الخليج

اقتصاد, إدارة وأعمال, فقرة حرة

16 أبريل 2023  00:29 صباحا

# الشركات بين مطرقة الهجمات الإلكترونية وسندان العمل عن بعد

زاد توجه الشركات والمؤسسات محلياً وعالمياً خلال السنوات الأخيرة في اعتماد نظام العمل الهجين أو العمل عن بعد، وساهمت جائحة كورونا في نمو هذا التوجه، الذي له العديد من الجوانب الإيجابية والسلبية.

من إيجابيات العمل عن بعد، تقليص التكاليف التشغيلية لدى المؤسسات والشركات المختلفة، ورفع مستويات الإنتاجية للعاملين، وتقليل نفقات التنقل لدى الموظفين، وتوفير الوقت والجهد لدى الكوادر البشرية، والاستعانة بمواهب وكفاءات تعمل من أي مكان بالعالم لأنهم يحتاجون فقط إلى جهاز إلكتروني يتصل بالإنترنت.

لكن سلبياته باتت خطراً كبيراً يواجه المؤسسات، بسبب سهولة اختراق أجهزة الموظفين في بيوتهم والاستيلاء على بيانات ومعلومات مهمة لعملاء الشركة، وهو ما أكدته العديد من التقارير أن الهجمات الإلكترونية زادت في الآونة الأخيرة، واستغل القراصنة ضعف النظام الأمني للإنترنت المنزلي، الذي سهل الحصول على بيانات قد تكون سرية للغاية، وكشفها قد يحدث زعزعة في أوسط الشركات والعملاء، الذين يقعون ضحية لابتزاز المالكين للمعلومات والبيانات.

الصورة

كما تختلف نوعية البيانات والمعلومات التي يتم تسريبها أو الحصول عليها عبر الإنترنت، من بيانات سرية للغاية ومن سري، ومن محظور ومن عام ومن عادي، وأخطرها النوع الأول، وما هي القطاعات التي تم اختراقها وتم الحصول على معلوماتها، هل البنوك أم العقارات أم الأسهم والاكتتابات، أم القطاع الصحي، وغيرها من القطاعات ذات الأهمية القصوى، وهل سربت من مؤسسة حكومية، أم أمنية، أم شركة في القطاع الخاص، التي يستهدفها القراصنة بكثرة حول العالم، من أجل بيعها أو نشرها مجاناً.

لذلك تبقى الشركات في دولة الإمارات بين مطرقة زيادة التوجه نحو تبني الأنظمة الإلكترونية الحديثة، مع الأخذ بعين الاعتبار بضرورة وجود نظام أمني يحميها من الاختراق، والاتجاه نحو استقطاب الكفاءات والمواهب من مختلف دول العالم للعمل عن بعد.

الصورة

**نموذج للاختراق •**

بداية شهر مارس/آذار 2023، تعرضت مؤسسة في دولة الإمارات لاختراق بياناتها، وتم سحب المئات من ملفات الأشخاص الذين يتعاملون مع هذه الجهة عن طريق فيروس تم من خلاله الدخول إلى البريد الإلكتروني للشركة والسيطرة المطلقة على جميع البيانات، لكن لحسن الحظ أن هذه المعلومات لم تكن سرية، حيث علم القراصنة بوجود ثغرة في النظام الأمني لهذه المؤسسة وتم الاختراق من نقاط ضعفها، وبعد 12 ساعة من العمل الإلكتروني تم سد الثغرة، وتم بيع العديد منها عبر الإنترنت، ولحساسية الشركة لن يتم ذكرها.

**قطاعات تتعرض للهجمات •**

يقول الدكتور محمد الكويتي، رئيس مجلس الأمن السيبراني لحكومة دولة الإمارات: «يعتبر القطاع المالي والبنوك الأكثر تعرضاً وباستمرار لهجمات إلكترونية متكررة، لكن بفضل معايير الأمن السيبراني التي يتبعونها تنتهي محاولة المخترقين بالفشل دون الولوج إلى ملفات وبيانات عملاء هذه الجهات».

وأضاف: «ستزداد الهجمات الإلكترونية عند التحول الرقمي غير الأمن، لكن عند امتثال الشركات والمؤسسات لمعايير الأمن السيبراني، بجانب وعي الأشخاص في خطورة البيانات التي يقومون بمشاركتها مع الآخرين عبر الإنترنت، سيجنب الشركات الدخول في معترك استنزاف بياناتهم من قبل القراصنة، الذين يتجولون خلف البريد الإلكتروني والثغرات الأمنية الضعيفة للشركات للانقضاض عليها».

وأوضح الكويتي، أن القطاع الحكومي في دولة الإمارات مؤمن ومحوكم بطريقة آمنة يجعل من الصعب اختراقه، عكس القطاع الخاص، الذي لا يزال أمامه مشوار طويل لتأمين بيانات العملاء، وبعض الشركات تعمل في القطاع المالي والصحي والتداول على الإنترنت، وتم التعامل مع الكثير من الحالات بطرق سرية وسد الثغرات التي تعرضوا لها.

وأكد أنه عند وصول تنبيه لـ«مجلس الأمن السيبراني» لحكومة دولة الإمارات بوجود اختراق يتم التعامل معه خلال ثوانٍ معدودة، والحيلولة دون حصول القراصنة على أي بيانات مهمة للشركة، داعياً إلى التواصل مع الجهات الشرطية أو عبر التطبيقات (الأمين-الأمان-999) والإبلاغ الفوري حال وقوع اختراق حتى يسهل التعامل معه وبسرية تامة.

