«زووم» تطلق حزمة أدوات «Zoom Rooms» لتعزيز مفهوم «العمل من أي مكان»

أعلنت «زووم فيديو كوميونيكيشن» عن طرحها حزمة أدوات Zoom Rooms المبتكرة لمساعدة الشركة على إعادة فتح أبوابها مع الالتزام بمعايير الصحة والأمان وفق مفهوم «العمل من أي مكان». ومع تطور بيئات العمل التقليدية وتكيفها مع متطلبات الموظفين وسعيهم للعمل من مختلف الأماكن والمساحات المتوفرة، سواءً كان ذلك في مقر الشركة، أو ضمن المساحات المشتركة، أو البعيدة، أو حتى في المنازل، باتت منصة «زووم» تلعب دوراً هاماً في تمكين الشركات من وضع صحة وسلامة موظفيها على رأس قائمة أولوياتها.

وفي إطار سعيها الدائم لضمان سلامة الموظفين والعملاء في آنٍ واحد، تواجه المؤسسات تحدياً كبيراً في التعامل المخاوف الثلاثة الرئيسية التي تعتري الموظفين بخصوص العودة والعمل ضمن مقرات الشركات، والتي تتلخص على النحو التالي: القلب من مرتادي مقرات العمل من المرضى، وازدحام مقرات العمل، وتوفير عامل التهوية المناسبة.

في هذا السياق، قال كريغ دور، كبير المحللين لدى شركة «وينهاوس ريسيرش» للأبحاث والدراسات: «لاتزال بيئات ومقرات العمل المكتبية تواصل تطورها وتغيرها بوتيرة مستمرة، إذ تشير الإحصائيات إلى أن أكثر من 80 بالمائة من الموظفين أفادوا بأنهم يعملون عن بُعد، وبأنهم يرغبون بمواصلة إنجاز 50 بالمائة على الأقل من أعمالهم وفق هذه الممارسات بمجرد عودتهم إلى مكاتبهم. لكن لتحقيق هذا الأمر، يجب أن يحظى الموظفون بتجارب عمل صحية وآمنة ضمن غرف الاجتماعات، وبما يلبي الاحتياجات المختلفة للقوى العاملة الصاعدة في يومنا الراهن، وهو ما توفره منصة «زووم» للجميع».

من جانبه، قال أوديد غال، رئيس وحدة المنتج لدى شركة زووم: «تحظى القوى العاملة البشرية بمحط اهتمام وتركيز جميع المؤسسات، لذا فإن الحفاظ على سلامتهم، وأمان قنوات اتصالهم، ومعدلات إنتاجيتهم يعد من أولوياتها القصوى. وبما أن الشركات، والمؤسسات التعليمية، ومرافق الرعاية الصحية، والهيئات الحكومية تستعد لفتح أبوابها من جديد في كافة أنحاء العالم وفق أعلى معايير الصحة والأمان، فإننا نصب جل جهودنا لابتكار كل ما يلبي ويدعم متطلباتهم عبر منصتنا».

وأشارت نتائج دراسة استطلاعية أجرتها مجموعة «بوسطن كونسلتينغ غروب» الاستشارية وشملت 12،000 خبير ومتخصص، إلى أن 60 بالمائة من الموظفين عبروا عن رغبتهم التمتع بالمرونة الكافية في مكان وزمان عملهم. وفي ظل تنامي وانتشار نماذج العمل الهجينة، تعمل شركة «زووم» جاهدةً لابتكار التقنيات الرائدة التي من شأنها تلبية احتياجات عملائها اليوم، والقادرة على التخطيط لتلبية احتياجاتهم المستقبلية، سواءً كان الأمر يتعلق بتسجيل الوصول بشكل افتراضي في مكتب الاستقبال، أو ربط قنوات اتصال بروتوكولات السلامة، أو تحقيق معايير السلامة والأمان في غرف الاجتماعات، مع الانتباه إلى القدرة الاستيعابية للمكان قبل وصول المشاركين إلى غرف الاجتماعات.

