// سلطنة عمان

هيئة تقنية المعلومات//

الدليل الاسترشادي لحوكمة الأمن السيبراني

المديرية العامة للسياسات والحوكمة

// سلطنة عمان

هيئة تقنية المعلومات//

الإصدار والتوزيع

	الاسم	البريد الإلكتروني	تاريخ الإصدار
إصدار:	المديرية العامة للسياسات والحوكمة	standards@ita.gov.om	2017
مراجعة:			
اعتماد:	اللجنة التوجيهية		

قائمة النشر	
-1	هيئة تقنية المعلومات
-2	الجهات الحكومية المعنية
-3	الموقع الإلكتروني

سجل الوثيقة:

النسخة	التاريخ	الجهة المُصدِرة	ملاحظات
1	2017	المديرية العامة للسياسات والحوكمة	النسخة الأولية للمستند

// سلطنة عمان

هيئة تقنية المعلومات//

جدول المحتويات

// سلطنة عمان

هيئة تقنية المعلومات//

1- مقدمة

نشأ الأمن السيبراني ضمن مجالات أمن المعلومات بغية التصدي لتفشي الجرائم الإلكترونية وفي بعض الأحيان الحرب السيبرانية. وهناك ثلاثة عوامل تساهم في الحاجة إلى الارتقاء بمستوى الأمن السيبراني وتطويره على النطاق العالمي والشامل، ألا وهي: تقنية النطاق العريض الموسع والشركات والمجتمعات التي تركز على استخدام تقنية المعلومات والتدرج الاجتماعي للمهارات في مجال تقنية المعلومات. ولكي يتسنى ذلك والتعامل مع التغيرات الحاصلة في المجتمعات، عكفت الكثير من الحكومات الوحدات على إطلاق مبادرات في الأمن السيبراني تتنوع بين المبادرات الإرشادية وتلك التي تُعنى بوضع المعايير والتشريعات والأنظمة الشاملة. ويعتبر هذا المستند بمثابة خطوة أولية في الطريق نحو تحقيق ذلك الهدف حيث يعمل على تقديم الإرشادات العملية ذات الصلة به والتي يمكن تطبيقها على أرض الواقع بما يتماشى والممارسات الدولية المقبولة.

1-1الفئات المستهدفة

يستهدف هذا المستند فئات عديدة ممن يتعاملون مع الأمن السيبراني بشكل مباشر أو غير مباشر بما فيهم مدراء الأعمال ومدراء أمن المعلومات ومدراء مخاطر تقنية المعلومات والمستخدمين النهائيين ومدققي تقنية المعلومات.

1-2الغرض

يتمثل الغرض الرئيسي من إعداد هذا المستند في وضع إطار موحد للجهات الحكومية في مجالات إدارة المخاطر وإدارة الشؤون الأمنية والحوكمة، بالإضافة إلى تقديم ارشادات عن المفاهيم والإجراءات التفصيلية لإحداث التحول في الأمن السيبراني وضمان اتساقها مع استراتيجيات أمن المعلومات المطبقة.

ويُعنى هذا المستند أساسًا بأنواع الهجمات السيبرانية التي تنطوي على مخاطر عالية بالنسبة للوحدات والشركات التابعة لها، وهو يُعد بمثابة وثيقة تكميلية عن أمن المعلومات يمكن للمنشآت والأفراد الاستعانة بها في مواءمة استراتيجياتهم الأمنية بطريقة شاملة ومنهجية. كما أنه يركز بشكل رئيسي على إحداث التغيير والتطور في الأمن الإلكتروني على مستوى الوحدات من أجل تعزيز سبل دفاعها ضد الهجمات الإلكترونية ودمج الأمن السيبراني ضمن النهج الشامل المتبع فيما يتعلق بحوكمة الأمن السيبراني وإدارة المخاطر والالتزام.

2- ما هو الأمن السيبراني؟

انتشر استخدام مصطلحات الأمن السيبراني والجريمة والحرب السيبرانية باعتبارها مفردات أساسية في عالم الأمن بوجه عام. ويُعزى ذلك في المقام الأول إلى الزيادة في الاختراقات الأمنية والأعمال الاجرامية ووجود أسلحة الحرب المعلوماتية، وفي جزء منه إلى الثورة التكنولوجية الهائلة.

