الأمن السيبراني

منهج مرجعي

عام

الأمن السيبراني

منهج مرجعي

عام

National Defence
Office of the Commander
Military Personnel Generation
P.O. Box 17000 Station Forces
Kingston, ON K7K 7B4

Défense nationale
Bureau du commandant
Génération du personnel militaire
CP 17000, Succursale Forces
Kingston, ON K7K 7B4

4500-1 (SSO EE)

6 October 2016

Cybersecurity: A Generic Reference Curriculum (RC)

Dear Partners/NATO Members,

It pleases us to share with you the document entitled *Cybersecurity: A Generic Reference Curriculum (RC)*, developed, on behalf of NATO and the Partnership for Peace Consortium (PfPC) of Defense Academies and Security Studies Institutes, by a multinational team of academics and practitioners. This document aims to provide NATO and partner countries with in-depth learning objectives and curriculum support for academic courses broadly related to Cybersecurity.

The Cybersecurity Reference Curriculum consists of four themes: i) Cyberspace and the Fundamentals of Cybersecurity, ii) Risk Vectors, iii) International Cybersecurity Organizations, Policies and Standards and iv) Cybersecurity Management in the National Context. The four themes and associated blocks have been carefully chosen to encompass the broadest spectrum of Cybersecurity issues and topics, and to provide the most pertinent level of education.

This document is best understood as a resource to NATO and partner countries looking to develop and gain greater appreciation of the spectrum of issues, national and international, entangled in the practices of cybersecurity. It is presented in the hope that it will be noted by NATO in due time through the appropriate committees. The next envisioned step will be to work with partner defense education establishments in

4500-1 (OSEM PED)

Le octobre 2016

Programme de reference (PR) générique de la Cybersécurité

Chers partenaires/membres de l'OTAN,

Il nous fait grand plaisir de partager avec vous le document intitulé *Programme de référence (PR) générique de la Cybersécurité* développé par une équipe multinationale d'universitaires et de praticiens au nom de l'OTAN et du Groupement d'institutions d'études de défense et de sécurité du Partenariat pour la paix (PPP). L'objectif de ce document est d'offrir à l'OTAN et aux pays partenaires un appui dans le développement d'objectifs d'apprentissage et de contenu pour les cours liés aux études de la Cybersécurité.

Le programme de référence de la Cybersécurité se compose de quatres étapes : i) cyberespace et les principes fondamentaux de la cybersécurité, ii) vecteurs de risque, iii) organisations internationales cybersécurité , politiques et normes, et iv) la gestion de la cybersécurité dans le contexte national. Les quatre étapes et les thèmes associés ont été choisis avec soin pour englober la plus grande gamme possible de questions et de thématiques de cybersécurité et fournir le niveau le plus pertinent d'éducation.

Ce document sert de ressource à l'OTAN et ses partenaires cherchant à développer une image plus complète de l'ensemble des questions nationales et internationales, empêtré dans les pratiques de la cybersécurité. Il est présenté dans l'espoir qu'il sera entériné par l'OTAN en temps opportun par le biais de comités appropriés. La prochaine étape consistera à collaborer avec les institutions partenaires d'éducation militaire lors de l'adoption et de la

their adoption and implementation of all or parts of this curriculum, guided by their Individual Partnership Action Plan (IPAP).

Only through dialogue and exchange of ideas can this document enhance the professional development and interoperability of alliance and partner military members. I invite your delegation personnel to distribute this document widely in your respective countries.

If you have any questions regarding this curriculum, please have your delegation personnel contact Mr. Sean Costigan, George C. Marshall European Center for Security Studies at sean.costigan@pfp-consortium.org or Dr. Michael Hennessy, Professor of History and War Studies, Royal Military College of Canada at hennessy-m@rmc.ca

Best wishes,

Le commandant,
Major-général

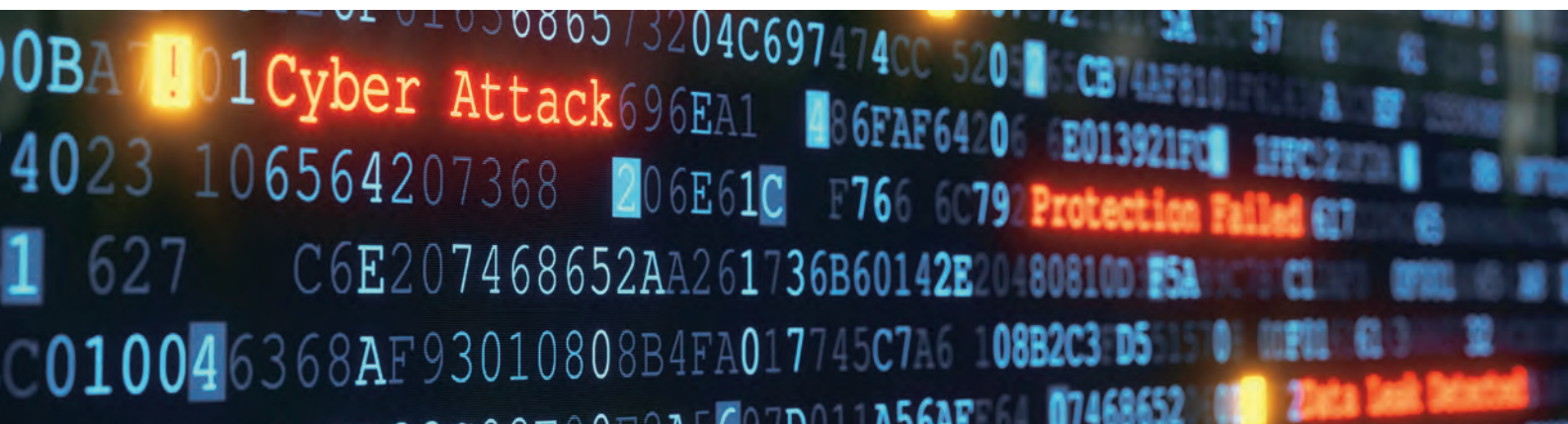
J.G.E. Tremblay
Major-General
Commander

mise en œuvre de ce programme, en tout ou en partie, selon leur plan d'action individuel pour le partenariat (IPAP).

C'est uniquement à travers le dialogue et l'échange d'expériences que ce document contribuera positivement à l'interopérabilité des sous-officiers de l'alliance et des pays partenaires, et à leur éducation militaire. Nous invitons le personnel de votre délégation à le diffuser à grande échelle dans vos pays respectifs.

Pour de plus amples renseignements sur le programme, le personnel de votre délégation peut communiquer avec M. Sean Costigan, Centre George C. Marshall European Center for Security Studies au sean.costigan@pfp-consortium.org ou M. Michael Hennessy, Professeur d'histoire et d'études sur la conduite de la guerre, Collège militaire royal du Canada au hennessy-m@rmc.ca

Nous vous prions d'agréer nos salutations les plus distinguées.



الدفاع الوطني
مكتب القائد
أكاديمية الدفاع الكندية
ص.ب 17000 Station Forces
كنجستون، ON K7K 7B4

4500-1 (SSO EE)

أكتوبر 2016

الأمن السيبراني: منهج مرجعي (RC) عام

السادة الشركاء /أعضاء حلف الناتو الأفاضل،

يسرني أن أشارككم هذه الوثيقة التي تحمل العنوان *الأمن السيبراني: منهج مرجعي عام*، والذي تم إعداده، نيابة عن حلف الناتو واتحاد الشراكة من أجل السلام (PFPC) لأكاديميات الدفاع ومعاهد الدراسات الأمنية، بواسطة فريق متعدد الجنسيات من الأكاديميين والممارسين. وتهدف هذه الوثيقة إلى تزويد حلف الناتو والدول الشريكة بالأهداف التعليمية المتعمقة والدعم المنهجي اللازم للدورات الأكاديمية الخاصة بالأمن السيبراني بوجهٍ عام.

يتألف المنهج المرجعي للأمن السيبراني من أربعة مباحث: 1) الفضاء السيبراني وأساسيات الأمن السيبراني، و2) موجهات المخاطر، و3) منظمات وسياسات ومعايير الأمن السيبراني الدولية، و 4) إدارة الأمن السيبراني في السياق الوطني. وقد أختيرت هذه المباحث الأربعة واللبنات ذات الصلة بعناية بما يغطي المجموعة الأوسع من قضايا وموضوعات الأمن السيبراني، وبما يضمن تقديم المستوى الأكثر ارتباطاً من التعليم.

من الأفضل التعامل مع هذه الوثيقة على أنها تمثل مرجعاً لحلف الناتو والدول الشريكة الذين يتطلعون إلى بناء وتعزيز إدراكهم لمجموعة القضايا، الوطنية والدولية، المتشابكة بشأن ممارسات الأمن السيبراني، وهي مقدمة على أمل أن تحظى بعين الاعتبار من قبل حلف الناتو في الوقت المناسب عبر اللجان المختصة. وتتمثل الخطوة التالية المأمولة في العمل مع مؤسسات التعليم الدفاعي للشركاء من أجل تبني وكذا تنفيذ هذا المنهج بشكل كلي أو جزئي بما يتوافق مع خطة عمل الشراكة الفردية (IPAP) الخاصة بكل منهم.

إذا كانت لديكم أي استفسارات فيما يتعلق بهذا المنهج، فبإمكان أفراد الوفود الاتصال بالسيد/ سين إس كوستيجان، مركز جورج كاتلت مارشال الأوروبي للدراسات الأمنية على sean.costigan@pfp-consortium.org أو الدكتور/ مايكل هينيسي، أستاذ التاريخ ودراسات الحرب، الكلية العسكرية الملكية في كندا على hennessy-m@rme.ea

مع خالص الأمنيات،

القائد،
اللواء

جيه جي إي تريمبلاي

لواء
قائد

NATO UNCLASSIFIED
Releasable to Montenegro

NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
HEADQUARTERS SUPREME ALLIED COMMANDER TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

5000/TSC TTX 0310/TT-161157/Ser: NU0766(INV)

TO: See Distribution

SUBJECT: Endorsement of the PfPC Emerging Security Challenges Working Group Cybersecurity Reference Curriculum as a NATO Educational Reference Document

DATE: 27 September 2016

1. In an effort to satisfy specific partner education and training needs, the Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group (ESCWG) has developed a Cybersecurity Reference Curriculum. The efforts, professionalism and dedication of those who contributed to the development of the curriculum is commendable.

2. The Cybersecurity Reference Curriculum is found compatible with NATO Education and Training on Cyber Defence and I am convinced that it can serve as a reference for partner countries in the design and development of course models and programmes for professional Cybersecurity military education. It will also serve as an enhancement of military interoperability between NATO and its partners and strengthen the collaboration on a responsive education and training system.

3. It is my pleasure to support the PfPC Emerging Security Challenges Working Group through publishing this Cybersecurity Reference Curriculum as a NATO document. I encourage all respective instructional designers of partner countries involved in the development of related learning opportunities to make full use of this guide.

4. Should there be any questions, please contact Mr. Salih Cem Kumsal, NATO Cyber Defence Education and Training Discipline POC at +1 (757) 747-3386, NCN 555-3386, or email cem.kumsal@act.nato.int.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

for
Stefano Vito Salamida
Major General, ITA AF
DCOS Joint Force Trainer

Releasable to Montenegro
NATO UNCLASSIFIED

الناتو غير مصنف
مصرح بنشره إلى الجبل الأسود

منظمة حلف شمال الأطلسي
منظمة حلف شمال الأطلسي
مقر تحويل القيادة العليا للحلفاء
7857 طريق بلاندي, الجناح 100
نورفولك، فيرجينيا، 23551-2490

5000/TSC TTX 0310/TT-161157/Ser :NU

المرسل إليه: انظر التوزيع

الموضوع: المصادقة على المنهج المرجعي للأمن السيبراني لفريق العمل المعني بالتحديات الأمنية الناشئة في اتحاد الشراكة من أجل السلام كوثيقة مرجعية تعليمية لحلف الناتو

التاريخ: سبتمبر 2016

1. سعيًا إلى تلبية احتياجات التعليم والتدريب المحددة للشركاء، قام فريق العمل المعني بتحديات الأمن الناشئة (ESCWG) في اتحاد الشراكة من أجل السلام (PFPC) بوضع منهج مرجعي للأمن السيبراني. ونحن نثني على الجهود والاحترافية والتفاني من جانب الأشخاص الذين ساهموا في وضع هذا المنهج.

2. لقد تأكد توافق المنهج المرجعي للأمن السيبراني مع التعليم والتدريب الذي يقدمه حلف الناتو بشأن الدفاع السيبراني وأنا على يقين من أنه يمكن أن يُستخدم كمرجع للبلدان الشريكة في تصميم ووضع نماذج وبرامج الدورات التدريبية بشأن الأمن السيبراني للعسكريين. ويمكن الاستعانة بالمنهج كذلك كوسيلة لتعزيز التوافق العسكري بين حلف الناتو وشركائه ودفع التعاون في نظام تعليم وتدريب سريع الاستجابة.

3. إنه لمن دواعي سروري أن أدعم فريق العمل المعني بتحديات الأمن الناشئة في اتحاد الشراكة من أجل السلام من خلال نشر هذا المنهج المرجعي كوثيقة خاصة بحلف الناتو. وأشجع جميع واضعي المناهج التعليمية المعنيين من البلدان الشريكة المشاركين في تطوير فرص التعلم ذات الصلة لتحقيق أقصى استفادة من هذا الدليل.

4. إذا كانت لديكم أي استفسارات، يُرجى الاتصال بالسيد/ صالح سيم كومسال، جهة الاتصال المعنية بمنهج التعليم والتدريب للدفاع السيبراني في حلف الناتو على 555-3386 ,NCN 747-3386 (757) 1+، أو عبر البريد الإلكتروني cem.kumsal@act.nato.int.

نيابة عن تحويل القيادة العليا للحلفاء:

ستيفانو فيتو سالاميدا
لواء، ITA AF
مدرب القوات المشتركة في DCOS

مصرح بنشره إلى الجبل الأسود
الناتو غير مصنف

حول هذا المنهج المرجعي

يُعد هذا المستند ثمرة جهود العمل الذي أجراه فريق دولي متعدد الجنسيات من الأكاديميين والباحثين المتطوعين الذين تم انتقاؤهم من 17 دولة مرتبطة بفريق العمل المعني بالتحديات الأمنية الناشئة (ESCWG) التابع لاتحاد الشراكة من أجل السلام (PfPC). وكان هدفنا يتمثل في وضع نهجٍ مرنٍ وشاملٍ بصفة عامة لمسألة الأمن السيبراني.

يهدف هذا المستند إلى تناول مسألة الأمن السيبراني بشكلٍ عام ولكن بعمق كافٍ، وبالتالي سيعمل الخبراء غير الفنيين على عرض صورة أكثر اكتمالاً للمسائل التكنولوجية بينما سيقوم الخبراء المتخصصون في مجال التكنولوجيا بإجراء تقدير أكثر اكتمالاً للآثار المترتبة على سياسة الأمن الوطني والدولي وسياسة الدفاع. ونعرض تحليلاً منطقيًا للموضوع من خلال فئات محددة، ونشير في ثنايا ذلك إلى مستوى المعرفة المقرر أن يكتسبه مختلف فئات الجماهير كما نوضح المراجع الرئيسية المفيدة بحيث يتسنى لكل دولة متبنية أن تُكيّف هذا الإطار مع احتياجاتها وتفاصيل الكتلة الطلابية المستهدفة.

ونعرب عن امتنانا الخاص لاتحاد أكاديميات الدفاع ومعاهد الدراسات الأمنية التابع لمنظمة الشراكة من أجل السلام، تحت قيادة رفائيل بيرل ورؤساء فريق العمل المعني بالتحديات الأمنية الناشئة، دكتور/ ديتليف بوهل (الناتو) ودكتور/ جوستاف لندستروم (مركز جنيف للسياسات الأمنية)، وكذلك للدعم المقدم من برنامج تعليم وتعزيز الدفاع التابع لاتحاد الشراكة من أجل السلام والفرق العاملة المعنية بالتعليم تحت قيادة دكتور/ ألان ستولبرج والسيد/ جين دي أندورين ودكتور/ ديفيد إمليفيونو. وإضافة إلى ذلك، ساعدت قيادة العديد من البلدان الشريكة، بما في ذلك أرمينيا وجورجيا ومولدوفا، على جعل هذا الجهد ممكنًا من خلال دعمها المباشر والملموس. وأخيرًا وليس آخرًا، فإننا ندين لجميع المتطوعين المدرجين باعتبارهم مساهمين بقدرٍ كبيرٍ من الامتنان، فعندما سألنا عمّا إذا كانوا مستعدين للالتزام ببذل جهودٍ لمدة عامين من شأنها أن تأخذهم إلى أعماق التفاصيل فيما يتعلق بتعليم الأمن السيبراني، لم يتخلف أيًا منهم. ونخص بالشكر كل من سكوت نايت ودراينوس كيريجان-كايرو وفيليب لارك وكريس بالاريس ودانيل بيدير باجي وجيجي رومان وناتاليا سبينو وتودور تاجاريف ورونالد تايلور وجوزيف فان، فمن دونهم، لم يكن هذا المستند صدر بهذا الشكل.

سين إس. كوستيجان ومايكل إيه هينيسي، محرران

أولاً. غاية هذا المستند

لقد كانت الوتيرة المتسارعة والدؤوبة للتغيرات والتحديات المتعلقة بالأمن السيبراني[1] هي القوة الدافعة التي حفزت ESCWG لطلب هذا المجهود المتعلق بالمنهج، وذلك وفقًا للتأكيد المتزايد من حلف الناتو على تحسين الوعي بالأمن السيبراني والاستعداد له والمرونة فيه.

تعج عناوين الأخبار بإشارات إلى حوادث الاختراقات التجارية، وانتهاكات البيانات، والاحتيال الإلكتروني، وتعطيل الخدمة الحكومية أو البنية الأساسية الحيوية، وسرقة الملكية الفكرية، وتسريب أسرار الأمن القومي، وإمكانية التدمير السيبراني. وتعد المجالات التي كانت تُعتبر بكل بساطة حربًا إلكترونية، أو الحرب المعلوماتية التي كان يهيمن عليها خبراء أمن الشبكات، بصدد التحول اليوم إلى مجال أوسع نطاقًا بكثير، يُشار إليه باسم "الأمن السيبراني".

نظرًا لكون هذه المسألة إحدى المسائل الناشئة، أي أنها مسألة لا يزال فيها خلاف حول المصطلحات الأساسية، فقد سعى ESCWG إلى إضفاء بعض الوضوح والقواسم المشتركة على هذه المسألة من خلال إنشاء هذا المنهج المرجعي. واعتمدنا التهجئة المتفق عليها cybersecurity (الأمن السيبراني) ككلمة واحدة في المستند ككل واستخدمنا مصطلح cyber (سيبراني) كصفة أو لتوضيح محور التركيز.

عند صياغة هذا المستند، تمكنا من استطلاع آراء جميع المؤسسات الأعضاء في اتحاد الشراكة من أجل السلام وكليات الدفاع الأخرى وراجعنا برامج التدريب العسكري للبلدان الشريكة في حلف الناتو واتحاد الشراكة من أجل السلام من أجل تحديد ما يجري تعليمه. وسعينا إلى رصد الفجوات وتحديد النهج المشتركة التي تتجاوز الحواجز التقليدية للهياكل الحكومية والعسكرية. وكانت أكبر فجوة رصدناها تتمثل في عدم وجود فهم كافٍ عن تكنولوجيا الأمن السيبراني وعن ممارسات التخفيف من حدة التهديدات والمخاطر بين قادة سياسة الأمن القومي والدفاع. كما رُصدَت فجوة مماثلة فيما يتعلق بفهم أطر السياسة الوطنية بين الخبراء الفنيين.

يقدم هذا المنهج المرجعي نقطة انطلاق راسخة يمكن من خلالها تطوير أو تحسين تدريس مسائل الأمن السيبراني لكبار الضباط وموظفي الخدمة المدنية والفئة المتوسطة من الموظفين العسكريين والمدنيين. وكما هو الحال بالنسبة للمناهج المرجعية الأخرى التي وضعها اتحاد الشراكة من أجل السلام، يُعد الهدف من هذا المستند مسألة تحفظية. فهو لا يقدم مخططًا رئيسيًا واحدًا للدورة التدريبية بحيث يتبعه الجميع. ولا يعتبر شاملاً من حيث المحتوى أو التفاصيل أو النُهُج المتعلقة بهذا الموضوع. ومع ذلك، فإننا نرى أنه يقدم نهجًا استكشافيًا مفيدًا لمختلف المجالات، حيث يضم مقدمة شاملة إلى مجموعة من المسائل المتشابكة فيما يتعلق بممارسات الأمن السيبراني. وسيجد أولئك الذين يحظون بخلفية فنية بسيطة مقدمة على مستوى معقول من التعقيد وسيكتسبون إدراكًا أفضل لأماكن العمق الفني ولماذا يُعد مطلوبًا. أما الذين يتحلون بالخبرة الفنية فقد يجدوا المادة عبارة عن لمحة عامة مفيدة بشأن المجالات التي هم على دراية بها ومقدمة إلى مسائل الممارسات والسياسات الدولية والوطنية والقانونية الأوسع نطاقًا. ونحن على ثقة بأن كل شخص سيجد في هذا المستند ما يمثل قيمة له.

ينبغي لمن يرغب في استخدام هذا المستند باعتباره نهجًا للأمن السيبراني تحليل ممارساتهم ومتطلباتهم الوطنية المحددة والفريدة لتكييفها مع احتياجاتهم. ويقدم هذا المستند إرشادات لرصد المجالات التي تستدعي الاهتمام ويوصي بالمصادر والنُهُج الرئيسية.

ثانيًا. الأمن السيبراني والمخاطر

غالبًا ما تُستمد الإجراءات الأمنية من خلال إجراءات التهديدات والمخاطر. وسيتم استكشاف كلا المفهومين بشيءٍ من الاستفاضة. ومع ذلك، وبعبارات بسيطة، يمتلئ الفضاء السيبراني بالتهديدات، ولكن يلزم أن تسترشد الإجراءات المتبعة للتخفيف من التهديدات بإجراءات المخاطر. وتُعرِّف المنظمة الدولية لتوحيد المقاييس (الأيزو) المخاطر على أنها "تأثير عدم اليقين على الأهداف" (قد يكون التأثير انحرافًا إيجابيًا أو سلبيًا عمّا هو متوقع). وبما أن الإجراءات المتخذة لتأمين شيء ما يجب أن تكون متناسبة مع قيمة ما يجري تأمينه، يوجد مستويات مختلفة من الأمن اعتمادًا على مقاييس القيمة والمخاطر. ومن ثمّ، فإن تأمين الفضاء السيبراني ينطوي على عدد من الاعتبارات للتخفيف من المخاطر والتهديدات فيما يتم التشجيع على إمكانية الوصول والانفتاح عبر مختلف أنواع الشبكات والأجهزة المترابطة. ويُعد تحقيق التوازن الضروري بين إمكانية الوصول وقابلية الاستخدام والأمن بمثابة التحدي الرئيسي. ويستكشف هذا المنهج النُهُج المتبعة لتقييم التهديدات والمخاطر ورصدها والتخفيف منها، على المستوى الفني وعلى مستوى أي وكالة أو سياسة حكومية، وذلك من خلال استكشاف أفضل الممارسات الموصى بها وبالمقارنة مع الممارسات المنشورة لدول أو منظمات معينة.

ثالثًا. هيكل هذا المنهج

حسبما ذُكر في مستندات المناهج المرجعية السابقة، فإن المنهج عبارة عن برنامج تعليمي محدد يصف، أو ربما مجموعة من الدورات التدريبية تصف، بشكلٍ جماعي مواد التدريس والتعليم والتقييم والطرق المناسبة لبرنامج دراسة معين. وبالتالي، فإن المنهج الناتج يمثل خارطة طريق لما قد يدرسه المتعلمون. وشأنها في ذلك شأن أي خارطة إذ يتم إعدادها بمستوى من التلخيص وقد لا تُظهِر جميع الطرق أو التفاصيل؛ ومع ذلك، فإنها تحدد ما يتعين على المتعلم دراسته.

عادة ما يُسفر أي منهج عام عن وجود هيكلٍ متداخلٍ يحتوي على الكثير من الموضوعات الفرعية والمسائل المتداخلة ضمن إطار واسع النطاق[2]. وترتبط هذه الأجزاء المتداخلة الكثيرة بالأهداف الأوسع نطاقًا للبرنامج الدراسي. ونظرًا لترابط الموضوعات والمسائل الواردة في منهجنا المرجعي للأمن السيبراني، لم نوصي بتقسيم المنهج إلى ثلاث مراحل تطويرية للضباط. وسوف نتطرق إلى هذه النقطة بمزيدٍ من التفصيل أدناه، عندما نتناول طريقة استخدام هذا المنهج.

[1] في خطوط عريضة، نتبع التعريف الذي وضعته وزارة الأمن الداخلي الأمريكية: "الأمن السيبراني هو النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها من و/أو الدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال".

تمشيًا مع هذه الهياكل المعتمدة في المناهج المرجعية الأخرى لاتحاد الشراكة من أجل السلام، يُعرَض هذا المستند من خلال أربعة مباحث، ينقسم كل منها إلى لبنات والتي يمكن تقسيمها أيضًا بشكل طبيعي إلى أقسام فرعية. وهذه الأقسام عبارة عن مباحث (م) ولبنات (ل) محددة، على النحو الموضح في جدول المحتويات (انظر ما يلي)

فيما يلي المباحث الأربعة لهذا المنهج:

المبحث 1: الفضاء السيبراني وأساسيات الأمن السيبراني

المبحث 2: متجهات المخاطر

المبحث 3: المنظمات والسياسات والمعايير الدولية للأمن السيبراني

المبحث 4: إدارة الأمن السيبراني في السياق الوطني

يتم وصف كل مبحث بالتفصيل في موضع ما من هذا المستند، ولكن يتناول كل منها مجالات ومسائل محددة واسعة رئيسية.

يندرج تحت كل مبحث عدة موضوعات متمايزة، ويتم استكشاف كل منها في لبنة أساسية، والتي يمكن تقسيمها هي الأخرى إلى وحدات تعليمية متمايزة، مثل المحاضرات أو العروض التقديمية أو العروض الإيضاحية أو الجولات أو التدريبات القائمة على السيناريو أو الأنشطة المماثلة. وبالنسبة لأغلب الأجزاء، نظرًا لأن هذا المنهج المرجعي سيتطلب تكييفًا محليًا، لم نقترح وحدات ومحاضرات متمايزة كون ذلك المستوى من التفصيل يعتمد على الحاجة الفردية. وتوفر مجموعة من اللبنات المختلفة بشكل جماعي معلومات عن كل مبحث. وتشير إلى أهداف ونتائج التعلم الذي من المقرر تحقيقها؛ والتي ترتبط بدورها بأهداف المبحث الأوسع نطاقًا.

ويمكن تقديم اللبنات جزءًا واحدًا أو مجتمعة أو مقسمة تقسيمًا فرعيًا إلى وحدات منفصلة. ولا يشير هذا المخطط إلى الطريقة التي سيتم التعامل بها مع كل لبنة من اللبنات، ولكن قد يتخذ عرض الموضوعات، في كلٍ من اللبنات أو الوحدات، شكل المحاضرات أو العروض التقديمية أو المهام التشاركية أو الجولات أو العروض الإيضاحية أو المساهمة في التدريبات القائمة على السيناريوهات.

