



// سلطنة عمان

هيئة تطوير المعلومات //

الدليل الاسترشادي لحكومة الأمن السيبراني

المديرية العامة للسياسات والemarket



// سلطنة عمان

هيئة تكنولوجيا المعلومات //

الإصدارات والتوزيع

الاسم	العنوان	التاريخ
النخبة لخدمة البيانات والمركبة	standards@ita.gov.om	2017
النخبة الترجمة		
الإصدار		

قائمة الشركاء

هيئة تكنولوجيا المعلومات	-1
الجهات الحكومية المعنية	-2
الموقع الإلكتروني	-3

سجل الريفيشن

الرقم	المؤشر	الملاحظات	الرقم
1	2017	النخبة لخدمة البيانات والمركبة	النخبة لخدمة البيانات والمركبة

رقم المعيار	العنوان	العنوان بالإنجليزية	العنوان باللغة العربية	العنوان باللغة الفرنسية	العنوان باللغة الإنجليزية	العنوان باللغة العربية	العنوان باللغة الفرنسية
1	2017	G5_G1_Cybersecurity_Governance	النخبة لخدمة البيانات والمركبة				

جدول المحتويات

٤	١-incipit
٣	١-افتتاحية للمقدمة
٣	٢-الغرض
٤	٢- ما هو الأمن السيبراني؟
٤	١-المفهوم السيبراني و التهدى المستحسن (APT)
٥	٢- العرب السيبرانية
٥	٣- تقنيات تهريب ذات صلة
٦	٣-مهام هيئة الأمن السيبراني
٨	٤-التحول إلى الأمان السيبراني
٨	٤- تحديد الواقع الراهن
٩	٤- تحديد الحالة المستهدفة
٩	٥-التحول الاستراتيجي والشامل
١١	٥- إرساء مفهوم هيئة الأمن السيبراني
١٢	٦- خطوة ١: تحديد مكونات الهيكل التنظيمي
١٢	٦- خطوة ٢: إدارة ستراتيجية للتحول في الأمان السيبراني
١٣	٦- خطوة ٣: تحديد هيكل الأمان السيبراني
١٤	٦- خطوة ٤: إدارة مخاطر الأمان السيبراني
١٤	٦- خطوة ٥: تحسين موارد الأمان السيبراني
١٤	٦- خطوة ٦: رصد دور هيئة الأمان السيبراني

نهاية ٢	بداية ٢٠١٧	السنة ١	رقم الملف	اسم الملف	العنوان للمؤتمر	العنوان للسابق	العنوان للمؤتمرات
			GS_G1_Cybersecurity_Governance				

1- نبذة

لذا الأمن السيبراني ضمن مجالات أمن المعلومات بقية الصدى للثاني العرادة الإلكترونية وهي بعض الأجهزة الحاسوبية المترسبة وذلك عوامل شائع في العمالة إلى الارتكاب بمستوى الأمن السيبراني وتطوره على النطاق العالمي والشأن. لا وهي: كلية النطاق العربي الواسع والشركات والمجتمعات التي تركز على استخدام تقنية المعلومات وتنوع الأجهزة المترسبة في مجال تقنية المعلومات. ولكن يقتصر ذلك واتصال مع التغيرات الحاسمة في المجتمعات، علقت الكثير من الحكومات الوحدات على إغلاق مدارس في الأمن السيبراني لتزويج عن المدارس الإرشادية وذلك التي تُغنى بروضي المعلم والتربويات والأطقم التعليمية ويعتبر هذا المستند بمثابة خطوة أولية في الطريق نحو تطبيق تلك الهدف حيث يحصل على تقييم الإرشادات التعليمية الصالحة والتي يمكن تطبيقها على أرض الواقع بما ينعكس على المدارس الورقية المفتوحة.

1-القصد المنشود

يساهم هذا المستند بذلك أهدافه من يكملون مع الأمن السيبراني بشكل مبشر أن غير مبشر بما فيه درء الأ殃 ودرء أمن المعلومات ودرء مخاطر تقنية المعلومات والمستخدمين التهالكين ويدركى تقنية المعلومات.

2-الغرض

يشكل الغرض الرئيسي من إعداد هذا المستند في وضع إطار موحد للمبادئ المكرمية في مجالات إدارة المخاطر وإدارة التهالك الأولى والمهنية، بالإضافة إلى تقديم ارشادات عن المفاهيم والإجراءات التقىسيية لإحداث التحول في الأمن السيبراني وضمان تنفيذها مع استدلالات أمن المعلومات المطلوبة.

وتحضر هذا المستند أساساً بأثره في تطوير على معايير عملية والتنمية للوحدات والتركيزات التابعة لها، وهو يؤكد بذلك وثيقة تقنية عن أمن المعلومات يعلن بذلك، والأفراد المسئولة عنها في موسمية استرجاعاته الآمنة بطريقة شاملة ومتقدمة كما أنه يركز بشكل رئيسي على إحداث التغير والتطور في الأمن الإلكتروني على مستوى الوحدات من أجل تعزيز سبل مكافحة هذه التهديدات الإلكترونية ودفع الأمن السيبراني ضمن النوع التناول المتفق فيما تتحقق بحركة الأمن السيبراني وإدارة المخاطر والاترداد.