يتطلب مصطلح "الأمن السيبراني" في سياق أمن المعلومات تفسيرًا لأنه عادة ما يُساء فهمه ويُستخدم على نطاق واسع للغاية. ولأغراض هذا المستند، يشمل الأمن السيبراني كافة الممارسات التي من شأنها أن تحمي الوحدات والأفراد من الهجمات والحوادث والانتهاكات المقصودة، فضلاً عما يترتب عليها من عواقب. ومن الناحية العملية، يُفيد الأمن السيبراني بشكل أساسي في التصدي لهذه الأنواع من الهجمات والاختراقات والحوادث التي يصعب اكتشافها أو التعامل معها. كما أصبح من الممكن التعامل مع الهجمات والجرائم الانتهازية بالاستعانة باستراتيجيات وأدوات بسيطة ولكنها تجدي نفعًا في هذا الخصوص. لذا، يركز الأمن السيبراني على ما يُعرف باسم الحرب السيبرانية والتهديدات المستعصية المتقدمة ومدى تأثيرها على الوحدات والأفراد.

وبغض النظر عن الاستخدام الشائع للمصطلح، فيجب إدراج متطلبات الأمن السيبراني ضمن الإجراءات التي تطبقها الوحدات الحكومية بما يتماشى وكافة الجوانب الأخرى لأمن المعلومات بحيث تشمل الحوكمة والإدارة والضمان للأمن السيبراني. وتجدر الإشارة في هذا السياق إلى إن مفهوم الأمن يتسم بالشمولية أكثر من كونه مباشرًا ومحددًا مع الاعتراف بفكرة أنه يتطلب إجراء صيانة وتحسين مستمر للوفاء باحتياجات ومتطلبات الجهات المعنية.

2-1 الجريمة السيبرانية والتهديد المستعصي المتقدم (APT)

في عالم التهديدات وسيناريوهات المخاطر ونقاط الضعف، قدم الأمن السيبراني استجابة مرنة لأنواع متعددة من الهجمات والانتهاكات والحوادث.

وتتفاوت درجة تواتر الهجمات وشدتها وتعقيدها إلى حد كبير بداية مما يمكن تسميته بالهجمات غير الضارة إلى الهجمات الغريبة والمعقدة للغاية على هدف تمت دراسته جيدًا.

يشمل التهديد المستعصي المتقدم (APT) الهجمات والاختراقات والتسريبات والأحداث الأخرى المتعلقة بالأمن بمستوى من مرتفع إلى مرتفع جدًا من المجهود (أو التعقيد) ونهج يستهدف وحدات حكومية أو أفراد معينة. وفي معظم الحالات يتضمن ذلك جهد لا بأس به في البحث عن المعلومات وجمعها، بالإضافة إلى التخطيط والتحضير بشكل تفصيلي. فعادة ما تكون تلك التهديدات عبارة عن مجموعة من الخطوات يتمثل الغرض المتوخى منها في زيادة الأثر الواقع على الهدف إلى أقصى حد، فكثير من التهديدات المستعصية المتقدمة لها خلفية مهنية او خلفية جريمة منظمة. وعلى عكس الأشكال الأصغر من الهجمات، يتضمن تنفيذ التهديدات المستعصية المتقدمة بذل مجهود لا يستهان به من حيث العامل الزمني والاستثمار. وحسب الهدف ومدى قابلية استقطابه، قد تتضمن التهديدات المستعصية المتقدمة حلولًا مخصصة ويمكن تطبيقها لمرة واحدة فقط.

كما أنه يصعب التعرف عليها والتنبؤ بها وغالبًا ما يصعب أيضًا تتبعها لمعرفة مصدرها أصولها مقارنة بالأدوات المنتشرة على نطاق أوسع ومتوفرة للعامة.

2-2 الحرب السيبرانية

تمثل الحرب السيبرانية المفهوم الأوسع للتهديدات المستعصية المتقدمة. فعندما تشارك الهيئات الحكومية في الهجمات التي تُشن على البنى التحتية الأساسية أو الوحدات الحكومية الهامة، تزداد حدة التهديدات نظرًا لحقيقة أن المهاجمين قد يكون لديهم بطبيعة الحال موارد ومصادر لا حصر لها تحت تصرفهم. ويشمل ذلك الوقت كمورد، حيث إن العمليات العسكرية أو الحكومية قد تستغرق عدة أعوام بداية من الفكرة الأولية وحتى التنفيذ.

