protiviti®
Face the Future with Confidence

KFAS
مؤسسة الكويت للتقدم العلمي
Kuwait Foundation for the Advancement of Sciences

رفع مستوى الأمن السيبراني

القطاع الخاص الكويتي

مستقبل نرعاه بالمعرفة

جدول المحتويات

مُقدمة

في الوقت الذي تتبنى فيه المؤسسات منصات تقنية جديدة لتحسين الإنتاجية، والتواصل مع العملاء، والتميز في السوق، والنمو المستقبلي، إلا أنها تواجه العديد من التهديدات المتعلقة بالأمن السيبراني. وهي ستُدرك قريباً جداً أهمية ذلك الأمن باعتباره أولوية قصوى لها، لأن تأثير حوادث الأمن السيبراني بعيد كل البعد عن تلك المتعلقة بالجانب التجاري والسمعة.

ومما يبعث على القلق هو اتسام مصادر التهديد بأنها فعالة جداً في هذا المجال، وفي الوقت نفسه يزداد مستوى التهديد بصورة مطردة. وإلى جانب التغيرات في بيئة الأعمال، تظهر مخاطر جديدة للمؤسسات بوتيرة متسارعة.

وفي هذا التقرير، ندرس المخاطر التي تواجه مؤسسات القطاع الخاص في دولة الكويت، ودور الجهات الرقابية، والاتجاهات العالمية في الأمن السيبراني وما يجب على المؤسسات فعله للتعامل مع هذه التحديات.

هذا التقرير هو دراسة تعاونية أجرتها مؤسسة الكويت للتقدم العلمي (KFAS)، ومركز التميز في الإدارة بجامعة الكويت (CEM)، وشركة بروتيفتي ممبر فيرم الكويت ذ.م.م (بروتيفتي).

وتقدم هذه الدراسة نظرة ثاقبة حول تأثير جائحة كورونا (كوفيد-19) على الثغرات الأمنية الناشئة عن التحول نحو أنماط العمل عن بعد من قبل الموظفين وزيادة الاعتماد على الإنترنت لممارسة الأعمال في الكويت ومنطقة الشرق الأوسط.

أعد هذا التقرير بتكليف من مؤسسة الكويت للتقدم العلمي لكلا من مركز التميز في الإدارة بجامعة الكويت (CEM)، وشركة بروتيفتي ممبر فيرم الكويت ذ.م.م (بروتيفتي) بهدف تقديم نظرة ثاقبة حول الأمن السيبراني ومدى تأثير جائحة كورونا (كوفيد-19) على مؤسسات القطاع الخاص في الكويت. وكجزء من البحث، تواصلنا مع مجموعة مختارة من المؤسسات الخاصة وأجرينا مناقشات متعمقة بالإضافة إلى تجميع الإجابات الموجودة في استبانات وزعت عبر الإنترنت من اثنين وثلاثين مشاركاً من مختلف القطاعات، بما في ذلك قطاع الخدمات المالية، والخدمات المصرفية، والرعاية الصحية، والتكنولوجيا.

الموضوعات الرئيسية في هذه الدراسة

تستعرض الدراسة ملاحظات أولية حول المقاييس الرئيسية، والتي تزودنا برؤى مهمة حول الاتجاهات الأمنية في الكويت.

اتجاهات الأمن في دولة الكويت

دور الجهات الرقابية

نماذج الأعمال المتغيرة والتي تؤثر بدورها على الأمن

- التحول الرقمي
- تبني تقنيات الحوسبة السحابية

المخاطر الرئيسية التي تمت مواجهتها

مجالات الأمن الهامة

- خصوصية وأمن البيانات
- أمن التطبيقات
- الهوية والوصول
- أمن تقنيات الحوسبة السحابية
- الاستراتيجية والهيكل
- اعتماد هيكل الثقة الصفرية

المُلخص التنفيذي

يعد دور الجهات الرقابية عاملاً حاسمًا ومحركًا أساسيًا لتعزيز الوضع الأمني للمؤسسات من خلال التزامها الدوري. وقد أصدرت الجهات الرقابية على مستوى منطقة الخليج والعالم العديد من أطر العمل الأمنية وقوانين خصوصية البيانات لتحقيق هذا الهدف.

تُظهر الدراسة أنه خلال عام 2020، مع بداية تفشي الجائحة، مرت مؤسسات القطاع الخاص في الكويت بتغييرات جذرية في أساليب عملها، ومن ثم أطلقت مبادرات كبيرة لإعادة هيكلة تكاليفها، فيما بدت وكأنها مؤسسات أصغر حجمًا. علاوة على ذلك، زادت ميزانيات الوظائف الأمنية لـــ 57٪ من المؤسسات، مما يؤكد حقيقة مفادها أن القيادة العليا ملتزمة بالأمن السيبراني. فلقد أدركت المؤسسات قيمة الحوسبة السحابية كعامل مساعد لها لتصبح أكثر مرونة وتكيفاً، فضلاً عن دعم القوى العاملة المنتشرة على نطاق واسع، وضمان مستوى نسبي من الأمن مثل البيئة المحيطة.

ومن ثم، تم تصنيف عملية تطوير رحلة آمنة إلى الخدمات السحابية كأولوية إستراتيجية قصوى في عام 2021، حيث تخطط 44٪ من المؤسسات للاستثمار وتطوير مبادرات الأمن السحابية الخاصة بها، في حين تعد بيئة الخدمات السحابية العامة الآن هي الخيار المفضل لاستضافة خدماتهم وتطبيقاتهم وبنيتهم التحتية.

لقد أدت الجائحة إلى تسريع وتيرة التحول الرقمي وتبني تقنيات جديدة لبناء مؤسسات أكثر مرونة وتكيف مع الأوضاع. وأصبح العمل مع القوى العاملة الموزعة، والاستفادة من البنية التحتية السحابية ضرورة ملحة، وقد أكدت الزيادة الهائلة في الهجمات على الحاجة إلى المبادرات الأمنية التي يجب على المؤسسات الشروع فيها.

عادة ما كانت المؤسسات آمنة – إلى حد ما – من خلال تنفيذ أمن الشبكات وأجهزة المستخدم النهائي لمنع الهجمات. ومع ذلك، فإنه في ضوء عالم اليوم شديد الاتصال، تدرك المؤسسات أنها لا تستطيع صد الهجمات بنسبة 100٪، حيث سيتم استهدافها وتعريضها للأخطار. ومن ثم فإنه بعد الاختراق، تكون الأولوية القصوى هي الاستجابة بفعالية واستعادة العمليات العادية في أقل وقت ممكن وبأدنى تأثير. يتعين أن تتوافق استراتيجيات الأمن مع نماذج الأعمال المعاد تصميمها. وعلى الصعيد العالمي، تتبع المؤسسات معايير المعهد الوطني للمعايير والتكنولوجيا، والتي تساعد على قياس مستوى النضج مقابل خمس خطوات وهي التحديد والحماية والاكتشاف والاستجابة والاسترداد. وتسهم نماذج الأعمال المعاد تصميمها في دفع عملية تنفيذ التقنيات الحديثة، ومن ثم استحداث مخاطر وثغرات أمنية جديدة. تتبنى الشركات هياكل أمنية جديدة مثل الثقة الصفرية، نظرًا لأن الهياكل القديمة غير قادرة على تلبية احتياجات أنظمة تكنولوجيا المعلومات والأعمال الحالية.

أبرز نتائج الاستبانات لمؤسسات القطاع الخاص في الكويت

57٪ يتوقعون زيادة في ميزانية الأمن

48٪ نفذوا معيار الأيزو رقم 27001 مقابل أساس مرجعي عالمي يبلغ 84٪

44٪ من المؤسسات تخطط للاستثمار وتطوير مبادرات الأمن السحابي الخاصة بها

تم تصنيف مستوى نضج أمن البيانات بواقع 2.1 عند مقارنته بالأساس المرجعي العالمي البالغ 3.68

تم تحديد عملية تأمين الهوية والوصول كأولوية استراتيجية قصوى للأمن

64٪ خططوا للاستثمار في مبادرات أمن التطبيقات

يتضح التخطيط الدقيق للاستراتيجية الأمنية من قبل مؤسسات القطاع الخاص في الكويت من تحديدها للتقنيات الرئيسية للاستثمار على مدى العامين القادمين لتعزيز الوضع الأمني لوظائف أعمالها. وأدى تنفيذ هذه المؤسسات لمشاريع التحول الرقمي إلى تطوير الكثير من تطبيقات المستخدم النهائي والتطبيقات الداخلية. ومن ثم، فإن اهتمام 64٪ من المؤسسات ينصب على مبادرات أمن التطبيقات. تعمل مشاريع التحول هذه على تسخير أحدث التقنيات للمساعدة على تبادل البيانات بسرعات فائقة، مما يجعل أمن وخصوصية البيانات محل اهتمام 60٪ من المؤسسات. ويتمثل المجال الثالث للاستثمار في العامين المقبلين لـــ 36٪ من المؤسسات في تأمين دورة حياة هوية المستخدمين النهائيين والمستخدمين المتميزين على حدٍ سواء من خلال تطبيق هذه التقنيات.

يتضح جلياً أن الأمن أصبح الآن وظيفة راسخة، حيث أكد 57٪ من المشاركين في الاستطلاع على مشاركة الأمن في تخطيط وبدء وتقييم التطورات الجديدة. ومع ذلك، لا يزال هناك الكثير مما يتعين إجراؤه في مجال وضع الضوابط الأمنية لتكون جاهزة للمستقبل. ولعلنا لا نعدو الحقيقة إذ قلنا بأن الفجوة بين مؤسسات القطاع الخاص في الكويت واسعة عند مقارنتها بمثيلاتها في دول الخليج أو على الصعيد العالمي، لا سيما في مجالات الأمن الأحدث مثل البيانات والهوية والتطبيقات والتحليلات الأمنية والحوكمة والمخاطر والالتزام فضلا عن أمن الشبكة، ويجب أن تكون ذات أولوية لتقليص الفجوة قدر الإمكان.

الكويت: التحول الرقمي وتبني تقنيات الحوسبة السحابية

بالنظر إلى جائحة كورونا (كوفيد-19) ومجموعة التدابير الوقائية والحجر الصحي المنزلي، على مستوى المنطقة، نجد أن التوقعات تستند بشكل أكبر إلى الابتكار والتكنولوجيا من أجل الاستمرارية، والاستفادة القصوى من هذه الإجراءات لتحقيق الفعالية والكفاءة والربحية.

أسفرت المخاوف الصحية الناجمة عن تفشي جائحة كورونا (كوفيد-19) على الصعيد العالمي إلى تحول مفاجئ ليس فقط تجاه العمل عن بعد، ولكن أيضًا في تلبية احتياجاتهم اليومية. وقد يكون للاستخدام الهائل للمنصات الرقمية والطلب على الخدمات الرقمية تأثير كبير على اقتصادات منطقة الخليج على المدى الطويل. وامتثالاً لإجراءات السلامة ومتطلبات الحجر الصحي، كان على معظم السكان العودة إلى المنصات المتاحة في التعليم والطب والتجارة الإلكترونية وغيرها.

سرعان ما أصبحت أهمية التحول الرقمي وإنترنت الأشياء (IoT) في مكان العمل وعبر القطاعات ضرورة ملحة في المنطقة. إلا أنه من أجل فاعلية سبل التمكين، يتعين معالجة عناصر محددة من النظام البيئي الرقمي من قبل الجهات الرقابية القطرية والحكومات على المستوى الإقليمي. هناك العديد من الأبعاد لتيسير عملية التحول الرقمي، وهذه العملية لا تعتمد فقط على المؤسسات نفسها، حيث يؤدي الإطار الرقابي والبنية التحتية دورًا محورياً، مع ضرورة تواجدهم لتحقيق تحول داخلي ناجح.

وعلى الرغم من أنه على مدى السنوات القليلة الماضية كان هناك تركيز قوي من قبل دول مجلس التعاون الخليجي على بناء تكنولوجيا المعلومات والبنية التحتية للاتصالات، مدعومة بتعزيز الإطار الرقابي لتسريع وتيرة طرح البرامج الرقمية.

إلا أن هناك المزيد مما يتعين القيام به لدعم الاحتياجات الديناميكية للتحول الرقمي، والتقنيات السحابية، وأمن البيانات، والخصوصية، إلى جانب إدارة هويات القوى العاملة الموزعة.

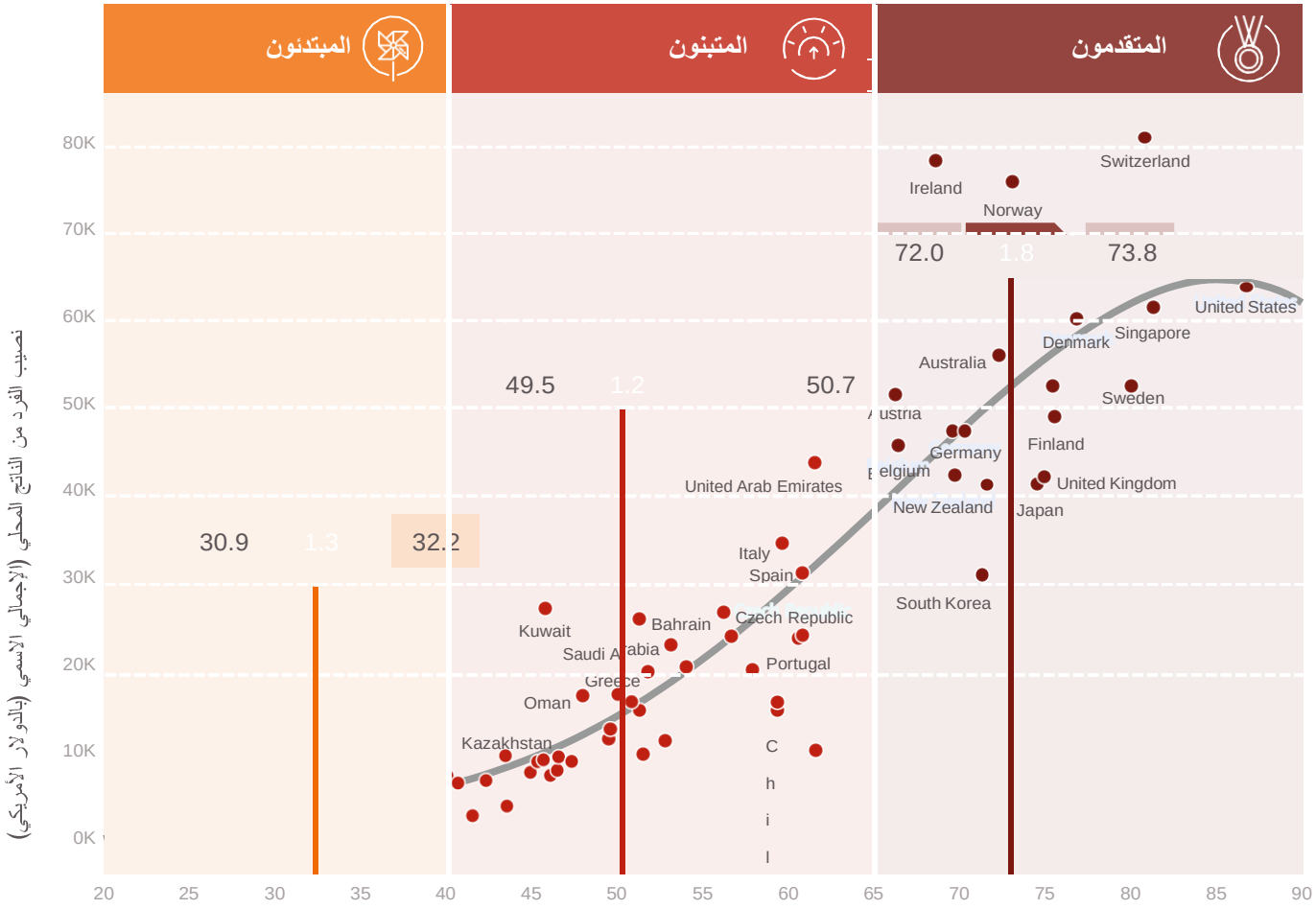
تُعد الكويت من بين أكثر الدول استهدافًا للهجمات السيبرانية في منطقة الخليج[1]، ومن ثم تحتاج إلى التصدي لهذه التهديدات التي تتعرض لها بنيتها التحتية الإلكترونية. ففي سنة 2017 وحدها، خسرت الكويت نحو 1.4 مليار دولار أمريكي بسبب الجرائم السيبرانية، بزيادة قدرها 4.9٪ عن العام السابق[2]. وقد اتخذت الجهات الرقابية مجموعة من الخطوات لتعزيز البنية التحتية للأمن السيبراني في الدولة من خلال إطلاق الاستراتيجية الوطنية للأمن السيبراني.

ويمكن اتخاذ مزيد من الخطوات في هذا الاتجاه من خلال إنشاء فريق الاستجابة للأحداث السبرانية (CERT) على المستوى الوطني وصياغة المناهج الإلكترونية وتفعيلها في الجامعات الكويتية.

تم اتخاذ مجموعة من المبادرات على المستوى الوطني، بما في ذلك تلك الموجودة في الهيئة العامة للاتصالات وتقنية المعلومات، والتي من شأنها تعزيز وضع الأمن السيبراني في الكويت. في 2018، دخل قانون يتنبأ بالعواقب الوخيمة للجرائم الالكترونية حيز التنفيذ في البلاد، والذي قضى أيضًا بالسجن لمدة تصل إلى 10 سنوات[3]. وقد ساهمت هذه الجهود المبذولة في السنوات الأخيرة في رفع ترتيب الكويت على مؤشر الاتصالات العالمي. وفي عام 2020، احتلت الكويت المرتبة 48 على مؤشر الاتصال العالمي (GCI)، وهي تقطع شوطًا طويلاً في فئة المتبنّين، بينما كانت تُعتبر سابقًا في تصنيفات فئة المبتدئين (الشكل 1).

