

الأمّن السيبراني: MODULE 7

اليوم: 3

الوقت: 2.0 ساعة

مستوى الفهم: فهم

استراتيجيات التعليم:

محاضرة -

مناقشة جماعية كبيرة -

معدات/مرافق الوحدة:

إعداد صف دراسي قياسي -

مواد/مطبوعات للمشاركين:

كتاب العمل 7.1: تقييم الأمن السيبراني -

(Terrorist Tactics and Trends Handbook) كتيب تكتيكات واتجاهات الإرهاب -

الهدف التعليمي النهائي

بنهاية هذه الوحدة، ستكون قادراً على شرح التهديدات السيبرانية لجهتك/مؤسستك

مقدمة

الفضاء السيبراني والبنية التحتية الأساسية التي يقوم عليها عرضة لمجموعة واسعة من المخاطر الناشئة عن كل من المخاطر المادية والتهديدات السيبرانية. ينقل الإرهابيون والمجرمون الجرائم التقليدية إلى الفضاء السيبراني من خلال استغلال نقاط الضعف لسرقة المعلومات والمال. كما يطوّرون قدرات لتعطيل أو تدمير أو تهديد توصيل الخدمات الأساسية. من القلق المتزايد وجود تهديدات سيبرانية تستهدف البنى التحتية الحيوية، والتي تتعرض بشكل متزايد لتدخلات سيبرانية متقدمة تطرح مخاطر جديدة. ومع تزايد تكامل تكنولوجيا المعلومات مع عمليات البنية التحتية المادية، يزداد خطر حدوث حوادث واسعة النطاق أو ذات عواقب كبيرة يمكن أن تتسبب في أضرار أو تعطيل الخدمات. ونظراً للمخاطر والعواقب المحتملة للأحداث السيبرانية، تظل تقوية أمن ومرونة الفضاء السيبراني مهمة مهمة

ستقدّم هذه الوحدة لمحة عامة موجزة عن الأمن السيبراني، واستراتيجيات الحماية من التهديدات السيبرانية، ومعلومات حول السياسات والإجراءات المتعلقة بالأمن السيبراني.

موضوعات الوحدة

فيما يلي مخطط للموضوعات الرئيسية وخطة زمنية تقريبية.

الموضوع — أهداف التعلم الممكنة — الوقت التقريبي

مقدمة الوحدة — غير منطبق — 5 دقائق

لمحة عامة عن الأمن السيبراني — تعريف الأمن السيبراني — 25 دقيقة

الحماية من التهديدات السيبرانية — وصف كيفية استخدام الأمن السيبراني للرد على التهديدات الجارية — 50 دقيقة

سياسات وإجراءات الأمن السيبراني — شرح سياسات وإجراءات الأمن السيبراني — 30 دقيقة

ملخص الوحدة — غير منطبق — 10 دقائق

أوقات الوحدة إرشادية فقط وقد تختلف فعلياً حسب مستوى وخبرة واهتمام المشاركين أو عوامل أخرى أثناء التدريب.

المصطلحات الأساسية

مصطلح — الوصف

تقنية أمان استباقية تسمح بتشغيل مجموعة محدودة من البرامج المعتمدة — (Application whitelisting) قائمة تطبيقات مسموح بها فقط، بينما يتم حظر كافة البرامج الأخرى (بما في ذلك معظم البرمجيات الخبيثة) بشكل افتراضي؛ تتيح للمدراء فقط تحديد البرامج المسموح بها، وليس للمستخدمين.

البنية التحتية الحرجة — الأنظمة والأصول، سواء كانت مادية أو افتراضية، ذات الأهمية الحيوية للأمة بحيث يؤدي عجزها أو تدميرها إلى تأثير مُنْهَك على الأمن أو الأمن الاقتصادي الوطني أو الصحة العامة أو السلامة أو أي مزيج منها.

أي خدمات حرجية مثل المصارف أو الاتصالات تقع في دولة أخرى — (Cross-border infrastructure) البنية التحتية عبر الحدود أو تعتمد بشكل حاسم على أنظمة معلومات خارج نطاق اختصاص دولة معينة.

اختراق إلى أنظمة المعلومات الإلكترونية والرقمية عبر الفضاء السيبراني، يستهدف استخدام — (Cyberattack) الهجوم السيبراني المؤسسة للفضاء السيبراني بغرض التعطيل أو التدمير أو السيطرة الخبيثة على بيئة الحوسبة أو البنية التحتية؛ أو لتدمير سلامة البيانات أو سرقة معلومات خاضعة للسيطرة.

أنظمة وقواعد بيانات المعلومات والاتصالات الإلكترونية أو الرقمية، والمعلومات — (Cyberinfrastructure) البنية التحتية السيبرانية المحتواة فيها؛ الشبكات الداخلية التنظيمية، الشبكات المشتركة، والإنترنت جزء من البنية التحتية السيبرانية.

منع الضرر أو الاستخدام غير المصرح به أو الاستغلال لأنظمة وقواعد بيانات المعلومات — (Cybersecurity) الأمن السيبراني والاتصالات الإلكترونية والمعلومات المحتواة فيها لضمان السرية والسلامة والتوفر؛ واستعادة أنظمة المعلومات والاتصالات الإلكترونية. في حالة هجوم إرهابي أو كارثة طبيعية.

دور وظيفي في قسم تكنولوجيا المعلومات يساعد في الأمن السيبراني عبر — (Cybersecurity engineer) مهندس الأمن السيبراني تحديد من يحتاج الوصول إلى أي معلومات؛ يخطط وينسق وينفذ برامج أمن المعلومات؛ ويساعد في الحماية من تهديدات الإنترنت التي تسهل الجرائم السيبرانية.

