اقتصاديات التغيير: أهمية تنمية "ثقافة التكنولوجيا الآمنة" في زمن التغيير

محمد النمر، مكان العمل الحديث والأمن، مايكروسوفت الشرق الأوسط وإفريقيا للأسواق الناشئة

رغم أن الأخبار العاجلة حول الانتهاكات الأمنية غير المسبوقة تصدرت عناوين وسائل الإعلام، إلا أن ظهور جائحة كوفيد-19 جلب معه فرصًا جديدة لمجرمي الإنترنت، الذين يعملون بلا كلل خلف الكواليس لضرب المؤسسات الآمنة.

تشير التقديرات إلى أن أكثر من مليار إفريقي سيتمكنون من الوصول إلى الإنترنت بحلول سنة 2022. وتشير الإحصاءات الحالية أن الجريمة السيبرانية تكلف إفريقيا أكثر من 4 مليارات دولار أمريكي سنويًا بسبب الضعف الكبير للتدابير الأمنية، حيث يبدو أن تراجع القارة في هذا المجال سيزداد مستقبلا.

ومع تبني الشركات حاليا لطريقة العمل الـ"هجينة"، أي أن بعض الموظفين يختارون العودة إلى المكتب والبعض الآخر يختار العمل عن بعد من المنزل، أضحت بعض التحديات الجديدة تطرح نفسها، لا سيما عندما لا تكون المؤسسات قد طورت لديها ثقافة البقاء آمنة في قلب نموذجها الاقتصادي. بشكل أساسي، يُعهد إلى الموظفين الذين يعملون عن بُعد باستخدام قدراتهم الخاصة إذا وقعوا ضحية لمحاولة "اختراق إلكتروني عن بُعد".

وبالتالي، إذا أرادت الصناعات أن تعيش الوضع الطبيعي الجديد بشكل عادي، لا بد من حدوث أمرين في إطار استراتيجيات الأمن الداخلي للمضي قدمًا. أولاً، التوعية من الأعلى إلى الأسفل حول مدى أهمية الحفاظ على الأمن وكيف يؤثر ذلك سلبًا وإيجابيًا على المؤسسة، وثانيًا، الاستثمار في التكنولوجيا الصحيحة والآمنة لكل موظف. سيقطع كلاهما شوطًا طويلاً في المساهمة في "الكثافة التكنولوجية" للمؤسسة. أي، كيف تتبنى مؤسسة ما أحدث التقنيات ودمجها في الشركة، وكيف تبني قدرتها الرقمية الفريدة وترفع من مستوى الثقة لديها.

ومع ذلك، قد تكون المخاطر أكبر من ذي قبل، خاصة خلال فترة الوباء الحالية، لأن ذلك لن يحدد فقط المؤسسات القادرة على مواجهة الأزمة الحالية، ولكن أيضًا تحديد المؤسسات المستعدة للتعامل مع الأحداث غير المتوقعة في المستقبل.

الموظفون يمثلون أكبر المخاطر المتعلقة بالأمن السيبراني

خلص استطلاع أجرته Gallagher سنة 2020، أن حوالي 60٪ من اختراق البيانات يكون ناتجا بدون قصد وعبر خطأ بشري، أي أن العديد من الموظفين يقعون ضحية لرسائل البريد الإلكتروني الاحتيالية التي يحتمل أن تكون مدمرة. على هذا النحو ، فإن البقاء آمنًا ليس فقط من اهتمامات C-suite. فالعديد من المؤسسات لم تقم بعمل جيد في إيصال أهمية ذلك للموظفين، ومدى لعب الدور الأهم بنفس القدر لضمان بقاء البيئة من حولهم آمنة.