1. https://documents.trendmicro.com/assets/rpt/rpt-a-constant-state-of-flux.pdf
2. https://www.naseba.com/what-we-do/commercial-services/cyber-defence-summit-kuwait-2018/
3. https://www.e.gov.kw/sites/kgoenglish/Forms/CAITLawNo.63of2015oncombatingInformationTechnologyCrimes.pdf

الشكل 1: المنحنى السيني – مؤشر الاتصال العالمي لعام 2020 مقابل الناتج المحلي الإجمالي للفرد



درجة مؤشر الاتصال العالمي لعام 2020

https://ict.moscow/en/research/global-connectivity-index-2020/

إطار العمل الرقابي في دولة الكويت

إن الجدل الدائر حول دور الحكومات في تنظيم المخاطر الإلكترونية لا ينتهي، وذلك رغم وجود وجهات نظر مختلفة حول هذا الموضوع إذ يفضل بعض الأشخاص نهج السوق في حين يدعو البعض الآخر إلى التدخل الحكومي. وبما لا يدع مجالاً للشك، فإن الحكومات أصبحت مطالبة بالتدخل وتمهيد الطريق نظرًا لأن البنية التحتية الحيوية في مختلف الاقتصادات أصبحت أكثر اعتمادًا على الإنترنت.

تتولى الحكومات مسؤولية حماية اقتصادها الوطني، وتأمين السكان من الهجمات السيبرانية وبناء الثقة باستمرار في فاعلية البنية التحتية الحيوية للدولة، وذلك نظراً لأن التهديدات الأمنية تتغير باستمرار وأي نهج لمنع الهجمات الإلكترونية يجب أن يكون على المنوال نفسه.

وتأخذ المؤسسات على عاتقها مسؤولية اتخاذ التدابير اللازمة والقيام بالاستثمارات المناسبة لضمان حماية أصولها وبياناتها بشكل جيد. إنه جهد تعاوني وجماعي يقود إلى السلامة الإلكترونية، ولجميع أصحاب المصلحة دور في ضمان الحماية الكافية وخلق الوعي.

على غرار بعض البلدان الأخرى، لا يوجد لدى الكويت كيان واحد مسؤول عن اللوائح العامة للأمن السيبراني.

الشكل 2: الجهات الرقابية لتكنولوجيا المعلومات بدولة الكويت

بنك الكويت *المركزي*	حل بنك الكويت المركزي محل مجلس النقد الكويتي الذي تأسس بموجب المرسوم الأميري رقم 41 لسنة 1960، ويدير بنك الكويت المركزي جميع اللوائح والتعليمات المتعلقة بالقطاع المالي، بما في ذلك إطار الأمن السيبراني للمؤسسات المالية.
الهيئة العامة للاتصالات وتقنية المعلومات	تأسست الهيئة العامة للاتصالات وتقنية المعلومات في العام 2014 وتتولى مسؤولية الإشراف على قطاع الاتصالات ورقابته وحماية مصالح المستخدمين ومزودي الخدمات وتنظيم خدمات جميع شبكات الاتصالات في الدولة بكفاءة عالية بما يحقق الأداء الأمثل لقطاع الاتصالات ويضمن الشفافية والمساواة والمنافسة الحرة..
الجهاز المركزي لتكنولوجيا المعلومات	يُحدد المرسوم الأميري اختصاصات الجهاز المركزي على النحو التالي: وضع الخطط وسياسات تكنولوجيا المعلومات على المستوى الوطني واعتمادها من مجلس الوزراء، والإشراف على عمليات تنفيذ خطة ومشروعات الحكومة الالكترونية بالتنسيق مع الوزارات والجهات الحكومية، وتنسيق كافة أعمال خطط تطوير تكنولوجيا المعلومات فيما بين الجهات الحكومية.
وزارة الداخلية بدولة الكويت	يوجد لدى وزارة الداخلية كيانان مرتبطان بالأمن السيبراني داخليًا وعلى المستوى الوطني، وهم: إدارة مكافحة الجرائم الإلكترونية، وإدارة الجرائم الإلكترونية التي تحقق في أي انتهاكات وحوادث..

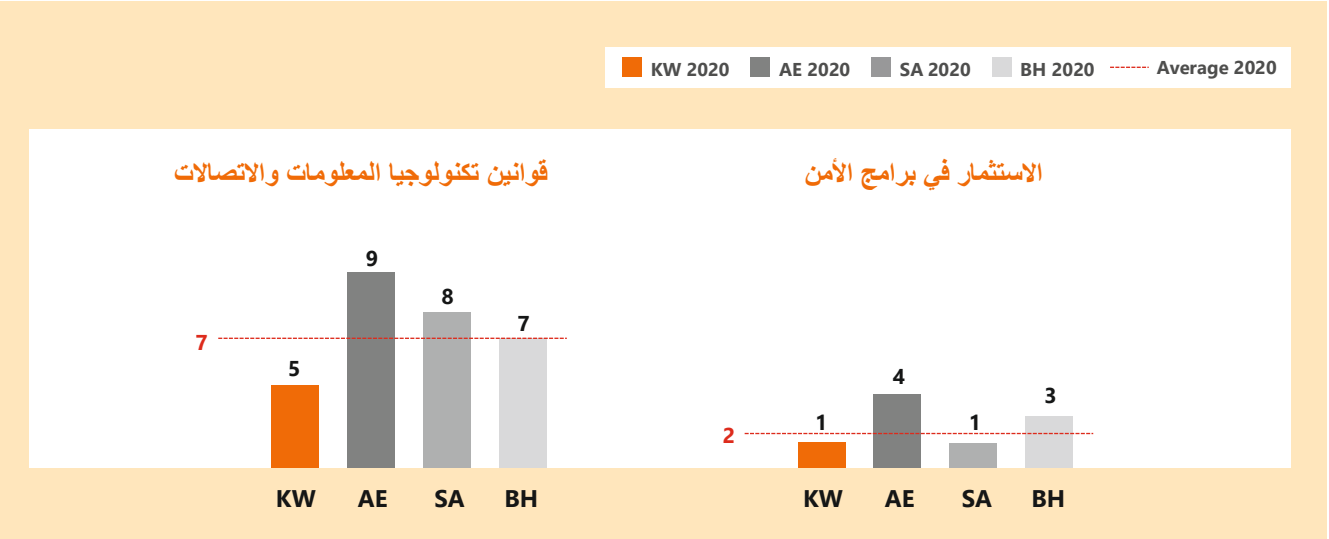
قرر مجلس الوزراء في 30 مايو 2021 الموافقة على توصية اللجنة الوطنية العليا للأمن السيبراني بشأن إنشاء المركز الوطني للأمن السيبراني، وتكليف وزير الدولة لشؤون مجلس الوزراء بالتنسيق مع الجهات المعنية لإعداد مشروع المرسوم اللازم.

المصدر: أخبار عامة

يقوم كل كيان بإدارة وتنظيم الأمن السيبراني للقطاع/المجال المحدد ويصدر توجيهات وإرشادات خاصة به. أصدر بنك الكويت المركزي الإطار الاستراتيجي للأمن السيبراني للقطاع المصرفي في فبراير 2020. ويدير الجهاز المركزي لتكنولوجيا المعلومات الأمور المتعلقة بالجهات الحكومية الكويتية فيما يتعلق بالتكنولوجيا والاتصالات. ووضع ذلك الجهاز الإطار الوطني لحوكمة تكنولوجيا المعلومات الذي ستنفذه من قبل جميع مراكز تكنولوجيا المعلومات في جميع الهيئات والجهات الحكومية في دولة الكويت.

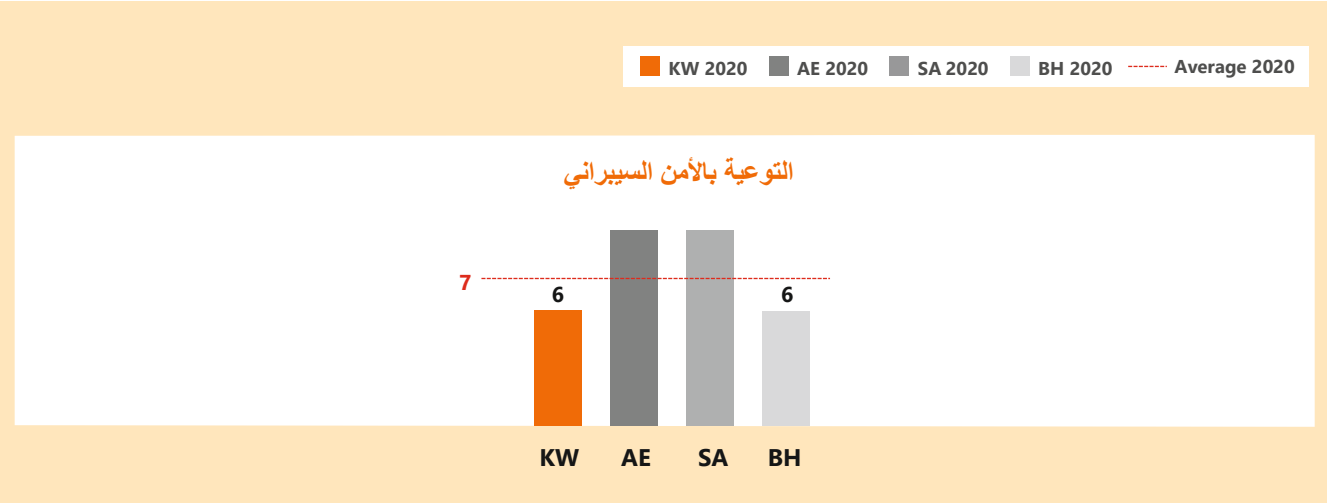
تحتاج الجهات الرقابية المعنية بدولة الكويت إلى تسريع وتيرة وضع السياسات وتطوير البنية التحتية بشكل جماعي في هذا المجال. وكما هو موضح في مؤشر الاتصال العالمي، تحتل الكويت مرتبة أقل بين نظيراتها في دول مجلس التعاون الخليجي. وتركز هذه الدراسة على ثلاثة مؤشرات رئيسية، ترتبط جميعها بالإطار الاستراتيجي الذي أقرته الدولة. فيما يتعلق بقوانين تكنولوجيا المعلومات والاتصالات، تحتل الكويت المرتبة الأدنى (الشكل 3) بين دول مجلس التعاون الخليجي الأخرى، ويتجلى ذلك أيضًا في الاستثمارات التي تتم على مستوى الدولة في برامج الأمن لتعزيز الحماية من الهجمات الإلكترونية كما هو موضح أدناه (الشكل 3).

الشكل 3: مؤشرات الإمداد في مؤشر الاتصال العالمي بالكويت مقارنة بدول مجلس التعاون الخليجي



علاوة على ذلك، يعد الوعي بالأمن السيبراني أيضًا هو الأدنى في الكويت كما هو موضح في الشكل 4، نظرًا لعدم وجود برامج أو لوائح وطنية تفرض الحاجة إلى خلق مثل هذا الوعي على المستوى الوطني. شرع قطاعان في الاقتصاد، وهما النفط والغاز والخدمات المالية، في وضع سياسات وأطر عمل معينة يدير كل قطاع من خلالها الأمن السيبراني، بيد أن ذلك لا ينطبق على القطاعات الأخرى داخل الاقتصاد.

الشكل 4: مؤشرات الخبرة في مؤشر الاتصال العالمي بالكويت مقارنة بدول مجلس التعاون الخليجي



مقارنة بالدول الأخرى في المنطقة، نجد أن لدى الكويت أقل عدد من اللوائح الرقابية فيما يتعلق بتكنولوجيا المعلومات والاتصالات. وكما هو موضح في الشكل 3، تحتاج الكويت إلى إصدار المزيد من اللوائح الرقابية لمعالجة القضايا المتعلقة بالأمن السيبراني. باستثناء الإطار الاستراتيجي للأمن السيبراني للبنوك، لا يوجد في الكويت أي لوائح أخرى، مقارنة بدول مثل الإمارات العربية المتحدة والمملكة العربية السعودية، حيث تم إصدار العديد من اللوائح مع التركيز على الأمن السيبراني والجرائم الإلكترونية.

تتجه الكويت تدريجياً نحو نهج أكثر تنظيماً لإدارة التهديدات والثغرات السيبرانية النابعة من استخدام الإنترنت والتكنولوجيا بشكل عام.

ومن ثم، يتعين بذل المزيد مقارنة بدول الخليج الأخرى. تستدعي الحاجة وجود أطر أمن إضافية حول خصوصية البيانات وتقنيات السحابة لتقديم توجيهات للقطاع الخاص. لا شك أن وجود برنامج قوي لتطوير المعايير الأمنية، وإصدارها، وتحديد قابلية التطبيق، ورصد وقياس أداء المؤسسات بشكل دوري سيساعد في زيادة النضج الأمني.

التأثير العالمي لفايروس كورونا (كوفيد-19) على الأمن السيبراني

كان لجائحة (كوفيد-19) تأثيراً طويل الأمد على المؤسسات، مما أضطرها على التراجع وإعادة التقييم ووضع استراتيجيات لعملياتهم المتعلقة بالابتكار والحلول الرقمية التي تلبي احتياجات القوى العاملة الموزعة وشبكة العملاء.

وأصبح الأمن السيبراني مُحركًا رئيسيًا لجهود التحول الرقمي للمؤسسات نظرًا لما يترتب على ذلك من آثار كبيرة على السمعة والتشغيل والشؤون القانونية والالتزام. ومن المتوقع الآن وجود ضرورة لتطبيق الأمن السيبراني وإدراجه ضمن عمليات الأعمال، باعتباره ذا قيمة قصوى للعملاء، فضلاً عن كونه عنصر حيوي في بناء الثقة.

في عام 2020، أعلن المنتدى الاقتصادي العالمي أن فشل الأمن السيبراني يمثل خطرًا واضحًا وقائمًا على فئة المخاطر قصيرة المدى الخاصة بهم وكان مصدر قلق لـــ 39 ٪ من المشاركين.

بحلول عام 2021، من المرجح أن تكلف الجرائم الإلكترونية العالم 6 تريليونات دولار سنويًا، فيما يعد أكثر من الناتج المحلي الإجمالي للمملكة المتحدة وفرنسا معًا. *

قد يتطلب ضمان إدارة الخصوصية والهوية وأمن المعلومات أو حماية النظام موارد كبيرة.*

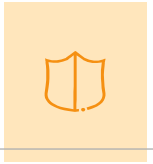
قد يتجاوز معدل التطور السريع للابتكارات التخريبية مدعومة بالتقنيات الحديثة والناشئة (مثل، الذكاء الاصطناعي والروبوتات وتعلم الآلة والمنصات هائلة التدرج "Hyper Scalable Platforms") و/أو قوى السوق الأخرى قدرة المؤسسات على التنافس و/أو إدارة المخاطر على نحو ملائم، دون إجراء تغييرات جوهرية على نموذج الأعمال.*

ربما لا تكون المؤسسات مستعدة بشكل كافٍ لإدارة التهديدات الالكترونية التي تمتلك القدرة على تعطيل العمليات الأساسية بشكل كبير و/أو الإضرار بعلامتها التجارية.*

IDC FutureScape: توقعات 2019 لقطاع تكنولوجيا المعلومات على مستوى العالم

https://www.idc.com/getdoc.jsp?containerId=US44403818

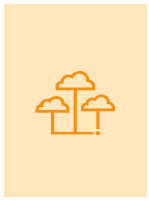
أدى تسريع عمليات التحول الرقمي، وتبني تقنيات السحابة المتعددة، وزيادة الهجمات الإلكترونية، واتساع الفجوة المستمرة بين متخصصي الأمن السيبراني في جميع أنحاء العالم، إلى تحفيز المؤسسات على إعادة التفكير في نماذج الأمن الخاصة بها، بما نتج عنه ظهور الاتجاهات التالية على مستوى العالم:



الدعم الأمني للقوى العاملة الموزعة: نظرًا لعمل الموظفين في جميع أنحاء العالم عن بُعد، فقد أصبح الانتشار الهائل للأدوات المساعدة، والمصادقة متعددة العوامل (MFA)، والشبكة الافتراضية الخاصة (VPN) من أهم أولويات المؤسسات. فلقد تبنوا جيدًا سيناريو العمل من المنزل واستمروا في الاستثمار بشكل أكبر في مجال نضج وتطوير أمن القوى العاملة الموزعة.

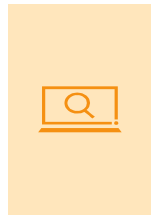
يحتل أمن وخصوصية البيانات مركز الصدارة: بينما تشرع المؤسسات في وضع خارطة طريق الأعمال الرقمية، لم يعد تأمين بيانات العملاء وضمان الخصوصية خيارًا، ولكنه مطلب رقابي صادر عن العديد من البلدان في جميع أنحاء العالم. وشجعت أطر العمل مثل اللائحة العامة لحماية البيانات (GDPR) ومتطلبات درع الخصوصية المرتبطة بها المؤسسات على الاستثمار في مبادرات مثل الخصوصية حسب التصميم.

الهوية ضرورة أساسية: مع عدم وجود حدود اليوم، تحتاج المؤسسات إلى تبني الحد الأدنى من الامتيازات. وإنه لمن الأهمية بمكان إدارة الهويات وأتمتة العمليات المتعلقة بدورة حياة المستخدم، والإشراف على حسابات الامتياز ومراقبتها. يتحقق المستوى المطلوب من الأمن عندما نجمع بين الوصول إلى الهوية والبيانات داخل التطبيقات التي قد تكون في مكان العمل أو على السحابة أو مختلطة.



خارطة طريق السحابة المتعددة: لقد كانت المؤسسات في جميع أنحاء العالم تستفيد بالفعل من التقنيات السحابية، ومع ذلك، فقد دفعت الجائحة تلك المؤسسات إلى تقييم عملية الجمع بين الخدمات السحابية والبنية التحتية من عدة مزودين مما يسمح لهم بالاستفادة من أفضل الميزات من كل مزود خدمة، فهم يعيدون تعريف مراكز البيانات التقليدية إلى مراكز البيانات المحددة بالبرمجيات (SDDC) من خلال استخدام الشبكات المحددة بالبرمجيات (SDN) وزيادة تطبيق برامج الأمن المتقارب على السحابة باستخدام نماذج جديدة مثل حافة خدمات الوصول الآمن (SASE).