رابعًا. استخدام هذا المنهج

يقدم هذا المنهج عددًا من الافتراضات الضمنية.

أولاً، تعتبر جميع المواد المحددة في هذا المستند غير سرية، إذ قد يرغب من يتبنى هذا الإطار الاطلاع على مواد سرية إذا اقتضت الحاجة ذلك.

ثانيًا، من المفترض أن تعمل المؤسسات التي تتبنى هذا المنهج المرجعي على تخصيص الوقت والموارد اللازمة إلى جانب فريق من الخبراء لتحديد السياسات والإجراءات الوطنية على مستوى التفصيل المطلوب للجمهور المستهدف. وقد تكون المعرفة الروتينية بالمسائل الفنية العابرة من الضرورة بمكان، ولكن الهدف هنا يكمن في التوصل إلى فهمٍ أوسع نطاقًا لتحديات الأمن السيبراني عبر مجموعة من القضايا.

عند تكييف هذا المنهج للاستخدام المحلي، قد يكون من الممكن تنفيذه بطريقة تدريجية ومتسلسلة عبر المراحل المهنية المختلفة، ولكن ينبغي اتباع المخطط الشامل على جميع المستويات. ومع ذلك، يُعتبر الهدف الرئيسي لهذا المنهج المرجعي هدفًا عملياتياً استراتيجيًا أكثر منه تكتيكيًا. وعند وضع دورات تدريبية محددة من هذا المنهج المرجعي، من المقترح أن يضع مُعِدو الدورات التدريبية المحلية في اعتبارهم الوقت والموارد المتاحة والمستوى التعليمي للطلاب والوظائف التي يُتوقع، أو سيُتوقع، من هؤلاء الطلاب تنفيذها بصرف النظر عن رتبهم.

ثالثًا، لا توجد لبنة بشأن الحرب السيبرانية أو النزاع السيبراني أو وسائل التواصل الاجتماعي على أنها قناة للدعاية أو التضليل المعلوماتي. ويتعين على لجنة التصميم المختارة ترك هذه المسائل التي هي محور التركيز للتطوير اللاحق.

في النهاية، نؤكد من جديد على أن هذا المنهج المرجعي ليس هيكلًا واحدًا أو مقترحًا للدورات التدريبية، بل من الأفضل استخدام المستند كمرجع رئيسي يوفر مخططًا عامًا للمسائل والموضوعات عبر مجموعة من القضايا المتعلقة بالأمن السيبراني. وقد يُستخدم المستند بمثابة دليل للموظفين الفنيين لمعرفة أين ينصب تركيزهم الخاص ضمن هذه المجموعة الواسعة من المسائل. وبالمثل، قد يعمل المستند كدليل لدورات تمهيدية بالنسبة لكبار صانعي السياسات الأمنية الوطنية بحيث يتمكنوا من تقدير سياساتهم الوطنية وتعيين موضعها بشكلٍ أفضل إلى جانب المعرفة بالسياق الفني. وستكمن العناصر الثلاثة التي تُشكل أكبر قدر من الاهتمام عند استمداد أي دورة تدريبية واحدة من هذا المخطط في الهدف أو الغرض من هذه الدورة التدريبية؛ والطلاب المقترحون، وعلى وجه الخصوص مستوى معرفتهم الفنية وطبيعة عملهم؛ والوقت المتاح. ويتعين أن ترشد هذه العناصر الثلاثة عن مستوى التفصيل الفني الذي تمت مناقشته وطبيعة التدريبات التعليمية (المحاضرات والأمثلة والرحلات الميدانية والعروض الإيضاحية وألعاب الحروب وما إلى ذلك).

[2] انظر الوثائق السابقة الخاصة بالمناهج المرجعية للوقوف على الأصول واستخدام هذه البنية.

خامسًا. مصادر إضافية

يتوسع حجم كل من المنشورات العامة والفنية المتعلقة بالأمن السيبراني بشكل سريع. ويتم تشجيع مصممي الدورات التدريبية على إصدار قائمة بالمصادر الرئيسية الخاصة بهم؛ ورغم ذلك، حرصنا على إدراج مجموعة واسعة من المصادر التي تعكس الكثير من وجهات النظر الوطنية والدولية المختلفة ذات الصلة بالمباحث الموضوعة لهذا المنهج المرجعي، وقمنا، حيثما أمكن ذلك، بتوفير روابط لموارد الإنترنت النشطة. وإضافة إلى العديد من المصادر المدرجة عبر هذا المستند، يوفر الموقع الإلكتروني لحلف الناتو الكثير من المقالات والمعلومات الحالية بشأن المسائل التي تحظى باهتمام مجتمع الناتو. وتتضمن المصادر المدرجة على www.natolibguides.info/cybersecurity ما يلي:

- مقالات/فيديوهات لمجلة ناتو ريفيو بشأن الهجمات السيبرانية إلى جانب طبعة يونيو 2013 بشأن السيبرانية—الجيدة والسيئة والخالية من الأخطاء (بما في ذلك أشرطة فيديو، وصور، وجدول زمني، ورسوم معلوماتية، وما إلى ذلك).
- مقال القدرات السيبرانية لحلف الناتو: الأمس واليوم وغدًا بقلم هيلي وفان بوكهوفن (فبراير 2012) يقدم لمحة عامة جيدة بشأن القدرات السيبرانية لحلف الناتو.
- تقرير حول الحرب السيبرانية (2012) الصادر عن فرد سشرير يتضمن مسرد مصطلحات وقائمة مراجع مختارة ومواضيعية جيدة جدًا (مستندات رسمية، حلف الناتو، منظمة التعاون الاقتصادي والتنمية، على حسب البلد، حرب معلوماتية، أمن سيبراني، كتب).
- الطبعة الخاصة السيبرانية *للدراسات الاستراتيجية ربع السنوية* 6، رقم 3 (خريف 2012).
- الأمن السيبراني: المخاطر المشتركة، والمسؤوليات المشتركة طبعة *I/S: مجلة القانون والسياسة لمجتمع المعلومات* 8، رقم 2 (2012).
- مقال الفضاء السيبراني ليس ميدانًا للحرب (2012) بقلم مارتن لبيكي.
- *دليل تالين بشأن القانون الدولي المُطبّق على الحرب السيبرانية* (2012).
- دليل يتألف من 300 صفحة تمت كتابته بواسطة مجموعة تضم 20 باحث بناءً على دعوة من مركز التميز للدفاع السيبراني التعاوني التابع للناتو في تالين، إستونيا.
- متابعة مشروع "تالين 2.0" المتعلق *بدليل تالين بشأن القانون الدولي المُطبّق على الحرب السيبرانية* والمصمم لتوسيع نطاق *دليل تالين* الأصلي. وسينتج عن تالين 2.0 الطبعة الثانية من *دليل تالين* وسيتم نشرها بواسطة مطبعة جامعة كامبريدج في 2016 (المصدر: مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو).
- دليل إطار عمل الأمن السيبراني الوطني (2012) بواسطة مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو.
- الدورة التدريبية للتعليم الإلكتروني المنظمة بواسطة مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو بشأن التوعية بالدفاع السيبراني (متوفرة مجانًا ولكن تتطلب التسجيل).
- قائمة مراجع عن النزاع السيبراني بواسطة مكتبة جايكوب بيرنز القانونية، كلية الحقوق بجامعة جورج واشنطن.
- جلسة الإحاطة الدفاع السيبراني في الاتحاد الأوروبي: هل تأخذ الاستعدادات اللازمة للحرب السيبرانية؟ (31 أكتوبر 2014) بواسطة دائرة البحوث البرلمانية الأوروبية.
- مقالة تالين رقم 8، المنشورة في إبريل 2015: "دور العمليات السيبرانية الهجومية في الدفاع الجماعي لحلف الناتو".

تشمل بعض الموارد الأخرى المفيدة ما يلي:

- معهد استمرارية الأعمال، *المبادئ التوجيهية للممارسات الجيدة 2013، الطبعة العالمية: دليل الممارسات الجيدة العالمية في مجال استمرارية الأعمال* (إنجلترا، 2013). http://www.thebci.org/index.php/resources/the-good-practice-guidelines
- جوستاف لندستروم "مواجهة تحدي الأمن السيبراني،" *أبحاث مركز جنيف للسياسات الأمنية - السلسلة البحثية* رقم 7 (يونيو 2012).
- مجلس المعايير الدولية لمراجعة الحسابات والضمان، المعيار الدولي لعمليات التأكيد رقم 3402 بعنوان تقارير التأكيد حول الضوابط في المؤسسات الخدمية.
- أيزو/آي إي سي 15408: المعايير المشتركة لتقييم أمن تكنولوجيا المعلومات، الإصدار 3.1، النسخة المنقحة 4.
- فريق الدراسة ITU-D 1، التقرير النهائي، *السؤال 1/1-22: تأمين شبكات المعلومات والاتصالات: الممارسات الفضلى لتنمية ثقافة الأمن السيبراني*، فترة الدراسة الخامسة 2014. انظر http://www.itu.int/ITU-D/study_groups أو http://www.itu.int/pub/D-STG-SG01.22.1-2014
- جيه لويس وكيه تيملين، "الأمن السيبراني والحرب السيبرانية: التقييم الأوليّ للعقيدة الوطنية والتنظيم،" مركز الدراسات الاستراتيجية والدولية، واشنطن العاصمة، 2011.
- المبادرة الوطنية لوظائف الأمن السيبراني ودراساته http://niccs.us-cert.gov/glossary

- نيل روبنسون ولوك غريبون وفيرونيكا هورفاث وكيت روبرتسون، تحديد الخصائص التي تهدد الأمن السيبراني: تحليل مقارن سريع (سانتا مونيكا، كاليفورنيا: مؤسسة راند، 2013)، تم إعداده لمركز دراسات التهديدات غير المتماثلة (CATS)، كلية الدفاع الوطني السويدية، ستوكهولم.
- المنشور الخاص للمعهد الوطني للمعايير والتقنية 800-82: دليل أمن نظم الرقابة الصناعية، يونيو 2011.
- رون ديبرت ورفال روهوسينسكي، *الظلال في السحابة: التحقيق في التجسس السيبراني 2.0*، تقرير مشترك صادر عن كل من راصد الحرب المعلوماتية، ومؤسسة شادوسيرفر JR-03-2010، 6 إبريل 2010. http://shadows-in-the-cloud.net
- وزارة الدفاع الأمريكية، *الاستراتيجية السيبرانية التي تنتهجها وزارة الدفاع*، إبريل 2015، واشنطن العاصمة.
- المنتدى الاقتصادي العالمي، *الشراكة من أجل المرونة السيبرانية: نحو قياس التهديدات السيبرانية كميًا*. بند جدول أعمال الصناعة (بالتعاون مع ديلويت)، المرجع 301214، لعام 2015.

جدول المحتويات

المبحث 1: الفضاء السيبراني وأساسيات الأمن السيبراني

الهدف

يكمن الهدف من هذا المبحث في وضع الأسس المعرفية لجميع التعليمات التالية عن طريق تحديد المكونات الهيكلية للفضاء السيبراني[3]، وبنيته الأساسية فضلاً عن أساسيات الأمن السيبراني. ويمثل رصد المخاطر وإدارتها التحدي المشترك الرئيسي الذي يربط المباحث والموضوعات المختلفة التي يتم تناولها في هذا المنهج.

الوصف

تتطلب تحديات الأمن السيبراني والفضاء السيبراني أكثر من مجرد إعادة تسمية المنظمات الحكومية المسؤولة عن أمن تكنولوجيا المعلومات أو أمن الاتصالات. ويتسبب انتشار النظم الحاسوبية الحديثة والقدرة على الاتصال والتفاعل من خلال مجموعة متنوعة من الوسائل، بدءًا من الأجهزة الجوالة حتى أجهزة الحاسوب التي يمكن ارتداؤها، في عرض عدد من مواطن الضعف الكامنة ومتجهات هجمات محتملة على كل من الجهات الفاعلة من الدول ومن غير الدول. وقد يترتب على استغلال مواطن الضعف آثار أمنية وطنية واسعة النطاق من خلال أعمال التجسس المتعمدة، أو تدهور مرافق القيادة والسيطرة، أو سرقة الملكية الفكرية والمعلومات الشخصية الحساسة، أو تعطل الخدمات والبنية التحتية الحيوية، أو الأضرار الاقتصادية والصناعية.

من خلال اللبنات الخمس لهذا المبحث، سيدرس الطلاب الهيكل الأساسي للفضاء السيبراني والنهج القائم على المخاطر للأمن السيبراني. T1-B1، الأمن السيبراني والفضاء السيبراني - مقدمة، يتم فيها استكشاف أصول الفضاء السيبراني وشكله العام ويعرّف مفهوم الأمن السيبراني. T1-B2، أمن ومخاطر المعلومات، تتناول أساسيات المنهجية الخاصة بتحليل مخاطر أمن المعلومات وتستكشف نهجًا قائمًا على التهديدات من أجل التقييم. T1-B3، هياكل الفضاء السيبراني: العمود الفقري للإنترنت والبنى التحتية الوطنية؛ تستكشف تشغيل وبنية الإنترنت العالمي وحوكمته. T1-B4، البروتوكولات والمنصات، تُعرّف بمعايير تكنولوجيا الشبكات وتكنولوجيا المعلومات من أجل استكشاف أساسيات تصميم الشبكة والعمليات التشغيلية الخاصة بها. وأخيرًا، T1-B5، البنية الأمنية والإدارة الأمنية، تقدم أساسيات البنية الأمنية استنادًا إلى تحليل التهديدات والمخاطر وقابلية التضرر. يجب أن يعمل تحليل المخاطر على توجيه وإرشاد تطوير البنى السيبرانية والاستراتيجية المتبعة في الحد من مواطن الضعف والتهديدات المعروفة وغير المعروفة على المستويين التنظيمي والوطني. وبناءً على ذلك، يتم تعريف الطلاب بالمنهجية الأساسية الخاصة بتحليل المخاطر السيبرانية والإدارة المستخدمة في تطوير بنية الأنظمة والاستراتيجيات الرامية إلى التخفيف من حدة هذه المخاطر.

نتائج التعلم

سيتمكن الطلاب من

- وصف ما يعنيه الفضاء السيبراني والأمن السيبراني؛
- توضيح بعض مواطن الضعف الأساسية للدول المتقدمة فيما يتعلق بالتهديدات السيبرانية، مثل جمع المعلومات الاقتصادية لتحقيق مكاسب وطنية أو تنميط الأفراد والمشاريع، أو سرقة البيانات، أو إفساد قواعد البيانات أو الاستيلاء على أنظمة التحكم الصناعية أو أنظمة الرقابة على العمليات (مثل التحكم الإشرافي والاستحواذ على البيانات)؛
- وصف الطوبولوجيا الأساسية للفضاء السيبراني، بما في ذلك هياكله المادية وكيفية إدارته من خلال البروتوكولات والإجراءات؛
- وتوضيح الاعتبارات الأساسية للبنية الأمنية المناسبة.

مراجع مقترحة

لوكاس جودون، "هيكل الإنترنت." http://internethistory.eu/index.php/structure-of-the-internet/

ديف كليمنتي، "الأمن السيبراني والترابط العالمي: ما الذي يُعد حيويًا؟"، بحث صادر عن تشاتام هاوس، *المعهد الملكي للشؤون الدولية*، الرقم الدولي المعياري للكتاب 978-1-86203-278-1، فبراير 2013.

مؤسسة أمن الاتصالات الكندية (CSEC)، *منهجية تقييم التهديدات والمخاطر المتسقة (TRA)*، 23 أكتوبر 2007.

دي بي كورنيش، *الأمن السيبراني والهجمات السيبرانية ذات الدوافع السياسية والاجتماعية والدينية*، الدائرة العامة للبرلمان الأوروبي لسياسات الاتحاد الخارجية، الدائرة ب - إدارة السياسة، فبراير 2009، EP/EXPO/B/AFET/FWC/2006-10/Lot4/15 .PE 406.997

http://www.europarl.europa.eu/ meetdocs/2004_2009/documents/dv/sede090209 wsstudy_/SEDE090209wsstudy_en.pdf

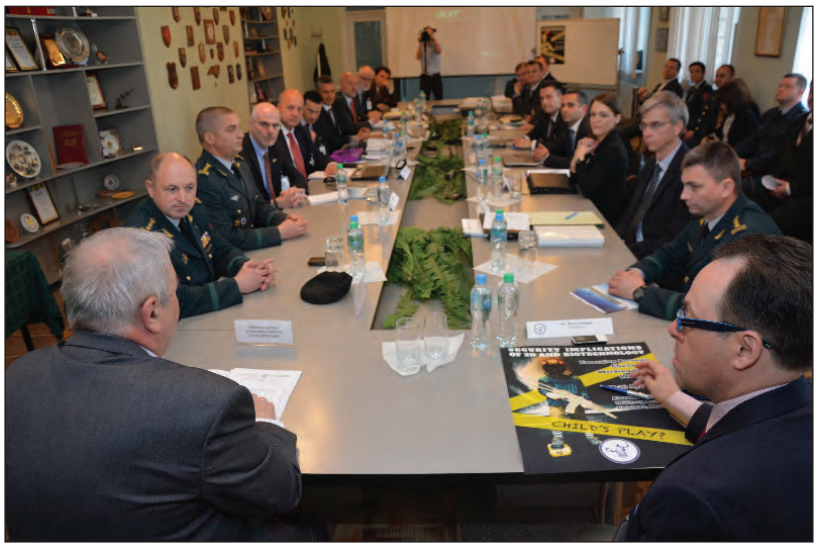
كريس هول وريتشارد كلايتون وروس أندرسون وإيفانجلوس أوزونيس، *انتر إكس: مرونة النظام البيئي للربط البيني للإنترنت - تقرير كامل*، الوكالة الأوروبية لأمن الشبكات والمعلومات، إبريل 2011. http://www.enisa.europa.eu

[3] تم تعريف الفضاء السيبراني في هذه الوثيقة باعتباره العالم الإلكتروني الذي أنشأته شبكات تكنولوجيا المعلومات المترابطة والمعلومات المتعلقة بهذه الشبكات. مستمد من استراتيجية الأمن السيبراني في كندا، 2014.

آر تيهان، *الأمن السيبراني: تقارير وموارد معتمدة، حسب الموضوع*، دائرة البحوث التابعة للكونجرس، تقرير الدائرة R42507 7-7500، بتاريخ 15 إبريل 2015. http://www.crs.gov

البيت الأبيض، *مراجعة سياسة الفضاء السيبراني*، 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

إيثان زوكرمان وأندريو ماكلولين "مقدمة إلى هندسة الإنترنت والمؤسسات." https://cyber.law.harvard.edu/digitaldemocracy/internet architecture.html



ورشة عمل للفريق المعني بكتابة المنهج المرجعي للأمن السيبراني في كيشيناو.

اللبنة T1-B1: الأمن السيبراني والفضاء السيبراني— مقدمة

الوصف

يتألف الفضاء السيبراني من نظم حاسوبية مختلفة متصلة بالشبكة ونظم اتصالات سلكية ولاسلكية متكاملة. وأصبح الفضاء السيبراني أحد سمات المجتمع الحديث، وهو ما يعمل على تعزيز وتمكين الاتصال السريع، وأنظمة القيادة والتحكم الموزعة، وتخزين ونقل البيانات بكميات هائلة ومجموعة من الأنظمة الموزعة بشكلٍ كبير. وسارت كل هذه الأشياء الآن من المسائل المسلم بها لدى المجتمع وأصبحت عاملاً أساسيًا للأعمال التجارية، وحياتنا اليومية وتقديم الخدمات. ويمكن رؤية انتشار الفضاء السيبراني في كل مكان والاعتماد عليه حتى في الميادين العسكرية، حيث تعتمد الاتصالات، والقيادة والتحكم، والاستخبارات والعناصر الهجومية الدقيقة جميعها على العديد من "النظم السيبرانية" ونظم الاتصالات ذات الصلة. وقد أدى انتشار هذه الأنظمة المترابطة إلقاء قدر من التبعية والضعف على الأفراد والصناعات والحكومات والتي يصعب التنبؤ بها أو إدارتها أو تخفيفها أو منعها. وترى بعض الأمم هذه التبعيات الضعيفة على أنها مصدر قلق ناشئ فيما يتعلق بالأمن القومي أو الدفاع الوطني، وكلفت العناصر الحالية لقوات الأمن التابعة لها بالاستجابة لها، في حين أنشأت أمم أخرى منظمات جديدة بالكامل منوطة بإدارة سياسات الأمن السيبراني الوطني أو تنسيقها. ونشأ الأمن السيبراني كمسألة شاملة هامة والتي تتطلب استجابات من الأفراد والشركات الخاصة والمنظمات غير الحكومية و"الحكومة برمتها" وكذلك مجموعة من الوكالات والهيئات الدولية.

تهدف هذه اللبنة إلى تعريف الطلاب بتكنولوجيات الاتصالات المعلوماتية (ICTs) في هذا المجال، والكشف عن انتشارها واعتمادنا الملازم على هذه الأنظمة. ويكمن الهدف في وضع تقديرًا اجتماعيًا وفنيًا وثقافيًا واسعًا لتكنولوجيا المعلومات الحديثة، وأدوارها المتعددة وأثر بيئة الفضاء السيبراني الافتراضية على الحياة العصرية والقدرة على إدارة شؤون الدولة والاتصالات العالمية. وتقدم هذه اللبنة دليلاً تمهيديًا لطلاب الأمن الوطني من أجل اكتساب فهمًا راسخًا عن الطوبولوجيا ومفاهيم الفضاء السيبراني والأمن السيبراني.

ومن أجل وضوح التعريفات، اعتمدنا على تعريف المعهد الوطني للمعايير والتقنية الأمريكي (NIST) للفضاء السيبراني، وهو "الشبكة المترابطة من البنى التحتية لتكنولوجيا المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات السلكية واللاسلكية والنظم الحاسوبية والمعالجات المدمجة وأجهزة التحكم...." أما الأمن السيبراني فقد تم تعريفه على أنه "النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يتم بموجبها حماية نظم المعلومات والاتصالات والمعلومات الواردة فيها من و/أو الدفاع عنها ضد الضرر أو الاستخدام أو التعديل غير المصرح به أو الاستغلال" ويُشكل هذا التعريف الأساسي ما قمنا بإدراجه في جميع أجزاء هذا المستند.

نتائج التعلم

سيتمكن الطالب من أن يُبدى فهمًا على مستوى مناسب لما يلي

- أهمية تكنولوجيا المعلومات والاتصالات وكيفية تغييرها لنسيج المجتمعات الحديثة؛
- الفروق الدقيقة للأمن السيبراني في مختلف السياقات الوطنية والثقافية، مع التشديد على نهجها وسياساتها الوطنية؛
- التحديات الرئيسية المتعلقة بتكنولوجيا الاتصالات المعلوماتية، ومقدمي الخدمات الرئيسيين، ومصادر السياسة الرئيسية، وأصحاب المصلحة الرئيسيين، والمسؤوليات القانونية والوظيفية؛
- الآثار السلبية والإيجابية للفضاء السيبراني على المجتمع؛
- توعية واسعة النطاق بالتهديدات والمخاطر المتعلقة بتشغيل الفضاء السيبراني بكفاءة وأمان؛
- كيفية تنظيم الإنترنت وتشغيله والحفاظ عليه من خلال شبكة من المؤسسات العامة والخاصة وغير الربحية؛
- السياقات الوطنية الفريدة في صنع السياسات والحوكمة المحلية للإنترنت؛
- دور المعايير والبروتوكولات في تصميم الإنترنت؛
- والضرورات العسكرية والسياسية المرتبطة بالفضاء السيبراني وحوكمة الإنترنت.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

سيعتمد عمق الاستكشاف على الجمهور والوقت المتاح؛ غير أنه يمكن تناول كل من الوحدات المتعلقة بالبنية التحتية الوطنية للإنترنت والاتصالات السلكية واللاسلكية، ومقدمي الخدمات الرئيسيين، والتقسيم الحالي للمسؤوليات بشأن السياسات والممارسات الأمنية واسعة النطاق داخل الحكومة الوطنية ومنظمة الدفاع بشكلٍ منفصل من أجل الوضوح والتأكيد.

طريقة/تقييم التعلم

قد تشمل طريقة التدريس محاضرات يُلقيها خبراء متخصصين (SMEs)، وحلقات دراسية، وعروض إيضاحية، وتدريبات وعمليات محاكاة للفصول الدراسية.

ينبغي تقييم الطلاب من خلال مشاركتهم ومناقشتهم في تدريبات القراءة والمناقشات المشتركة، يليه اختبار معرفة بالدورة التدريبية.

المراجع

جي وانج، أيه زاكري كيسل، "مقدمة إلى أمن الشبكات: النظرية والممارسة العملية"، سنغافورة: وايلي، 2015. الرقم الدولي المعياري للكتاب 9781118939505. رقم المُعرِّف الفريد: BLL01017585410.

الوكالة الأوروبية لأمن الشبكات والمعلومات، "الأمن السيبراني كأحد عوامل التمكين الاقتصادي" هيراكليون، كريت، اليونان. مارس 2016. متوفر على: www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler (تم الاسترجاع في 14 يوليو 2016).

المكتب الفيدرالي لأمن المعلومات (BSI)، "حالة أمن تكنولوجيا المعلومات في ألمانيا، 2015". متوفر على: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2

إف لانتنهامر، أيه شولتز، أيه زايدل، أيه شتبلز، أيه، "الدفاع السيبراني والتوعية بأمن تكنولوجيا المعلومات"، في *Europäische Sicherheit & Technik: ES&T*. رقم 8، لعام 2012. الرقم التسلسلي المعياري الدولي للمجلة: 2193-746X. رقم المُعرِّف الفريد: ETOCRN316565061.

سيعمل الخبراء المتخصصون مع البلد المضيف لتحديد القراءات الأساسية الملائمة استنادًا إلى تركيز الدورة التدريبية المخطط لها والمتطلبات الزمنية.

قد تتضمن القراءات المختارة ما يلي:

"المدخلات المغلوطة تؤدي إلى نتائج خاطئة (جيجو) (1969) سجل الحاسوب - نظرة بريطانية" على يوتيوب، تم الوصول إليه في 25 إبريل 2015. http://youtu.be/R2ocgaq6d5s

جيمس آر. بينيجر، *ثورة التحكم: الأصول التكنولوجية والاقتصادية للمجتمع المعلوماتي* (كامبريدج، ماساتشوستس: مطبعة جامعة هارفارد)، 1986.

فينتون جي سيرف (الرئيس) وآخرون، *دور آيكان في النظام البيئي لحوكمة الإنترنت*، تقرير خاص بفريق استراتيجية آيكان، 20 فبراير 2014.

بول إي سيروزي، *تاريخ الحوسبة الحديثة*، الطبعة الثانية. (كامبريدج، ماساتشوستس: مطبعة معهد ماساتشوستس للتكنولوجيا)، 2003.

بول هوفمان، محرر، "طاو فرقة العمل المعنية بهندسة الإنترنت: دليل المبتدئين لفرقة العمل المعنية بهندسة الإنترنت" 2015.

