٧ أخطاء شائعة يقع فيها المُستخدمين الجُدد للسحابة

في الوقت الذي يشهد فيه العالمُ تسارعًا وتطورًا ملموسًا في تكنولوجيا المعلومات، نجد أن الكثير من المؤسسات الحكومية والخاصة تتجه نحو تبنّي تكنولوجيا السحابة في تخزين البيانات الخاصة بها.

ومن الطبيعي أن تكون السحابة (Cloud technology) هي الوجهة الأقرب والخيار الأمثل لأي مؤسسة تضع المرونة والأمن الصارم والتخزين والتوسّع المُستقبلي من ضمن أولوياتها.

أوضحت **دراسة** مؤخراً أن أكثر من ٩٠ % من المؤسسات والشركات حول العالم تحوّلت إلى استخدام استراتيجية السحابة المُتعددة، بجانب ٨٧ % يتبنون خيار السحابة المزدوجة أو الهجين. علاوة على ذلك فمن المتوقع ان يتحوّل ٥٩ % من المستخدمين إلى تكنولوجيا السحابة بعد انجلاء جائحة كورونا، وذلك بسبب بنية السحابة الفريدة وفعاليتها من حيثُ التكلفة والمرونة، إذ تُمثّل السحابيات ميزة انتاجية واعدة للمؤسسات.

في ديسمبر ٢٠١٩ قامت وزارة المواصلات والاتصالات بدولة قطر بتوقيع عقد مع شركة مايكروسوفت لإنشاء مركز **للبيانات السحابية**، ونظراً لطبيعة الخدمات السحابية العابرة للحدود فإن **قانون حماية خصوصية** البيانات **وسياسة تأمين المعلومات الوطنية** يتطلّب تعامُلاً ومنظورًا مختلفًا لجميع المُعاملات والاتصالات.

وعلى الرغم من ذلك نلاحظ أن المُستخدمين الجُدد يقعون في عدة أخطاء قد تؤدي إلى خسارة كبيرة في المال والوقت، ومن أجل ذلك سنستعرض في هذه المُدونة أكثر سبعة أخطاء شائعة يقع فيها مُعظم المستخدمين الجُدد للسحابة.

أولًا الانتقال غير الضروري من مزوّد سحابي إلى آخر

أحد الأخطاء الشائعة التي تقع فيها الكثير من المؤسسات والشركات هو التبديل والتنقّل غير الضروري بين مزودي خدمات السحابة، ولكن من المهم علينا إدراك أن جميع مزودي الخدمات السحابية ليسوا متشابهين، فإن كان السبب الرئيسي من تبديل مزوّد السحابة، هو مساحة تخزين البيانات أو مُشكلة بالأمان فمن الأفضل التحدّث مع مزودك الحالي والتعرف على الخيارات التي يوفرها. وهذا الأمر لا يختصر لك الوقت فحسب بل يُقلل الكثير من الصعوبات في الجُهد والمال.

ثانيًا الانتقال الكامل

بسبب التطوّر الذي تشهده التكنولوجيا أصبح الانتقال إلى السحابة سلسًا وسهلًا. لكن ذلك لا ينفي احتمالية حدوث أخطاء جسيمة ومؤسفة في حال عدم وجود المعرفة الكافية في المؤسسة بتكنولوجيا السحابة.

عندما تريد الانتقال إلى السحابة، فيجب أن تقوم بذلك بعد استشارة الخبراء. ويُوصى بشدّة أن تنتقل انتقالاً جُزئياً وليس انتقالاً مرةً واحدة. ومن الأفضل أن تبدأ ببعض التطبيقات خلال

المرحلة الأولية، ومن ثم الانتقال إلى المراحل التي تليها، حيثُ يُمكن البداية بالتطبيقات الغير حساسة أو في طور التجربة .

الانتقال الجُزئي يُتيح لك حماية بياناتك الضخمة من الخطر في حال حدوث خطأ ما، حيث يُمكّنك هذا الانتقال من استكشاف الأخطاء ومعالجتها قبل الانتقال بالكامل .
إذا كنت تقوم بتشغيل شركة مالية أو شركة رعاية صحية فأنت في الحقيقة تقوم بتشغيل كمية ضخمة من البيانات عبر مجموعة تطبيقات حساسة، فإن الانتقال الكامل رُبما يُعرضك لتحديات قاسية في الأمن والامتثال، ولذلك الانتقال الجزئي هو الطريق الآمن للتوجه نحو السحابة .

ثالثاً عدم النظر إلى الأمن كمسؤولية مشتركة

يفترض الكثير من القادمين الجدد إلى السحابة أن مُزوّد خدمات السحابة مسؤول بالكامل عن التعامل مع جميع جوانب الأمان، ولا يدركون أنه بالرغم من انتقالهم للسحابة لا تزال المؤسسة هي المسؤولة في المقام الأول عن أمانها .

بإختصار، أمن السحابة هو دائمًا مسؤولية مُشتركة، ويجب على الجميع تكريس جهودهم للحفاظ عليه، ويتحقق ذلك فقط من خلال تطوير القُدرات(الموارد البشرية والعمليات والأدوات) التي تُساعد في إدارة المخاطر الأمنية، حيث نُلاحظ أن إطار عمل الأمن السيبراني في قطر ٢٠٢٢ يُسلّط الضوء أيضًا على الحاجة إلى فهَم المسؤولية المشتركة للأمان كشرط أساسي قبل الانتقال إلى السحابة .