تأمين سلسلة الإمداد: تعتمد معظم الشركات اليوم على العديد من الموردين للتكنولوجيا والخدمات وتطوير البرمجيات التي يمكن أن تنتشر على مستوى العالم. وقد أجبرهم الاضطراب الأخير في سلسلة الإمداد على إجراء تقييم لنمذجة سلسلة الإمداد وزيادة الوعي بما يفعله الموردون/مزودو الخدمات للتخفيف من المخاوف الأمنية التي قد تؤدي إلى حدوث اضطرابات في المستقبل. أصبح تقييم أمن البيانات التي يتم جمعها وقدرات المرونة محل اهتمام كبير من جانب المؤسسات.



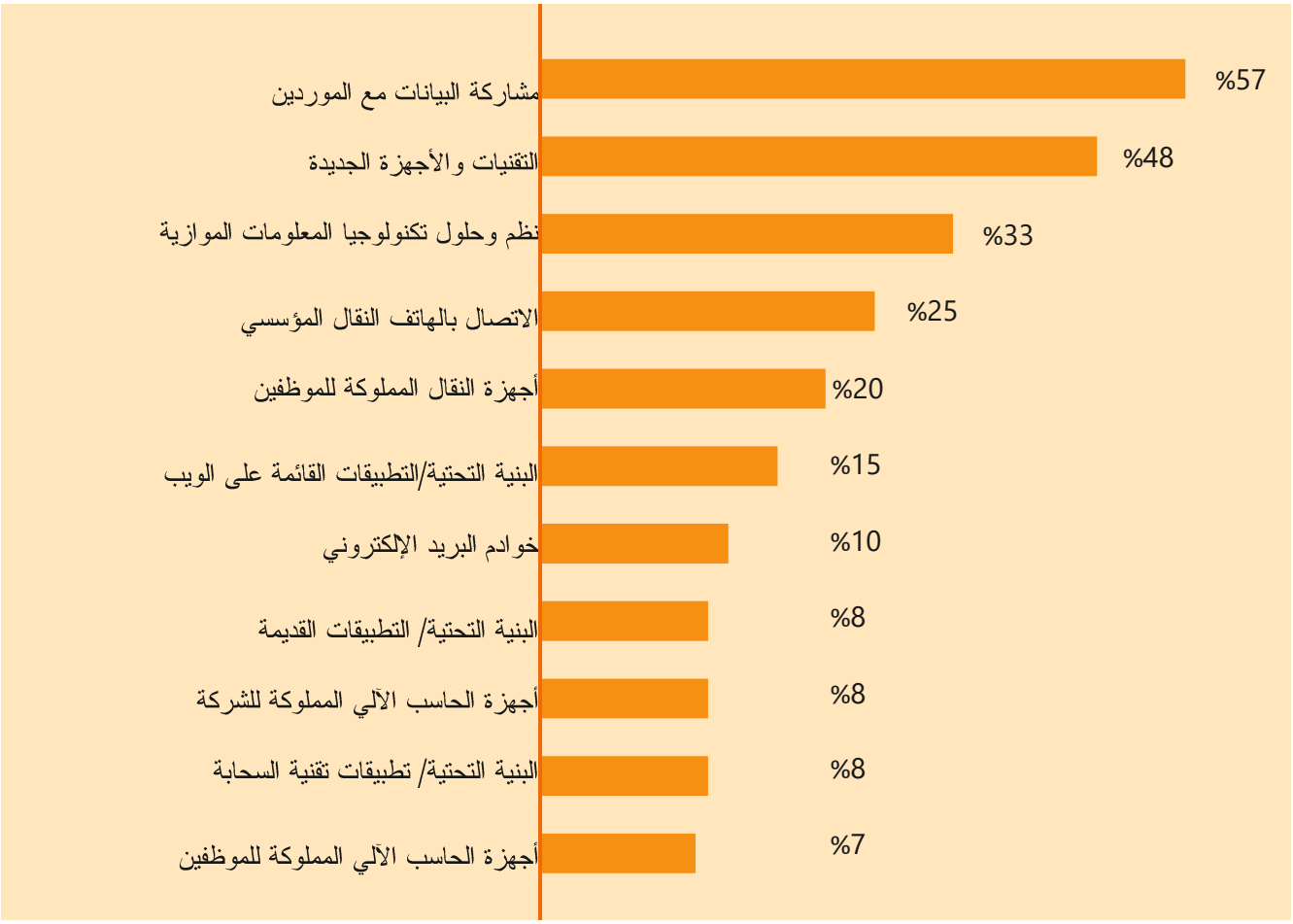
تعزيز قدرات المراقبة والاستجابة الأمنية: اعتمد محللو الأمن بشكل تقليدي وكبير على التنسيق الوثيق أثناء الاستجابة للحوادث لأنه يساعد على تبادل المعلومات وإدارة الحالات الطارئة. مع التغيير الفوري لأماكن عمل القوى العاملة أثناء الجائحة، تم توزيع فرق الأمن أيضًا، مع وجود فرص قوية لفقدان حوادث الخرق الأمني. ونظرًا لاتساع بيئة تشغيل المؤسسات بشكل كبير بعد جائحة كورونا (كوفيد-19)، فإنها تحاول التأكد من أن أدوات المراقبة وإمكانات التحقق من التهديدات المقدمة لفرق الأمن لديها تحقق أقصى قدر من الرؤية.

تبني هيكل الثقة الصفرية (ZTA): زاد الاهتمام، بشكل كبير، بهيكل الثقة الصفرية بنسبة 230٪ في عام 2020 مقارنة بالعام الماضي. بدأت المؤسسات تجربتها لهيكل الثقة الصفرية، مما سيساعد على تنفيذ مبدأ الحد الأدنى للامتياز عبر جميع الشبكات.

4. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

التصنيف حسب الأولوية: تصنيف الثغرات الأمنية

الشكل 4: مؤشرات الخبرة في مؤشر الاتصال العالمي بالكويت مقارنة بدول مجلس التعاون الخليجي



حالة الأمن السيبراني في دولة الكويت

لم يعد نموذج وتدفق العمل الرقمي يُمثل رؤية تتسم بالطموح، وهي أمر ضروري للمؤسسات. ولتحقيق ذلك من خلال التحول الرقمي، تتبنى مؤسسات القطاع الخاص في دولة الكويت بشكل متزايد تقنيات جديدة لإعادة ابتكار نماذج وتدفقات العمل الخاصة بهم. ويتم النظر إلى التقنيات الجديدة مثل السحابة، وإنترنت الأشياء (IoT)، وشبكات الجيل الخامس (G5)، وإيدج (Edge) وما إلى ذلك من منظور جديد لحل مشكلات العمل الجوهرية، مع توفير كمية ضخمة من البيانات. تستثمر مؤسسات القطاع الخاص في هذه التقنيات الحديثة بهدف نهائي يتمثل في تعزيز نماذج أعمالها، وزيادة إيراداتها الأعلى، ومُعدل الأرباح في الأعمال، وحصتها الإجمالية في السوق في دولة الكويت. ومع هذه الزيادة الهائلة في البيانات التي يتم إعدادها وتبادلها، يظل أمن المعلومات نقطة أساسية مطروحة للمناقشة لأعضاء مجلس الإدارة. حيث تقدم جهود التحول الرقمي لهذه المؤسسات أيضًا فرصة لإعادة التفكير في إستراتيجية الأمن السيبراني الخاصة بهم والقدرة على غلق الثغرات الأمنية ومشكلات التصميم في مراحل مبكرة جدًا. وأدى هذا المزيج الذي يتضمن تسريع التحول الرقمي، والتكنولوجيا الحديثة، وانتشار الجائحة إلى خلق دوافع متعددة في مجال الأمن السيبراني في دولة الكويت.

يُعد التحول الرقمي، والتكنولوجيا، وجائحة كورونا هي المُحركات الرئيسية للأمن السيبراني

لقد فرض علينا انتشار جائحة كورونا العمل عن بعد مما أدى إلى إضعاف الحدود التشغيلية للمؤسسات.

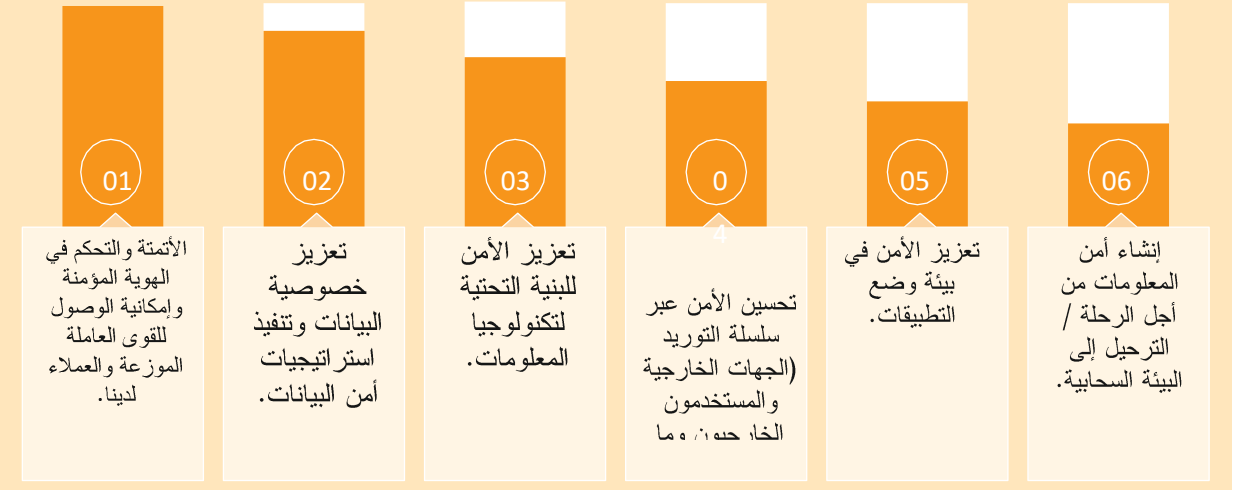
وتمثلت الاستجابة الفورية من قبل المؤسسات، عندما تم فرض الإغلاق، في تسريع وتمكين تدابير وإجراءات العمل عن بعد كأولوية للتخفيف من مخاطر الحضور إلى مكان العمل. وبذل مسؤولو الشبكات وقادة الأمن جهوداً حثيثة لضمان توفير إمكانية الوصول إلى الموارد الهامة للمستخدمين الداخليين والمستخدمين المُميزين والشركاء من الجهات الخارجية.

على الرغم من أن هذا النظام الوقائي (Firefighting Mode) أتاح تطبيقات الأعمال للموظفين بسرعة كبيرة، بيد أنه أدى أيضًا إلى اتخاذ قرارات آنية وبالتالي إدخال مخاطر جديدة. ولقد شكّل هذا السيناريو تحديًا لقدرات مرونة المؤسسات، وجعل فرق العمل تدرك أهمية وضع استراتيجيات للأمن مُسبقًا. وفي الوقت الحاضر، يعتبر دور قائد الأمن أمرًا بالغ الأهمية وينقسم بين تحقيق رؤية التحول الرقمي للمؤسسات مع معالجة المخاطر الجديدة والقائمة في الوقت نفسه في بيئة تتضمن مخاطر وتهديدات على نطاق أوسع من ذلك بكثير.

ومع التركيز على هذا التطور المهم، سُئل المشاركون في الاستبانات من مؤسسات القطاع الخاص في دولة الكويت عن أهدافهم الأمنية الاستراتيجية لعام 2021 لتمكين التحول الرقمي لمؤسساتهم.

الجدول 2: إجابات الاستبانات (الأهداف الأمنية)

بُناءً على مقياس من (1) إلى (6)، صنف المشاركون في ملء الاستبانات هذه الأهداف الأمنية، حيث أن (1) يعني الهدف الأكثر أهمية و (6) هو الهدف الأقل أهمية لمؤسستهم.



لمحة عامة عن الأهداف الاستراتيجية لهذه المؤسسات (مُرتبة حسب الأولوية) ومُحركات الأمن السيبراني في دولة الكويت:

01

تنفيذ الهوية والوصول

يدرك قادة الأعمال مدى الحاجة إلى التحكم في إمكانية الوصول إلى موارد المؤسسة ومراقبتها. تُسهم أدوات الاستفادة من إدارة الهوية والوصول (IAM) والحوكمة في تمكين المؤسسات من تبسيط هويات المستخدمين لاستخدام تطبيقات متعددة محليًا على الحواسيب والخوادم أو على السحابة.

في الوقت المناسب

- إضافة إمكانية الوصول وتغييره وإزالته
- إعادة الاعتماد والتصديق

التمتع بإمكانية الوصول السليم

- المُنضمون "Joiner" / المُنتقلون "Mover" / المُغادرون "Leaver"
- الطلبات / الموافقة
- تحديد المهام التلقائية

التأكد من توفر الموظفين المؤهلين

- تحديد أساليب التدقيق
- التعيين والتأهيل
- المصادقة

02

تأمين التطبيقات

تُعد التطبيقات، في معظم الحالات، نتاجاً لرحلة التحول الرقمي للمؤسسة، من خلال إطلاق خدمات جديدة، حيث تقوم المؤسسات بإنشاء تطبيقات يمكنها تلبية متطلبات العملاء رقميًا بطريقة آمنة وسهلة. تُرحل التطبيقات من السيناريوهات محليًا على الحواسيب والخوادم إلى السيناريوهات السحابية بالإضافة إلى السيناريوهات المختلطة. ومن المؤسسات التي تقوم بتخصيص أو تطوير تطبيقاتها الخاصة على سبيل المثال، شركات الطيران والبنوك حيث تعتمد وسائل تطوير مرنة من شأنها أن تتواءم بشكل أفضل مع أولويات أعمالهم. كما أنها تشكل محورًا أساسيًا في رحلة التحول الرقمي. وقد دفع السعي إلى تحقيق أقصى قدر من الأتمتة وقصر الفترة الزمنية لتنفيذ الأعمال العديد من الأشخاص إلى اعتماد عمليات التطوير "DevOps". ومع ذلك، فإن ضوابط الرقابة الأمنية داخل عمليات التطوير "DevOps" تمثل أحد التحديات. وعلى الرغم من أن اعتماد عمليات تطوير الأمن "DevSecOps" لا يزال مستمر ويساعد في سد الثغرات الأمنية، إلا أن المؤسسات تتطلع نحو الحماية الشاملة من خلال إضافة تقييمات الأمن وعملية المراجعة بدءًا من مرحلة التطوير إلى مرحلة ما بعد الإنتاج.

03

إصلاح البنية الهيكلية

يعتمد الإصلاح الرقمي من خلال التحول الرقمي على تقنيات مثل السحابة (Cloud)، وإنترنت الأشياء (IoT)، وإيدج (Edge)، وشبكات الجيل الخامس (G5) وما إلى ذلك، مما يوفر مزايا هائلة لتبادل البيانات في الوقت الآني والمرونة. ومع ذلك، ومن خلال الاستعانة بهذه التقنيات، تصبح المؤسسات أقل حدودًا، وربما لا تكون تقنيات الأمن التقليدية مناسبة. ومن ثم، تضع المؤسسات استراتيجيات لخارطة طريق التكنولوجيا الخاصة بها على مدى السنوات القليلة المقبلة لتطوير القدرات بما يتواءم مع الأطر المشهود لها عالميًا مثل الثقة الصفرية (Zero Trust) أو حافة خدمات الوصول الآمن (SASE).

يتطلب اعتماد هذه الأطر وتحويلها إلى خطط قابلة للتنفيذ إجراء التخطيط الدقيق ومراعاة العديد من التقنيات والخيارات مثل التجزئة الدقيقة، وإدارة الهوية والوصول (IAM)، وإدارة الوصول المميز (PAM)، وتقنيات وسيط أمن الوصول إلى السحابة (CASB)، ومنع تسريب/ فقدان البيانات (DLP)، والشبكة الافتراضية الخاصة (VPN) وما إلى ذلك من أجل العمل المُشترك. يهدف هذا التعاون بين التقنيات والأطر إلى تحقيق التقارب بين الخدمات الأمنية، وتقليل التعقيد في إدارة بيئة التهديدات الهائلة، مع تحسين سرعة الاتصال.

بناء الثقة

04

مع إطلاق البلدان في جميع أنحاء العالم لأطر الخصوصية الخاصة بها، فقد دخلنا رسميًا في عصر الخصوصية. وهناك كمية ضخمة من البيانات التي يتم إنشاؤها كل يوم. وستصبح متطلبات البيانات ورسم الخرائط أكثر تعقيدًا مع زيادة استخدام السحابة، وزيادة عدد المستخدمين ممن لديهم اتصال خارجي، وزيادة الاعتماد على الجهة الخارجية خلال السنوات القليلة المقبلة. ويثير هذا التعقيد مخاوف بشأن أمن البيانات والخصوصية في عالم بلا حدود. ومن الضروري أن ينظر مسؤولو أمن المعلومات (CISOs)في الضوابط الرقابية المناسبة للتأكد من أنها تعمل على تطوير نهج أمن وخصوصية البيانات بشكل كامل في السنوات المقبلة (لكل من البيانات المهيكلة وغير المهيكلة).

في الواقع، تتوقع المؤسسات في دولة الكويت بالفعل حدوث تغييرات في اللوائح المتعلقة بأمن وخصوصية البيانات وتقوم بتصميم الضوابط الرقابية من بدايتها إلى نهايتها وتجهيز هذه المتطلبات في جهود التحول الرقمي الخاصة بها. كيف ستتعامل المؤسسات مع معلومات التعريف الشخصية (PII) لعملائها في السنوات المقبلة سيساعد على بناء علاقة موثوق بها معهم وتقوية تصورهم للعلامة التجارية بشأن الاستخدام الأخلاقي للبيانات.

