الوحدة 7

الأمن السيبراني

هدف الوحدة

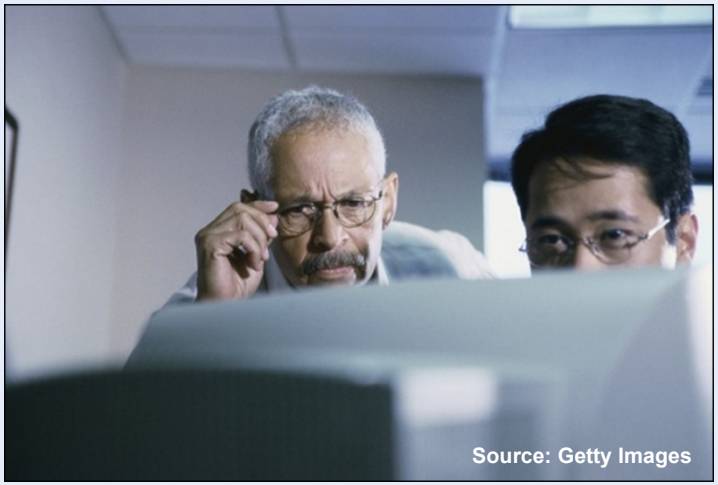
- عند نهاية هذه الوحدة التعليمية، ستتمكن من شرح التهديدات السيبرانية لمنظمتك.

Module Objective

- By the end of this module, you will be able to explain cyberthreats to your organization

نظرة عامة على الأمن السيبراني -- تعريفات هامة

- نظم المعلومات
- الفضاء السيبراني
- البنية الأساسية السيبرانية
- التهديد السيبراني
- الهجوم السيبراني
- الأمن السيبراني



Cybersecurity Overview —
Important Definitions

- Information system
- Cyberspace
- Cyberinfrastructure
- Cyberthreat
- Cyberattack
- Cybersecurity

سؤال للمناقشة

- ما هي أنماط البنية الأساسية الحرجة في بلدك والتي تتطلب الأمن السيبراني؟

Discussion Question

- What types of critical infrastructure in your nation require cybersecurity?

توجهات الأمن السيبراني (1 من 3)

- الهجوم السيبراني المتكرر على البنية الأساسية الحرجة
- استمرار تزايد التهديد السيبراني ضد البنية الأساسية الحرجة
- الاعتماد المتبادل على الإنترنت

Cybersecurity Trends (1 of 3)

- Repeated cyberattacks on critical infrastructure
- Cyberthreat to critical infrastructure continues to grow
- Cyberinterdependency

توجهات الأمن السيبراني (2 من 3)

- التهديدات الداخلية على أنظمة الكمبيوتر
- الملكية الأجنبية للبنية الأساسية
- التحديات الخطيرة التي تواجهها الدولة في مجال الأمن القومي

Cybersecurity Trends (2 of 3)

- Insider threats to computer systems
- Foreign ownership of infrastructure
- Serious national security challenges for a nation to confront

توجهات الأمن السيبراني (3 من 3)

- أهداف معالجة التوجهات:
  - تحسين المستوى الأمني والمرونة فيما يتعلق بالبنية الأساسية الحرجة في البلاد
  - الحفاظ على بيئة سيبرانية تعمل بكفاءة بغرض تدعيم السلامة والخصوصية
  - الشراكة مع الجهات المالكة للبنية التحتية والكوادر التشغيلية لتحسين مشاركة المعلومات

Cybersecurity Trends (3 of 3)

- Goals to address trends:
  - Enhance security and resilience of a nation's critical infrastructure
  - Maintain an efficient cyberenvironment that promotes safety and privacy
  - Partner with infrastructure owners and operators to improve information sharing

سؤال للمناقشة

- في حالة تعرض البنية الأساسية الحرجة لهجوم سيبراني ناجح نتج عنه إيقاف العمليات، فما هي العواقب الناجمة في بلدك؟

Discussion Question

- If any of your critical infrastructure experienced a successful cyberattack and stopped operations, what would be the consequences for your nation?