باري لينر وفينتون سيرف وديفيد دي كلارك وروبرت إي كاهن وليونارد كلينروك ودانيال سي لينش وجون بوستيل ولاري جي روبرتس وستيفن وولف، "تاريخ موجز للإنترنت"، تم الوصول إليه في 25 أبريل 2015. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

ماري-لوري ريان ولوري إميرسون وبنجامين جيه روبرتسون، محررون، *دليل جونز هوبكنز للوسائط الرقمية* (بالتيمور: مطبعة جامعة جونز هوبكنز)، 2014.

لانس سترات، "أنواع الفضاء السيبراني: مشاكل في التعريف والتحديد،" *ويسترن جورنال كوميونيكيشن* 63، رقم 3 (1999): 382–412. معرف الكائن الرقمي: 10.1080/10570319909374648

البيت الأبيض، *الاستراتيجية الدولية لازدهار الفضاء السيبراني والأمن والانفتاح في عالم مترابط شبكيًا* (واشنطن العاصمة: المكتب التنفيذي لرئيس الولايات المتحدة، مجلس الأمن القومي)، 2011.

T1-B2: مخاطر وأمن المعلومات

الوصف

بصفة عامة، يتميز أمن المعلومات (IS) بالأهمية عبر فئات عريضة من المعلومات - المعلومات الخاصة والعامة والحساسة والسرية وغيرها - والتي تتطلب ممارسات وبروتوكولات للإدارة سواءً في شكلها الرقمي أو غيره. ففي المجال السيبراني، تجد المتسللين والمجرمين وأجهزة الاستخبارات الأجنبية هم المعنيون باستغلال مواطن الضعف في نظام أمن المعلومات. تُعرّف هذه اللبنة الطلاب بالمفهوم العام لمخاطر وأمن المعلومات، مع تأكيد على مجال الأمن السيبراني[4]. ولاحقًا في هذه الدورة سيتم تقديم المزيد من التفاصيل عن نهجهم الوطني لأمن المعلومات (راجع المبحث 4)، هنا، يتعين أن تتحول المناقشة من كيفية تصنيف المعلومات إلى التمييز بين أمن المعلومات وضمان المعلومات، ثم تنتقل لاستكشاف الأنواع المختلفة لمواطن ضعف الأمن السيبراني واستعراض عملية الهجمات أو "سلسلة القتل" للحوادث السيبرانية. تنتقل المناقشة بعد ذلك إلى إدارة مخاطر أمن المعلومات من خلال نُهج مثل نموذج تقييم التهديدات والمخاطر (TRA)[5]، وبالأخص في ضوء التهديدات المستمرة المتقدمة (APTs)[6]. ودون الحاجة إلى التفصيل في هذه المرحلة، ينبغي تعريف الطلاب بالهيئات الوطنية والتنظيمية الأساسية المسؤولة عن صياغة سياسات أمن المعلومات وإجراءاته وممارساته.

الخلفية

يشمل أمن المعلومات الآليات والعمليات التي تُتيح إمكانية الوصول إلى الأصول المادية والبيانات المتضمنة في تلك الأنظمة أو المنقولة عبرها. ويركز أمن المعلومات على التكنولوجيا والعمليات المعنية بتطبيقات الأمن والبنية التحتية. ولا يشمل ضمان المعلومات (والذي قد يُطلق عليه أسماء مختلفة على الصعيد الوطني) مسائل أمن المعلومات فحسب ولكنه يضم أيضًا التركيز على إدارة المعلومات، وسلامة البيانات وأنظمة وبروتوكولات الحماية لتقليل أو إدارة المخاطر الكلية والتخفيف من حدة أثر الحوادث. تشمل أهداف الأمن الرئيسية عمومًا السرية والسلامة والتوافر والمصداقية وعدم التنصل. وهناك ممارسات وأنظمة لأمن المعلومات على مستوى الأفراد والمنظمات/المشاريع وعلى المستوى الوطني.

نتائج التعلم

يُظهر الطالب إلمامًا ودراية بما يلي

- معايير تصنيف الأمن للمعلومات والنظم المعلوماتية والإلكترونية؛
- تحليل التهديدات والمخاطر على المستوى المناسب؛
- وعينات متنوعة من "سلاسل القتل السيبرانية."
- سوف يتمكن الطلاب من تعريف المصطلحات الرئيسية ذات الصلة (البيانات، المَعرفة، المعلومات، أمن المعلومات، سلسلة القتل السيبرانية)؛
- فهم ضمان المعلومات وأهمية الأهداف الأمنية المتمثلة في السرية والسلامة والتوفر والمصداقية وعدم التنصل؛
- القدرة على شرح الدور الذي يلعبه تحليل مخاطر التعرض للتهديد في إدارة أمن المعلومات؛
- والقدرة على تحديد المنظمات المسؤولة عن التعبير عن سياسات وممارسات وإجراءات أمن معلوماتهم الوطنية.
- مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة بشأن تطور أمن المعلومات
- مصادر للممارسات الدولية الجيدة
- تحديد السلطات الوطنية الأساسية للأمن السيبراني

طريقة/تقييم التعلم

قد تشتمل أساليب التدريس على المحاضرات والبيان العملي بالأمثلة التوضيحية على الممارسات والحالات الفعلية. ينبغي أن يتمكن الطلاب من تعريف أمن المعلومات، وسلسلة القتل السيبرانية، والتهديدات المستمرة المتقدمة، وتقييم التهديدات والمخاطر.

المراجع

إيه روتوسكي، و واي كادوباياشي، وآي فيوري، ودي راجنوفيتش، وآر مارتن، وتي تاكاهاشي، "CYBEX - إطار تبادل معلومات الأمن السيبراني (X.1500)"، مجلة مراجعة الاتصالات الحاسوبية الخاصة بمجموعة *SIGCOMM التابعة لرابطة مكائن الحوسبة*، المجلد 40، رقم 5، لعام 2010. متوفر على: http://www.beepcore.org/p59-3v40n5i-takahashi3A.pdf

4 غالبًا ما يهدف نظام أمن المعلومات الإلكتروني على الأقل إلى ضمان استمرارية الخدمة والسرية والنزاهة والتوافر والمصادقة وعدم التنصل - أي وصول المستخدمين المصرح لهم بشكل مناسب على المستوى المناسب.

5 كما سيوضح ذلك بمزيدٍ من التفصيل، يعمل نموذج TRA على وزن أصول المعلومات والتهديدات ومواطن الضعف والضوابط.

6 تعني كلمة "متقدمة" هنا منسقة وهادفة ومتطورة، بينما كلمة "مستمرة" تعني دائمة. وعلى وجه الخصوص، تستلزم APTs وجود وكلاء "أذكياء" بغرض السعي للحصول على الفرصة اللازمة لقراءة القدرات السيبرانية أو تعديلها أو إفسادها أو منع الوصول إليها أو استغلالها أو تدميرها.

باباك أخجار وآخرون "تطبيقات البيانات الضخمة من أجل الأمن القومي: دليل الممارسين للتكنولوجيات الناشئة". أمستردام: بتروورث-هاينمان، 2015. الرقم الدولي المعياري للكتاب 9780128019733. رقم الرف في المكتبة البريطانية: المجموعة المرجعية العامة 28766.ELD.DS DRT. رقم المُعرِّف الفريد: BLL01017039420.

إم واتن-أوجوارد، "التهديدات السيبرانية: Un Trait Saillant du Livre Blanc"، في، *الإدارة: Revue d'étude et d'information Publiée par l'Association du Corps Préfectoral et des Hauts Fonctionnaires du Ministère de l'intérieur*. رقم 239، لعام 2013. الرقم التسلسلي المعياري الدولي للمجلة: 0223-5439.

إتش فوكاتسو، (أمن تكنولوجيا المعلومات ضد الهجمات السيبرانية؛ موضوع مشترك للبلدان المتقدمة والنامية" في نيهون إيجاكو هو شاسن جاكي زاسي؛ مؤتمر علم الأشعة الأوقيانوسي الآسيوي؛ موضوع مشترك للبلدان المتقدمة والنامية 2014، كوبي، اليابان. الرقم التسلسلي المعياري الدولي للمجلة: 0428-0048. رقم الرف في المكتبة البريطانية: 6113.254000. رقم المُعرِّف الفريد: ETOCCN087891561

صفا، نادر صحرابي، وروسو فون سولمز، ولين فتشر. "الجوانب البشرية لأمن المعلومات في المنظمات." الاحتيال والأمن الحاسوبي 2016، رقم 2 (2016): 15-18.

الشيخ، منير، وشون بي مايناردـ وعاطف أحمد، وشانتون تشانج. "سياسة أمن المعلومات: منظور الممارسة الإدارية." أرخايف بريبرنت أرخايف: 1606.00890 (2016).

روس جيه أندرسون، *الهندسة الأمنية: دليل لبناء نظم موزعة يمكن الاعتماد عليها*، الطبعة الثانية (إنديانابوليس، إنديانا: وايلي)، 2008.

الحكومة الأسترالية، وزارة الدفاع، الاستخبارات والأمن، *دليل أمن معلومات الحكومة الأسترالية 2015: الضوابط*، صادر بتصريح من د/ بول تالوني، مدير، مديرية الإشارات الأسترالية، كومنولث أستراليا، 2015 http://www.protectivesecurity.gov.au

الحكومة الأسترالية، وزارة الدفاع، الاستخبارات والأمن، *دليل أمن معلومات الحكومة الأسترالية 2015: المبادئ*، صادر بتصريح من د/ بول تالوني، مدير، مديرية الإشارات الأسترالية، كومنولث أستراليا، 2015 http://www.protectivesecurity.gov.au

مؤسسة أمن الاتصالات الكندية، *منهجية تقييم التهديدات والمخاطر المتسقة (TRA)*، 23 أكتوبر 2007.

دي إي جلبشتاين، *أمن المعلومات للمديرين غير الفنيين*، الطبعة الأولى، 2013. الرقم الدولي المعياري للكتاب 978-87-403-0488-6.

إيريك إم هتشينز، ومايكل جيه كلوبيرتي، وروهان إم أمين، "دفاع الشبكات الحاسوبية الموجهة بالاستخبارات والمسترشد بتحليلات الحملات العدائية وسلاسل القتل الاقتحامية"، *إجراءات المؤتمر الدولي السادس بشأن الحرب المعلوماتية وأمن المعلومات*، واشنطن العاصمة، 17-18 مارس 2011.

اتحاد تدقيق ومراقبة أنظمة المعلومات (ISACA)، *نتائج دراسة التوعية بالتهديدات المستمرة المتقدمة*, الولايات المتحدة الأمريكية، 2014.

ريتشارد كيسل، محرر، *مسرد المصطلحات الرئيسية لأمن المعلومات*، تقرير المعهد الوطني للمعايير والتقنية المشترك بين الوكالات (IR) 7298 التنقيح 2، المعهد الوطني للمعايير والتقنية، قسم الأمن الحاسوبي، مختبر تكنولوجيا المعلومات، مايو 2013.

جيل كلين، "كشف أسرار الأمن السيبراني: يناقش خبراء الصناعة تحديات الاختراق والتتبع والهجوم في عالم افتراضي،" مجلة أتشيفر كولدج بجامعة ماريلاند (ربيع 2013): 6–20. https://www.umuc.edu/globalmedia/upload/Spring2013-Achiever.pdf

جاري ستونبرنر، *المنشور الخاص من المعهد الوطني للمعايير والتقنية 800-33: النماذج الفنية الأساسية لأمن تكنولوجيا المعلومات*، المعهد الوطني للمعايير والتقنية، ديسمبر 2001.

"المعايير المشتركة لتقييم أمن تكنولوجيا المعلومات،" تم الوصول إليه في 17 يوليو 2015. http://www.commoncriteriaportal.org/

سلاسل تكنولوجيا المعلومات الصادرة عن المنظمة الدولية للمعايير:

1) ISO/IEC 27001:2013 تكنولوجيا المعلومات—أساليب الأمن—نظم إدارة أمن المعلومات—المتطلبات
2) ISO/IEC 27005:2011 تكنولوجيا المعلومات—أساليب الأمن—إدارة مخاطر أمن المعلومات
3) ISO/IEC 27031:2011 تكنولوجيا المعلومات—أساليب الأمن—المبادئ التوجيهية للاستعداد لتكنولوجيا المعلومات والاتصالات من أجل استمرار الأعمال
4) ISO/IEC 27032:2012 تكنولوجيا المعلومات—أساليب الأمن—المبادئ التوجيهية للأمن السيبراني

T1-B3: هياكل الفضاء السيبراني: العمود الفقري للإنترنت والبنى التحتية الوطنية

الوصف

تهدف هذه اللبنة إلى تعريف الطلاب بالنسيج الفني للفضاء السيبراني، مع التركيز على البنية التحتية العالمية والوطنية والمؤسسية؛ وهو ما يتضمن بنية الإنترنت والشبكات الحاسوبية وشبكات الهواتف الخلوية. وينبغي أن يشكل المنطق الكامن للهيكل العام والطوبولوجيا الوطنية المحددة (أي خصائص البنية التحتية الوطنية الداعمة للشبكات، ومقدمي خدمات الاتصالات السلكية واللاسلكية، وقنوات التوجيه) محور التركيز الرئيسي لهذه اللبنة.

الخلفية

تتألف بنية العمود الفقري للإنترنت من مسارات البيانات الرئيسية بين نظم الشبكات الحاسوبية الرئيسية الكبيرة والموجهات الأساسية، حيث تستضيف مراكز الشبكات التجارية والحكومية والأكاديمية وغيرها من المراكز عالية القدرة هذه الشبكات والموجهات، وتعمل على التحكم في نقاط تبادل الإنترنت ونقاط الوصول إلى الشبكة، كما تتبادل حركة الإنترنت كذلك بين البلدان والقارات. عمومًا، يشارك مقدمو خدمات الإنترنت الكبار (ISPs) (على سبيل المثال شبكات المستوى 1) في تبادل حركة العمود الفقري للإنترنت من خلال اتفاقات التوصيل البيني التي يتم التفاوض بشأنها بصورة خاصة. ويجري تسجيل مقدمي خدمات الإنترنت القائمين على إدارة أقسام فرعية منفصلة من الإنترنت يُطلق عليها اسم النظم المستقلة (AS) وتعيين أرقام نظم مستقلة (ASN) لهم. ويتم تنفيذ عملية التوجيه والقابلية للوصول بين النظم المستقلة عبر مجموعة من موجهات الإنترنت الأساسية باستخدام بروتوكول البوابة الحدودية (BGP). وتُدار العلاقة بين أسماء المجال (على سبيل المثال. www.google.com) وعناوين الإنترنت القابلة للتوجيه الخاضعة لسيطرة النظم المستقلة عن طريق نظام اسم النطاق (DNS) وسلطات التسجيل الخاصة به.

وسجل الإنترنت الوطني (NIR) هو منظمة تتولى مسؤولية تنسيق عملية تخصيص بروتوكول الإنترنت (IP) وغير ذلك من وظائف إدارة موارد الإنترنت على المستوى الوطني من خلال سجل إنترنت دولي. وقد تقوم حكومة وطنية أيضًا بتنظيم مقدمي خدمات الإنترنت في منطقتها الاقتصادية.

تشكل شبكات أجهزة الجوال/الهواتف الخلوية حاليًا عنصرًا كبيرًا من البنية التحتية لتوزيع الإنترنت. وهذه الشبكات تتصل فيما بينها بالإنترنت ويُشار إليها باسم "ويب الجوال." وقد تتطرق هذه اللبنة إلى استكشاف بنيتها العامة والخصائص الوطنية لها.

نتائج التعلم

سيتمكن الطلاب من

- تكوين فهم متعمق عن الطوبولوجيا المادية والافتراضية وتوجيه العمود الفقري للإنترنت؛
- شرح دور أرقام النظم المستقلة في الربط البيني العالمي للإنترنت ومسؤولية سلطة أرقام الإنترنت المخصصة (IANA)؛
- فهم العلاقة بين مقدمي خدمات الإنترنت (المستوى 1) رفيعي المستوى، ومقدمي خدمات الإنترنت الفرعيين، وشبكات المنطقة المحلية للمستخدم النهائي (LANs)؛
- شرح دور خوادم الاسم الموثوق في الربط البيني العالمي للإنترنت ومسؤولية هيئة الإنترنت للأسماء والأرقام المخصصة (آيكان)؛
- فهم طوبولوجيا وجغرافيا الفضاء السيبراني الوطني الخاص بهم، بما في ذلك السجلات الوطنية وسلطات حوكمة مقدمي خدمات الإنترنت؛
- والإلمام بهيكل شبكات الهواتف الخلوية/الجوال وتوجيهها واتصالها بالإنترنت في السياق الوطني.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

لطرح مقدمة فعالة للجمهور غير الفني، فإن أولئك الذين يستخدمون هذا المنهج المرجعي لوضع إطار دورة أو دورات تدريبية محددة سيتعين عليهم إيلاء قدر كبير من الاهتمام لإيجاد المستوى الملائم من التفصيل الفني للتحقق من أن المادة مفهومة لطلابهم.

يمكن استكشاف الشبكة الوطنية وشبكات الاتصال السلكية واللاسلكية بمستوى معين من التعمق.

طريقة/تقييم التعلم

قد يتم التدريس إما عن طريق المحاضرة أو البيان العملي. ويمكن إضفاء مزيدًا من الحيوية على المنهج من خلال الجولات في المرافق الوطنية، وجلسات الإحاطة مع الخبراء، واختبارات التحدي الشفوية والعملية.

المراجع

كونستانتينوس مولينوس، روسيلا ماتيولي، الوكالة الأوروبية لأمن الشبكات والمعلومات "ترابطات شبكة الاتصالات في الشبكات الذكية"، إيراكليو، كريت، اليونان. مارس 2016. متوفر على: www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids (تم الاسترجاع في 14 يوليو 2016).

عبد الرحمن القحطاني. "نحو إطار للتهديدات الإرهابية السيبرانية المحتملة على البنية التحتية الوطنية الحيوية: دراسة كمية" الأمن المعلوماتي والحاسوبي. المجلد 23، رقم 5؛ لعام 2015؛ 369-532. الرقم التسلسلي المعياري الدولي للمجلة: 2056-4961. رقم الرف في المكتبة البريطانية: 4481.796000. رقم المُعرِّف الفريد: ETOCvdc_100027180236.0x000001

إي ستنيكوفا، إي فوو، آر بي فوغن، "قوة التدريبات العملية في مجال تعليم الأمن السيبراني من SCADA"، الاتحاد الدولي لمعالجة المعلومات -الإصدارات- IFIP؛ تعليم أمن المعلومات؛ هايدلبيرج؛ سبرنجر؛ 2013. الرقم التسلسلي المعياري الدولي للمجلة: 1868-4238. رقم الرف في المكتبة البريطانية: 4540.183500. رقم المُعرِّف الفريد: ETOCCN085265877

أو نيتكاشوف، بي بوبوف، كيه سالاكو، "القياس الكمي لأثر الهجمات السيبرانية على البنى التحتية الحيوية"، في *مجلة علم الدلالة المتعلق بالبيانات؛ الموثوقية والجوانب الأمنية لحماية البنية التحتية الحيوية*، فلورنسا، إيطاليا، 2014؛ سبتمبر، 2014، الصفحات 316-327. الرقم التسلسلي المعياري الدولي للمجلة: 0302-9743. رقم المُعرِّف الفريد: ETOCCN088306466.

موسياني، وفرانشيسكا، وديريك إل. كوغبيرن، ولورا ديناردیس، ونانيت إس ليفينسون، محررون. التحول إلى البنية التحتية في حوكمة الإنترنت. سبرنجر، 2016.

آيكان، "دليل المبتدئين لأسماء النطاقات،" 6 ديسمبر 2010.

سلطة أرقام الإنترنت المخصصة, *وظائف IANA: مقدمة إلى وظائف سلطة أرقام الإنترنت المخصصة*، آيكان، يونيو 2015.

بول كرزيزانوسكي، "فهم النظم المستقلة: التوجيه والاقتران،" 5 إبريل 2013، تم الوصول إليه في 17 يوليو 2015. https://www.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html

مايكل ميلر، "كيف تعمل شبكات الجوال،" بيرسون للتعليم، كيو ببليشنج، 14 مارس 2013، تم الوصول إليه في 17 يوليو 2015.

رام موهان، "مهاجمة جوهر الإنترنت،" موقع ويب سيكيورتي ويك، 16 مارس 2011، تم الوصول إليه في 17 يوليو 2015 http://www.securityweek.com/attacking-internets-core

جيف تايسون، "كيف يعمل بروتوكول WAP"، موقع ويب هاوستفوركس، تم الوصول إليه في 17 يوليو 2015. http://computer.howstuffworks.com/wireless-internet3.htm

ردولف فان دير برج، "كيف "يعمل الإنترنت: مقدمة إلى الاقتران والنقل،" 2 سبتمبر 2008، تم الوصول إليه في 17 يوليو 2015. http://arstechnica.com/ features/2008/09/peering-and-/transit/4

T1-B4: البروتوكولات والأنظمة الأساسية

الوصف

تستخدم أنظمة الاتصال تنسيقات رسائل مُعرَّفة جيدًا، تُدعى البروتوكولات، لتبادل الرسائل. وبروتوكول الاتصال هو نظام من القواعد لتبادل البيانات في أجهزة الحاسوب أو فيما بينها (سواءً أكانت متصلة بالشبكة أم لا). ويمكن فهم البروتوكولات بأنها أشبه بمكونات عنوان على مظروف في البريد حيث تحدد المُرسل والمُستلم والإحداثيات الخاصة بكل منهما. كل رسالة لها معنى محدد مقصود لاستخلاص رد من مجموعة ردود محتملة محددة مسبقًا لهذا الموقف تحديدًا. وهكذا، يجب أن يحدد أي بروتوكول القواعد لبناء الجملة (القواعد)، والدلالات (المعنى) ومزامنة الاتصال؛ ومن ثم فإن السلوك المحدد عادةً ما يكون مستقلاً عن الطريقة التي من المقرر معالجته بها أو عن الأنظمة المختلفة التي قد يمر بها من أجل الوصول إلى الوجهة المقصودة.

ويكون لكل طبقة أو عملية بروتوكول مواطن الضعف والمخاطر الكامنة فيها، والتي يمكن استكشافها عبر عدة مستويات خبرات مختلفة. فيمكن مناقشة هذا الموضوع على مستوى أساسي جدًا، وإن كان من الممكن، في وجود المشاركين الملائمين، تناوله على المستوى المصنف.

الخلفية

توجد طريقتان لتصور وتصميم نظام شبكي.

إن وجهة النظر المنطقية لكيفية عمل الإنترنت يمكن اعتبارها قائمة على البروتوكول. وحزمة البروتوكول هي قيام البرامج بتنفيذ مجموعة من معايير بروتوكول الاتصالات، حيث تحكم حزم البروتوكولات كيفية حزم البيانات ونقلها، وعادة ما تكون عمليات البروتوكول المنفذة مُرتّبة في بنية ذات مستويات (أي حزمة). وعمليات البروتوكول المنفذة بالقرب من الجزء السفلي من الحزمة تقوم بخدمات اتصالات ذات طابع أوليّ، مثل الاتصال الأساسي لمجموعة صغيرة من البيانات بجهاز حاسوب آخر متصل بالشبكة المحلية (على سبيل المثال إيثرنت). وفي المستويات الأعلى من الحزمة، تقدم البروتوكولات خدمات مثل المعالجة المشتركة للشبكات العالمية (مثل IP)، وتصحيح الأخطاء وإعادة تجميع كائنات بيانات أكبر (مثل TCP، أو بروتوكول التحكم في الإرسال). وتقدم البروتوكولات عالية المستوى أكثر الخدمات المجردة على مستوى التطبيقات، مثل إرسال البريد الإلكتروني (بالبروتوكول البسيط لنقل رسائل البريد (SMTP)) أو استعراض صفحات الويب (ببروتوكول نقل النص التشعبي (HTTP)). وتعتمد المستويات الأعلى في حزمة البروتوكول على الخدمات الأساسية بشكل أكبر في المستويات الأدنى.

بدلاً من ذلك، يمكن وصف النظرة المادية للإنترنت بالكيفية التي يجري بها تنفيذ البروتوكولات عبر أجهزة الشبكة والأنظمة الأساسية (مثل المبدلات والموجهات والبوابات والوكالات وجدر الحماية) وأشكال الاتصال البيني بين أجهزة الشبكة هذه. فعلى سبيل المثال، قد تصل مبدلات الشبكة التي تنفذ بروتوكول الإيثرنت بين أجهزة الحاسوب الموجودة على شبكة LAN. وقد تكون شبكات LAN متصلة بموجهات الشبكة التي تنفذ بروتوكول الإنترنت لإعادة توجيه حزم البيانات بين الشبكات وربما بقية الإنترنت. وقد ينفذ خادم البريد المتصل بالشبكة البروتوكول البسيط لنقل البريد.

لقد بات من الصعب رسم خرائط مباشرة للعلاقة بين الأجهزة المادية ومسؤوليتها في تنفيذ البروتوكول في الشبكات المعاصرة مع وجود أجهزة وشبكات افتراضية. ففي هذه الشبكات، يمكن تنفيذ أجهزة الشبكة وتوصيلها فيما بينها على نحو افتراضي باستخدام البرامج التي تعمل على خوادم كبيرة (كما في حالة "الحوسبة السحابية"). إن الطابع الافتراضي لهذه الأنظمة يضيف مستوىً من التعقيد للأمن وهو ما يُعتبر مسألة ناشئة تحتاج إلى دراسة.

ويمكن تصميم وتنفيذ حزم البروتوكول للتطبيقات المتخصصة. وتعد نظم التحكم الصناعية (ICSs) مثل نظام التحكم الإشرافي والاستحواذ على البيانات (SCADA) أمثلة على حزم بروتوكول الاتصالات الشبكية التي يجري استخدامها للإبلاغ عن بيانات قياسات أجهزة الاستشعار وإرسال رسائل التحكم. في شبكة طاقة، على سبيل المثال، قد تكون هذه الأنظمة مسؤولة عن رصد الأحمال وتبديل وصلات الإمداد على حسب تغير الطلب. ويمثل أمن نظم SCADA موضوعًا هامًا في مجال أمن البنية التحتية الوطنية نظرًا لأن النظم التي يتم التحكم فيها قد تكون ذات أهمية وطنية. والكثير من أنظمة الأسلحة الحديثة تستخدم نظمًا إلكترونية مماثلة لنظم SCADA الصناعية تلك وقد تكون أيضًا معرضة للمخاطر.

وينطوي كل مستوى من مستويات البروتوكول على مخاطر ومواطن ضعف كامنة. وهذه يمكن استكشافها على مستويات مختلفة من الخبرات، بدءًا من المعرفة العامة وحتى مستوى الخبراء (المصنف).

تعريف بروتوكول أمن الشبكة

بصفة عامة، توفر بروتوكولات أمن الشبكة الأمن والسلامة للبيانات عند نقلها عبر الاتصال بالشبكة، حيث تحدد هذه البروتوكولات العمليات والمنهجية لتأمين بيانات الشبكة. وليس هناك بروتوكول يضمن أمن البيانات. بل، يوفر كل بروتوكول طريقة خاصة لإحباط نهج محدد لمهاجمة نظام أو شبكة. ملاحظة: قد يتم تطبيق تعريفات وطنية محددة أو دولية متفق عليها.