حتمية الرحلة إلى السحابة

05

في غضون أيام قليلة من انتشار جائحة كورونا، أدركت المؤسسات أنها ستحتاج إلى نقل بعض أعباء العمل إلى بيئة سحابية للاستفادة من مزايا المرونة وقابلية التوسع التي توفرها المنصة. تختلف أولويات اعتماد السحابة بين المؤسسات وفقًا لمتطلبات العمل واللوائح التي تخضع لها، مما يجعلها معيارًا رئيسيًا لاتخاذ القرار بين اعتماد الخدمات السحابية العامة أو الخاصة أو المختلطة. يعد نقل أعباء العمل الهامة وخدمات الأعمال مهمة شاقة لأنها تتطلب من المؤسسات مراجعة المتطلبات بشكل نقدي، كما تتطلب في كثير من الحالات إعادة صياغة تطبيق قديم من بدايته إلى نهايته. ومع ذلك، فإن الانتقال إلى تقنيات الحوسبة السحابية في الوقت الحالي لا يتعلق بـــ "لو" بل "متى".

على الرغم من أن الحوسبة السحابية تتضمن مزايا هائلة تتمثل في قابلية التوسع والمرونة وإمكانية التوافر، فإن هناك تحديات أمنية متعددة يجب معالجتها ومراجعتها والتخفيف منها في الوقت المناسب. ويجب مراجعة المخاطر بالتفصيل مثل عمليات تأمين الموردين، وفصل المهام، وقيود الموقع الجغرافي، واتفاقيات مستوى الخدمة، وما إلى ذلك لضمان وجود الضوابط الأمنية. يجب أيضًا على المؤسسات التي تبدأ رحلتهم السحابية وضع خارطة طريق أمنية لبيئتهم السحابية المتعددة النهائية.[4]

أبرز النتائج العالمية

لا يدرج صانعو القرار في مجال تكنولوجيا المعلومات الأمن السيبراني فحسب ضمن أهم اعتباراتهم عندما يتعلق الأمر بالتحول الرقمي، بل إنه أيضًا يُمثل ثاني أكبر أولوية استثمارية لديهم (35%)، وأقل بقليل من السحابة (37%)، وفقًا لدراسة حديثة باستخدام مقياس الارتفاع "Altimeter".[5]

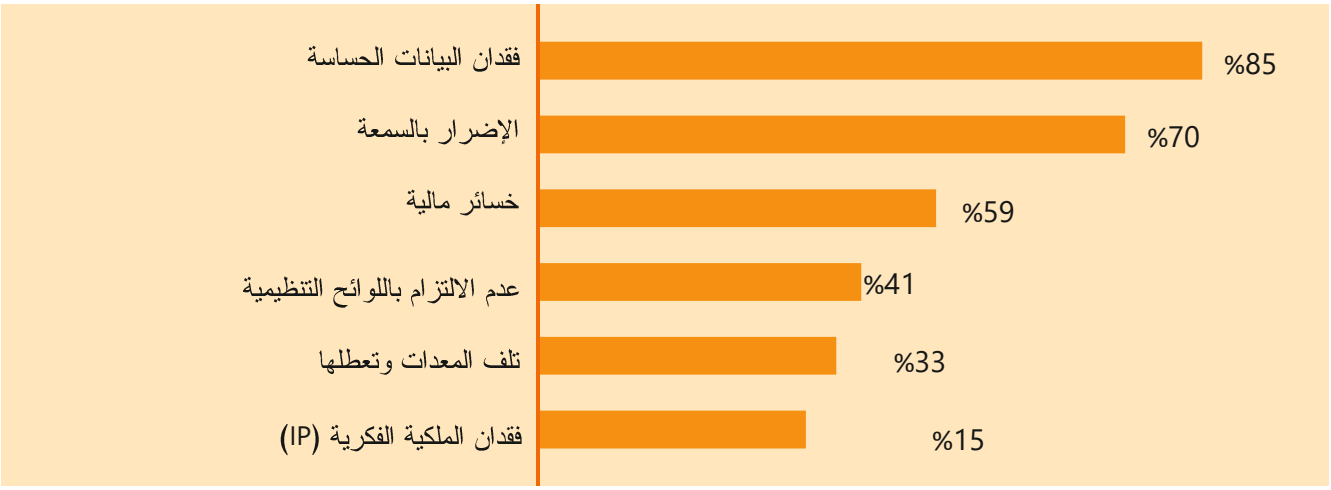
5. https://www.gartner.com/en/information-technology/role/security-risk-management-leaders

تزايد الهجمات السيبرانية خلال انتشار جائحة كورونا (كوفيد-19)

نظرًا لطريقة العمل الموزعة، شهد عام 2020 ارتفاعًا في الهجمات السيبرانية، بدءًا من التصيد الاحتيالي وهجمات برامج الفدية (Ransomware) وصولًا إلى هجمات سلسلة التوريد المعقدة والمستهدفة بشكلٍ كبير. مع زيادة عدد الهجمات، واجهت قدرات المؤسسات تحديًا بشكل يومي في مقاومة هذه الهجمات. لا تزال معظم المؤسسات قلقة جداً بشأن فقدان البيانات الحساسة من خلال هجمات برامج الفدية (Ransomware) التي لا يمكن تداركها أو الهجمات المستهدفة المعقدة. وعلى الرغم من أن العديد من المؤسسات تبذل قصارى جهدها لحماية نفسها، فإن تداعيات هذا الهجوم لا تقتصر في بعض الأحيان على الخسائر المالية فحسب، لكن لها تأثير مباشر أيضًا على سمعة المؤسسة نفسها، كما أنها تُلحق ضرراً بالغاً بالعلامة التجارية وكذلك الثقة في التعامل التي تجتهد المؤسسة بشكل كبير لاكتسابها.

ومن المتوقع أيضًا أن يستمر اتجاه الزيادة في عدد الهجمات أكثر من ذلك في عام 2021.

الجدول3: إجابات الاستبانات (فقدان البيانات)



وفقًا لهذه الاستبانات فإن **فقدان البيانات الحساسة (85%)**، **متبوعًا بإضرار بالسمعة (70%)** ثم **خسائر مالية بلغت (59%)**، قد أثر بشكل كبير على **المناطق الثلاث الأولى** في حالة وقوع حادث يتعلق بالأمن السيبراني.

في حين أن المناطق الأقل تأثرًا نسبيًا تُمثل عدم الالتزام باللوائح التنظيمية (41%) وتلف المعدات وتعطلها (33%) وفقدان الملكية الفكرية (15%).

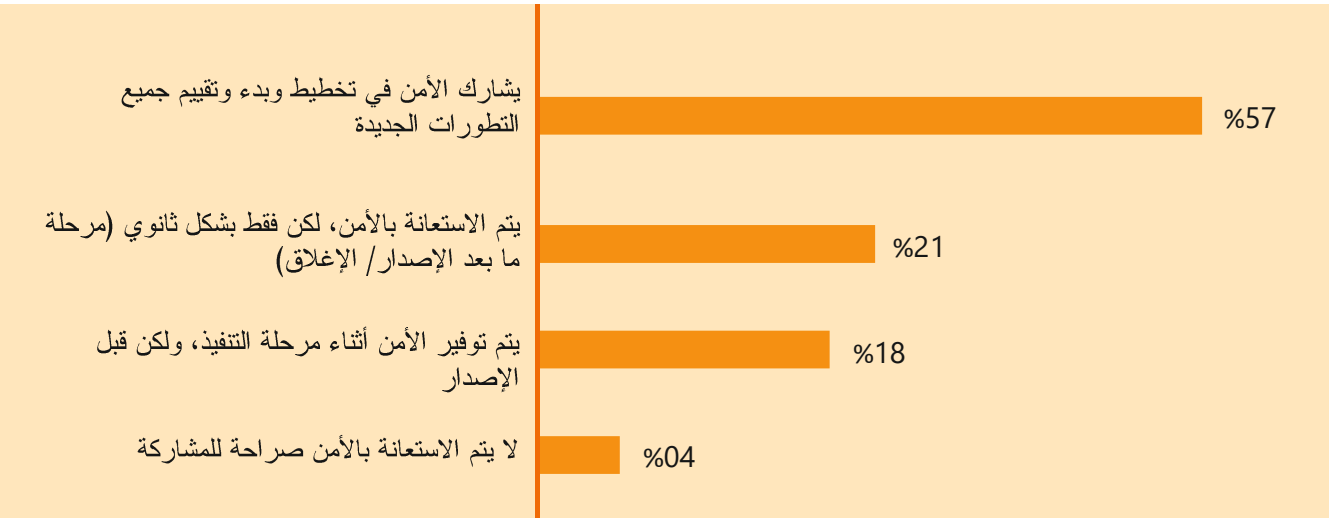
الأمن - لم يعد بعد أمرًا ثانويًا

لعدة سنوات، كان مسؤولو أمن المعلومات (CISOs) مؤيدين بشدة للأمن باعتباره وظيفة عمل بالغة الأهمية ويجب ألا يكون مجرد أمر ثانوي. وفي ضوء زيادة الهجمات السيبرانية، أصبح لدى مجالس الإدارات وعمليات الأعمال القدر نفسه من الاهتمام فيما يتعلق بالمبادرات الأمنية والقيمة التي يمكن للأمن تحقيقها من خلال التخطيط وما بعده. تُشير نتائج هذه الاستبانة التي استطلعنا آراء المشاركين فيها إلى أن 57% من المؤسسات أعادت وضع المسؤوليات الأمنية للمشاركة في مبادرات التحول الرقمي وغيرها من مبادرات الأعمال بدءًا من مرحلة التخطيط ذاتها. ويُعد هذا النهج له فوائده الواضحة، ليس فقط في تقليل تكلفة أدوات الأمن السيبراني والتقييمات في وقت لاحق، بل يساعد أيضًا على تنفيذ الدفاع المتعمق (Defense-in-Depth) الذي يعد ذا تأثير كبير في تصميم الأمن.

وعلى الرغم من أنه من الجيد رؤية معظم المؤسسات وهي تشارك في الأمن ضمن مراحل مُبكرة، فإن من المثير للاهتمام أيضًا ملاحظة أن 21% من هذه المؤسسات لا تزال تتبنى الأمن باعتباره أمرًا ثانويًا، فيما تستعين 18% منها بالأمن فقط أثناء مرحلة التنفيذ.

من الضروري أن تسعى المؤسسات نحو ضمان أن الأمن لم يعد أمرًا ثانويًا. مدى دمج أمن تكنولوجيا المعلومات في مبادرات الأعمال الجديدة من قبل المؤسسات

الجدول4: إجابات الاستبانات (أهمية الأمن)



خط الأساس عبر أطر العمل الأمنية

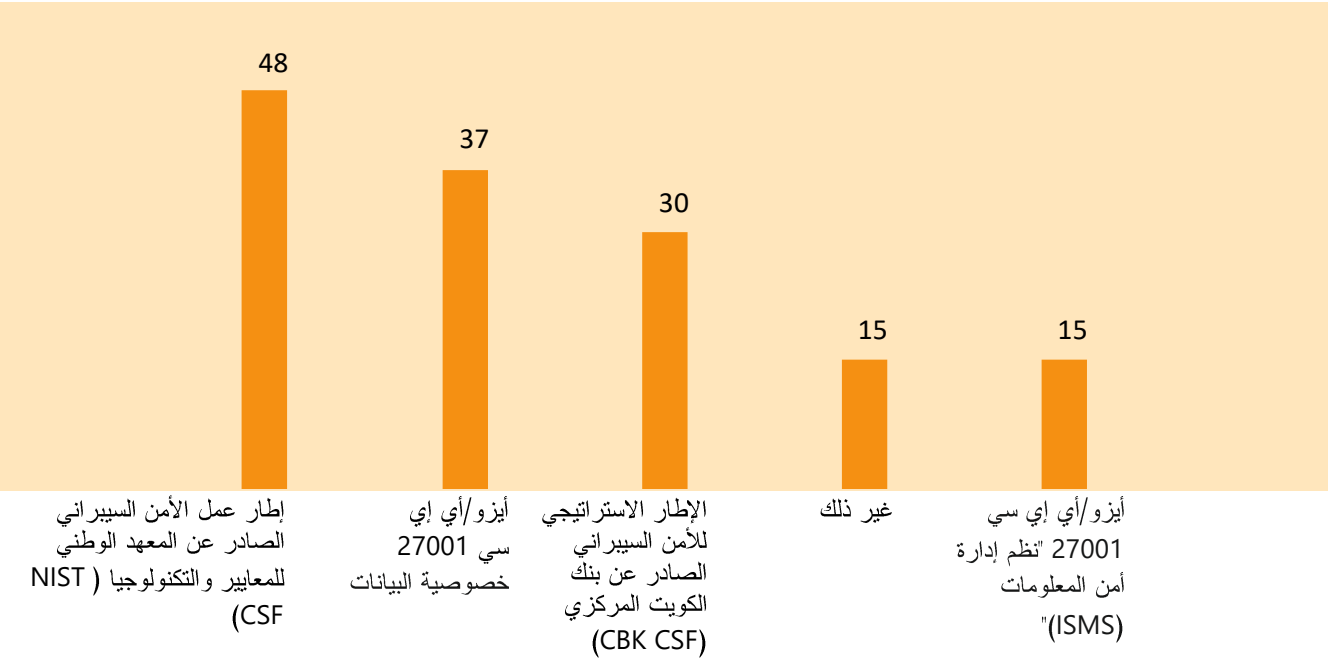
من الحقائق المعروفة جيدًا أن أطر العمل الأمنية غالبًا ما تكون أفضل مورد لتصميم الضوابط الرقابية ووضع السياسات والتقييم أثناء تنفيذ أحد برامج الأمن داخل المؤسسة. في الوقت الحالي، هناك أطر عمل أمنية أصدرتها الجهات الرقابية في القطاعات الحيوية مثل البنوك والبنية التحتية الحيوية والسحابة وما إلى ذلك، وهي تساعد على ضمان ممارسات الأمن الأساسية التي يمكن اتباعها عبر القطاع الذي يخضع للتنظيم. تبدأ معظم المؤسسات في تنفيذ إطار عمل معروف ومعتمد على نطاق واسع مثل معيار إدارة أمن المعلومات (ISO 27001)، وهو أحد المعايير الدولية. تجدر الإشارة إلى أن 48% من المؤسسات في دولة الكويت اعتمدت بالفعل إطار عمل معيار إدارة أمن المعلومات (ISO 27001) ووضعت إطار عمل لأنظمة إدارة أمن المعلومات (ISMS) وفق هذا المعيار وحده. تتمثل أكبر ميزة لإطار عمل معيار إدارة أمن المعلومات (ISO 27001) في أن المؤسسة تحقق حالة الاعتماد وتساعد على بناء الثقة مع عملائها الحاليين والمحتملين.

المعهد الوطني للمعايير والتكنولوجيا (NIST) – إطار عمل الأمن السيبراني (CSF) هو إطار عمل معياري آخر يزداد معدل استخدامه في المنطقة مع زيادة قابلية تبني واعتماد إطار العمل. يبلغ معدل اعتماد إطار عمل الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتكنولوجيا (NIST CSF) في دولة الكويت في الوقت الحالي 15% وسوف يزداد باستمرار للمؤسسات التي ترغب في زيادة تعزيز ضوابطها الأمنية الحالية.

أخيرًا، سنُلقي نظرة على الأطر التنظيمية في دولة الكويت. الإطار الأول هو إطار عمل الأمن السيبراني لبنك الكويت المركزي (CBK CSF) الصادر عن بنك الكويت المركزي (CBK)، وينطبق على البنوك العاملة خارج دولة الكويت. تم تطبيق إطار عمل الأمن السيبراني لبنك الكويت المركزي (CBK CSF) في 30% من المؤسسات في دولة الكويت. الإطار الثاني هو إطار عمل الأمن السيبراني (CITRA CSF) الصادر عن الهيئة العامة للاتصالات وتقنية المعلومات (CITRA) والذي ينطبق على الفئات المستهدفة من القطاع العام والقطاع الخاص والأفراد. بما أن هذه الاستبانة لا تغطي سوى مؤسسات القطاع الخاص، فإن نسبة اعتماد إطار العمل تبلغ 7% فقط.

ويتضح من هذه الاستبانة أن معيار إدارة أمن المعلومات (ISO 27001) أصبح هو إطار العمل الفعلي للأمن السيبراني المفضل لمعظم المؤسسات. ومع تقدمهم في رحلة التحول الرقمي الخاصة بها، من المتوقع إضافة المزيد من أطر الأمن السيبراني إلى برامج نظم إدارة أمن المعلومات (ISMS) الخاصة بها بحيث يمكن إضافة المزيد من ضوابط الأمن مما يؤدي إلى نضج أمني أفضل بكثير داخل المؤسسة.

الجدول5: إجابات الاستبانات (الأطر الأمنية التي تم اعتمادها)



أبرز النتائج العالمية

وفقًا لاستبانة "اتجاهات تبني إطار العمل الأمني" الذي أجرته شركة (Tenable)، **تعالج 84% من المؤسسات في الولايات المتحدة هذه المشكلة بمساعدة إطار عمل أمني، وتستخدم 44% منها أكثر من إطار عمل أمني واحد.**

يستخدم **47% من المؤسسات معيار أمن بيانات صناعة بطاقات الدفع (PCI DSS) والذي يتم تصنيفه في المرتبة الأولى**، يليه **(35%) لمعيار إدارة أمن المعلومات (ISO 27001)**، و (32%) ضوابط الأمن الحرجة لمركز أمن الإنترنت (CIS)، و(29%) إطار العمل الصادر عن المعهد القومي للمعايير والتقنية (NIST) لتحسين أمن البنية التحتية الحرجة[6].

6. Top 4 cybersecurity frameworks - IT Governance USA Blog

أهم التحديات التي تواجه تنفيذ برنامج الأمن

تعتمد قدرة برنامج الأمن على النجاح داخل المؤسسة بشكل مباشر على فريق عمل الأمن التابع لتلك المؤسسة. ومع ذلك، فإن فجوة مهارات الأمن السيبراني تتزايد بشكل مستمر خلال السنوات الماضية. وبالتالي، ليس غريباً أن تصرح 78% من المؤسسات بأن التحدي الأكبر أمامها هو إيجاد المهارات الأمنية التي يمكنها معالجة التهديدات في بيئتها.

وتتمثل أهم ثلاثة تحديات تواجه المؤسسات لتنفيذ برنامج الأمن الخاص بها في نقص المهارات، والقيود المفروضة على الميزانية، وتصنيف البيانات.

