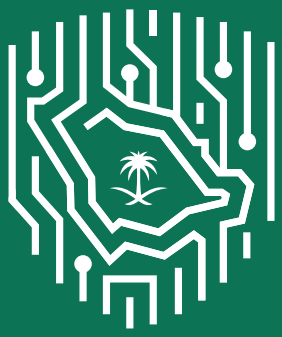
النموذج السعودي لتعزيز صمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين ٢٠٢١م

تصنيف الوثيقة: متاح
إشارة المشاركة: أبيض



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تعمل الهيئة الوطنية للأمن السيبراني منذ إنشائها؛ مع الجهات الحكومية وجهات القطاع الخاص، والشركاء الدوليين على تعزيز الأمن السيبراني في المملكة العربية السعودية بهدف حماية مصالحها الحيوية وأمنها الوطني، والبنى التحتية الحساسة، والقطاعات ذات الأولوية والخدمات، والأنشطة الحكومية؛ بما يتسق مع رؤية المملكة 2030. فقد تمثلت الرؤية الإستراتيجية التي طورتها الهيئة الوطنية للأمن السيبراني في (فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار) ، لتعكس الطموح الإستراتيجي للمملكة، بطريقة توازن بين الأمن والثقة والنمو.

يسلط هذا التقرير الضوء على الجهود التي اتخذتها الجهات المعنية المختلفة على مستوى المملكة العربية السعودية؛ لتأمين أصحاب المصلحة، والأصول ذات العلاقة بأحداث مجموعة العشرين؛ خلال فترة رئاسة المملكة لمجموعة العشرين، والقمة الافتراضية للقادة. ونود في الهيئة الوطنية للأمن السيبراني أن نؤكد على شكرنا الكبير لوزارة الاتصالات وتقنية المعلومات، والهيئة السعودية للبيانات والذكاء الاصطناعي، وكذلك الأمانة العامة لمجموعة العشرين، والشركة السعودية لتقنية المعلومات(سايت)، وإس تي سي وذلك على إسهامهم في رفع مستوى جاهزية الفضاء السيبراني السعودي وصموده خلال فترة رئاسة المملكة لمجموعة العشرين.

المحتويات

الملخص التنفيذي

في ظل التحول الرقمي الكبير الذي يشهده العالم في وقتنا الحالي، أصبح الأمن السيبراني ضرورة ملحة تتطلب اهتمامنا الفوري. ونظرًا لجائحة فيروس كورونا المستجد (كوفيد-19)، عُقدت معظم الفعاليات افتراضياً عبر المنصات الرقمية خلال سنة رئاسة المملكة العربية السعودية لمجموعة العشرين، مما غيّر من طبيعة التهديدات وفرض تحديات جديدة تتعلق بالأمن السيبراني حيث توجب التعامل معها بشكل سريع.

إن مجموعة العشرين عبارة عن منتدى دولي يجمع أكبر اقتصادات العالم، وتمثل الدول الأعضاء في المجموعة أكثر من 80% من الناتج المحلي الإجمالي العالمي و75% من حجم التجارة العالمية و60% من التعداد السكاني العالمي. وبالنظر إلى مستوى الأطراف المشاركة ودرجة أهميتها، فضلاً عن الطبيعة الرقمية للتواصل، تبرز الأهمية الكبيرة لتعزيز الأمن السيبراني خلال رئاسة مجموعة العشرين.

في عام 2020م، تسلّمت المملكة العربية السعودية رئاسة مجموعة العشرين. وفي سبيل ترسيخ أطر التعاون الدولي لتحقيق صمود الأمن السيبراني في الأنظمة الاقتصادية العالمية، عمل فريق عمل الاقتصاد الرقمي على إدراج أولوية بعنوان "الأمن في الاقتصاد الرقمي"، بما يتوافق مع الأهداف العامة لسنة الرئاسة.

علاوةً على ذلك، كانت جاهزية وصمود الأمن السيبراني في غاية الأهمية لنجاح سنة الرئاسة، لا سيما مع انعقاد معظم الفعاليات افتراضياً عبر المنصات الرقمية أول مرة على الإطلاق، بسبب جائحة فيروس كورونا المستجد.

وقد أدى تحويل رئاسة مجموعة العشرين إلى تجربة رقمية بالكامل إلى تغيير طبيعة التهديدات التي واجهها منظمو قمة المجموعة وفرض تحديات جديدة تتعلق بالأمن السيبراني لا بد من التصدي لها بشكل سريع.

حصلت المملكة العربية السعودية على المرتبة **الأولى** بين الدول العربية في مؤشر الأمن السيبراني العالمي (GCI) لعام 2020م والمرتبة **الثانية** عالمياً بين 194 دولة.

وللتغلب على هذه التحديات، فقد اعتمدت المملكة على خبرتها في الأمن السيبراني واستفادت من أفضل الممارسات الدولية. وقد تولت الهيئة الوطنية للأمن السيبراني قيادة هذه الجهود، باعتبارها الجهة الحكومية المسؤولة عن الأمن السيبراني في المملكة والتي بدورها طورت برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين.

ويعتمد البرنامج على نموذج سعودي يُعنى بتأمين الجهات المعنية والأصول المستخدمة في تنظيم فعاليات مجموعة العشرين على مدار سنة رئاسة المجموعة، وصولاً إلى القمة الافتراضية لقادة الدول الأعضاء.

ورغم وجود بعض الأمثلة على كيفية تأمين الفعاليات الضخمة، إلا أن الساحة الدولية تفتقر لوجود منهجيات معترف بها يمكن الاسترشاد بها في تأمين فعالية بهذا الحجم بشكل فعال. لهذا السبب، كان من الضروري تصميم استراتيجية لنموذج تعزيز الأمن السيبراني لدى الهيئة الوطنية للأمن السيبراني خلال سنة رئاسة المملكة مجموعة العشرين.

ويوضح هذا التقرير تجربة الهيئة الوطنية للأمن السيبراني في تأمين فعاليات مجموعة العشرين من منظور الأمن السيبراني بالتعاون مع ذراعها التقني، الشركة السعودية لتقنية المعلومات (سايت)، ومقدمي الخدمات، بهدف تقديم أفكار ورؤى قيمة يمكن للدول المستضيفة لفعاليات مجموعة العشرين في المستقبل ولغيرها من الجهات المنظمة للفعاليات الكبرى الاستفادة منها.

المبادئ - اتّبع برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين النموذج السعودي الذي تم تصميمه والذي يستند إلى ثلاثة مبادئ: الشمولية، والصمود، والتعاون.

المنهجية - وفقًا لمنهجية شاملة تستفيد من

التجارب الدولية السابقة، تمت هيكلة برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين باستخدام النموذج السعودي الذي تم تصميمه والذي يتكون من مستويين (الشكل 1)، مع التركيز على إمكانية التكيّف والتحسين المستمر.

المستوى الأول - استهدف تعزيز جاهزية وصمود الأمن السيبراني على مدار سنة رئاسة المملكة لمجموعة العشرين.

ركز هذا المستوى على تحديد الأدوار والمسؤوليات، وتحديد أصول تقنيات المعلومات، وتطوير الضوابط للأمن السيبراني. وقد أتاح هيكل الحوكمة هذا لمنظمي فعاليات مجموعة العشرين تقييم احتياجات الأمن السيبراني وتنفيذ عمليات الأمن السيبراني و تعزيز الوعي بالأمن السيبراني على مدار سنة رئاسة المجموعة.

المستوى الثاني - ركّز على تعزيز جاهزية وصمود الأمن السيبراني خلال القمة الافتراضية لقادة الدول الأعضاء.

انعقدت هذه القمة افتراضيًا لأول مرة في نهاية سنة الرئاسة. وبالنظر إلى مستوى التعقيد الرقمي الإضافي الناتج عن تأمين قمة مجموعة العشرين لعام 2020م، تم تفعيل النموذج بما يتناسب مع المتطلبات المحددة للقمة الافتراضية لقادة الدول الأعضاء. وقد اشتمل ذلك على تحديد أدوار ومسؤوليات جديدة وتعزيز قدرات الأمن السيبراني.

تم إجراء أكثر من **120 تقييمًا** مختلفًا للأمن السيبراني لتقييم مدى جاهزية وصمود الأمن السيبراني على مدار سنة الرئاسة.

كما تمت مراقبة جميع أصول تقنيات المعلومات والمنصات عن كثب، مع تطبيق خطة للحد من مخاطر الهجمات السيبرانية. كذلك، تم تشكيل فريق متخصص للاستجابة للحوادث بهدف تعزيز جهود الفرق الموجودة بالفعل.

وأخيرًا، تم إجراء العديد من التمارين السيبرانية المخصصة بما يتناسب مع القمة الافتراضية لقادة الدول الأعضاء بهدف إعداد سبل الاستجابة للهجمات السيبرانية المحتملة وتحقيق التكامل بينها.

اشتمل كل مستوى على 4 مسارات (الشكل 1):

المسار الأول: حوكمة البرنامج – استند الإشراف على البرنامج إلى آلية تنسيق مركزية للتواصل والتفاعل مع الجهات المعنية الرئيسية، ومراقبة العمليات التشغيلية للبرنامج.

وقد تم تحديد الأدوار والمسؤوليات وتقنينها وتخصيصها بما يتناسب مع الأهداف المحددة للمنهجية ذات المستويين. وتكوّن هيكل حوكمة البرنامج وآليات الإشراف عليه من اللجنة التنفيذية، و فريق برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين، وإدارة الأمن السيبراني في الأمانة السعودية لمجموعة العشرين.

كانت **إدارة الأمن السيبراني في الأمانة السعودية لمجموعة العشرين** هي المسؤولة عن دعم الأمانة في تنفيذ برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين والتنسيق له بصفة يومية.

وفي نهاية المطاف، فقد مكّن هيكل الحوكمة الشامل الجهات المعنية من تعزيز الكفاءة التشغيلية مع التنسيق فيما بينها في الوقت نفسه.

المسار الثاني: التقييمات السيبرانية – استهدفت تلك التقييمات تحديد وإدارة أي مخاطر أو ثغرات في الأصول ضمن نطاق التقييم. وتضمّن ذلك تقييمات المخاطر، واختبارات الاختراق، وتقييمات الثغرات، وتقييمات الاختراق السيبراني، وتقييمات الالتزام بضوابط الأمن السيبراني، ومراجعة

إعدادات ومعمارية الأمن السيبراني ومراجعة صلاحيات وصول المستخدمين، وقد تم العمل على ذلك بالتعاون مع الذراع التقني للهيئة، الشركة السعودية لتقنية المعلومات (سايت)، ومقدمي الخدمات.

المسار الثالث: العمليات السيبرانية – تم تحديد عمليات الأمن السيبراني المشمولة في البرنامج وتنفيذها على المستويين، ففي البداية تم تنفيذها طوال سنة رئاسة مجموعة العشرين، ثم تم تعزيزها استعدادًا للقمة الافتراضية لقادة الدول الأعضاء. وقد اشتملت تلك العمليات على نمذجة التهديدات السيبرانية، ومراقبة الأمن السيبراني، والاستجابة للحوادث (وخضع كل منها للتقييم المستمر بهدف تعزيز جاهزية وصمود الأمن السيبراني للبرنامج ككل).

المسار الرابع: التوعية بالأمن السيبراني والتمارين السيبرانية – تم تطوير حملات توعية وورش عمل وتمارين تدريبية، مثل التمارين السيبرانية، استرشادًا بالمنهجية ذات المستويين. وقد خُصّصت تلك الأنشطة ليشارك فيها جميع موظفي الأمانة السعودية لمجموعة العشرين والجهات المعنية الرئيسية.

الشكل 1

الدروس المستفادة

هناك العديد من الدروس المستفادة والتوصيات المستخلصة من تجربة الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين:

المشاركة والدعم القيادي – مكّنت القيادة الرشيدة للمملكة الأمانة السعودية لمجموعة العشرين من خلال حشد الموارد والقدرات اللازمة لها، وكان الدعم المقدم منها جوهريًا لضمان نجاح النموذج وتحقيق أهداف برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين.