وغالبًا ما تستخدم بروتوكولات أمن الشبكة أساليب التشفير والترميز لتأمين البيانات بحيث يمكن فك تشفيرها أو تعديلها فقط باستخدام خوارزمية محددة و/أو مفتاح منطقي و/أو مزيج منها. تضم البروتوكولات الشائعة لأمن الشبكة الصدفة الآمنة (SSH)، وبروتوكول نقل الملفات الآمن (SFTP)، وبروتوكول نقل النص التشعبي الآمن (HTTPs)، وطبقة مأخذ التوصيل الآمنة (SSL).

نتائج التعلم

سيتمكن الطلاب من

- وصف ومناقشة أدوار ومسؤوليات كل مستوى في حزمة بروتوكول الشبكة القياسية (TCP-/IP استنادًا إلى حزمة بروتوكولات الإنترنت)؛
- وصف أجهزة الشبكة المشتركة مثل الموزعات والمبدلات والموجهات والبوابات وخوادم التطبيق والعلاقة بين تنفيذ الأجهزة لطبقات حزمة بروتوكول الشبكة ودورها الوظيفي في الشبكة؛
- مناقشة المفاهيم الأساسية لافتراض أجهزة الشبكة، والشبكات المعرفة بالبرامج، وأثر هذه المفاهيم على بنية الشبكة، وعلاقتها ببيئات الحوسبة السحابية؛
- وصف العناصر الأساسية لبيئة نظم التحكم الصناعية القائمة على SCADA (يمكن أن ينطوي هذا على المكونات الخاصة بنظم ICS وأسس تشغيلها في بروتوكولات الإنترنت القياسية)؛
- وتحديد ووصف بروتوكولات الأمن المشتركة، وعلاقتها بالبنية الشبكية متعددة المستويات القائمة على البروتوكول ومواطن ضعف الأمن المحددة التي يعالجها كل بروتوكول.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

يمكن التطرق إلى أنظمة التحكم الصناعية (مثل نظام SCADA) ونظم تكنولوجيا المعلومات للمنصات العسكرية بقدر من التفصيل من أجل رصد مواطن ضعفها ومغريات استهدافها.

طريقة/تقييم التعلم

المحاضرة والبيان العلمي ودراسات الحالة من الطرق الموصى بها. وينبغي أن يكون التقييم في صيغة كتابية ومستندًا إلى المستوى الملائم بالنظر إلى تفاصيل أي دورة تدريبية معينة مستقاة من هذا المنهج.

المراجع

إي فان بارس، آر فيربروج، آر "خوارزمية التواصل للعمل الجماعي في بيئة متعددة الوكلاء"، *مجلة أشكال المنطق غير الكلاسيكي التطبيقي، المنطق وأمن المعلومات؛* لايدن، هولندا، 2008، سبتمبر، 2009، 431-462، لافوازييه؛ 2009. رقم الرف في المكتبة البريطانية: 4943.400000، رقم المعرّف الفريد: ETOCCN074941483

سي دبليو تشان "بروتوكولات التبادل الرئيسية لخدمات الاتصالات متعددة الأطراف"، الندوة الدولية المعنية بالعوالم السيبرانية؛ طوكيو، 2002. مؤتمر الرقم الدولي المعياري للكتاب: 0769518621. رقم الرف في المكتبة البريطانية: 4550.208900. رقم المُعرِّف الفريد: ETOCCN046776823.

جان جاتسكوسكي، بيرند كلينيوهان، "إعادة التكوين الذاتي للاتصالات الفورية في النظم السيبرانية المادية"، 2016. بحث إلكتروني محفوظ لدى المكتبة البريطانية. رقم المُعرِّف الفريد: ETOCvdc_100033448082.0x000001.

جيه إيفيما، تي كيرت، "الخوارزميات التطورية للاختيار الأمثل للتدابير الأمنية". وقائع المؤتمر الأوروبي العاشر بشأن الحرب المعلوماتية والأمن بجامعة تالين للتكنولوجيا؛ تالين، إستونيا، 7-8 يوليو 2011، الصفحات 172-184. رين أوتيس (محرر). الرقم الدولي المعياري للكتاب 9781908272065 (pbk.) رقم المُعرِّف الفريد: BLL01015873308.

قدير، وجوناهيد، وأرجونا، وساثياسيلان، وليانغ وانغ، وبارات رغافان. "الاتصال الشبكي التقريبي من أجل الوصول العالمي إلى شبكة إنترنت للجميع (GAIA)." أرخايف بريبرنت أرخايف: 1603.07431 (2016).

جمعية معايير IEEE، معايير IEEE 802. http://standards.ieee.org/about/get/

فريق العمل المعني بهندسة الإنترنت، طلب تعليقات (RFC)، تم الوصول إليه في 17 يوليو 2015. https://www.ietf.org/rfc.html

سيرتيولوجي، أجهزة الشبكة، تم الوصول إليه في 17 يوليو http://www.certiology.com/computing/computer-networking/network-devices.html2015.

سيسكو سيستمز انك، بروتوكول ربط VLAN لشبكات LAN الافتراضية، (VLANs VTP)، تم الوصول إليه في 17 يوليو 2015. http://www.cisco.com/c/en/us/tech/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/index.html

دي كلارك، "فلسفة تصميم بروتوكولات الإنترنت لوكالة مشاريع البحوث المتقدمة للدفاع [DARPA]، *وقائع مجموعة SIGCOMM "88*, 14–106

(نيويورك: رابطة مكائن الحوسبة)، أغسطس 1988.

كيفن آر فوول ودبليو ريتشارد ستيفنز، *شرح TCP/IP ، المجلد 1: البروتوكولات*، الطبعة الثانية، سلسلة الحوسبة الاحترافية لأديسون-ويزلي (بوسطن، ماساتشوستس: أديسون ويزلي بروفيشنال)، 15 نوفمبر 2011.

جونيبر نتووركس إنك، "الكتاب الأبيض: بنية شبكات نظام SCADA ونظام التحكم الموزعة الآمنة"، 2010، تم الوصول إليه في 17 يوليو 2015. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf

راديا بيرلمان، "دروس عن الجسور والموجهات والمبدلات" تم الوصول إليه في 17 يوليو 2015. https://www.ietf.org/proceedings/62/slides/protut-0.pdf

بارت برينيل، "بروتوكولات أمن الإنترنت،" فيديو لمحاضرة ألقيت على SecAppDev في 2013، لوفان، بلجيكا. https://www.youtube.com/watch?v=CZzd3i7Bs2o

أندريو إس تانينباوم ودايفيد جيه ويثرال *الشبكات الحاسوبية*، الطبعة الخامسة (نيويورك: بيرسون)، 27 سبتمبر 2010.

T1-B5: بنية وإدارة الأمن

الوصف

تتعامل هذه اللبنة مع البنية الأمنية الأساسية (BSA) بما يتضمن الجوانب التكنولوجية والتشغيلية والسياقات الإدارية التي تؤثر على هيئتها. وتشكل BSA على الصعيد الوطني البنية والممارسات بما يشمل البنية التحتية (على سبيل المثال الأعمدة الفقرية لشبكات الاتصالات السلكية واللاسلكية) وعوامل تصفية المحتوى على المستوى الوطني وهياكل الحوكمة للأمن السيبراني. ويكمن الهدف العام من هذه اللبنة في تدريس الطلاب كيفية تصميم/إنشاء البيئات الأمنية استنادًا إلى تحليل المخاطر بما يضمن إبقاء المخاطر ضمن الحدود المقبولة. وتتضمن البنية الضوابط الفنية والضوابط المادية إلى جانب السياسات والتدريبات. ومن أمثلة الضوابط الفنية جُدر الحماية وأنظمة كشف التسلل وإدارة السجلات. وتشمل أمثلة الضوابط المادية إدارة الوصول وأجهزة إنذار الحريق والتحكم في الرطوبة. وسوف يتعلم الطلاب كيفية إجراء تحليل المخاطر وعمل التهيئة الأمنية على المستوى الوطني وعلى مستوى الأفراد والمنظمات.

وتسترشد BSA بالسياسات الوطنية والمعايير الأمنية المختلفة ودورة حياة النظام ومبادئ التصميم وعناصر البُنَى المادية. وتستعرض هذه اللبنة، عند دراستها تصميم البنية الأمنية الأساسية، المفاهيم التكميلية المتعلقة بالمراقبة الملائمة للأصول، والرقابة المادية والبيئية، وخطط الإدارة، والجوانب البشرية، بما في ذلك فحص الموظفين، واستمرارية العمليات، وخطط الطوارئ، ومرونة النظم السيبرانية.

الخلفية

يتعين أن تكون بنية الأمن موجهة بالسياسة؛ أي أنها تبدأ بفهم أصول المعلومات الخاضعة للإدارة. وتشكل قيمة أصول المعلومات بالنسبة للمدافع (أي أثر فقدانها أو تعديلها) وقيمة هذه الأصول لمرتكبي التهديد المحتمل أحد الاعتبارات المحورية في هذا الخصوص. إن مرحلة تحديد الأصول وتقدير قيمتها هي التي توجه تطوير السياسة نحو التحكم في إمكانية الوصول إلى معلومات.

وتحدد مرحلة تقييم التهديدات مرتكبي التهديدات الذين يُتوقع منهم إلى حد معقول الإضرار بالأصول المحددة كما تحدد قدراتهم الفنية. ويكون تطوير البنية الأمنية مدفوعاً بمتطلب تصميم نظام مادي ومعايير التوكيد المرتبطة به والإجراءات التي تحد من مخاطر قدرة مرتكبي التهديدات على الإضرار بالأصول. وقد يكون هناك معايير وطنية لتقييم التهديدات والمخاطر ومعايير لاعتبارات التصميم والإرشادات في اختيار آليات مراقبة الوصول وتخطيطات البُنى.

وكثيرًا ما يُوصف اختيار وتنظيم البنية الأمنية للمشروع على أنه دفاع في العمق، حيث يحمي الاستخدام المُنسّق لآليات الأمن المتعددة سلامة أصول المعلومات. ويبدأ الدفاع عن أصول المعلومات بوضع ضوابط وصول إلى بياناتها الخاصة ويتجه نحو المكونات الخارجية، من خلال آليات الأمن في التطبيقات التي يمكنها الوصول إلى البيانات، ومضيفي أجهزة الحاسوب التي تعمل عليها هذه التطبيقات، ونسيج الشبكة المؤسسية، وينتهي على الشبكة المؤسسية وهيكلها الأساسي، وينتهي بالمحيط الأمني للمؤسسة حيث تنضم إلى البنية التحتية للشبكة العالمية.

تضم البنية الأمنية المؤسسية حزمة من الآليات المصممة للتخفيف من حدة المخاطر على هذه المؤسسة بعينها. وتشمل الآليات المشتركة، أو عناصر البنية، المخصصة لتنفيذ السياسة الأمنية تعيين مناطق الشبكة، وجدر الحماية، وأنظمة كشف التسلل (IDSs)، وتطبيقات مكافحة الفيروسات، وتقنيات التشفير، ونظم إدارة المعلومات والأحداث الأمنية (SIEM). ولا يوجد أي نظام من هذه النظم يضمن لك تحقيق الأمن وحده. فأساليب الهجوم متباينة وبإمكانها استغلال مواطن الضعف الموجودة في الكثير من البروتوكولات والنظم وتطبيقات البرامج مما يعرض البنية التحتية المؤسسية للمخاطر.

وتعتبر أنشطة ضمان الأمن إجراءات يتم اتخاذها أثناء تطوير وتقييم بنية أمن المؤسسة للتحقق من أن التدابير الأمنية المطبقة فيما يتعلق بالنظام فعَّالة. ملحوظة: في بعض الحالات تكون هذه التدابير افتراضية أكثر منها حقيقية. فعلى سبيل المثال، تُعلن منتجات مراقبة الوصول أنها تتضمن مجموعة من الوظائف الأمنية. وقد يكون نشاط ضمان الأمن المرتبط مجرد اختبار منهجي لهذه الوظيفة بواسطة منظمة معايير معترف بها لتوفير الدليل على أن المنتج يؤدي المهام الصحيحة، دون أخطاء. ومن الأمثلة الأخرى على أنشطة ضمان الأمن المراجعات الرسمية أو شبه الرسمية للتصميم، ووضع وثائق وأدلة إرشادية للأمن لمجتمع مستخدمي ومشغلي الأنظمة، وإدارة دورات حياة مكونات الأمن، وإدارة التكوين، وإدارة أمن بيئات مطور/مُصنِّع مكونات البنية، والتسليم الموثوق لمكونات البنية من المُطور/المُصنّع إلى البيئة المؤسسية. وينطوي ضمان الأمن أيضًا على برامج لإجراء فحوصات المعلومات الأساسية والتصاريح الأمنية للأفراد من أجل إنشاء مستوى من الثقة في مستخدمي النظام والقائمين على تشغيله.

نتائج التعلم

سيتمكن الطلاب من

- مناقشة كيفية تضمين المستويات المتعددة لآليات الأمن عبر بنية مؤسسية قائمة على الدفاع المتعمق من أجل توفير دعم احتياطي في حال فشل الضوابط الأمنية أو استغلال ثغرة أمنية؛
- تقديم مقترحات، وذلك على المستوى الأوليّ، مقترحات بشأن تعيين مناطق الأمن الملائمة، ووضع تدابير مثل جُدر الحماية باستخدام مخطط شبكي؛
- فهم نطاق المعايير الوطنية والوثائق الإرشادية بشأن إجراء تقييمات التهديدات والمخاطر، ووضع سياسة أمنية على المستوى المؤسسي/التنظيمي، وتنفيذ البنية الأمنية؛
- فهم علاقة مرحلة تحديد الأصول ضمن تقييم التهديدات والمخاطر (TRA) بتوصيف السياسة الأمنية للمؤسسة؛
- فهم علاقة مرحلة تقييم التهديدات في تقييم TRA بتحديد مواطن الضعف التي يمكن استغلالها بواسطة مرتكبي

التهديدات المتوقعين وفهم كيف يوجه ذلك المتطلبات المتعلقة بالتدابير الأمنية التي يتم نشرها عبر البنية المؤسسية؛

- وإدراك نطاق نظام تصنيف الأمن الوطني لحماية الوثائق والمعلومات واكتساب القدرة على وصف علاقته بفحص الأفراد وبرامج التصريح الأمني.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

تتعين مناقشة الأشكال المتعددة لإدارة بنية النظام وتقسيم أمن الشبكة لتمكين الطلاب من تقييم النماذج التي تبنتها منظمتهم أو التي ينبغي عليها تبنيها.

قد تستدعي هندسة العوامل البشرية وآليات استغلال الهندسة الاجتماعية دراسة مفصلة.

وقد يحتاج النظام الأساسي لتصنيف الأمن الوطني المعني بالوصول المادي، وحماية المستندات والمعلومات، وبرامج فحص الأفراد، والتصريح الأمني إلى المراجعة والجمع.

طريقة/تقييم التعلم

قد يتضمن أسلوب التدريس العمل في مجموعات صغيرة لتناول الجوانب البشرية والتكنولوجية والتشغيلية.

ويمكن إثراء المناقشة وخبرة التعلم من خلال عقد محاضرات زائرين من المنظمات الخاصة والدولية المناقشة.

تختلف وسائل التقييم باختلاف مستوى المعرفة المطلوب بما يتوافق مع الطلاب الذين يتم تعليمهم.

المراجع

إس إيه تشون، في أتلوري، بي بي بهاتاشاريا، "التحكم في الوصول القائم على المخاطر لخدمات البيانات الشخصية"، *العلوم الإحصائية والبحوث متعددة التخصصات*؛ المؤتمر الدولي بشأن أمن نظم المعلومات؛ الخوارزميات والبنى، كلكتا؛ الهند، 2006؛ ديسمبر 2009، 284-263. الرقم التسلسلي المعياري الدولي للمجلة: 6195-1793. مؤتمر الرقم الدولي المعياري للكتاب: 9789812836236؛ 9812836233. رقم الرف في المكتبة البريطانية: 8448.954000. رقم المُعرِّف الفريد: ETOCCN071364080.

جيرارد ديسمارتز، *الجاسوسية السيبرانية*، *Ou, Comment Tout Le Monde épie Tout le Monde!*، باريس: تشيرون، 2007 الرقم الدولي المعياري للكتاب 9782702712122 (pbk.) رقم المُعرِّف الفريد: BLL01014343705.

إيه روتوسكي، وواي كادوباياشي، وآي فيوري، ودي راجنوفيتش، وآر مارتن، وتي تاكاهاشي، "CYBEX - إطار تبادل معلومات الأمن السيبراني - (X.1500)،" مجلة مراجعة الاتصالات الحاسوبية الخاصة بمجموعة SIGCOMM التابعة لرابطة مكائن الحوسبة، المجلد 40، رقم 5، لعام 2010

آي عتوم، إيه العتوم، إيه إيه علي، "إطار شامل لتنفيذ الأمن السيبراني"، في *إدارة المعلومات والأمن الحاسوبي*،المجلد 22؛ رقم 3، لعام 2014، الصفحات 264-251. الرقم التسلسلي المعياري الدولي للمجلة: 0968-5227. رقم المُعرِّف الفريد: ETOCRN359424579.

هيونجوك يون، وتايشك شون. "التحديات والاتجاهات البحثية للنظام غير المتجانس السيبراني - المادي القائم على معايير IEC 61850: مواطن الضعف، ومتطلبات الأمن، والبنية الأمنية." الجيل القادم لأنظمة الحاسوب 61 (2016): 128-136.

الحكومة الاسترالية، وزارة الدفاع، الاستخبارات والأمن، *دليل أمن معلومات الحكومة الأسترالية: الضوابط*، صادرة بتصريح من د/ بول تالوني، مدير، مديرية الإشارات الأسترالية، كومنولث أستراليا، 2015. انظر www.protectivesecurity.gov.au

الحكومة الاسترالية، وزارة الدفاع، الاستخبارات والأمن، *دليل أمن معلومات الحكومة الأسترالية: المبادئ*، صادرة بتصريح من د/ بول تالوني، مدير، مديرية الإشارات الأسترالية، كومنولث أستراليا، 2015. انظر www.protectivesecurity.gov.au

ديبورا جيه بودياو ودي جيه غراوبارت، إطار عمل هندسة المرونة السيبرانية، تقرير ميتر الفني MTR 110237 (بيدفورد، ماساتشوستس: مؤسسة ميتر)، سبتمبر 2011.

مؤسسة أمن الاتصالات الكندية، *متطلبات الأمن الأساسية لمناطق أمن الشبكات في الحكومة الكندية (ITSG-22)*، يونيو 2007.

مؤسسة أمن الاتصالات الكندية، *منهجية تقييم التهديدات والمخاطر المتسقة (TRA-1)23*، أكتوبر 2007.

مؤسسة أمن الاتصالات الكندية، *المبادئ التوجيهية لأمن تكنولوجيا المعلومات: تقسيم أمن الشبكة إلى مناطق: اعتبارات التصميم لتعيين الخدمات ضمن المناطق (ITSG-38)*، مايو 2009.

مؤسسة أمن الاتصالات الكندية، *المبادئ التوجيهية لأمن تكنولوجيا المعلومات: إرشادات مصادقة المستخدم لأنظمة تكنولوجيا المعلومات (ITSG-31)*، مارس 2009.

جورج فرح، "البنية الأمنية للنظم المعلوماتية—نهج جديد للحماية متعددة المستويات: دراسة حالة، "النسخة العملية 1.4ب للشهادة العالمية لأساسيات الأمن (GSEC)، معهد سانس، 9 سبتمبر 2004. www.sans.org

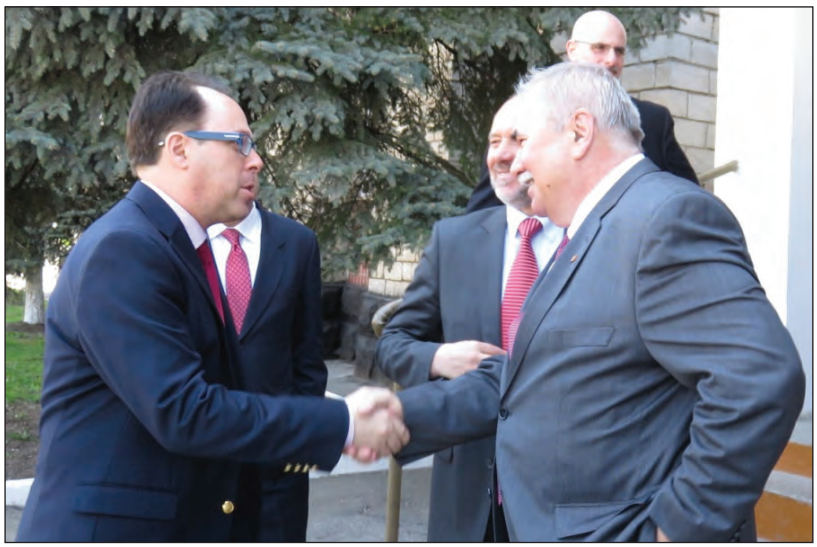
دي إي جلبشتاين، *أمن المعلومات للمديرين غير الفنيين*، الطبعة الأولى، 2013. الرقم الدولي المعياري للكتاب 978-87-403-0488-6.

جيل كلين، "كشف أسرار الأمن السيبراني: خبراء الصناعة يناقشون تحديات الاختراق والتتبع والهجوم في عالم افتراضي، " مجلة أنتشيفر كولدج بجامعة *ماريلاند* (ربيع 2013): 6–20. https://www.umuc.edu/globalmedia/upload/Spring2013-Achiever.pdf

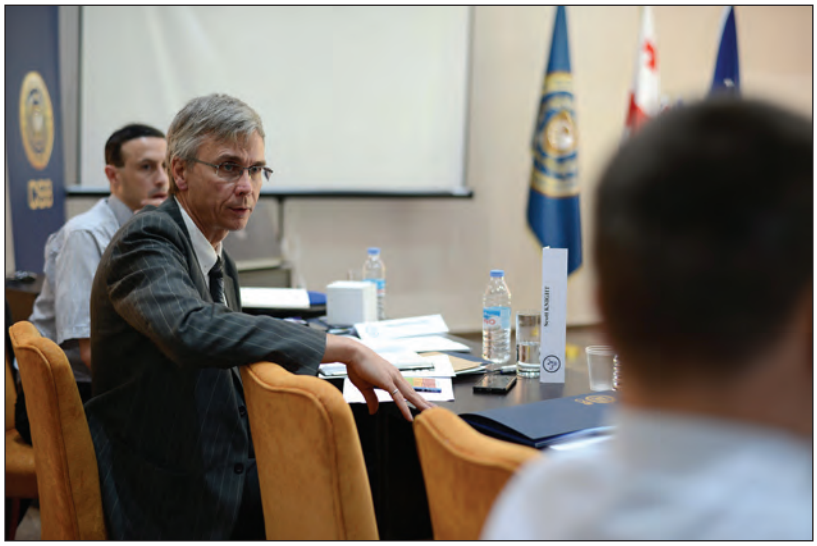
ألكسندر كلمبرج، محرر، *دليل إطار عمل الأمن السيبراني الوطني*,منشور خاص بمركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو، تالين، إستونيا 2012. الرقم الدولي المعياري للكتاب 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

ويليام بيلجرين، "نموذج للتغيير الإيجابي: إحداث التغيير الإيجابي في إستراتيجية الأمن السيبراني، والعوامل البشرية، والقيادة"، مركز أمن الإنترنت.

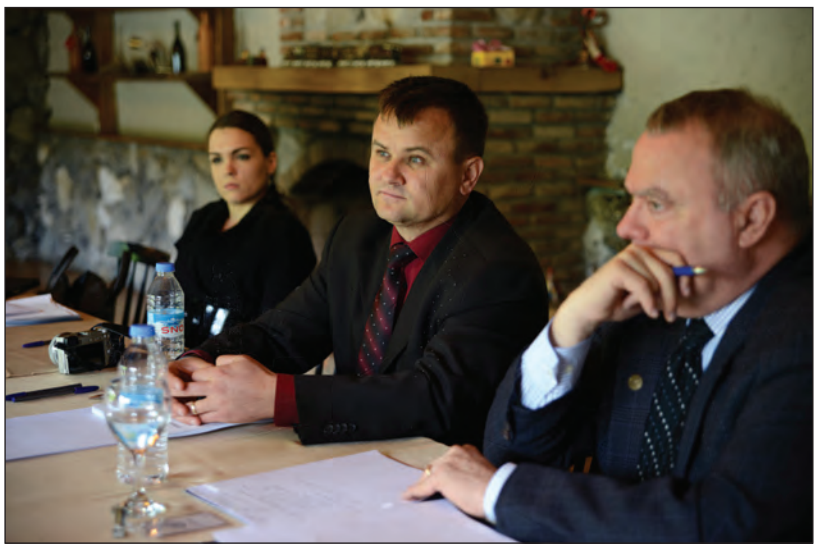
أنطوني ثورن، وتوبياس كريستين، وبياتريس جروبر، ورولاند بورتمان، ولوكاس روف، "ما هي البنية الأمنية؟" بحث مقدم من فريق العمل المعني بالبنية الأمنية، جمعية أمن المعلومات السويسرية (ISSS)، 29 سبتمبر 2008.



دول أعضاء وغير أعضاء في الناتو يتحدون في تأليف المنهج المرجعي للأمن السيبراني. اجتماع وزير الدفاع المولدوفي مع المحررين.



ورشة عمل للفريق المعني بكتابة المنهج المرجعي للأمن السيبراني في تبليسي (المساهمون من جامعة جرينتش والكلية العسكرية الملكية في كندا).



ورشة عمل للفريق المعني بكتابة المنهج المرجعي للأمن السيبراني في تبليسي (المساهمون من مدرسة الناتو في أوبرميرجاو، وآي انتليجنس، وإس إل سي إي).

المبحث 2: متجهات المخاطر

الهدف

يقدم هذا المبحث دراسة استقصائية تمهيدية عن مواطن الضعف الكامنة في الفضاء السيبراني والطرق والوسائل لاستغلال مواطن الضعف هذه من خلال سلاسل هجمات أو موجهات متنوعة. ويُعد فهم مواطن الضعف هذه مقومًا أساسيًا لتقييم المخاطر وسياسة التخفيف، حسبما سيتم تناوله كذلك.

الوصف

تبنى هذا المنهج المرجعي المقترح الوارد في تقرير الفريق الوطني الأمريكي للدراسات السيبرانية المقدم إلى مدير الاستخبارات الوطنية الأمريكية بأن جميع مواطن الضعف السيبرانية المختلفة يمكن تصنيفها بسهولة في إطار نماذج موجهات المخاطر التالية (انظر تشابينسكي 2010 في المراجع): "سلسلة التوريد ووصول المُورّدين؛ وإمكانية الوصول عن بعد؛ وإمكانية الوصول عن قرب؛ والوصول من الداخل." وبالتالي، وفي إطار هذا المبحث، تتناول اللبنة T2-B1 نموذج سلسلة التوريد/الموردين وتسلط الضوء على المسائل الأمنية بدءاً من أرضية الإنتاج مرورًا بالمتعاقدين من الباطن والشحن وضوابط التخزين والصيانة؛ واللبنة T2-B2، هجمات الوصول عن بعد والوصول عن قرب، وتستكشف مواطن الضعف المرتبطة بالوصول غير المصرح به (بدون امتيازات)؛ واللبنة T2-B3، الوصول من الداخل (هجمات الوصول المحلي) وتتطرق إلى مواطن الضعف المرتبطة بالوصول القائم على الامتيازات إلى النظم؛ واللبنة T2-B4، مخاطر التنقل، ونظام إحضار الأجهزة الشخصية والاتجاهات الناشئة، وتناقش المخاطر المرتبطة بسياسات نظام إحضار الأجهزة الشخصية ("BYOD")، والحوسبة "السحابية" وقضايا التنقل الأخرى.