الأدوات المبتكرة التي من شأنها المساهمة في إعادة التوجه إلى مقرات العمل بأمان، والقادرة على تلبية المتطلبات المختلفة للموظفين بشكل أفضل:

ربط حزمة أدوات «Zoom Room» مع الأجهزة المحمولة: بالإمكان ربط حزمة أدوات «Zoom Room» مع الأجهزة المحمولة للعملاء التي تعمل وفق نظام تشغيل «آبل» أو «آندرويد»، كي يتمكنوا من الانضمام وبكل بسهولة إلى الاجتماعات التي تتم عبر قنوات «Zoom Rooms» مباشرةً، وذلك انطلاقاً من الأجهزة المحمولة للعملاء، التي سيتم تعريفها وفق وضعية المشارك بشكل تلقائي أثناء الاجتماعات. فبمجرد تحميل تطبيق Zoom Rooms Controller على هاتفك المحمول، ستتمكن من الوصول إلى عناصر التحكم الإضافية بالغرفة، بما فيها القدرة على بدء اجتماع أو الانضمام إليه، وإمكانية التحكم بشكل كامل في مستوى الصوت وعرض الفيديو، وبعدد المشاركين، وهو ما يضمن تمتع المستخدمين الأفراد بالقدرة على التحكم بمستوى تجربة غرفة الاجتماعات الخاصة بهم انطلاقاً من أجهزتهم المحمولة، ما يلغي حاجة المستخدمين إلى لمس وحدة التحكم المشتركة المتاحة داخل غرفة الاجتماعات.

عرض بيانات المشاركين ضمن الزمن الحقيقي: بفضل الكاميرات المدعومة، أصبح بالإمكان معرفة عدد الأشخاص المتواجدين في غرف اجتماعاتك للتحقق من معدلات العديد من العناصر، بما فيها جودة الهواء، ومستوى الرطوبة، ومعدل ثاني أكسيد الكربون، ونسب المركبات العضوية المتطايرة، وذلك بهدف الحفاظ على صحة وسلامة وأمن المشاركين. وبالإمكان أيضاً استعراض هذه البيانات الحيوية والبيئية عن طريق لوحة بيانات نظام Zoom، وعلى لوحة التحكم بغرف الاجتماعات Zoom Rooms Controller، وبواسطة شاشة عرض جدول المشاركين Scheduling Display، وذلك لتلقي الملاحظات والتعليقات المتعلقة بصحة وسلامة غرف الاجتماعات الخاصة بك ضمن الزمن الحقيقي.

وضعية منصة/موظف الاستقبال الافتراضية: توفر وضعية منصة/موظف الاستقبال الافتراضية الجديدة تجربة دخول دون لمس لضيوف المقر أو المبنى، وذلك عن طريق تخصيص زر بدء الاجتماع Start Meeting على وضعية اللمس ضمن جهاز Zoom Rooms الموجود في ردهة مقر العمل لديك، وذلك من أجل ربط الزوار بموظف الاستقبال، والترحيب بهم وفق معايير الصحة والأمان.

كما تتوفر وضعية منصة/موظف الاستقبال الافتراضية الخاصة باللمس في كافة أجهزة Zoom Rooms. التحكم بسطح المكتب المشترك من وضعية اللمس بجهاز Zoom Rooms: يستطيع مستخدمي وضعية اللمس بجهاز Zoom Rooms التحكم بشكل مباشر، وانطلاقاً من أجهزتهم، بسطح مكتب الشخص الذي يشاركهم حالياً شاشة الكمبيوتر المحمول، ما يسهل التعاون ومستوى التشاركية.

تخصيص اللوحة البيضاء (السبورة) للدردشة: أصبح بإمكان الأشخاص الآن مشاركة وضعية لمس اللوحة البيضاء (السبورة) الخاصة بجهاز Zoom Rooms عن طريق Zoom Chat أو البريد الإلكتروني. وفي حال كانت غرفة الـ Zoom Room شخصية، فإنه بإمكانك مشاركتها أيضاً مع مجموعات الدردشة الخاصة بك، الأمر الذي من شأنه المساهمة في تبسيط عملية مشاركة المحتوى خارج نطاق غرفة الاجتماعات، ما يؤدي إلى توطيد الترابط بدرجة كبيرة بين الجيل الصاعد من الموظفين الجدد، ومتطلباتهم المختلفة. بالنتيجة، فإن الركائز الثلاث الرئيسية التي يستند عليها العمل المؤسسي، والتي تسعى لتحقيقها المؤسسات، هي احتضان المواهب، وتحقيق عمليات التحول، وتعزيز الثقة، وهي الركائز التي تطرق إليها «إريك س. يوان»، المؤسس والرئيس التنفيذي لدى شركة «زووم»، من خلال مدونة Zoom تحت عنوان آلية تطور ونمو الأعمال How Business Will Build Forward، وتحدث من خلالها عن أهمية هذه الركائز في تهيئة البيئة المثالية القادرة على تمكين الموظفين من تأدية أعمالهم وفق أعلى المستويات.