قيمة البيانات والحوكمة وتصميم النموذج – يجب جمع وتوثيق البيانات والمعلومات عن تجارب الدول التي سبق لها استضافة الفعاليات الكبرى بهدف دعم التطوير في مجال الأمن السيبراني. ومن شأن تحليل هذه البيانات أن يساعد في تحديد الجوانب الأساسية التي قد تحتاج إلى كفاءات وخبرات إضافية. ويمكن توفير بعض تلك الخبرات من خلال تشكيل فريق من الجهات المعنية الوطنية والدولية – يضم أطرافًا خارجية – وتحديد الأدوار والمسؤوليات المنوطة بها لتحقيق التكامل بين المجالات المختلفة. فعلى سبيل المثال، تم إنشاء إدارة للأمن السيبراني ضمن الأمانة السعودية لمجموعة العشرين والحرص على أن يكون للأمن السيبراني دور أساسي على المستويين الإداري والتشغيلي، وبالتالي يمكن الاستفادة من ذلك كنموذج مرجعي للدول التي ستتسلم رئاسة مجموعة العشرين في المستقبل.

الحاجة للمرونة والتنسيق مع الشركاء – قد تقع أحداث غير متوقعة، ومن المفترض وضع ذلك في الحسبان عند تصميم أي نموذج قادر على الصمود. ويلزم توافر المرونة لإشراك الجهات المعنية الجديدة بشكل سريع واتخاذ القرارات التنفيذية في الوقت المناسب وتعزيز الكفاءات ومراقبة قدرات الأمن السيبراني.

التحضير المبكر وإمكانية التوسع في الجهود – يجب أن تكون جهود الأمن السيبراني مناسبة لتأمين جميع عناصر فعاليات مجموعة العشرين، وذلك بالنظر إلى حجم الاجتماعات والفعاليات وورش العمل المنعقدة على مدار العام. كذلك من الضروري تعزيز الجهود التنسيقية التي تبذلها الأمانة لضمان اتباع

منهجية متسقة ومستدامة في التعامل مع الأمن السيبراني. كما يجب تشكيل فرق للاستجابة للحوادث خلال فعاليات مجموعة العشرين بالكامل، مع عدم الإخلال في التركيز بشكل خاص على الفعاليات الحيوية كقمة القادة. كما أن التوسع في قدرات الاستجابة للحوادث يمكن أن يمنح هذه الفرق القدرة على الاستجابة للعديد من الحوادث في وقت واحد. وتقتضي أفضل الممارسات البدء بالاعتماد على الخطط والقدرات والمنهجيات القائمة، إذ يمكن تخصيصها وتعزيزها لتتناسب مع ظروف معينة.

إدارة النطاق – من الخطوات الأساسية في تأمين أي فعالية كبرى أن يتم تحديد الجهات المعنية المباشرة وغير المباشرة. ويشمل ذلك أصول تقنية المعلومات وتنظيم الفعاليات، والتي يجب تحديد الجهات المسؤولة عنها بوضوح لضمان استيعاب الجهات المعنية لأدوارها ومسؤولياتها. وقد تم استخدام منهجية مركزة ومتعددة المستويات لمراقبة وحماية الأمانة السعودية لمجموعة العشرين. علاوةً على ذلك يجب تحديد الارتباطات الخارجية والأطراف الثالثة وسلاسل الإمداد، بالإضافة للأمانة السعودية لمجموعة العشرين، بنظرة شمولية عن مواقعها الجغرافية. وبالنظر إلى احتمال تفاوت قدرات ومهارات الأمن السيبراني باختلاف الجهات المشاركة في منظومة مجموعة العشرين ككل، إلا أنه يجب وضع مستويات نضج الأمن السيبراني وحماية البنية التحتية لدى تلك الجهات في الاعتبار. ويمكن التعامل مع مستويات نضج الأمن السيبراني المختلفة لدى تلك الجهات باتخاذ إجراءات للحد من المخاطر وتعزيز القدرات.

أهمية التقييمات السيبرانية المنتظمة – من خلال التقييمات المنتظمة، يمكن للمتخصصين المسؤولين عن الأمن السيبراني لفعاليات مجموعة العشرين تحديد الثغرات في الأصول بشكل فوري واتخاذ الإجراءات اللازمة للحد من المخاطر. وقد تضمَّن النموذج السعودي مجموعة من التقييمات (مثل اختبار الاختراق، وتقييم الثغرات، وتقييم الاختراق، ومراجعة إعدادات ومعمارية الأمن السيبراني). وبالنظر إلى ارتفاع عدد التقييمات المطلوبة لضمان تأمين فعالية بحجم مجموعة العشرين، جمع النموذج السعودي بين التقييمات المباشرة التي أجرتها أمانة مجموعة العشرين والتقييمات الذاتية التي أجرتها الجهات المختلفة. وكان من الضروري وضع خطة للحد من مخاطر التهديدات السيبرانية وأن تتضمن تشكيل فريق مخصص للاستجابة للحوادث، بالإضافة للفريق المعتاد.

فهم خصائص الجهات المستهدفة وإشراكها – تنطوي الفعاليات الضخمة مثل فعاليات مجموعة العشرين على العديد من الجهات المعنية الداخلية والخارجية، وبالتالي من الضروري إطلاق حملات لتوعية المشاركين بأهمية الأمن السيبراني. كذلك من الضروري تحديد الجهات المناسبة المستهدفة للمشاركة في تلك الجلسات والاستعانة بالأشخاص المناسبين ذوي الأدوار والمهام المحددة ضمن مجموعة العشرين. ويجب أيضًا تخصيص حملات التوعية والتمارين السيبرانية بما يتناسب مع مسؤوليات كل مجموعة لضمان تحقيق نتائج فعالة. ويمكن تشجيع المشاركين على اتباع نمط تفكير يتسم بالمرونة والتعاون من خلال توضيح الرؤية بشأن تداعيات قرارات معينة في حالة وقوع أي هجوم وتحديد قنوات تواصل واضحة، ومن شأن ذلك أن يعزز من برنامج جاهزية وصمود الأمن السيبراني بوجه عام.

أبرز إحصائيات برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين

حوكمة البرنامج

أكثر من 400
عدد مختصي الأمن السيبراني المشاركين في البرنامج

أكثر من 350
عدد الجهات التي تم رفع مستوى جاهزية الأمن السيبراني لديها

أكثر من 450
عدد التقارير الصادرة

أكثر من 400
عدد أيام التحضير والتنفيذ

التقييمات السيبرانية

أكثر من 120
عدد تقييمات الأمن السيبراني التي تم إجراؤها، وتشمل:

1. تقييم المخاطر السيبرانية
2. اختبار الاختراق وتقييم الثغرات
3. مراجعة إعدادات ومعمارية الأمن السيبراني
4. تقييم الاختراق السيبراني
5. تقييم استمرارية الأعمال
6. تقييم الالتزام بضوابط الأمن السيبراني
7. مراجعة صلاحيات وصول المستخدمين

أكثر من 100
عدد الجهات التي تم تقييمها

عمليات الأمن السيبراني

أكثر من 10 آلاف
عدد ساعات المراقبة المستمرة للأمن السيبراني

أكثر من 600
عدد تحذيرات الأمن السيبراني التي تمت مشاركتها مع الجهات ذات الصلة

أكثر من 385 ألف
عدد الهجمات السيبرانية التي تم رصدها

361
عدد التهديدات السيبرانية التي تم تحليلها والتعامل معها

التوعية بالأمن السيبراني والتمارين السيبرانية

100
عدد الجهات المشاركة في التمارين السيبرانية

9
عدد التمارين السيبرانية التي تم تنظيمها للجهات ذات الصلة

أكثر من 60
عدد ورش العمل المنعقدة للجهات ذات الصلة، بمشاركة مدراء وقيادات الأمن السيبراني

مقدمة

يقدم هذا التقرير توجيهات حول أفضل ممارسات الأمن السيبراني للدول التي ستستضيف رئاسة مجموعة العشرين والفعاليات الكبرى المشابهة في المستقبل.

في عام 2020م، تسلّمت المملكة العربية السعودية رئاسة مجموعة العشرين، وكانت هذه فرصة لإحداث أثر ملموس في أجندة عمل المجموعة في بيئة عالمية معقدة وسريعة التغير.

إن الترابط المتزايد للاقتصاد العالمي يزيد من أهمية الأمن الرقمي للأنظمة الاقتصادية، وهو ما يؤكد على قيمة التعاون الدولي.

عمل فريق عمل الاقتصاد الرقمي (DETF) ضمن مجموعة العشرين، خلال سنة رئاسة المملكة العربية السعودية، على إدراج أحد المجالات ذات الأولوية بعنوان "الأمن في الاقتصاد الرقمي"، بما يتوافق مع الأهداف العامة لسنة الرئاسة.

وعلى مدار عام 2020م، تعاون فريق عمل الاقتصاد الرقمي مع العديد من الجهات المعنية، ومن بينها مجموعة الأعمال (B20) والمنظمات الدولية ذات الصلة، للعمل على نتائج أولوية "الأمن في الاقتصاد الرقمي". وقد تم توثيق نتائج تلك الجهود من خلال ما يلي:

• في يوليو 2020م، تم إصدار البيان الوزاري لفريق عمل الاقتصاد الرقمي لعام 2020م والملحق المتعلق بممارسات "الأمن في الاقتصاد الرقمي" لدى مجموعة العشرين.

• في نوفمبر 2020م، اعتمد قادة مجموعة العشرين هذه الأولوية ونتائجها في بيان القادة الصادر عن قمة الرياض لمجموعة العشرين.

بالإضافة إلى ذلك، استضاف فريق عمل الاقتصاد الرقمي أول فعالية مخصصة بالكامل لمناقشة المسائل المتعلقة بالأمن السيبراني في مجموعة العشرين، وهي: حوار الأمن السيبراني في مجموعة العشرين.

كان برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين الذي تقوده الهيئة الوطنية للأمن السيبراني قد تم تصميمه على أساس أن فعاليات رئاسة مجموعة العشرين ستُقام بصورة فعلية وبمشاركة شخصية من المشاركين، لكن مع تطور جائحة فيروس كورونا المستجد (كوفيد-19) على مدار عام 2020م، أصبح من الواضح صعوبة المشاركة حضوريًا في الفعاليات، لذلك تم اتخاذ قرار تنفيذي لتحويل فعاليات المجموعة بالكامل -بما في ذلك قمة القادة- بحيث تُعقد افتراضيًا. وقد استلزم ذلك من فريق البرنامج حشد الجهود وزيادة التركيز على الأمن السيبراني.

ومقارنةً بالفعاليات الضخمة الأخرى التي تستمر لبضعة أيام أو أسابيع أو حتى لبضعة أشهر على أقصى تقدير، تستمر فعاليات مجموعة العشرين لعام كامل، وتشمل العديد من الاجتماعات التي يشارك فيها الوزراء وكبار المسؤولين الحكوميين وممثلو المجتمع المدني. وفضلاً عن كونه أحد محاور النقاش الأساسية خلال فعاليات المجموعة، فقد كان الأمن السيبراني أيضًا من النقاط الحاسمة في التخطيط للفعاليات نفسها وتنظيمها، لا سيما وأن غالبية الفعاليات عُقدت افتراضيًا للمرة الأولى في تاريخ رئاسة مجموعة العشرين.

