Deloitte.

استبيان مستقبل الأمن السيبراني في الشرق الأوسط لعام 2024

آفاق الأمن السيبراني

تعزيز القيمة التحويلية من خلال صمود الأمن السيبراني

حقبة جديدة من استراتيجيات الأمن السيبراني التحويلية

التركيز على النتائج والصمود

يشهد مستقبل الأمن السيبراني تطوراً مستمراً حيث تواجه المؤسسات في جميع أنحاء العالم تعقيدات وتغييرات مستمرة في أعمالها، بالإضافة إلى عدد لا يُحصى من التهديدات والمخاطر الجديدة. إلا أن أمراً واحداً لا يزال ثابتاً في هذا المشهد المتغير: الترابط العميق بين الأمن السيبراني وقيمة الأعمال، ولا يزال الأمن السيبراني يشكل مسألة محورية في كيفية تحقيق المؤسسات في كل قطاع للنتائج التي ترغب فيها باستمرار.

تبرز هذه العلاقة القوية بين الأمن السيبراني وتأثيره على الأعمال بشكل واضح في النسخة الرابعة من الاستبيان العالمي لمستقبل الأمن السيبراني الذي أجرته ديلويت - والذي طلبت فيه ديلويت من حوالي 1,200 من مدراء المؤسسات العاملة في مختلف القطاعات حول العالم إعطاء آرائهم حول التهديدات السيبرانية، والأنشطة التي تقوم بها مؤسساتهم، والمستقبل. شمل هذا الاستبيان المدراء التنفيذيين في مختلف المؤسسات، بالإضافة إلى كبار القادة الآخرين المسؤولين عن تقنية المعلومات، وأمن المعلومات، والمخاطر، والأعمال.

للاطلاع على المزيد من المعلومات، يرجى زيارة الموقع الالكتروني **http://www.deloitte.com/futureofcyber**

كيف يبدو مستقبل الأمن السيبراني في الشرق الأوسط؟

تقدم هذه المجالات الخمسة الرئيسية لمحة عما وصلت إليه المؤسسات في الشرق الأوسط الآن في مجال الأمن السيبراني - وإلى أين تتجه.

اعتماد الذكاء الاصطناعي

%62 %84

من المستجيبين في الشرق الأوسط أفادوا باستخدام مؤسساتهم لقدرات الذكاء الاصطناعي في برامج الأمن السيبراني الخاصة بهم إلى حد معتدل أو كبير.

حوكمة الذكاء الاصطناعي

%83 %80

من المستجيبين في الشرق الأوسط في المتوسط أفادوا بوجود ضعف في حوكمة استراتيجياتهم الناشئة للذكاء الاصطناعي التوليدي مما يؤدي إلى مخاطر تتعلق بالبيانات وسلامتها وسريتها

التزام الإدارة التنفيذية

%89 %88

من المستجيبين في الشرق الأوسط أفادوا بأن مجالس إدارة مؤسساتهم تعالج المشكلات المتعلقة بالأمن السيبراني مرة واحدة كل ثلاثة أشهر، إن لم يكن أكثر من ذلك

المؤسسة الموسّعة

%64 %71

من المستجيبين في الشرق الأوسط أفادوا بأن مؤسساتهم تستعين بمزوّدين خارجيين لتطبيق إطار إدارة مخاطر الأمن السيبراني وتقنيات مراقبة المنظومة السحابية

اختراقات الأمن السيبراني

%61 %74

من المستجيبين في الشرق الأوسط قالوا إنهم أبلغوا علنًا عن واحد إلى عشرة اختراقات للأمن السيبراني في السنة الماضية

النتائج العالمية

رؤى لاستشراف مستقبل الأمن السيبراني

كيف يستطيع كبار المدراء الارتقاء بالأمن السيبراني في جميع أنحاء مؤسساتهم العاملة في الشرق الأوسط في ظل مشهد سيبراني دائم التطور؟ من شأن الاستنتاجات الخمس التالية والإجراءات الخمسة المقابلة لكل منها أن توفر نقطة انطلاق لاستشراف مستقبل الأمن السيبراني استناداً إلى خبرة ديلويت ونتائج الاستبيان الذي أجرته مؤخراً