ومع ذلك، فمن الناحية الفنية والإدارية تمثل الحرب السيبرانية مجرد شكل آخر من التهديدات المستعصية المتقدمة على الرغم مما يترتب عليها من عواقب قانونية واجتماعية.

لذلك، يجب أن يشمل الأمن السيبراني احتمالية العواقب المباشرة وغير المباشرة من نشاط عسكري أو حكومي مستهدف موجه ضد الوحدات الحكومية والشركات التابعة والبنى التحتية الحيوية. ومن حيث التأثير، تكون عواقب الحرب الصريحة أو المقنعة مشابهة تمامًا للعواقب المترتبة على الأعمال الإجرامية أو القرصنة ذات الدوافع السياسية.

3-2تهديدات أخرى ذات صلة

رغم أن الجريمة السيبرانية والظواهر المرتبطة بها قد شهدت زيادة غير ثابتة في الآونة الأخيرة، إلا أنه قد ترسخت أشكال أخرى من التهديدات والهجمات، منها النشاط السياسي والاختراق في المجال الرياضي و الضرر المستهدف لسمعة الوحدات. وغالبًا، لا يمكن التنبؤ بهذه الأشكال من الهجمات وقد لا يتمكن مديرو الأمن من توقع حدوثها. من هذا المنطلق، فهي تعتبر بمثابة مخاطر محتملة وتهديدات مجهولة يجب التعامل معها على هذا الأساس. من هنا، يستلزم الأمر عناصر استراتيجية تتعامل مع كل ما هو غير متوقع ومجهول بحيث تشتمل على عناصر أخرى لاستمرارية الأعمال وخدمات تقنية المعلومات. وبالتالي، يجب أن تدرس استراتيجيات الأمن وأنشطة الإدارة التهديدات والحوادث المجهولة مع الإشارة إلى مفاهيم إدارة استمرارية الأعمال وخدمات تقنية المعلومات متى كان ذلك مناسبًا.

3-مباديء حوكمة الأمن السيبراني

تشكل حوكمة وإدارة والمحافظة علىتدابير الأمن السيبراني تحديًا لمدراء الأعمال ومدراء أمن المعلومات والمدققين على حد سواء. ولعرض القيمة التجارية للأمن السيبراني ولمعادلة الخطر المصاحب للهجمات أو الانتهاكات، يجب تطبيق الإرشادات التالية. وبالرغم من أن هذه المبادئ وضعت على مستوى عالي وليس شاملاً، إلا أنها تقدم مبدأ معقولا للأمن السيبراني كجزء لا يتجزأ من نظام أمن المعلومات الشامل.

مبدأ1. التعرف على التأثير المحتمل للجرائم والحرب السيبرانية

إن مفهوم الأمن السيبراني يجب أن يسلط الضوء على الضرر المحتمل والتأثيرات واسعة النطاق للجرائم والحرب السيبرانية. ولكي نقوم بإدارة الأمن السيبراني على نحو ملائم، يلزم معرفة المستويات المحتملة للخطر والتأثير التجاري أو تقديرها بشكل متحفظ. ويشمل ذلك المعرفة المتعمقة للطريقة التي قد يُستهدف بها المستخدمون النهائيون ومدى تأثرهم بهجمات وحوادث الأمن السيبراني.

مبدأ2. فهم الثقافة المؤسسية والفردية وأنماط السلوك

تتأثر القيمة التجارية والخطر التجاري المتعلقان بتدابير الأمن السيبراني بشدة بالثقافة المؤسسية والفردية. ويتجلى ذلك في أنماط سلوك المستخدمين النهائيين والعادات والفعاليات الاجتماعية. وعند حوكمة وإدارة الامن السيبراني، يجب أن تؤخذ هذه العوامل في الحسبان وتدمج في مقاييس أمن المعلومات الاستراتيجية والتكتيكية والتشغيلية...