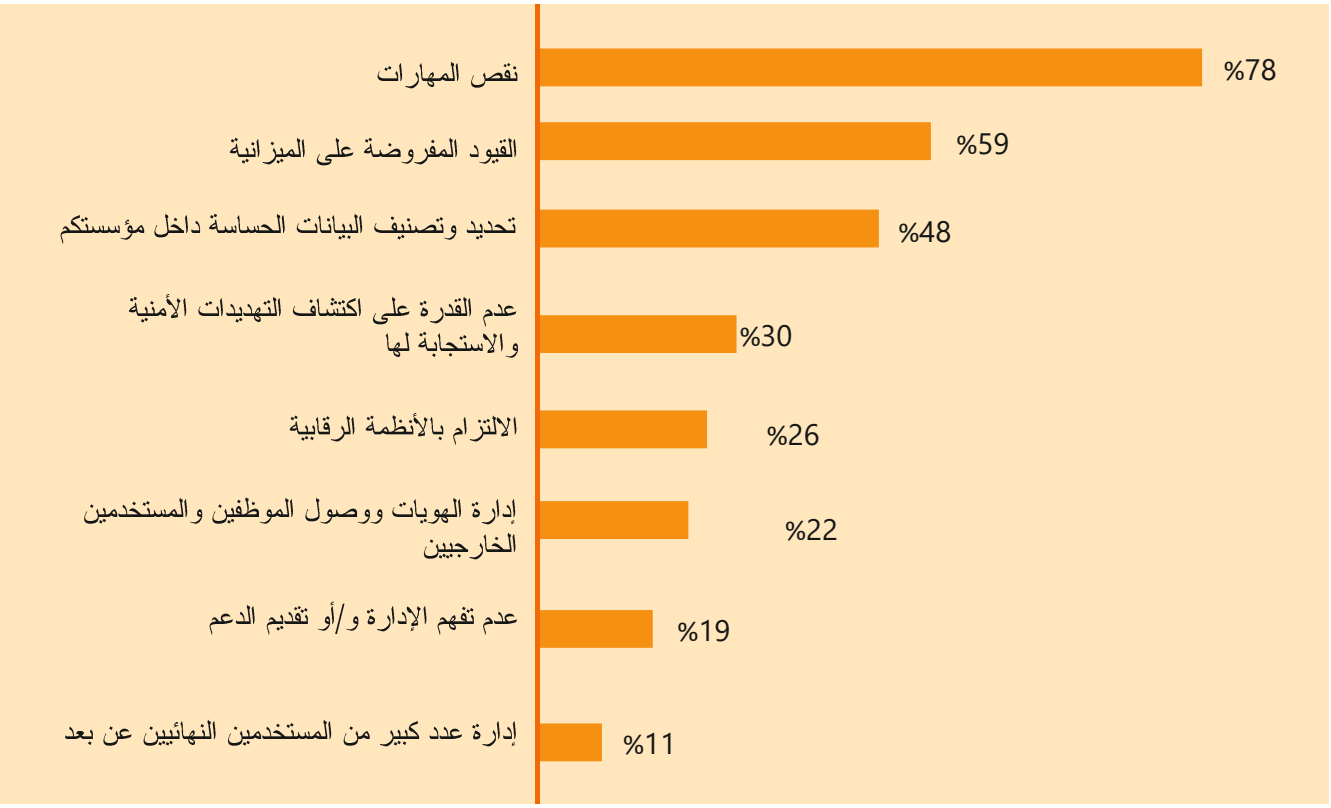
إن مجموعات المهارات الخاصة بالأمن السيبراني متنوعة بحيث يصبح العثور على خبراء في مجالات متعددة مثل أمن الشبكة، وأمن التطبيقات، وأمن البيانات، وخصوصية البيانات، والهوية والوصول وما إلى ذلك أمرًا صعبًا جداً. ويزداد الأمر تعقيدًا مع تحرك المؤسسات نحو اعتماد السحابة، حيث تزداد ندرة المهارات الأمنية في هذا المجال في المنطقة.

ونظرًا لأن الأعمال أصبحت تتسم بالسرعة والمرونة في العالم ما بعد انتشار جائحة كورونا، يتم تقليص الميزانيات ويُطلب إلى المؤسسات تحقيق أقصى استفادة من الوضع الراهن. إن القيود المفروضة على الميزانية هي أحد التحديات التي ذكرتها 59% من المؤسسات في دولة الكويت.

يتم إنشاء البيانات في الوقت الحالي من قبل العملاء، والموظفين، والتطبيقات المُخصصة، وأجهزة استشعار إنترنت الأشياء (IoT Sensors)، وأنظمة النسخ الاحتياطي والعديد من المصادر الأخرى. وبالنسبة للمؤسسات صار تحديد وتصنيف البيانات التي يتم إنشاؤها أمراً صعباً جداً. أمن البيانات هي مبادرة إستراتيجية تنقل المؤسسات خلال رحلة طويلة من النضج، وإحدى الخطوات الأولى تتمثل في تحديد وتصنيف البيانات الموجودة حاليًا. ومع ذلك فهو يمثل تحديًا لنحو 48% من المؤسسات في دولة الكويت.

وأدى انتشار جائحة كورونا إلى زيادة هائلة في الهجمات في منطقة دول الخليج. تنجح العديد من هذه الهجمات في محاولاتها بسبب عدم وجود الحزم الأمنية (Security Stack) التي يمكن من خلالها اكتشاف التهديدات والرد عليها في الوقت المناسب. وفي معظم الأحيان، تكتشف المؤسسات هذه الهجمات في وقت لاحق وفي ذلك الحين الوقت يكون الضرر قد حدث بالفعل. لا تزال هذه القدرة على الاستجابة للتهديدات في الوقت المناسب وبشكل فعال تمثل تحديًا لـــ 30% من المؤسسات في دولة الكويت.

الجدول 6: إجابات الاستبانات (التحديات الرئيسية)



لقد أدركت المؤسسات على مستوى العالم أنه من غير الممكن منع 100% من الهجمات، وهي تقوم حالياً بموازنة استثماراتها من منع وقوع الهجمات إلى الاكتشاف والاستجابة لتعزيز مرونتها.

أبرز النتائج العالمية

- يعتقد 62% من مسؤولي أمن المعلومات (CISOs) أن النقص في المواهب العالمية في مجال الأمن السيبراني سوف يزداد سوءًا خلال السنوات الخمس المقبلة، وفقًا لتقرير منظمة غلوبال ديجيتال سناب شوت (Global Snapshot): "دور مسؤولي أمن المعلومات (CISOs) في عام 2020"[7].
- يتسبب انتشار جائحة فيروس كورونا الحالي في ضغوط كبيرة على المستهلكين والشركات على حد سواء. بينما تتأرجح الولايات المتحدة على حافة الركود، تعمل الشركات على خفض معدل إنفاقها – بما في ذلك في مجال الأمن السيبراني. **وفقًا لتقديرات شركة الأبحاث والاستشارات العالمية غارتنر (Gartner) فإن الأمن يواجه تخفيضات تصل إلى 6.7 مليار دولار[8].** ومع ذلك، فإن 15% فقط من المؤسسات تُخفض ميزانياتها الأمنية في الكويت.

الأمن السحابي

على الرغم من أن المؤسسات تبنت الحوسبة السحابية لدعم القوى العاملة الموزعة ومبادرات التحول الرقمي، فإن هناك مخاوف ومخاطر يجب معالجتها على المدى البعيد لضمان تصميم وتنفيذ الضوابط الأمنية بشكل مناسب. فيما يلي أهم 3 مخاوف لمؤسسات القطاع الخاص في دولة الكويت أثناء طرح مبادرات الحوسبة السحابية:

أ. مخاطر تسريب البيانات

عبرت 59% من المؤسسات عن مخاوفها بشأن احتمالات تسريب البيانات أثناء طرح مبادراتها السحابية. يجب تحديد هذه المخاطر ومعالجتها مُسبقًا حتى تتمكن هذه المؤسسات من نشر تقنيات الأمن النسبية وبالتالي التخفيف من المخاطر. وعلاوة على ذلك، يجب الاتفاق على فصل الأدوار والمسؤوليات بين مزود الخدمة السحابية (CSP) والعميل (CSC) بشكل مناسب وتوثيقها لتجنب أي نزاع.

ب. الالتزام باللوائح التنظيمية المحلية

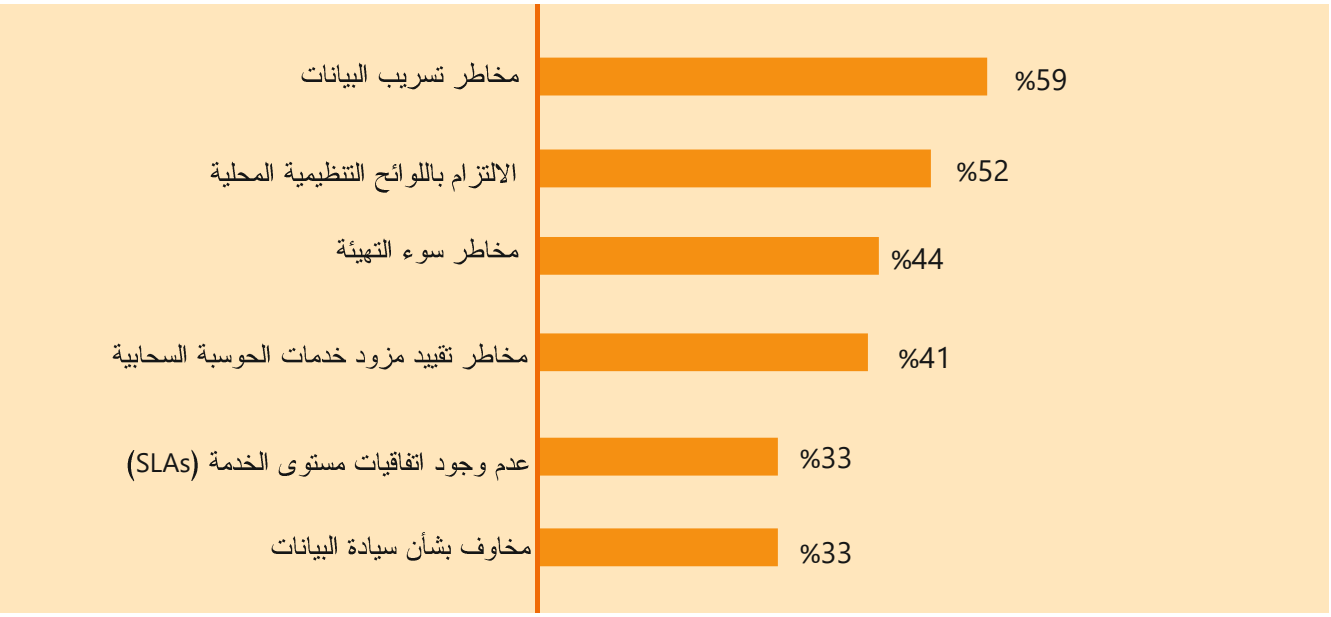
على الرغم من قيام مزودي خدمات الحوسبة السحابية بتنفيذ أطر عمل محلية ودولية على مراكز البيانات السحابية الخاصة بهم، فإن 52% من هذه المؤسسات تهتم بشكل أساسي باللوائح الحكومية المتعلقة بكيفية ومكان تخزين البيانات واستخدامها من قبل مزودي خدمات الحوسبة السحابية (CSPs). يجب على المؤسسات بذل العناية الواجبة المناسبة على عروض مزودي خدمات الحوسبة السحابية والحصول على الرأي التنظيمي بشأن المناطق المهمة، مثل سيادة البيانات (Data Sovereignty) قبل طرح مبادرتها السحابية.

ج. مخاطر سوء التهيئة

يعتمد أمن البنية التحتية الافتراضية بشكل كبير على الطريقة التي تم تهيئة ذلك وفقًا لها وما إذا كان قد تم اتباع إرشادات خط الأساس المتشددة. اعتمادًا على نموذج النشر الذي تختاره المؤسسة، تنتقل مسؤولية التنسيق بين مزودي خدمات الحوسبة السحابية والعميل (CSC). تعتبر هذه المخاطر مهمة جداً بالنسبة لنحو 44% من المؤسسات في دولة الكويت، وقد تُلحق الضرر بالمؤسسة إذا لم يتم اتباع إرشادات التهيئة أو إذا لم يتم التحكم في إدارة التغيير. من الضروري أن تفهم المؤسسات مسؤولياتها وتضمن أن بيئتها الافتراضية مؤمنة بشكل مناسب.

7. https://www.marlinhawk.com/docs/Marlin-Hawk-Global-CISO-Research-Report.pdf
8. How can security leaders maximize security budgets during a time of budget cuts? - Help Net Security

الجدول7: إجابات الاستبانات (المخاوف الرئيسية)



أبرز النتائج العالمية

- توقعت شركة الأبحاث والاستشارات العالمية غارتنر (Gartner) أن تعاني 60% من الشركات الرقمية من أوجه قصور في الخدمة بحلول عام 2020 بسبب عدم قدرة فرق الأمن على إدارة المخاطر الرقمية[9].
- لتحديد أهم المخاوف، أجرت مؤسسة تحالف أمن الحوسبة السحابية (CSA) استطلاعاً للخبراء في القطاعات لجمع الآراء المهنية حول أكبر مشكلات الأمن في الحوسبة السحابية. تتمثل أهم ثلاثة تهديدات تم التعرف عليها **في خروقات البيانات، وسوء الإدارة، وعدم كفاية التحكم في إدارة التغيير، وعدم وجود بنية واستراتيجية أمن السحابة**[10].

9. https://www.gartner.com/en/newsroom/press-releases/2016-06-06-gartner-says-by-2020-60-percent-of-digital-businesses-will-suffermajor-service-failures-due-to-the-inability-of-it-security-teams-to-manage-digital-risk
10. top cloud security threats | CSO Online

نضج وتطور أمن البيانات

في الأعمال الرقمية، فإن الإيرادات الأساسية التي تعتمد عليها المؤسسات هي البيانات، من خلال معالجة البيانات أو تقييمها أو بيعها. ومع ذلك، فإن أمن البيانات هو مسار عمل طويل ومُعقد يجمع بين العديد من التقنيات والسياسات والضوابط الرقابية، والعمل جنبًا إلى جنب وفي الوقت الآني لضمان حماية البيانات طوال دورة حياتها.

ولا يتم تشجيع المؤسسات بسبب الجهود اللازمة لرفع مستوى نضج ممارسات أمن البيانات لأنها تلقي بعضًا من المسؤولية على كاهل مُعد البيانات (Data Creator) وكذلك مسؤولي الإجراء لتصنيف البيانات.

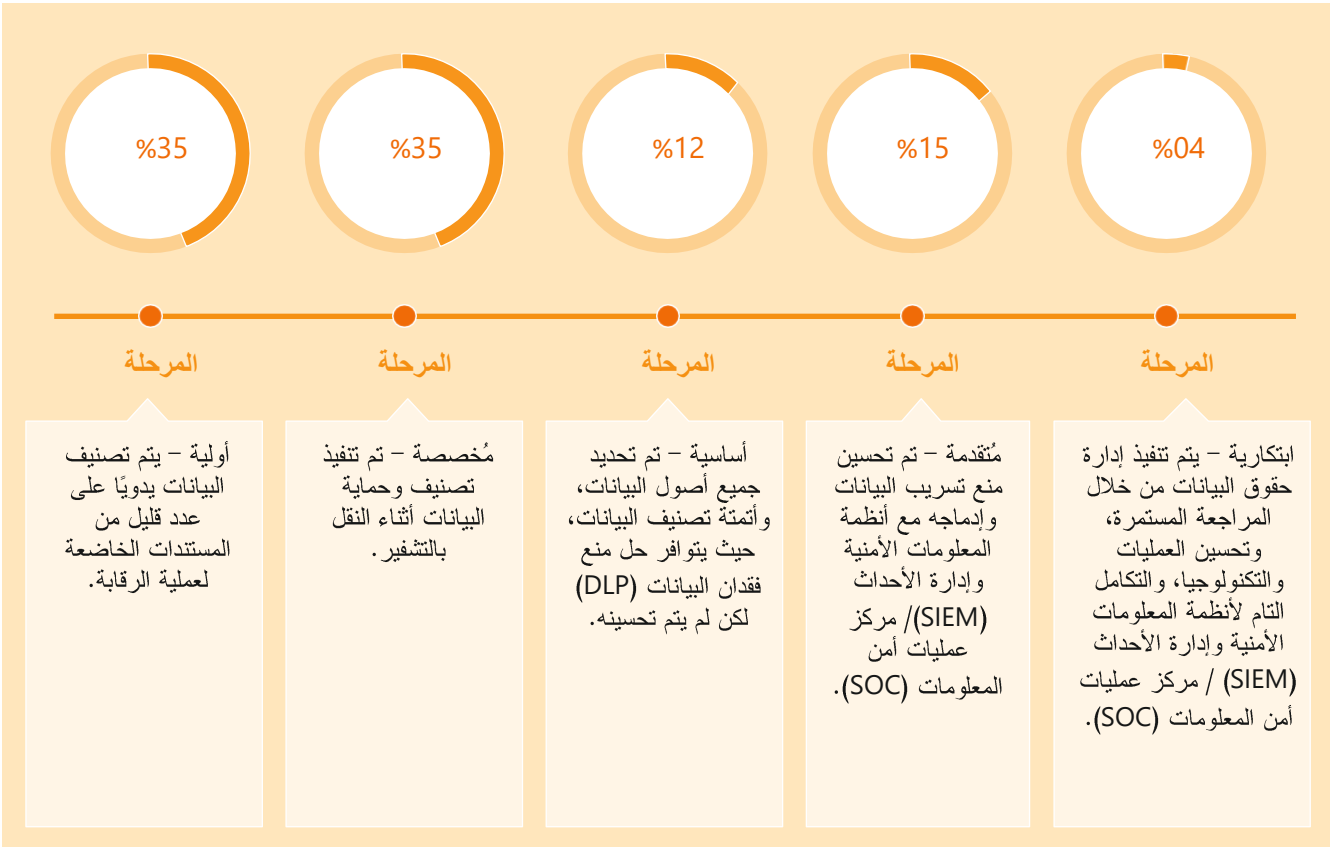
بمجرد أن تتخطى المؤسسات هذه العقبة، غالبًا ما يتم تخفيف التحديات الأخرى من خلال التنفيذ المناسب للتكنولوجيا وعن طريق السياسات والإجراءات السليمة.