نوعية المعلومات	الصلة والمرتكبة	الصلة الثانوية	الصلة الثالثة	الصلة الرابعة	الصلة الخامسة	الصلة الستة	الصلة السبعين	الصلة السبعين	الصلة السبعين	الصلة السبعين	الصلة السبعين
3	2017	1	GS_G1_Cybersecurity_Governance	رئى عريف المست							



2. ما هو الأمن السيبراني؟

تشرَّف استخدام مصطلحات الأمان السيبراني والعرب المهرانية باعتبارها مفردات أساسية في عالم الأمن بوجه عام، وبعزم ذلك في العقد الأول إلى اليمين في الإختلاف الأهم والأصل الأهم وهو روح أسلحة العرب العظيمة، وفي هذه منه إلى التزام التكثيفية بهذه.

يطلب مصطلح "الأمن السيبراني" في سياق آمن المعلومات تفسيرًا إلهيًّا عذراً ما يُلمس له، ويتخدم على نطاق واسع للإشارة إلى أنفس هذه المصطلحات، يمثل الأمان السيبراني كلية الممارسات التي من شأنها أن تحمي الوحدات والأفراد من الهجمات والاعتداءات والانتهاكات المقصودة بحسبًا عمليًّا عليها من عروض، ومن الناحية العملية، يهدِّي الأمان السيبراني بشكل أساسي في الصدد لهذه: الارتكاب من الهجمات والإختلاف والجروح التي يصعب التáchي أو التعامل معها، كما أصبح من الممكن التعامل مع الهجمات والجرائم الإلكترونية بالاستثناء بالاعتراضات والروابط مساعدة وتقديم الدعم في هذا النصوص. لذا، يؤكد الأمان السيبراني على ما يُعرف باسم العرب المهرانية والتهديدات المستحسنة المتقدمة وبدى تأثيرها على الوحدات والأفراد.

ويحضر النظر عن الاستخدام الشائع للمصطلح، ليجد بدرج مصطلحات الأمان السيبراني ضمن الإجراءات التي تطبقها الوحدات الحكومية بما يكفي، وكلمة الموارد الأخرى للأمن المعلومات يجد تفعيل المركبة والإدارة والسلامة للأمن السيبراني، ولنشر الإشارة إلى هذا السياق ابن ابي طهير الأمان ينسد بالمسؤولية لأكثر من كونه مهندسًا، ومحضًا مع الاعتزاز بذلك؛ لأنه يطلب بدوره مساعدة وتقديم مساعدة مهارات ومتطلبات الجهات المعنية.

2-2. أمنية المهرانية والتهديد المستحسن المتقدمة (APT)

في هذه التهديدات وسبل مواجهتها المختلفة وتقدير الضغط، قدم الأمان السيبراني استجابة مبنية على نوع متعدد من الوحدات والاعتراضات والجروح.

وتقترن برؤية تغذى الوحدات ورئاستها وتتفقدها إلى حد كبير، بدأية مما يمكن تسميتها بالوحدات غير الصلة إلى البعثة التربية والمعطاء للبلدية على هذه تتم برأسه هبها.

يشغل التهديد المستحسن المتقدمة (APT) الوحدات والإختلاف والتسريرات والأحداث الأخرى المتعلقة بالأمن بمستوى من مرافق إلى مرتفع جدًّا من المجهود (أو العقد)، ولنحو سلائف وحدات حوكمة أو قيادة معينة، وفي مقدم الحالات يتضمن ذلك جهد لا يُلمس به في التحدث عن المعلومات وبصفتها بالاضافة إلى التطبيق والتصنيف بشكل تفصيلي، فعدة ما تكون تلك التهديدات عدراً عن معرفة من التهديدات يشكل الفرق بين المعرفتين منها في زيدات الأثر الواقع على الوحدات إلى قيس، مما فلتشر من التهديدات المستحسنة المتقدمة لها خلفية وخلفية مزدوجة، وعلى حكم الأشكال الأصغر من الوحدات، يتضمن تفاصيل التهديدات المستحسنة المتقدمة إلى مفهوم، لا يستهان به من حيث العامل الزمني والاستقرار، وبحسب الهدف وبدى آلية استلطنه، قد تتضمن التهديدات المستحسنة المتقدمة خطأً مقصصًا يمكن تطبيقها أمنة واحدة فقط.

رقم الملف:	اسم الملف:	الجهة المختصة:	جهة المقررات:
الصفحة:	التاريخ:	العنوان:	العنوان:
4	2017	GS_G1_Cybersecurity_Governance	نهرية الأمان السيبراني
1			نهرية الأمان السيبراني



كما أنه يصعب التعرف عليها أو التأثر بها وإنما ما يصعب أيضًا تبعها بمعرفة مصدرها أصلها مقارنة بالأدوات المنشورة على نطاق أوسع ومتفرقة للغاية.