نطاق عالمي ضمن بيئة المعلومات يتكوّن من الشبكة المتداخلة لأنظمة البنية التحتية للمعلومات — (Cyberspace) الفضاء السيبراني بما في ذلك الإنترنت، شبكات الاتصالات، أنظمة الحاسوب، والمعالجات والمتحكمات المدمجة.

التوافق والقواسم المشتركة لأنظمة تشغيل الحاسوب والشبكات وقواعد — (Cyberinterdependency) الاعتماد السيبراني المتبادل البيانات عبر أنظمة متعددة.

أي ظرف أو حدث لديه الإمكانية للتأثير سلباً على نظام معلومات عن طريق الوصول غير — (Cyberthreat) التهديد السيبراني المصرح به أو التدمير أو الكشف أو تعديل المعلومات أو منع الخدمة.

نظام أمني للشبكات مصمم لتوفير الحماية ضد المهاجمين الخارجيين عن طريق حجب حركة الشبكة — (Firewall) جدار الحماية الخبيثة أو غير الضرورية ومنع البرمجيات الخبيثة من الوصول إلى الشبكة.

شخص يسعى للحصول على وصول غير مصرح به إلى بيانات حاسوبية تخص شخص أو منظمة أخرى — (Hacker) المخترق.

مجموعة منفصلة من موارد المعلومات المنظمة لجمع أو معالجة أو صيانة أو استخدام أو — (Information system) نظام المعلومات مشاركة أو نشر أو التخلص من المعلومات.

المخاطر الناشئة عن فقدان السرية أو السلامة أو — (Information system-related security risks) مخاطر أمن نظم المعلومات التوفر للمعلومات أو نظم المعلومات والنظر في تأثير ذلك على المنظمة (بما في ذلك الأصول، المهمة، الوظائف، الصورة أو السمعة)، الأفراد، منظمات أخرى، والدولة.

أي معدات أو نظام مترابط أو نظام فرعي من المعدات يُستخدم للاكتساب — (Information technology) تكنولوجيا المعلومات الآلي أو التخزين أو المعالجة أو الحركة أو التحكم أو العرض أو التبديل أو النقل أو الاستقبال للبيانات أو المعلومات — ويشمل ذلك الحواسيب والمعدات الملحقة والبرمجيات والبرمجيات الثابتة والإجراءات والخدمات ذات الصلة (بما في ذلك خدمات الدعم) والموارد ذات الصلة.

مستخدم مخول لنظام حاسوب يهاجم النظام بعد تسجيل الدخول أو يتجاوز صلاحياته أو ينتهك — (Insider threat) التهديد الداخلي. سياسة أمنية تنظيمية أو القوانين؛ قد يكون موظفاً مستاءً أو متعاقداً لديه وصول للنظام.

عملية مراقبة الأحداث التي تحدث في نظام حاسوب أو شبكة وتحليلها بحثاً عن مؤشرات — (Intrusion detection) كشف التسلل لحوادث محتملة.

عملية مراقبة الأحداث في نظام حاسوب أو شبكة وتحليلها بحثاً — (Intrusion detection and prevention) كشف ومنع التسلل عن مؤشرات لحوادث محتملة ومحاولة إيقاف الحوادث المكتشفة.

برنامج يتضمن جميع قدرات نظام كشف التسلل — (Intrusion detection and prevention system) نظام كشف ومنع التسلل. ويمكنه أيضاً محاولة إيقاف الحوادث المحتملة.

برنامج يؤتمت عملية كشف التسلل؛ قد يكون مكشوفاً للمخترق أو قد لا يكون — (Intrusion detection system) نظام كشف التسلل.

انظر كشف ومنع التسلل — (Intrusion prevention) منع التسلل

انظر نظام كشف ومنع التسلل — (Intrusion prevention system) نظام منع التسلل

مجموعة من المكونات الإلكترونية التي تتشارك المعلومات أو تتفاعل مع بعضها من أجل أداء وظيفة — (Network) شبكة

الموضوع: مقدمة الوحدة — 5 دقائق

الشريحة 1: الأمن السيبراني

شريحة العنوان -

وصف رسومي: علم الولايات المتحدة وختمها

تحضير الوحدة

التوقيت والأساليب: استخدم خطة الوقت المقترحة في بداية الوحدة. كما في جميع وحدات هذا المساق، اقرأ كل المحتوى (دليل الميسر - وشرائح العرض) وتأكد من الاطلاع على ملاحظات الميسر قبل الحصة.

كن مستعداً تماماً للتمارين والمناقشات والأنشطة الأخرى المطلوبة في الوحدة. اتبع ملاحظات الميسر. استخدم مزيجاً من المحاضرة - TeachBack والمناقشة الجماعية والأنشطة الصغيرة ولحظات

افحص الرابط في الشريحة 19 لاختبار الاتصال في القاعة قبل تقديم الوحدة -

- إذا عمل الرابط والتنقل، اعرض للمشاركين ما هو موضح في ملاحظات الميسر
- إذا لم يعمل الرابط، وصف عناصر الموقع المدرجة في ملاحظات الميسر واكتب الرابط على ورق فليب تشارت وعلقه في القاعة

توجيه المشاركين إلى دليل المشارك

:عند البدء -

- ارشد المشاركين إلى بداية هذه الوحدة في دليل المشارك
- أشر إلى قائمة الملاحق التي سيستخدمونها خلال هذه الوحدة
- راجع المصطلحات الأساسية قبل بدء الوحدة

الشريحة 2: هدف الوحدة

بنهاية هذه الوحدة، ستكون قادراً على شرح التهديدات السيبرانية لمنظمتك -

وصف رسومي: لا يوجد

ناقش باختصار الهدف التعليمي النهائي -

:أبرز الموضوعات الرئيسية -

- لمحة عامة عن الأمن السيبراني
- الحماية من التهديدات السيبرانية
- سياسات وإجراءات الأمن السيبراني

أخبر المشاركين أن معلومات هذه الوحدة يمكن استخدامها لشرح أنواع التدابير التي يجب أن تمتلكها الوكالة والسياسات والعمليات - والإجراءات التي يجب تطويرها لتقليل التهديدات السيبرانية في وكالاتهم.

