

شركات عالمية: «إكسبو» بيئة رقمية آمنة



إكسبو 2020 دبي: حمدي سعد

- عماد حفار: أهمية الحدث فرضت تأميناً صارماً
- أشرف كُحيل: حماية الجميع من أية أهداف خبيثة
- راي كافييتي: تأمين المعلومات على رأس الأولويات

شدد خبراء ومتخصصون في أنظمة وحلول حماية المعلومات من الهجمات الإلكترونية والسيبرانية أن بيئة «إكسبو 2020 دبي» الرقمية والشبكية الداخلية مؤمنة بصورة تامة؛ حيث تتسلح هذه البنية بعتاد تقني شديد التطور يعمل بصورة استباقية لرصد أية هجمات إلكترونية ضد الموقع أو على لزوار على حد سواء.

وقال الخبراء إن «إكسبو 2020 دبي» وباعتباره حدثاً عالمياً يتمتع بشهرة واسعة لدى الجمهور العالمي، كما يعد بيئة مثالية لعقد الصفقات الاقتصادية في جميع المجالات، لذا فقد خضعت البيئة الشبكية والرقمية في الموقع لتحصينات

قوية ضد أية هجمات خبيثة لأي سبب. وأشاروا إلى أنه قد تم في موقع «إكسبو 2020 دبي»، العديد من العمليات التقنية المعقدة لمحاكاة أعلى وأقوى الهجمات الإلكترونية والسيبرانية الخبيثة التي تستهدف البنية الشبكية أو الرقمية في الموقع.

في الوقت نفسه أطلق الخبراء رسائل تحذيرية لجميع المهتمين بالحدث من داخل وخارج الإمارات عند التعامل مع الرسائل التي تستخدم اسم الحدث في الترويج لأي شيء أو الدعوة لزيارة الحدث أو للتوظيف أو لأي سبب آخر دون التأكد تماماً من مصداقية المصدر أو الروابط أو البرامج أو غيرها عند التعامل مع هذه الرسائل أو الروابط.

وكشف العديد من الجهات الحكومية المعنية بتأمين موقع «إكسبو 2020 دبي» رقمياً ومعلوماتياً عن إجراء عدد من التمارين السيبرانية، بهدف تأمين المعلومات والشبكات ورفع كفاءة الاستجابة وسرعة التعامل مع أية محاولات لاختراق «البنية الرقمية الخاصة بموقع الحدث العالمي «إكسبو 2020 دبي».

وتم تنفيذ العديد من عمليات المحاكاة الواقعية للتعامل مع أية هجمات سيبرانية أو إلكترونية بالتعاون مع الفريق المختص بهذه العمليات في موقع «إكسبو 2020 دبي» لضمان الجاهزية التامة والتعامل مع أية مخاطر متوقعة أو غير متوقعة.

وأكدت الجهات المعنية أن جميع التمارين وعمليات المحاكاة أثبتت الجاهزية التامة للبنية الرقمية في موقع «إكسبو 2020 دبي» لصد أية هجمات سيبرانية أو إلكترونية على الشبكات أو على الزوار اعتماداً على بنية دولة الإمارات المعروفة عالمياً فيما يخص تطبيق أعلى معايير الأمن السيبراني في العالم.

ويتعاون «إكسبو 2020 دبي» مع عدد من أبرز الشركاء التقنيين والرقميين في العالم وينسق بشكل كامل مع كافة الجهات الحكومية والخاصة بهدف تعزيز بنية تأمين المعلومات وصد الهجمات السيبرانية والرقمية وفق منظومة تتسم بالاستباقية والمرونة والاستدامة والصلابة والاحترافية.

تأمين قوي للشبكات والاتصالات

أكد عماد حفار، رئيس الخبراء التقنيين الإقليمي في شركة «كاسبرسكي» العالمية، أن حدثاً عالمياً بحجم وأهمية «إكسبو 2020 دبي» قد تم تأمينه شبكياً ومعلوماتياً واتصالياً بصورة صارمة، كونه يمثل فرصة ثمينة لمجرمي وقراصنة المعلومات الساعين ليل نهار للاستفادة منه كحدث شهير إما بقصد التخريب أو طلب الفدية المالية.