مبدأ3ا تحديد دراسة الجدوى بوضوح فيما يتعلق بالأمن السيبراني ومدى تقبل الوحدة للمخاطرة

سوف تحدد دراسة الجدوى استراتيجية الأمن السيبراني العامة التي تطبقها الوحدة من حيث القيمة المتوقعة والمخاطر المحتملة: الجهد اللازم والاستثمار في منع حدوث الخطر، مقابل المخاطر المتبقية وكيفية التعامل معها. ولضمان الوصول إلى تطبيق إجراءات أمنية كافية ومناسبة، يلزم تحديد دراسة الجدوى بوضوح ويجب أن تفهمها جميع مستويات الإدارة بشكل كامل بحيث يشمل ذلك الاعتبارات المتعلقة بالتكلفة والفوائد، بالإضافة إلى الثقافة والقيم المؤسسية السائدة المتعلقة بالأمن السيبراني.

مبدأ4 إرساء دعائم حوكمة الأمن السيبراني

يُشكل الأمن السيبراني جزءًا لا يتجزأ من قيم الوحدة وأهدافها. وبناءً عليه، فهو يخضع لقواعد حوكمة واضحة توفر الإرشادات والتوجيهات اللازمة، فضلاً عن وضع الحدود المعقولة والمقبولة. وتشمل هذه القواعد اعتماد إطار الحوكمة المؤسسية للأمن السيبراني وتعزيزه.

مبدأ 5 المعرفة بأهداف ضمان الأمن السيبراني

يغطي الأمن السيبراني جوانب ومجالات متعددة ومتخصصة ضمن نظام أمن المعلومات الشامل. فعلى الرغم من أن أهداف ضمان الأمن السيبراني واضحة ومعقولة ويسهل التعامل معها، إلا أنه يتم أخذ المخاطر والمسائل المرتبطة به في الاعتبار نظرًا لأن العديد من جوانب الأمن السيبراني قد تكون خارج نطاق سيطرة الوحدة.

مبدأ6 إرساء دعائم الأمن السيبراني الشامل وتطويره

تستهدف الجريمة والحرب السيبرانية والهجمات والاختراقات الرابط الأضعف في النظام. ولذلك، يجب التعامل مع الأمن السيبراني على أنه عبارة عن منظومة من العناصر المترابطة ببعضها البعض تتطلب فهما شاملاً لهذه المنظومة الديناميكية وإدراك حقيقة أنه لا يمكن النظر إلى الحوكمة والإدارة والضمان للأمن السيبراني بمعزل عن بعضهم البعض.

4-التحول في الأمن السيبراني

يقوم التحول في الأمن السيبراني -شأنه شأن أي عملية أخرى طويلة الأجل- على التحسن المستمر والتتابع من خلال مستويات متنوعة من النضج. ويعني هذا أيضًا أنه يلزم مراجعة الاستراتيجية والعناصر المرتبطة بها والتصديق عليها بصفة منتظمة مع مراعاة أية تغييرات قد تطرأ على ملف المخاطر ومدى تقبل الوحدة لها.

يعرف التحول عادة على أنه تغير شامل من حالة مستقرة للنظام إلى المستوى التالي لها وبينهما قد يحدث مجموعة من التغيرات سواء من تلقاء نفسها أو بطريقة يمكن التحكم فيها. وفيما يتعلق بالأمن السيبراني، يمكن تعريف التحول على أنه تطوير النظام الكلى للأحكام المنظمة وأنشطة الإدارة والضوابط والعناصر الأخرى من حالتها الراهنة الي الحالة (المستهدفة) التالية المستقرة بواسطة إجراء تغييرات يمكن التحكم فيها عادة على عناصر وعمليات معينة ومكونات أخرى. وعلى الرغم من أن هذا التعريف يعتبر مفيدًا كتعريف رفيع المستوى، إلا أن بعض الأمثلة قد تساعد في فهم عملية التحول.

4-1تحديد الوضع الراهن

يجب في المقام الأول تقييم وتحديد الوضع الراهن للأمن السيبراني ونموذج الحوكمة المعمول به. ويعني هذا أنه بعيدًا عن الافتراضات التي ربما قد وجدت مسبقًا، يلزم وصف الأمن السيبراني بحالته الراهنة بما فيه من مواطن ضعف وأوجه قصور. ففي الغالب، يشمل ذلك مواطن الضعف التي تم تحديدها مسبقًا (يرجى الرجوع إلى القسم السابق) ونقاط الضعف التي قد أظهرت الحاجة إلى التحول. ويكمن الهدف الأساسي من ذلك في التحول من الملاحظة الأولية التي تفيد بأننا "لا يمكننا أن نستمر على هذا النحو" إلى رؤية تتسم بالمزيد من الإيجابية بشأن الحوكمة والإدارة والضمان لأمن المعلومات.