الموضوع: لمحة عامة عن الأمن السيبراني — 25 دقيقة

:هدف التعلم الممكن

.تعريف الأمن السيبراني -

الشريحة 3: لمحة عامة عن الأمن السيبراني — تعريفات مهمة

- نظام المعلومات

- الفضاء السيبراني

- البنية التحتية السيبرانية

- التهديد السيبراني

- الهجوم السيبراني

- الأمن السيبراني

وصف رسومي: شخصان ينظران إلى شاشة حاسوب

.أخبر المشاركين بأهمية مراجعة هذه التعريفات المتعلقة بالسيبر قبل المتابعة لضمان فهم مشترك -

عرف المصطلحات التالية (كما وردت أعلاه): نظام المعلومات، الفضاء السيبراني، البنية التحتية السيبرانية، التهديد السيبراني، الهجوم - السيبراني، الأمن السيبراني.

الشريحة 4: سؤال للمناقشة

ما أنواع البنية التحتية الحرجة في بلدكم التي تتطلب الأمن السيبراني؟ -

وصف رسومي: لا يوجد

ذكر تعريف البنية التحتية الحرجة كما في الوحدة 2 -

اطرح السؤال على المشاركين: ما أنواع البنية التحتية الحرجة في بلدكم التي تحتاج إلى الأمن السيبراني؟ -

دون الإجابات على ورق فليب تشارت وعلّقها. إذا لم يقدم المشاركون أمثلة، أضف أمثلة مثل -

الزراعة، الغذاء، المياه، مرافق الصحة العامة، خدمات الطوارئ، الحكومة، القاعدة الصناعية الدفاعية، المعلومات والاتصالات، الطاقة، النقل، المصارف والتمويل، الصناعات الكيماوية، البريد والشحن.

(الشريحة 5: اتجاهات الأمن السيبراني (1 من 3

تكرار الهجمات السيبرانية على البنية التحتية الحرجة -

تزايد التهديدات السيبرانية للبنية التحتية الحرجة -

الاعتماد السيبراني المتبادل -

وصف رسومي: لا يوجد

(الشريحة 6: اتجاهات الأمن السيبراني (2 من 3

التهديدات الداخلية لأنظمة الحاسوب -

ملكية أجنبية للبنية التحتية -

تحديات أمنية وطنية خطيرة يجب على الدولة مواجهتها -

وصف رسومي: لا يوجد

اشرح أن التداخلات السيبرانية المتكررة والمستمرة على البنية التحتية الحرجة تُبرز الحاجة إلى تحسين الأمن السيبراني -

عرّف الاعتماد السيبراني المتبادل وبيّن أنه يجعل الشبكات والأنظمة عرضة للهجمات بسبب الطبيعة المترابطة والمتداخلة لتلك الأنظمة:

- هجمات يمكن أن تنتشر بسرعة وتحدث تأثيراً مُنهكاً
- زيادة نقاط الضعف عبر اتصال الإنترنت
- تقليل السيطرة على التكنولوجيا المشتركة عبر الفضاء السيبراني في الاقتصاد العالمي

عرّف التهديد الداخلي وشرح أن التهديدات الداخلية (الموظفون الحاليون أو السابقون أو المتعاقدون) قد تشكل نحو ثلث خروقات الأمن - بسبب معرفتهم أو وصولهم للأنظمة والبيانات. قد تُقلّل قلة الإبلاغ من وضوح النسبة الحقيقية

اشرح أن ملكية البنية التحتية الحرجة من جهات خارج الدولة قد تمثل تهديداً ليس فقط عبر هجوم مادي أو سيبراني أو عبر الاعتماد - المتبادل للأنظمة، بل أيضاً لأن المالك قد يوقف تشغيل الموقع لأسباب خبيثة.

أخبر المشاركين أن التهديد السيبراني للبنية التحتية الحرجة يستمر في التزايد ويشكل أحد أهم تحديات الأمن الوطني -

(الشريحة 7: اتجاهات الأمن السيبراني (3 من 3)

أهداف لمواجهة الاتجاهات -

- تعزيز أمن ومرونة البنية التحتية الحرجة الوطنية
- الحفاظ على بيئة سيبرانية فعّالة تشجع السلامة والخصوصية
- الشراكة مع مالكي ومشغلي البنية التحتية لتحسين تبادل المعلومات

وصف رسومي: شخص في مقهى يستخدم حاسوباً محمولاً

اشرح أن هذه الأهداف تساعد على مواجهة الاتجاهات السابقة -

- تعزيز الأمن والمرونة
- الحفاظ على بيئة سيبرانية تشجع الكفاءة والابتكار والازدهار الاقتصادي مع تعزيز السلامة والسرية وحقوق الخصوصية والمدنية
- الشراكة مع المالكين والمشغلين لتحسين مشاركة معلومات الأمن السيبراني وتطوير معايير مبنية على المخاطر وتنفيذها

