

## نشرة إخبارية

للمراجعة: السيدة نادين الحسن  
المسؤولة عن العلاقات العامة في ديلويت الشرق الأوسط  
هاتف: +961-1-748 444  
[nelhassan@deloitte.com](mailto:nelhassan@deloitte.com)

### ديلويت تشير إلى ارتفاع معدل التهديدات السيبرانية بسبب التحول الرقمي

- 72% من المشاركين أشاروا إلى تعرّض مؤسساتهم إلى 1 - 10 حادثة ومخالفة سيبرانية في السنة الماضية لوحدها.
- بالرغم من هذه المخاطر، الغالبية العظمى من الرؤساء الماليين المشاركين أعربوا عن عزمهم على مواصلة الانتقال بالأنظمة المالية أو برامج (ERP) في مؤسساتهم إلى السحابة.
- 75% تقريباً من المؤسسات التي تزيد إيراداتها عن 30 مليار دولار سوف تنفق أكثر من 100 مليون دولار على الأمن السيبراني هذه السنة.

**24 نوفمبر 2021** - أجرت ديلويت مؤخراً استبياناً عالمياً حول **"مستقبل الأمن السيبراني لعام 2021"** شمل حوالي 600 من المدراء التنفيذيين لمؤسسات عالمية ممن لديهم معرفة بطبيعة عمل إدارات أو أقسام الأمن السيبراني في مؤسساتهم بحكم إدارتهم لهذه الأقسام. يهدف هذا الاستبيان إلى استخلاص المزيد من المعلومات ونشرها حول إدخال الخدمات السيبرانية في صلب عمل كل مؤسسة، واستخلاص الرؤى والأفكار لتعريف مختلف أنواع المؤسسات على منظومات التقنيات المعقدة، وكيفية تطبيق أفضل الممارسات استعداداً لمواجهة التبعات التي لا يمكن التنبؤ بها للمستقبل السيبراني.

بعد تحليل إجابات المشاركين في الاستبيان، وجدت ديلويت أن 69% من المؤسسات العالمية قد تعرّضت إلى زيادة ملحوظة في الهجمات السيبرانية هذه السنة وفق ما ذكره المدراء التنفيذيون فيها. وتعرّض ديلويت هذه الزيادة إلى الوتيرة المتسارعة في التحول الرقمي الذي شهدته هذه المؤسسات. وبالرغم من ارتفاع هذه المخاطر السيبرانية، يخطط قادة المؤسسات إلى مواصلة استثمارهم بكثافة في التحول الرقمي، حيث أفاد 94% من المدراء الماليين المشاركين في الاستبيان أنهم يخططون للانتقال بالأنظمة المالية أو برامج (ERP) في شركاتهم إلى السحابة. وخلص التقرير إلى أنه لا يوجد حلّ بسيط للحيلولة دون وقوع الهجمات السيبرانية، غير أنه يتوفر عدد من الإجراءات التي يمكن لها مجتمعة مساعدة الشركات على إدخال خدمات الأمن السيبراني في كل جانب من جوانب العمل لديها.

تعليقاً على نتائج هذا الاستبيان العالمي، قال طارق أجمل، الشريك المسؤول عن الخدمات السيبرانية في ديلويت الشرق الأوسط: "خلال السنة الماضية، عملت الشركات، سواء في الشرق الأوسط أو دول العالم، ليلاً نهاراً للإبقاء على قدرتها التنافسية وسط التغيرات التكنولوجية السريعة بعد أن أدى التحول الرقمي بوتيرة متسارعة في هذه الشركات إلى زيادة خطيرة في الثغرات فيها وبالتالي إمكانية تعرّضها للهجمات السيبرانية. ومع استمرار الزيادة في التعقيدات الناجمة عن ربط وتكامل مختلف الأنظمة الإلكترونية، يتعين على رؤساء هذه المؤسسات أن يضعوا في سلم أولوياتهم ضرورة إدخال الأمن السيبراني في جميع مجالات أعمالهم، وإلا سوف تتعرّض شركاتهم للمخاطر الناجمة عن عدم توفير مستوى كافٍ من الحماية السيبرانية."

### زيادة الحاجة للاستراتيجيات السيبرانية بسبب الزيادة في التحول الرقمي

أظهرت نتائج الاستبيان أن أكثر من نصف الشركات المشاركة قد شهدت زيادة في معدل التهديدات السيبرانية خلال العام 2020؛ وقد تفاقمت هذه المخاطر وبلغت معدلات مرتفعة غير مسبوقة من قبل بعد أن أصبح الانتقال إلى نموذج العمل عن بُعد وساعات العمل المختلطة (عن بُعد وفي المكاتب) أمراً أكثر شيوعاً بين الشركات في مختلف دول العالم. ونتيجة لهذه التهديدات، لا تزال الشركات تواجه تحديات في تحقيق التوازن بين استثماراتها في التحول الرقمي للإبقاء على قدرتها التنافسية وبين حماية أنظمتها الإلكترونية من حوادث اختراقها المحتملة. وهذا ما دفع 41% من مدراء تقنية المعلومات ومدراء أمن المعلومات ممن شملها الاستبيان إلى الإقرار بأن أخطر التحديات التي تواجه شركاتهم تتمثل في التحول الرقمي واكتساب المعرفة حول المنظومات التكنولوجية الهجينة (المختلطة) التي تزداد تعقيداً يوماً بعد يوم.