شركة «زووم فيديو كوميونيكيشن»

المجددي : 70 في المئة من المحاصيل الزراعية تعتمد على تلقيح النحل


محمد المجددي

أكد خبير إنتاج العسل وتربية النحل ومدير شركة معجزة الشفاء محمد قاسم المجددي أن النحل من الحشرات المهمه في الحياة البشرية، لذلك فإن ظاهرة إنقراض النحل لشيء مخيف، لأنه يهدد حياة البشر، وفي ضوء ذلك طالب خبراء البيئة بمواجهة تلك الظاهرة للحفاظ على الثروة الإقتصادية المتمثلة في « النحل « .

وفي سياق متصل ، أفاد خبير تربية النحل بأن من بين 100 نوع من المحاصيل التي توفر لنا 90% من غذائنا، يتم تلقيح 70% بواسطة النحل، فالنحل هو العنصر الأساسي في تكاثر النباتات، لأنه يعمل على نقل حبوب اللقاح من السداة الذكور إلى المدقات الإناث. وكشف المجددي خلال تصريح صحفي له عن أهم أسباب أختفاء النحل حسب أراء العلماء المتمثلة في المبيدات الحشرية والأمراض والطفيليات فضلاً عن تأثير ظاهرة الاحتباس الحراري والأحوال الجوية بجانب ذبذبات الموجات اللاسلكية.

وقال : تعد حبوب لقاح المحاصيل المعدلة وراثياً سبب رئيسي في موت النحل، لأنها تضعف من مقاومته أمام عدة أنواع من الفطريات، مما يعرض خلايا النحل للسموم.

وأفاد انه بحسب أراء الخبراء والمختصين فإن التعديل الجيني للنباتات قد يكون سبباً لتناقص مستعمرات النحل، لانه يؤدي إلى تحوير وراثي يتزامن مع غبار الطلع للزهور، فتلقح الزهور لتنتج ثماراً معدلة وراثياً ، فضلا عن «عث الفاروا» الذي يعد مصدر رئيسي لمرض معوي يصيب النحل ويؤدي إلى وفاته ، مشيراً الى أن إستخدام علاجات ضد هذا العث، قد تتسبب بأمراض تستدعي استخدام مضادات حيوية قد يؤدي الإفراط باستخدامها إلى خلل في الجهاز المناعي للنحل.

ينتهج إستراتيجيات متعددة المستويات توصي بها «آتيفو نتوركس»

قطاع المصارف الإماراتية يستثمر بشكل واسع في حلول الأمن السيبراني

مع بداية جائحة «كوفيد-19» ونتيجة لتبني معظم الشركات والمؤسسات بشكل فوري سياسات العمل عن بُعد، شهدت دولة الإمارات ودول المنطقة ارتفاعاً ملحوظاً بعدد الهجمات السيبرانية. وضمن الجهود الذي يبذلها المصرف المركزي لدولة الإمارات العربية المتحدة لتعزيز جهود الأمن السيبراني للقطاع المالي على وجه الخصوص، أجرى تدريبا يحاكي الهجمات السيبرانية التي تجرى في الزمن الحقيقي، حيث صُمم هذا التدريب لاختبار مرونة القطاع المصرفي في دولة الإمارات ضد أي تهديدات سيبرانية محتملة.