2-2. العرب السيبرانية

لدى العرب السيبرانية النفوذ الأرسع للتهديدات المستعصية لـ المكافحة، فضلاً عن ذلك، اليهود المكرمية في اليهودية التي كُنّ هي التي التحليّة الأساسية أو الوحدات المكرمية الوجهة، تزداد هذه التهديدات تقدّمًا بصفة أنّ الهدف من هذه هي أن تكون لهم مقدمة العمل موزعة، ومصادر لا يُمسّ لها تحت تصريحهم، وبشكل ذلك الورق المكون، حيث إن العطلات المركبة أو المكرمية قد تستقرّ على آفراه بدلاً من الفكرة الأولى وهي التهدّد.

ويعتبر ذلك، ضمن الناحية التقنية والإدارية، لدى العرب السيبرانية مجرد نشاط آخر من التهديدات المستعصية لـ المكافحة على الرغم من معايير ذلك، حيث أن عوائق قوية واعتراضية.

لذلك، يجب أن يبذل الأمان السيبراني احتماله لـ التعرف على المدمرة وغير المدمرة من شاهد عسكري أو حكومي مستهدف، موّجه ضد الوحدات المكرمية والشرارات التابعة راضي التحلية الحربية، ومن حيث لا يُقدر، تكون عوائق العرب السيبرانية أو المكافحة مشكلة لهذا التعرف المدمرة على الأبعد الإيمانية أو المؤسسة ذات الارتفاع الشهابي.

2-3. التهديدات أخرى ذات صلة

رغم أن المجموعة السيبرانية والغيرها من المجموعات التي تهدّد المكافحة، إلا أنه قد تسرّع في إشكال أخرى من التهديدات والتهديدات، منها التسلّط السياسي والاختراق في العمل العسكري والسيادي المستهدف لـ المجموعة الوحدات، وإنما، لا يمكن التأثر بهذه، إلاشكال من التهديدات وقد لا يمكن معرفة الأمان من ترافق حدوثها من هذا المعنطلق، ففي تعرّف بـ مخاطر مختلطة وتهديدات مهorreنة يجب التحالّ معها على هذا الأساس، من هنا، يستلزم الأمر عناصر استـ العجنة للتعامل مع كل ما هو غير مترافق ومحظوظ بـ بحث شامل على عذسر آخر لـ لاستقرارية الأصول وخدمات تـ لـ المعرفة، وبالتالي، يجب أن تدرس استـ العجنة الأمان والتـ لـ المجموعة الإدارية للـ التهديدات والمعلومات الم gioveilleة مع الإشارة إلى مطابقه إدارة استـ العجنة الأمان وخدمات تـ لـ المعرفة حتى يكون ذلك ممكنًا.

نـدة	الـ	الـ	الـ	الـ	الـ	الـ	الـ
5	مـارس	الـ	الـ	رمـم عـرفـ المـ	اسمـ المـ	المـ	نـدة

GS_G1_Cybersecurity_Governance

المـ

المـ

المـ

// سلطنة عمان

هيئة تطوير المعلومات //



3- مقدمة: هيئة أمن السيبراني
 تتخلل جريمة إدراك واعادة منتشر لأنّ السيبراني تحملها لغيره الأفضل وعمره أنّ المعلومات والبيانات على حد سواء، ولعرض قيمة العزيمة لأنّ السيبراني ولعمدة الغرض المصاحب للجهات أو الإنتهاكات، يجب تحقيق الإرشادات الآتية ويدار به من أنّ هذه البيانات رصحت على مساري على وليس شفاعة، إلا أنها تقدم معاييرًا لأنّ السيبراني يكره؛ إذنًّا من نظمه أنّ المعلومات تتغادر
مبدأ 3: التعرف على التغير المحتمل تجاهه والعرب السيبرانية

إن طبيعة أمن السيبراني يجب أن يسلط الضوء على العصر العصلي والتكنولوجيات واسعة النطاق لغيره والعرب السيبرانية، ولكنّ قيود
بـ 4- إدارة أمن السيبراني على نحو متعدد، بناءً على معرفة المستويات المختلفة للخطر والتأثير الجذري أو التغير الذي يشكّل منظومة ويشمل ذلك
النوعية المطلقة للظرفية التي قد تُؤثّر بها المستخدمون اليابانيون ومتى تأثره بمحدث وحرارة أمن السيبراني.

مبدأ 4- لمبة التقافة المدرسية والتربية والتحفيظ السلوكي

تتلاشى قيمة التحذير والتغيير المتطلبات بـ 5- التأثير المدرسي والتربية وتحفيظ السلوكي، وبختلي ذلك في المدرسة
المستخدمين اليابانيين والمدارس والآباء والآباء الاصدقاء، وعده جريمة وإدارة أمن السيبراني، يجب أن تأخذ هذه الموارد في الحساب وتشجع
في مفهوم أمن المعلومات الاستراتيجية والتكتيكية والتحفيظية... .