## موجة انعدام الثقة

بخصوص بناء التكنولوجيا مستقبلاً وحماية الشركات، ترى ديلويت، على ضوء نتائج الاستبيان، أن الجوانب التي تضع أخطر التحديات في وجه مدراء تقنية المعلومات ومدراء أمن المعلومات في سعيهم للتعامل مع المخاطر السيبرانية تتمثل في أمرين هما: التحوّل الرقمي/تكنولوجيا المعلومات الهجينة (41%) والصحة السيبرانية (26%). وبناءً على ذلك، يتعين على الشركات الاستفادة من مبدأ "الثقة صفر"، وهو عبارة عن مجموعة من الإرشادات البنوية القائمة على المبدأ الأساسي التالي: "لا تثق أبداً، دائماً تحقق" – وذلك بهدف ردم الفجوة بين الشركة، وتكنولوجيا المعلومات والنطاقات السيبرانية مما يساهم في تقليص التعقيدات التشغيلية وتبسيط تكامل واندماج المنظومات الإلكترونية. ورأى تقرير ديلويت أن الشركات التي تطبق مبدأ "الثقة صفر" هي في طليعة الشركات الأخرى في مجال التغيير التنظيمي / المؤسسي الرامي إلى تحقيق التحوّل الرقمي بشكل أفضل من خلال بناء البنى التحتية للأمن السيبراني من أجل التعامل مع سرعة هذه التحوّلات الرقمية.

## الاستثمار في الأمن السيبراني يعني الاستثمار في مدراء أمن المعلومات

مع زيادة معرفة وتمرّس القراصنة الإلكترونيين، تميل الشركات أكثر من ذي قبل إلى زيادة ميزانياتها المخصصة للحماية السيبرانية. هذا ما أكدته نتائج الاستبيان حيث أفاد 75% تقريباً من المدراء التنفيذيين للشركات، التي تزيد إيراداتها عن 30 مليار دولار، أن شركاتهم تنوي إنفاق أكثر من 100 مليون دولار هذه السنة على الحماية التي يوفرها الأمن السيبراني. ورغم نية هذه الشركات توزيع هذه الاستثمارات بشكل متساو نسبياً بين جميع جوانب العمل فيها لتوسيع دائرة التخفيف من حدة المخاطر السيبرانية، أشارت إجابات المشاركين إلى أن شركاتهم سوف تولي مزيداً من الاهتمام إلى جوانب محددة أكثر من غيرها مثل المعلومات الاستباقية حول التهديدات السيبرانية، كشف ومراقبة الهجمات السيبرانية، التحوّل الرقمي، وأمن البيانات.

خلال السنوات الثلاث القادمة، سيواصل مدراء تكنولوجيا المعلومات ومدراء أمن المعلومات إعطاء الأولوية للأمن السيبراني؛ فقد أفاد المشاركون أنهم سيواصلون جهودهم لتبني التقنيات الناشئة في شركاتهم وذلك تحت تأثير مجموعة من الدوافع تأتي في مقدمتها على التوالي: قدرات الأمن السيبراني (64%)؛ تعزيز قدرات الخصوصية (59%)؛ إظهار قدرات الامتثال للقوانين واللوائح السيبرانية (50%)؛ وتحسين كفاءة العمل والمعلومات الاستباقية (45%).

أضاف أجمل قائلاً: "بالرغم من هذه التحديات المستقبلية، من المؤكد أن أنظمة الأمن السيبراني الأساسية والهجينة تشكل عاملاً أساسياً لحماية الشركات العاملة في الشرق الأوسط وفي مختلف دول العالم من الهجمات المحتملة باستخدام برمجيات الفدية التي تزداد بوتيرة متسارعة. لذلك، فإن الشركات التي تعمل حالياً على إجراء تغييرات تنظيمية استراتيجية، وثقافية وتشغيلية سوف تنجح في إدخال الأمن السيبراني في أعمالها الجوهرية، وهذا ما يساعدها بشكل مطلق على بناء مستقبل يتسم بالمرونة والصمود في مواجهة هذه التهديدات المحتملة."

لمزيد من المعلومات، وللاطلاع على النتائج الكاملة لاستبيان مستقبل الأمن السيبراني لعام 2021 الذي أجرته ديلويت، يُرجى زيارة الرابط التالي: [www.deloitte.com/futureofcyber](http://www.deloitte.com/futureofcyber).