إضافةً إلى ذلك، نظم اتحاد مصارف الإمارات العربية المتحدة مؤخراً مؤتمراً عبر الويب حول الأمن السيبراني والذي حمل عنوان «ريس» (RaCE)، والذي سيعقد على مدى يومين متتاليين في الفترة الممتدة بين 3 - 4 من شهر فبراير الجاري، والذي سيتم التركيز فيه على أفضل الممارسات في مجال خصوصية البيانات وحمايتها من خطر التهديد السيبراني بالتزامن مع اعتماد العديد من الشركات لبيئة العمل الهجينة أو المختلطة. وفي هذا السياق، تحدث باهي هور، مدير هندسة النظم في منطقة الشرق الأوسط وأفريقيا لدى شركة «أتيفو نتوركس»، قائلاً: «لقد وسّعت جهود التحول الرقمي المتسارعة في القطاع المالي والمصرفي في المنطقة من زيادة مساحة سطح الهجوم التي يمكن استغلالها من قبلي مجرمي الإنترنت والجهات الفاعلة. وبالإضافة إلى هجمات التصيد الاحتيالي والبرامج الضارة، طور المهاجمون وعززوا أنفسهم بأساليب التهديد المستمر المتقدمة «آيه بي تي» (APT) لتجنب الدفاعات الأمنية و إمكانية اختراق الشبكات دون القدرة على اكتشافهم. ما يعزز حاجة مدراء أمن المعلومات لاعتماد إستراتيجية متعددة الطبقات للأمن السيبراني الأمر الذي يضمن سلامة أصولهم الرقمية الثمينة».

أدت سياسات العمل عن بُعد لزيادة حجم الاعتماد على الشبكات الافتراضية الخاصة (VPN) لضمان إمكانية وصول العاملين إلى شبكة الشركة، الأمر الذي وفر مساراً إضافياً للمجرمين لتنفيذ هجماتهم. حيث يكفي استغلال ثغرة أمنية واحدة أو إجراء هندسة اجتماعية على أحد الموظفين للكشف عن بيانات اعتماد الوصول والدخول إلى الشبكة. ويتوقع الخبراء، مع استمرارية الموظفين العمل من المنزل، زيادة في نسبة هجمات التصيد الاحتيالي المتعلقة والمرافقة لجائحة «كوفيد19-» بشكل ملحوظ خلال عام 2021. وقبل انتشار الوباء، كان المحيط الآمن كافياً لمنع مثل هذا النوع من الهجمات الخبيثة، ولكن مع تبني سياسات العمل عن بُعد تبين أنه من الصعب اكتشاف أو معرفة الوصول غير المصرح به، كون الموظفون ينفذون عمليات تسجيل دخولهم في جميع الأوقات ومن أماكن مختلفة وباستخدام أجهزة متعددة.


راي كافيتي

وفي الوقت الحالي، تغير الجهات الفاعلة خططها والتقنيات المتبعة لتجنب اكتشافهم داخل الشبكة وبالتالي زيادة الإيرادات المادية من هذه الهجمات. حيث تبنت هذه الجهات الخبيثة إستراتيجية جديدة تتمحور حول مكوثهم أشهراً مختبئين في النظام والتنقل بحذر داخل الشبكة وانتظارهم بفارغ الصبر لتحديد الأصول الأكثر قيمة لضحاياهم. فقد كشف تقرير صادر عن معهد «بونيمون» لعام 2020 أن متوسط الوقت الذي تستغرقه الشركات في المملكة العربية السعودية والإمارات العربية المتحدة للكشف عن اختراق البيانات هو 269 يوماً.

وقد أدى زيادة عدد الهجمات السيبرانية التي استهدفت المؤسسات المالية في المنطقة إلى تشجيعها بشكل أكبر في ضرورة الاستثمار في عدد من التدابير والحلول الأمنية لمواجهة عديد التهديدات السيبرانية. وهذا ما اجتمع عليه المشاركون في استطلاع للرأي أجرته شركة «كي بي إم جي» (KPMG) لجرائم الأمن السيبراني في الإمارات العربية المتحدة في عام 2020، حيث توقع ما يقارب نسبته 75% من عدد المشاركين بأن تنفق المؤسسات والشركات وتستثمر بشكل أكبر في تقنيات وحلول الأمن السيبراني.

