها أهدافاً سهلة لمجرمي الإنترنت، الذين يستخدمون الأدوات الآلية لاختراقها والوصول غير المصرح به إلى المعلومات الحساسة. ومن خلال تشجيع الموظفين على استخدام مجموعات معقدة من الحروف، والأرقام، والمعارف الخاصة، يمكن للشركات الصغيرة التخفيف من مخاطر الانتهاكات المتعلقة بكلمات المرور.

فعّل المصادقة متعددة العوامل

تضيف المصادقة متعددة العوامل (MFA) طبقة إضافية من الأمان من خلال مطالبة المستخدمين بتوفير تحقق إضافي يتجاوز الاكتفاء بكلمة مرور فحسب. ويمكن أن يشمل ذلك البيانات البيومترية، أو كلمات المرور أحادية الاستخدام المرسلة إلى جهاز محمول، أو أسئلة الأمان. وبينما قد ترى الشركات الصغيرة أن المصادقة متعددة العوامل (MFA) معقدة أو غير ضرورية، إلا أنها إجراء أمني بالغ الأهمية يمكنه الحماية من التهديدات السيبرانية المختلفة، مثل سرقة كلمة المرور والوصول غير المصرح به إلى الحساب. كما يؤدي تمكين المصادقة متعددة العوامل (MFA) إلى تخفيض شديد لمخاطر الوصول غير المصرح به إلى حسابات الشركات الصغيرة، وذلك حتى في حال اختراق كلمات المرور.

حدّث كلمات المرور بانتظام

تعد التحديثات المنتظمة لكلمات المرور ضرورية للحفاظ على «النظافة الأمنية» وتقليل مخاطر الاختراقات المرتبطة بكلمات المرور. يجب على مالكي الشركات الصغيرة تشجيع الموظفين على تغيير كلمات المرور الخاصة بهم بشكل دوري، بالإضافة إلى فرض سياسات انتهاء صلاحية كلمة المرور لمنع إعادة استخدام كلمات المرور القديمة. علاوة على ذلك، يجب تحديث كلمات المرور بسرعة استجابةً لتغييرات الموظفين أو عند الاشتباه في حدوث انتهاكات أمنية.

ثقّف الموظفين

يعد وعي الموظفين أمراً بالغ الأهمية ضمن الشركات الصغيرة للحماية الفعالة لكلمات المرور والسلامة الشاملة على الإنترنت. لذا يجب تثقيف الموظفين حول أهمية كلمات المرور القوية، ومخاطر مشاركة كلمات المرور، والعواقب المحتملة للوقوع ضحية للهجمات السيبرانية. ومن خلال تعزيز ثقافة الوعي بالأمن السيبراني، يمكن للشركات الصغيرة تمكين الموظفين من لعب دور نشط في حماية المعلومات الحساسة وتقليل أثر التهديدات السيبرانية.

أمن الأجهزة والشبكات

بالإضافة إلى تأمين كلمات المرور، يجب على الشركات الصغيرة اتخاذ خطوات لحماية أجهزتها وشبكاتها باستخدام حلول الأمن السيبراني مثل Kaspersky Small Office Security. ومع تزايد انتشار العمل عن بعد والخدمات السحابية، يجب على الشركات الصغيرة التأكد من أن أجهزتها وشبكاتها محمية بشكل كاف ضد البرمجة الخبيثة، وهجمات التصيد الاحتياليّ، والتهديدات السيبرانية الأخرى. ومن خلال تثبيت برامج الأمن السيبراني الموثوقة، وتفعيل جدران الحماية، والحفاظ على تحديث أنظمة التشغيل والبرمجيات، يمكن للشركات الصغيرة تعزيز دفاعاتها بشكل كبير.