مبدأ 5- تقييم دراسة السيبراني بمحضها يتعلّق بالأمن السيبراني، ومدى خليل الوحدة المتطرفة

سوف، تحدد دراسة السيبراني استراتيجية أمن السيبراني المعايير التي تحظى الوحدة من حيث القيمة المترقبة والمخاطر المحتملة، فهو
الذري والإستقرار في نوع جديّر بالخطر، مثقل المخاطر المتفاوتة ريشقة التأثير عليها، وأصحابه الوصول إلى تحقيق إجراءات أمنية كافية
ووظيفية يذكره تجاه دراسة السيبراني بوضوح وبهدف أن توجهها جميع مستويات الإداري، بشكل كامل بحيث يشمل ذلك الإختارات المختلفة
بالكلفة والفرز، بالإضافة إلى الكلفة والكلفة المدرسية لـ 6- أمن السيبراني.

مبدأ 6- إدراك واعادة جريمة أمن السيبراني

لذلك أمن السيبراني جزءًا لا يتجزأ من لمبة الوحدة وأداتها، وبذاته عليه، فهو يضع توجيهات جريمة وأوضاع توفر الإرشادات والتوجيهات
الذريمة، فضلًا عن وضع التحرب، المطرورة والخطولة، وتتمثل هذه التوجيهات اعتماد إطار الحركة المدرسية لأنّ السيبراني يتعرّف

مبدأ 7- التعرف بأهداف هيئة أمن السيبراني

يعطي أمن السيبراني حوار ووحدات متعددة ومتخصصة ضمن نظام أمن المعلومات الشامل، على الرغم من أن أهداف هيئة أمن
السيبراني ونسبة رموزه ورسائل التأثير عليها، إلا أنه يهدى لـ 8- المخاطر والسائل المترافق به في الإشعار نظرًا لأنّ تعبه من حوله
أمن السيبراني قد تكون خارج نطاق سيطرة الوحدة.

نوعية المعلومات	العنوان والعنوان	العنوان العنوان	نوعية المعلومات	نوعية المعلومات	نوعية المعلومات
مقدمة	التاريخ 2017	السنة	1	رائد تطوير المحتوى	GS_G1_Cybersecurity_Governance



بيان إرساء دعائم الأمان السيبراني للتحول والتطور

تتهدى الجريمة والعرب المليارية والجهات والهيئات والهيئات والهيئات لربط الأخطاف في النهاية وذلك بعد التعامل مع الأمان السيبراني حتى أنه هناءً عن مقتربة من الخسائر التي تطرأ على بعضها البعض تطلب لها شهاداً له، لافتة إلى أن هناك خطأ في ذلك خطأ أنه لا يمكن التفكير في التحرك أو الادارة والتحكم للأمن السيبراني بعزل عن بعضه البعض.

| العنوان | الجهة المختصة |
|--|---------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|---------------------------------------|
| بيان إرساء دعائم الأمان السيبراني للتحول والتطور | الهيئة العامة للرقابة على التكنولوجيا |
| العنوان | الجهة المختصة |
| بيان إرساء دعائم الأمان السيبراني للتحول والتطور | الهيئة العامة للرقابة على التكنولوجيا |

// سلطنة عمان

هيئة ثلاثة المعلومات//



٤- التحول في الأمن السيبراني
 يغدو التحول في الأمن السيبراني شأنه شأن أي عملية أخرى طفرة الأجل، على التحسن المستمر والتتابع من خلال مستويات متقدمة من التحول ويعني هنا أيضًا أنه يلزم برفعه الاستراتيجية والتطور المترافق بها والتحسين عليها بصفة متقدمة مع مراعاة لـ“غيرات” في ظل التحديات ومتى تقلّل الوحدة لها.

يعد التحول عذراً على أنه تغير شامل من حالة مستقرة للبقاء إلى المستوي التالي لها وبعدها قد يهدى بمحوره من التغيرات سواءً من تفاصيل التحكم فيها، وفيما يتحقق بالأمن السيبراني، يمكن تعريف التحول على أنه تغير القسم الكلي للأحكام المتعلقة وأنشطة الإدارية والضرائب والضرائب الأخرى من حالاتها الراهنة إلى الحالة (السلبية) الآتية المطلوبة، بواسطة إجراء غيرات يمكن التحكم فيها عدداً على خصائص وتعديلات معينة ومكونات أخرى. وعلى الرائد من أن هذا التحريف يطرأ مثلاً بتغيير رفعه التحول، إذ أن بعض الأسئلة قد تساعد في فيه عملية التحول.