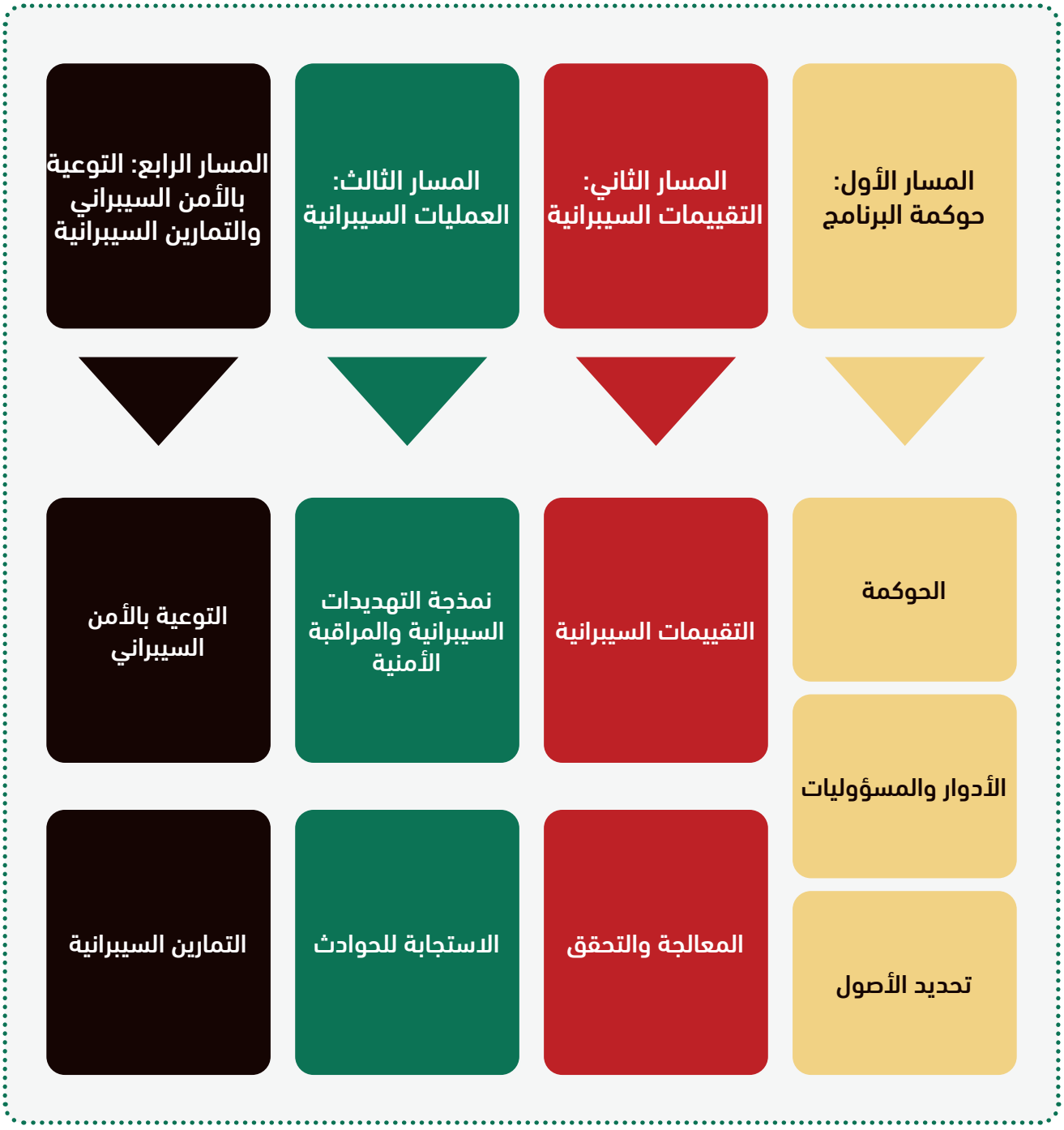
ويستعرض هذا التقرير كيفية تضمين الأمن السيبراني ضمن جهود تأمين سنة رئاسة مجموعة العشرين، كما يتناول ويحلل ويوثّق أنشطة الأمن السيبراني والنقاشات التي دارت حوله قبل بداية رئاسة مجموعة العشرين وحتى نهاية القمة الافتراضية للقادة.

ويسلط هذا التقرير الضوء على أهمية التعاون الدولي لتعزيز صمود الأمن السيبراني العالمي، وذلك باستعراض النموذج السعودي لتعزيز صمود الأمن السيبراني خلال سنة رئاسة مجموعة العشرين. كذلك، يستعرض التقرير النموذج الذي طورته المملكة لتأمين فعاليات مجموعة العشرين خلال عام 2020م ويعكس النموذج الدور الكبير للتكامل المميز بين الهيئة الوطنية للأمن السيبراني وذراعها التقني، الشركة السعودية لتقنية المعلومات (سايت)، ومقدمي الخدمات، كما يوضح الدروس المستفادة من ذلك. وأخيرًا، يمثل هذا التقرير دليلاً توجيهيًا حول أفضل ممارسات الأمن السيبراني ومرجعًا للدول المستضيفة لرئاسة مجموعة العشرين أو الفعاليات الضخمة المشابهة في المستقبل.

برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين

تم إطلاق برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين بهدف تعزيز صمود الأمن السيبراني للأمانة السعودية لمجموعة العشرين والجهات ذات العلاقة.

مكونات برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين



الشكل 2

تم إطلاق برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين بهدف تعزيز صمود الأمن السيبراني للأمانة السعودية لمجموعة العشرين وجميع الجهات ذات العلاقة، بما في ذلك الأطراف الخارجية.

اتبع برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين النموذج السعودي الذي يستند إلى ثلاثة مبادئ:

1

أولاً، **الشمولية**، وينطوي ذلك على تحديد الجهات المعنية الرئيسية المشاركة في استقبال المشاركين واستضافتهم ونقلهم وحمايتهم. ويشمل ذلك إنشاء إدارة للأمن السيبراني داخل الأمانة السعودية لمجموعة العشرين.

2

ثانيًا، **الصمود**، وتم الاسترشاد فيه بتحليل مدى تعقيد المجال السيبراني وتحديات الأمن السيبراني لتأمين رئاسة مجموعة العشرين. وقد أتاح هذا التحليل إعداد نموذج يعتمد على سبل الحماية التي تتسم بالصمود والموثوقية والقدرة على التحذير من التهديدات السيبرانية والاستجابة لها، مع العمل في الوقت نفسه على اكتشاف الثغرات السيبرانية ومعالجتها في مرحلة مبكرة. كذلك، أُطلقت حملات لتوعية جميع الجهات المعنية بهدف تعزيز ثقافة الأمن السيبراني طوال سنة رئاسة مجموعة العشرين وخلال قمة القادة.

3

ثالثًا، **التعاون**، وقد تضمّن ذلك الربط بين منظومة معقدة تتكون من الجهات العامة والخاصة على الصعيدين الوطني والدولي. وقد أثمرت الشراكات الناتجة عن تعزيز الثقة بين جميع الجهات وتمكين النموذج من تحقيق مستويات عالية من المشاركة. كما كان التكامل بين الهيئة وذراعها التقني، الشركة السعودية لتقنية المعلومات (سايت)، من أهم العوامل التي ساهمت في نجاح النموذج.

المنهجية

ركزت المنهجية المتبعة على الاستفادة من التجارب الدولية وخبرات الهيئة الوطنية للأمن السيبراني لتطوير نموذج مخصص. وفي سبيل ذلك تم إجراء مقارنة معيارية مبدئية للاستفادة من التجارب السابقة كما هو موضح في الشكل 3 أدناه:

الشكل 3

أ. المقارنة المعيارية

نظرًا للطبيعة المعقدة للتخطيط للفعاليات الضخمة وتنظيمها وتنفيذها، مثل فعاليات مجموعة العشرين الممتدة لعام كامل، فإن ذلك يتطلب فهمًا عميقًا للتجارب السابقة. ومن أبرز التحديات التي تم اكتشافها منذ بداية التخطيط لفعاليات مجموعة العشرين لعام 2020م قلة البيانات العامة المتاحة عن الفعاليات السابقة. علاوةً على ذلك كانت الفرق المسؤولة عن تأمين رئاسة مجموعة العشرين في الكثير من الحالات السابقة تُشكَّل ويُحتفَظ بها خلال مدة الفعالية فقط، وبمجرد انتهاء رئاسة المجموعة، يعود أفراد تلك الفرق إلى أدوارهم السابقة.

ويؤدي ذلك إلى فقدان المعرفة المؤسسية القيّمة ويجعل من الصعب للغاية التعرف على البيانات. لهذا السبب، تم الاسترشاد في إعداد النموذج السعودي للأمن السيبراني بتحليل لنماذج المقارنة والدروس المستفادة في الفعاليات الضخمة الأخرى غير مجموعة العشرين.

لطالما كانت الفعاليات الضخمة مستهدفة بالهجمات السيبرانية، والتي أصبحت أكثر انتشارًا بسبب تزايد الاعتماد على القنوات الرقمية والتقنيات الحديثة. وقد تضمنت المقارنة المعيارية تحديد وتحليل الأنماط الشائعة للهجمات والخصوم والتهديدات السيبرانية.

ويمكن ملاحظة نمو التحول الرقمي لتلك الفعاليات في زيادة البث الافتراضي والتفاعلات قبل وأثناء الفعاليات وقنوات التواصل الرقمية والمؤتمرات المنعقدة افتراضياً.

وقد أصبح بإمكان منفذي التهديدات السيبرانية استخدام العديد من الأدوات للوصول بشكل غير مسموح به إلى المعلومات الحيوية، مما قد يتسبب في ضرر كبير حال استغلال ذلك.

منفذو التهديدات السيبرانية

قد تختلف مصادر التهديدات السيبرانية باختلاف دوافعها وأهدافها. فإذا ما نظرنا إلى الفعاليات الضخمة، سنجد أن تلك المصادر تشمل:

الدول

الإرهابيين و المتعاطفين

مجرمي الهجمات السيبرانية

التهديدات الداخلية

تستهدف مصادر التهديدات تلك في الغالب الأنظمة والأجهزة والبنية التحتية لدى الجهات المعنية الرئيسية، سواءً كانت من المشاركين في الفعاليات أو منظميها أو من الجمهور العام.

التهديدات السيبرانية

تُظهر فعاليات مجموعة العشرين وغيرها من الفعاليات الضخمة التي عُقدت مؤخرًا (والتي تم تحليلها في إطار المقارنة المعيارية) أنه عند وقوع الأحداث السيبرانية خلال تلك الفعاليات الضخمة قد تصل في المجمل إلى مئات الآلاف، إلا أنه لم يتم الإبلاغ سوى عن عدد قليل منها. ويُظهر التحليل أن أبرز التهديدات خلال تلك الفعاليات هي:

اختراق البيانات – يتمثل هذا التهديد في الوصول غير المسموح به إلى البيانات واستخلاصها. ويمكن للخصوم إرسال دعوات تصيّد إلى المشاركين في الفعاليات، بحيث تحتوي تلك الدعوات على رابط يتضمن برمجيات خبيثة لتمكينهم من الوصول إلى المعلومات الحساسة، مما يؤدي إلى فقدان البيانات الشخصية والمالية والوثائق السرية الأخرى.

حجب الخدمة – يمكن أن تؤدي هجمات حجب الخدمة الموزعة إلى تعطيل الموقع الإلكتروني الرسمي للفعالية، وقد يتعذر على المشاركين الوصول إلى المعلومات المتعلقة بالفعاليات. ويمكن أن تبدأ مثل هذه الهجمات حتى قبل الحفل الافتتاحي وتستهدف الأطراف الخارجية المسؤولة عن الخدمات الإلكترونية للفعاليات. كذلك فإن الاضطرابات المؤقتة الناتجة عن حجب الخدمة الموزعة قد يتيح الفرصة للمهاجمين السيبرانيين للوصول إلى المنصة الإلكترونية وسرقة البيانات.

اختراق الحسابات الشخصية – يتمثل هذا التهديد في اختراق أحد الخصوم لبيانات الحساب الشخصي، مثل اسم المستخدم وكلمة المرور، مما يتيح له سرقة المعلومات الخاصة أو طلب فدية من صاحب الحساب لإعادة الحساب المسروق إليه.

اختراق الجهاز الشخصي – يحدث ذلك عندما يسيطر المهاجمون على أحد الأجهزة لاستخدامه في أعمال غير قانونية، ومنها، على سبيل المثال لا الحصر، سرقة البيانات القيّمة.

اختراق كاميرات المراقبة والأجهزة الأمنية – يحدث ذلك عندما يخترق المهاجمون أجهزة المراقبة والأمن، مما يؤدي إلى تعطيل الأمن أو فقدان السيطرة.