إن سياسات الحوكمة السحابية وتحسينات الأمان تُضفي على مؤسستك الحماية اللازمة التي تُساعدك على العمل بكفاءة، وعلى هذا النحو فإن الأدوات التي تستخدمها للأمان هي الأكثر أهمية حيث تُساعدك في الحصول على تحليلات مُفصّلة تُقلل من الانتهاكات والمخاطر الأمنية المتوقّعة .

رابعًا عدم الإهتمام بالجانب الأمني لسلسلة التوريد بأكملها

يُمكن أن تُسبب مصادر الإمداد الخارجية العديد من التهديدات، فعلى سبيل المثال فإن عدداً كبيراً من المؤسسات في قطر يستفيد من العديد من المكتبات البرمجية إلا أن استخدام رموز أو شفرات Codes ذات مصادر غير معروفه ومن دون فهم وتدقيق كافيين يمكن أن يُفسح المجال للثغرات البرمجية غير الآمنة .
هذه المشكلة على المؤسسات التي تنتقل حديثاً إلى السحابة فحسب بل أن مُعظم الشركات الكبرى في جميع أنحاء قطر تكون عُرضة للوقوع فيها. ويرجع ذلك بالأساس إلى عدم إمكانية التحقُق من أمان الرموز والشفرات المُستخدمة، ولذلك نجد أنّ تبني مثل هذه الأساليب يبقي القضايا الأمنية دائماً في خطر, وبالتالي يُرجى منك –قبل الانتقال– التأكد من أن الأدوات التي يتم توريدها من مصدر خارجي سواء كانت برامج أو شفرات أو أجهزة قد تم اختبارها من الناحية الأمنية بشكل جيّد .

خامسًا تجاهل التغيُّر في النموذج الأمني

على عكس اعتبارات الأمن السيبراني التقليدي داخل الشركة، يُمكن اعتبار أمان السحابة بمثابة نقلة نوعية حيث سيتوجّب عليك تأمين البيانات والهوية، مما يجعل الهوية كبُعد جديد عليك العمل على تأمينه. حيثُ يُمكن أن يؤدي الفشل في فهم التغيير من النموذج التقليدي إلى ابطاء عمليات الانتقال إلى السحابة، مما يُؤثّر سلبًا على مُبادرات التحوّل الرقمي .

عليك أن تتذكّر دائماً، أنه وبغض النظر عن السياسات الأمنية لمُزودي الخدمة السحابية، فإن اللائحة الأساسية هي أن يتحكّم أصحاب الأعمال في بياناتهم الحساسة .

يُعد إطار العمل للأمن السيبراني في قطر لكأس العالم ٢٠٢٢ نقطة انطلاق جيّدة للمؤسسات للتأكد من امتلاكها للإمكانيات اللازمة والاستعداد قبل الانتقال إلى السحابة .

سادساً عدم التحكّم في الوصول إلى منصّات السحابة

التحكُم في الوصول إلى منصّات السحابة أحد أهم ركائز الأمان، بحيث يجب أن تكون

إمكانية الوصول إلى السحابة فقط للموظفين المُعتمدين وذلك بناءً على مستوى الحقوق المطلوبة لأداء مهامهم. ومن أجل المحافظة على الأمان، على المؤسسة أن تتبنّي نهج الوصول المميّز، والذي يساعد في تحديد أشكال الوصول المطلوبة للنظام، وتعريف الحسابات التي تتطلب إمتيازاً خاصاً لجميع التطبيقات والبيانات .

أخيراً يجب وضع وتطبيق إجراءات مُحددة للمساعدة في ضمان الوصول فقط للذين يُسمح لهم بالوصول إلى البيانات السحابية المطلوبة والتطبيقات المُرتبطة بها، مما يُمّكن إدارة الحساب بالكامل من لحظة إنشائه إلى حذفه عندما تزول الحاجة إليه .

سابعاً الإفراط في استخدام حسابات المُشرف/ المسؤول

عندما يتم اختراق حساب المُشرف/المسؤول فإنه يُعرّض الشبكة السحابية بأكملها للخطر، وهذا هو السبب الذي يُحتّم على المؤسسة وضع قيود صارمة للوصول إلى حساب المُشرف/المسؤول والاحتفاظ به بشكل صارم فقط لأداء المهام الضرورية القصوى .
لا تسمح أبداً للموظفين باستخدام الحساب الأول (حساب الجذر) للمهام اليومية لأنه يجعلك عُرضة للبرامج الضارة مما يؤدي لخلل في نظام الأمان .

الخُلاصة

الآن وبعد أن عرفت الأخطاء الشائعة التي يرتكبها الأشخاص أثناء الإنتقال إلى السحابة نتمنى أن تكون في وضع أفضل لمواصلة خطواتك نحو السحابة. ومن قبل ذلك تعرّف على احتياجاتك وأحصل على النتائج الصحيحة وأعد النظر في متطلباتك وناقش المخاطر والتهديدات والتحديات الكامنة التي قد تضطر إلى التعامل معها .

وتذكّر دائماً ان الحوسبة السحابية هي التكنولوجيا الأهم التي يجب عليك دائماً بذل الجهود لتخفيف الأخطاء وتقليل التكاليف على جميع المستويات فيها، وذلك من أجل تحقيق أقصى استفادة من هذه التكنولوجيا الواعدة .