علّق كيريل ليتفين، المدير الأول لتسويق المنتجات في كاسبرسكي قائلا: «تواجه حتى أصغر الشركات مخاطر كبيرة فيما يخص الأمن السيبراني. لذلك، من المهم لهم الاهتمام بالتدابير الأمنية واستخدام منتجات الأمن السيبراني المتخصصة لحماية عملياتهم وبيانات عملائهم. فعلى سبيل المثال، تم تصميم حل Kaspersky Small Office Security لتلبية احتياجات الشركات الصغيرة خصيصاً، ويعد حلاً أمنياً لا يحتاج إلى التدخل ويوفر حماية تتيح «التثبيت والنسيان»، كما أنه يوفر نفقات الشركات، وهو أمر بالغ الأهمية، وبالأخص في المراحل الأولى من تطوير الأعمال. كما يوفر هذا الحل حماية شاملة ضد البرمجيات الخبيثة، والتصيد الاحتيالي، وبرمجيات الفدية، وكلمات المرور الضعيفة، وغيرها.»

○ كيريل ليتفين.

خبراء: أنشئ كلمات مرور قوية.. وثقّف الموظفين

أول كلب آلي يحمل قاذفاً للهب

في خطوة غريبة بعض الشيء، كشفت شركة Throwflame عن أول كلب آلي يحمل قاذفًا للهب في العالم.

ويعد Thermonator روبوتًا رباعي الأرجل يحمل على ظهره قاذف لهب من شركة Throwflame، ويبدو أن المستخدمين سيتحكمون في الروبوت بواسطة وحدة تحكم متصلة بهواتفهم الذكية مثل Backbone

. ويستخدم الروبوت كاميرات مدمجة لتقدم للمستخدم منظور الشخص الأول، في حين تسمح له مستشعرات LiDAR برسم خريطة للمنطقة المحيطة به وبذلك يتجنب العقبات التي يمكن أن يصطدم بها.

توقف المنبهات من تلقاء نفسها.. مشكلة في آيفون

خلال الأسابيع الماضية، انتشرت العديد من التقارير والشكاوى من مستخدمي هواتف آيفون عبر منصات التواصل الاجتماعي ومنتدى الدعم الفني لأبل بشأن مشكلة في نظام التشغيل تتسبب في توقف المنبهات من تلقاء نفسها من دون إصدار صوت للتنبيه.

وتسببت تلك المشكلة في إثارة استياء أولئك المستخدمين، إذ يؤدي ذلك العطل إلى التأخر عند الاستيقاظ من النوم وتفويت مواعيد العمل وغيرها من المواعيد الهامة، خاصة مع اعتماد الكثيرين على أصوات المنبه، وفق البوابة العربية للأخبار التقنية.

من جهتها، أكدت شركة أبل لصحيفة «وول ستريت جورنال» أنها على علم بالمشكلة التي تسبب عدم تشغيل هواتف آيفون أصوات المنبهات، وأنها تعمل جاهدة على إصلاح تلك المشكلة.

حوكمة الذكاء الاصطناعي في الإعلام

بقلم:
د. جاسم حاجي ○

تشهد صناعة الإعلام والصحافة تحولاً مع دمج تكنولوجيا الذكاء الاصطناعي، وهو ما قطع خطوات كبيرة في إحداث ثورة في كيفية جمع المعلومات ومعالجتها ونشرها. من إنشاء المحتوى إلى توصيل الأخبار الشخصية، توفر تقنيات الذكاء الاصطناعي العديد من المزايا من خلال إعادة تشكيل كيفية إنتاج المعلومات واستهلاكها في هذا العصر الرقمي. قامت المؤسسات الإخبارية الكبرى بتبني تقنيات الذكاء الاصطناعي لأتمتة المهام، وتعزيز الكفاءة، وتوفير تجارب أكثر جاذبية لجماهيرها.