كما أن دراسة الوضع الراهن تساعد في الكشف عن مواضع الضعف في المواقف الإدارية. ويتبين مما تم ذكره سابقاً، استبعاد احتمالية أن يجدي الاتجاه القائم على خفض المخاطر إلى الحد الأدنى أو منعها نفعًا. كما أن جزء من عملية إنشاء دراسة الجدوى هي التعريف بالوضع الفعلي للوحدة من حيث المواقف والمعتقدات وسلوك الإنفاق الأمني. وموجز القول، قد يقدم نموذج الحوكمة الذي اختارته الوحدة على معلومات ومرئيات شاملة ودقيقة بشأن ما الذي أدى إلى الحالة الراهنة غير المرضية ظاهريًا.

فعلى الرغم من أن هذا التقييم يعتبر عملية مضنية للغاية، غير أنه يُعد عنصرًا أساسيًا لا يمكن الاستغناء عنه كنقطة بداية في التحول في الأمن السيبراني. وعندما تدرك الوحدة مواطن الضعف بشكل لا يتخلله شك ومبين بوضوح، ستصبح قادرة على تطبيق طريقة محسنة لإدارة الامن السيبراني.

2-4 تحديد الحالة المستهدفة

بمجرد تحديد الوضع الراهن للأمن السيبراني وإدراكه بشكل كامل، يمكن عندئذ تحديد الحالة المستقبلية أو المستهدفة بناءً على مواطن الضعف وأوجه القصور والمخاطر وإلى أي حد ستكون الوحدة قادرة على التغيير والتكييف مع ما هو سائد وشائع في الهجمات والاختراقات والحوادث السيبرانية. وعندما تكون الحالة المستهدفة غير مفهومة بوضوح، قد لا يجدي نهج التحول نفعًا حينها.

وتشمل العقبات التي لا يمكن إدراكها ما يلي:

- الافتقار إلى الواقعية- حيث يتم تحديد الحالة المستهدفة بشكل مثالي، بدلاً من الوضع الراهن الواضح (والمستقر) لنظام الأمن السيبراني الشامل.
- تصعيد الالتزام- تحدد الحالة المستهدفة على أنها أكثر قليلا مما نقوم بفعله الآن دون دمج التهديدات المتغيرة ومواطن الضعف دون الحاجة إلى ذكر الهجمات والاختراقات الفعلية.
- الرؤية الضبابية- تحدد الحالة المستهدفة بناءً على افتراضات خاطئة-مثلا عندما لا تقوم الإدارة المؤسسية بدمج الاتجاهات المستقبلية في الجريمة والحرب السيبرانية.
- التحيز لنموذج الحوكمة- يتم الإبقاء على نموذج الحوكمة الراهن (مثلا اعتماد النهج القائم على منع المخاطر أو ذلك القائل بأننا "نحن مؤمنين") مع تجاهل الإشارات القوية التي قد تدل على وجود اختلال وظيفي أو افتقار إلى الفعالية.

فيكون الهدف من منظور الحوكمة هو تحديد المستوى التالي المستقر-وبالتالي الممكن تحقيقه والذي عنده سيكون الأمن السيبراني قادرًا على الوفاء بمتطلبات الجهات المعنية وعنده سيكون هناك مستوى معقول من الحماية من الهجمات والاختراقات السيبرانية. ويُعد التحول في الأمن السيبراني ممارسة تكرارية تشبه دورة الحياة أكثر من كونه مشروعًا يُنفذ لمرة واحدة.