وهذا يعني أن تصنيف البيانات يتم إما يدويًا أو يتم تنفيذه بشكل آخر. قامت أيضًا 35% من المؤسسات الموجودة في المرحلة 2 (المُخصصة) بتنفيذ آليات التشفير الأساسية التي تحمي البيانات أثناء عملية النقل. وهناك 12% من المؤسسات في منتصف رحلتها وقد حددت جميع أصول البيانات أثناء أتمتة تصنيف البيانات مع حل منع فقدان البيانات (DLP). وهناك 15% من المؤسسات في حالة متقدمة نسبيًا حيث تم ضبط حلول منع فقدان البيانات (DLP) الخاصة بها مع مجموعات قواعد الأعمال ودمجها أيضًا مع حلول المعلومات الأمنية وإدارة الأحداث (SIEM) لتوحيد تحديد التهديدات في حالة وقوع حادث أمني. وصلت 3% فقط من المؤسسات إلى المرحلة الابتكارية تمامًا مع التنفيذ الكامل لحلول إدارة حقوق البيانات (DRM)، وإجراء المراجعات على أساس مستمر.

وفقًا لنتائج الاستبانة، لا تزال 70% من مؤسسات القطاع الخاص في دولة الكويت في مراحلها الأولى من نضج أمن البيانات.

من المهم ملاحظة أنه بحلول المرحلة (5)، تقوم المؤسسات بتطوير القدرة على تأمين ومراقبة استخدام البيانات طوال دورة حياة البيانات.

الجدول 8: إجابات الاستبانات (نضج أمن البيانات)



أبرز النتائج العالمية

33% من المؤسسات العالمية لديها نهج ناضج لدرجة كبيرة لأمن البيانات من خلال تطبيق التقنيات المُتقدمة والسياسات التفصيلية الدقيقة. وتقوم هذه المؤسسات بإدارة البيانات بما يتواءم مع استراتيجية المخاطر لحماية سرية المعلومات وسلامتها وتوافرها وحقوق الخصوصية لموضوعات البيانات[11].

نضج إدارة الهوية والوصول

زادت الحاجة إلى حلول إدارة الهوية والوصول (IAM) بشكل كبير في عام 2020. ومعظم هذه الزيادة هي نتيجة مباشرة لانتشار جائحة كورونا، حيث حاولت المؤسسات تمكين الوصول الآمن لموظفيها وعملائها إلى موارد مؤسستهم. أصبحت حلول إدارة الهوية والوصول أمرًا ضروريًا حيث أعدت الشركات مُخطط رحلة السحابة الخاصة بهم.

إن تنفيذ حلول وضوابط وسياسات إدارة الوصول والهوية الفعالة داخل المؤسسة، يُمكّن المؤسسات من أتمتة وإدارة دورة حياة تأهيل وعدم تأهيل الموظفين والعملاء على حد سواء.

يتوزع نضج إدارة الهوية والوصول للمؤسسات في دولة الكويت بشكل متساوٍ تقريبًا بين المراحل من (1) إلى (4). وقد وضعت 28% من المؤسسات في المرحلة الأولى بعض سياسات إدارة وصول المستخدمين ونفذتها على موارد تكنولوجيا المعلومات الخاصة بهم. وعلى الصعيد الداخلي، تمتلك المؤسسات أيضًا تطبيقات متعددة تم وضعها للأعمال أو لزيادة معدل إنتاجية الموظفين، وغالبًا لا يتم دمجها في بنية تسجيل الدخول المُوحّد (SSO). وقد نفذت 24% من المؤسسات سياسات فعالة وتم تسجيل بعض الموارد في بنية تسجيل الدخول المُوحّد (SSO) داخل المؤسسة.

قامت 24% من المؤسسات بأتمتة دورة حياة وصول المستخدم بصورة جزئية، مما يقلل بشكل كبير من النفقات العامة على فريق عمل مكتب المساعدة، من خلال توفير حقوق وصول المستخدم وإلغاء حقوق الوصول إليها.

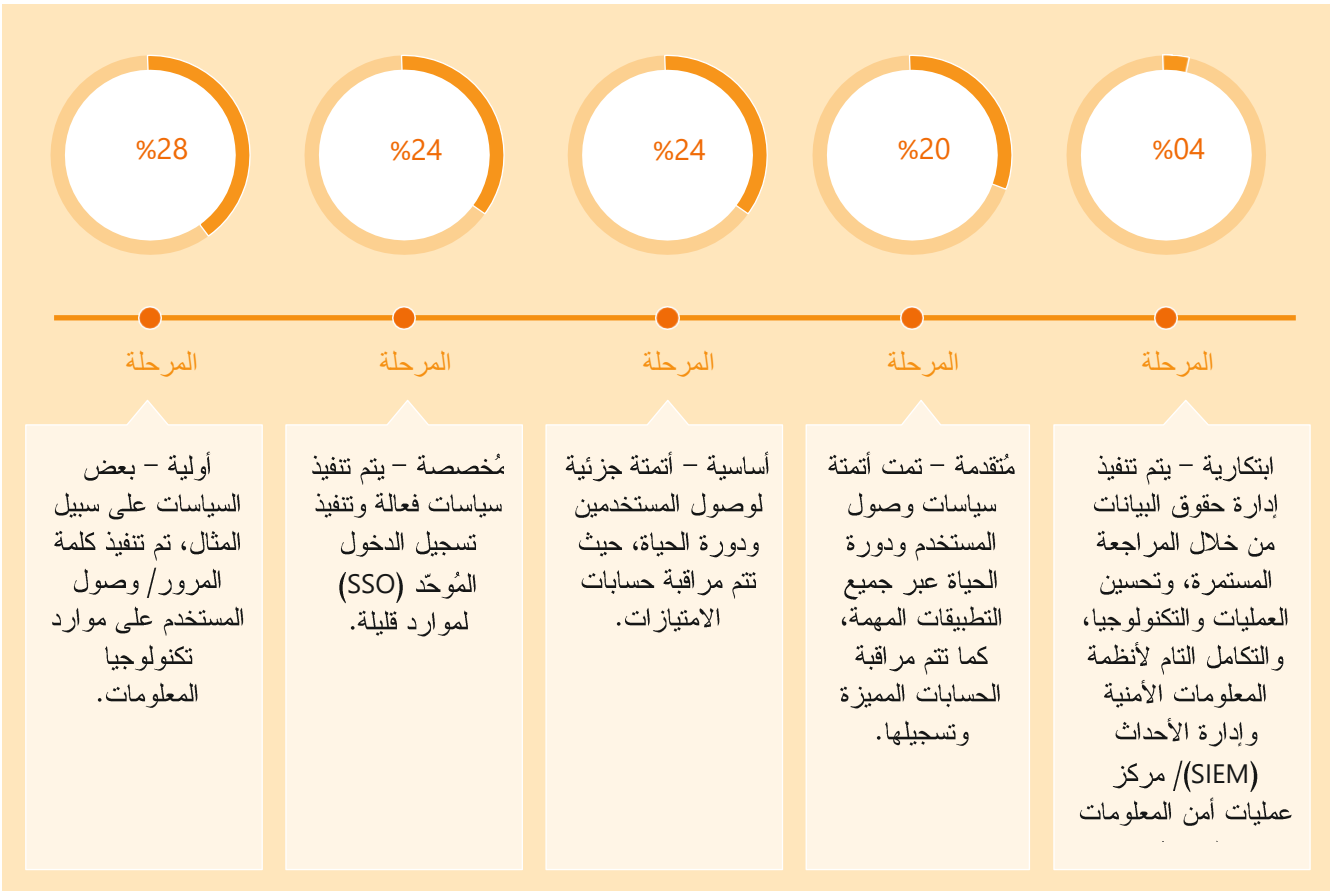
تحتاج العديد من الشركات الكبرى إلى توظيف مستخدمين متميزين (أو ممن يعتمدون على جهات خارجية) مثل مسؤولي النظام أو قواعد البيانات لإدارة العمليات اليومية. ونظرًا لأن لدى هؤلاء المستخدمين إمكانية وصول مباشر إلى المعلومات الهامة، يجب مراقبتهم عبر حلول إدارة الوصول المميز (PAM). تساعد حلول إدارة الوصول المميز (PAM) المؤسسات على إبراز المخالفات في سلوك المستخدم لحلول المعلومات الأمنية وإدارة الأحداث (SIEM) ورفع الحوادث الأمنية. وصلت 20% فقط من المؤسسات إلى النقطة التي لا تكون عندها دورة حياة وصول المستخدم مؤتمتة بالكامل فحسب، بل تتم أيضًا مراقبة إمكانية الوصول المتميز وتسجيله.

يجب دمج جميع حلول الأمن هذه مع حل المعلومات الأمنية وإدارة الأحداث (SIEM) حتى يتمكن فريق مركز عمليات أمن المعلومات (SOC) من تحديد الحوادث الأمنية المحتملة والتحقيق فيها، وقد وصلت 4% فقط من هذه المؤسسات إلى هذه المرحلة.

فجوة بين الأهداف الاستراتيجية والاستثمارات الأمنية

11. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

الجدول 9: إجابات الاستبانات (إدارة الهوية والوصول)



أبرز النتائج العالمية

وصول نحو 38% من المؤسسات على مستوى العالم إلى مرحلة النضج في إدارة الهوية والتحكم في الوصول من خلال الوصول المحدود إلى المرافق المرتبطة بالأصول المادية والمنطقية للمستخدمين المُصرح لهم وللعمليات والأجهزة[12].

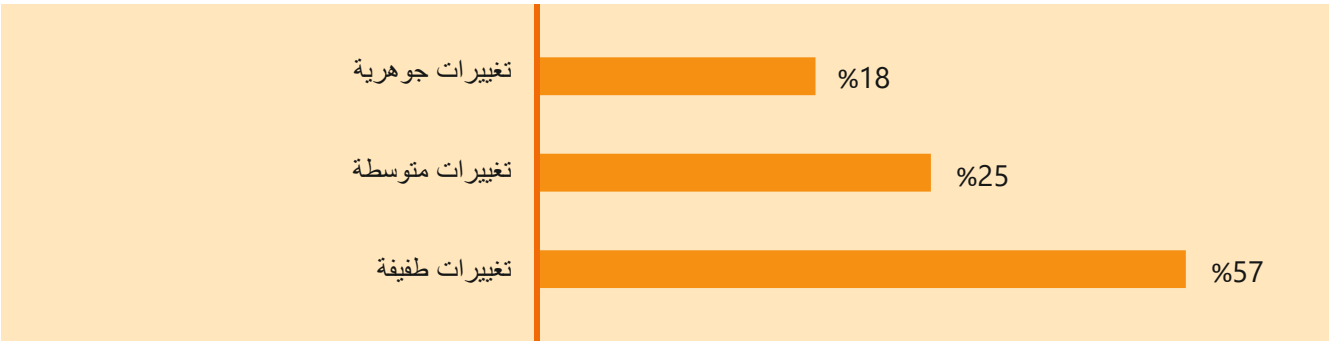
12. https://www.protiviti.com/sites/default/files/united_states/insights/cybersecurity-tech-industry-path-accelerating-progress-protiviti.pdf

التأثير الاستراتيجي طويلة الأجل

نظرًا لأن المؤسسات تعيد تصميم تدفقات العمل وتصور مستقبل العمل، فإن وضع الاستراتيجيات الأمنية له أهمية قصوى. تخطط معظم مؤسسات القطاع الأهلي (57٪) في الكويت لإجراء تغييرات طفيفة في استراتيجياتها الأمنية وذلك لهدف واحد فقط ويتمثل في تبني طريقة آمنة للعمل لموظفيها. هذا التغيير الطفيف لا يتعلق فقط بالاستثمار في الشبكة الافتراضية الخاصة (VPN) أو تقنيات التعاون، لكنه يتضمن أيضًا إنشاء التطبيقات (التي كانت تقتصر بشكل تام على الشبكة الداخلية) التي يمكن إتاحتها للموظفين الذين يعملون عن بُعد.

وقد زاد الاعتماد على الحوسبة السحابية والتحول إلى السحابة العامة والخاصة على حد سواء بسبب الجائحة، مما أدى إلى اتساع نطاق التهديدات. للتعامل مع هذا التحدي الهائل، من المتوقع أن تشهد 43٪ من المؤسسات في دولة الكويت تغييرات تتراوح من معتدلة إلى كبرى في إستراتيجيتها الأمنية على المدى البعيد. تخطط هذه المؤسسات للاستثمار في تقنيات وخدمات الأمن في السنوات المقبلة للتأكد من أنها تخطط للضوابط الرقابية الأمنية وتنفذها بعناية على مستوى نطاق التهديدات المتسع.

الجدول 10: إجابات الاستبانات (التغييرات الاستراتيجية في الأمن)



أبرز النتائج العالمية

- لا يمكن إغفال تأثير جائحة كورونا (كوفيد - 19) على الأعمال، حيث أفادت نحو نصف الشركات، بنسبة بلغت (52٪) أنها شهدت بعض الآثار السلبية في العام الماضي، وأبلغت 10٪ منها أنها شهدت تأثيرًا سلبيًا كبيرًا، في حين لم تشهد منها نسبة 13٪ أي تأثير على الإطلاق.
- من المرجح أن تتأثر الشركات الأصغر حجمًا بدرجة كبيرة عن الشركات الأكبر، وذلك نظرًا لأن قاعدة عملائها تميل أيضًا إلى أن تكون في نطاق الشركات الصغيرة والمتوسطة، وهي التركيبة السكانية الأكثر تضررًا من إغلاق الشركات والقيود المفروضة عليها[13].

13. IT Industry Outlook 2021 (comptia.org)

أثناء إجراء المقابلات مع المشاركين في الدراسة، لوحظ أن معظم تلك المؤسسات ليست لديها استراتيجية أمنية موثقة ومنقحة ومعتمدة

يعتبر الأمن السيبراني أحد المخاطر الرئيسية التي تتعرض لها أي مؤسسة وقد أدت الجائحة إلى زيادة نطاق تلك الهجمات. وبالنسبة لأي مؤسسة ترغب في أن تصبح قادرة على تحديد الهجمات والكشف عنها والاستجابة لها، فهي بحاجة إلى التحقيق في العديد من المفاهيم التقنية المختلفة مثل:

1. **حوكمة الأمن والنموذج التشغيلي**
2. **العمليات والسياسات**
3. **الالتزام بالأمن**
4. **الضوابط الرقابية الفنية والتشغيلية**
   - إدارة الهوية والوصول
   - أمن التطبيقات
   - سرية وأمن البيانات
   - أمن البنية الأساسية
   - أمن نقطة النهاية
   - مراقبة الأمن والتحليلات
   - أمن السحابة

الطريقة الوحيدة للتأكد من أنه تم تهيئته بشكل صحيح هي من خلال وجود برنامج مستدام للأمن، تتم مراقبته وإدارته بشكل جيد. لوضع برنامج ناجح للأمن ومواءمته مع الأعمال، فمن الضروري وضع استراتيجية أمنية سليمة.

مناطق الاستثمار الأمني

يتم ابتكار تقنيات الأمن الحديثة بسرعة البرق، نظرًا للتهديدات الجديدة التي يتم تحديدها كل يوم، لذا فإن المؤسسات لم تكن تمتلك القدرة على تقييم تلك التهديدات في جميع أنحاء العالم، ولكن من خلال استخدام خوارزميات الذكاء الاصطناعي (AI)، أصبحت قادرة على تحديد التهديدات التي تواجه أعمالها. ويعتبر ذلك بمثابة قفزة هائلة في التكنولوجيا. يعد تصميم بنية أمنية مدروسة جيدًا إضافة إلى توافر التكنولوجيا اللازمة جانبًا مهمًا من استراتيجية الأمن للمؤسسة.

على الرغم من أن حزمة تكنولوجيا الأمن الناضجة تجلب منافع متعددة للمؤسسات عند الدفاع ضد الهجمات، فإن لها جانبًا سلبيًا في عمليات الدمج والتنفيذ المعقدة وذلك بسبب نقص موارد الأمن التي تتسم بالقدرة على مستوى المنطقة.

ومن المتوقع أن تشهد مجالات تكنولوجيا الأمن تغييراً جوهرياً في الاستثمار في العام أو العامين المقبلين.

الجدول 11: إجابات الاستبانات (الاستثمارات المتوقعة في تكنولوجيا الأمن)

المجالات	عدد الاستثمارات المخططة	المخططة لسنة 2021	المخططة لسنة 2022
إدارة الهوية والوصول (IAM/SSO/PAM)	%32	%24	%12
بناء / تعهيد عمليات الأمن	%28	%20	%20
مبادرات خصوصية البيانات وأمن البيانات	%8	%44	%16
مبادرات أمن السحابة	%20	%28	%16
مبادرات أمن التطبيقات	%0	%28	%36
تنفيذ حالات استخدام الذكاء الاصطناعي وتعلم الآلة (AI/ML) لأتمتة مهام الأمن	%44	%12	%32
تحديث الشبكة بنموذج الثقة الصفرية (Zero Trust)، و Micro-segmentation والشبكات المُعرفة بالبرمجيات (SDN) وغيرها.	%56	%20	%16

باستثناء التقنيات التي تم تنفيذها بالفعل

تستثمر مؤسسات القطاع الأهلي في الكويت في تقنيات الأمن المختلفة في عامي 2021 و2022، وفيما يلي بعض النقاط البارزة في الاستطلاع الذي تم إجراؤه (حسب الأولوية):

أ. مبادرات أمن التطبيقات

ليس من المستغرب أن تخطط 64٪ من المؤسسات للاستثمار في مبادرات أمن التطبيقات في العامين المقبلين كنتيجة مباشرة لحماية مبادرات السحابة والتحول الرقمي (DX) الخاصة بها. تتوافر حالياً تقنيات أمن التطبيقات التي يمكن نشرها بداية من مرحلة الإعداد حتى مرحلة النشر. لذلك، ستخطط المؤسسات للاستثمار في حلول اختبار أمن التطبيقات الثابتة/ الديناميكية (SAST/ DAST)، أو جدران حماية تطبيقات الويب (WAF) أو تقنيات وسيط أمن الوصول إلى السحابة (CASB) وذلك بهدف التخفيف وإدارة المبادرات المتعلقة بأمن التطبيقات.