في السنوات الأخيرة، كانت هناك طفرة في الابتكارات المدعومة بالذكاء الاصطناعي في صناعة الإعلام والصحافة لكتابة الأخبار وإنشاء المحتوى. على سبيل المثال، تستخدم هيئة الإذاعة الوطنية الفنلندية (Yle) تقنية الذكاء الاصطناعي (Viotto) لتعزيز تخصيص الأخبار وتقديم توصيات ذكية للقراء أثناء إنشاء مقالات وتصورات متعددة حول موضوعات الأخبار الأكثر صلة. وبالمثل، تساعد أداة الذكاء الاصطناعي التي تقدمها بلومبرج للصحفيين، والتي تسمى (Cyborg)، في تحليل البيانات وتوليد القصص. تستخدم صحيفة واشنطن بوست أيضًا برنامج الذكاء الاصطناعي (Heliograf) وهو نظام توليد اللغة الطبيعية (NLG)، لإنتاج مقالات إخبارية موجزة عبر مختلف القطاعات، وبالتالي تحرير الصحفيين لإعداد تقارير أعمق.

في حين يقدم الذكاء الاصطناعي العديد من المزايا، فإن استخدامه في قطاع الإعلام والصحافة يثير مخاوف أخلاقية. إحدى القضايا المهمة هي احتمال قيام أنظمة الذكاء الاصطناعي بإدامة التحيزات الموجودة في البيانات المستخدمة للتدريب، مما قد يؤدي إلى نشر محتوى متحيز أو تمييزي، مما يضعف مبادئ الموضوعية والعدالة التي تعتبر حيوية في الصحافة. بالإضافة إلى ذلك، هناك مخاوف بشأن التأثير على النزاهة الصحفية والتآكل المحتمل للرقابة البشرية في إنتاج الأخبار. قد يؤدي الاعتماد على المحتوى الناتج عن الذكاء الاصطناعي أيضًا إلى أن تصبح مصادر الأخبار متشابهة للغاية، ما يقلل من تنوع وجهات النظر المتاحة.

علاوة على ذلك، لا يمكن إغفال تأثير الذكاء الاصطناعي على الخصوصية والشفافية داخل قطاع الإعلام والصحافة. ومع قيام خوارزميات الذكاء الاصطناعي بمعالجة كميات هائلة من بيانات المستخدم لتخصيص المحتوى واستهداف الإعلانات، تنشأ أسئلة بخصوص خصوصية البيانات والموافقة وإمكانية المراقبة. علاوة على ذلك، فإن الطبيعة الغامضة للعديد من خوارزميات الذكاء الاصطناعي غير الخاضعة للتنظيم والافتقار إلى القابلية للتفسير في عمليات صنع القرار تشكل تحديات أمام الشفافية والمساءلة. يجب على المؤسسات الإعلامية أن تسعى جاهدة لتحقيق التوازن بين الاستفادة من قدرات الذكاء الاصطناعي والحفاظ على المعايير الأخلاقية، وضمان ثقة الجمهور في سلامة مصادر الأخبار.

يحمل مستقبل الذكاء الاصطناعي في قطاع الإعلام والصحافة إمكانات هائلة، ولكنه يحمل أيضًا مسؤوليات كبيرة. يجب على القطاع تطوير أطر الحوكمة بشكل استباقي لمواجهة هذه التحديات من خلال التعاون مع أصحاب المصلحة وصانعي السياسات والخبراء لوضع مبادئ توجيهية لتطوير ونشر الذكاء الاصطناعي الأخلاقي. ويجب أن تتناول هذه المبادئ التوجيهية قضايا مثل خصوصية البيانات، والشفافية الخوارزمية، والرقابة البشرية، ومنع التحيزات. بالإضافة إلى ذلك، سيكون التدريب والتعليم المستمر للصحفيين والإعلاميين أمرًا حاسمًا في تشجيع فهم أفضل لقدرات الذكاء الاصطناعي وقيوده، مما يتيح التكامل المسؤول والفعال لهذه التقنيات. ومن خلال تبني الحوكمة الأخلاقية والتدابير الاستباقية، يمكن لقطاع الإعلام والصحافة تسخير قوة الذكاء الاصطناعي مع الحفاظ على القيم الأساسية للصحافة، والحفاظ على ثقة الجمهور وضمان الدور الحيوي لوسائل الإعلام في المجتمع.

نافذة تكنولوجية