٤- التحول الوعي الرابع

يعد على الأداء الأول للنقد وتحديث الواقع الرابع في الأمن السيبراني ونحوه لحركة المعلوم به، ويحيى هنا أنه يتعذر عن الإلزامات التي ربما قد وجدت مسلكاً يلزم رصد الأمان السيبراني بهذه الراحتها بما هي من مواطن ضعف وأوجه السوء. في ذلك، يتخلّل ذلك مرويّن للفحص التي تم تجديدها ماسّةً (برهن الارجاع إلى القسم السادس) وتقاطع الفحص التي قد أثبتت العادة إلى التحول. يمكن لهذه الأسئلة من تكامل التحول من العادلة الراهنة التي تمهّد بذلك لإمكانية أن تستمر على هذا النحو“ إلى رؤية تتسم بالذكاء من الأجهزة داخل الحكومة والإدارة، والضمان لأنّم المعلومات.

كما أن مراسلة لوضع الرابع السادس في التكفل عن مواضع الفحص في المؤوك الإدارية، وبينما يذكر، سلباً سلبيات انتهاكها إلى بعد الأداء القائم على مطعن المطهّر إلى بعد الأسئلة التي طلبها ذلك، يمكن عزوه من عملية إنشاء دراسة المدى في التحالف بالوضع الفعلي لترجمة من حيث الفوائد وأهميتها وستوك الإنفاق الأخرى، ويعجز القول، قد يهدى بدوره المعرفة الذي يختاره الوحدة على معلومات وعمليات ثانية وباقية يشار إلى العادة الراهنة غير المرغبة قاتلها.

لعل الرائد من أن هذا التحريم يطرأ عملية مصلحة التحدة، غير أنه لم يصرّ أنسنة لا يمكن الاستفادة به كلفة دينها في التحول في الأمن السيبراني، وإنّما تدرك الوحدة بموازن الفحص، بشكل لا يختلف شكه ومن دون بوضوح، سلبيات قاتلة على تحفيظ مصلحة لإدارة الأمان السيبراني.

الصفحة	التاريخ	رقم البريد الإلكتروني	اسم المستخدم	الوحدة	الوحدة	الوحدة
٣	٢٠١٧	١	G9_G1_Cybersecurity_Governance	المدير العام للمعلومات	المدير العام للمعلومات	المدير العام للمعلومات



4- تعدد الملة المستهدفة

بحصر، تعدد الوضع الرابع لائن السيرفر وارائه بشكل كامل، يمكن هنا تعدد الملة المستهدفة او المستهدفة بذلك على مراحل تضطر وارجه القصور والمخاطر والتي ادى الى حدوث تكون الوحدة قادرة على التغير والتكيف مع ما هو سائد وتابع في الهداف والاحتياطات والحوارات التسللية وظلت تكون الملة المستهدفة غير مفهومة بوضوح، قد لا يدرك نوع الحزن الذي جعلها وتحدد العيوب التي لا يمكن ادراكها ملائمة.

- الاختار الى الموجهة حيث يتم تعدد الملة المستهدفة بشكل ملائم، بدلاً من الوضع الرابع (المسفر) لخطاب الامن المعنوي الشامل
- تعدد الاتصالات تعدد الملة المستهدفة على اية اثر فيها معاذقة بعدها الا ان دون دفع التهديدات المعنوية، ومواطن الضغط دون الماحة الى تذكر الهداف والاحتياطات المعنوية
- اربعة الموجهة تعدد الملة المستهدفة ذلك على انها ليست متعلقة بذلك عندما لا تدرك الازمة المعنوية بحسب معنى الاتصالات المعنوية في العربية والعرب المعنوية
- التحذير تنويع الموجهة يتم الارتفاع على تنويع الموجهة الرابع القائم على من المخاطر او ذلك (فالآن يكفي بالآن "الآن عوائل") مع تحالف الاتصالات المعنوية التي قد تدل على وجود ادخال وظيفي او خلل في المقدمة

فيكون الهدف من متغير الموجهة هو تعدد المستوى الثاني للمسفر من خلال تحققه والآن هذه يمكن ان يكون الامن المعنوي قدرًا على ابراء بمعتقدات الجهات المعنوية وهذه يمكن هنا مستوى معمول من المواجهة من الهداف والاحتياطات المعنوية والموجهة ولهذا يتبعه ذلك اصلنا بمشروع الامن المعنوي، وبتحول بعد الشمولي للجهات وارجه التزكيتين عاصم خفاء الامن المعنوي التي من شأنها التأثير على الكيفية التي يمكن بها تتحقق التغير ونهاية التأثيرات المعنوية والكلوية.

يمتد امر التحول في الامن المعنوي الشامل من الوضع الرابع والملة المستهدفة على الموجهة والازمة، فبحصر، تعدد الملة المستهدفة يوجه بحال تتحقق بعض التحديات لها وارتها ومررتها، فتشمل البعد الاستراتيجي وضيق الاستراتيجيات والخطط وتطبيع الاعمالات رقيقة المستوى والرابع ذات الصفة بمشروع الامن المعنوي، وبتحول بعد الشمولي للجهات وارجه التزكيتين عاصم خفاء الامن المعنوي التي من شأنها التأثير على الكيفية التي يمكن بها تتحقق التغير ونهاية التأثيرات المعنوية والكلوية.