الهجمات على البنية التحتية التقنية – يمكن أن تؤثر الهجمات السيبرانية على البنية التحتية التقنية من خلال التسلل إليها باستخدام الهندسة الاجتماعية أو البرمجيات الضارة أو أشكال الهجوم الأخرى، وقد يؤدي ذلك إلى ضرر مادي مما يؤثر بشدة على الفعالية.

التهديد الداخلي – هو التهديد الذي تتعرض له المؤسسة من أحد المصادر الداخلية لها، مثل الموظفين الحاليين أو السابقين أو المقاولين أو الشركاء في العمل.

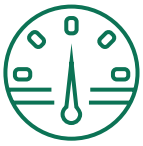
المخرجات الرئيسية:

عند إجراء المقارنة المعيارية للفعاليات الضخمة، تم تحليل إجراءات الأمن السيبراني فيها وبرزت خمس نقاط رئيسية مستخلصة:

طريقة تنظيم الأمن السيبراني خلال الفعالية – اعتمدت الفعاليات الأخيرة على إسناد خدمات الأمن السيبراني لشركات متخصصة.

أنواع التهديدات السيبرانية – تعتبر رسائل التصيد الإلكتروني التي تحتوي على مرفقات وروابط خبيثة أكثر التهديدات السيبرانية شيوعًا والتي تؤثر على الفعاليات الضخمة.

أهداف الهجمات السيبرانية – يعتبر المسؤولون الحكوميون والوفود الحكومية، وكذلك الجهات المنظِّمة ومقدمي الخدمات الخارجيين، هم الأهداف الأساسية لتلك الهجمات.



حجم الهجمات السيبرانية – عند تحليل جميع الفعاليات، يتضح أن حجم الهجمات السيبرانية يتزايد كل عام، مما يدل على تأثير رقمنة الفعاليات الضخمة.

توقيت الهجمات السيبرانية – كانت الهجمات السيبرانية تُرصد بشكل كبير خلال الأيام السابقة للقمة وكذلك خلال الاحتفالات الافتتاحية.

أفضل الممارسات:

وفقًا لذلك، أتاح لنا تحليل التجارب السابقة وخبرات الهيئة الوطنية للأمن السيبراني تحديد ست من أفضل الممارسات لتأمين الفعاليات الضخمة، ومن بينها فعاليات رئاسة مجموعة العشرين على مدار عام كامل:

1. **التخطيط الاستراتيجي واستكشاف الآفاق**: في بداية أي تخطيط لتعزيز الأمن السيبراني يجب تحديد الأهداف الاستراتيجية وتحليل التهديدات بشكل مناسب.

2. **الحوكمة**: يجب وضع نموذج واضح للحوكمة، مع تعزيزه بفريق يضم كوادر مؤهلة ولجنة تنفيذية تضم بين أعضائها فريق إدارة الأمن السيبراني وكفاءات لتحليل وفهم وضع الأمن السيبراني وفريق للاستجابة للحوادث وغير ذلك من الجهات الحكومية والخاصة ذات الصلة. وتتيح اللجنة التنفيذية اتخاذ القرار والتنسيق بشكل فعال.

3. **إدارة الأصول**: يتم تحديد الأنظمة والشبكات الحيوية، ومن بينها تلك الخاصة بمقدمي الخدمات الخارجيين والجهات الخارجية، وتعزيزها لزيادة صمود الأمن السيبراني.

4. **فريق مخصص للمراقبة والتقييم والاستجابة**: يتم تشكيل فرق لإجراء التقييمات السيبرانية ومراقبة الأمن السيبراني ورصد التهديدات

والاستجابة لها بصفة مستمرة بهدف جمع وتحليل البيانات من الجهات الحكومية ومقدمي الخدمات الخارجيين والاستجابة للهجمات / الحوادث السيبرانية.

5. **مشاركة المعلومات**: يتم تشجيع مشاركة المعلومات حول التهديدات السيبرانية بين الجهات المعنية المشاركة وغالبًا ما يتم تمكين ذلك من خلال منصات مخصصة لمشاركة المعلومات.

6. **التوعية بالأمن السيبراني والتمارين السيبرانية**: يتم تنفيذ برامج التوعية بالأمن السيبراني للموظفين والجهات المعنية الرئيسية، ومن بينها مقدمو الخدمات الخارجيون، لضمان اتباعهم للتوجيهات المتعلقة بالأمن السيبراني.

ب. النموذج

في ضوء تحليل الفعاليات الضخمة السابقة، من الواضح أنه لا يمكن قصر الأمن السيبراني على جوانب معينة، بل يعتبر أحد الجوانب الأساسية في التحضير لفعاليات رئاسة مجموعة العشرين وعقدها بنجاح. لهذا السبب، طورت المملكة العربية السعودية نموذجًا لتعزيز صمود الأمن السيبراني وتأمين فعاليات رئاسة مجموعة العشرين بالكامل. وقد تم تصميم النموذج السعودي، الذي تم تطبيقه طوال سنة الرئاسة، باتباع منهجية ذات مستويين:

المستوى الأول:

ينطوي هذا المستوى على تعزيز جاهزية وصمود الأمن السيبراني خلال سنة رئاسة مجموعة العشرين وتم تمكينه في البرنامج من خلال نموذج حوكمة شاملة يرتكز على جانبين أساسيين: إدارة الأمن السيبراني في الأمانة السعودية لمجموعة العشرين والتنسيق مع جميع الجهات ذات العلاقة.

وقد تولّت إدارة الأمن السيبراني في الأمانة السعودية لمجموعة العشرين:

- **دعم وتيسير تنفيذ البرنامج؛**
- **تحديد أصول تقنيات المعلومات؛**
- **مراقبة جميع الأصول عن كثب؛**
- **تشكيل فريق مختص للاستجابة للحوادث ضمن الأمانة السعودية لمجموعة العشرين؛**
- **إجراء التقييمات السيبرانية؛**
- **تحليل الثغرات السيبرانية وعلاجها.**

وتضمنّت مجالات تركيز الجهات ذات العلاقة:

- **الالتزام بضوابط الهيئة الوطنية للأمن السيبراني؛**

- إجراء التقييمات الذاتية للأمن السيبراني؛
- تحليل جميع النتائج ذات الصلة بالتقييمات السيبرانية واتخاذ الإجراءات وفقًا لها؛
- الإبلاغ عن الحوادث السيبرانية.

المستوى الثاني:

تضمّن هذا المستوى تفعيل النموذج في القمة الافتراضية للقادة باعتباره أحد محاور التركيز. وقد عُقدت قمة القادة بشكل افتراضي لأول مرة في تاريخ المجموعة وتم التعامل معها كنسخة مركزّة تعكس النموذج المتبع طوال سنة رئاسة مجموعة العشرين. ومع ذلك، تم التوسع في النموذج بهدف رفع مستوى القدرات ذات الصلة تبعًا لمستوى العُمق والتعقيد المطلوب للتحضير لهذه الفعالية وتأمينها. كذلك، تم تخصيص الأدوار والمسؤوليات بما يتناسب مع المتطلبات المحددة لقمة القادة، كما تمت مراقبة جميع أصول تقنيات المعلومات والمنصات عن كثب وتفعيل خطة خاصة للحد من مخاطر الهجمات السيبرانية، فضلاً عن تشكيل فريق مختص للاستجابة للحوادث لتعزيز جهود فريق العمل الموجود بالفعل. وأخيرًا، تم تنظيم العديد من التمارين السيبرانية المخصصة بما يتناسب مع القمة الافتراضية للقادة بهدف تحضير قدرات الاستجابة للهجمات السيبرانية المحتملة وتحقيق التكامل فيما بينها.

ملخص النموذج السعودي لتعزيز الأمن السيبراني خلال سنة رئاسة مجموعة العشرين:

يعتبر الأمن السيبراني أحد المجالات الرئيسية للاستعداد لأعمال مجموعة العشرين خلال سنة الرئاسة، إلا أن التحول الذي شهدته رئاسة المملكة بانتقال الفعاليات إلى المنصات الرقمية وعقدها افتراضياً، كان له دور كبير في زيادة أهمية الأمن السيبراني ورفع الجاهزية السيبرانية والذي انعكس على النموذج وتصميمه. تم تفعيل هذا النموذج من خلال برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين، حيث تم تنفيذه بالشكل التالي:

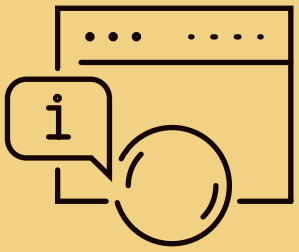
المسارات	المستوى الأول – تعزيز صمود الأمن السيبراني خلال سنة الرئاسة	المستوى الثاني – تعزيز صمود الأمن السيبراني خلال القمة الافتراضية للقادة
حوكمة البرنامج	• تشكيل لجنة تنفيذية وفريق تقني وتحديد مجموعة من الجهات المعنية: - الأمانة السعودية لمجموعة العشرين - اللجنة التنفيذية - الهيئة الوطنية للأمن السيبراني - مقدمو الخدمات - الأطراف الخارجية - الجهات ذات الصلة - الشركة السعودية لتقنية المعلومات (سايت) • تحديد وحماية أصول تقنيات المعلومات • تطوير ضوابط الأمن السيبراني	• توضيح الأدوار والمسؤوليات • تعزيز مشاركة الجهات المعنية الرئيسية: - الأمانة السعودية لمجموعة العشرين - اللجنة التنفيذية - الهيئة الوطنية للأمن السيبراني - مقدمو الخدمات - الأطراف الخارجية - الجهات ذات الصلة - الشركة السعودية لتقنية المعلومات (سايت) • التنسيق اليومي على مستوى القيادة العليا • تسريع عملية اتخاذ القرار

التقييمات السيبرانية	• إجراء مجموعة من التقييمات السيبرانية مع التركيز على الأمانة السعودية لمجموعة العشرين وموفري البنية التحتية والمنصات الرقمية: - تقييم المخاطر - اختبار الاختراق - تقييم الثغرات - تقييم الاختراق السيبراني - تقييم الالتزام بضوابط الأمن السيبراني - مراجعة صلاحيات وصول المستخدمين - مراجعة إعدادات ومعمارية الأمن السيبراني	• إجراء مجموعة من التقييمات السيبرانية مع التركيز على الأمانة السعودية لمجموعة العشرين وموفري البنية التحتية والمنصات الرقمية: - تقييم المخاطر - اختبار الاختراق - تقييم الثغرات - تقييم الاختراق السيبراني - تقييم الالتزام بضوابط الأمن السيبراني - مراجعة صلاحيات وصول المستخدمين - مراجعة إعدادات ومعمارية الأمن السيبراني
العمليات السيبرانية	• نمذجة التهديدات السيبرانية • الاستجابة للحوادث السيبرانية • مراقبة الأمن السيبراني والدراية الأمنية	• التركيز الشديد على الموفر الوطني للبنية التحتية الرقمية • تعزيز تدابير حماية الأمن السيبراني • نمذجة التهديدات السيبرانية • تعزيز قدرات الاستجابة للحوادث وتخصيص فريق وطني للاستجابة للحوادث من أجل القمة الافتراضية • المراقبة المشدده لأحداث الأمن السيبراني لدى الأمانة السعودية لمجموعة العشرين وموفر البنية التحتية والمنصة الرقمية
التوعية بالأمن السيبراني والتمارين	• التمارين السيبرانية المخصصة بما يتناسب مع سنة الرئاسة بالكامل • ورش العمل المخصصة لجميع الجهات المعنية المشاركة • حملات التوعية بالأمن السيبراني	• التمارين السيبرانية المخصصة بما يتناسب مع القمة الافتراضية للقادة • ورش العمل المخصصة للجهات المعنية المشاركة • حملات التوعية بالأمن السيبراني

المستوى الأول – تعزيز صمود الأمن السيبراني خلال سنة الرئاسة

المسار الأول: حوكمة البرنامج

من الخطوات الأساسية عند إعداد أي برنامج ضخم وتجهيز عناصره أن يتم بناء أساس متين له لضمان نجاحه. وفي سبيل بناء ذلك الأساس، تشمل حوكمة البرنامج إنشاء الهيكل التنظيمي، بحيث يتم تحديد نطاق البرنامج وتوضيح الأدوار والمسؤوليات المنوطة بالجهات ذات العلاقة المختلفة وتحديد العلاقة بين الوظائف المختلفة. كذلك، تُطبَّق آليات إشرافية لضمان المراجعة المستمرة والحرص على إجراء التعديلات اللازمة. وتعتبر هذه العملية بأكملها في غاية الأهمية لتحقيق النتائج المنشودة لتأمين رئاسة مجموعة العشرين.