3-4التحول الاستراتيجي والشامل

يعتمد أمر التحول في الأمن السيبراني الشامل من الوضع الراهن والحالة المستقبلية على الحوكمة والإدارة. فبمجرد تحديد الحالة المستهدفة، يوجد بعدان للتغيير يجب التخطيط لهما وإدارتهما ومراقبتهما. فيشمل **البعد الاستراتيجي** وضع الاستراتيجيات والخطط وتطبيق الإجراءات رفيعة المستوى والبرامج ذات الصلة بمشروعات الأمن السيبراني. ويتناول **البعد الشمولي** التبعيات وأوجه الترابط بين عناصر نظام الأمن السيبراني التي من شانها التأثير على الكيفية التي يمكن بها تحقيق التغيير وماهية التأثيرات الفورية والثانوية.

ويعني التحول في الأمن السيبراني بطريقة شاملة أنه سيكون هناك حاجة لدراسة أي تغيرات فيما يتعلق بالآثار غير المرغوبة. كمثال، قد يكون نشر برنامج توعية للموظفين مفيدًا من حيث توخي الحذر والاهتمام بالتفاصيل.

ومع ذلك، قد تتمثل تلك الآثار في أن العديد من النتائج الإيجابية الخاطئة تزيد من تكلفة إدارة الحوادث وتصـــرف الانتباه عن الهجمات المســتمرة المتقدمة الحقيقية (ولكنها غير مزعجة). كما أنه قد توجد تبعيات أكثر تعقيدًا في أنظمة الأمن الســيبراني والتي لن تظهر إلا إذا تم النظر إلى التحول على اعتبار أنه ممارسة منهجية وشاملة.

5- إرساء دعائم حوكمة الأمن السيبراني

بوجه عام، تضـــع حوكمة أمن المعلومات إطارًا وحدودًا لإدارة الأمن والحلول ذات الصـــلة بها. ويتضـــمن ذلك بالضـــرورة الســـياســـات والإجراءات الرسمية والإرشادات التي تلتزم الوحدات الحكومية باتباعها وتطبيقها. وعلى أية حال تعني الحوكمة في أفضل معنى لها "الأداء السليم"، في حين أن قسم كبير من الأمن السيبراني يُعنى بتناول الحوادث الغير متوقعة والتعامل معها.

تجمع حوكمة الأمن السيبراني بين الإجراءات الوقائية والتصحيحية فهي تشمل الاستعدادات والاحتياطات التي تتخذ ضد كافة أشكال الجرائم السيبرانية وغيرها من الهجمات ذات الصلة، هذا جنبًا إلى جنب مع تحديد العمليات والإجراءات اللازمة للتعامل مع الحوادث الفعلية الناشئة عن الهجمات أو الاختراقات الأمنية. وتجدر الإشـارة في هذا السـياق إلى أنه مبادئ وتدابير الحوكمة يجب أن تكون مرنة بشـكل كافٍ بحيث تراعي حقيقة أن هذه الهجمات تعتبر غير اعتيادية وغالبًا ما تخترق القواعد ويُسـتهدف من ورائها التحايل على هذه الإجراءات والتصـورات المشتركة التي تضعها الوحدة التي تحافظ على استمرارية الأعمال.

يمكن إرساء دعائم حوكمة الأمن السيبراني بالاستناد إلى النهج القائم على الخطوات الستة المبينة أدناه:

5-1 خطوة 1: تحديد احتياجات الجهات المعنية

- تحديد الجهات المعنية الداخليين والخارجيين (عادة مقيدين) ومصـــلحتهم في تطبيق الأمن الســـيبراني على مســـتوى الوحدات الحكومية.
- تضمين متطلبات السرية المقررة في عملية التحديد.
- الدراية بالأساليب التي يمكن من خلالها للأمن السيبراني أن يساعد في تحقيق أهداف الوحدة العامة ويحمي مصالح الجهات المعنية.
- تحديد متطلبات الإبلاغ للتواصل والابلاغ عن المسائل ذات الصلة بالأمن السيبراني (المحتويات والتفاصيل).
- توضيح أمثلة على حالات للاعتماد على عمل الآخرين (بالنسبة للمدققين الخارجيين).
- تحديد متطلبات السرية للمدققين الخارجيين والإبلاغ بها بشكل رسمي.

5-2 خطوة 2: إدارة استراتيجية التحول في الأمن السيبراني

- مراجعة النصوص والأحكام القانونية والتنظيمية فيما يتعلق بالجرائم والحرب السيبرانية.
- تحديد مدى تحمل الإدارة العليا فيما يتعلق بالهجمات والانتهاكات.
- التثبت من صحة متطلبات العمل (الصريحة والضمنية) فيما يتعلق بالهجمات والانتهاكات.