الحماية من التهديدات السيبرانية (1 من 2)

- استخدام تكنولوجيا المعلومات
- فحص الخلفيات الخاصة بجميع العاملين والمتعاقدين
- إشراك الوكالة بكاملها -- المستويات القيادية العليا، والمدراء في الطبقة المتوسطة وضباط الصفوف الأولى وكوادر التحليل

Protecting against Cyberthreats (1 of 2)

- Using information technology
- Checking backgrounds of all personnel and contractors
- Involving the entire agency — senior leadership, mid-level leaders, front-line officers, and analysts

الحماية من التهديدات السيبرانية (2 من 2)

- بناء الشراكات المجتمعية
- تحديد البنية الأساسية السيبرانية الحرجة
- عدم مركزية البنية الأساسية السيبرانية الحرجة
- دمج التكنولوجيا لحماية التكنولوجيا


Source: Getty Images

Protecting against Cyberthreats (2 of 2)

- Building community partnerships
- Determining critical and cyberinfrastructure
- Decentralizing critical and cyberinfrastructure
- Incorporating technology to protect technology

رصد ومنع التسلل (1 من 2)

- عملية مراقبة الأحداث التي تقع داخل نظام الكمبيوتر أو الشبكة مع تحليلها بحثاً عن وقائع محتملة ومحاولة إيقاف عمليات التسلل المحتملة

Intrusion Detection and Prevention (1 of 2)

- The process of monitoring the events occurring in a computer system or network, analyzing them for signs of possible incidents, and attempting to stop detected possible incidents

رصد ومنع التسلل (2 من 2)

العيوب	المزايا
• توفر معلومات بشأن تسلل مشبوه بعد وقوعه • احتواء المعلومات التي قد تتقادم بسرعة • التوجه لتوليد عدد أكبر من الإنذارات الكاذبة بنسبة أكثر من الهجمات الحقيقية - الأمر الذي يسفر عن عدم الإلتفات إلى الهجمات الحقيقية أو إهمالها	• مراقبة المرور والتنبيهات الخاصة بأي مرور غير طبيعي • التنبيهات الخاصة بتوقيع الحاسوب المدرج في تهديدات قواعد البيانات

Intrusion Detection and Prevention (2 of 2)

Advantages	Disadvantages
• Monitors traffic and alerts on what is unusual about an aspect of the traffic • Alerts on a computer signature that is listed in a database of threats	• Provides information about a suspected intrusion after it has occurred • Contains information that becomes outdated quickly • Tends to generate a greater number of false alarms than real attacks — resulting in real attacks being missed or ignored

رصد التسلل والمرونة

- الوقاية من التسلل تحول دون الإحتياج إلى إعادة بناء النظم وإعادة هيكلة البيانات
- ويساعد فصل الأنظمة على تيسير الجهود الرامية إلى إعادة التنظيف بتكاليف أقل
- الحفاظ على خطة استجابة مرنة
- تنفيذ الإستجابات الجاهزة بسرعة
- إذاعة تنبيهات مبكرة لتوعية الجمهور في حالة استجابة الإغلاق الكامل

Intrusion Detection and Resilience

- Preventing an intrusion avoids the need to rebuild systems and reconstruct data
- Separating systems makes incident cleanup significantly less costly
- Maintaining a resiliency plan of response
- Executing prepared responses quickly
- Broadcasting advance public awareness in case of total shutdown response

الجدار الناري (1 من 3)

- نظام أمني شبكي مصمم لتوفير الحماية ضد عناصر الهجوم الخارجي عن طريق عمل درع لحماية أجهزة الكمبيوتر أو الشبكة المعلوماتية من أي دخول خبيث أو غير ضروري ومنع البرمجيات الخبيثة من دخول الشبكة

Firewall (1 of 3)

- A network security system designed to provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic and preventing malicious software from accessing the network

الجدار الناري (2 من 3)

- الخصائص:
  - قد يتكون من معدات أو برمجيات
  - يجب أن يكون مبرمجا بطريقة صحيحة تتوافق مع المستوى الأمني المطلوب
  - الحد من المرور بين الشبكات

Firewall (2 of 3)

- Characteristics:
  - May be hardware or software type
  - Must be properly configured for desired level of security
  - Limits traffic between networks

الجدار الناري (3 من 3)

- يقوم بإيقاف المرور المتسلل ويمنع محاولات الدخول
- لا يوفر الحماية ضد البرامج الخبيثة التي تم تحميلها
- لا يعطئ إشارة تنبيه عند حدوث تسلل
- يستخدم مع برمجيات مضادة للفيروسات والممارسات الحسنة لأجهزة الكمبيوتر