والهدف العام من هذا المبحث يتمثل في توفير أساس عام لمجموعة قضايا الضعف الكامنة في مكونات الفضاء السيبراني. ومع هذا، قد تختار الدورات الأكثر تطورًا التي تسترشد بهذه الوثيقة المنهجية عمل ذلك على مستوى الخبراء والمستوى المصنف من أجل معالجة السياسات والإجراءات الوطنية الفعلية.

أهداف التعلم

سيتمكن الطلاب من

- فهم الأهمية والتأثير المحتمل لسلسلة التوريد المستخدمة وإمكانية الوصول عن بعد والوصول عن قرب ومن الداخل إلى مواطن الضعف في الفضاء السيبراني المستهدفة وتلك المواطن المرتبطة بتسهيل إمكانات التنقل المُحسّنة،
- وتحديد أنواع الموازنات الأمنية المرتبطة بتحسين إمكانات التنقل وموجهات المخاطر الأخرى المحددة في هذا المبحث.

مراجع مقترحة

ستيفين أر شابينسكي، "استراتيجية الأمن السيبراني: كتاب تمهيدي لصناع السياسات وأصحاب الأدوار القيادية" *مجلة قانون وسياسة الأمن الوطني 4*، رقم 27 (أغسطس 2010): 27–39. http://jnslp.com/wp-content/uploads/2010/08/04_Chabinsky.pdf

وينكي لي وبو روتولوني *تقرير التهديدات السيبرانية الناشئة 2015*، تقرير مُعد بواسطة مركز أمن المعلومات في جامعة جورجيا تك للتكنولوجيا (GTISC) ومعهد بحوث جورجيا التقنية (GTRI) لقمة الأمن السيبراني بجامعة جورجيا تك، 2014. https://www.gtisc.gatech.edu/pdf/Threats_Report_2015.pdf

لويس مارينوس، *الوكالة الأوروبية لأمن الشبكات والمعلومات نظرة عامة على تهديدات 2013: نظرة عامة على التهديدات السيبرانية الحالية والناشئة*، الوكالة الأوروبية لأمن الشبكات والمعلومات، 11 ديسمبر 2013، الرقم الدولي المعياري للكتاب 978-92-79-00077-5. http://www.enisa.europa.eu, doi:10.2788/14231

مارك ماتسكي، وكاسندرا إم تريفينو، وسينثيا كيه فيتش، وجون ميكاليسكي، وجيه مارك هاريس، وسكوت ماروكا وجيسون فراي، *مقاييس التهديدات السيبرانية*، مختبرات ساندیا الوطنية، مارس 2012. http://fas.org/irp/eprint/metrics.pdf

فرانشيسكا سبيناليري، *مؤسسات التعليم العسكري المهنية المشتركة في عصر التهديدات السيبرانية*، مركز بيل للعلاقات الدولية والسياسة العامة، جامعة سالف ريجينا، أغسطس 2013.

مكتب مدير الاستخبارات الوطنية الأمريكي, *فهم التهديدات السيبرانية: دليل الشركات الصغيرة والمتوسطة*، محلل مجتمع الاستخبارات، برنامج القطاع الخاص، 2014.

معايير الأيزو بشأن تقييم/إدارة المخاطر.

T2-B1: سلسلة التوريد/الموردين

الوصف

تتناول هذه اللبنة مواطن الضعف في سلسلة التوريد وتطرح مفهوم الممارسات الفضلى في إدارة مخاطر سلسلة التوريد (SCRM).

تعتبر سلسلة التوريد برمتها نقطة ضعف معروفة، بل إن رصد وتأمين سلاسل التوريد يُعد أمرًا في غاية الصعوبة في السوق العالمي. وتشمل التحديات الأمنية لسلسلة التوريد السلامة والجودة وضمان الأمن فضلاً عن الحيلولة دون وقوع حالات التعطل واستغلال الثغرات وهجمات المتابعة. كما تشمل سلاسل التوريد العالمية المسارات التي تسلكها المعدات الحساسة من مرحلة الإنتاج حتى الشحن، لكل من المكونات المفردة والمنتجات النهائية مثل الأجهزة والبرامج. وتعتبر سلاسل التوريد عرضة للإخلال: يمكن اعتراض المنتجات والتلاعب بها وإدخال عناصر معيبة أو رموز خبيثة على مختلف مراحل التصنيع أو الشحن أو التخزين أو التثبيت أو التصليح ويمكن استخراج البيانات القيّمة أثناء عملية التخلص. وبهذا، يمكن أن يحدث التلاعب في أي مكان من دورة حياة المنتج. كما يمكن أن تتعرض العُقد الأخرى في البنية التحتية المؤسسية أو الوطنية للخطر عبر سلسلة التوريد أو المُوردين مما يسفر عن انتهاكات غير عادية. هل يمكن لمقدمي الخدمات لديك ضمان الأمن الكافي؟ ما الذي يتعين فعله لتحقيق الأمن عبر سلسلة التوريد برمتها؟

نتائج التعلم

سيتمكن الطلاب من

- الإلمام بالتحديات الرئيسية المتعلقة بدورة حياة المنتجات، من بدايتها إلى نهايتها؛
- شرح الدور الذي تلعبه إدارة التكوين (أي تصميم النظام) فيما يتعلق بأمن سلسلة التوريد؛
- وفهم دور ومتطلبات السياسات والممارسات الموضوعة لإدارة مخاطر سلسلة التوريد.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

- مواطن ضعف سلسلة التوريد أمام الجريمة والجاسوسية السيبرانية
- النُهج وأفضل الممارسات بشأن التخفيف من المخاطر
- ممارسات وسياسات التخفيف الوطنية القائمة للحد من مخاطر سلسلة التوريد

طريقة/تقييم التعلم

يمكن أن يتضمن أسلوب التدريس محاضرات ودراسات حالة للانتهاكات والعواقب.

مهمة فردية: حدد مثالًا على أحد انتهاكات سلسلة التوريد واذكر العلاجات الممكنة.

ممكن: قم بتخطيط سلسلة إمداد وتحديد مناطق الخاطر.

المراجع

إيه سوكولوف، في ميسروبيان، إيه تشولوك، إيه، آجي، "الأمن السيبراني لسلسلة التوريد: توقعات روسية،" *تكنوفيشن: مجلة دولية للابتكار التقني وريادة الأعمال*. 2014. المجلد 34، رقم 7؛ لعام 2014؛ 389-391. الرقم التسلسلي المعياري الدولي للمجلة: 4972-0166. رقم الرف في المكتبة البريطانية: 8761.150000. رقم المُعرِّف الفريد: ETOCRN353289650.

فلورين غورغي فيليب، لومينيتا دوتا، "أنظمة دعم القرار في إدارة سلسلة التوريد العكسية"، ورقة من إيلسيفير، 2015. رقم المُعرِّف الفريد: ETOCvdc_100030799942.0x000001.

ديميتري إيفانوف، ألكسندر دولجوي، بوريس سوكولوف، بوريس، فرانك فيرنر، مارينا إيفانوفا، "نموذج ديناميكي وخوارزمية لجدولة سلسلة التوريد قصيرة الأجل في صناعة المصانع الذكية 4.0" في*المجلة الدولية لبحوث الإنتاج*،المجلد 54، العدد 2، (2016)؛ 2016؛ الصفحات 386-402. الرقم التسلسلي المعياري الدولي للمجلة: 7543-0020. (إلكتروني). رقم الرف في المكتبة البريطانية: المتجر الرقمي ELD 4542.486000. رقم المُعرِّف الفريد: ETOCvdc_100031962439.0x000001

جيه ستيبانوفيتس، وآخرون "OpenMETA: سلسلة أدوات التصميم القائم على النماذج والمكونات للنظم السيبرانية-المادية"، في مجلة علم الدلالة المتعلق بالبيانات. رقم 8415، (2014)، الصفحات 235-248. الرقم التسلسلي المعياري الدولي للمجلة: 0302-9743. رقم المُعرِّف الفريد: ETOCRN350535700.

تيانبو لو، وزياوبو جو، وبنج شو، ولنجيلنج تشاو، ويونج بينج وهونجيو يانج. "الشيء الكبير القادم في البيانات الضخمة: أمن سلسلة التوريد في مجال تكنولوجيا المعلومات والاتصالات." في الحوسبة الاجتماعية (سوشالكوم)، 2013 المؤتمر الدولي، الصفحات 1066-1073. IEEE, 2013.

جون بوينز، سيليا بولسن، راما مورثي ونااديا بارتول، إدارة مخاطر سلسلة التوريد لمنظمات ونظم المعلومات الفيدرالية، منشور خاص من المعهد الوطني للمعايير والتقنية 161-800، مسودة عامة ثانية، وزارة التجارة الأمريكية، واشنطن العاصمة، 2014.

ستيفين أر شابينسكي، "استراتيجية الأمن السيبراني: كتاب تمهيدي لصناع السياسات وأصحاب الأدوار القيادية" *مجلة قانون وسياسة الأمن الوطني 4*، رقم 1 (2010): 27.

تراستيد كمبيوتنج جروب بيان حقائق. 2009. http://www.trustedcomputinggroup.org/files/resource_files/7f38fa36-1d09-3519-add14cb3d28efea6/fact%20sheet%20May202009.pdf

لوكا أورسيولي وتوني مانيستو وجوها هينتسا وتامانا خان. "الأمن السيبراني لسلسلة التوريد - التهديدات المحتملة،" *المعلومات والأمن: مجلة دولية 29*، العدد 1 (2013): 51–68. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf

مكتب مساءلة الحكومة الأمريكية، "معالجة المخاطر الأمنية المحتملة للمعدات المصنعة في الخارج"، شهادة مارك إل جولدشتاين، مدير قسم قضايا البنية التحتية المادية، أمام اللجنة الفرعية المعنية بالاتصالات والتكنولوجيا، لجنة الطاقة والتجارة، مجلس النواب الأمريكي، مكتب مساءلة الحكومة الأمريكية، GAO-13-652T، 21 مايو 2013. http://www.gao.gov/assets/660/654763.pdf

T2-B2: هجمات الوصول عن بعد أو الوصول عن قرب

الوصف

يمكن افتراض أن الهجمات السيبرانية إما أن تكون عن بعد أو محلية. ومع ذلك، يمكن تصنيف الهجمات المحلية على أنها تلك التي يتم إجراؤها من خلال الوصول عن قرب إلى الأنظمة أو من خلال شخص موثوق من الداخل. ويتم تناول الهجمات من الداخل في اللبنة T2-B3. يُشير الوصول عن بعد إلى جميع الأساليب والنهج التي يتم اتخاذها للوصول إلى الشبكات أو تعطيلها عندما لا يكون هناك وصول مادي واضح إلى أجهزة النظام. وفي الهجوم عن بعد، قد لا يكون المهاجم قد قام بأي وصول مادي مسبق للنظام قيد الهجوم؛ يكون وصول المهاجم عبر شبكة أو جهاز اتصال آخر وقد لا يكون للمهاجم أي امتيازات قائمة سابقًا على النظام. وعلى العكس من ذلك، في الهجمات المحلية، يتمتع المهاجم بشكلٍ عام ببعض أشكال الوصول أو الامتيازات القائمة في النظام ويحاول زيادة مستوى الامتياز الخاص به لتحقيق الوصول غير المصرح به إلى المعلومات. وفي هذه الوثيقة، سنتناول هذا النشاط الذي تقوم به جهة خبيثة فاعلة ليست شخصاً موثوقاً من الداخل باعتباره إحدى هجمات الوصول عن قرب. وكما يوضح شابينسكي (2010)، يشير "الهجوم القائم على الوصول عن قرب" إلى قدرة جهة خبيثة فاعلة على تعطيل أو اعتراض أو الوصول بخلاف ذلك إلى الشبكات وأنظمة الحاسوب في حين أنه يكون بالقرب من مكوناتها المختلفة، مثل محطات العمل والكابلات أو أجهزة الاستقبال اللاسلكية. ويُعد الوصول عن قرب شكل من أشكال الوصول عن بعد. ومن الطرق التي يمكن للمهاجمين الوصول عن قرب من خلالها لاستغلال نقاط الضعف، التقنيات المشتركة مثل "التعرف" اللاسلكي (اعتراض المعلومات المرسلة عبر الشبكات اللاسلكية والوصول إليها) وتسجيل النقرات على لوحة المفاتيح والتقاط الشاشة واعتراض الدخيل وإدخال تعليمة برمجية ضارة من خلال الوسائل المادية.

تتناول هذه اللبنة هجمات الوصول عن قرب والوصول عن بعد (تلك التي ليست هجمات من الداخل). وتهدف هذه اللبنة إلى تسليط الضوء على المخاطر المعروفة الأكثر شيوعاً التي ترتبط بهجمات الوصول عن بعد والوصول عن قرب، وتناقش وسائل مختلفة لتخفيف أو إحباط هذه المحاولات.

الخلفية

في تطبيقات الشبكة الكلاسيكية، هناك مفهوم خاص ببرنامج العميل والخادم. ويرسل التطبيق البرمجي "العميل" طلبات إلى التطبيق البرمجي "الخادم" وفقا لبعض البروتوكولات، حيث يطلب منه الحصول على معلومات أو تنفيذ إجراء. ودائمًا ما يبدأ تطبيق العميل بالاتصال. ودائمًا ما ينتظر تطبيق الخادم حتى يتلقى اتصالاً على بعض العناوين المعروفة على الشبكة. وتتضمن البروتوكولات التي تتحكم في هذا السلوك خدمات الويب (HTTP أو HTTPS) وخدمات نقل الملفات (FTP) وخدمات البريد الإلكتروني (SMTP أو POP3 أو IMAP). ويمكن أن تستهدف الهجمات عن بعد نقاط الضعف في الخادم (البرامج أو أخطاء التكوين) التي تسمح للمهاجم بالوصول إلى المعلومات من حاسوب الخادم أو حتى التحكم فيه عن بعد.

ويمكن القيام بهجمات عن بعد من جانب الخادم إذا كان المهاجم يستطيع تحديد التكوين الخاطئ أو الخطأ في البرامج المطبَّقة على الخادم. فعلى سبيل المثال، قد يعمل الخطأ في إعدادات التكوين على السماح للمهاجم بإدخال وضع محجوز لصيانة النظام بشكل غير مناسب، وبالتالي الوصول إلى النظام على نطاق واسع للغاية. وهناك مثال آخر يتمثل في الهجوم على خادم ويب HTTP يستخدم قاعدة البيانات الموجودة على الخادم لتوفير موارد البيانات الخاصة به. ويمكن لطلبات صفحة الويب المفحوصة بشكل غير سليم والقادمة من المهاجم أن تسمح للمهاجم بتمرير سلاسل أوامر خطيرة بقاعدة البيانات إلى قاعدة البيانات الموجودة على الخادم؛ وهذا يمكن أن يمنح المهاجم التحكم في قاعدة البيانات. ويُسمى هذا النمط من الهجوم "حقن لغة الاستعلامات المركبة (SQL)".

وقد أدى ظهور حماية أفضل للخوادم (جُدُر الحماية والتحكم في الوصول وما إلى ذلك) إلى تحويل تركيز الهجوم من الخادم إلى تطبيقات العميل. ومع ذلك، لا يمكن الاتصال بتطبيقات العميل مباشرةً على الشبكة؛ دائمًا ما تكون تطبيقات العميل هي التي تبدأ بتبادل الاتصالات. وبدلا من ذلك، يجب على المهاجم إيجاد طريقة لإغراء مستخدم تطبيق العميل من أجل الاتصال بخادم خبيث قد يتلف تطبيق العميل خلال التبادل. وتُعد أنشطة الإغراء أو الإفخاخ هذه، المشار إليها بمجموعة متنوعة من الأسماء، ذرائع مختلفة تستخدم مبادئ الهندسة الاجتماعية لإقناع المشغل بالقيام بسلوكيات مثل فتح مرفق بريد إلكتروني مصاب.

نتائج التعلم

يتمثل الهدف الرئيسي من هذه اللبنة في ضمان تعرف الطلاب على مجموعة المخاطر المرتبطة بهجمات الوصول عن بعد والوصول عن قرب.

سيتمكن الطلاب من

- استيعاب وامتلاك القدرة على وصف سيناريو الهجوم القائم على الوصول عن بعد وتحديد الأجزاء المكونة لهذا الهجوم ومقارنته بسيناريوهات الهجوم القائمة على الوصول عن قرب؛
- معرفة بنية التطبيقات القائمة على خادم العميل وطوبولوجيا الشبكة الخاصة بهم والتمتع بالقدرة على تحديد مدى تناسب البروتوكولات الشائعة مثل HTTP وHTTPS وبروتوكول نقل الملفات وبروتوكولات البريد الإلكتروني مع هذا النموذج؛
- التمتع بالقدرة على وصف كيفية الاستفادة في الهجمات من جانب الخادم من خلال مرحلة جمع المعلومات باستخدام تقنيات مثل أدوات تحليل تعرض الشبكة للخطر والاختبار العشوائي والتمتع بالقدرة على شرح الأسباب الكامنة وراء كون أدوات تحليل تعرض الشبكة للخطر قيِّمة لكلٍ من المهاجم والمدافع؛

- امتلاك معرفة أولية عن سيناريوهات الهجوم من جانب الخادم مثل استغلال التكوينات الضعيفة وانتحال IP ورفض الخدمة ورفض الخدمة الموزع (DoS وDDoS) وحقن SQL وتجاوزات المخزن المؤقت القائم على بروتوكول الشبكة؛
- القدرة على وصف كيف أدى نضوج الأمن في محيط الشبكة وتحسين أمن الخادم إلى تطوير وانتشار تقنيات الهجوم من جانب العميل؛
- امتلاك معرفة أولية حول سيناريوهات الهجوم من جانب العميل مثل البرمجة عبر المواقع وتزوير الطلب عبر المواقع واستغلال المتصفح الإلكتروني ووثائق طروادة؛
- والقدرة على تحديد ومناقشة العلاقة بين الهجمات من جانب العميل وتقنيات الهندسة الاجتماعية مثل هجمات التصيد الاحتيالي وهجوم سقي الحفرة.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

- قد يحتاج عمق التغطية الفنية إلى أن يتباين بشكل كبير، نظرًا لضيق الوقت والخلفية الفنية للطلاب.
- استكشاف أنواع مختلفة من الهجمات التي تستخدم طرق الهندسة الاجتماعية

طريقة/تقييم التعلم

قد يتضمن التدريس إلقاء محاضرات وعروض توضيحية. ويمكن أن تتناول العروض التقديمية التي يقدمها مسؤولو الشبكة الحاليون التهديدات الدائمة والمستمرة. وينبغي توليد وتحديد أمثلة وطنية حقيقية لتوضيح المسائل العملية والمباشرة. كما ينبغي وضع العديد من تدابير التقييم العملي، تبعًا لمستوى العمق الذي يُتوقع أن يصل إليه الطلاب.

المراجع

إيمانويل ترانوس وبيتر نيجكامب وكريمة كورتيت "إعادة النظر في القضاء على المسافات: الفضاء السيبراني، أوجه التقارب المادية والعلائقية"، مجلة العلوم الإقليمية، المجلد 53، العدد 5، لعام 2013. الرقم التسلسلي المعياري الدولي للمجلة: 1467-9787.

إي أنيفرو، "القومية السيبرانية: المجتمع الكاميروني المُتصور الناطق بالإنجليزية في الفضاء السيبراني"، في الهويات الأفريقية، المجلد 6، العدد 3، (2008)، الصفحات 253-273. الرقم التسلسلي المعياري الدولي للمجلة: 1472-5843. رقم الرف في المكتبة البريطانية: 0732.501500. رقم المُعرِّف الفريد: ETOCRN234554771

أيه ألمالاوي، إكس يو، زِد تاري، أيه فهد، آي خليل، "نهج الكشف القائم على الانحراف غير الخاضع للرقابة بالنسبة لهجمات التكامل على أنظمة SCADA"، في أجهزة الحاسوب والأمن. المجلد 46، (2014)، الصفحات 94-110. الرقم التسلسلي المعياري الدولي للمجلة: 0167-1048 . رقم الرف في المكتبة البريطانية: 3394.781000. رقم المُعرِّف الفريد: ETOCRN359669860.

واي لي، إل شي، جيه تشينغ، دي أيه كويفيدو، "هجمات التشويش على تقدير الدولة عن بعد في الأنظمة المادية السيبرانية: النهج النظري القائم على اللعبة"، معاملات IEEE بشأن التحكم التلقائي. المجلد 60؛ العدد 10، لعام 2015. الرقم التسلسلي المعياري الدولي للمجلة: 0018-9286. رقم المُعرِّف الفريد: ETOCRN375325720.

ستيفين أر شابينسكي، "استراتيجية الأمن السيبراني: كتاب تمهيدي لصناع السياسات وأصحاب الأدوار القيادية،" *مجلة قانون وسياسة الأمن القومي 4*، العدد 1 (2010): 27.

شيرلي راداك، محرر، *مجلة مختبر تكنولوجيا المعلومات: إدارة السجلات: استخدام سجلات الحاسوب والشبكة في تحسين أمن المعلومات*، 1، 2 (أكتوبر 2006)، المعهد الوطني للمعايير والتقنية، إدارة التكنولوجيا، وزارة التجارة الأمريكية. http://csrc.nist.gov/publications/nistbul/b-10-06.pdf

موروجيا سوبايا وكارين سكارفون، *دليل الوقاية من حوادث البرمجيات الضارة والتعامل معها فيما يخص أجهزة الحاسوب المكتبية والمحمولة*، المنشور الخاص بالمعهد الوطني للمعايير والتقنية 800-83، النسخة المنقحة 1، وزارة التجارة الأمريكية، يوليو 2013. http://dx.doi.org/10.6028/NIST.SP.800-83r1

وزارة الأمن الداخلي الأمريكية، فريق الاستعداد لطوارئ الحاسوب الأمريكي، *استخدام التكنولوجيا اللاسلكية بشكل آمن*، فريق الاستجابة للطوارئ السيبرانية الأمريكي، 2008. http://www.us-cert.gov/reading_room/Wireless-Security.pdf

T2-B3: الوصول من الداخل (هجمات الوصول المحلي)

الوصف

يستغل الهجوم القائم على الحاسوب على نظام أو شبكة المعلومات ضعف النظام أو أحد البرامج الحاسوبية لتنفيذ بعض أشكال الأعمال الخبيثة من أجل اختراق سرية المعلومات أو سلامتها أو توافرها. وهذه "الثغرات" قد يمكن اعتبارها بعيدة أو محلية. ففي الثغرات المحلية، كان المهاجمون يتمتعون بالوصول القائم مسبقًا إلى النظام قيد الهجوم، ولهذا فهم لديهم بالفعل بعض الامتيازات على النظام وتعد الهجمات محاولات لزيادة هذا المستوى من الامتيازات لتحقيق الوصول غير المصرح به إلى المعلومات. وتتناول هذه اللبنة هجمات الوصول المحلي. ويمكن أن يتسبب الأشخاص الخبثاء من الداخل الذين يستطيعون الوصول مادياً إلى العديد من الأنظمة في إحداث ضررٍ كبير للعملية أو الشركة أو المنظمة. وقد يفعلون ذلك مقابل المال أو بغرض الانتقام أو لأن لديهم ضغينة أو لأنهم معارضين للمنظمة من الناحية الأيديولوجية. ومع ذلك، فمن الممكن أيضًا إحداث خسارة أو تعطيل مماثل من خلال خطأ المشغل أو إهمال آخر.

الخلفية

"الامتياز" في أمن الحاسوب هو الإذن بإجراء عمل. في هذه الحالة، يُعد الإذن حقاً يتمتع به مستخدم معين للوصول إلى مورد نظام معين، مثل ملف أو تطبيق أو لاستخدام أوامر نظام معينة أو للوصول إلى خدمة معينة، مثل أحد أجهزة الشبكة. وعادةً ما يتم التحكم في السياسة الخاصة بالتحكم في مستوى الامتيازات التي يتمتع بها المستخدم من خلال التحقق السليم من الهوية الإلكترونية للمستخدم وتوظيف مجموعة من قواعد التحكم في الوصول (البروتوكولات) التي تحكم إجراءات القراءة والكتابة وتنفيذ البرنامج الخاصة بالمستخدم على النظام. وقد يحاول المهاجم "رفع الامتياز" والوصول إلى مزيد من المعلومات على النظام عن طريق الاستيلاء على هوية مستخدم آخر (غالباً عن طريق الاستيلاء على برنامج يتم تشغيله من قبل مستخدم يتمتع بامتيازات أعلى) أو عن طريق تعديل بروتوكولات سياسة الأمن المضمّنة. وإذا حصل المهاجمون على امتيازات كافية، يمكنهم أن يتولوا التحكم الإداري في النظام. وفي مثل هذا السيناريو، قد يكون المهاجم مستخدماً مصرحاً له باستخدام النظام - شخص خبيث من الداخل يحاول تنفيذ أعمال غير مسموح له بتنفيذها. وبدلاً من ذلك، قد يكون المهاجم شخص خارج المنظمة، ينفذ هجوماً عن بعد من أجل الاستيلاء على بيانات الاعتماد الخاصة بمستخدم يتمتع بامتيازات محدودة. ومن نقطة الوصول هذه، يمكن للمهاجم استخدام بيانات الاعتماد المسروقة لتنفيذ هجوم الوصول المحلي لرفع مستوى امتيازه، وبالتالي الحصول على وصول أوسع نطاقاً. ومن الناحية التقنية، يصعب التمييز بين هذين السيناريوهين، فهما في الأساس من قبيل هجمات الوصول المحلي وهناك تشابه بينهما في العديد من تقنيات التخفيف.

يُعد مبدأ "الحاجة إلى المعرفة"، الذي لا يتمكن فيه المستخدمون من الوصول إلا إلى المعلومات اللازمة لأداء واجباتهم الرسمية، هو أحد المبادئ الأساسية المستخدمة للحد من نقاط الضعف الخاصة بالهجوم القائم على الوصول المحلي. ويطبَّق مبدأ "الامتياز الأقل" على تصميم وتنفيذ سياسة/قواعد التحكم في الوصول لضمان وصول المستخدمين إلى الموارد التي يحتاجون إلى معرفتها فقط. وتمتد هذه الفلسفة لتشمل مبدأ "فصل الواجبات" - على سبيل المثال، ضمان عدم تمكن أحد المسؤولين من إجراء تغييرات على سياسة الأمن والموافقة أيضًا على تلك التغييرات.

يُعد التحاوز أيضًا مبدأ كلاسيكياً للحد من تأثير هجمات الوصول المحلي. ويُعد تقسيم أمن الشبكة إلى مناطق تقنية تحاوز آمنة. ويستخدم تقسيم الشبكة إلى مناطق في الحد من المخاطر من خلال تقسيم خدمات البنية التحتية إلى مجموعات منطقية تمتلك نفس سياسات أمن الاتصالات ومتطلبات الأمن. ويتم فصل المناطق باستخدام حواجز أمنية مفروضة من خلال أجهزة الشبكة والأمن (جُدُر الحماية وأنظمة IDS وبرامج منع فقدان البيانات).