الشريحة 8: سؤال للمناقشة

إذا تعرّضت أي من بنيتكم التحتية الحرجة لهجوم سيبراني ناجح وتوقفت العمليات، ما العواقب على بلدكم؟ -

وصف رسومي: لا يوجد

اطلب من المشاركين مناقشة العواقب المحتملة. أشر إلى أن الردود ستختلف وارجع إلى قائمة البنى التحتية الحرجة المنشورة سابقاً -

الموضوع: الحماية من التهديدات السيبرانية — 50 دقيقة

هدف التعلم الممكن:

وصف كيفية استخدام الأمن السيبراني للرد على التهديدات الجارية -

(الشريحة 9: الحماية من التهديدات السيبرانية (1 من 2

استخدام تكنولوجيا المعلومات -

التحقق من خلفيات جميع العاملين والمتعاقدين -

إشراك المؤسسة بأكملها — القيادة العليا، القادة المتوسطون، الضباط وحملة الخطوط الأمامية، والمحللين -

وصف رسومي: لا يوجد

(عَرَفَ تكنولوجيا المعلومات (كما وردت في المصطلحات -

اشرح كيف أن فحوصات الخلفية قد تساعد في تنبيه الجهات إلى الأشخاص غير المناسبين أو الخطيرين -

- لمقدمي الطلبات للتوظيف أو التعاقد

- بشكل دوري للعاملين الحاليين للكشف عن تغيّرات منذ وقت التعيين

بيّن أن حماية البنية التحتية الحرجة السيبرانية تستلزم مشاركة مؤسسية كاملة -

- القيادة العليا تقدم الرؤية الاستراتيجية والأهداف لتكنولوجيا المعلومات

- القادة المتوسطون يخططون ويديرون الأمن وإدارة المخاطر

- الضباط والموظفون التنفيذيون يديرون أنظمة المعلومات وينفذونها

(الشريحة 10: الحماية من التهديدات السيبرانية (2 من 2

بناء شراكات مجتمعية -

تحديد البنية التحتية الحرجة والسيبرانية -

لامركزية البنية التحتية الحرجة والسيبرانية -

دمج التكنولوجيا لحماية التكنولوجيا -

وصف رسومي: مجتمع من الأشخاص

:اشرح أن الشراكة مع القطاع الخاص تتضمن -

- بناء الثقة والتواصل لأن لا جهة واحدة يمكنها معالجة احتياجات الاستجابة والمرونة وحدها
- تبادل المعلومات والبروتوكولات والممارسات الفضلى والحلول
- التخطيط للأمن وتخصيص الموارد في حالة الهجمات أو الكوارث الطبيعية
- تشجيع الوعي العام
- تطوير نظام موحد بين الحكومة والصناعة والقطاع الخاص لزيادة الوعي بالتهديدات

.ذكر أهمية تحديد وترتيب الأولويات للبنية التحتية الحرجة لتسهيل تخطيط الميزانيات والحماية والمرونة -

اشرح أن المركزية في التحكم تعني أن هجوماً أو كارثة في موقع واحد قد يكون لها أثر متسلسل على مواقع أخرى، ولذلك قد تكون -
لامركزية البنية التحتية وسيلة أمنية مفيدة.

اشرح أن التكنولوجيا تُستخدم الآن في الحماية المادية للبنى التحتية (مثل التحقق من نقاط الدخول والكاميرات وأجهزة استشعار -
الحركة)، ويجب أن تُستخدم أيضاً لحماية نفسها.

.أخبر المشاركين أنه ستُعرض أمثلة لتقنيات حماية البنية التحتية السيبرانية تالياً -

(الشريحة 11: كشف ومنع التسلل (1 من 2

عملية مراقبة الأحداث التي تحدث في نظام حاسوب أو شبكة وتحليلها بحثاً عن دلائل لحوادث محتملة ومحاولة إيقاف الحوادث -
المكتشفة

وصف رسومي: لا يوجد

(الشريحة 12: كشف ومنع التسلل (2 من 2

:المزايا -

- يراقب حركة المرور وينبّه بشأن ما هو غير اعتيادي
- ينبّه استناداً إلى توقيع حاسوبي موجود في قاعدة بيانات التهديدات

:العيوب -

- يعطي معلومات عن تسلل مشتبه به بعد وقوعه

- يحتوي معلومات تصبح قديمة سريعاً •

- يميل إلى توليد عدد أكبر من الإنذارات الكاذبة مقارنة بالهجمات الحقيقية — ما قد يؤدي إلى تفويت هجمات فعلية أو تجاهلها •

وصف رسومي: لا يوجد

• "أخبر المشاركين أن التسلل ليس مسألة "إن" بل "متى" -

• (عرّف المصطلحات: كشف التسلل، نظام كشف التسلل، كشف ومنع التسلل، ونظام كشف ومنع التسلل (كما ورد أعلاه -

• اشرح مزايا وعيوب أنظمة كشف التسلل -

- ترصد حركة المرور وتنبه عن السلوك غير الاعتيادي

- تستخدم توقعات موجودة في قواعد بيانات تهديدات

- تقدم معلومات بعد وقوع التسلل غالباً •

- بيانات التوقيع قد تصبح قديمة بسرعة •

- تولد إنذارات كاذبة كثيرة •

• اقترح على الوكالات استخدام أنواع متعددة من تقنيات أنظمة كشف ومنع التسلل لتحقيق اكتشاف ومنع أكثر شمولاً ودقة، وفصل -
الأنظمة إلى أقسام لاحتواء المخترق إذا تم اختراق جزء منها والحد من الضرر المحتمل