ويعنى التحول في الامن المعنوي بطريقة شديدة انه يمكن هناك ملحة دراسة ان تغيرات فيما يتعلق بالتأثير غير المعنوية كمثل، قد يكون اثر برامج توعية المعنوقين فيها من حيث تزكي التغير والاهتمام بالتفاصيل.

العنوان	العنوان	العنوان	العنوان	العنوان	العنوان
العنوان	العنوان	العنوان	العنوان	العنوان	العنوان
9	يناير 2017	1	GS_G1_Cybersecurity_Governance	رد عرض است	اسم المستخدم
				نوفمبر 2016	نوفمبر 2016



// سلطنة عمان

هيئة تطبيق المعلومات //

ويع ذلك، قد تتمثل تلك الأذكى في أن العديد من القطاعات الإنجولية المخالفة تزيد عن ثلاثة يدار بغير الموارث وتفسرها الآلية عن الهداف المستقرة المتقدمة الحقيقة (ولكنها غير مرجعية) كما أنه قد توجه تجاه تأثير تأثيرها في إقامة الأمان السيبراني والتي لن تتحقق إلا إذا تم التغیر إلى التحول على اعتبار أنه مدارسة منهجه وشكنته

رقم	التاريخ	السنة	رقم المرسوم	اسم المنشئ	الجهة أو الكونجية	الجهة العاملة	الجهة المسؤولة	بيان
١٥	٢٠١٧	١	GS_01_Cybersecurity_Governance	المجلس	لعمان	الحكومة	والموارد	ل المعلومات



// سلطنة عمان

هيئة ثلاثة المعلومات //

5. إرساء دعائم هوكمة الأمان السيبراني

يرجع ذلك لضعف حوكمة الأمان المعلوماتي بطنز وحدوداً لإدارة الأمان والحلول ذات الصلة بها، وبخصوص ذلك بالخصوص، المسارات والإمدادات الرسمية والإرشادات التي تلزم الوحدات الحكومية بذلكها وتنفيذها، وهي لا تزال تطبيقاتها في أفضل مطابق لها "إذاء النساء"؛ في حين أن العديد من الأمان السيبراني يُخسّن بتزويد الموارد الفنية متزامنة والمتعلقة بهما.

تتعذر حوكمة الأمان السيبراني عن الإيمادات الرؤافية والتصحيحية فهي تتطلب الاستعدادات والاحتياطات التي تتحدد هذه كثافة التكليل العلامة السيبرانية وغيرها من الجمادات ذات الصلة، هنا جنباً إلى جنب مع تحديد العمليات والإمدادات اللازمة للتعامل مع الموارد الفنية المطلقة عن الجمادات أو الإختراقات الأمنية، وتصر الإستراتيجية هنا بالسؤال إلى أنه يمكننا وننذر حوكمة بعض أن تكون مرنة بشكل تأثير يبعث تراوين مطلقة أن هذه الجمادات تضرر غير انتقامية وذلك ما ينذر المؤسسات والهيئات والسلطات من ورائها التحذير على هذه الإيمادات والتصورات المنشورة التي تخصها الوحدة التي تعامل على استمرارية الأعمال.

يمكن إرساء دعائم هوكمة الأمان السيبراني بإلاستدال إلى النفع القائم على الخطوات المطلوبة لجهة إدار

5.5 خطوة 4: تحديد احتياجات الجهات المعنية

- تحديد الجهات المعنية الداخلية والخارجية (عذراً علينا) ومصالحها في تحقيق الأمان السيبراني على مستوى الوحدات الحكومية.
- تحديد متطلبات السرية المطلوبة في عملية التصدية.
- البراعة والأسلوب التي يمكن من خلالها الأمان السيبراني أن يمسك في تحقيق أهداف الوحدة المطلبة وبمعنى صلاح الجهات المعنية.
- تحديد متطلبات الإذاعة للتوصيل والإبلاغ عن المصالح ذات الصلة بالأمان السيبراني (المعلومات والتوصيات).
- توضيح مفهوم معاشرات لآلات الاتصال على عمل الآخرين (بالنسبة للذويين الخارجيين).
- تحديد متطلبات البراعة لمعاقب الخارجيين والإبلاغ بها بشكل رسمي.

5.5 خطوة 2: إدارة سترategية التحول في الأمان السيبراني

- براغماتية التصوّر و الأحكام القانونية والتقدّمية فيما يتعلق بالجرائم والعدالة السيبرانية.
- تحديد مدى تحمل الإدارة العليا فيما يتعلق بالجهات والهيئات والاتصالات.
- التثبت من صحة متطلبات العمل (الصريحة والضمنية) فيما يتعلق بالجهات والاتصالات.