وأضاف حفار، أن قراصنة الإنترنت والمعلوماتية بشكل عام دائماً ما يستخدمون جميع الوسائل المغرية والتي تبدو صحيحة وبديهية للمستهدفين ويمثل حدث «إكسبو» العالمي أحد أهم الفعاليات العالمية التي يستغلها القرصنة للإيقاع بالضحايا عبر الرسائل الاحتمالية من خلال الرسائل والإعلانات الترويجية عبر الإيميلات أو المواقع المزورة أو عن طريق الرسائل النصية أو برامج التخاطب أو مواقع التواصل الاجتماعي.

وأوضح أن قراصنة الإنترنت بدأوا مؤخراً في التركيز على اصطيد الأشخاص والمعلومات التي تمثل قيمة سواء للجهات أو الشركات أو الأفراد بغرض طلب الفدية أو بيع هذه المعلومات لجهات أخرى أو لطلب الفدية لإرجاع هذه البيانات مرة أخرى لأصحابها.

ونصح حفار، بضرورة عدم الانسياق وراء الرسائل أو المخاطبات عبر التفاعل أو الرد عليها قبل التأكد تماماً من مصداقية الجهة المرسله أو عدم مشاركة أية بيانات حساسة أو مالية أو تنزيل أية برمجيات أو ملفات مشكوك فيها أو الرد على الرسائل مجهولة المصدر أو غيرها من الوسائل التي تمثل الخط الأول للهجمات السيبرانية والإلكترونية. «الخبثة، لاسيما التي تستغل اسم «إكسبو»

وأوصى رئيس الخبراء التقنيين الإقليمي في شركة «كاسبرسكي» كافة الجهات والأفراد بعدم التعامل مع أية جهات مشبوهة تستخدم اسم إكسبو في الترويج أو توفير الوظائف أو حتى الانسياق وراء مطالبة القراصنة بدفع المال لإرجاع البيانات المقرصنة، مع ضرورة عمل نسخ احتياطية للبيانات وحفظها في مكان غير مربوط بشبكة الإنترنت أو وحدات تخزين بيانات تتوافر فيها كافة معايير التشفير وحفظ البيانات

منع اكتشاف الهويات والبيانات

ويقول راي كافيتي، نائب الرئيس الإقليمي في شركة «آتيفو نتوركس» عندما تجذب الأحداث الضخمة مثل «إكسبو 2020 دبي» ملايين الزوار، تجذب معها أعين قراصنة الإنترنت أيضاً

ففي الوقت الذي يسهم فيه الحدث في تعزيز اقتصاد الدولة لا يمكن أن نغفل أنه ممن الممكن أن يكون مركزاً لضحايا محتملين سواء كانوا من الدولة أو الزوار و المشاركين في الحدث

وأضاف كافيتي، أن عمليات الاحتيال باسم «إكسبو 2020 دبي» بدأت في الظهور قبل انطلاقه؛ حيث ظهر العديد من حملات الاحتيال التي استهدفت الأفراد عن طريق إيهامهم بوجود فرص عمل، كما شهدنا أيضاً عمليات احتيال عبر الهاتف كان الهدف منها جمع المعلومات المصرفية للضحايا بأنهم سيدخلون السحب على جوائز تقدم ضمن فعاليات الحدث.

وتابع: تعتبر هذه الحوادث وغيرها بمثابة تحذير بأن قراصنة الإنترنت لاحظوا الشغف لزيارة «إكسبو 2020 دبي» من مختلف بقاع العالم، مما يزيد احتمالية سرقة بيانات الضحايا، وجني الأرباح من المشاركين الأبرياء، لذا كان من المهم وضع جميع المشاركين في الحدث على رأس أولويات الجهات المعنية بأمن المعلومات داخل الموقع والتأكد التام من أن الجهات الخبيثة لن تتمكن من اكتشاف هوياتهم وبياناتهم واستغلالها

وأكد كافيتي، ضرورة وضع التدابير المناسبة في مكانها الصحيح لتأمين الهويات من خلال اعتماد حلول اكتشاف التي ترسل التنبيهات في حال حدوث سوء استخدام لبيانات الاعتماد أو لأي سبب مريب (IDR) الهوية والاستجابة

