مستقبل الأمان الرقمي

جمال مراد قيس

2025-11-04

الأمن السيبراني في عام 2025 لم يعد مجرد درعٍ رقمي يحمي الأنظمة من الاختراق، بل أصبح عنصرًا استراتيجيًا يمكّن المؤسسات من الابتكار والنمو بأمان. في ظل التحول الرقمي السريع الذي يشمل كل القطاعات، بات الأمن السيبراني اليوم جزءًا لا يتجزأ من عمليات الأعمال، وأصبح يُنظر إليه بوصفه عامل تمكين وليس عبئًا ماليًا. تشير تقارير حديثة إلى أن العديد من المؤسسات العالمية والعربية بدأت تتعامل مع الأمن كاستثمار في الثقة والمرونة الرقمية، لا كتكلفة إضافية. لم يعد الهدف هو تفادي الهجمات فحسب، بل بناء أنظمة قادرة على الصمود والتكيّف في مواجهة أي تهديد محتمل.

تشهد بيئة التهديدات السيبرانية تحولات جذرية بفعل الذكاء الاصطناعي، حيث أصبحت الهجمات أكثر تعقيدًا وتنظيمًا. لم يعد المهاجم شخصًا يجلس خلف شاشة، بل شبكة من الخوارزميات القادرة على التعلم والتخفي ومهاجمة نقاط الضعف بسرعة مذهلة. وتشير الدراسات إلى أن نحو نصف المؤسسات حول العالم تعتبر الهجمات المدعومة بالذكاء الاصطناعي الخطر الأكبر في العام الحالي، خاصة تلك التي تستهدف سلاسل الإمداد وأنظمة الخدمات السحابية. أمام هذا المشهد، لم يعد كافيًا الاعتماد على أنظمة الحماية التقليدية، بل بات لزامًا تبني استراتيجيات تعتمد على التحليل الاستباقي واستخدام الذكاء الاصطناعي في الدفاع ذاته.

في المنطقة العربية، تتسارع الجهود لتأسيس منظومات أمنية رقمية متكاملة. فقد حصلت مؤخرًا شركة متخصصة في الأمن السيبراني في مصر على اعتماد رسمي من هيئة الاتصالات، في خطوة تعكس نضوج البنية التنظيمية العربية واستعدادها لاحتضان الكفاءات المحلية. هذا التطور لا يمثل إنجازًا تقنيًا فحسب، بل خطوة استراتيجية في بناء الثقة الرقمية داخل الاقتصاد العربي المتنامي. غير أن الطريق لا يزال طويلًا، إذ تتطلب المرحلة القادمة الاستثمار في البنية التحتية، وتدريب الكفاءات، وتطوير التشريعات لتواكب سرعة الابتكار التقني.

الأمن السيبراني ليس فقط مسألة تقنية، بل ثقافة يجب أن تتجذر في سلوك الأفراد والمؤسسات. تشير التجارب الخليجية إلى أن حملات التوعية والتدريب العملي أسهمت في تقليل حوادث الاختراق بنسبة ملحوظة. ففي قطر مثلًا، نظمت الجهات الوطنية حملات توعوية مكثفة شارك فيها آلاف الموظفين لتعليمهم كيفية اكتشاف محاولات التصيّد الإلكتروني والتعامل مع الرسائل المشبوهة. مثل هذه المبادرات تبرهن أن العنصر البشري يظل الحلقة الأضعف والأقوى في الوقت ذاته، وأن أمن المؤسسة يبدأ من وعي موظفيها.

ومع تصاعد التهديدات وتعقّد المشهد الرقمي، يتجه التفكير العالمي نحو تحويل الأمن من رد فعل إلى ثقافة وقائية. أصبح على المؤسسات بناء أنظمة تستشرف الهجمات قبل وقوعها، وتضع سيناريوهات واقعية للتعامل مع الانتهاكات المحتملة. كما يجب أن يتحول الأمن إلى مسؤولية جماعية لا تقتصر على فرق تكنولوجيا المعلومات، بل تشمل كل المستويات الإدارية. الذكاء الاصطناعي يمكن أن يكون السلاح الأمضى للدفاع إذا استُخدم بوعي، من خلال أنظمة قادرة على اكتشاف الأنماط الشاذة وتحليل سلوك المستخدمين والبرمجيات في الزمن الحقيقي.

يمكن القول إن الأمن السيبراني في 2025 يمثل نقطة تحول في العلاقة بين الإنسان والتقنية. لم يعد الأمان هدفًا نهائيًا، بل رحلة مستمرة نحو التكيّف مع بيئة متغيرة. في عالمٍ باتت فيه البيانات أغلى من النفط، يصبح الحفاظ عليها مسؤولية مشتركة بين الحكومات والشركات والأفراد.

الأمان الرقمي ليس جدارًا نُشيّده، بل وعيًا نزرعه في عقولنا وسلوكًا نمارسه كل يوم. حين ندرك أن ضغطة زر واحدة قد تفتح الباب لهجوم أو تحمي منظومة كاملة، سنفهم أن الأمن الحقيقي يبدأ منا نحن، من وعينا وسلوكنا وقدرتنا على أن نكون خط الدفاع الأول عن ذواتنا ومجتمعاتنا في العالم الرقمي الجديد.

المصادر

Mitigation Strategies Against Phishing Attacks: A Systematic Review

Understanding and How to Protect Against Evolving Phishing Attacks

Preventing Phishing Attacks

تواصل مع الكاتب: mohamedmouradgamal@gmail.com

/https://arsco.org/articles/article-detail-47621