وبالنظر إلى مجموعة نقاط الضعف المحددة في هذه اللبنة، ينبغي إبراز المنطق الخاص بالبرامج والإجراءات المصممة للتقليل من نقاط الضعف الكامنة في الوصول إلى النظام إلى أدنى حد باستخدام نهج الوقاية والكشف والردع. وسيجري تناول هذه التدابير بشكلٍ كامل في أماكن أخرى في هذا المنهج.

نتائج التعلم

سيتمكن الطلاب من

- إظهار الوعي بالتهديدات التي تتعرض لها المنظمة والتي قد تأتي من أفراد داخل المنظمة؛
- وصف هجمات الوصول المحلي وتحديد الأجزاء المكونة لهذا الهجوم؛
- شرح الاختلافات بين هجوم الوصول عن بعد وهجوم الوصول المحلي؛
- إثبات فهم مفاهيم الأذون والامتيازات وكيفية استخدامها للتحكم في وصول المستخدمين إلى موارد المعلومات على النظام؛
- إظهار المعرفة الأساسية بالتقنيات التي يستخدمها المهاجمون لإساءة استعمال مستويات امتيازاتهم الحالية وزيادة الامتياز؛
- شرح تطبيق مبدأ الامتياز الأقل والحاجة إلى المعرفة وكيفية استخدامهما لإنشاء سياسة الأمن؛

- وتحديد كيفية الاستخدام المناسب لسياسة تقسيم أمن الشبكة إلى مناطق من أجل تقسيم المعلومات إلى فئات صغيرة.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

- ينبغي الخروج من هذه اللبنة بنبذة عن جميع السياسات والبرامج المتعلقة بتدريب الموظفين والفحص والتخفيف من التهديدات والتوعية العامة بالمشاكل الكامنة في الوصول المادي إلى النظم والمكونات، ولكن يمكن دراستها بمستويات مختلفة من التفصيل.
- قد يكون العمل من خلال أمثلة واقعية ووطنية وسيلة جيدة لإشراك الطلاب في هذا الموضوع.
- يمكن مناقشة الأدوات المتعلقة باكتشاف وجود التهديدات النشطة في الشبكة وتمييز خصائصها.

طريقة/تقييم التعلم

يُوصى بإلقاء محاضرات وعروض توضيحية تستند إلى الأمثلة.

وينبغي مناقشة دراسات الحالة والسيناريوهات النموذجية والفحص العدلي للحالات الفعلية.

تمرين متقدم محتمل: اطلب من الطلاب، الذين يعملون في مجموعات، العثور على مثال واقعي لهجوم خبيث من الداخل وتحليله واقتراح أساليب يمكن من خلالها تجنب التهديدات. يمكن للطلاب العمل من خلال مثال على شخص خبيث من الداخل يقوم بإساءة استعمال الامتيازات الممنوحة له لاختراق الموارد التي ليس لديه حق الوصول إليها استناداً إلى الحاجة إلى المعرفة.

يجب أن تعتمد أساليب التقييم على مستوى المعرفة التي سيُطلب من الطلاب إظهارها وفقًا لأهداف التعلم والأداء المطلوبة للدورة التدريبية الخاصة التي قد يكونوا فيها.

المراجع

ماركوس كونت، ماونو بيهلجاس، جيسي فوجتكوياك، لورينا ترينبرغ، آنا-ماريا أوسولا، مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو، تالين، 2015 "دراسة كشف التهديدات من الداخل". متوفر على: https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf

بي جولا وجي ورونكا، دليل حماية بيانات الموظف، المبادئ التوجيهية القانونية والإجرائية للممارسة التشغيلية، الطبعة 5، كولونيا، 2009

إف شواند "عندما يستخدم موظفو الشركة أجهزة الحاسوب المحمولة الخاصة، لا بد من تنظيمها،" شركة أكانت سيرفيس جي إم بي إتش، 23 أبريل 2014 [عبر الإنترنت]. متوفر على: http://www.acantmakler.de/2014/04/23/unternehmen-laptops-private-nutzung/ [تم الوصول إليه في 14 سبتمبر 2015]

تفتيش حماية البيانات الإستونية (التفتيش على حماية البيانات)، معالجة البيانات الشخصية في علاقات العمل،" 2011. [عبر الإنترنت]. متوفر على: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhe58tes%20juhendmaterjal26%2005%202014_0.pdf [تم الوصول إليه في 16 يوليو 2015]

البرلمان الألماني "مشروع قانون لتنظيم حماية بيانات الموظف،" 15 ديسمبر 2010. [عبر الإنترنت]. متوفر على: http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf

مركز حماية البنية التحتية الوطنية، "إساءة استخدام أنظمة تكنولوجيا المعلومات من الداخل"، مايو 2013. https://www.cpni.gov.uk/documents/publications/2013/2013008-insider-misuse_of_it_systems.pdf?epslanguage=en-gb وانظر أيضًا "الهجمات السيبرانية من الداخل،" https://www.cpni.gov.uk/advice/cyber/Cyber-research-programmes/Cyber-insiders/

مؤسسة أمن الاتصالات الكندية، *المبادئ التوجيهية لأمن تكنولوجيا المعلومات: تقسيم أمن الشبكة إلى مناطق: اعتبارات التصميم فيما يتعلق بوضع الخدمات داخل المناطق* (ITSG-38), مايو 2009. https://cse-cst.gc.ca/en/system/files/pdf_documents/itsg38-eng_0.pdf

بي أيه ليج وآخرون، "نحو نموذج مفاهيمي وهيكل عقلاني للكشف عن التهديد من الداخل،" مركز الأمن السيبراني، إدارة علوم الحاسوب، جامعة أوكسفورد، 2013. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-insider_threat_detection.pdf?epslanguage=en-gb

جاسون إر سي نيرس وآخرون، "فهم التهديد من الداخل: إطار عمل خاص بتمييز الهجمات،" *ورش عمل الأمن والخصوصية لعام 2014 لدى IEEE*. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-understanding_insider_threat_framework.pdf?epslanguage=en-gb أو http://www.ieee-secrity.org/TC/SPW2014/papers/5103a214.pdf

إس ساجان وإم بون، *دليل الممارسات الأسواء المؤدية إلى التهديدات من الداخل: الدروس المستفادة من الأخطاء الماضية* (كامبريدج بولاية ماساتشوستس: الأكاديمية الأمريكية للعلوم)، 2014، رقم الرقم الدولي المعياري للكتاب 3-097-87724-0. https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderthreats.pdf

ديريك أيه سميث، معهد الأمن السيبراني الوطني، "التهديد من الداخل،" فيديو. https://www.youtube.com/watch?v=z-CDyZdcGck

وزارة الدفاع الوطني الأمريكية، *دليل الأمن الإداري للمعلومات الحساسة المقسمة (SCI): إدارة أمن الموظفين والأمن الصناعي والأنشطة الخاصة* دليل وزارة الدفاع 5105.21-V3، 19 أكتوبر 2012. http://www.dtic.mil/whs/directives/corres/pdf/510521m_vol3.pdf

شركة فيرايزون للاتصالات، "تقرير تحقيقات خرق البيانات 2015". www.verizonenterterprise.com

ورشة عمل للفريق المعني بكتابة المنهج المرجعي للأمن السيبراني في غارميش (المساهمون من جمهورية التشيك، والمملكة المتحدة، والولايات المتحدة).

T2-B4: مخاطر التنقل وسياسة BYOD والاتجاهات الناشئة

الوصف

يُعد التحول المجتمعي إلى الاتصالات المتنقلة أمر لا رجعة فيه، كما أن تداعياته الأمنية يعوزها الفهم. بالإضافة إلى ذلك، يعمل ظهور وسائل الإعلام الاجتماعية مثل Facebook وTwitter على تحويل الاتصالات الشخصية والعالمية. وتشكل البصمات الرقمية للأفراد والمنظمة والوصول الموزع من الأجهزة الشخصية غير الآمنة إلى الأنظمة التي قد تكون مرتبطة بأنظمة آمنة وشركات النقل التجارية وسلسلة التطورات المماثلة والحديثة مخاطر على البيانات والأنظمة الحساسة. فعلى سبيل المثال، قد يؤدي فقدان أو سرقة جهاز حاسوب محمول أو هاتف جوال مزود باتصالات أو مستندات أو اختصارات إلكترونية إلى الإضرار بفرد أو منظمة أو شركة أو بلد ما. وتتناول هذه اللبنة مسائل الأمن المتعلقة بهذه الاتجاهات.

"أحضر جهازك الخاص" (BYOD) هي السياسة التي تتضمن السماح للموظفين بإحضار الأجهزة المحمولة الخاصة بهم (أجهزة الحاسوب المحمولة والحاسوب اللوحي والهواتف الجوالة) إلى أماكن عملهم واستخدام هذه الأجهزة، أثناء عملهم، للوصول إلى المعلومات والتطبيقات المتميزة. وتخلق هذه السياسة توترًا بين المنظمة التي تهدف سياساتها الأمنية إلى التحكم في سرية وسلامة موارد معلوماتها والموظفين الذين يرغبون في الحفاظ على ملكية الجهاز والبيانات الشخصية وحماية أنفسهم من المراقبة. ويجب على المنظمات وضع سياسات وممارسات للمواقف التي تتضمن ترك الموظف وظيفته أو فقدان الجهاز أو سرقته أو بيعه ولضمان عدم استخدام الأجهزة غير المؤمنة من قبل المهاجمين للوصول إلى أنظمة المؤسسة من خلال الشبكة. يشكل استخدام "السحابة" لتخزين البيانات مشاكل مماثلة خاصة بالتحكم في الوصول والتكوين.

الخلفية

تتمثل الممارسة الأمنية الشائعة للمؤسسات في بناء بنية أمنية محددة المناطق بعناية، وتوفير "نقاط اختناق" خاضعة للتحكم من أجل إدارة الدخول إلى الإنترنت. وتقدم سياسة BYOD للأجهزة المزودة بخدمات الإنترنت نقاط وصول جديدة لا يُرجح أن تخضع لسيطرة سياسة أمن المؤسسة. ويُعد من المبادئ الأساسية التي تتعلق بأمن الحاسوب أنه في نظام الحاسوب عادةً ما تُعامل سلامة المستويات الأقل على أنها بديهية من قِبل المستويات الأعلى. وهذا يمنع من أن تُطبّق على الجهاز الشخصي سياسات الأمن الخاصة بتطبيقات المؤسسة التي لا يمكن تدميرها من قبل الشخص الذي يسيطر على نظام تشغيل BYOD، وعادة ما يكون هو المالك. وبعبارة أخرى، قد لا يتم تثبيت أنظمة أمن المؤسسة (التطبيقات وما إلى ذلك) على الأجهزة الشخصية بشكل ثابت، حيث يحتفظ المالك بالتحكم الإداري النهائي في الجهاز. ولا يمكن أن يتم تأمين جهاز غير آمن، مثل الهاتف الذكي الشخصي، من خلال مجرد تثبيت تطبيقات آمنة أو أدوات أمن. وهناك عدد من الممارسات التي يمكن أن تجعل الأجهزة الشخصية أكثر أمنا أو تحد من المخاطر التي تشكلها. وتعتمد هذه الممارسات على بنية الأمن للحد من وصول الجهاز إلى شبكة المؤسسة والحد من المعلومات التي يمكن نقلها إلى الجهاز. ويمكن أن تعمل سياسات تقسيم المناطق التي توفر تجزئة الشبكة وفصلها على تمكين تنفيذ تنقل القوى العاملة واستراتيجية آمنة نسبياً لأنظمة BYOD. ومع ذلك، توجد حلول أكثر أمنًا تتعارض مع إمكانية استخدام الأجهزة الشخصية.

بالإضافة إلى ذلك، يؤدي التحول إلى استخدام البنية التحتية المقدمة كخدمة من خلال التقنيات السحابية إلى فقدان محتمل للسيطرة على البنية الأمنية الأساسية والممارسات الأمنية. وتخلق الأجهزة المحمولة نفسها تدفقات بيانات قد تكون ذات أهمية لكل من وكالات الاستخبارات الأجنبية والكيانات التجارية. كما أن استخدام وسائل التواصل الاجتماعي يُعرِّض الأفراد لاستغلال المعلومات التي أفصحوا عنها والتي يتم الوصول إليها أو تخزينها على أجهزتهم المحمولة، مما يُعرِّض للاختراق المحتمل ثروة من المعلومات التي يُحتمل أن تكون خطرة فيما يتعلق بالعلاقات والآراء والمواقع والعادات. وقد تعمل وسائل التواصل الاجتماعي هذه أيضًا كموجهات تهديد عن طريق العمل كقناة تؤدي إلى مختلف نظم تكنولوجيا المعلومات، مما يجعلها عرضة للإصابة أو التسلل. وقد تكون وسائل التواصل الاجتماعي أيضا قناة مفيدة لنشر الدعاية والتضليل والتعهيد الجماعي والرسائل الجماعية بغرض حشد الجمهور والأنشطة المماثلة.

نتائج التعلم

سيتمكن الطلاب من

- إظهار الفهم للجوانب الإيجابية والسلبية للموازنات في سياسة الأمن المتعلقة باستخدام وسائل الإعلام الاجتماعية في بيئة المؤسسة من وجهة نظر الموظف وصاحب العمل؛
- تحليل التنقل وسياسات BYOD في سياق البنية الأمنية للمؤسسات وتحديد الموازنات الأمنية وإمكانية الاستخدام؛
- وتحليل سياسات الحوسبة السحابية فيما يتعلق بتخزين المعلومات ومعالجتها (مثل السجلات الصحية والبيانات الحكومية/العسكرية) في السياقات الوطنية والدولية.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

- سيتم التعامل مع قدرات جهات التهديد الفاعلة على المستوى المناسب من التفاصيل للجمهور المحدد.
- خلق وعي بالحاجة إلى إمكانية تكييف الأمن مع التكنولوجيا المتغيرة باستمرار.
- المتطلبات والقيود الفريدة المفروضة على منصات الاتصالات المتنقلة، بما في ذلك نظام BYOD.
- المتطلبات والقيود الفريدة المفروضة على الاستخدام السحابي.
- إنشاء واعتماد أفضل الممارسات في بيئة المؤسسة، استنادًا إلى التوجيهات الوطنية والدولية.
- استغلال المعلومات الشخصية التي تتم مشاركتها على مواقع التواصل الاجتماعي - "هل قمت بالبحث اليوم عن اسمك باستخدام محرك البحث جوجل؟" المناقشة والتمرين.

طريقة/تقييم التعلم

قد يشمل التدريس العروض التقديمية والمناقشات داخل الفصل والمجموعات الفرعية ومناقشة دراسات الحالة.

ينبغي إجراء تقييم مستمر لأداء المناقشة في الفصل والمناقشة الجماعية والمشاركة فيها.

المراجع

إن ماستالي وجي أي أجبينيا، "التحقق من الموضوعات والأجهزة باستخدام المقاييس الحيوية ونظم إدارة الهوية فيما يخص الحوسبة المتنقلة الإقناعية: ورقة دراسة استقصائية"، في المؤتمر الدولي الخامس بشأن الاتصالات واسعة النطاق والطب الأحيائي لعام 2010 (2010 IB2Com).

إتش كاركاينين "شركة أبل تبيع الهواتف في فنلندا بشكل خطير - وتغلق أفواه تجار التجزئة"، 30 أكتوبر 2014. [عبر الإنترنت]. متوفر على: http://www.digitoday.fi/tietoturva/2014/10/30/-apple-myy-suomessa-vaarallisia-puhelimia--ja-sulkee-kauppiaiden-suut/201415103/66. [تم الوصول إليه في يوليو 2016]

تيمو فايسانن، أليكساندريا فارار، نيكولاوس بيسانيديس، كريستيان براكسيني، برناردز بلومبرجس، وإنريك ديز. مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو، تالين، 2015 "الدفاع عن الأجهزة المحمولة الخاصة بالمسؤولين رفيعي المستوى وصناع القرار". متوفر على: https://ccdcoe.org/sites/default/files/multimedia/pdf/Defending%20mobile%20devices%20for%20high%20level%20officials%20and%20decision-makers.pdf

جابريل كوستا، ميرلو أليسيو، لوكا فيرديرام، كونراد ورونا، "تطوير سياسة أمن BYOD الخاصة بحلف الناتو"، المؤتمر الدولي للاتصالات العسكرية ونظم المعلومات (ICMCIS) 2016. IEEEm بروكسل، بلجيكا، 24-23 مايو 2016. معرّف الوثيقة الرقمي: 10.1109/ICMCIS.2016.7496587. متوفر على: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=7496587&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7496587

ري سي هو، هيانغ كيه تشوا، "تأثير التعلم النقال على قدرة المتعلم الاستيعابية: حالة بيئة التعلم الخاصة بنظام أحضر جهازك الخاص (BYOD)"، في *وقائع 2014 لمؤتمر تايلور السابع للتعليم والتعلم*، سنغافورة: سبرنجر، 2015. الصفحات 479-471. 2015. معرّف الوثيقة الرقمي: 10.1007/978-981-287-399-6_43. الرقم الدولي المعياري للكتاب المطبوع: 978-981-287-398-9. الرقم الدولي المعياري للكتاب عبر الإنترنت: 978-981-287-399-6.

نيرانجان سوري وماورو تورتونيسي وجيمس ميكايلس وبيتر بودولاس وجياكومو بينينكاسا وستيفن راسل وسيزار ستيفانيلي وروبرت وينكلر. "تحليل إمكانية تطبيق إنترنت الأشياء على بيئة ساحة المعركة." في المؤتمر الدولي للاتصالات العسكرية ونظم المعلومات لعام 2016 (ICMCIS)، الصفحات 8-1. IEEE, 2016.

بورش الثالث، إسحاق أر. التهديدات والآثار السيبرانية الناشئة. مؤسسة راند، 2016.

دبليو أربوغ ودي فاربر وجيه سميث، "بنية تحضيرية آمنة وموثوق بها،" *وقائع ندوة IEEE بشأن الأمن والخصوصية لعام 1997* (أوكلاند، كاليفورنيا) 1997، 71-65.

دي بي كورنيش، "الأمن السيبراني والهجمات السيبرانية ذات الدوافع السياسية والاجتماعية والدينية"، سياسة المديرية العامة للاتحاد الأوروبي - للسياسات الخارجية لمديرية الاتحاد [الأوروبي] ب، فبراير 2009. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

رافي جوبتا وهيو بروكس، *استخدام وسائل التواصل الاجتماعي فيما يتعلق بالأمن العالمي* (إنديانابوليس، إنديانا: جون وايلي أند سنز)، 2013، الرقم الدولي المعياري للكتاب 978-1-118-44231-9.

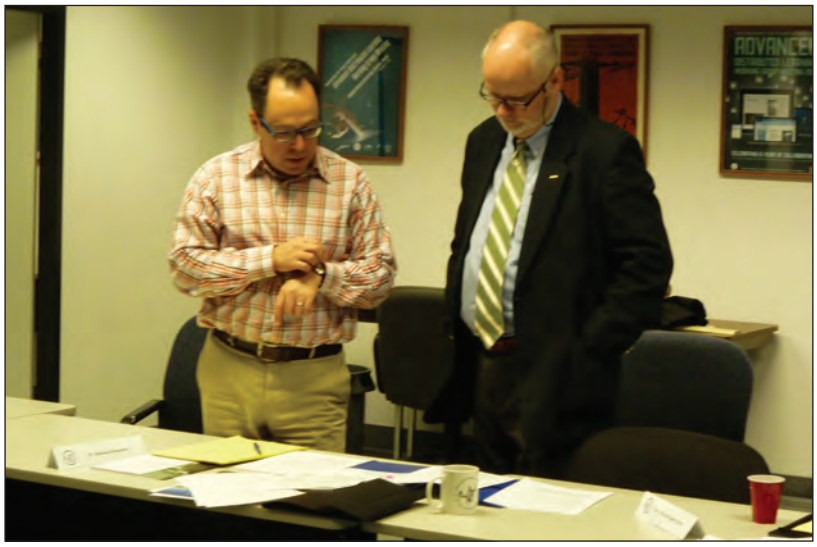
زيب هالوك وآخرون، *تصميم سيسكو المصدق عليه بشأن الوصول الموحد (UA) ونظام إحضار الأجهزة الشخصية في مكان العمل (BYOD) لدى شركة سيسكو*، سيسكو سيستمز إنك، تم التنقيح في 28 أغسطس 2014، تم الوصول إليه في 30 يوليو 2015. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.pdf

شركة رايثيون، *الأمن في النظام البيئي النقال الجديد*، تقرير بحوث معهد بونيمون، أغسطس 2014.

موروجياه سوبايا وكارين سكارفون، *المبادئ التوجيهية لإدارة أمن الأجهزة المحمولة في المؤسسة*، منشور خاص بالمعهد الوطني للمعايير والتقنية 124-800، النسخة المنقحة 1، المعهد الوطني للمعايير والتقنية، وزارة التجارة الأمريكية، يونيو 2013. http://dx.doi.org/10.6028/NIST.SP.800-124r1

مركز مدير الاستخبارات الوطنية الأمريكية لمكافحة الجرائم السيبرانية، *مكافحة سرقة الهوية من خلال التعليم والتكنولوجيا*، أكتوبر 2014.

مجلس كبير مسؤولي المعلومات الفيدرالي الأمريكي ووزارة الأمن الداخلي الأمريكية، مديرية الحماية والبرامج الوطنية، *البنية المرجعية للأمن النقال*، 23 مايو 2013. https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf



محررو المناهج المرجعية للأمن السيبراني.

المبحث 3: المنظمات والسياسات والمعايير الدولية للأمن السيبراني

الهدف

يتمثل الهدف العام من هذا المبحث في تعريف الطلاب بالمعايير والمنظمات الدولية، مثل المعهد الوطني للمعايير والتقنية الأمريكي والمعهد البريطاني للمعايير (وربما غيرهما)، والطرق التي ترتبط بها هذه المعايير والمنظمات بالسياقات الوطنية. وسوف يقدم الطلاب على التعرف على دور هيئات المعايير الدولية والتعرف على المنظمات الدولية الكبرى المعنية بأدوار ووظائف الأمن السيبراني. وبالإضافة إلى ذلك، ينبغي عليهم دراسة سياسات الأمن السيبراني الوطنية الخاصة بهم في ضوء المعايير الدولية وأفضل الممارسات الموصى بها وذلك من خلال مقارنتها بالعديد من أمثلة السياسات الوطنية. وأخيرًا، سيتناول نطاق هذا المبحث تطوير الأنظمة القانونية الدولية للأمن السيبراني.

الوصف

يتعين على كل دولة تصميم هذا القسم بحسب احتياجاتها، من خلال تحديد الهيئات الوطنية المسؤولة عن سياسة وممارسات الأمن السيبراني وكيفية تأثيرها على سياسات ومنظمات الأمن السيبراني لديها. وبينما ستختلف التفاصيل لكل دولة، إلا أن النهج المأخوذ لتقديم هذا المبحث قد يتبع هذه السطور: T3-B1، منظمات الأمن السيبراني الدولية، بحسب صلتها بالسياق الوطني، وT3-B2، المعايير والمتطلبات الدولية ـــدراسة استقصائية للهيئات والممارسات؛ وT3-B3، أُطُر عمل الأمن السيبراني الوطني، التي تهدف إلى تحليل الأطر الوطنية مقارنةً بأطر عمل الدول الأخرى؛ وT3-B4، الأمن السيبراني في القانون الوطني والدولي.

أهداف التعلم

أخذت الاستجابات الوطنية والدولية المختلفة للأمن السيبراني ترتسم في المنظمات القائمة والمنظمات الجديدة، باعتبارها مسألة ناشئة تتعلق بالأمن. ويتطلب الأمن السيبراني، باعتباره مسألة وطنية شاملة، سياسةً وتنسيقاً على مستوى عالٍ، ولكن كانت الاستجابات الوطنية متنوعة تماماً.

ومن خلال استكشاف الممارسات الناشئة في الدول التي تقوم بتطوير سياسات وطنية للأمن السيبراني الحكومي والتجاري والفردي ودعم الجهات الفاعلة غير الحكومية في تطوير أنظمة لإدارة المخاطر والتهديدات، سيتمكن الطالب من

- تطوير الوعي بأن الاستجابات الوطنية والدولية تتطلب نوعًا من نهج أصحاب المصلحة المتعددين؛
- التعرف على المنظمات الوطنية الرئيسية المسؤولة عن الأمن السيبراني؛
- تحديد وفهم الأدوار ومتطلبات وكالات المعايير الوطنية والدولية؛
- فهم أهمية العلاقة بين الأمن السيبراني والاستخبارات والمؤسسات العسكرية؛
- القدرة على تحليل الممارسات والسياسات الوطنية في ضوء المعايير الدولية والممارسات الجيدة؛
- فهم أدوار المنظمات الدولية الرئيسية التي تلعب دورًا قياديًا في مجال الأمن السيبراني؛
- معرفة الإطار القانوني الدولي المتطور ومواقف السياسة الرسمية للحكومة الوطنية في إطار هذا النظام الناشئ.

مراجع مقترحة

إدارة العمل الخارجي للاتحاد الأوروبي، "سياسة الأمن السيبراني الدولية الخاصة بالاتحاد الأوروبي". http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

شركة أي تي جافرنانس ليمتد، "أمن المعلومات وISO 27001: مقدمة،" الورقة الخضراء لشركة أي تي جافرنانس، أكتوبر 2013

أليكسندر كليمبرج، محرر، *دليل إطار عمل الأمن السيبراني الوطني*، مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو، تالين، إستونيا، 2012.

المعهد الوطني للمعايير والتقنية، وزارة التجارة الأمريكية ، *ضوابط الأمن والخصوصية لأنظمة المعلومات والمنظمات الفيدرالية*، مبادرة تحويل قوة العمل المشتركة، منشور خاص للمعهد الوطني للمعايير والتقنية 800-53، النسخة المنقحة 4، أبريل 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

شركة برايس ووترهاووس كوبرز إل إل بي، "لماذا ينبغي عليك تبني إطار عمل الأمن السيبراني الخاص بالمعهد الوطني للمعايير والتقنية،" مايو 2014. https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

البيت الأبيض، *تقرير مراجعة سياسة الفضاء السيبراني*. https://www.whitehouse.gov/cyberreview/documents

مكتب مساءلة الحكومة الأمريكية، *تقرير مُقدم إلى الكونجرس: الفضاء السيبراني: الولايات المتحدة تواجه تحديات في معالجة الأمن السيبراني والحوكمة على المستوى العالمي*، GAO-10-606، يوليو 2010.

T3-B1: منظمات الأمن السيبراني الدولية

الوصف

يُعتبر عدد المنظمات الدولية، الحكومية وغير الحكومية، المعنية بمسائل الأمن السيبراني العالمي أو الإقليمي كبير ومتزايد. وتتراوح مصالحها من مصالح تحقيقية إلى تنظيمية إلى قانونية ومتعلقة بتأييد السياسة والرقابة ومجموعة من المصالح الأخرى. وتعمل العديد من هذه المنظمات على تحقيق نُهج جماعية لحل التحديات السيبرانية، في حين قد يعمل البعض الآخر على تضخيم الأهداف الوطنية أو التجارية. ولأسباب عدة، يجب دراسة توصياتهم المتنوعة بصورة نقدية.