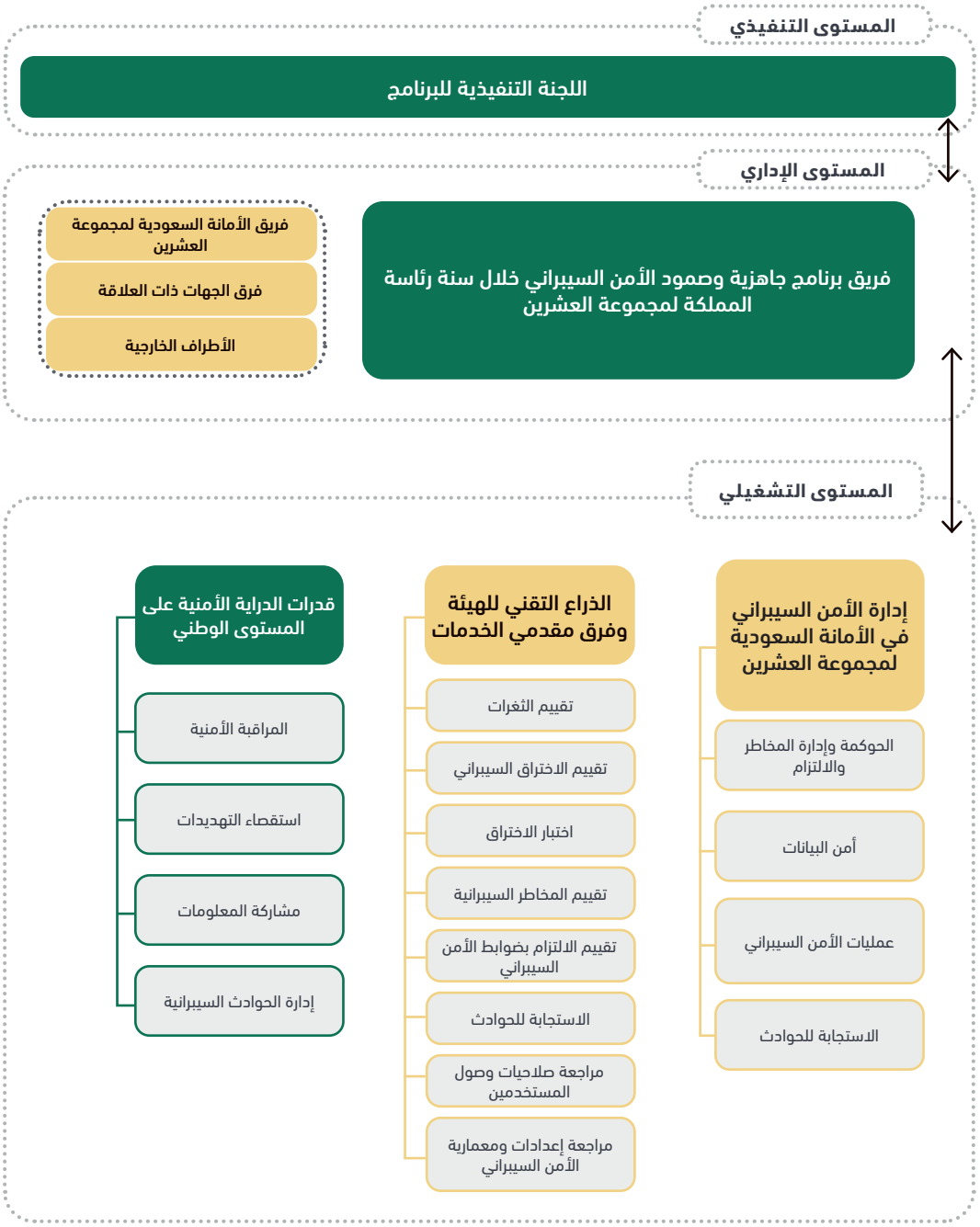


استغرق إعداد البرنامج وتنفيذه أكثر من **400 يوم**.

أ.حوكمة البرنامج

أثمرت حوكمة البرنامج عن ضمان التغطية الفعالة لجميع جوانب فعاليات مجموعة العشرين. ويوضح الشكل 4 هيكل الحوكمة بالكامل والذي كان من أهم ركائزه التعاون والتكامل، كما كان التكامل المتميز في هذا النموذج بين الهيئة الوطنية للأمن السيبراني وذراعها التقني، الشركة السعودية لتقنية المعلومات (سايت)، ومقدمي الخدمات، حجر الأساس لنجاحه.

ب. الأدوار والمسؤوليات



الشكل 4

بالاعتماد على هيكل الحوكمة الاستراتيجي، تضمّنت المرحلة التالية تحديد الجهات المعنية الرئيسية، والتي تم تقسيمها إلى ثلاثة مستويات من الإشراف: المستوى التنفيذي، والمستوى الإداري، والمستوى التشغيلي. وبوجه عام، شاركت أكثر من 100 جهة و400 أخصائي وأخصائية أمن سيبراني في البرنامج. كما تم تحديد الأدوار والمسؤوليات المنوطة بكل جهة ذات علاقة بحسب مدى ارتباطها برئاسة مجموعة العشرين، وذلك وفقًا لما يلي:

المستوى التنفيذي

اللجنة التنفيذية للبرنامج: تقودها الهيئة الوطنية للأمن السيبراني وتضم أعضاء آخرين، من بينهم الأمانة السعودية لمجموعة العشرين ومقدمو الخدمات الأساسيين، مثل الذراع التقني للهيئة الوطنية للأمن السيبراني، الشركة السعودية لتقنية المعلومات(سايت)، وشركات الاتصالات والتقنيات وموفرو حلول وخدمات الأمن السيبراني والموفر الوطني للبنية التحتية الرقمية، الذي استضاف البنية التحتية الرقمية الوطنية للمنصة الافتراضية لقمة القادة المشمولة في المستوى الثاني. وكان دور اللجنة هو الإشراف على تطور البرنامج بإعداد ونشر التقارير والمؤشرات السيبرانية بصفة دورية؛ بهدف تقييم المخاطر التي واجهتها رئاسة المجموعة. كذلك، كانت اللجنة مسؤولة في نهاية المطاف عن الإشراف على خطط معالجة التحديات والحد من المخاطر وعن تصعيدها والتواصل بشأنها. وقد عقدت اللجنة التنفيذية اجتماعاتها بصفة منتظمة وأصدرت أكثر من 450 تقريرًا.

المستوى الإداري

فريق الأمانة السعودية لمجموعة العشرين: يمثل الجهة المعنية الأساسية وهو المسؤول عن التنسيق والمشاركة في جميع الأنشطة ذات الصلة برئاسة المملكة لمجموعة العشرين وتطبيق ضوابط الأمن السيبراني. وقد قامت الأمانة السعودية، للمرة الأولى في تاريخ مجموعة العشرين، بإنشاء إدارة للأمن السيبراني والتي تم تكليفها خصيصًا بدعم جهود الأمن السيبراني داخليًا على مستوى الأمانة فقط.

فريق برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين: تولت الهيئة الوطنية للأمن السيبراني مسؤولية الإدارة العامة للبرنامج والإشراف على تنفيذه بالتعاون مع الأمانة السعودية لمجموعة العشرين ومقدمي الخدمات الآخرين، ومن بينهم الذراع التقني للهيئة الوطنية للأمن السيبراني، الشركة السعودية لتقنية المعلومات(سايت)، وشركات الاتصالات والتقنيات وموفرو حلول وخدمات الأمن السيبراني. بالإضافة إلى ذلك، كانت هي المسؤولة عن تحديد ضوابط الأمن السيبراني لتعزيز صمود الأمن السيبراني خلال سنة رئاسة مجموعة العشرين (المستوى الأول) وخلال القمة الافتراضية للقادة (المستوى الثاني). وفي إطار التحضير للقمة الافتراضية للقادة، انضم الموفر الوطني للبنية التحتية الرقمية أيضًا إلى فريق البرنامج كمضيف للقمة الافتراضية للقادة بهدف تنفيذ أنشطة المستوى الثاني.

فرق الجهات ذات العلاقة: تكونت هذه الفرق من الجهات الوطنية ذات العلاقة المشاركة في ورش العمل والاجتماعات الدورية.

الأطراف الخارجية: يشمل ذلك أي طرف خارجي له علاقة برئاسة مجموعة العشرين، على مستوى مجموعة كبيرة من الجهات. ويشمل ذلك أيضًا المطارات وموفري الخدمات الفندقية المسؤولين عن استضافة الضيوف حين كان من المقرر عقد فعاليات مجموعة العشرين حضوريًا.

المستوى التشغيلي

إدارة الأمن السيبراني في الأمانة السعودية لمجموعة العشرين: هي المسؤولة عن تنفيذ وإدارة قدرات الحوكمة وإدارة المخاطر والالتزام مع أمن البيانات والاستجابة للحوادث ضمن عمليات الأمن السيبراني الأوسع نطاقًا والتي تم تنفيذها في إطار التحضير لسنة الرئاسة وعلى مدار السنة بالكامل، كما تم توفير خدمات المراقبة المدارة لإدارة الأمن السيبراني في الأمانة من قبل الذراع التقني للهيئة الوطنية للأمن السيبراني، الشركة السعودية لتقنية المعلومات(سايت).

قدرات الدراية الأمنية على المستوى الوطني: كان الفريق -الذي تقوده الهيئة الوطنية للأمن السيبراني ويضم مقدمي خدمات الأمن السيبراني- مسؤولاً عن مراقبة الأمن السيبراني على مدار الساعة والدراية الأمنية بالتهديدات والمخاطر السيبرانية ومشاركة المعلومات (التقارير التفصيلية عن التهديدات المحتملة) مع الجهات ذات العلاقة والأمانة السعودية لمجموعة العشرين وتقديم الدعم في إدارة الحوادث السيبرانية.

الذراع التقني للهيئة وفرق مقدمي الخدمات: تم تصنيف مقدمي الخدمات في فئتين: الجهات المستضيفة للبنية التحتية الرقمية، ومقدمي خدمات الأمن السيبراني. وبالنسبة للمستوى الثاني، تولى الموفر الوطني للبنية التحتية الرقمية استضافة المنصة الافتراضية لعقد القمة بالتعاون مع مقدم خدمات الاتصالات والتقنيات. وقدّم مقدمو خدمات الأمن السيبراني الأساسيين، ومن بينهم الذراع التقني للهيئة الوطنية للأمن السيبراني، الشركة السعودية لتقنية المعلومات(سايت)، الدعم لبرنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين من خلال تقديم خدمات الأمن السيبراني. وكان مقدمو الخدمات هم المسؤولون عن الكشف عن الثغرات وتقييمات الاختراق السيبراني واختبار الاختراق و تقييمات المخاطر السيبرانية والالتزام بضوابط الأمن السيبراني. بالإضافة إلى ذلك، كان هناك تعاون وثيق لتقديم الدعم في الاستجابة للحوادث في حينها.

ج. تحديد الأصول

تم تنفيذ هذه العملية في الفترة السابقة لرئاسة المجموعة بهدف تحديد جميع أصول تقنيات المعلومات ذات الصلة برئاسة المجموعة وتصنيفها، سواءً كانت مرتبطة بالأمانة السعودية لمجموعة العشرين بشكل مباشر أو غير مباشر.

المسار الثاني: التقييمات السيبرانية

تم تنفيذ سلسلة من التقييمات التقنية والفعالة لأصول تقنيات المعلومات من منظور الأمن السيبراني من قبل الذراع التقني للهيئة الوطنية للأمن السيبراني، الشركة السعودية لتقنية المعلومات(سايت) ومقدمي الخدمات. وقد اشتملت تلك التقييمات على الأنشطة التالية:

تقييم المخاطر السيبرانية: آلية لتحديد المخاطر السيبرانية التي تتعرض لها أصول تقنيات المعلومات، سواءً كانت أجهزة أو برمجيات، وذلك بتحديد مدى احتمال وقوع الهجوم السيبراني والتأثير المحتمل له.

