

توقعات للأمن الإلكتروني في المستقبل القريب 8



استعرضت شركة جارتنر للأبحاث أبرز توقعاتها للأمن الإلكتروني خلال الأعوام القليلة القادمة. وقال ريتشارد أديسكوت، كبير المحللين لدى «جارتنر»: «لا شك أن تركيز الرؤساء التنفيذيين لأمن المعلومات والفرق العاملة معهم يجب أن يكون منصباً على ما يجري اليوم لضمان تحقيق أعلى مستويات الأمان في مؤسساتهم. لكن يتوجب عليهم أيضاً إيجاد الوقت المناسب ضمن مشاغلهم في التعامل مع التحديات اليومية، وذلك من أجل التفكير فيما هو قادم في الأفق لمعرفة ما قد يجري مستقبلاً وقد يؤثر على برامجهم الأمنية خلال الأعوام القليلة المقبلة، هذه التوقعات السابقة تعتبر مؤشراً على بعض هذه الأمور التي يمكن أن تطرأ ويجب أن تؤخذ بعين الاعتبار أي مدير تنفيذي لأمن المعلومات يتطلع إلى إيجاد برنامج أمن سيبراني فعال ومستدام».

وجاءت توقعات جارتنر على النحو التالي:

1. حتى العام 2027، فإن 50% من الرؤساء التنفيذيين لأمن المعلومات سوف يتبنون رسمياً تصاميم ممارسات تركّز على العامل البشري ضمن برامجهم للأمن السيبراني، وذلك بهدف الحدّ من التدخّلات في سير العمليات وتشجيع الاعتماد على خيارات التحكم. أظهرت دراسة «جارتنر» أن ما يزيد على 90% من الموظفين الذين

- أقرّوا بإقدامهم على القيام بإجراءات غير آمنة خلال أنشطة عملهم كانوا يعلمون أن ممارساتهم هذه تزيد من تعريض مؤسساتهم للمخاطر، لكنهم أصرّوا على ممارساتهم على الرغم من ذلك
2. بحلول العام 2024، سوف تغطّي القوانين التنظيمية الحديثة غالبية بيانات المستهلك، إلا أن أقل من 10% فقط من المؤسسات سوف تكون قادرة على توظيف حماية البيانات لكسب أفضلية تنافسية. بدأت المؤسسات تُدرك أن بإمكان برامج حماية بيانات الخصوصية أن تمكّنهم من استخدام البيانات على نطاق أوسع، وتوظيف هذه الميزة للتمييز عن المنافسين، ومدّ جسور الثقة مع العملاء، والشركاء، والمستثمرين، والجهات التنظيمية
3. بحلول العام 2026، سوف يمتلك 10% من الشركات الكبرى برامج أمان الثقة الصفرية لحماية شاملة، وناضجة، وقابلة للقياس، مقارنة بنسبة لا تتعدى اليوم 1%. إن تطبيق حلول أمان الثقة الصفرية على نطاق واسع وناضج يتطلب تكامل وإعداد عدد مجموعة من المكونات، وهي مهمة يمكن أن تصبح تقنية ومعقدة. إن النجاح يعتمد إلى حد كبير على ترجمة ذلك إلى قيمة للأعمال
4. بحلول العام 2027، فإن 75% من الموظفين سوف يمتلك، أو يطور، أو ينشئ تقنيات لا تقع ضمن نطاق رقابة أقسام تقنية المعلومات - لترتفع النسبة من معدّل 41% كانت عليه في العام 2022. إن طبيعة الدور المنوط بالرؤساء التنفيذيين لأمن المعلومات ونطاق مسؤولياتهم يشهد تحولاً من كونهم المسؤولين عن السيطرة إلى اتخاذ القرارات التي تتعلّق بالمخاطر. ولذا، فإن إعادة تعريف إطار عمليات الأمن السيبراني باتت مطلباً أساسياً للتعامل مع التغييرات القادمة
5. بحلول العام 2025، سيكون 50% من قادة الأمن السيبراني قد جرّبوا دون جدوى استخدام التقييم الكمي للمخاطر لتعزيز آليات اتخاذ القرار في المؤسسات. تشير أبحاث شركة «جارتنر» إلى أن 62% ممن اعتمد التقييم الكمي للمخاطر السيبرانية أقرّوا بتحقيق مكاسب بسيطة على صعيد المصدقية والتوعية بالمخاطر الأمنية، إلى أن 36% فقط نجحوا في تحقيق نتائج بالاعتماد على هذه الإجراءات، شملت الحدّ للمخاطر، وتوفير التكاليف، أو حتى التأثير فعلياً في القرار
6. بحلول العام 2025، فإن قرابة نصف قادة الأمن السيبراني سيعمدون إلى تغيير وظائفهم، بل سيّجّه 25% منهم إلى أعمال مختلفة كلياً بسبب الضغوط المرتبطة بأعمالهم. بعد تسارعها في ظل الجائحة ونقص الكفاءات في مختلف مجالات الصناعة، فإن ضغوط العمل على المختصين في مجال الأمن السيبراني لم تعد تُحتمل. وفي حين لا تظنّ «جارتنر» أن التخلّص تماماً من هذه الضغوط يبدو واقعياً، فإنه بإمكان الأفراد التعامل مع التحديات وضغوط العمل في بيئة توفّر لهم الدّعم الذي يحتاجون إليه
7. بحلول العام 2026، فإن 70% من مجالس الإدارة سوف تضمّ عضواً يمتلك خبرة في الأمن السيبراني. لا بدّ لقادة أمن المعلومات الراغبين في اعتبارهم شركاء في الأعمال أن يدركوا استعداد الشركات ومجالس إدارتها للتعامل مع المخاطر. وهذا يعني ألا تقتصر المهمة على إظهار قدرة برامج الأمن السيبراني على منع حدوث أمور غير مرغوب بها، بل أيضاً قدرتها على تحسين قدرة الشركات على التعامل مع المخاطر بفاعلية
8. سوف تعتمد على TDIR بحلول العام 2026، فإن 60% قدرات حلول كشف التهديدات، والتحقّق والاستجابة لبيانات إدارة الهجمات وذلك للتحقّق من التهديدات وتحديد أولوياتها، علماً أن نسبتها لا تتعدى 5% اليوم. مع استمرار نمو الأسطح المعرضة للهجمات لدى الشركات في ظل تعدّد خيارات الاتصال، واستخدام خيارات مثل وتطبيقات حوسبة السحاب، فإن الشركات باتت اليوم بحاجة أوسع من أدوات المراقبة SaaS البرامج- كخدمة وإدارتها مركزياً للتحقّق من الرقابة المستمرة وأية تهديدات

"حقوق النشر محفوظة" لصحيفة الخليج. © 2024.