صفحة	تاريخ	الصفحة	رمز تعرف المحدث	اسم المستخدم	العنوان	العنوان	العنوان
11	2017	1	G5_G1_Cybersecurity_Governance	لهمان التوجهية لعمارة الأمان السيبراني	لعمارة السيبرانية لعمارة السيبرانية	لعمارة السيبرانية لعمارة السيبرانية	



- تحدد أن تغيرات في الاتجاه أو تأثير نوافذ فيما يتعلق بالأمن السيبراني.
- توثيق مرواغات الخطط الشاملة في الأمن السيبراني المتعلقة بالجهات وأهدافها.
- تحديد استراتيجية الأمان السيبراني والتحقق منها (التي يقتضي ذلك منع المخاطر مثلك (كيف؟)).
- تحديد مدى استجابة وروابط الاستراتيجية من حيث الجهات والاختلافات السيبرانية.
- تحديد خصوصيات الحركة الفنية والبيئة التي قد تؤدي بشكل غير مقصود إلى العولاد والعرب السيبرانية (مثل الإفراد في الحكم والسيطرة).
- تحديد الرؤى ذات الصلة مع الاستراتيجية (التي يقتضي ذلك ملء المخاطر مثلك (كيف؟)) فيما يتعلق بالأمن السيبراني، بما في ذلك الاختلافات والتباين.
- إبقاء الصورة على التفاصيل الأخلاقية والتكتيكية لمجموعة العمل أو تلك المختلقة قيودها.
- تحديد القضايا المستهدفة للأمن السيبراني وتعرفيها ووضع الفروع التفصيلية بحسبها.
- التزام الإداري بتحقيق الاستراتيجية المحددة.

3.5 خطوة 3: تحديد هيكل الأمان السيبراني لبيطل

- تحديد الهيكل التنظيمي للأمن السيبراني، (كتابه منصة أو تتكون الجهة بما يناسب مع وظائف أمن المعلومات ومخاطرها).
- تحديد الصورة على الواقع لغيرها من عمليات الحصول على البيانات على مستوى الوجهة.
- التكليف بوظيفة مناسبة للأمن السيبراني، بما في ذلك الاستجابة لغيرات وحالات.

الأدوار والمسؤوليات

- تحديد التدريع الأفضل لائحة القرارات في مجال الأمان السيبراني، وقد تكون مستقلة عن تقديم أمن المعلومات الإعدادي أو ممكناً لها.
- تحديد نموذج على المستوى (المسلسل، المعاين للمساهمة المستشار، المطلع) لوفقاً للأمن السيبراني بما ينبع إلى موارد خارجية.
- مراعاة الطرق ذات الصفة لأخذ القرارات والتي قد يتطلب منها عذر منها عند التعامل مع الازمات أو غيرها.
- تحديد التزمات ومسؤوليات ومهام الأمان السيبراني للأدوار الأخرى (الفنون الفنية والآخرين).
- ضمان المشاركة في معارضات الأمان السيبراني على مستوى الجهة التفصيلية.
- دفع الأنشطة ذات الصفة بالتحول في الأمان السيبراني في جدول أعمال الجهة التفصيلية.

الاتصالات والإبلاغ

- تحديد حيث تتصفح فيما يتعلق بالجهات والاختلافات والغيرات (أمن المعلومات وإدارة الازمات وغيرها).

صفحة	التاريخ	الصفحة	رمز معرفة المستند	اسم المستند	المدير الفرعي	الجهة المسئولة	الجهة المسئولة والمعرفة
12	يناير 2017	1	GS_G1_Cybersecurity_Governance	GS_G1_Cybersecurity_Governance	المدير الفرعي	لعمادة الأمان السيبراني	الجهة المسئولة والمعرفة



// سلطنة عمان

هيئة ثلاثة المعلومات//

- تحدد مسارات التصحح لأنشطة الأمن السيبراني والمعابر التمويلية (مثل: نقاط الصدف والتهيئات الجديدة).
- وضع الإجراءات المتعلقة بالقدرة على القرارات والتخطيط بها في وقت الآزمات مع التسجّل إلى الأداء العادي.
- تحدد وسائل وقوف انتقال من الأسس والمعايير التي تتصدر الأمن السيبراني.
- ترتقي الإجراءات في إبلاغ الجهات المعنية عن المصالح التي تتصل بالأمن السيبراني من خلال تطبيق الأسلوب القائم على تحذير الجهات المعنيّة بإبلاغها وأولئك الذين لا يندرّون بالائهم.
- وضع الإرشادات الفنية للركائز الناجحة.

النتائج

- تضمن المعايير الأمن السيبراني في الإتجاهات الثمانية للأمن المعلومات بالقدر المناسب مع توضيح معايير الأمان السيبراني التي يهدى الإنذار إليها مفصلاً ورسالة ذاتها بصورة مفصولة.
- ارتبطين وظائف الأمن السيبراني وأدوار الأمان المعلومات الأخرى.
- يسع النفع من المصالح ذات الصلة بالأمن السيبراني في طريق الإبلاغ المنهجي فيما يتعلق بالأمن المعلومات.