• أخبر المشاركين أن مزيداً من التفاصيل حول هذه الإجراءات سيُعطى لاحقاً -

الشريحة 13: كشف التسلل والمرونة

• منع التسلل يجنب الحاجة لإعادة بناء الأنظمة وإعادة تكوين البيانات -

• فصل الأنظمة يقلل من تكلفة تنظيف الحوادث -

• الحفاظ على خطة مرونة واستجابة -

• تنفيذ الاستجابات المعدة بسرعة -

• نشر الوعي العام مقدماً في حال الحاجة لوقف تشغيل تام -

وصف رسومي: لا يوجد

• اشرح العلاقة بين كشف ومنع التسلل والمرونة -

- أنظمة الكشف/المنع تساعد في منع النشاط الإجرامي وتتفادى إعادة البناء المكلفة •

- فصل الخوادم والشبكات يجعل تنظيف الحوادث أرخص بكثير.
- تدريب فرق الدفاع الشبكي على تنفيذ خطط استجابة مدروسة يضمن استعداد الفرق.
- تنفيذ استجابات معدة جيداً يمكن من مواجهة التسللات بسرعة وفعالية.
- تزويد الجمهور بمعلومات عامة مسبقاً يمكن التعاون المجتمعي عند اللزوم، خصوصاً إذا تطلبت الحالة إيقاف تشغيل كامل للبنية التحتية الحرجة.

(الشريحة 14: جدار الحماية (1 من 3

نظام أمني للشبكة مصمم لتوفير الحماية ضد المهاجمين الخارجيين عن طريق حجب حركة شبكية خبيثة أو غير ضرورية ومنع - البرمجيات الخبيثة من الوصول إلى الشبكة

وصف رسومي: لا يوجد

اشرح أن جدران الحماية وسيلة وقائية ضرورية لحجب البيانات من مواقع أو تطبيقات معينة مع السماح بمرور البيانات الضرورية -
(عرّف جدار الحماية (كما ورد أعلاه -

(الشريحة 15: جدار الحماية (2 من 3

:الخصائص -

- قد يكون جهازاً مادياً أو برنامجاً
- يجب تهيئته بشكل صحيح لمستوى الأمان المطلوب
- يحد من حركة المرور بين الشبكات

وصف رسومي: سلسلة من الأقفال الرقمية، واحد منها مفتوح

(الشريحة 16: جدار الحماية (3 من 3

- يوقف حركة المرور التطفلية من الدخول -
- لا يحمي من البرامج الخبيثة المثبتة داخلياً -
- لا ينبه لحدوث تسلل -
- يُستخدم مع برامج مضادة للفيروسات وممارسات حوسبة آمنة -

وصف رسومي: لا يوجد

:اشرح خصائص جدران الحماية -

- قد تكون جهازاً خارجياً بين الإنترنت أو اتصال الشبكة وجهاز الحاسوب أو نظام متعدد الحواسيب، أو ميزة مدمجة بنظام التشغيل —
- يجب تمكين جدار الحماية البرمجي حتى لو كان هناك جدار حماية مادي
- الجدران التجارية مُهيأة افتراضياً، لكن المستخدم يجب أن يقيم ما إذا كانت الإعدادات الافتراضية كافية لحماية نظم البنية التحتية
- الحرجة وقد تحتاج لتعزيز
- تحد من الوصول الخارجي بين الشبكات لمنع التسلات
- تراقب الحركة الخارجة وتحاول منع مرور حركة التسلل
- لا تحمي من البرامج الخبيثة التي يتم تثبيتها مع برمجيات أخرى أو التي تثبت عن طريق الخطأ
- لا تنبه مشغلي النظام بتسللات داخل الشبكة
- يجب استخدامها مع مضادات الفيروسات وممارسات حوسبة آمنة لتعزيز المقاومة

الشريحة 17: الاستجابة — مهندس الأمن السيبراني

دور وظيفي في قسم تكنولوجيا المعلومات يساعد في الأمن السيبراني بتحديد من يحتاج الوصول إلى أي معلومات؛ يخطط وينسق وينفذ -
برامج أمن المعلومات؛ ويساعد في الحماية من تهديدات الإنترنت
وصف رسومي: أيدي تكتب على لوحة مفاتيح

:اشرح أن نظام كشف ومنع التسلل يجب أن يكون داعماً بوجود مهندس أمن سيبراني -

.(عرّف مهندس الأمن السيبراني (كما ورد أعلاه -

الشريحة 18: مصادر الجرائم السيبرانية

:المصادر الرئيسية لجرائم البنية التحتية الحرجة السيبرانية -

- حكومات وطنية
- إرهابيون
- جواسيس صناعيون وجماعات الجريمة المنظمة

وصف رسومي: خريطة العالم مع شفرة حاسوبية فوقها

:اشرح أن المصادر الرئيسية قد تكون -

الحكومات الوطنية: تهديداتها تتراوح من تشويه صفحات الويب ودعائية إلى التجسس وتعطيل شديد مع خسائر في الأرواح والبنى التحتية؛ الدول وحدها تبدو قادرة على تطوير قدرات كاملة لمهاجمة البنى التحتية الحرجة.

الإرهابيون: حتى الآن أقل تطوراً في قدرات الشبكات مقارنة بغيرهم، ومن المرجح أن يشكلوا تهديداً سيبرانياً محدوداً في المدى القريب، إذ أن البدائل التقليدية (مثل القنابل) قد تكون أكثر فعالية الآن؛ ولكن على المدى البعيد قد يزداد التهديد مع دخول أجيال أكثر مهارة تقنياً.