Firewall (3 of 3)

- Stops intrusive traffic from entering
- Does not protect against installed malicious programs
- Does not signal an intrusion
- Use with anti-virus software and safe computing practices

الاستجابة -- مهندس الأمن السيراني

- وظيفة يضطلع بها فرد مسؤول عن قسم تكنولوجيا المعلومات بغرض المساعدة في تحقيق الأمن المعلوماتي السيبراني عن طريق تحديد الأفراد المصرح لهم بالوصول للمعلومات؛ وتحديد الخطط والإحداثيات وتطبيق المعلومات الخاصة ببرامج الأمن، والمساعدة في الحماية ضد تهديدات الأمن عن طريق الإنترنت والتي تعمل على تسهيل الجرائم الإلكترونية


Source: Getty Images

Response — Cybersecurity Engineer

- A personnel role in the information technology department that aids in cybersecurity by determining who requires access to which information; plans, coordinates, and implements information security programs; and helps protect against Internet threats that facilitate cybercrime

مصادر الجرائم الإلكترونية

- المصادر الرئيسية للجرائم الإلكترونية ضد البنية الأساسية الحرجة:
  - الحكومات الوطنية
  - الإرهابيون
  - عناصر التجسس الصناعي وجماعات الجريمة المنظمة

Cybercrime Sources

- Primary sources of critical infrastructure cybercrime:
  - National governments
  - Terrorists
  - Industrial spies and organized crime groups

قف- فكّر- تواصل

- حملات التوعية العامة لزيادة فهم التهديد السيبراني وتدعيم الجمهور لاستخدام الإنترنت بطريقة سالمة وآمنة
- تتضمن المواقع الشبكية تعليمات وأدوات وعروض فيديوهات ومواقع مدونات ومواد ترويجية
- للحصول على مزيد من المعلومات

www.dhs.gov/about-stopthinkconnect

Stop.Think.Connect

- Public awareness campaign to increase the understanding of cyberthreats and empower the public to be safer and more secure online
- Website includes tips and tools, videos, blog, and promotional materials
- More information at www.dhs.gov/about-stopthinkconnect

تقييم الأمن السيبراني من حيث المرونة (1 من 3)

راجع


الكتيب 7.1

- هل تستخدم الوكالة أو المنظمة:
  - أسلوب أمني يحدد البرامج التي يمكن تشغيلها في وقت واحد؟
  - ضمان أن جميع تحميلات البرامج وتحسيناتها آتية من مصدر مضمون؟
  - عزل الشبكات من أية مواقع غير موثوقة خصوصاً المواقع الشبكية الإلكترونية؟

Evaluating Cybersecurity for Resilience (1 of 3)

Refer To: Workbook 7.1

- Does the agency or organization:
  - Use a security technique that limits what programs can run at one time?
  - Ensure that all program downloads and upgrades come from verified sources?
  - Isolate networks from any untrusted networks, especially the Internet?

تقييم الأمن السيبراني من حيث المرونة (2 من 3)

راجع

الكتيب 7.1

- هل يتم فصل نظام الكمبيوتر في أجزاء منفصلة ومتميزة؟
- هل تتوافر سياسة صارمة لإصدار وترخيص الإطلاع على الوثائق داخل النظام؟
- هل يتم السيطرة على الدخول عن بعد والتأكد من المؤهلات ومحدوديات الوقت؟

Evaluating Cybersecurity for Resilience (2 of 3)

Refer To: Workbook 7.1

- Separate its computer system into distinct parts?
- Have a strict policy for issuing and authenticating access credentials to the system?
- Control remote access with strong credentials and time limits?