اختبار الاختراق: محاكاة هجوم سيبراني يستهدف البنية التحتية التقنية، وتكمن الفائدة من ذلك في مساعدة المسؤولين والجهات المعنية في اكتشاف الثغرات التي يمكن استغلالها واختبار الإجراءات التي سيتم اتخاذها في حالة حدوث أي هجوم سيبراني. ويمكن الاستفادة أيضًا من اختبار الاختراق في الكشف عن الثغرات في العمليات الأمنية، وبالتالي المساعدة في تفادي الآثار التي قد تنتج عن الهجمات السيبرانية.

تقييم الثغرات السيبرانية: يتم تقييم الثغرات في جميع أصول تقنيات المعلومات بهدف تحديد أي ثغرات سيبرانية.

تقييم الاختراق السيبراني: من الأساليب المفيدة للغاية في تحديد وتحليل أي إشارة على وجود اختراق في الوقت الحالي.

تقييم الالتزام بضوابط الأمن السيبراني: هو تقييم يتيح تحديد أي فجوة للالتزام بضوابط الهيئة الوطنية للأمن السيبراني (الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة). إن تحديد أي مخاطر محتملة لعدم الالتزام من شأنه أن يساعد جميع الجهات في فهم مدى تعرضها للمخاطر المتعلقة بالالتزام بضوابط الأمن السيبراني.

مراجعة صلاحيات وصول المستخدمين: هو تقييم يتيح للجهات التأكد بصفة دورية من عدم إمكانية وصول غير المستخدمين المصرح لهم إلى البنية التحتية، مما يحد بدوره من مخاطر الوصول غير المسموح به.

مراجعة إعدادات ومعمارية الأمن السيبراني: هو تقييم يساعد في تحديد نقاط الضعف في معمارية الأمن السيبراني وإعدادات الأمن السيبراني والثغرات في مكونات البنية التحتية التقنية.

تم إجراء أكثر من **120 تقييمًا سيبرانيًا** بصفة دورية على مدار سنة رئاسة مجموعة العشرين بهدف تحديد الثغرات السيبرانية لدى الجهات ذات العلاقة.

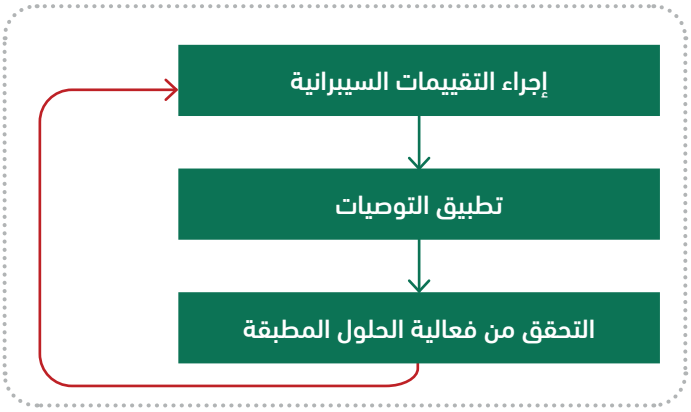
مراحل التقييم

تم إجراء التقييمات لأصول تقنيات المعلومات الموجودة من خلال منهجية من مرحلتين. وفي الوقت الذي تم فيه إجراء تقييم مباشر لأمانة مجموعة العشرين ولأي جهة أخرى ذات علاقة مباشرة بها، طُلب إجراء عدد من التقييمات الذاتية للجهات الأخرى المشمولة ضمن النطاق.

وقد تم تصنيف جميع التهديدات السيبرانية المُبلغ عنها بحسب إطار تحديد الأولويات الذي يحدد الأولويات بناءً على تأثير الهجوم ذي الصلة.

وكجزء من المنهجية لتحديد الثغرات وعلاجها، تم استخلاص عدد من التوصيات المستخلصة من التقييم وتصعيدها إلى الجهات المعنية المختلفة ومعالجتها باتباع منهجية مقسمة إلى مراحل، مع تحديد المتطلبات العاجلة ذات الأولوية.

وفي النهاية، تم التحقق من جميع الأنشطة المشمولة في نطاق خطط معالجة الثغرات والمخاطر وتطبيقها لضمان التأكد من تطبيق توصيات ومتطلبات الأمن السيبراني.



الشكل 5

المسار الثالث: العمليات السيبرانية

بالتوازي مع إجراء التقييمات الدورية للأمن السيبراني، تم تنفيذ عدد من عمليات الأمن السيبراني على مدار مدة البرنامج.

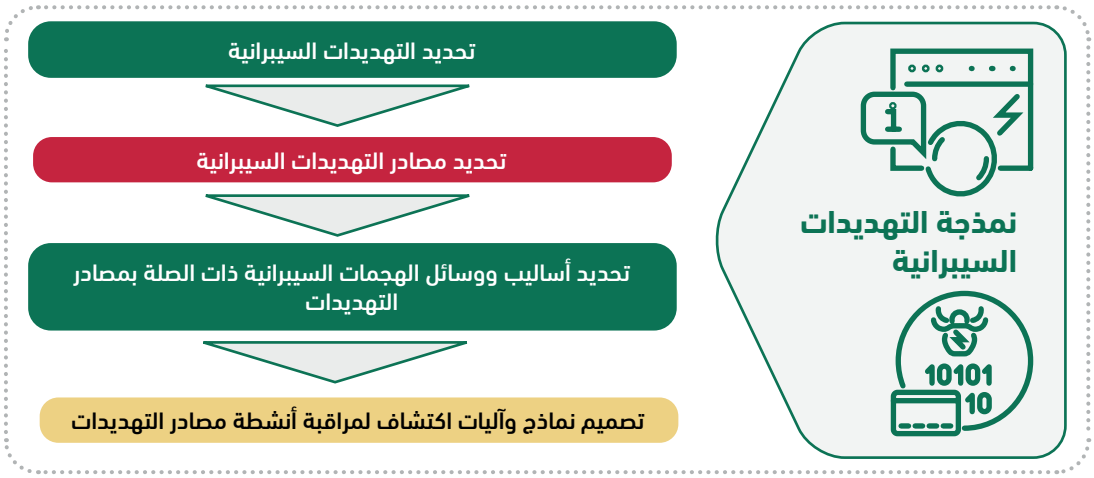
نمذجة التهديدات السيبرانية، ومراقبة الأمن السيبراني، والاستجابة للحوادث السيبرانية:

نظرًا لزيادة التحول الرقمي للعمليات التشغيلية واتساع مجال الهجمات السيبرانية، يتزايد حجم التهديدات السيبرانية بشكل مستمر. وكان الهدف والغرض الأساسي من هذه المرحلة هو تعزيز جاهزية وصمود الأمن السيبراني في مواجهة الهجمات السيبرانية، بهدف حماية الفضاء السيبراني خلال فعاليات مجموعة العشرين. وقد تم تطوير قدرات الأمن السيبراني من خلال توفير خدمات وحلول الأمن السيبراني، ومن بينها تلك الخاصة بالحد من مخاطر حجب الخدمة الموزعة وحماية البريد الإلكتروني. واشتملت هذه المرحلة على تحديد آلية لمراقبة وإدارة التهديدات والاستجابة لها، وانقسمت العملية إلى ثلاث مراحل: نمذجة التهديدات السيبرانية، و المراقبة الأمنية، والاستجابة للحوادث وإدارتها.

الشكل 6

استنادًا لأفضل الممارسات، تم اتباع مجموعة شاملة من أساليب نمذجة التهديدات السيبرانية بهدف تصنيف تهديدات الأمن السيبراني المتعلقة بالأصول المشمولة في النطاق وفحصها وإعداد نماذج لها. وتتيح عملية نمذجة التهديدات السيبرانية وضع منهجية منظمة لتحديد التهديدات السيبرانية والتعامل معها من خلال تقييمها بحسب خطورتها واحتمال وقوعها.

وبالسماح للفريق بتحديد خطط وأساليب وإجراءات المهاجمين السيبرانيين التي تمت مواجهتها خلال سنة رئاسة مجموعة العشرين، كان فريق الأمن السيبراني على استعداد للاستجابة للهجمات الناتجة عن تلك التهديدات وتعزيز جاهزية وصمود الأمن السيبراني.



الشكل 7

تم تصميم مصفوفة لتقييم التهديدات، مع مراعاة أهمية أصول تقنيات المعلومات ومستوى التهديدات. وقد أسفر ذلك عن أربع فئات: التهديدات الحرجة، والتهديدات العالية، والتهديدات المتوسطة، والتهديدات المنخفضة.

كانت المراقبة الأمنية تجري على مدار الساعة لمراقبة مختلف أصول تقنيات المعلومات ذات العلاقة بالأمانة السعودية لمجموعة العشرين، وكذلك البنية التحتية للبرنامج وأصوله.

وصل إجمالي عدد ساعات المراقبة المستمرة للأمن السيبراني إلى أكثر من **10,000 ساعة.**

ساعد ذلك في توضيح الرؤية بشأن التهديدات السيبرانية المحتملة التي قد تعيق قدرات الحماية الكاملة والمستمرة. وقد تم تحديد ثلاثة مستويات تتطلب المراقبة لتحقيق مستويات متقدمة من الدراية الأمنية: أولاً، الأمن السيبراني على الصعيد الوطني ككل، باعتباره أحد المسؤوليات الأساسية؛ ثانيًا، الجهات الرئيسية المعنية برئاسة مجموعة العشرين؛ وأخيرًا، أمانة مجموعة العشرين.

تمت مشاركة أكثر من **600 تحذير أمني** مع الجهات ذات العلاقة. وقد تم معالجة الثغرات والتهديدات المحددة في تحذيرات الأمن السيبراني والتعامل معها بوتيرة سريعة.

كانت مرحلة **الاستجابة للحوادث** السيبرانية هي الجانب الأخير من هذه المرحلة الثالثة، وتم تطويرها لضمان الجاهزية الفورية لإدارة حوادث الأمن السيبراني والاستجابة لها على مدار سنة رئاسة المجموعة. ولتحقيق ذلك تم تشكيل فرق الاستجابة للحوادث بمشاركة الذراع التقني للهيئة الوطنية للأمن السيبراني، الشركة السعودية لتقنية المعلومات(سايت)، بحيث تستجيب للحوادث على ثلاثة مستويات: على الصعيد الوطني، وعلى مستوى الأمانة السعودية لمجموعة العشرين، وعلى مستوى قمة القادة تحديدًا.

المسار الرابع: التوعية بالأمن السيبراني والتمارين السيبرانية

ركزت هذه المرحلة على نشر الوعي بالأمن السيبراني وإجراء التمارين السيبرانية. وتعتبر هذه العناصر جوهرية في أي استراتيجية لتحديد الفجوات في المعرفة بالأمن السيبراني والمجالات التي تتطلب تركيزاً أكبر لنشر المعرفة. ويفيد نشر الوعي من خلال الأنشطة المختلفة في تعزيز الوعي البنّاء بين الجهات المعنية الرئيسية بشكل فعال. وبالتالي، يُعد ذلك من الوسائل الرئيسية الداعمة لتأمين الفعاليات والأفراد والأصول، مع ضمان جاهزية وصمود الأمن السيبراني في الوقت نفسه. وقد تم تنفيذ ذلك كله من خلال البرامج التدريبية التي تشرف عليها الأكاديمية الوطنية للأمن السيبراني.

أ. التوعية بالأمن السيبراني

ارتكزت هذه المرحلة من النموذج على رفع مستوى الوعي بالأمن السيبراني، ويرجع ذلك إلى أهمية العامل البشري، باعتباره أحد المكونات الأساسية لتعزيز الصمود السيبراني للبنية التحتية، في تنفيذ وإيجاد منظومة سيبرانية آمنة. ويمكن تنفيذ الهندسة الاجتماعية من خلال استغلال نقاط الضعف في الجانب البشري. ففي حين يمكن استخدام الحلول التقنية لتحسين أمن البنية التحتية، تظل "التهديدات الداخلية" محتملة -كأن يقوم أحد الأفراد داخل المؤسسة بالإضرار بها من خلال الاستفادة من معرفته وصلاحياته-.