## منهجية الاستبيان

جرى تنفيذ استبيان مستقبل الأمن السيبراني لعام 2021 بالتعاون بين ديلويت وشركة ويكيلد للأبحاث، وشمل حوالي 600 من المدراء التنفيذيين تم استطلاع آرائهم حول الأمن السيبراني، واقتصرت المشاركة في الاستبيان على الشركات التي لا تقل إيراداتها السنوية عن 500 مليون دولار. وقد توزع هذا العدد على النحو التالي: حوالي 200 من مدراء أمن المعلومات، 100 من مدراء تكنولوجيا المعلومات، 100 من الرؤساء التنفيذيين، 100 من المدراء الماليين، و 100 من مدراء التسويق.

- انتهى -

deloitte.com/about للحصول على وصف مفصل للهيكل القانوني لديلويت توش توهاماتسو المحدودة والشركات الأعضاء فيها. إن المعلومات الواردة في هذا البيان الصحفي صحيحة إلى حين التوجه إلى الصحافة النشر.

عن ديلويت آند توش (الشرق الأوسط) شركة ذات مسؤولية محدودة:

ديلويت آند توش (الشرق الأوسط) شركة ذات مسؤولية محدودة (د إم إي) هي شركة تابعة لديلويت شمال جنوب أوروبا شركة ذات مسؤولية محدودة (ن س إي) بالنسبة لمنطقة الشرق الأوسط وقبرص. وديلويت ن س إي هي شركة مرخص لها من قبل ديلويت توش توهاماتسو المحدودة، وهي شركة بريطانية خاصة محدودة بضمناً.

د إم إي هي واحدة من الشركات الرائدة في تقديم الخدمات المهنية الإستشارية وقد تأسست في منطقة الشرق الأوسط ويمتد وجودها منذ سنة ١٩٢٦ في المنطقة من خلال 26 مكتباً في 14 بلداً وتضم قرابة ٥,٠٠٠ شريك ومدبر وموظف. إن وجود شركة د إم إي في منطقة الشرق الأوسط وقبرص مكرّس من خلال الشركات الحائزة على ترخيص لتقديم الخدمات وفقاً للقوانين والمراسيم المرعية الإجراء في البلد التابعة له وتمتع بالشخصية القانونية المستقلة. لا تستطيع الشركات والكيانات المرخصة من قبلها إلزام بعضها البعض و/أو إلزام شركة د إم إي. وعند تقديم الخدمات، تتعاقد كل شركة أو كيان بشكل مستقل مع العملاء الخاصين بهم وتكون هذه الشركات والكيانات مسؤولة فقط عن أفعالها أو تقصيرها.

عن ديلويت

يُستخدَم اسم "ديلويت" للدلالة على واحدة أو أكثر من الشركات الأعضاء المرخص لها من قبل ديلويت توش توهاماتسو المحدودة، وهي مجموعة عالمية من شركات الأعضاء المرخص لها، والكيانات المرتبطة بها. تتمتع الأخيرة وكل من الشركات المرخص لها بشخصية قانونية مستقلة خاصة بها. ولا تستطيع الشركات والكيانات المرخصة من قبلها إلزام بعضها البعض. وعند تقديم الخدمات، تتعاقد كل شركة أو كيان بشكل مستقل مع العملاء الخاصين بها، وتكون هذه الشركات والكيانات مسؤولة فقط عن أفعالها أو تقصيرها. لا تقدم ديلويت توش توهاماتسو المحدودة أو ديلويت ن س إي أو د إم إي أي خدمات للعملاء. يُرجى مراجعة موقعنا الإلكتروني على العنوان التالي:

[www.deloitte.com/about](http://www.deloitte.com/about)

تعتبر ديلويت شركة عالمية رائدة في مجال التدقيق والمراجعة، والإستشارات الإدارية والمالية، وخدمات إستشارات المخاطر، خدمات الضرائب والخدمات المتعلقة بها. وهي توفر خدماتها لأربع من بين خمس شركات على قائمة مجلة فورتشن العالمية لأفضل ٥٠٠ شركة، بفضل شبكة عالمية مترابطة من شركات الأعضاء المرخص لها في أكثر من ١٥٠ دولة. للحصول على المزيد من التفاصيل حول مهنتي ديلويت ال ٣٠٠٠٠٠ وأثرهم الإيجابي في مختلف القطاعات، يُرجى مراجعة موقعنا الإلكتروني على العنوان التالي: [www.deloitte.com](http://www.deloitte.com).

المعلومات الواردة في هذا البيان الصحفي صحيحة في وقت إرسالها للصحافة.

للتوقف عن تلقي الرسائل الإلكترونية، يرجى إرسال رسالة رد إلى المرسل تحمل عبارة "Unsubscribe" في خانة الموضوع.

### Nadine El Hassan

Senior Manager | Brand & Communications

Deloitte & Touche (M.E.)

Gefinor Center - Block D

Clemenceau Street

Beirut, P.O. Box 113 - 5144

Lebanon

D: +9611748444

[nelhassan@deloitte.com](mailto:nelhassan@deloitte.com) | [www.deloitte.com](http://www.deloitte.com)

