

آفاق الأمن السيبراني

تعزيز القيمة التحويلية من خلال صمود الأمن السيبراني

حقة جديدة من استراتيجيات الأمن السيبراني التحويلية

التركيز على النتائج والصمود

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.

يشهد مستقبل الأمن السيبراني تطوراً مستمراً حيث تواجه المؤسسات في جميع أنحاء العلم تعقيدات وتغيرات مستمرة في أعمالها، بالإضافة إلى عدد لا يحصى 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.

للاطلاع على المزيد من المعلومات، يرجى زيارة الموقع الإلكتروني <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.

اعتمد 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

الترام 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 الموسعة



%64  %71

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

اختراقت الأمن السيبراني



%61  %74

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

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

تحويل الذكاء الاصطناعي إلى عامل تمكين في استراتيجية الأمن السيبراني بدلاً من أن يكون خطراً عليها. بناء القدرات الأمنية المعززة بالذكاء الاصطناعي 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 والأئمة والاستجابة. كما يجب نشر أدوات معززة بالذكاء الاصطناعي، وتوفير الشفافية والرقابة، بما يضمن دعمها للخبرات البشرية.

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.

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.

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 الموردين، بالإضافة إلى التأكد من أن الموردين يستوفون معايير الأمان التي تضعونها وجاهزون لتنفيذ تدابير الاستجابة للحوادث لمعالجة التهديدات الخارجية.

توقع الانتهاكات ورصدها والاستجابة لها. حتى لو لم تواجه مؤسستك اختراقاً علنيًا، فمن المهم أن تكون استباقياً 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 .

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).

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.

3. الأمن السيبراني كضرورة استراتيجية. تترك 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.

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.

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.

هذه الوثيقة سرية، وقمنا بإعدادها حصرياً لإطلاعكم أنتم والمستفيدين الآخرين على المعلومات والمشورة الواردة في خطاب التكليف. لذلك، لا يجوز لكم الإشارة إلى اسم ديلويت وهذه الوثيقة أو استخدامهما لأي غرض آخر. كما لا يجوز لكم الإفصاح عنهما أو الإشارة إليهما في أي نشرة أو وثيقة أخرى، ولا توفيرهما أو إرسالهما إلى أي طرف آخر. وفي جميع الظروف، لا يحق لأي طرف آخر الاستناد على وثيقتنا هذه لأي غرض مهما كان؛ وبالتالي، فإننا لا نتحمل أي مسؤولية تجاه أي طرف آخر تم عرض هذه الوثيقة عليه أو اطلع عليها.

إن ديلويت أند توش (الشرق الأوسط) هي شراكة فرعية مرخصة من الباطن تابعة لشركة ديلويت شمال جنوب أوروبا ذات المسؤولية المحدودة وليست مملوكة قانونياً لشركة ديلويت توش توهاماتسو المحدودة. إن شركة ديلويت شمال جنوب أوروبا ذات المسؤولية المحدودة هي شركة عضو مرخصة في مجموعة ديلويت توش توهاماتسو المحدودة.

يشير اسم ديلويت إلى واحدة أو أكثر من الشركات الأعضاء في مجموعة ديلويت توش توهاماتسو المحدودة، على الشركات الأعضاء في شبكتها العالمية، والجهات التابعة إليها. إن شركة ديلويت توش توهاماتسو المحدودة (ويُشار إليها أيضاً باسم “ديلويت غلوبال”) وكل واحدة ومن الشركات الأعضاء فيها هي كيانات منفصلة ومستقلة قانونياً. إن شركة ديلويت توش توهاماتسو المحدودة، وديلويت شمال جنوب أوروبا، وديلويت الشرق الأوسط لا تقدم الخدمات إلى العملاء. لمزيد من المعلومات، يُرجى زيارة موقعنا: www.deloitte.com/about

إن ديلويت شركة عالمية رائدة تقدم خدمات التدقيق والمراجعة، والاستشارات الضريبية والقانونية، والخدمات المتصلة بها. تنتشر الشركات الأعضاء في شبكتنا في أكثر من 150 دولة ومنطقة جغرافية، وتقدم خدماتها إلى أربع من بين خمس شركات مدرجة على قائمة مجلس فورتشن لأفضل 500 شركة. للتعرف على قدرة موظفي ديلويت البالغ عددهم 457,000 موظف تقريباً على إحداث الأثر الذي يصنع فرقاً، يُرجى زيارة موقعنا: www.deloitte.com

تُعتبر ديلويت الشرق الأوسط شركة رائدة للخدمات المهنية، وقد تأسست في منطقة الشرق الأوسط في عام 1926، ولا تزال تقدم خدماتها دون انقطاع منذ ذلك التاريخ. وقد رسخت ديلويت حضورها في منطقة الشرق الأوسط من خلال كياناتها المستقلة قانونياً التابعة لها والتي يحمل كل منها الترخيص للعمل وتقديم خدماتها بموجب القوانين واللوائح السارية في الدولة التي تعمل فيها. إن الشركات التابعة والكيانات المتصلة بديلويت الشرق الأوسط لا تستطيع أن تمارس نفوذاً على بعضها البعض و/أو على شركة ديلويت الشرق الأوسط. وعند تقديم الخدمات، فإن كل شركة تابعة وكيان متصل يتعامل مباشرة وبصورة مستقلة مع العملاء الخاصين به، وبالتالي يتحمل المسؤولية وحده عن أفعاله وأخطائه، وليس عن أفعال وأخطاء تلك الشركات التابعة والكيانات المتصلة.

تقدم ديلويت الشرق الأوسط خدماتها عبر 23 مكتباً منتشرة في 15 دولة، ويعمل فيها أكثر من 7,000 شريك، ومدير، وموظف. كما فازت بالعديد من الجوائز خلال السنوات الخمس الماضية مثل جائزة أفضل مكان للعمل لعام 2022 و 2023 على التوالي في دولة الإمارات العربية المتحدة، وجائزة أفضل مكان للعمل لعام 2023 في المملكة العربية السعودية، وكذلك جائزة شركة العام في مجال الخدمات الضريبية في منطقة الشرق الأوسط.