وقد تم تطوير مجموعة من برامج التوعية بالأمن السيبراني للجهات المعنية المشاركة، مع الاستفادة فيها من المحتوى الصادر عن المركز الوطني الإرشادي للأمن السيبراني، بهدف رفع مستوى الوعي. واستهدفت هذه البرامج توعية الجمهور بشأن حماية المعلومات والاستخدام المقبول للتقنيات والتعرف على الحوادث والاستجابة لها. وفي هذا الصدد، عُقدت جلسات ربع سنوية للتوعية بالأمن السيبراني.

ب. التمارين السيبرانية

تم تنظيم ورش عمل لأعضاء البرنامج من مختلف الجهات ذات الصلة لتوضيح الأدوار والمسؤوليات والمتطلبات ذات الصلة بالأمن السيبراني في البرنامج وتمكين التنسيق المستمر فيما بينهم. وخلال ورش العمل هذه، تبادلت الجهات المعنية المعلومات بشأن التهديدات وأفضل الممارسات للاستجابة للتهديدات السيبرانية.

كذلك، تم توفير المزيد من التدريب عالي الجودة وبصفة منتظمة للموظفين من الجهات المعنية لتزويدهم بالمعرفة التقنية وغير التقنية بشأن الأمن السيبراني.

وفي إطار برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين تم تنفيذ العديد من التمارين السيبرانية، للتحضير لرئاسة مجموعة العشرين. إن التمارين السيبرانية تُعد محاكاة للهجمات والحوادث السيبرانية المحتملة؛ فهي تتيح اختبار مدى فعالية استراتيجية اكتشاف الحوادث والاستجابة لها، وتعزيز التعاون من أجل رفع مستوى الجاهزية والتنسيق بين الجهات المشاركة، وتعزيز قدرات الأمن السيبراني ورفع مستوى الوعي به من أجل الاستجابة للمخاطر والتهديدات السيبرانية المختلفة. وتعتبر تلك التمارين مهمة، ليس فقط من منظور الأمن السيبراني، وإنما لضمان إلمام جميع الجهات المعنية بجهود التحضير والمعالجة والتقليل من المخاطر والتهديدات. وقد تم تنفيذ العديد من التمارين، التي استهدفت في الأساس الجهات الوطنية ذات الصلة بمجموعة العشرين وغيرها من الجهات المعنية الرئيسية، كجلسات تفاعلية بحيث

يتعامل مسؤولو الاستجابة للحوادث السيبرانية مع العديد من السيناريوهات السيبرانية من خلال نظام المحاكاة. وقد تضمنت السيناريوهات أربعة أنواع من الهجمات: اختراق البيانات، والبرمجيات الخبيثة، وتشويه المواقع الإلكترونية، وحجب الخدمة الموزعة.
وتضمنت المنهجية أيضًا مراعاة المراحل الأساسية للاستجابة للحوادث السيبرانية، إذ تساعد تلك المراحل في تقييم شمولية العمليات وآثار القرارات والإجراءات خلال الحوادث التي تمت محاكاتها.

تم إجراء أكثر من **9 تمارين سيبرانية**، بمشاركة أكثر من **100 جهة**.

تم تنظيم أكثر من **60 ورشة عمل** للجهات ذات العلاقة بمشاركة مدراء وقيادات الأمن السيبراني في تلك الجهات.

وقد تم تحليل نتائج التمارين السيبرانية لتحديد وتصنيف نقاط القوة الأساسية والجوانب التي يمكن تطويرها لدى كل جهة مشمولة في النطاق، وتم الاسترشاد بذلك التحليل في إجراءات الحد من المخاطر والتهديدات التي تم تنفيذها للتغلب على أي تحديات وضمان توافر القدرات المناسبة للاستجابة للحوادث في حينها بهدف تعزيز الأمن السيبراني خلال سنة الرئاسة وخلال القمة الافتراضية للقادة، على وجه الخصوص.

المستوى الثاني: تعزيز صمود الأمن السيبراني خلال القمة الافتراضية للقادة

تجْمع قمة قادة مجموعة العشرين رؤساء الدول أو الحكومات في 19 دولة بالإضافة إلى الاتحاد الأوروبي، إلى جانب قادة الدول الضيوف وممثلي المنظمات الإقليمية والدولية المدعوّة للمشاركة. وقد عُقدت قمة قادة مجموعة العشرين لعام 2020م افتراضيًا يومي 21 و22 نوفمبر برئاسة خادم الحرمين الشريفين، الملك سلمان بن عبد العزيز آل سعود. وقد اعتمدت رئاسة مجموعة العشرين على نجاح القمة الاستثنائية الافتراضية لقادة المجموعة التي عُقدت في شهر مارس، ومخرجات ونتائج اجتماعات مجموعات العمل والاجتماعات الوزارية الافتراضية التي تجاوزت 100 اجتماع. وبالتالي، كانت هذه القمة هي أهم فعاليات مجموعة العشرين.

نظرًا لأهمية القمة الافتراضية لقادة المجموعة، كان لا بد من التعامل معها كنسخة مركزة تعكس وتعزز المنهجية المتبعة لتأمين الفعاليات طوال سنة رئاسة المجموعة. وكان هذا في غاية الأهمية، لا سيما وأن القمة الافتراضية للقادة عُقدت في عدة مواقع، مما زاد من مستوى تعقيد العمليات، فضلاً عن الحاجة إلى موارد إضافية لضمان الجاهزية المناسبة للأمن السيبراني.

وبالنسبة للمستوى الثاني، فقد تم تنفيذ كل مرحلة من النموذج المصمم وتعزيزها لتأمين القمة الافتراضية، وذلك على النحو التالي:

حوكمة البرنامج

تخصيص الأدوار والمسؤوليات المحددة على المستويات التنفيذية والإدارية والتشغيلية في المستوى الأول بما يتناسب مع عدد الجهات ذات العلاقة، على أن يشمل ذلك التنسيق الدائم والمباشر مع الموفر الوطني للبنية التحتية الرقمية المسؤول عن استضافة القمة الافتراضية.

التقييمات السيبرانية

إجراء العديد من التقييمات السيبرانية مع التركيز على الموفر الوطني للبنية التحتية الرقمية، بما في ذلك اختبار الاختراق وتقييمات المخاطر وتقييمات الثغرات وتقييمات الاختراق السيبراني وتقييمات الالتزام بضوابط الأمن السيبراني ومراجعات صلاحيات وصول المستخدمين ومراجعات إعدادات ومعمارية الأمن السيبراني.

العمليات السيبرانية

أُجريت المراقبة الأمنية على الموفر الوطني للبنية التحتية الرقمية، المسؤول عن استضافة القمة الافتراضية، والأمانة السعودية لمجموعة العشرين عن كثب وتطبيق خطة مصممة خصيصًا للحد من مخاطر الهجمات السيبرانية. وقد تضمّن ذلك خدمات وحلول حماية الأمن السيبراني مثل الوقاية من حجب الخدمة الموزعة وحماية البريد الإلكتروني.

وسعيًا للحد بشكل أكبر من أي مخاطر محتملة في البرنامج نتيجة العوامل الخارجية غير المتوقعة التي قد تؤثر على انعقاد قمة القادة، فقد تم تشكيل فريق إضافي للاستجابة للحوادث بالإضافة إلى الفريق الموجود بالفعل. وتكوّن هذا الفريق الإضافي من أخصائيي الاستجابة للحوادث الموجودين في المملكة العربية السعودية، وقد تم اختيارهم بحيث تضمن خبراتهم مجتمعة جاهزيتهم للعمل كفريق احتياطي في حالة وقوع أي حادث -لا قدر الله-.

التوعية بالأمن السيبراني والتمارين السيبرانية

بالإضافة إلى التمارين السيبرانية المنتظمة، أجريت العديد من التمارين المخصصة بما يتناسب مع طبيعة قمة القادة بهدف إعداد سبل الاستجابة لأي هجوم سيبراني محتمل وتحقيق التكامل فيما بينها. كذلك، تم تعزيز حملات التوعية وورش العمل لدعم التحضير للقمة وضمان انعقادها بسلاسة، مع تدريب جميع الجهات المعنية المشاركة وتحضيرها

لمواجهة أي حدث سيبراني -لا قدر الله-.

اشتملت خطة تعزيز الأمن السيبراني التي تم تنفيذها خصيصًا من أجل تأمين القمة الافتراضية على العناصر الأساسية في برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين، وقد تم إعدادها لحماية الأصول الحيوية الرئيسية، مع ضمان سير أعمال القمة بسلاسة في الوقت نفسه. وتمثل تلك الخطة في حد ذاتها استراتيجية فعالة لتأمين أي فعالية عالمية، فضلاً عن تحقيقها للجاهزية والصمود المطلوبين للأمن السيبراني.

الشكل 8

التوصيات والدروس المستفادة

تم استخلاص عدد من الدروس المستفادة والتوصيات من تعزيز الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين.

المشاركة والدعم القيادي

في ظل التغيرات المتسارعة التي شهدها العالم مع جائحة فيروس كورونا المستجد كانت المشاركة القيادية حاسمة لإدراك الواقع سريعًا ووضع رؤية استراتيجية جديدة مع السعي لتحقيقها.

وقد فتح القرار التنفيذي المُتخّذ لنقل فعاليات رئاسة مجموعة العشرين بالكامل إلى المنصات الافتراضية مجالاً جديدًا لاستضافة وتأمين الفعاليات الضخمة، كان لدعم القيادة الرشيدة الدور الأكبر في تمكين نجاح البرنامج الذي اعتمد على حوكمة النموذج وتنفيذ أنشطته. ومع زيادة آثار الجائحة وتطور طبيعة التهديدات تبعًا لذلك، تم تنفيذ آليات الإشراف والدعم المستمر من القيادة لضمان المراجعة المستمرة وإجراء التحسينات بصفة فورية.

كما مكّنت القيادة الرشيدة الأمانة السعودية لمجموعة العشرين من خلال حشد الموارد والقدرات اللازمة لها لضمان نجاح النموذج وتحقيق أهداف برنامج جاهزية وصمود الأمن السيبراني خلال سنة رئاسة المملكة لمجموعة العشرين بهدف تأمين فعاليات رئاسة المجموعة وقمة القادة.

قيمة البيانات والحوكمة وتصميم النموذج

يُعد إيجاد البيانات الكافية والمعلومات ذات الصلة عن تجارب فعاليات مجموعة العشرين السابقة وغيرها من الفعاليات الضخمة أمرًا معقدًا. ففي حين تعذّر إيجاد أي منهجية أو نهج معترف به على الساحة الدولية يمكن الاسترشاد به، كان من الضروري للغاية تصميم نموذج يتيح وضع استراتيجية ناجحة ومستدامة. كما كان من المهم للغاية تطوير وتوثيق التجربة للمساهمة في تطور مجتمع الأمن السيبراني ككل.

وبالتالي، يوصى دائماً بعقد ورش عمل بالتعاون مع الدول المستضيفة للفعاليات الضخمة السابقة؛ بحيث يمكن مشاركة البيانات والمعلومات وتحليلها. وتُعد النتائج الرئيسية المستخلصة من البيانات المجمعة في غاية الأهمية لتحديد المجالات والمحاور ذات الصلة بالفعالية نفسها، والتي تتطلب التحليل بدورها وفق نموذج يتيح استخلاص الغاية والأهداف والمستهدفات، مما يسفر بدوره عن تحديد الكفاءات والخبرات المطلوبة. بالإضافة إلى أن تشكيل فريق من الجهات المعنية الوطنية –يضم أطرافًا خارجية – وتحديد الأدوار والمسؤوليات المنوطة بها في كل مجال سيساعد في تحقيق التكامل بين مجالات الخبرة المختلفة. كما إن تحديد الأدوار والمسؤوليات للنموذج سيتيح القدرة على الصمود في وجه الأحداث السلبية، إذ تكون كل جهة معنية على وعي تام بوظيفتها ومسؤولياتها للتعامل مع أي عائق.