وبالتالي ، فإن التكوين المستمر في جميع المجالات أمر بالغ الأهمية، لا سيما في وقتنا الحالي. حيث يجب أن تشكل الموارد والدورات التدريبية جزءًا لا يتجزأ من استراتيجية أمنية مستدامة للمؤسسات. تتمثل إحدى طرق القيام بذلك في وجود برنامج وميزانية مخصصين للتكوين والتوعية (E&A). كما يُعد الاستثمار في الأشخاص والموارد لضمان التحسيس والتوعية الأمنية بشكل استباقي ومستمر، أحد أفضل الطرق للحماية من نقاط الضعف على مستوى المؤسسة. يمكن بدء ذلك من خلال تحديد خطة تضمن دمج الأمن والحماية في وقت مبكر من دورة الحياة التشغيلية للشركة والنظر في تخصيص ميزانية للمساعدة في غرس ثقافة الأمان والحماية عبر المؤسسة ككل.

هناك طريقة أخرى لضمان إحراز تقدم في هذا المجال، وهي تعزيز بيئة "بدون خجل". إذ لن يتوقف المهاجمون عبر الإنترنت عن استهداف الموظفين. بالإضافة إلى الوعي والتكوين، من المهم خلق بيئة حيث يمكن للموظفين مشاركة نقاط الضعف المحتملة التي يواجهونها حتى يمكن إرشادهم في الخطوات التالية - مثل الإبلاغ عن الحادث. فلا يرغب الناس في الوقوع في المشاكل أو فقدان وظائفهم بسبب وقوعهم ضحايا لهجوم ما. إذ يجب تعزيز الثقة بهم وارتباطهم الوثيق بالمؤسسة، وعدم تحسيسهم بأنهم مستهدفون، بل طمأنتهم بالوقوف إلى جانبهم ضد الأعداء الحقيقيين.

الاستثمار في التقنيات الصحيحة

في مايكروسوفت، نلتزم دائمًا ونشجع المقاربة المرتكزة على الأمن والسلامة. من خلال ابتكار تقنيات تحمي عملائنا الذين يعتمدون على البرامج والخدمات السحابية. يعد تركيزنا الأمني ضروريًا لتلبية متطلبات الدورة التجارية على مدار الساعة طوال أيام الأسبوع، ويساعد على ضمان أن العملاء نادرًا ما يواجهون فترات توقف عن العمل من خلال حدث أمني. على هذا النحو، فإننا نستثمر أكثر من مليار دولار أمريكي سنويًا في الجوانب الأمنية - يشتغل بها أكثر من 3500 متخصصًا في مجال الأمن، وقد أنشأنا العديد من الشراكات القوية في منظومتنا الاقتصادية. ونظرًا لتزايد تعقيدات أماكن العمل الحديثة، فإننا نهدف إلى مواصلة بناء وتعزيز قدراتنا الأمنية لمساعدة عملائنا على البقاء متيقضين في مواجهة التهديدات الحديثة.

تساعد الحلول المتخصصة في الحماية من التهديدات مثل Microsofts 365، في التخفيف من التهديدات المتقدمة، وتوفر حلاً شاملاً يؤمن مجمل مساحة الهجوم على المؤسسة. ستواجه المؤسسات التي تختار هذا الحل الحماية من التهديدات المتقدمة مثل التصيد الاحتيالي المستهدف وبرامج الفدية وخدمات الكشف عند حدوث خرق، وقدرات الاستجابة للتصحيح من هجوم وإعادة المؤسسة إلى حالة عدم وجود تهديد. هذا ويسمح

Azure Stack بإنجاز وتشغيل التطبيقات المختلطة عبر المواقع والمكاتب البعيدة والسحابة، باعتبار أن الحجم الواحد لا يناسب الجميع عندما يتعلق الأمر باحتياجات محددة للمؤسسات.

على مستوى المنطقة، لدينا الكثير من العمل الذي يتعين علينا القيام به لمواصلة نشر رسالة التمكين التكنولوجي، وأثناء قيامنا بذلك ، يجب ألا ننسى مشاركة التأثير السلبي المحتمل أيضًا إن لم نكن مدربين ومجهزين بشكل كامل. وذلك يعتمد على كيفية المضي قدمًا ورغبتنا في التعاون والتعلم.