رؤى ملهمة	إجراءات يجب مراعاتها
1. التركيز على حلول الأمن السيبراني المعززة بالذكاء الاصطناعي. يتطور مستقبل الأمن السيبراني بالتزامن مع تطور الذكاء الاصطناعي. تشمل أهم الطرق التي تركز عليها المؤسسات استخدام الذكاء الاصطناعي لتعزيز قدرات الأمن السيبراني لديها، والتي تشمل مراقبة البنى التحتية الرقمية، والمحاكاة المتقدمة، وإجراءات الأمن الآلية (المؤتمتة).	**تحويل الذكاء الاصطناعي إلى عامل تمكين في استراتيجية الأمن السيبراني بدلاً من أن يكون خطراً عليها.** بناء القدرات الأمنية المعززة بالذكاءالاصطناعي داخل المؤسسات من أجل استباق التهديدات المتطورة مع الحفاظ على الثقة والامتثال. يجب البدء بتحديد المجالات التي يمكن أن يعزز فيها الذكاء الاصطناعي عمليات الكشف عن المخاطر والأتمتة والاستجابة. كما يجب نشر أدوات معززة بالذكاء الاصطناعي، وتوفير الشفافية والرقابة، بما يضمن دعمها للخبرات البشرية.
2. تحقيق التوازن بين ابتكارات الذكاء الاصطناعي والأمن السيبراني. بينما يُحدث الذكاء الاصطناعي تحولاً في الأعمال، إلا أنه يطرح تحديات جديدة في مجال الحوكمة من أبرزها إمكانية تعرّض البيانات الحساسة لخطر الاختراق في ظل غياب قواعد واضحة لحمايتها. بناء على ذلك، تعمل الشركات الرائدة على إنشاء أطر حوكمة الذكاء الاصطناعي لضمان أن تتعامل نماذج الذكاء الاصطناعي مع البيانات الحساسة بطريقة آمنة مع الحفاظ على الامتثال للوائح التنظيمية المتطورة.	**إنشاء حوكمة قوية للاستفادة من قوة الذكاء الاصطناعي مع حماية البيانات.** قد يؤدي اعتماد الذكاء الاصطناعي إلى مخاطر أمنية كبيرة في ظل عدم وجود إطار حوكمة واضح. لذلك، يجب أولاً صياغة سياسات لإدارة البيانات التي يتم إنشاؤها بالذكاء الاصطناعي، وفرض ضوابط السرية، وإجراء تقييمات منتظمة للمخاطر. كما يجب تشكيل فريق حوكمة الذكاء الاصطناعي لكي يتعاون مع إدارات / أقسام الأمن والامتثال والأعمال لضمان استخدام الذكاء الاصطناعي بطريقة مسؤولة وآمنة.
3. الأمن السيبراني كضرورة استراتيجية. تدرك مجالس الإدارة والمدراء التنفيذيين أن مخاطر الأمن السيبراني تؤثر بشكل مباشر على أعمال مؤسساتهم. لذلك، تحرص المؤسسات على طرح المناقشات المتعلقة بأمن المعلومات في اجتماعات مجلس الإدارة، وضمان توافق استراتيجيات أمنها السيبراني مع صمود أعمالها بشكل عام. ومن شأن المناقشات المتكررة التي تجريها مجالس الإدارة والمدراء التنفيذيين حول مخاطر الأمن السيبراني أن تؤدي إلى اتخاذ مواقف أقوى وأكثر استباقية تجاه مسائل الأمن السيبراني.	**جعل الأمن السيبراني موضوعاً رئيسياً في مناقشات مجلس الإدارة.** تؤثر المخاطر السيبرانية على الأعمال بشكل مباشر، وعليه يجب على قيادة المؤسسة المشاركة بفعالية في هذه المناقشات. وفي حال عدم مناقشة الأمن السيبراني على مستوى مجلس الإدارة، ينبغي تنفيذ جلسات إحاطة منظّمة، وإنشاء لوحات معلومات في الوقت الحقيقي، وجلسات تدريب للإدارة التنفيذية. كما يجب إجراء عمليات محاكاة لأزمات الأمن السيبراني لإعداد القيادة لمواجهة التهديدات الحقيقية، وضمان توافق الاستثمارات في مجال الأمن السيبراني مع أهداف العمل الأوسع.
4. يتجاوز صمود الأمن السيبراني الحدود المادية للمؤسسات. في عالم اليوم المترابط، تشكل المخاطر المرتبطة بالأطراف الخارجية وسلسلة التوريد مصدر قلق متزايد للمؤسسات؛ الأمر الذي يدفع هذه المؤسسات نحو مراقبة تلك الأطراف الخارجية بشكل مستمر، وتعزيز العناية الواجبة، وإجراء تقييمات آلية (مؤتمتة) للمخاطر. ونتيجة لهذه المخاطر التي تقف على قمة منحنى المخاطر، تتجه المؤسسات إلى تضمين متطلبات الأمن السيبراني في عمليات المشتريات، واستخدام أدوات الأمن السحابية والفورية للكشف عن الثغرات الأمنية في سلسلة التوريد والاستجابة لها.	**تعزيز أمن سلسلة التوريد الأطراف الخارجية لحماية منظومتكم.** لا تقتصر مخاطر الأمن السيبراني على محيط مؤسستكم فقط. لذلك، يجب وضع إطار لإدارة مخاطر الأطراف الخارجية يشمل تقييمات أمن سلسلة التوريد والتزامات الأمن التعاقدية والمراقبة في الوقت الفعلي. كما يجب دمج تقنية مراقبة المنظومة السحابية لتتبع الوضع الأمني باستمرار لدى العديد من المورّدين، بالإضافة إلى التأكد من أن المورّدين يستوفون معايير الأمان التي تضعونها وجاهزون لتنفيذ تدابير الاستجابة للحوادث لمعالجة التهديدات الخارجية.
5. الانتقال من ردود الفعل إلى النهج الاستباقي في التعامل مع الاختراقات. مع ازدياد درجة تعقيد تهديدات الأمن السيبراني، تنتقل المؤسسات من مجرد الاستجابة كرد فعل على الحوادث السيبرانية إلى العمل الاستباقي لمنع وقوع هذه التهديدات. لذلك، يستثمر قادة المؤسسات في الأدوات الأمنية المعززة بالذكاء الاصطناعي، ويجرون عمليات محاكاة للهجمات السيبرانية، ويقدمون التدريب للموظفين لتمكينهم من التعرّف على التهديدات السيبرانية والإبلاغ عنها.	**توقّع الانتهاكات ورصدها والاستجابة لها.** حتى لو لم تواجه مؤسستك اختراقًا علنيًا، فمن المهم أن تكون استباقيًا في حماية أصولك الرقمية. تعزيز قدراتك في مجال الحصول على معلومات عن التهديدات ومراقبتها والاستجابة لها للكشف عن الاختراقات في وقت مبكر. كما يجب عليكم تدريب الموظفين والقيادة على التعرف على الحوادث الأمنية والإبلاغ عنها، والتأكد من اختبار خطة الاستجابة للحوادث وتعديلها والتأكد من جاهزيتها للحد من تعطيل أعمال المؤسسة .

Deloitte.