- تحديد أي تغيرات في القواعد أو نقلات نوعية فيما يتعلق بالأمن السيبراني.
- توثيق مواطن الضعف الشاملة في الأمن السيبراني المتعلقة بالعمل وأهدافه.
- تحديد استراتيجية الأمن السيبراني والتحقق نها (النهج القائم على منع المخاطر مقابل التكيف معها).
- تحديد مدى استجابة ومرونة الاستراتيجية من حيث الهجمات والاختراقات السيبرانية.
- تحديد عناصر الحوكمة القوية والهشة التي قد تؤدي بشكل غير مقصود إلى الجرائم والحرب السيبرانية (مثلا الإفراط في التحكم والسيطرة).
- تحديد التوقعات بشكل متسق مع الاستراتيجية (النهج القائم على منع المخاطر مقابل التكيف معها) فيما يتعلق بالأمن السيبراني، بما في ذلك الأخلاقيات والثقافة.
- إلقاء الضوء على الفجوات الأخلاقية والثقافية الموجودة بالفعل أو تلك المحتمل ظهورها.
- تحديد الثقافة المستهدفة للأمن السيبراني وتعريفها ووضع البرامج التوعوية بشأنه.
- التزام الإدارة بتطبيق الاستراتيجية المحددة.

3-5 خطوة 3: تحديد هيكل الأمن السيبراني

الهيكل

- تحديد الهيكل التنظيمي للأمن السيبراني- إنشاء منصة أو تشكيل لجنة بما يتناسب مع وظائف أمن المعلومات ومخاطره.
- تسليط الضوء على العوائق أو غيرها من عمليات الفصل بين المهام على مستوى الوحدة.
- التكليف بوظيفة مناسبة للأمن السيبراني، بما في ذلك الاستجابة للحوادث والهجمات.
-

الأدوار والمسئوليات

- تحديد النموذج الأمثل لاتخاذ القرارات في مجال الأمن السيبراني- وقد يكون مستقلاً عن نظام أمن المعلومات الاعتيادي أو مختلفا عنه.
- تحديد نموذج عالي المستوى (المسئول، الخاضع للمساءلة، المستشار، المطلع) لوظيفة الأمن السيبراني بما يشمل أي موارد خارجية
- مراعاة الحقوق ذات الصلة باتخاذ القرارات والتي قد يتم ممارستها عند التعامل مع الأزمات أو الحوادث.
- تحديد التزامات ومسئوليات ومهام الأمن السيبراني للأدوار الأخرى (تشمل الفرق والأفراد).
- ضمان المشاركة في ممارسات الأمن السيبراني على مستوى اللجنة التوجيهية.
- دمج الأنشطة ذات الصلة بالتحول في الأمن السيبراني في جدول أعمال اللجنة التوجيهية.

الاتصالات والإبلاغ

- تحديد جهات للتصعيد فيما يتعلق بالهجمات والاختراقات والحوادث (أمن المعلومات وإدارة الأزمات وغيرها).

- تحديد مسارات التصعيد لأنشطة الأمن السيبراني والخطوات التحولية (مثال: نقاط الضعف والتهديدات الجديدة).
- وضع الإجراءات المتعلقة باتخاذ القرارات والتعجيل بها في وقت الأزمات مع التصعيد إلى الإدارة العليا.
- تحديد وسائل وقنوات للإبلاغ عن المسائل والمعلومات التي تخص الأمن السيبراني.
- ترتيب الأولويات في إبلاغ الجهات المعنية عن المسائل التي تتعلق بالأمن السيبراني من خلال تطبيق الأسلوب القائم على تحديد الجهات المتعين إبلاغها وأولئك الذين لا يلزم إبلاغهم.
- وضع الإرشادات المناسبة للشركات التابعة.

الدمج

- تضمين اتجاهات الأمن السيبراني في الاتجاهات الشاملة لأمن المعلومات بالقدر المناسب مع توضيح مجالات الأمن السيبراني التي يتم الإبقاء عليها منفصلة ومستقلة بذاتها بصورة مقصودة.
- الربط بين وظائف الأمن السيبراني وأدوار أمن المعلومات الأخرى.
- دمج التبليغ عن المسائل ذات الصلة بالأمن السيبراني في طرق الإبلاغ العامة فيما يتعلق بأمن المعلومات.