ويمثل النموذج السعودي منهجية موصى بها للدول التي ستتسلم رئاسة مجموعة العشرين في المستقبل، إذ يركز على إنشاء إدارة للأمن السيبراني ضمن أمانة مجموعة العشرين لضمان أن يكون للأمن السيبراني دور أساسي على المستويين الإداري والتشغيلي.

الحاجة للمرونة والتنسيق مع الشركاء

لقد وصلت جائحة فيروس كورونا المستجد (كوفيد-19) إلى جميع أركان العالم، مما أسفر عن آثار طويلة الأجل على حياة جميع البشر فحينما ظهرت الجائحة خلال سنة رئاسة المجموعة؛ أصبح من الواضح أن عقد الفعاليات حضوريًا سيمثل خطورة على المواطنين في أنحاء المملكة وعلى مستوى العالم. وفي الوقت الذي بدأت فيه الدول حماية أنفسها في سبيل مكافحة انتشار الفيروس اتخذت المملكة قرارًا تنفيذيًا بنقل فعاليات رئاسة المجموعة بالكامل، ومن بينها قمة القادة، إلى المنصات الافتراضية واتضح حينها جدوى التحول الرقمي والاتصالات الآمنة وأنه سيكون بديلاً عمليًا لعقد الفعاليات.

وقد تحقق تأمين فعاليات مجموعة العشرين الرقمية بالكامل بالاستناد على النموذج الأصلي الذي كان يعتمد على الصمود والالتزام بالتعافي من آثار الأحداث السلبية. وفي حين كان الأمن السيبراني في صميم النموذج الأصلي، الأمر الذي ضمن جاهزية وصمود الأمن السيبراني، كان لا بد من تنفيذ عدد من الأنشطة الإضافية العاجلة بصورة سريعة.

وفي ظل زيادة مصادر الهجمات السيبرانية والآثار المحتملة لها تم تعزيز النموذج بشكل سريع لإشراك جهات معنية جديدة والاستفادة من العلاقات الوطيدة القائمة لتعزيز القدرات ورفع مستوى مراقبة الأمن السيبراني الموجودة. وفي هذا الإطار تم تحديث الأدوار والمسؤوليات المنوطة بالجهات المعنية الرئيسية لتعزيز التواصل والتنسيق فيما بينها، إلى جانب إرساء نقاط لمعالجة التحديات وتصعيدها لضمان الاستجابة الفورية وتعزيز صمود الأمن السيبراني.

التحضير المبكر وإمكانية التوسع في الجهود

تتضمن أعمال مجموعة العشرين سلسلة من الاجتماعات والفعاليات وورش العمل، وقد استلزم عقدها افتراضيًا التأقلم مع الوضع والتوسع في الجهود لتأمين تلك الفعاليات لذلك؛ كان التحضير المبكر لفعاليات مجموعة العشرين من أهم الخطوات، إذ كشف ذلك عن الفجوات التي تتطلب مزيدًا من الخبرات والقدرات، كما أتاح الوقت لتلبية تلك الاحتياجات.

وقد تم الاستناد على إطار وإجراءات إدارة الحوادث السيبرانية لدى الهيئة الوطنية للأمن السيبراني بما يتناسب مع فعاليات مجموعة العشرين، مما أتاح لرئاسة المجموعة ضمان اتباع الجهات المعنية لمنهجية متسقة في إدارة حوادث الأمن السيبراني.

وبالتالي، يوصى بتشكيل فرق مخصصة للاستجابة للحوادث، ليس من أجل فعاليات مجموعة العشرين فحسب، وإنما أيضًا من أجل الفعاليات ذات الأهمية البالغة، مثل قمة القادة. ويتيح التوسع في قدرات الاستجابة للحوادث للمتخصصين إمكانية الاستجابة للعديد من الحوادث في الوقت نفسه.

كذلك، من أفضل الممارسات الموصى بها أن تتم الاستفادة من الخطط والقدرات والمنهجيات الموجودة في مختلف المجالات، فغالبًا ما يلزم تعديلها وتخصيصها وتعزيزها بحيث تتناسب مع الظروف الخاصة.

إدارة النطاق

من الخطوات الأساسية في تأمين أي فعالية كبرى تحديد الجهات ذات العلاقة المباشرة وغير المباشرة. ويشمل ذلك أصول تقنيات المعلومات وتنظيم الفعاليات، والتي يجب تحديد الجهات المسؤولة عنها بوضوح لضمان استيعاب كل جهة معنية لأدوارها ومسؤولياتها.

علاوةً على ذلك، يجب تحديد الارتباطات الخارجية والأطراف الأخرى المعنية وسلاسل الإمداد والتموين ووضعها في الاعتبار حتى يمكن وضع خطط مناسبة للحد من المخاطر والتهديدات السيبرانية. كما يجب تحقيق التوازن بين السماح لتلك الجهات بالعمل بشكل مستقل وبين توفير المستوى المناسب من حماية ومراقبة الأمن السيبراني. ويجب أيضًا وضع منهجية متسقة مع شمولية التوزيع الجغرافي للجهات المختلفة، والتنسيق لها بشكل وثيق. ويمكن تحقيق ذلك من خلال عقد شراكات قوية وفعالة، إلى جانب مشاركة المعلومات، مع جميع الجهات المعنية الرئيسية.

وأخيرًا، عند إدارة نطاق البرنامج، يجب مراعاة حماية البنية التحتية لجميع الجهات المشاركة في منظومة فعاليات مجموعة العشرين ككل، بالنظر إلى تفاوت قدرات ومهارات الأمن السيبراني بين الجهات المختلفة في كثير من الأحيان.

أهمية التقييمات السيبرانية المنتظمة

من خلال التقييمات المنتظمة، يمكن للمتخصصين المسؤولين عن الأمن السيبراني لفعاليات مجموعة العشرين تحديد الثغرات في الأصول بشكل فوري و اتخاذ الإجراءات اللازمة للحد من المخاطر. وقد تضمَّن النموذج السعودي مجموعة من التقييمات، مثل اختبار الاختراق وتقييم الثغرات وتقييم الاختراق السيبراني و مراجعة إعدادات ومعمارية الأمن السيبراني. و بالنظر إلى ارتفاع عدد التقييمات المطلوبة لضمان أمن فعالية بحجم مجموعة العشرين، جمع النموذج السعودي بين التقييمات المباشرة التي أجرتها أمانة مجموعة العشرين و التقييمات الذاتية التي أجرتها الجهات

المختلفة. وكان من الضروري وضع خطة للحد من مخاطر التهديدات السيبرانية وأن تتضمن تشكيل فريق مخصص للاستجابة للحوادث السيبرانية، بالإضافة إلى الفريق المعتاد.

فهم خصائص الجهات المستهدفة وإشراكها

تنطوي الفعاليات الضخمة مثل فعاليات مجموعة العشرين على العديد من الجهات المعنية الداخلية والخارجية، وبالتالي، من الضروري إطلاق حملات توعية لتسليط الضوء على أهمية الأمن السيبراني وتمكين الأفراد من المساهمة في تحقيقه، للتقليل من المخاطر السيبرانية.

ولضمان نجاح هذه العملية في تحقيق النتائج المنشودة، تحدد الجهات المستهدفة الكوادر المناسبة لاستفادة من هذه الحملات، بما في ذلك الأفراد الذين قد يكون لهم أدوار ومسؤوليات محددة. كما يجب تخصيص حملات التوعية وفقًا لذلك، بناءً على معرفة الجهات المعنية بالأمن السيبراني.

وتفيد التمارين السيبرانية وورش العمل والبرامج التدريبية في تعريف المشاركين بالتهديدات والمخاطر السيبرانية التي قد تواجهها الفعالية ومسؤولياتهم للحد منها. وبالنظر إلى حجم فعاليات مجموعة العشرين فإن الجهات المستهدفة كبيرة ومتنوعة، ومن الضروري إشراك الأفراد المناسبين. كما يجب تصنيف الجهات المعنية بحسب الأدوار المنوطة بها وتنظيم تمارين وبرامج تدريبية محددة تتناسب مع مسؤوليات كل مجموعة.

ويمكن من خلال هذه الحملات أن يدرك جميع الأفراد الذين لهم دور أساسي في تأمين فعاليات مجموعة العشرين الآثار المترتبة على اتخاذ قرارات أو إجراءات معينة، ومن شأن ذلك أن يحسن من جاهزية الأمن السيبراني بوجه عام. كذلك، يمكن تحديد السيناريوهات ومحاكاتها لتحسين الاستجابة للمخاطر السيبرانية. ومن المفيد بشكل خاص إجراء المناورات والتمارين السيبرانية خلال الأحداث غير المتوقعة، مثل جائحة فيروس كورونا المستجد، إذ يعزز ذلك من مرونة الأفراد وقدرتهم على مواجهة الأحداث غير المتوقعة.

بالإضافة إلى ذلك فقد كان لوجود نقاط اتصال وقنوات تواصل بين الهيئة الوطنية للأمن السيبراني والجهات المعنية الرئيسية دور كبير في تيسير التواصل الفوري والمستمر، وكان هذا جوهريًا في الاستجابة الفعالة. وتجدر الإشارة إلى أهمية تحديد وتقنين تلك القنوات لتعزيز التعاون والاستجابة بين الجهات المعنية الرئيسية.

الخاتمة

تشرفت المملكة العربية السعودية باستضافة أبرز القادة والوزراء والوفود على مستوى العالم خلال رئاستها لمجموعة العشرين في عام 2020م وحرصت على تعزيز رسالة القمة لاغتنام فرص القرن الحادي والعشرين للجميع. وبالنظر إلى حجم المشاركين في مجموعة العشرين وتنوعهم، وكذلك مدة فعالياتها، تمثل المجموعة منتدىً رائدًا للتعاون الدولي؛ ففضلاً عن حشد الموارد والخبرات والقدرات من أجل غاية مشتركة، فإن نتائج فعاليات المجموعة توفر زخمًا إيجابيًا لمواصلة التنسيق للعمل على المشاكل التي تواجهها مجتمعاتنا جميعًا.

و مع استمرار الاهتمام المتزايد بالأمن السيبراني على الصعيد العالمي، برزت أهميته بشكل أكبر بسبب الحاجة إلى نقل معظم فعاليات مجموعة العشرين، ومن بينها القمة الافتراضية للقادة، إلى المنصات الرقمية وضرورة تأمينها.

وبالتالي، كان لا بد من مواءمة التحضيرات الدقيقة والمتأنية التي اتُخذت لإقامة الفعاليات حضورياً، ووضع تصور مستحدث لها لتتوافق مع الواقع الرقمي الجديد.

وعلى ضوء ذلك، تم تصميم النموذج بالاعتماد على الخطط والقدرات الموجودة وبالاعتماد على التجارب السابقة وخبرات الهيئة الوطنية للأمن السيبراني بهدف تطوير نموذج قادر على الصمود.

وقد ساهم هيكل الحوكمة في الاستفادة من الكوادر الوطنية المؤهلة في هذا المجال، وكان ذلك ضروريًا لتأمين فعاليات سنة الرئاسة. وتحقق ذلك من خلال تعزيز قيمة قنوات التواصل الموجودة والتنسيق لمشاركة المعلومات على مدار العام.

بالإضافة إلى ذلك، تم تحديد الأدوار والمسؤوليات المتعلقة بعمليات الأمن السيبراني على مدار العام، وتضمّن ذلك إجراء تقييمات الأمن السيبراني، و نمذجة التهديدات السيبرانية و مراقبة الأمن السيبراني، و الاستجابة الصارمة للحوادث. كذلك، تم إطلاق حملات التوعية والتمارين السيبرانية، لتعزيز ثقافة الأمن السيبراني لدى جميع الجهات المعنية الرئيسية. وقد أدت جميع الجهود التي بُذلت خلال سنة الرئاسة إلى أهم فعالية ضمن فعاليات مجموعة العشرين، وهي القمة الافتراضية للقادة، وحينها تم التوسع في جميع جهود النموذج السعودي للأمن السيبراني وتعزيزها.

https://nca.gov.sa/ Info@nca.gov.sa NCA_KSA