يُعد الموقع الإلكتروني الذي يحتفظ به مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو (CCD COE)، https://ccdcoe.org/، مصدرًا جيدًا فيما يخص روابط العديد من الوكالات الإقليمية المعنية بسياسة وممارسة الأمن السيبراني على نطاق واسع. وتتضمن هذه الاتحاد الأوروبي (انظر على وجه التحديد عمل الوكالة الأوروبية لأمن الشبكات والمعلومات، ENISA (https://www.enisa.europa.eu/), منظمة الأمن والتعاون في أوروبا، (http://www.osce.org/) OSCE، الأمم المتحدة (http://www.un.org/en/index.html)، وبالتأكيد حلف الناتو (http://www.nato.int/). وبالإضافة إلى هذه المصادر هناك أيضًا وكالات مثل المؤتمر العالمي لفرق الاستجابة للحوادث والأمن (www.first.org)، والشراكة الدولية متعددة الأطراف لمكافحة التهديدات السيبرانية (IMPACT)، وجمعية القوات المسلحة للاتصالات والإلكترونيات (AFCEA). تحتفظ الوكالة الأوروبية لأمن الشبكات والمعلومات بقائمة لمنظمات الاستجابة للأزمات السيبرانية وفرق الاستجابة للطوارئ السيبرانية في الدول الأعضاء بالاتحاد الأوروبي (CERTs) وتحدثها بشكل منتظم.

وتشمل الهيئات الدولية الأخرى المعنية بالأمن السيبراني المنظمة الدولية للمعايير (التي تمت مناقشتها في اللبنة 2 من هذا المبحث)، وهيئة الإنترنت للأسماء والأرقام المخصصة (ICANN)، ومنتدى إدارة الإنترنت (IGF) والاتحاد الدولي للاتصالات الذي تدعمه الأمم المتحدة (ITU).

وتركز هذه اللبنة على كيفية تفاعل الحكومات مع هذه المنظمات الدولية العديدة واعتماد ممارسات مشتركة تقوم غالبًا على توصياتهم.

نتائج التعلم

فيما يتعلق بالأمن السيبراني، سيتمكن الطلاب من:

- توضيح التحديات المختلفة التي تؤثر على الحكومات وتفاعلاتها مع المنظمات الدولية؛
- التعرف على المنظمات الدولية الرئيسية ومحور تركيز سياساتها ودورها في التعريف بالأمن السيبراني الوطني ودعمه؛
- والتعرف على المنظمات الوطنية التي تتحمل مسؤوليات فيما يتعلق بالتعاون والمشاركة الدولية.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

ينبغي استخدام خبير متخصص وطني لتحديد الهيئات الدولية الأكثر أهمية في الدولة والتي تعتمد عليها الدولة في التوجيه وتعبر عن شواغلها من خلالها.

قد تتضمن الموضوعات الأخرى التي يمكن تغطيتها ما يلي:

- الهيئات الدولية الرئيسية للتعريف بالممارسات الوطنية: الاتحاد الأوروبي وحلف الناتو والحكومة الأمريكية (القيادة السيبرانية وغيرها) واليوروبول (انظر www.europol.europa.eu/ec3)
- كيف تتداخل المصالح الوطنية مع المنظمات الدولية وأهدافها
- تحديد الجوانب الإيجابية والسلبية للنهج التنظيمية الدولية للأمن السيبراني
- الترتيبات والآليات الوطنية لإيجاد حلول للتحديات الدولية
- استخدام الإنترنت للأغراض الإجرامية والإرهابية والجرائم المنظمة العابرة للحدود

طريقة/تقييم التعلم

قد تشمل طرق التدريس تحليلات للقضايا الراهنة. ينبغي على الطلاب إجراء بحوث ومراجعات بشأن دراسات حالة تتعلق بالاستجابات التنظيمية الدولية ودراسة التحديات الدولية السائدة وتأثيرها على الدول.

ينبغي إجراء التقييم من خلال مشروع جماعي مع المشاركة في الفصول الدراسية وتكليف كتابي بشأن استجابة إحدى المنظمات الدولية للأمن السيبراني.

المراجع

تاكيشي تاكاهاشي، يوكي كادوباياشي، "التوصيف المرجعي فيما يتعلق بالمعلومات التشغيلية للأمن السيبراني"، *مجلة الحاسوب* المجلد 50، رقم 10، لعام 2014. الرقم التسلسلي المعياري الدولي للمجلة: 2067-1460.

فارزان كوليني، ليش جانكزوسكي "نموذج قدرة الدفاع السيبراني: تصنيف الأساس"، (2015). CONF-IRM 2015. الوقائع. الوثيقة 32. متوفر على: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2015

فينج شيه، يونج بينج، وي زاو، يانج غاو، زويفينج هان، "تقييم أمن أجهزة الرقابة الصناعية: المعايير والتقنيات والتحديات"، في، *نظم المعلومات الحاسوبية والإدارة الصناعية*، الصفحات 624-635، 2014. سبرنجر برلين هايدلبرغ. معرّف الوثيقة الرقمي: 10.1007/978-3-662-45237-0_57 الرقم الدولي المعياري للكتاب المطبوع: 978-3-662-45236-3. الرقم الدولي المعياري للكتاب عبر الإنترنت: 978-3-662-45237-0.

أكينولا أجيجولا، بافول زافارسكي، رون روهل، "مراجعة وتقييم مقارن للمبادئ التوجيهية للتحليلات العدلية للمنشور الخاص بالمعهد الوطني للمعلومات والتقنية 800-101 النسخة المنقحة 1: 2014 و2012 :ISO/IEC 27037". أوراق بحثية مُقدمة في "المؤتمر العالمي لأمن الإنترنت (WorldCon) "2014. الصفحات 66-73. 10.1109/WorldCIS.2014.7028169. متوفر من IEEE على: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7028169&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7028169

إضافة إلى الموارد الإلكترونية السابقة، انظر ما يلي:

إن شكري، وإس مادنيك وجيه فيرويردا، "مؤسسات الأمن السيبراني: الاستجابات الدولية والضرورات العالمية،" *تكنولوجيا المعلومات الخاصة بالتنمية 20*، رقم 2 (2013): 96–121. http://dx.doi.org/10.1080/02681102.2013.836699

T3-B2 المعايير والمتطلبات الدولية—دراسة استقصائية بشأن الهيئات والممارسات

الوصف

تُعرِّف هذه اللبنة الطلاب بمجموعة المعايير الدولية التي وضعتها المنظمات المعنية بوضع المعايير. سيدرك الطلاب دور المعايير والمتطلبات التقنية الدولية. كما سيتم تعريفهم بمجموعة معايير المنظمة الدولية للمعايير (ISO) بالإضافة إلى أهداف التحكم في المعلومات والتكنولوجيا ذات الصلة (COBIT) واتحاد تدقيق ومراقبة أنظمة المعلومات (ISACA) ومكتبة البنية التحتية التقنية الدولية (ITIL). وستشمل المناقشات المعهد الوطني للمعايير والتقنية الأمريكي (NIST)، والمعهد البريطاني للمعايير (BSI)، المكتب الفيدرالي لأمن المعلومات بألمانيا، والجمعية الأمريكية الدولية للأمن الصناعي (ASIS) (وغيرها من المعايير حيثما كان ذلك ممكنًا أو مرغوبًا فيه) لتسليط الضوء على الأنواع والأعباء التي يخلقها تطبيق المعايير والتحديات التي تمثلها المعايير المتنافسة. بالإضافة إلى ذلك، تسلط هذه اللبنة الضوء على النهج الوطني للتوافق مع المعايير الدولية. وأخيرًا، فإنها تتناول حدود المعايير وتوضح الأسباب التي من أجلها قد تقوم المنظمات العسكرية أو منظمات الدفاع أو المنظمات الحكومية الأخرى بوضع معايير خاصة بها.

نتائج التعلم

سيتمكن الطلاب من

- فهم دور المعايير والمتطلبات التقنية الدولية؛
- تحديد المنظمات الدولية المعنية بوضع المعايير (مثل ISO, NIST)؛
- تحديد مصادر المعايير الدولية للتعريف بالاستراتيجية السيبرانية الوطنية الخاصة بهم؛
- استيعاب التحديات والصعوبات التي ينطوي عليها تنفيذ المعايير الدولية؛
- وإظهار المعرفة بكيفية وعن طريق أي هيئة يتم وضع معايير الأمن السيبراني الخاصة بمنظماتهم والحفاظ عليها ونشرها.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

قد تشمل ما يلي:

- المعايير الوطنية والدولية المعتمدة وطنيًا التي تتناول الأمن الإلكتروني بشكلٍ مباشر
- المعايير الإجرائية أو التنظيمية الوطنية ذات الصلة
- التحديات والصعوبات التي ينطوي عليها تنفيذ المعايير الدولية

طريقة/تقييم التعلم

ينبغي أن تكون وسائل وطرق التقييم مناسبة لمستوى الأداء المحدد للدورات التدريبية والدروس المستمدة من هذا المنهج المرجعي.

وسيقوم خبير وطني بتلخيص المعايير المختلفة المعتمدة من قبل الدولة وشرح علاقتها بالمعايير الدولية والناشئة فيما يتعلق بالأمن السيبراني.

يمكن للطلاب تحديد دراسات حالة بشأن تنفيذ المعايير الدولية والقيام بتحليلها.

ينبغي إجراء مناقشات جماعية بشأن تحديات تنفيذ المعايير الدولية. ينبغي وضع أمثلة من الخبرة المحلية.

المراجع

إينيجو باريرا، إيزينبي، جيروم بورديير، سيبيلويب، أوليفير ديلوس، أرنو فيدلر، نيمبوس تيكنولوجيبيراتانج جي إم بي إتش، توماش ميلنيكي، جيمالتو، أرتور ميكينا، بوليش سيكيوريتي برينتينج وركس، جون شامة، إج كونسالتانتس، كليمنس وانكو، تي يو في إنفورماشانستيكنيك جي إم بي إتش، كلارا جالان مانسو، الوكالة الأوروبية لأمن الشبكات والمعلومات، سلومير جورنياك، الوكالة الأوروبية لأمن الشبكات والمعلومات، "تحليل المعايير المتعلقة بمقدمي خدمات الإئتمان - وضع متطلبات eIDAS إلى المعايير الحالية"، الوكالة الأوروبية لأمن الشبكات والمعلومات، 1 يوليو 2016. متوفر على: https:// www.enisa.europa.eu/publications/tsp_standards_2015

مانموهان شاتورفيدي، ابهيشيك نارين سينغ، مانموهان براساد جوبتا، جيجيت باتاشاريا، (2014) "تحليلات قضايا أمن المعلومات في السياق الهندي"، *تحول الحكومة: الأفراد والعملية والسياسة*، المجلد 8 الإصدار: 3، الصفحات 397-374. معرف الوثيقة الرقمي (متوفر على): http://www.emeraldinsight.com/doi/ abs/10.1108/TG-07-2013-0019

إل تشانغ، كيو وانغ، بي تيان "التهديدات والتدابير الأمنية الخاصة بالأنظمة السيبرانية المادية"، في، *مجلة جامعات الصين للبريد والاتصالات السلكية واللاسلكية*، المجلد 20، تكملة 1، لعام 2013، الصفحات 29-25. الرقم التسلسلي المعياري الدولي للمجلة: 1005-8885. رقم المُعرِّف الفريد: ETOCRN339930374

بلاز ماركيلج، سابينا، سابينا زجاجا، "فهم التهديدات السيبرانية ونتائجها في سلوفينيا"، في، *مجلة مراجعة قانون وأمن الحاسوب: المجلة الدولية لقانون وممارسة التكنولوجيا*. المجلد 32. الإصدار 3 (2016). الرقم التسلسلي المعياري الدولي للمجلة: 2212-473X (إلكتروني - المتجر الرقمي ELD في المكتبة البريطانية) رقم المُعرِّف الفريد: ETOCvdc_100032209717.0x000001.

شاكلفورد، وسكوت، وسكوت إل، وراسل، وجيفري هوت. "التحليلات التصاعدية: مقارنة أطر عمل الأمن السيبراني الطوعية." مجلة القانون التجاري لجامعة كاليفورنيا بدافيس (2016).

اتحاد تدقيق ومراقبة أنظمة المعلومات، *تنفيذ الأمن السيبراني الأوروبي: نظرة عامة*، التقرير الرسمي لاتحاد تدقيق ومراقبة أنظمة المعلومات، 2014. http://www.isaca.org أو http://www.isaca.org/knowledge-center

اتحاد تدقيق ومراقبة أنظمة المعلومات، سلسلة تنفيذ الأمن السيبراني الأوروبي: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/european-cyber-security-implementation-series.aspx؛ انظر أيضًا تقارير اتحاد تدقيق ومراقبة أنظمة المعلومات بشأن المرونة وإرشادات المخاطر والضمان وبرامج التدقيق.

شركة برايس وتر هاووس كوبرز إل إل بي، *"لماذا ينبغي عليك تبني إطار عمل الأمن السيبراني الخاص بالمعهد الوطني للمعايير والتقنية"*، مايو 2014. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

ستيفي بارسر، "المعايير الخاصة بالأمن السيبراني" في إم إي هاثاوي (محرر)، *أفضل الممارسات في الدفاع عن شبكة الحاسوب: الكشف عن الحوادث والاستجابة لها* (أمستردام: مطابع أي أو إس)، 2014: 106. معرّف الوثيقة الرقمي: 10.3233/978-1-61499-372-8-97

سلسلة معايير أخرى (بالإضافة إلى ISO 27000):

- ISO 9000 (إدارة الجودة)
- ISO 22300 (إدارة استمرارية الأعمال)
- ISO 31000 (إدارة المخاطر)
- BSI PAS 555

T3-B3: أطر عمل الأمن السيبراني الوطنية

الوصف

باعتبارها مسألة وطنية تتجاوز الحدود التقليدية بين الحكومة والصناعة والمواطنين، يتطلب الأمن السيبراني سياسة وتنسيقًا على مستوى عالٍ. وبالنظر إلى الترابط بين النظم، فقد أدرك العديد من الحكومات الحاجة إلى نهج شامل للحكومة فقط من أجل إدارة أمن النظم التشغيلية الخاصة بها، بالإضافة إلى المساعدة في تقليل المخاطر على الصناعة والأفراد. ومع ذلك، كانت الاستجابات الوطنية متنوعةٍ إلى حدٍ كبير. فقد أنشأت بعض الدول هيئات وطنية مسؤولة عن إدارة الأمن السيبراني الوطني فيما فوضت دول أخرى مسؤولية صياغة السياسات الوطنية إلى هيئات تنسيقية بينما تركت إدارة وتنفيذ السياسات لأجهزة حكومية مختلفة. ولا تزال دول أخري تكافح من أجل إيجاد إطار العمل المناسب.

وقد ذهبت بعض الحكومات إلى أبعد من وضع تدابير الأمن السيبراني أو دعمها فقط من أجل حماية آليات الحكومة وتبنت هذه المسألة كإحدى المخاطر الوطنية وبذلت مجهودًا لدعم أفضل الممارسات وتشجيعها في القطاع الخاص وبين المواطنين. وكان دعم هذه التدابير وتفويضها هو الممارسة السائدة على الأخص فيما يتعلق بحماية البنية التحتية الحيوية والتي غالبًا ما تكون ملكية خاصة. ومع ذلك، هناك بعض المتطلبات المشتركة مثل تحديد الأدوار والمسؤوليات الهيكلية وإصدار التوجيهات الفنية المعتمدة وتحديد الأدوار والمسؤوليات للتخفيف من المخاطر والاستجابة للمسائل النشطة.

وتهدف هذه اللبنة إلى تعريف الطلاب بسياسات واستراتيجيات وهياكل الأمن السيبراني في بلدانهم. يحتاج الطلاب إلى التعرف على إطار استراتيجية السياسة الخاص ببلدهم (إذا كان إطارًا واحدًا) والمنظمات المسؤولة عن وضع التوجيهات الوطنية والمواصفات التقنية. وسيجري الطلاب مقارنة بين العديد من نهج ووثائق استراتيجية الأمن السيبراني الوطنية والدولية من أجل فهم النهج والوثائق الخاصة ببلدانهم بشكل أفضل وتقييم مجالات المخاطر والمسؤوليات.

نتائج التعلم

سيتمكن الطلاب من

- تحديد المنظمات المسؤولة عن سياسة الأمن السيبراني الوطنية؛
- تحديد الملامح الرئيسية لسياسة الأمن السيبراني الوطنية؛
- تحديد المنظمات المسؤولة وفهم دورها في وضع وإصدار التوجيهات/التعليمات الفنية؛
- تحديد الخصائص الرئيسية للتوجيهات/التعليمات الفنية؛
- مناقشة مصادر أفضل الممارسات في تنظيم الأمن السيبراني الوطني؛
- وتحليل النهج الوطني في بلدانهم بشكل نقدي مقارنةً بأطر عمل السياسات المرجعية.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

- النهج المركزي في مقابل القائم على أصحاب مصلحة متعددين في التعامل مع الأمن السيبراني
- النهج الوطنية بشأن التعاون والتنسيق والتشارك
- المنظمات الدولية: الأدوار والتفاعل في السياق الوطني
- أطر السياسة المرجعية—مراجعة أمثلة مختلفة

طريقة/تقييم التعلم

ينبغي أن تكون وسائل وطرق التقييم مناسبة لمستوى الأداء المحدد للدورات التدريبية والدروس المستمدة من هذا المنهج المرجعي.

قد تشمل طرق التدريس مناقشات ومحاضرات بواسطة خبراء متخصصين ودراسات حالة للمقارنة وتحديد الممارسات الجيدة وزيارات لهيئات الأمن السيبراني المحلية.

المراجع

سلومير غورنياك، جورج إشويلر، برتولد جربر، وأليساندرو جوارينو، كاي رانبرغ، جون شامة، سلومير غورنياك، "إطار عمل إدارة المعايير الأوروبية: مواءمة السياسة والصناعة والبحث، المجلد 1.0"، إيراكليو، اليونان، الوكالة الأوروبية لأمن الشبكات والمعلومات، 2015، الرقم الدولي المعياري للكتاب 9789292041540.

توماس ميناريك، "منظمة الأمن السيبراني الوطنية: جمهورية التشيك"، النسخة المنقحة الثانية، تالين، 2016 مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو. متوفر على: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf

فيتوتاس باتريماس، "منظمة الأمن السيبراني الوطنية: ليتوانيا"، تالين، 2015. مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو. متوفر على: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf

ليا هريكيكوفا، كادري كاسكا، "منظمة الأمن السيبراني الوطنية: سلوفاكيا"، تالين، 2015. مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو. متوفر على: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SLOVAKIA_042015.pdf

ليتو مارتي، وجارنو ليمنيل. "قدرة الأمن السيبراني وحالة فنلندا." في المؤتمر الأوروبي بشأن الحرب السيبرانية والأمن السيبراني، الصفحة 182. مجلة المؤتمرات الأكاديمية الدولية المحدودة، 2016.

مجلس علوم الدفاع، وزارة الدفاع الأمريكية، *تقرير فريق العمل: النظم العسكرية المرنة والتهديد السيبراني المتقدم*، يناير 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

جورج فرح، *بنية أمن نظم المعلومات: نهج جديد للحماية ذات المستويات—دراسة حالة*، النسخة العملية 1.4ب للشهادة العالمية لأساسيات الأمن (GSEC)، معهد سانس، 9 سبتمبر 2004. www.sans.org

ألكسندر كليمبرج، محرر، *دليل إطار عمل الأمن السيبراني الوطني*، منشور خاص بمركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو، تالين، إستونيا، 2012، الرقم الدولي المعياري للكتاب 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

المعهد الوطني للمعايير والتقنية، *ضوابط الأمن والخصوصية الخاصة بأنظمة المعلومات والمنظمات الفيدرالية*، تقرير أصدرته مبادرة تحويل فرقة العمل المشتركة في المعهد الوطني للمعايير والتقنية، منشور خاص بالمعهد الوطني للمعايير والتقنية 800-53، النسخة المنقحة 4، المعهد الوطني للمعايير والتقنية، وزارة التجارة الأمريكية، واشنطن العاصمة، أبريل 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

منظمة التعاون الاقتصادي والتنمية (OECD)، *إعداد سياسة الأمن السيبراني في نقطة تحول: تحليل جيل جديد من استراتيجيات الأمن السيبراني الوطني لاقتصاد الإنترنت*، 2012. http://oe.cd/security

T3-B4: الأمن السيبراني في القانون الوطني والدولي

الوصف

يتسم المشهد القانوني للأمن السيبراني بالتعقيد وسرعة التغير. فهناك سجالات بشأن إمكانية تطبيق القوانين الحالية والناشئة الدولية والوطنية لمعالجة قضايا الأمن السيبراني وتحدياته. كما أن هناك تباين واسع في كيفية تعامل الدول مع الأمن السيبراني ضمن القانون المحلي. وبعض الدول تمتلك قوانين محددة خاصة بالأمن السيبراني فيما البعض الآخر لا تمتلك مثل هذه القوانين. ويؤدي تحدي العزو — أي صعوبة تتبع مصدر نشاط سيبراني خبيث أو مهدد أو غير قانوني— إلى إضفاء مزيد من التعقيد على المشكلات في المجال المحلي والدولي.

ويوجد عدد متنام من المنشورات فيما يتعلق بالقانون الدولي والوطني المطبق على الأمن السيبراني. وتعرِّف هذه اللبنة الطلاب بالقوانين الدولية والوطنية المسؤولة عن مجموعة من قضايا الأمن السيبراني. تخضع العديد من الدول والمنظمات بداخلها لقوانين الامتثال، على سبيل المثال تلك التي تتطلب الإبلاغ عن أنواع معينة من خروقات المعاملات المالية أو البيانات. وتوجد كذلك معايير وممارسات دولية متطورة تتعلق بالقوانين وإنفاذها (مثل أنظمة التعاون التي يضعها الإنتربول). وقد تم تبني المتطلبات القانونية للإبلاغ عن الحوادث السيبرانية من قبل العديد من الدول وهناك جهود يجري بذلها لوضع قانون دولي خاص بالأخلاقيات السيبرانية. ومع ذلك، لا توجد هيئة أو منظمة دولية حاكمة تشرف على الجوانب القانونية للأمن السيبراني.

سيتعرف الطلاب على المواقف الوطنية بشأن القانون المحلي والدولي المتعلق بالفضاء السيبراني، مع التركيز على الأمن السيبراني. وتشمل الجوانب المحلية ذات الأهمية الخصوصية وضمان الأنظمة والامتثال التنظيمي ومقتضيات التأمين التجاري في الأنظمة القانونية الوطنية والدولية الناشئة.

نتائج التعلم

سيتمكن الطلاب من

- إدراك التحديات الرئيسية ومصادر السياسة في القانون السيبراني الدولي؛
- شرح المسؤوليات القانونية لأصحاب المصلحة والقوانين التي تتعلق بالأمن السيبراني الوطني؛
- والإلمام بالنظم القانونية الوطنية فيما يتعلق بالأمن السيبراني (إن وجدت) وتحديد السلطات القانونية الرئيسية داخل المنظمات الخاصة بهم.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

- يمكن التطرق بمزيدٍ من التفصيل إلى موضوعات مثل الخلاف بشأن الوضع القانوني الدولي للهجمات السيبرانية التي تقودها أطراف حكومية وغير حكومية والمسائل السيبرانية في القانون المحلي ومتطلبات الامتثال التنظيمي والمسؤولية القانونية الفردية.
- استكشاف السجال بشأن مدونة قواعد السلوك الدولية لأمن المعلومات المقترحة للأمم المتحدة.
- لوائح الامتثال المحلية
- التأمين التجاري والمسؤولية عن المخاطر السيبرانية

طريقة/تقييم التعلم

ينبغي وضع المحاضرات بالتنسيق مع الممثلين القانونين المسؤولين والقادرين على التعبير بشكلٍ حاسم عن موقفهم الوطني بشأن هذه القضايا.

وينبغي تناول دراسات حالة بشأن الاستجابات القانونية الدولية والوطنية فيما يتعلق بحوادث الأمن السيبراني.

يتعين وضع اختبار كتابي قصير مناسب لمستوى التفصيل الذي يتسم به المنهج كأداة تقييم.

المراجع

هونج شو "القانون السيبراني في الصين" ألفن آن دن راين: كليور للقانون الدولي، 2010. الرقم الدولي المعياري للكتاب 9789041133335. رقم الرف في المكتبة البريطانية: YC.2011.a.9251. رقم المُعرِّف الفريد: BLL01015641102

رادزيويل ياروسلاف "الهجمات السيبرانية والثغرات في القانون الدولي التي يمكن استغلالها." لايدن: بريل نيجهوف، 2015. الرقم الدولي المعياري للكتاب 9789004298330.

آنا-ماريا أوسولا وهنري جويجاي (محرران)، *المعايير السيبرانية الدولية: وجهات النظر حول القانون والسياسة والصناعة* (2015). مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو. كتاب إلكتروني. يتوفر الكتاب في نسخته الكاملة على: https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html

زينب كراكي، الشيخة لبنى القاسمي، *الأمن السيبراني في الاقتصادات النامية والناشئة*، 2010، شلتنهام: إدوارد إلجار بابلشينج.

ديفيد بي فيلدر، وريتشارد بريجينت، وأليكس فاندورمي. "حلف الناتو والدفاع السيبراني والقانون الدولي." مجلة القانون الدولي والمقارن 4، رقم 1 (2016): 1.

ساران، سمير. "السعي إلى توافق آراء دولي بشأن الأمن السيبراني: دروس من القرن العشرين." السياسة العالمية 7، رقم 1 (2016): 93-95.

دان أرنودو، "مذكرة بحثية: الكفاح من أجل تعريف سياسة الأمن السيبراني ومشاركة المعلومات في الولايات المتحدة" معهد ASA للمخاطر والابتكار، 2013. http://www.anniesearle.com/research.aspx?topic=researchnotes

نيلس ميزلر، *الحرب السيبرانية والقانون الدولي*، معهد الأمم المتحدة لبحوث نزع السلاح (UNIDIR)، جنيف، 2011. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

حلف الناتو، *الجريدة القانونية: المسائل القانونية المتعلقة بالفضاء السيبراني* 35 (ديسمبر 2014). يتناول هذا العدد، في مقالات منفصلة، (1) الجوانب القانونية للأمن السيبراني والمسائل ذات الصلة بالفضاء السيبراني التي تؤثر على حلف الناتو؛ و(2) الدفاع السيبراني النشط إلى الدفاع السيبراني سريع الاستجابة؛ و(3) استكشاف حد "الهجوم المسلح" والمسائل القانونية ذات الصلة بالعزو والمشاركة في الحرب السيبرانية. https://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو (مايكل إن شميت، محرر عام)، *دليل تالين بشأن القانون الدولي المُطبّق على الحرب السيبرانية* (كامبردج، المملكة المتحدة: مطابع جامعة كامبردج)، 2013. https://ccdcoe.org/tallinn-manual.html

مايكل إن شميت، "قانون الحرب السيبرانية: إلى أين؟،" *مجلة ستانفورد للقانون والسياسية* 25 (2014): 269–299.

المبحث 4: إدارة الأمن السيبراني في السياق الوطني

الهدف

يكمن الهدف العام من هذا المبحث في استكشاف الممارسة الخاصة بإدارة الأمن السيبراني في السياق الوطني.