تقييم الأمن السيبراني من حيث المرونة (3 من 3)

راجع

الكتيب 7.1

- هل يتم مراقبة النظام باستمرار والإستجابة الفورية لحوادث التسلل؟
  - التحديات القائمة والمستجدة
  - المرونة جزء من الدفاع لدينا

Evaluating Cybersecurity for Resilience (3 of 3)

Refer To: Workbook 7.1

- Monitor the system continuously and respond immediately to intrusion incidents?
  - Ongoing and evolving challenge
  - Resilience is part of our defense

نقاش ضمن إطار المجموعة الكبيرة: التهديدات الداخلية

- التهديدات الداخلية هي أخطر التهديدات السائدة ضد الوكالة
- ما هي القضايا المتعلقة بالأمن السيبراني المرتبطة بالعناصر الداخلية؟
- ما هي في رأيكم بعض دوافع العناصر الداخلية المتواطئة؟
- ماذا يمكن أن تقوم به الوكالة أو المنظمة لتقليص احتمالات التعرض لهجوم من العناصر الداخلية؟

Large-Group Discussion: Insider Threats

- The most predominant threats that exist to an agency are insider threats
- What cybersecurity issues could involve an insider?
- What do you think are some of the personal motivations of an insider?
- What could an agency or organization do to reduce the possibility of insider threats?

السياسات والإجراءات الخاصة بالأمن السيبراني (1 من 3)

- خواص الأمن السيبراني في أنظمة المعلومات بالوكالة
- بروتوكولات الإنتقاء والعمل مع شركاء المجتمع المحلي
- التعاون مع شركاء المجتمع المحلي لصياغة السياسات والإجراءات
- محدوديات التشارك في المعلومات

Cybersecurity Policies and Procedures (1 of 3)

- Specific to cybersecurity of agency information systems
- Protocols to select and work with community partners
- Collaboration with community partners to write policies and procedures
- Limitations of information sharing

السياسات والإجراءات الخاصة بالأمن السيبراني (2 من 3)

- سياسات لمعالجة 3 عناصر خاصة بمرونة التخطيط:
  - القوة
  - الحيلة
  - التعافي السريع

Cybersecurity Policies and Procedures (2 of 3)

- Policies to address three elements of resilience planning:
  - Robustness
  - Resourcefulness
  - Rapid recovery

السياسات والإجراءات الخاصة بالأمن السيبراني (3 من 3)

- السياسات والإجراءات للإبلاغ عن الحادث:
  - الحوادث الداخلية
  - الحوادث ضد البنية الأساسية عبر الحدود
  - نقاط الاتصال الخاصة بالإبلاغ
  - تدريب الموظفين


Source: Getty Images

Cybersecurity Policies and Procedures (3 of 3)

- Policies and procedures for incident reporting:
  - Internal incidents
  - Cross-border infrastructure incidents
  - Reporting points-of-contact
  - Personnel training

أسئلة المناقشة

- ما هي متطلبات الإبلاغ الخاصة بالأمن السيبراني القائمة بالفعل في منظمتك أو بلدك؟
- ما هي متطلبات الإبلاغ الخاصة بالأمن السيبراني التي تعتزم إضافتها؟

Discussion Questions

- What cybersecurity reporting requirements are already in place in your agency or nation?
- What cybersecurity reporting requirements would you consider adding?

دليل التكتيكات والتوجهات الإرهابية الصادر عن مكتب المساعدة في مكافحة الإرهاب

راجع

دليل التكتيكات والتوجهات الإرهابية

- التعريف
- التهديدات المتزايدة والأسلحة
- التكتيكات والتوجهات الإرهابية
- استخدام الإرهابيين للإنترنت
- منشورات الإرهابيين
- مراجع لمتابعة الموقف باستمرار

Source: ATA Library

ATA Terrorist Tactics and Trends Handbook	Refer To: Terrorist Tactics and Trends Handbook

- Definition
- Growing threats and weapons
- Terrorist tactics and trends
- Terrorist use of the Internet
- Terrorist publications
- References to stay informed

لحظة التعليم الإسترجاعي

- ما هو تعريف الأمن السيبراني؟
- كيف يستخدم الأمن السيبراني للإستجابة للتهديدات السيبرانية القائمة؟
- ما هي بعض الأمثلة حول سياسات وإجراءات الأمن السيبراني؟

TeachBack Moment

- What is the definition of cybersecurity?
- How is cybersecurity used to respond to ongoing cyberthreats?
- What are some examples of cybersecurity policies and procedures?

ملخص الوحدة

- نظرة عامة على الأمن السيبراني
- الحماية ضد التهديدات السيبرانية
- سياسات وإجراءات الأمن السيبراني

Module Summary

- Cybersecurity overview
- Protecting against cyberthreats
- Cybersecurity policies and procedures