ب. مبادرات خصوصية البيانات وأمن البيانات

أظهر تقييم الوضع الراهن لأمن البيانات أن معظم المؤسسات لا تزال عالقة في المراحل الأولية. للتغلب على هذا التحدي ورسم مسارها إلى الأمام، تفكر 60٪ من المؤسسات في زيادة خصوصية بياناتها ونضجها الأمني من خلال التقنيات التي تساعدها. التقنيات الهامة اللازمة في خصوصية البيانات وأمنها هي حلول منع فقدان البيانات (DLP)، وأدوات تصنيف البيانات، وإدارة الحقوق الرقمية (DRM)، وحلول إدارة الخصوصية والتشفير وما إلى ذلك.

ج. مبادرات أمن السحابة

أدى دور الحوسبة السحابية أثناء الجائحة كمحفز لمبادرات السحابة والتحول الرقمي (DX) مع مزايا المرونة وقابلية التوسع والتوافر إلى زيادة اعتماد الحوسبة السحابية. ومن ثم، سوف تزيد 44% من المؤسسات من إنفاقها على مبادرات أمن السحابة. فالأمن في السحابة مختلف عن الأمن المركزي لمركز البيانات التقليدي. سوف تستفيد المؤسسات من حزمة التكنولوجيا الحالية وتشترك في التقنيات التي يمكنها زيادة تعزيز الأمن في السحابة. وستنظر أيضًا في تصميم بناها السحابية المتوافقة مع أطر عمل مثل الثقة الصفرية (Zero Trust) أو حافة خدمات الوصول الآمن (SASE) لاختبار التقنيات الحالية وتأمين البنية الأساسية لشبكة الاتصالات واسعة النطاق المعرفة بالبرمجيات (SD-WAN).

د. تنفيذ حالة استخدام الذكاء الاصطناعي وتعلم الآلة (AI ML) لأتمتة مهام الأمن

ستستمر فجوة المهارات الأمنية في جميع أنحاء العالم في التوسع وستواجه المؤسسات تحديًا هائلاً في الوفاء بالأدوار الحالية / الاحتفاظ بالمهنيين المؤهلين في مجال الأمن. لحسن الحظ، قطع الذكاء الاصطناعي (AI) وتعلم الآلة (ML) شوطًا طويلاً في السنوات القليلة الماضية. على مدار العامين المقبلين، ستتطلع 44٪ من المؤسسات إلى تطوير حالات استخدام مخصصة من خلال استخدام الذكاء الاصطناعي وتعلم الآلة (AI & ML) لأتمتة مهام الأمن العادية ومعالجة فجوة المهارات المتزايدة.

ه. بناء/تعهيد عمليات الأمن

إن فجوة المهارات المذكورة أعلاه إلى جانب عدم قدرة المؤسسات على تحديد التهديدات الأمنية والاستجابة لها في الوقت المناسب (قسم التحديات الرئيسية)، تجعل 40٪ من المؤسسات تقوم ببناء مركز عمليات الأمن الخاص بها (SOC) أو تتطلع نحو الشراكة مع مزودي خدمات الأمن الموثوقين للاستعانة بهم في تنفيذ هذه الأنشطة الهامة. وقد تطورت مراكز عمليات الأمن بشكل كبير خلال السنوات القليلة الماضية، حيث نمت من حل المعلومات الأمنية وإدارة الأحداث (SIEM) المُدار إلى تقديم خدمات كشف التهديدات والاستجابة الأمنية المُدارة المتقدمة (MDR). بعض التقنيات الرئيسية التي يتم اعتمادها والعمل بها في هذا المجال هي حلول المعلومات الأمنية وإدارة الأحداث (SIEM)، وأدوات تقييم الثغرات الأمنية (VA)، ومنصات استخبارات التهديدات (TIP)، وتقنيات أمن الشبكات، وأدوات إعداد التقارير، وأدوات التجميع والارتباط، إلخ.

و. إدارة الهوية والوصول

تعد إدارة الهوية والوصول للقوى العاملة الموزعة على نطاق واسع أكثر أهميةً من أي وقت مضى، لا سيما في أوقات اتساع المشهد التكنولوجي. وهنالك حاجة إلى ضمان أن تحفز الهويات الآمنة 36٪ من المؤسسات على اعتماد حلول إدارة الهوية والوصول (IAM) لتأمين دورة حياة الهوية لمستخدميها النهائيين والتكملة بحلول إدارة الوصول المميز (PAM)، وذلك لتعزيز أمن المستخدمين ممن يتمتعون بإمكانية الوصول المميز مثل مشرفي النظم، والمستخدمين السلطويين (Power Users)، إلخ.

أبرز النتائج العالمية

إن تقنيات الأمن الخمسة (5) الناشئة هي مصادقة الأجهزة، وتحليلات سلوك المستخدم، ومنع فقدان البيانات، والتعلم العميق، والسحابة التي سيكون لها تأثير تحويلي على صناعة تكنولوجيا الأمن بشكل عام[14].

السحابة العامة - خيار الاستخدام/التوظيف

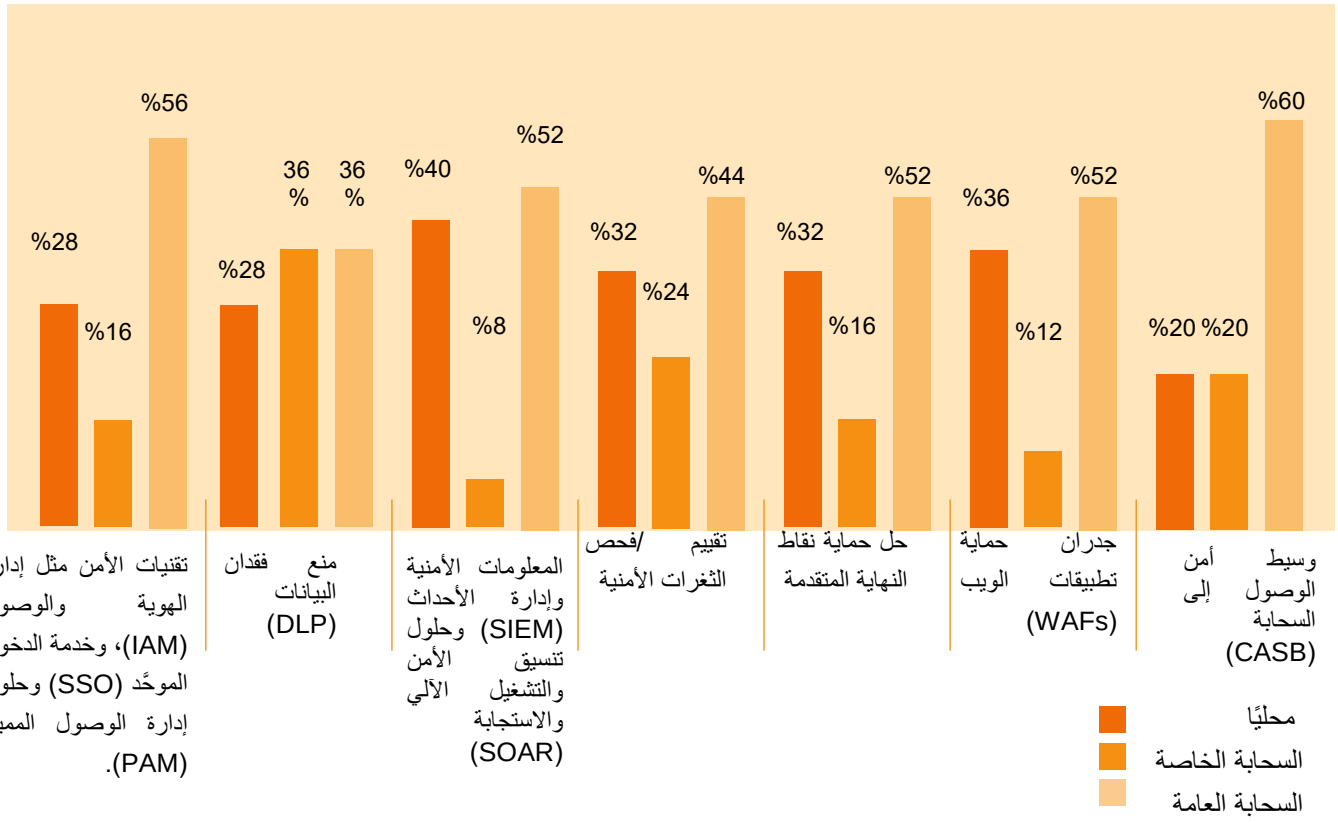
خلال هذه الدراسة، اتضح أن الأمر انتهى بالمؤسسات إلى اعتماد منصات الحوسبة السحابية في شكل أو آخر من نماذج النشر. على الرغم من أن عمليات النشر في السحابة الخاصة تجلب مزيدًا من التحكم والأمن للمؤسسة، فإن تكلفة الحفاظ عليها مرتفعة نسبيًا على المدى البعيد. ومن ثم، فإن المزيد من المؤسسات في دولة الكويت تتبنى نماذج نشر السحابة العامة وتخطط لتوفير حزمة الأمن الخاصة بها في الغالب في بيئة السحابة العامة.

بالنسبة لعدد قليل من تقنيات الأمن مثل حلول المعلومات الأمنية وإدارة الأحداث (SIEM) وحلول تنسيق الأمن والتشغيل الآلي والاستجابة (SOAR)، لا يزال تقييم الثغرات الأمنية وجدران حماية تطبيقات الويب (WAFs)، وإدارة الهوية والوصول (IAM)، ومنع فقدان البيانات (DLP) خياراتٍ مهمة يجب نشرها وإدارتها داخل المؤسسة نظرًا للطبيعة الحساسة للسجلات والتنبيهات التي يجب أن تدار داخليًا من قبل المؤسسات.

يتركز اعتماد السحابة الخاصة لتقنيات الأمن حول نطاق يتراوح من 10٪ – 25 ٪ باستثناء حلول منع فقدان البيانات، حيث تحتاج المؤسسات إلى مراقبة أي بيانات تغادر نطاقها. ومع ذلك تظل السحابة العامة خيار النشر للمؤسسات في الكويت، حيث يخططون لنشر مجموعة تقنيات الأمن الهامة، وتحتفظ تقنية وسيط أمن الوصول إلى السحابة (CASB) بأعلى نسبة وتبلغ 60٪ كخيار للتكنولوجيا التي أصبحت أمرًا واقعيًا عندما يتعلق الأمر بحماية تطبيقات الويب في السحابة. حصلت التقنيات المتعلقة بالهوية، مثل إدارة الهوية والوصول (IAM)، وخدمة الدخول الموحّد (SSO) وحلول إدارة الوصول المميز (PAM)، والتي أصبحت ضرورية لدعم القوى العاملة الموزعة على نطاق واسع، على الحصة الأكبر التالية بنسبة 56٪ على السحابة. يتبع ذلك حلول إدارة التهديدات مثل حلول المعلومات الأمنية وإدارة الأحداث (SIEM) وتنسيق الأمن والتشغيل الآلي والاستجابة (SOAR) بنسبة 52%. مع تحول المزيد من المؤسسات إلى السحابة وإنشاء البنية التحتية الافتراضية لسطح المكتب (VDI) لمستخدميها النهائيين، فإن حماية نقاط النهاية يعتبر أمرًا بالغ الأهمية أيضًا، ومن فإن نحو 52٪ من المؤسسات ستنفق في حلول حماية نقطة النهاية المتقدمة في بيئة السحابة العامة. يتضح أيضًا النمو المتوقع بنسبة 52٪ في السحابة العامة بالنسبة لجدران حماية تطبيقات الويب (WAFs) لضمان الحماية المستمرة في طبقة التطبيق لتطبيقات الويب المهمة للمؤسسات ونشرها في السحابة العامة.
البيئة (البرمجيات المحلية المثبتة على الأجهزة أو السحابة) التي تخطط الشركات لاستخدامها لتوفير حلول الأمن الخاصة بها في عام 2021.

14. Top 5 emerging information security technologies (techbeacon.com)

الجدول 12: إجابات الاستبانات (البرمجيات المحلية المثبتة على الأجهزة والخوادم مقابل حلول أمن السحابة)



أبرز النتائج العالمية

- تتوقع شركة غارتنر أن تنمو أرباح السحابة العامة بنسبة 6.3% عام 2020 بإجمالي أرباح يقارب 258 مليار دولار أمريكي، بزيادة قدرها 15مليار دولار عن العام الماضي[15].
- سينمو سوق البنية التحتية السحابية الخاصة بمعدل أبطأ من سوق الخدمات السحابية العامة، وفقًا لشركة أبحاث السوق (آي دي سي)، لكنه سيستمر في كسب الأهمية في قرارات الاستثمار في تكنولوجيا المعلومات، حيث تسعى المؤسسات إلى بدائل آمنة وموثوقة لنشر مراكز البيانات داخليًا[16].

تغيير البنية الأساسية لأمن المعلومات

استمرت جهود حماية التطبيقات من الضرر الخارجي منذ عقود مع تطور جدران الحماية لأنظمة منع التسلل لمنصات تنسيق الأمن والتشغيل الآلي والاستجابة (SOAR). ومع ذلك ففي الوقت الحالي، في عصر القوى العاملة الموزعة بشكل كبير، يتم توزيع البيانات والموارد على نطاق واسع عبر مراكز البيانات، والأجهزة السحابية والأجهزة المحمولة، فيما لم يعد الأمن المحيط كافياً بعد الآن. بدأت المؤسسات في التحرك ببطء نحو تمكين البنية الأساسية للشبكات المعرفة بالبرمجيات (SDN)، مما أدى إلى خفض التكلفة والتحكم الدقيق في طبقة الشبكة. وهذه القفزة في تكنولوجيا الشبكات سوف تؤدي أيضًا إلى التبخر السريع للمحيط التقليدي الذي نعرفه.

15. https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020
16. https://www.idc.com/getdoc.jsp?containerId=prUS47279621

على الرغم من أن مفهوم إطار عمل الثقة الصفرية (Zero Trust Framework) كان موجودًا منذ فترة فإن اعتماده كان بطيئًا بسبب مقاومة التغيير. ومع ذلك، فإن تبني السحابة والشبكات المُعرفة بالبرمجيات (SDN) جعلها نقطة محورية للاهتمام. تم تصميم إطار عمل الثقة الصفرية (Zero Trust Framework) من دون أخذ أي تقنية في الاعتبار ولكن ما هي الطريقة المُثلى لتصميم البنية الأساسية لضمان أن تكون الثقة ضمنية حتى داخل الشبكة.

هيكل الثقة الصفرية (Zero Trust Architecture)

الثقة الصفرية هو مصطلح يطلق على مجموعة متطورة من نماذج أمان الشبكة التي تنقل دفاعات الشبكة من محيط الشبكة الواسعة إلى التركيز الضيق على مجموعات فردية أو صغيرة من الموارد. استراتيجية هيكل الثقة الصفرية (Zero Trust Architecture) هي إحدى الاستراتيجيات التي لا توجد فيها ثقة ضمنية ممنوحة للأنظمة بناءً على موقعها الفعلي أو موقع الشبكة (أي شبكات المنطقة المحلية مقابل الإنترنت). يمنح الوصول إلى موارد البيانات حينما تكون هناك حاجة إلى تلك الموارد، ويتم إجراء المصادقة (للمستخدم والجهاز) قبل إنشاء الاتصال. إن استراتيجية هيكل الثقة الصفرية هي استجابة لاتجاهات الشبكة المؤسسية التي تشمل المستخدمين البعيدين والأصول القائمة على السحابة التي لا تكون موجودة داخل

يمضي إطار العمل قُدمًا حتى يشير ضمنيًا إلى أن شبكة الشركة قد تم اختراقها بالفعل علاوة على ضرورة التحقق من جميع الاتصالات لتجنب أي حركة جانبية من الخصوم. لمواجهة التهديدات في وقت حرج مثل الوقت الحالي، ينبغي النظر في إطار عمل الثقة الصفرية (Zero Trust Framework) وتنفيذه لحماية المؤسسات ونطاقها من الهجمات الأوسع أنتشارًا.

حدود الشبكة المملوكة للمؤسسة. تركز الاستراتيجية على حماية الموارد، وليس قطاعات الشبكة، حيث لم يعد يُنظر إلى موقع الشبكة على أنه المكون الرئيسي للوضع الأمني للمورد.
الانتقال إلى هيكل الثقة الصفرية هو رحلة تحتاج إلى التفكير والتخطيط والتنفيذ الجيد على مراحل متعددة، لأنها مزيج من التكنولوجيا والعمليات. تركز الثقة الصفرية على حماية البيانات باعتبارها موضوعها المركزي وتشمل عناصر أخرى من الشبكة والبنية التحتية والتطبيقات والهوية والوصول للبيئات المحلية أو السحابية.

الشكل 5: تنفيذ هيكل الثقة الصفرية

وبينما خطط عدد قليل من المؤسسات في دولة الكويت لاعتماد الثقة الصفرية على مدى السنتين أو الثلاثة المقبلة، فقد شهدنا معدل تبن أسرع من قبل المؤسسات البارزة الأخرى في الخليج والعالم. لذا، فنحن

نوصي المؤسسات في دولة الكويت أن تعتمد هياكل مثل الثقة الصفرية أو غيرها مع اعتماد المبادئ ذاتها على مدار العامين المقبلين.