الجواسيس الصناعيون والجريمة المنظمة: يشكلون تهديداً متوسطاً إلى كبيراً للبنية التحتية بسبب إمكانياتهم في التجسس الصناعي والسرقات المالية واسعة النطاق وقدرتهم على توظيف أو تطوير خبراء اختراق؛ أهدافهم الأساسية مالية، وثانويات مثل سرقة الأسرار التجارية والابتزاز.

حملة Stop.Think.Connect الشريحة 19:

حملة توعية عامة لرفع فهم التهديدات السيبرانية وتمكين الجمهور ليكون أكثر أماناً على الإنترنت -

الموقع الإلكتروني يتضمن نصائح وأدوات وفيديوهات ومدونة ومواد ترويجية -

www.dhs.gov/about-stopthinkconnect مزيد من المعلومات على -

وصف رسومي: خريطة العالم مع شفرة حاسوبية

افحص الرابط لاختبار الاتصال قبل عرض الشريحة؛ إذا عمل، أظهر الموقع للمشاركين، وإن لم يعمل، صف عناصر الموقع واكتب -
الرابط على ورق فليب تشارت وعلقه.

:كمثال "Stop.Think.Connect" اشرح أهمية نشر الوعي العام باستخدام حملة وزارة الأمن الداخلي الأمريكية -

• حملة وطنية لرفع فهم التهديدات السيبرانية وتمكين الجمهور ليكون أكثر أماناً على الإنترنت.

• مع انتشار استخدام التقنيات والوقت الذي يقضيه الناس على الإنترنت، تزداد الحاجة إلى موارد بسيطة وسهلة الفهم لضمان الأمان.

• الحملة توفر نصائح وأدوات ومواد تعليمية وتشجع اعتبار سلامة الإنترنت مسؤولية مشتركة في المنزل ومكان العمل والمجتمع.

• National Cyber Security Alliance هي شراكة فريدة بين القطاعين العام والخاص تنفذ بالتنسيق مع.

• أهداف الحملة تتضمن رفع وعي الوطنية بأمن المعلومات وعلاقته بالأمن الوطني، إشراك الجمهور والقطاع الخاص والحكومات المحلية والولائية، والتواصل حول استراتيجيات لحماية الأفراد والأسر والمجتمعات على الإنترنت.

• مزيد من المعلومات على: <https://www.dhs.gov/about-stopthinkconnect>.

اسأل المشاركين إذا كان لديهم برنامج مشابه في بلدانهم، وإذا لا، كيف يمكنهم تنفيذ مثل هذا البرنامج -

(الشريحة 20: تقييم الأمن السيبراني للمرونة (1 من 3) (كتاب العمل 7.1)

هل تستخدم الوكالة/المنظمة تقنية أمان تقيد البرامج القابلة للتشغيل في وقت واحد؟ -

هل تضمن أن كل التنزيلات والتحديثات تأتي من مصادر موثوقة؟ -

هل تعزل الشبكات عن أي شبكات غير موثوقة، خاصة الإنترنت؟ -

وصف رسومي: لا يوجد

(الشريحة 21: تقييم الأمن السيبراني للمرونة (2 من 3) (كتاب العمل 7.1)

هل تفصل نظام الحاسوب إلى أجزاء مميزة؟ -

هل لديها سياسة صارمة لإصدار وتصديق بيانات الوصول للنظام؟ -

هل تتحكم في الوصول عن بعد بمصادقات قوية وحدود زمنية؟ -

وصف رسومي: لا يوجد

(الشريحة 22: تقييم الأمن السيبراني للمرونة (3 من 3) (الملحق 7.1)

هل تراقب النظام باستمرار وتستجيب فوراً لحوادث التسلل؟ -

تحدي مستمر ومتطور -

المرونة جزء من دفاعنا -

وصف رسومي: لا يوجد

اشرح أن التداخلات السيبرانية في أنظمة البنية التحتية الحرجة تزداد تكراراً -

أشر المشاركين إلى كتاب العمل 7.1 وناقش كل سؤال حسب مستوى تفصيل الملحق وخبرة المشاركين -

اشرح أن الدفاع الحديث يتطلب تدابير تحمي ليس فقط محيط البنية التحتية بل أيضاً الداخل، وأن الدفاع عملية مستمرة ومتطورة -

اشرح أن إطار عمل أمن سيبراني معرف بوضوح يوفر المرونة اللازمة لضمان استمرار عمل نظم المعلومات في بيئة محمية من -
محاولات الوصول الخبيثة من إرهابيين أو مجرمين

الشريحة 23: مناقشة جماعية كبيرة: التهديدات الداخلية

التهديدات الداخلية هي أكثر التهديدات بروزاً للوكالة -

ما قضايا الأمن السيبراني التي قد يرتكبها الداخلون؟ -

ما الدوافع الشخصية المحتملة للداخل؟ -

ماذا يمكن للوكالة أن تفعل لتقليل احتمال التهديدات الداخلية؟ -

وصف رسومي: لا يوجد

يبين للمشاركين أن التركيز الآن سينتقل لمناقشة التهديدات الداخلية -

اشرح أن رغم رغبة معظم الوحدة في معالجة نشاطات الدخلاء الخارجيين، إلا أن التهديد الداخلي يعد أحد أبرز التهديدات للمنظمة -