ووفقاً لراي كافيتي، نائب رئيس منطقة الشرق الأوسط وأفريقيا لدى شركة «أتيفو نتوركس»: «بأنه يمكن لمدراء أمن المعلومات التصدي بشكل مسبق للهجمات التي تنفذها مجموعات التهديد المستمر المتقدمة «آيه بي تي» عن طريق استخدام مجموعة من الحلول التي تؤدي إلى اكتشاف وعزل مثل هذا النوع من الهجمات ومعالجتها. في حين توفر الأدوات التي تستخدم تقنيات الخداع والإخفاء وأمان النهاية الطرفية، إمكانات التعرف المبكر للكشف عن أنشطة الاستيلاء على بيانات الاعتماد، ومراقبة الحركة الجانبية، وعمليات تصعيد الامتيازات، بالإضافة إلى أنشطة جمع البيانات».

وأحدثت المؤسسات نقلة نوعية بتحولها من أسلوب الوقاية إلى أسلوب الكشف المبكر عن التهديدات عندما يتعلق الأمر بالأمن السيبراني. وأثبتت الدراسات بأن استخدام العديد من الحلول والمنصات مثل منصة «التصدي للهجمات» (ThreatDefend®) من «آتيفو نتوركس»، بالإضافة إلى حلول أمن النهاية الطرفية، يمنح المؤسسات زيادة بنسبة 42 بالمائة في الإكتشاف المبكر للتهديدات، نظراً لما تتمتع به هذه الحلول من ميزات في تقليل زمن مكوث المهاجم وتقديمها تنبيهات مبنية على أدلة وبراهين قابلة للتنفيذ.

شركة لين تحصل على تصنيف «VMware Cloud Verified»

أعلنت شركة لين ، مزود الخدمات السحابية الخاصة ومقرها الكويت والذي تقدم خدمات مراكز البيانات الافتراضية ، والتعافي من الكوارث ، وحلول النسخ الاحتياطية أنها قد حصلت على تصنيف VMware Cloud Verified. ويدل تصنيف Cloud Verified على أن شركة لين تقدم خدمات متكاملة اعتماداً على البنية التحتية الكاملة لـ VMware Cloud. وبذلك يحصل عملاء الشركة على كافة إمكانيات البنية التحتية السحابية لـ VMware ، بما في ذلك التكامل والتشغيل البيني وتحسين التكلفة والمرونة.

وفي هذا السياق صرح فجحان المطيري ، الرئيس التنفيذي لشركة لين: "لقد كانت لين منذ إنشائها شريكًا لـ VMware. حيث كان هدفنا الاول هو تبسيط عملية تحديث تكنولوجيا المعلومات لعملائنا من خلال تقديم منصة VMware والتي تلبي متطلبات العملاء للحصول على بنية تحتية عالية الأداء وقابلة للتطوير". وأكد المطيري قائلاً: "شركة لين هي اول شركة كويتية تحصل على شارة Cloud Verified ، مما يدلل على مستوى أداء الخبراء والفنيين وموظفي الدعم الذين يمكن لعملائنا الاعتماد عليهم أثناء تحديث عمليات تكنولوجيا المعلومات الخاصة بهم."

وقال هيرفي رينو ، المدير الأول ، VMware Cloud Provider Business :، EMEA "شركاؤنا الحاصلون على تصنيف VMware Cloud Verified يزودون عملائهم بتقنيات VMware Cloud الكاملة والمتقدمة ، مع إمكانية التشغيل البيني عبر السحابة لتحقيق مزايا أكبر. يمكن للخدمات السحابية التي المعتمدة والتي يقدمها موفرو VMware Cloud توفير الكفاءة وخفة الحركة والموثوقية المتأصلة في الحوسبة السحابية. نتطلع إلى دعم خدمات شركة لين لأنها توفر للشركات والمؤسسات مسار بسيط ومرن إلى الحوسبة السحابية ".

شبكة VMware العالمية تضم أكثر من 4000 شريكا من مزودي خدمة VMware Cloud وتوفر البنية التحتية السحابية المتسقة لـ VMware مجموعة واسعة من الخدمات ، كضمان الخصوصية الجغرافية والصناعية ، وكذلك مساعدة العملاء على تلبية المتطلبات التنظيمية المعقدة. يقدم مزودي الخدمات السحابة العاملون في إطار برنامج VMware Cloud Provider حلولًا وخدمات سحابية مصممة بشكل فردي في أكثر من 120 دولة.