عتاد قوي لحماية البيانات

بدوره قال أشرف كُحيل، مدير وحدة تطوير الأعمال الإقليمي في «جروب-آي بي»: يعتبر معرض «إكسبو 2020 دبي» حافزاً اقتصادياً للعديد من الحكومات والمؤسسات في الوقت نفسه يوفر فرصاً هائلة لقراصنة الإنترنت والجهات المهاجمة للاستفادة من الاهتمام الهائل لمجتمع الأعمال العالمي ومحاولة تحقيق أهداف خبيثة أو ضارة أو مالية من الحدث العالمي وهو ما استدعى منذ البداية تجهيز الموقع بعتاد قوي من نظم حماية البيانات بشكل أكثر صرامة. وقال كحيل: يعد استخدام البريد الإلكتروني الآن أحد أكثر ناقلات الهجوم تفضيلاً وذو أولوية لدى الجهات الفاعلة والمحتملين الصغار الذين يرغبون في قطف الثمار السهلة والقريبة من متناول اليد، كما أن جهات التهديد الفاعلة

الكبيرة تستخدم البريد الإلكتروني لإرسال برمجيات الفدية العديدة للأهداف ذات القيمة المادية العالية مثل المشاركين «ومنظمي معرض «إكسبو 2020 دبي»».

وأوضح، برزت أهمية برمجيات الفدية باعتباره خطراً على العالم بأسره، كونها تحدث ضرراً في عمل المنظمة ككل، كما أنها لا تعتمد على جني الأموال من عائدات الابتزاز فحسب؛ بل تجنبها أيضاً من عمليات تسريب البيانات المهمة والسرية عبر شبكة الإنترنت، لذا يعد الاستثمار الأمثل في تعزيز أمان البريد الإلكتروني القادر على حظر التهديدات الإلكترونية وتخفي مخاطر الاختراقات من أكثر الأمور حكمة وعقلانية عوضاً عن الامتثال لمطالب الجهات الفاعلة. ودفع المبالغ الطائلة كفدية

وأضاف، نتوقع ظهور جميع أنواع عمليات الاحتيال التي تسعى للحصول على البيانات الشخصية وبيانات الدفع البنكي على مستوى الفرد المرافقة لهذا الحدث

وتتمثل عمليات الاحتيال هذه بانتحال قراصنة الإنترنت شخصيات وهمية تمثل منظمي الحدث مما يوهم الضحايا بضرورة عرض وإبراز جميع المعلومات الشخصية التي يتم استخدامها لاحقاً لأغراض احتيالية أخرى، لذا فإن السبيل الوحيد للمضي قدماً في مواجهة مثل هذه المخاطر هو مراقبة البنى التحتية للجهات الاحتياطية وإجراء عمليات الاستقصاء لجمع المعلومات حول مخططاتهم المتطورة التي صممت لاستهداف كيان معين

وأكد كُحيل، أنه من الواجب أيضاً إجراء حملات توعية لتنبهه العامة والزوار بخطر عمليات الخداع التي تتخذ من معرض «إكسبو 2020 دبي» غطاء لتنفيذ عملياتها

الجاهزية التقنية التامة

يقول عماد فهمي، مدير هندسة النظم الإقليمي في شركة «نتسكاوت»: يعد الحفاظ على خدمات وتقنيات الاتصال خلال «إكسبو 2020 دبي» عاملاً حاسماً لتحديد نجاح الحدث على المستوى التقني الذي يمثل عصباً مهماً وعاملاً حاسماً في نجاح تنظيم الحدث العالمي؛ حيث يقدم الحدث العظيم العديد من التقنيات المستقبلية من مختلف أنحاء العالم، والتي تعتمد بشكل كبير على اتصال آمن وموثوق. وقال: وفقاً لأحدث تقاريرنا «استقصاء معلومات التهديدات» والذي غطى النصف الأول من عام 2021، فإن عمليات الابتزاز الثلاثي، المتمثلة في تشفير الملفات وسرقة البيانات وهجمات. يمثل أحدث استراتيجيات برامج الفدية في العام الماضي (DDoS) «حجب الخدمة الموزعة

وتحجب مثل هذه الهجمات البيانات الحساسة وتؤثر بشكل مباشر في أداء المؤسسة من خلال إبطاء شبكتها من خلال هجمات حجب الخدمة الموزعة لذا وكون المعارض العالمية الكبرى ك«إكسبو 2020 دبي» جذاباً للجهات المهاجمة تعمل هذه الجهات الخبيثة على تعطيل الخدمات المقدمة للمشاركين أو الزوار بهدف الإيقاع بالضحايا لدفع مبالغ طائلة كفدية لاستعادة الخدمات المحجوبة وضمان استمراريتها