اطرح السؤال: ما قضايا الأمن السيبراني التي قد يخطر فيها الداخلون؟ -

إن لم يرد المشاركون، أضف أمثلة مثل -

- استخدام غير مصرح به لحاسوب حكومي أو جهاز
- مشاركة بيانات الاعتماد أو كلمات المرور أو دخول عدة مستخدمين على حساب واحد
- الوصول إلى مواقع محظورة
- سرقة أو فقدان ممتلكات حكومية
- الإفراج أو الوصول غير المصرح به إلى معلومات مملوكة أو حساسة أو سرية
- تحميل أو تخزين أو نقل معلومات سرية إلى برمجيات أو أجهزة أو أنظمة غير مصرح بها
- إدخال أجهزة أو برامج أو وسائط دون تفويض
- حركة بريد إلكتروني بمرفقات أو نقل ملفات كبيرة إلى عناوين خارجية غير حكومية أو غير عسكرية

اطرح السؤال: ما الدوافع الشخصية المحتملة للداخل؟ -

إن لم تُقدّم إجابات، أضف الدوافع التالية -

- الجشع أو الحاجة المالية
- الغضب أو الرغبة في الانتقام
- (مشاكل في العمل) (نقص تقدير، نزاعات، استياء، فصل محتمل)
- الأيديولوجيا أو الانتماء لقضية
- (ولاءات منقسمة) (لشخص آخر أو شركة أو دولة أخرى)

- الرغبة في المغامرة أو التشويق
- القابلية للابتزاز
- الأنا أو صورة الذات
- السعي لنيل منفعة أو معروف
- السلوكيات الإدمانية أو المدمرة
- مشاكل عائلية

اطرح السؤال: ماذا يمكن للوكالة أن تفعل لتقليل احتمال التهديدات الداخلية؟ -

:إن لم تُقدّم إجابات، اقترح إجراءات مثل -

- إجراء تحريات خلفية دقيقة على الموظفين ومستخدمي الشبكة عند التعيين وفواصل عشوائية أثناء العمل، خاصة لمن لديهم وصول كبير إلى نظم المعلومات وبروتوكولات الأمن السيبراني
- توفير مراقبة مستمرة لأنظمة الشبكة للتأكد من عدم طلب أو حصول المستخدمين على وصول غير مناسب
- تقديم تدريب مستمر للأمن السيبراني للموظفين لمناقشة كيف يتجنبون أن يصبحوا داخلين غير مقصودين وتوضيح العواقب القانونية للسلوك العمدي

الموضوع: سياسات وإجراءات الأمن السيبراني — 30 دقيقة

:هدف التعلم الممكن

.شرح سياسات وإجراءات الأمن السيبراني -

(الشريحة 24: سياسات وإجراءات الأمن السيبراني (1 من 3

- محددة لأمن نظم معلومات الوكالة -
- بروتوكولات لاختيار والعمل مع شركاء المجتمع -
- التعاون مع الشركاء المجتمعيين لكتابة السياسات والإجراءات -
- حدود مشاركة المعلومات -
- وصف رسومي: لا يوجد

:اشرح أن على الوكالات وضع سياسات وإجراءات للأمن السيبراني وفق التوجيهات التالية -

- ضمان أن السياسات والإجراءات تعالج ضوابط الأمان الخاصة بنظام المعلومات في وكالتك
- تضمين بروتوكولات تعالج كيفية اختيار الشركاء المجتمعيين وكيف ستعمل الوكالة معهم خلال الأزمات أو الكوارث الطبيعية
- التعاون مع الشركاء خلال كتابة الوثائق لضمان تفاهمهم وموافقتهم ووجود حقوق اعتماد على الوثائق التي ستصبح جزءاً من سياساتهم أيضاً
- تحديد نطاق وحدود مشاركة المعلومات مع وكالات أو منظمات أو شركاء مجتمعين؛ يجب أن تتضمن الإرشادات القانونية سياسات وإجراءات ومنهجيات لكل منظمة بشأن:
 - الإبلاغ والإخطار عن الحوادث -
 - المراقبة للكشف عن الحوادث -
 - تنفيذ تدابير أمنية لمنع واكتشاف الحوادث -
 - الاحتفاظ بالوثائق الأمنية لتحديث التدابير -

(الشريحة 25: سياسات وإجراءات الأمان السيبراني (2 من 3

:سياسات لمعالجة ثلاثة عناصر لتخطيط المرونة -

- الصلابة
- القدرة على التدبير (Resourcefulness)
- الاسترداد السريع

وصف رسومي: حارس أمن يقف ينظر إلى أفق المدينة

:عالج العناصر الثلاثة في سياسات وإجراءات الأمان السيبراني للشركاء الداخليين والخارجيين -

- الصلابة: القدرة على الحفاظ على العمليات والوظائف الحيوية أثناء الأزمة
- القدرة على التدبير: القدرة على التحضير بمهارة والاستجابة وإدارة الأزمة أو الاضطراب أثناء حدوثه
- الاسترداد السريع: القدرة على العودة إلى العمليات الطبيعية أو إعادة تشكيلها بأسرع صورة ممكنة وفعالة بعد الاضطراب

(الشريحة 26: سياسات وإجراءات الأمان السيبراني (3 من 3

:سياسات وإجراءات للإبلاغ عن الحوادث -

- حوادث داخلية

- حوادث البنية التحتية عبر الحدود
- نقاط اتصال للإبلاغ
- تدريب الأفراد

وصف رسومي: مجرم سيبراني يسرق معلومات من حاسوب

:اشرح أن يجب وجود سياسات وإجراءات للإبلاغ عن تسلل النظام، تشمل -

- الحوادث الداخلية
- حوادث البنية التحتية عبر الحدود: عرّف البنية التحتية عبر الحدود كما في المصطلحات — هذه الاعتمادات تخلق نقاط ضعف إضافية ومصدر محتمل لعدم الاستقرار حتى في دول ذات تدابير داخلية قوية
- معلومات نقاط الاتصال للإبلاغ عن الحوادث
- سياسات تحدد تدريب الأفراد حول إجراءات الإبلاغ