17. Reference – NIST 800-207 – Zero Trust Architecture

وضع برنامج الأمن والاستراتيجية

تعد استراتيجية الأمن السيبراني أمرًا حيويًا كنقطة انطلاق لمساعدة المؤسسات على اتباع نهج طويل الأجل للأمن وتصميم خارطة طريق لرد الفعل الحالي للنهج الاستباقي. يجب ألا تتماشى استراتيجية الأمن الخاصة بالمؤسسة مع رؤية المؤسسة ورسالتها وأهدافها فحسب، بل أيضًا أن تتماشى مع استراتيجية الأمن السيبراني الشاملة للبلد نفسه. يعتبر توضيح أهداف العمل أمرًا أساسيًا مثل التعرف على جهات التهديد عند تصميم الاستراتيجية الأمنية.

يذهب تعريف الاستراتيجية إلى أعمق بكثير من إنشاء خارطة طريق لعدد من المشاريع لتنفيذها داخل المؤسسات. حيث يجب أن تبدأ نقطة البداية بتحليل عميق للوضع الراهن للأعمال والتهديدات التي تواجهها المؤسسة. يوفر التحليل مؤشرات تؤدي إلى إنشاء الأهداف بناءً على رؤية المؤسسة ورسالتها ورغبة أصحاب المصلحة في المخاطرة (Risk Appetite) والفرص. يجب تصميم برنامج وإستراتيجية الأمن الخاصة بكل مؤسسة وفقًا لاستراتيجية وخطط العمل الخاصة بها. يعد فهم سياق العمل أحد العناصر أو المدخلات الجوهرية لاستراتيجية الأمن ذات الصلة. تقطع الاستراتيجيات الأمنية شوطًا طويلاً بالنسبة للمؤسسات لأنها تساعدها على مواءمة رؤيتها مع رؤية الأمن السيبراني.

الخطوات الرئيسية لوضع استراتيجية الأمن الخاصة بكم:

الشكل 6: مراحل إعداد استراتيجية الأمن

نظرة ثاقبة لكل الخطوات عند وضع استراتيجية الأمن الخاصة بكم:

1. التخطيط الاستراتيجي

من الثابت الآن أن الأمن لم يعد وظيفة قائمة على تكنولوجيا المعلومات، ولكنه ضروري لضمان الأمن عبر خطوط الخدمة التي تقدمها المؤسسة. ومن ثم، يجب مواءمة أهداف الأمن والعمل، وهذا يتطلب فهمًا ليس فقط للتهديدات الأمنية والقدرات ولكن أيضًا فهمًا عميقًا لبيئة الأعمال والأهداف المؤسسية. من خلال موازنة الاحتياجات الأمنية مع استثمارات الأعمال الأخرى، يمكن النظر إلى الأمن على أنه شريك في الأعمال وليس مجرد مركز تكلفة.

2. الأهداف الاستراتيجية

تحدد المهمة والرؤية والأهداف التي تريد تحقيقها وتضع القواعد الأساسية حول سبب وجود المؤسسة وما ترغب في تحقيقه. وبالمثل، فإن بيان المهمة والرؤية التي سبقت صياغته جيدًا للأمن يساعد على توجيه القرارات التي يتعين على إدارة الأمن اتخاذها. كما تساعد الأهداف على وضع أهداف واضحة ودقيقة لفريق الأمن على المدى البعيد ويجب إعادة النظر فيها وتحديثها بشكل دوري.

3. وضع البرامج

يستلزم وضع برنامج الأمن السيبراني انتباه المؤسسات في اختيار اللوائح والأطر المحلية والدولية المناسبة كخط أساس عند إنشاء برنامج الأمن السيبراني الخاصة بها. توجد أطر عمل متعددة تنطوي على مجموعة واسعة من مجالات التكنولوجيا للمؤسسات وتعمل كمبدأ توجيهي رائع.

يمكن للمؤسسات أيضًا إنشاء أطر أمن مخصصة لمشهدها التكنولوجي المعقد. يجب أن يقترن تنفيذ إطار العمل ببرنامج قوي لإدارة المخاطر يمكنه أن يتناول مخاطر التكنولوجيا والأعمال فيما يتعلق بالأمن السيبراني. قد تساعد دورة حياة إدارة المخاطر على تحديد وإدارة المخاطر وخطط التخفيف لخفض المخاطر إلى مستويات مقبولة.

4. الوضع الراهن مقابل الوضع المستهدف

تقييم الوضع الراهن هو عندما يتم أخذ إطار العمل كخط أساس وتقوم المؤسسة بتقييم مدى نضج الضوابط الحالية الموجودة بالفعل. يساعد ذلك المؤسسات على فهم حالة الأمن السيبراني بها والقدرات الموجودة لحمايتها من الجهات الفاعلة في التهديدات. على النقيض من ذلك، فإن الوضع المستهدف هو حالة الأمن السيبراني التي يريد فريق الأمن تحقيقها في فترة زمنية محددة.

قد تختار المؤسسات تقسيم المبادرات الهامة وتطويرها على مدى فترة معينة.

تؤدي التكنولوجيا دورًا حاسمًا. وفي هذه المرحلة تحتاج المؤسسات إلى المواءمة والتوافق مع المعايير العالمية، مثل (المعهد الوطني للمعايير والتقنية (NIST) والثقة الصفرية (Zero Trust). سوف تساعد خارطة الطريق أو رحلة التكنولوجيا تجاه الثقة الصفرية على خفض المخاطر نظرًا لاعتماد التقنيات الجديدة والتحول الرقمي.

5. التقييم والتوكيد

تعتبر القياسات الملموسة طريقة رائعة للمؤسسات لتحديد الأهداف والغايات التي وضعتها إدارة الأمن حتى يتسنى تحقيقها. تضع المؤسسات مؤشرات الأداء الرئيسية (KPIs) التي تتم مراجعتها على أساس دوري لتقييم إداء الفريق والتكنولوجيا الموجودة. ومع ذلك، فمن المهم تحديد مؤشرات الأداء الرئيسية (KPIs) بعناية وتوثيقها مع القابلية الواقعية لتحقيقها ومراعاة الطبيعة الاستراتيجية والتكتيكية والتشغيلية. وفي النهاية، من الأفضل دائمًا للمؤسسات إجراء تقييم خارجي مستقل لبرامجها الأمنية لضمان التأكيد وتحديد مناطق التحسين الرئيسية للتطوير المستمر.

مُلخص التوصيات

إحدى الملاحظات الأساسية التي أسفرت عنها هذه الدراسة هي أنه على الرغم من تحدي الجائحة لقدرات قادة تكنولوجيا المعلومات والأمن في جميع أنحاء المنطقة على دعم أعمالهم، فقد استجاب قادة التكنولوجيا ونجحوا في تبني الوضع الطبيعي الجديد، والتركيز بصورة سريعة على تقليل الخسارة في الإنتاجية والموظفين. يجب تقدير الدقة التي استجاب بها قادة التكنولوجيا والأعمال في المؤسسات على المدى القصير والكيفية التي يتصورون من خلالها المستقبل الرقمي لمؤسساتهم.

وفيما يلي عرض لأبرز التوصيات الرئيسية التي نرغب في تنفيذها:

1. **وضع استراتيجية الأمن**

أصبح وضع الاستراتيجيات الأمنية بمثابة نقطة البداية الأساسية للمؤسسات لتمكين الأعمال الرقمية الآمنة في المستقبل.

يجب أن تستثمر المؤسسات في بناء خطة استراتيجية أمنية لمدة 3 سنوات يمكن أن تأخذ في الاعتبار رؤية المؤسسة ورسالتها وتُكملها.

2. **دورة حياة المخاطر المستمرة**

واجه بعض المستخدمين الأوائل لتقنيات معينة مشكلات تتعلق بالأمن والتوافر بسبب عدم بذل العناية الواجبة. على الرغم من أن تجنب خسارة الإنتاجية هو الدافع الرئيسي وراء الاعتماد السريع للتقنيات، فإنه لا يزال يتعين على المؤسسات اتباع نهج قائم على إدارة المخاطر عند التفكير في حل جديد يتم إدخاله في بيئة الإنتاج الخاصة بها لضمان تخفيف مستوى المخاطر الأمنية ومعالجتها بصورة استباقية.

3. **اعتماد ونضج أطر عمل الأمن**

لفترة طويلة، كان معيار الأيزو 27001 هو الاختيار الرئيسي لمعيار الأمن السيبراني عند تنفيذ نظام إدارة أمن المعلومات (ISMS) داخل المؤسسة. ومع ذلك، يعتمد عالم ما بعد الجائحة بشكل كبير على التقنيات التي تتجاوز بيئة تكنولوجيا المعلومات التقليدية مثل إنترنت الأشياء (IoT)، والسحابة، والجيل الخامس وما إلى ذلك. لمواجهة هذا التحدي، يجب على المؤسسات التفكير في تعزيز برامج الأمن السيبراني الخاصة بها من خلال أطر الأمن السيبراني الناضجة مثل إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا (NIST CSF) ومصفوفة ضوابط الخدمات السحابيّة لأمن الحوسبة السحابيّة (CSA CCM)، والأيزو 27701 (الخصوصية)، إلخ. وكلها تهدف إلى إنشاء إطار رقابي موحد ومفصل ومصمم حسب الطلب.

4. **المواءمة مع هيكل الثقة الصفرية (Zero Trust Architecture) أو ما يماثلها**

في بيئات العمل الديناميكية، تحتاج التقنيات الجديدة إلى أن تتكيف المؤسسات مع خارطة طريق التكنولوجيا التي تستند إلى سياسات وعمليات فاعلة. بينما تحتاج المؤسسات إلى تعزيز النضج حول السحابة والبيانات والهوية والعمليات الأمنية، فإن هذه تعد اللبنات الأساسية لتنفيذ هياكل الثقة الصفرية (Zero Trust Architecture).

- **تقييم أمن السحابة** - أصبحت السحابة بمثابة الركيزة المحورية لمشاريع التحول الرقمي في دولة الكويت، ومع تزايد اعتماد عمليات النشر السحابية العامة والخاصة، تحتاج المؤسسات إلى التأكيد على تقييم ضوابط الأمن مسبقًا. تبدأ هذه العملية من مرحلة التقييم حيث يجب تقييم المخاطر المناسبة مع استكمال ضوابط التخفيف الخاصة بها لتكون مستويات المخاطر المتبقية مقبولة لدى المؤسسة.
- **إعطاء الأولوية لأمن البيانات وحوكمة الهوية** - يعد تخطيط تكنولوجيا الأمن وتصميم تعزيز الهيكل النهائي أمرًا ضروريًا لقدرة المؤسسات على بناء الثقة مع عملائها النهائيين. إن متطلبات اللوائح المعقدة، والتطبيقات كثيفة البيانات، والخصوصية حسب التصميم، والأمن، إلخ، هي المجالات التي تتطلب نضجًا أمنيًا مع مزيج من التحسينات التقنية ومجموعات قواعد الأعمال والعمليات. وأمن البيانات والهوية هي ركائز جوهرية في

استراتيجية أمن المؤسسة. يجب أن يكون الجمع بين هذه المناطق المهمة هو أحد الاعتبارات الرئيسية للمؤسسات التي تخطط لتحسين نضج تقنياتها الحالية.

الاستثمار في العمليات الأمنية - اتسع مشهد التهديدات اليوم بشكل كبير فيما تكافح المؤسسات من أجل جذب موظف متخصص في مجال الأمن بحيث يمكن أن يساعدها على ضمان اليقظة الدائمة والمراقبة المستمرة لأصولها. وبينما يتزايد عدد الهجمات وتصبح أكثر تعقيدًا، تظل فرص خسارة البيانات أو العلامات التجارية أكثر انتشارًا. ولمجابهة تلك التهديدات والتحديات، يجب على المؤسسات ان تنظر إما في بناء مراكز عمليات الأمن الخاصة بها أو الدخول في شراكة مع مزودي خدمات الأمن الموثوقين الذين تتوافر لديهم القدرة على إدارة تلك التهديدات.

تمتلك الهيئات التنظيمية في دولة الكويت خططًا مستقبلية، ومع ذلك، فعليهًا أن تبذل الكثير عند مقارنتها بالجهات التنظيمية في منطقة الخليج وعلى الصعيد العالمي أيضًا. يجب أن تكون هناك أطر عمل إضافية حول برامج الأمن، وأمن السحابة، وأمن التكنولوجيا التشغيلية، وقوانين خصوصية البيانات لتقديم التوجيه للقطاع الأهلي. إن وجود برنامج قوي لوضع معايير الأمن، وإصدار وتحديد قابلية تطبيقها، ومراقبة وقياس أداء المؤسسات بشكل دوري سيساعد بشكل كبير على زيادة النضج الأمني.

مُلحق

الجدول 13: قائمة اللوائح على مستوى دول مجلس التعاون الخليجي

الأنظمة / اللوائح على مستوى دول مجلس التعاون الخليجي	البلد	المصدر	التوزيع
نظام مكافحة الجرائم المعلوماتية	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
إطار عمل هيئة السوق المالية	المملكة العربية السعودية	هيئة السوق المالية	انتقائي
الإطار التنظيمي للأمن السيبراني (هيئة الاتصالات وتقنية المعلومات)	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
دليل الشركات لخدمات الحوسبة السحابية	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
دليل الجهات الحكومية لخدمة الحوسبة السحابية	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
دليل مقدمي الخدمات السحابية	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
الإرشادات التوجيهية بشأن التخطيط للتعافي من كوارث تكنولوجيا المعلومات والاتصالات	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
إطار العمل التنظيمي بشأن التخطيط للتعافي من كوارث تكنولوجيا المعلومات والاتصالات	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
إطار العمل التنظيمي لإنترنت الأشياء (IoT)	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
الضوابط الأساسية للأمن السيبراني - الهيئة الوطنية للأمن السيبراني (NCA)	المملكة العربية السعودية	الهيئة الوطنية للأمن السيبراني (NCA)	عام
إطار عمل استمرارية الأعمال لمؤسسة النقد العربي السعودي (SAMA)	المملكة العربية السعودية	مؤسسة النقد العربي السعودي	
إطار الأمن السيبراني لمؤسسة النقد العربي السعودي	المملكة العربية السعودية	مؤسسة النقد العربي السعودي	عام
إطار العمل التنظيمي للحوسبة السحابية	المملكة العربية السعودية	هيئة الاتصالات وتقنية المعلومات	عام
قانون رقم (16) لسنة 2014 بشأن حماية معلومات ووثائق الدولة	البحرين	الحكومة الإلكترونية	عام
قانون رقم (60) لسنة 2014 بشأن جرائم تقنية المعلومات	البحرين	الحكومة الإلكترونية	عام
قانون رقم (2) لسنة 2017 بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات	البحرين	الحكومة الإلكترونية	عام
قانون رقم (30) لسنة 2018 بإصدار قانون حماية البيانات الشخصية	البحرين	الحكومة الإلكترونية	عام

الأنظمة / اللوائح على مستوى دول مجلس التعاون الخليجي	البلد	المصدر	التوزيع
هيئة أبوظبي الرقمية	الإمارات العربية المتحدة / أبو ظبي	هيئة أبوظبي الرقمية	انتقائي
معيار - مواصفات إدارة استمرارية الأعمال	الإمارات العربية المتحدة	الهيئة الوطنية لإدارة الطوارئ والأزمات	عام
الإرشادات التوجيهية لمعيار إدارة استمرارية الأعمال	الإمارات العربية المتحدة	الهيئة الوطنية لإدارة الطوارئ والأزمات	عام
قانون حماية البيانات لسنة 2020 لمركز دبي المالي العالمي (DIFC)	الإمارات العربية المتحدة/دبي	مركز دبي المالي العالمي	عام
لوائح حماية البيانات	الإمارات العربية المتحدة/مركز دبي المالي العالمي	مركز دبي المالي العالمي	عام
قانون تنظيم نشر وتبادل البيانات في إمارة دبي	الإمارات العربية المتحدة/دبي	مدينة دبي الذكية	عام
سياسة بيانات دبي	الإمارات العربية المتحدة/دبي	مدينة دبي الذكية	عام
معيار بيانات دبي	الإمارات العربية المتحدة/دبي	مدينة دبي الذكية	عام
مرسوم بقانون اتحادي رقم (2) لسنة 2011	الإمارات العربية المتحدة	الهيئة الوطنية لإدارة الطوارئ والأزمات	عام
مرسوم بقانون اتحادي رقم 5 لسنة 2012 بشأن مكافحة الجرائم السيبرانية	الإمارات العربية المتحدة	هيئة تنظيم الاتصالات والحكومة الرقمية	عام
القانون الاتحادي رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية	الإمارات العربية المتحدة	هيئة تنظيم الاتصالات والحكومة الرقمية	عام
السياسة العامة لقطاع الاتصالات في الإمارات العربية المتحدة 2006 - 2010	الإمارات العربية المتحدة	هيئة تنظيم الاتصالات والحكومة الرقمية	عام
لوائح أمن المعلومات - الإصدار 2.0 (ISR)	الإمارات العربية المتحدة/دبي	كلية دبي للمحادثة الانجليزية	انتقائي
السياسة التنظيمية - إنترنت الأشياء (IoT)	الإمارات العربية المتحدة	هيئة تنظيم الاتصالات والحكومة الرقمية	عام
الإجراء التنظيمي - إنترنت الأشياء (IoT)	الإمارات العربية المتحدة	هيئة تنظيم الاتصالات والحكومة الرقمية	عام
وثيقة سياسة تعريف الخدمات الذكية	الإمارات العربية المتحدة/دبي	مدينة دبي الذكية	عام
معيار تأكيد المعلومات - الإمارات العربية المتحدة	الإمارات العربية المتحدة	هيئة تنظيم الاتصالات والحكومة الرقمية	عام
الإطار الاستراتيجي للأمن السيبراني للقطاع المصرفي	الكويت	بنك الكويت المركزي	عام

إطار كأس العالم لكرة القدم (فيفا)	قطر	اللجنة العليا للمشاريع والإرث (SCDL)	انتقائي
الإطار الوطني لضمان أمن المعلومات	قطر	الفريق القطري للاستجابة لطوارئ الحاسب "كيوسرت" (Q-CERT)	عام
قانون حماية البيانات القطري	قطر	وزارة المواصلات والاتصالات	عام

مؤسسة الكويت للتقدم العلمي
Kuwait Foundation for the Advancement of Sciences

WWW.KFAS.ORG