4-5 خطوة 4: إدارة مخاطر الأمن السيبراني

- تحديد مستويات تقبل المخاطر وتحملها من حيث الجرائم والهجمات والاختراقات السيبرانية على مستوى مجلس الإدارة أو الإدارة.
- مواءمة مستويات تحمل المخاطر مع الاستراتيجية الشاملة (النهج القائم على منع المخاطر مقابل التكيف معها).
- مقارنة مستويات تحمل المخاطر في الأمن السيبراني وأمن المعلومات وإلقاء الضوء على التناقضات.
- إدراج تقييم مخاطر الأمن السيبراني وإدارتها ضمن عملية إدارة أمن المعلومات الشامل.

5-5 خطوة 5: تحسين موارد الأمن السيبراني

- تقييم مدى فعالية موارد الأمن السيبراني مقارنةً بمتطلبات أمن المعلومات ومخاطره.
- التحقق من فعالية موارد الأمن السيبراني من حيث الأهداف المحددة.
- ضمان أن إدارة موارد الأمن السيبراني متوافقة مع متطلبات أمن المعلومات الشاملة.
- تضمين إدارة الموارد الخارجية.

6-5 خطوة 6 رصد مدى فعالية الأمن السيبراني

- مراقبة النتائج والتأثيرات الناشئة عن تطبيق نظام الأمن السيبراني خاصة بالنظر إلى التغيرات في الهجمات والاختراقات والحوادث السيبرانية.

- مقارنة النتائج بخطوات التحول ومعالمه-توقعات الحالة الأولية (الوضع الراهن) والمستقبلية (الحالة المستهدفة).
- تضمين المعايير المتعلقة بالأمن السيبراني في آليات التحقق من الامتثال الروتينية.
- تقييم التهديدات ونقاط الضعف المتعلقة بالأمن السيبراني ودمج التهديدات المتغيرة في استراتيجية الأمن السيبراني.
- مراقبة ملف المخاطر بحثًا عن الهجمات أو الاختراقات السيبرانية وتقييم مدى تقبل المخاطرة لتحقيق التوازن المثالي بين المخاطر المرتبطة بالأمن السيبراني وفرص العمل.
- تقييم مدى فعالية موارد الأمن السيبراني (الداخلية والخارجية) فيما يتعلق بمتطلبات امن معلومات وأهدافه وأغراضه المحددة.

الخاتمة:

يُعد الطابع المرن والتكيفي للأحكام المتعلقة الحوكمة من عوامل النجاح الرئيسية في حوكمة الأمن السيبراني. فعلى الرغم من أن الحوكمة المؤسسية تضع غالبًا حدودًا (صارمة تمامًا) لتقنية المعلومات واستخداماتها، إلا أنه تحتاج حوكمة الأمن السيبراني للاعتراف بحقيقة أن الهجمات والحوادث والاختراقات تستهدف دائمًا الروابط الأضعف في

سلسلة القيمة الأمنية للوحدة ويتطلب هذا بدوره وضع إطار حوكمة أمنية يُعنى ببعدين رئيسيين، ألا وهما:

- أحكام الحوكمة الرئيسية، على سبيل المثال التعبير عن النوايا والأهداف الشاملة للإدارة العليا،
- أحكام الحوكمة المحسنة، على سبيل المثال وضع الإرشادات ذات الصلة بالإجراءات التي تُعنى بالتصدي للجرائم والهجمات السيبرانية أو تلك التي تتعلق بالاستمرارية في الأعمال.

ويسمح البعد الثاني بدرجة معينة من الارتجال وخاصة عندما تواجه الوحدات الحكومية مخاطر وتهديدات مجهولة. وفي مثل هذه الحالة، تكون عناصر الحوكمة صارمة للغاية مما قد يؤدي إلى تفاقم الوضع ويسفر عن نتائج عكسية. كما يجب تجنب الإفراط في التحكم والسيطرة عند مواجهة الهجمات والاختراقات المعقدة وغير المتوقعة مع التقيد في ذلك بتطبيق الإجراءات التصحيحية على نحو يتسم بالفعالية.