سجلت دولة الإمارات انخفاضاً بنسبة 14% في إجمالي هجمات البرمجيات الخبيثة خلال عام 2022، مقابل زيادة بنسبة 2% على أساس سنوي في الهجمات الإلكترونية على مستوى العالم، وتخطى عدد الهجمات 71 مليون هجمة.

الصورة

**حساسية البيانات •**

يقول مروان أبو نواس المهيري، رئيس إدارة المواهب والكفاءة المؤسسية في مجموعة «مجموعة بنك الإمارات دبي الوطني»: «يعتبر البنك من أقوى المؤسسات المصرفية في الدولة، بفضل بنيته التحتية التكنولوجيا القوية التي يصعب اختراقها»، ولم يؤكد مروان تعرض البنك مسبقاً للهجمات الإلكترونية.

وأضاف: «لدينا نظام العمل عن بعد مع العديد من الموظفين، وهم مجهزون بنظام إلكتروني قوي لحماية بيانات ومعلومات العملاء من التسرب عبر الإنترنت». وأوضح أنه لا يوجد غياب للأمن الإلكتروني في أنظمة البنك لحساسية وسرية المعلومات التي يمتلكها، وهناك حماية كاملة ومطلقة لجميع التطبيقات.

وأشار رئيس إدارة المواهب والكفاءة المؤسسية في «مجموعة بنك الإمارات دبي الوطني»، أن التطور التكنولوجي المتسارع الذي يشهده العالم اليوم، جعل هناك شريحة كبيرة من الأفراد خاصة الموهوبين يحبون العمل عن بعد، ولا يريدون التقيد في العمل من المكاتب، وهذا سهل علينا الوصول لهؤلاء الأفراد من مختلف دول العالم للعمل معنا بشروط تكون أكثر صرامة عن العمل داخل البنك لأهمية البيانات التي يمتلكها البنك.

وأكد المهيري، أنه نظام العمل عن بعد في دولة الإمارات لن يؤثر في استقطاب المواهب للعمل في الدولة، لأن الفرص والخيارات التي تتاح للعاملين في هذا المجال كثيرة ومتعددة، والمزايا التي تقدم لهم لن يجدوها متاحة في أي بلدان أخرى.

وحسب تقرير (سونيك وول)، سجّل عام 2022 ثاني أعلى نسب لمحاولات برامج الفدية على الصعيد العالمي، وزيادة بنسبة 87% في البرامج الخبيثة التي تهدد إنترنت الأشياء وعدداً قياسياً من هجمات التعدين الخبيث (الكريبتوجاكينغ) التي بلغت 139.3 مليون.

**العمل الهجين •**

يرى الدكتور إبراهيم الخاجة، مدير إدارة الموارد البشرية بجمارك أبوظبي، أن نظام العمل عن بعدي يعتمد على أمرين، حجم ونوع العمل، حيث يصعب أن يتم تحويل العمل الميداني إلى عمل عن بعد، خاصة وأن الجمارك تمتلك مفتشين معظم عملهم يكون في الميدان، لكن هناك أعمالاً لا تتطلب الحضور ويتم إنجازها عن بعد.

وكشف الخاجة أن الجمارك لديها نظام العمل الهجين، وهناك خطة لتحويل العمل في المبنى الرئيسي إلى عمل عن بعد بنسبة 100%، وحالياً لدينا 30% من الموظفين من يعملون بنظام الهجين، ولا يوجد داخل منظومة الجمارك موظفون يعملون عن بعد من خارج الدولة لحساسية البيانات والمعلومات التي تمتلكها الجهة.

وأكد مدير إدارة الموارد البشرية بجمارك أبوظبي، أن الجمارك لم تتعرض مسبقاً لأي هجمات إلكترونية بسبب النظام التكنولوجي الآمن الذي تم تبنيه، من خلال تفادي أي هجوم استباقي تتعرض له بياناتهم ومعلوماتهم.

وأوضح أن هناك بعض الوظائف في الجهات الحكومية أو القطاع الخاص، لا يصلح أن يعمل الموظف فيها عن بعد من خارج الدولة، خاصة الشواغر الحساسة، وهناك بعض الوظائف العادية التي لا تكون البيانات السرية فيها خطرة، ولا توجد مشكلة في أن يكون الموظف يعمل من الخارج.

**«أنجري بيردس» •**

«استطاعت مجموعة من القراصنة الاستيلاء على بيانات 20 مليون شخص بعدما اخترقوا تطبيق «أنجري بيردس Angry Birds حيث تم وضع فيروس في التطبيق، وتم تنزيله على أكثر من 20 مليون جهاز حول العالم، وكان هدف المخترقين هو الوصول إلى بيانات البطاقات الائتمانية للأشخاص، وتم سد الثغرة في وقت قياسي والحفاظ على بيانات العملاء.

على الشركات والمؤسسات في دولة الإمارات وعلى اختلاف قطاعاتها وأهميتها وقيمة البيانات والمعلومات التي تمتلكها، في ظل التقدم التكنولوجيا الرهيب الذي يشهده العالم، أن تتبع معايير الأمن السيبراني، من أجل الحفاظ على بياناتها وملفاتها المهمة، والتي عند وقوعها في يد القراصنة سوف يكلفها الكثير، من الابتزاز المستمر الذي ستتعرض له بجانب انهيار الشركة وتشويه سمعتها.

وعند الحديث عن العمل عن بعد الذي بات أسلوب حياة، يجب اختيار الأشخاص المناسبين والكفاءات التي ستحافظ على سرية البيانات التي بين أيديهم، وإلا سوف يكون هؤلاء الموظفون خاصة الذين يوجدون خارج الدولة، حملاً ثقيلاً على المؤسسات من خلال تسريب وبيع بيانات العملاء عبر الإنترنت.