الشريحة 27: أسئلة للمناقشة

- ما متطلبات الإبلاغ عن الأمن السيبراني الموجودة حالياً في وكلاتكم أو بلدكم؟
- ما متطلبات الإبلاغ التي تفكرون في إضافتها؟
- وصف رسومي: لا يوجد

.اطلب من المشاركين مناقشة متطلبات الإبلاغ الموجودة وما الذي قد يضيفونه. سجّل الردود؛ ستختلف الإجابات حسب السياق -

لتكتيكات واتجاهات الإرهاب ATA الشريحة 28: كتيب

- التعريف
- التهديدات والأسلحة المتنامية
- تكتيكات واتجاهات الإرهابيين
- استخدام الإرهابيين للإنترنت
- منشورات إرهابية
- مراجع للبقاء مطلعين

وصف رسومي: شاشة لابتوب تعرض شخصاً يشير إلى سلاح

ATA Terrorist Tactics and Trends Handbook. أشر المشاركين إلى كتيب -

:أشير باختصار إلى عناصر الإرهاب في الكتيب -

- التعريف: عنف مُدبّر ودوافع سياسية ضد أهداف غير مقاتلة
- وأشكال تهديد وسيبرانية MANPADS: التهديدات والأسلحة المتنامية
- تكتيكات واتجاهات الإرهابيين: التفجير الأكثر شيوعاً، هجمات الذئاب المنفردة
- استخدام الإرهابيين للإنترنت: تكنولوجيا المعلومات ووسائل التواصل الاجتماعي
- المنشورات الإرهابية وموارد للاطلاع

شجّع المشاركين على قراءة الكتيب كاملاً خلال وقت الدراسة هذا الأسبوع -

TeachBack الشريحة 29: لحظة

ما تعريف الأمن السيبراني؟ -

كيف يُستخدم الأمن السيبراني للرد على التهديدات الجارية؟ -

ما أمثلة السياسات والإجراءات الخاصة بالأمن السيبراني؟ -

وصف رسومي: لا يوجد

لتقييم فهم المشاركين TeachBack نفذ لحظة -

اسأل: ما تعريف الأمن السيبراني؟ إن لم يذكر المشاركون، أضف التعريف: الأمن السيبراني هو منع الضرر أو الاستخدام غير المصرح به أو استغلال أنظمة وقواعد بيانات المعلومات والاتصالات الإلكترونية والمعلومات المحتواة فيها لضمان السرية والسلامة والتوفر؛ واستعادة أنظمة المعلومات والاتصالات الإلكترونية في حالة هجوم إرهابي أو كارثة طبيعية.

اسأل: كيف يُستخدم الأمن السيبراني للرد على التهديدات الجارية؟ إن لم تُقدّم إجابات، أضف النقاط التالية: استخدام تكنولوجيا المعلومات؛ فحوصات خلفية لجميع العاملين والمتعاقدين؛ إشراك المؤسسة بأكملها؛ بناء شراكات مجتمعية؛ تحديد البنية التحتية الحرجة. والسيبرانية؛ لامركزية البنية التحتية؛ دمج التكنولوجيا لحماية التكنولوجيا؛ استخدام أنظمة كشف ومنع التسلل؛ استخدام جدران حماية.

اسأل: ما أمثلة السياسات والإجراءات؟ إن لم تُقدّم إجابات، أضف: سياسات لتخطيط المرونة؛ سياسات وإجراءات للإبلاغ عن الحوادث -

اسأل المشاركين إن كانت لديهم أي أسئلة حول ما تم تغطيته -

الموضوع: ملخص الوحدة — 10 دقائق

الشريحة 30: ملخص الوحدة

- لمحة عامة عن الأمن السيبراني -
- الحماية من التهديدات السيبرانية -
- سياسات وإجراءات الأمن السيبراني -
- وصف رسومي: لا يوجد

لخص الوحدة بمراجعة النقاط التالية -

- لمحة عامة عن الأمن السيبراني: نظام المعلومات، الفضاء السيبراني، البنية التحتية السيبرانية، التهديد السيبراني، الهجوم السيبراني، الأمن السيبراني
- الحماية من التهديدات السيبرانية: استخدام تكنولوجيا المعلومات، فحوصات الخلفية، إشراك المؤسسة بأكملها، بناء شراكات مجتمعية، تحديد البنية التحتية الحرجة والسيبرانية، لامركزية البنية التحتية، دمج التكنولوجيا لحماية التكنولوجيا، استخدام أنظمة كشف ومنع التسلل، جدران الحماية
- مصادر الجرائم السيبرانية
- للتوعية العامة Stop.Think.Connect حملة
- تقييم الأمن السيبراني للمرونة
- سياسات وإجراءات الأمن السيبراني: سياسات لتخطيط المرونة وسياسات وإجراءات للإبلاغ عن الحوادث
- اسأل إن كانت هناك أي أسئلة حول محتوى الوحدة -
- اشرح أن الوحدة 8: الوعي بالمراقبة — ما الذي يمكنك فعله ستشرح الإجراءات اللازمة لاكتشاف والإبلاغ عن أنشطة المراقبة - المشبوهة المرتبطة بالمراقبة العدائية