4-5 هدفاً 4: إدارة مخاطر الأمان السيبراني

- تحدد مستويات تقليل المخاطر وتخلصها من حيث الحرارة والتهيئات والإختراقات السيبرانية على مستوى مجلس الإدارة إلى الإدارة.
- مراعاة مستويات تحمل المخاطر مع الاستراتيجية الثمانية (نحو القائم على نوع المخاطر مقابل التكلفة معها).
- مقارنة مستويات تحمل المخاطر في الأمان السيبراني وأمن المعلومات وإبقاء الضغط على التقنيات.
- إدراج تقدير مخاطر الأمان السيبراني وإدارتها ضمن عملية إدارة أمن المعلومات الشامل.

4-5 هدفاً 5: تعزيز موارد الأمان السيبراني

- تقييم مدى فعالية موارد الأمان السيبراني مقارنة بمتطلبات أمن المعلومات ومخاطرها.
- التحقق من فعالية موارد الأمان السيبراني من حيث الأهداف المحددة.
- ضمان أن إدارة موارد الأمان السيبراني متواقة مع متطلبات أمن المعلومات الثمانية.
- تضمين إدارة الموارد الخارجية.

4-5 هدفاً 6: رصد مسوّلية الأمان السيبراني

- مناقبة للنتائج والاتجاهات الثمانية عن تحقيق نظم الأمان السيبراني خاصة بالنظر إلى التغيرات في التهديدات والإختراقات والموازنات السيبرانية.

الصفحة	التاريخ	الصفحة	رمز تعرف المصدّر	اسم المصدّر	الصورة	العنوان	العنوان
13	2017	1	65_G1_Cybersecurity_Governance	المجلس	المجلس	المجلس	المجلس

- مقارنة النتائج بمحظوظات التحول وبيانات متغيرات الدولة الأردنية (الوضع الراهن) والمستقبلة (الدولة المستهدفة).
- تحديد المعايير المتعة للأمن السيبراني في آفاق التحقق من الأفضل الروتينية.
- تحديد التهديدات و نقاط الضغط المتوجهة للأمن السيبراني ووضع التهديدات الفعلية في استقصاء للأمن السيبراني.
- مرافق مفتاح تحفظها بخطاب عن البيانات للاختراقات السيبرانية وتقدير مدى تحفظ المخاطر: تتحقق التوازن المعياري عن المخاطر الفرعية للأمن السيبراني وفرض العمل.
- تحديد مدى تحالفية مواد الأمان السيبراني (الداخلية والخارجية) فيما يتعلق بمتطلبات امن معلومات وأدائه والفرص المحددة.

الخلاصة:

لقد أتت النتائج والتقييم للأحكام المتعلقة بالحكومة من عوامل النجاح الرئيسية في حركة الأمان السيبراني، فعلى الرغم من أن الحكومة الفرعية تضع غالباً حرباً (صارمة شديدة) لتنمية المطرادات واستخدامها، إلا أنه نجاح حركة الأمان السيبراني للأدوار يتحقق أن البيانات والعمليات والاحتراقات تتوقف ، وهذا هو وظيفة الأدوات في سلسلة القبضة الأمنية الموحدة وبذلك هذا يدور، ووضع إطار حركة أمنية يُعني بحقوق البيانات، لا وهذا:

- أحكام الحكومة الرئيسية على سهل العقل للغير عن التوبي والأهداف الشعاعية (غير العادي).
- أحكام الحكومة الفرعية، على سهل العقل ووضع الإرشادات ذات الصلة بالإجراءات التي تُعنى بالتصدى لغيره وبيانات السيبرانية لـ تلك التي تتحقق والاستقرارية في الأفعال.

ويُسجع العد الذي يترجم معيناً من الأرثوذكسي . ونأمل أن يتم التوجيه الوحدات الحكومية مخاطر وبيانات مجهولة . وفي مثل هذه الحالة تكون غافر الحركة صارمة للغاية مما قد يؤدي إلى قلق اوضاع وسفر عن نتائج عملية . كما يجب تحفظ الإثارة في التحكم والسيطرة على مواجهة الوجهات والاحتراقات الفعلية وغير المترقبة مع ذلك في تلك تحقيق الإجراءات الفصححة على نحو قائم بالذاتية.

نوع المعلومة	الجهة الحكومية	الجهة الفرعية	الجهة الفرعية للأمن السيبراني	الجهة الفرعية للأمن السيبراني	الجهة الفرعية للأمن السيبراني	الجهة الفرعية للأمن السيبراني	الجهة الفرعية للأمن السيبراني
صفحة 14	05/09/2017	صفحة 1	رقم بريدي المعرفة GS_G1_Cybersecurity_Governance				