الوصف

ستختلف النُهج المتعلقة بإدارة قضايا الأمن السيبراني الوطنية اختلافًا كبيرًا بين البلدان. وفي حين أن التحديات والاستجابات قد تختلف من حيث التفاصيل، ستكون المشكلات العامة متشابهة فيما بين الأمم. وقد تختلف الأطر الوطنية للأمن السيبراني في تفاصيلها، ولكن غالبًا ما يتضمن نظام شامل بوجه عام القضايا التالية، والتي تتطلب الإدارة والتنسيق بشكلٍ فعّال: (1) إدارة الأصول المادية المتعلقة بتكنولوجيا المعلومات؛ (2) إدارة الضوابط؛ (3) تكوين النظم وإدارة تغيير التكوين؛ (4) تحديد مواطن الضعف وإدارتها؛ (5) إدارة الحوادث؛ (6) إدارة استمرارية الخدمة؛ (7) تحديد التهديدات وإدارة المعالجة؛ (8) إدارة التبعيات والروابط الخارجية؛ (9) التدريب والتوعية؛ (10) الحفاظ على الوعي الظرفي[7].

ويستكشف هذا المبحث الممارسات الوطنية لإدارة الأمن السيبراني ويضع سياق استعداد الأمن الوطني في إطار المخاطر. وعلى وجه الخصوص، تتعمق T4-B1، الممارسات والسياسات والمنظمات الوطنية الخاصة بالمرونة السيبرانية، في عملية تخطيط الطوارئ والتعافي من الحوادث السيبرانية للحد من الانقطاع. وتقدم T4-B2، أطر عمل الأمن السيبراني الوطني، ممارسات إدارة الأمن السيبراني الوطني، والتي تشمل العمليات والاستجابة للحوادث وتخفيف المخاطر. وتُعلّم T4-B3، التحاليل العدلية السيبرانية، الطلاب الأدوات والممارسات والإجراءات العدلية لجمع وتحليل وتفسير البيانات للإسناد والاستخبارات. ويُعرّف T4-B4، التدقيق والتقييم الأمني على المستوى الوطني، الطلاب بأفضل الممارسات المتبعة في تقييم الاستعداد الوطني للأمن السيبراني.

أهداف التعلم

سيتمكن الطلاب من

- فهم نهج النُظم للتخطيط من أجل الصمود أمام التهديدات والهجمات والأحداث المماثلة؛
- وضع الممارسة الخاصة باستخدام النظم المرنة في السياق الوطني؛
- تحليل استخدام أطر العمل والمصفوفات من أجل التخطيط والتفويض؛
- وإثبات معرفتهم بالأنواع الشائعة لمنظمات الاستجابة الوطنية، والتعرّف على دور ومهمة وهيكل نظمها الوطنية الحالية والمنظمات التنظيمية لإدارة الحوادث والأزمات.

المراجع المقترحة

ديبورا جيه. بودياو وريتشارد غراوبارت، *إطار هندسة المرونة السيبرانية*، تقرير ميتر الفني MTR 110237، مؤسسة ميتر، سبتمبر 2011. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

محمد ظافر الشريف الكتاني وطيب دباغ، "مخطط RACI الوطني لإطار عمل "أمن سيبراني وطني" قابل للتشغيل المتبادل"، *إجراءات المؤتمر الأوروبي المعني بحرب وأمن المعلومات*، يناير 2009.

نيكول فاليسي ورازفان غافريلا والرائد ريتر كلينستروب وكونستانتينوس مولينوس، *استراتيجيات الأمن السيبراني الوطني: دليل عملي بشأن التطوير والتنفيذ*، الوكالة الأوروبية لأمن الشبكات والمعلومات، ديسمبر 2012. https://www.enisa.europa.eu

كريس هول وريتشارد كلايتون وروس أندرسون وإيفانجيلوس أوزونيس، *انتر إكس: مرونة النظام البيئي للربط البيني للإنترنت*، تقرير كامل، الوكالة الأوروبية لأمن الشبكات والمعلومات، إبريل 2011.

أنطوني ثورن وتوبياس كريستن وبياتريس غروبر ورولاند بورتمان ولوكاس روف، "ما هي البنية الأمنية؟"، كتاب بواسطة الفريق العامل المعني بالبنية الأمنية، جمعية أمن المعلومات، سويسرا، 29 سبتمبر 2008.

وزارة الأمن الداخلي الأمريكية، *مراجعة المرونة السيبرانية (CRR): دليل المستخدم بشأن وصف الطريقة والتقييم الذاتي*، جامعة كارنيجي ميلون، فبراير 2014.

انظر الموارد في CERT-RMM (نموذج CERT لإدارة المرونة) الصادر عن قسم CERT (فريق الاستجابة للطوارئ السيبرانية) بمعهد هندسة البرمجيات التابع لجامعة كارنيجي ميلون: www.cert.org/resilience/rmm.html

[7] مستمد من نموذج CERT-RMM بجامعة كارنيجي ميلون.

T4-B1: الممارسات والسياسات والمنظمات الوطنية الخاصة بالمرونة السيبرانية

الوصف

يجتاز الأمن السيبراني ويسمو فوق العديد من الحدود التنظيمية. وقد تبنى عدد من الدول نهجًا شاملاً على مستوى الحكومة بأكملها لتوضيح الأدوار والمسؤوليات المتعلقة بإدارة المرونة السيبرانية. وتهدف المرونة السيبرانية إلى ضمان بقاء البنية الأساسية السيبرانية الوطنية جاهزة للعمل عندما تكون في وضع الأزمات وأن تتعافى بشكلٍ سريع وفعّال بعد الانقطاع. ومع أخذ هذه المرونة في الحسبان، تتناول هذه اللبنة الممارسات الوطنية والتنظيمية في سياق مقارن.

في هذه اللبنة، سوف يتعرض الطلاب لعدد من النهج الشاملة النموذجية فيما يتعلق بالأمن السيبراني كما هو موضح في التوجيهات رفيعة المستوى المنشورة (مثل توجيهات المملكة المتحدة أو الولايات المتحدة) من أجل تحليل نقاط القوة والضعف في سياساتها الوطنية. وسيتم مقارنة السياسات الوطنية ذات الصلة بالكتلة الطلابية ببعضها بعضًا. وينبغي توجيه المناقشة بوجه خاص إلى دراسة السياسات والممارسات القائمة الرامية إلى منع وقوع الحوادث السيبرانية والحماية منها والتصدي لها وإدارتها. وينبغي التطرق أيضًا إلى بعض الإجراءات مثل التدقيق والتحقق ووسائل المراجعة المستقلة.

نتائج التعلم

سيتمكن الطلاب من

- تفسير وثائق المرونة السيبرانية الوطنية؛
- المساهمة في تطوير وتوسيع نطاق إجراءات المرونة السيبرانية الوطنية؛
- شرح الأدوار والمسؤوليات المنوطة بالأفراد والمنظمات المسؤولة عن المرونة السيبرانية الوطنية؛
- استيعاب التحديات المتعلقة بتنسيق العمليات السيبرانية خلال مواقف الأزمات؛
- وفهم عمليات تحليل القرارات المستخدمة في اتخاذ قرارات الامتثال خلال مواقف الأزمات.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

ينبغي أن يعمل أحد الخبراء المتخصصون الوطنيون على تحليل السياسات الوطنية القائمة لاستخراج المستوى المناسب من المعلومات لاستخدامها في الخطط الدراسية.

طريقة/تقييم التعلم

قد تشتمل أساليب التدريس على محاضرات وعروض إيضاحية وزيارات ميدانية وتدريبات كتابية. وينبغي أن يتألف التقييم من التحقق الكتابي والشفوي على حدٍ سواء.

المراجع

جمعية كلاوزفيتز؛ الأكاديمية الاتحادية للسياسة الأمنية. "السياسة الأمنية في العصر السيبراني: هل الدفاع السلبي كافيًا؟" بون، ألمانيا: دار Mittler Report Verlag، 2014. معرّف المكتبة البريطانية: 016828758. رقم تسليم الوثيقة: 3829.361655 رقم المعرّف الفريد: BLL01016828758

غويدو ناناريلو، "التجارة الإلكترونية وحماية المستهلك: دراسة استقصائية بشأن مدونات قواعد السلوك وعمليات التصديق"، إسبرا: مركز البحوث المشترك، معهد أمن وحماية المواطن، قطاع الأمن السيبراني، 2001. رقم المُعرِّف الفريد: BLL01011092147.

إف كاسيم، "معالجة هاجس الجريمة السيبرانية المتنامي في أفريقيا: تقييم التدابير التي اعتمدتها جنوب أفريقيا وغيرها من الجهات الفاعلة الإقليمية"، في، *مجلة القانون المقارن والقانون الدولي لأفريقيا الجنوبية*، المجلد 44، العدد 1، 2011، الصفحات 123-138 (جامعة جنوب أفريقيا). الرقم التسلسلي المعياري الدولي للمجلة: 4051-0010. رقم المُعرِّف الفريد: ETOCRN296687880.

إن شيرازي، "إطار عمل لإدارة المرونة في السحابة"، في، *مجلة Elektrotechnik und Informationstechnik*، المجلد 132؛ العدد 2، لعام 2015، الصفحات 122-132. الرقم التسلسلي المعياري الدولي للمجلة: 0932-383X. رقم المُعرِّف الفريد: ETOCRN370071353.

كالبرج، جان "تقييم المرونة السيبرانية في الهند: مسائل الاستقرار المؤسسي". التحليل الاستراتيجي 40، رقم 1 (2016): 5-1.

سيتعين على أحد الخبراء المتخصصين تجميع السياسات والمراجع الوطنية المناسبة. وتشمل المراجع الأكثر عمومية ما يلي:

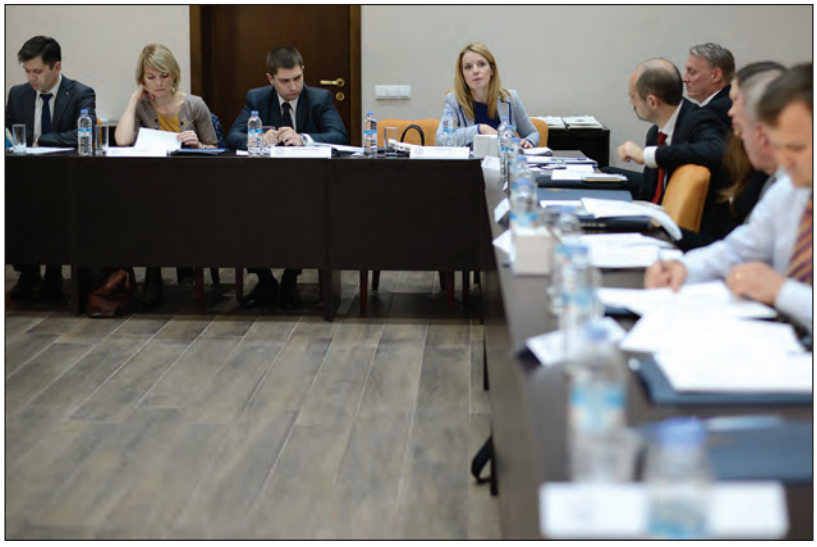
ديبورا جيه. بودياو ودي جيه غراوبارت، *إطار عمل هندسة المرونة السيبرانية*،تقرير ميتر الفني MTR 110237 (بيدفورد، ماساتشوستس: مؤسسة ميتر)، سبتمبر 2011.

كريس هول وريتشارد كلايتون وروس أندرسون وإيفانجيلوس أوزونيس، *انتر إكس: مرونة النظام البيئي للربط البيني للإنترنت*، تقرير كامل، الوكالة الأوروبية لأمن الشبكات والمعلومات، إبريل 2011.

وزارة الأمن الداخلي الأمريكية، *مراجعة المرونة السيبرانية (CRR): دليل المستخدم بشأن وصف الطريقة والتقييم الذاتي*، جامعة كارنيجي ميلون، فبراير 2014.

وزارة الأمن الداخلي الأمريكية، *مراجعة المرونة السيبرانية (CRR): مجموعة أسئلة مع التوجيه*، جامعة كارنيجي ميلون، فبراير 2014.

انظر الموارد في CERT-RMM (نموذج CERT لإدارة المرونة) الصادر عن قسم CERT (فريق الاستجابة للطوارئ السيبرانية) بمعهد هندسة البرمجيات التابع لجامعة كارنيجي ميلون: www.cert.org/resilience/rmm.html



ورشة عمل للفريق المعني بكتابة المنهج المرجعي للأمن السيبراني في تبليسي.

T4-B2: أطر عمل الأمن السيبراني الوطنية

الوصف

تقدم هذه اللبنة للطلاب فهمًا لاستراتيجية الأمن السيبراني الوطني وتنفيذها في سياق إدارة العمليات السيبرانية والتعامل مع حوادث الأمن السيبراني على المستوى الوطني وإدارة مخاطر الأمن السيبراني الوطني. وينبغي أن ينصب التركيز على الأطر التي تساعد في تخصيص الموارد وتحديد الأدوار والمسؤوليات التنظيمية وتحديد الإجراءات على طول سلسلة القيادة فيما يتعلق بالمسؤولية والإبلاغ.

استنادًا إلى المعايير الدولية والوطنية، تتناول هذه اللبنة الأسس والأطر الأمنية، وتفحص العديد من الأطر الشاملة لتوضيح الأدوار والمسؤوليات لإدارة مخاطر الأمن السيبراني والاستجابة لحوادث الأمن السيبراني. وغالبًا ما يتم تلخيص أطر العمل هذه في شكل مصفوفة تفويض المسؤولية والمسائلة والقيادة والمعلومات (RACI). وتساعد أدوات تفويض المصفوفة هذه في إدارة عمليات الأمن السيبراني أيضًا. وسيتم استخدام مثالاً لأحد مخططات RACI باعتباره المثال التعليمي. وسيدرس الطلاب التصميم العام لهذه الأدوات قبل التطرق إلى مسؤولياتهم الوطنية ومصفوفات الاستجابة. وإذا أمكن، سيتم تحديد واستكشاف أدوات السياسة الوطنية الفعلية لإدارة عملية تفويض المسؤوليات والمهام. وستطرق المناقشة لأدوات دعم القرار وأدوات وأطر إدارة المخاطر والممارسات والمسؤوليات. وفي النهاية، سيعمل الطلاب على فحص إطار الإدارة المفوضة للأمن السيبراني المعتمد بواسطة حكومتهم الوطنية أو على الأقل بواسطة المنظمة التي يتبعونها.

قد تشمل مرونة النظام السيبراني الأنشطة التالية: إدارة الأصول، وإدارة الضوابط، وإدارة التكوين والتغيير، وإدارة التهديدات ومواطن الضعف، وتخطيط وإدارة استمرارية الخدمات، وإدارة التبعيات الخارجية، والتدريب، والتوعية التنظيمية والفردية، والإدارة الفعالة للوعي الظرفي.

نتائج التعلم

سيتمكن الطلاب من

- إثبات أنهم على دراية بمفهوم تخطيط مصفوفة المسؤولية وتفويضها؛
- استكشاف القضايا العامة المحيطة بتنفيذ استراتيجية الأمن السيبراني خاصتهم؛
- إدراك كيفية التفاعل مع القيادة الوطنية المعنية بالاستجابة للحوادث وهياكل المراقبة؛
- استيعاب الإدارة المفوضة للعمليات السيبرانية على المستوى الوطني؛
- فهم كيفية إدارة المخاطر السيبرانية في سياق السياسة الوطنية؛
- وفهم الجوانب الإيجابية والسلبية لأطر إدارة الموارد الرسمية المطبقة على سياق الأمن السيبراني الوطني.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

يمكن أن تشمل الموضوعات التي يتم تغطيتها نظام RACI أو الأدوات الخاصة بأي من مصفوفات المسؤولية المماثلة لمعالجة الحوادث والتعافي منها وإدارة الاستجابة.

طريقة/تقييم التعلم

ينبغي أن يقدم أحد الخبراء المتخصصون مسحًا موجزًا عن الطرق (مثل مخططات RACI) قبل تحديد أين توجد التوجيهات الصريحة والسلطات الوطنية والتنظيمية. ويمكن للخبير المتخصص بعد ذلك تحديد الطرق الأكثر ارتباطًا بتفاصيل الكتلة الطلابية.

ينبغي تطوير نظام التقييم بما يتوافق مع مستوى المعرفة والدراية المناسبة للدورات التدريبية المستمدة من هذه المنهج المرجعي.

المراجع

فرانسيس دومينغو، "السياسة السيبرانية في الصين"، الدراسات الأوروبية والآسيوية، 2015. معرّف الوثيقة الرقمي: 10.1080/09668136.2015.1102519. متوفر على: http://www.tandfonline.com/doi/full/10.1080/09668136.2015.1102519

تيوجا كوسيستو، رونو كوسيستو، "قيادة الأمن السيبراني في العلاقات بين القطاعين العام والخاص"، في آر كوش، جي رودوسك (محرران)، *إجراءات المؤتمر الخامس عشر بشأن الحرب والأمن السيبرانيين*، ميونخ، يوليو 2016. الرقم الدولي المعياري للكتاب 1910810932، 9781910810934.

ماري مالفينيشف، "أدوار وأهداف مكتب الأمن السيبراني". عرض تقديمي عبر الإنترنت بواسطة مكتب الأمن السيبراني في جورجيا، 2015. متوفر على: /www./slideplayer.com/slide/9759466

سارما، سانغاميترا. "آلية الأمن السيبراني في الاتحاد الأوروبي". (2016).

بول سيشونسكي، توم ميلار، تيم غرانس وكارين سكارفون، *دليل التعامل مع حوادث أمن الحاسوب: توصيات المعهد الوطني للمعايير والتقنية*، المنشور الخاص بالمعهد الوطني للمعايير والتقنية 800-61، الطبعة المنقحة 2، وزارة التجارة الأمريكية، أغسطس 2012.

محمد ظافر الشريف الكتاني وطيب دباغ، "مخطط RACI الوطني لإطار عمل "أمن سيبراني وطني" قابل للتشغيل المتبادل"، *إجراءات المؤتمر الأوروبي المعني بحرب وأمن المعلومات*، 2009.

مخططات المسؤولية (RACI). http://www.thecqi.org/Documents/community/South%20Western/Wessex%20Branch/CQI%20Wessex%20-%20RACI%20approach%207Sep10.pdf

وزارة الأمن الداخلي الأمريكية، *مراجعة المرونة السيبرانية (CRR): مجموعة أسئلة مع التوجيه*، جامعة كارنيجي ميلون، فبراير 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

سلسلة ISO 22300 وسلسلة ISO 27000 لدى المنظمة الدولية للمعايير - انظر القائمة السابقة.

T4-B3: التحاليل العدلية السيبرانية

الوصف

التحاليل العدلية السيبرانية عبارة عن تطبيق يضم أساليب التحقيق والتحليل بغرض جمع الأدلة الرقمية والاستفادة منها والمحافظة عليها. ويتألف مجال النشاط هذا من التحاليل العدلية الرقمية والتحاليل العدلية للأجهزة والتحاليل العدلية للعامل البشري. وبينما يعد النشاط العدلي عاملاً جوهريًا لصيانة الأنظمة وكفاءتها التشغيلية اليومية، قد يلزم فرض رقابة أكثر صرامة على هذه الأنشطة لإنتاج مواد إثباتية للتحقيقات الجنائية. وأخيرًا، توفر الممارسات العدلية الجيدة أدوات هامة لفهم كيف يسعى الخصوم إلى استغلال إمكانية الوصول إلى النظم القائمة عن طريق، على سبيل المثال، الكشف عن كيفية سعيهم للوصول إلى عُقدات القيادة والتحكم أو الكيفية التي يعملون من خلالها على تصميم البرمجيات الخبيثة.

تعرض هذه اللبنة التحديدات العدلية الرئيسية فيما يتعلق بإدارة الحوادث السيبرانية. ويمكن تطبيق الأساليب العدلية على التحقيق في الحوادث السيبرانية وجمع المعلومات الاستخبارتية والملاحقة القضائية بموجب إنفاذ القانون. وتشمل المواد التي سيتم تغطيتها الأدوات والأساليب اللازمة للحصول على البيانات من مصادر متعددة، وتحليل البيانات، ووضع جدولاً زمنيًا للأحداث. وقد تُستخدم هذه المواد لبناء حالة إسناد أو فيما يتعلق بمختلف أشكال أنشطة المتابعة، بدءًا من تتبع الأنشطة ورصدها حتى إقامة دعوى جنائية ضد الجناة. وسيدرس الطلاب أيضًا عملية جمع البيانات العدلية وفحصها فيما يتعلق بجرائم مالية مثل غسل الأموال.

سيتعلم الطلاب حول المسائل المرتبطة بجمع البيانات الخاصة بالتحاليل العدلية من مصادر متعددة، بما في ذلك أجهزة الحاسوب والشبكات وأجهزة الجوال وقواعد البيانات وأجهزة الاستشعار.

نتائج التعلم

سيُظهر الطلاب استيعابًا لما يلي

- المسائل المرتبطة بجمع البيانات الخاصة بالتحاليل العدلية من مصادر متعددة، بما في ذلك أجهزة الحاسوب والشبكات وأجهزة الجوال وقواعد البيانات وأجهزة الاستشعار؛
- أهمية تحليل البيانات العدلية لأغراض وضع جدولاً زمنيًا وتعيين الإسناد؛
- والقوانين واللوائح الوطنية المعنية بجمع البيانات دعمًا لإنفاذ القانون.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

- إنشاء نظامًا مرنًا لدعم التعافي بعد وقوع أي من الحوادث السيبرانية
- الفحص العدلي لعناصر الهندسة الاجتماعية التي يتم استغلالها للوصول إلى النظم
- الأجهزة التي يمكن أن تكون ذات قيمة للتحاليل العدلية
- استخدام نتائج التحقيق العدلي للملاحقة الجنائية
- الأدوات المؤتمتة للتحاليل العدلية العملياتية الأساسية

طريقة/تقييم التعلم

ينبغي أن تشمل أساليب التدريس محاضرات وعروض إيضاحية ومناقشة العديد من دراسات الحالة التي توضح مختلف العناصر العدلية.

ينبغي تطوير نظام التقييم بما يتوافق مع مستوى المعرفة والدراية المناسبة للدورات التدريبية المستمدة من هذه المنهج المرجعي.

وينبغي تقييم الطلاب بشكل شفوي وكتابي.

المراجع

ريستو فاراندي، باول نيزينسكي، مركز التميز في الدفاع السيبراني التعاوني التابع لحلف الناتو، تالين، إستونيا. 2013 "تحليل مقارن لحلول إدارة السجلات مفتوحة المصدر لمراقبة الأمن والتحليلات العدلية للشبكات" متوفر على: https://ccdcoe.org/sites/default/files/multimedia/pdf/VaarandiNizinski2013_Open-SourceLogManagementSolutions.pdf

زيوزين تشنغ، ميروسلاو كوتيسكي، كواي شو، هاوجين تشو، "إصدار خاص بشأن الأمن السيبراني والجريمة والتحليلات العدلية للشبكات والتطبيقات اللاسلكية". *شبكات الأمن والاتصالات*. المُجلّد 8، الإصدار 17. 2015. الرقم التسلسلي المعياري الدولي للمجلة: 1939-0122.

أوتيفا، ناتا، ميليفا أليسكاندرا؛ لوليسكي ماريو، "تحديد الأدلة العدلية للعديد من هجمات الويب"، *المجلة الدولية لتكنولوجيا الإنترنت والمعاملات المضمونة*, المجلد 6، العدد 1، لعام 2015 الرقم التسلسلي المعياري الدولي للمجلة: 1748-5703.

أكينولا أجيجولا، بافول زافارسكي، رون روهل، "مراجعة وتقييم مقارن للمبادئ التوجيهية للتحليلات العدلية للمنشور الخاص بالمعهد الوطني للمعلومات والتقنية 800-101 النسخة المنقحة 1: 2014 و2012 :ISO/IEC 27037". أوراق بحثية مُقدمة في "المؤتمر العالمي لأمن الإنترنت (2014 "WorldCon). الصفحات 66-73 .WorldCIS.2014.7028169/10.1109 متوفر من IEEE على: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7028169&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7028169

تشوي يانغسيو وجو يونغ لي وسونوه تشوي وجونغ هيون كيم وإكيون كيم. "مقدمة إلى نظام التحليلات العدلية للشبكات لتحليل الحوادث السيبرانية". المؤتمر الدولي الثامن عشر لتكنولوجيا الاتصالات المتقدمة لعام 2016 (ICACT) الصفحات 50-55. IEEE, 2016. سانثوش بابو وإس ماني ميجالاي، "التحقيق والاستكشاف العدلي السيبراني في بيئة الحوسبة السحابية،"*المجلة العالمية لعلوم وتكنولوجيا الحاسبات* ب: *الحوسبة السحابية والموزعة* 15 (العدد 1، الإصدار 1) 2015 https://globaljournals.org/GJCST_Volume15/1-Cyber-Forensic-Investigation.pdf

إبراهيم باجيلي وفرانك بريتينجر، مختبر أبحاث وتعليم التحليلات العدلية السيبرانية بجامعة نيو هيفن، "مصادر البيانات للنهوض بالتحليلات العدلية السيبرانية: ما الذي يتعين على العالم الاجتماعي عرضه،" *وثائق من منتدى الربيع الذي عقدته رابطة AAAI عام 2015* (بالو ألتو، جامعة ستانفورد بكاليفورنيا)، مارس 2015. http://www.researchgate.net/profile/Ibrahim_Baggili/publication/274065229_Data_Sources_for_Advancing_Cyber_Forensics_What_the_Social_World_Has_to_Offer/links/55134a630cf283ee0833818c.pdf

T4-B4: التدقيق والتقييم الأمني على المستوى الوطني

الوصف

يُعد تقييم التأهب الأمني دوراً هاماً للبلدان. فالتقييم يساعد في اختبار الضوابط الأمنية وكذلك تحديد الفجوات في البنية التحتية والسياسة الأمنية. ويمكن إجراء التقييم الأمني على مستويات متعددة. أولاً، يمكن اختبار الضوابط الأمنية الفردية باستخدام أدوات التدقيق. ثانياً، يمكن إجراء التقييم على مستوى شامل أو نظامي أو تنظيمي من خلال التمارين وعمليات المحاكاة في الوقت الحقيقي. وتتناول هذه اللبنة الأدوات والعمليات الخاصة بالتدقيقات والتقييمات الأمنية. وهذا سيُتيح للطلاب معرفة كيف يمكن تحديد ووزن التقييم الخاص بمدى الضعف المتبقي في الأنظمة؛ وعلاوة على ذلك، تساعد عمليات التقييم والتدقيق هذه في تحديد كيفية قياس استعداد النظم السيبرانية للتعامل مع أنواع محددة من جهات التهديد الفاعلة المعروفة والاستعداد للأنشطة التي ينشأ فيها تهديد غير معروف (ما يُسمى بالتهديدات الفورية لأنه لا يوجد تحذير بشأن الوسائل المحددة للهجوم أو العمل الخبيث لهذه التهديدات).

وتتنوع أدوات وتقنيات الوعي الذاتي بالأمن السيبراني على المستوى الشخصي والمنظمي، حيث تتراوح من عمليات الاستبيان إلى الأدوات التقنية. وتهدف هذه اللبنة إلى زيادة استيعاب دور الوعي الذاتي من حيث اتصاله بالأمن السيبراني للفرد والمنظمة. ويُعتبر تحليل نقاط القوة والضعف في الأدوات والنُهُج المختلفة أمراً حيوياً لاستيعاب قيمة تلك الأدوات والنُهُج. ويمكن أن يعمل التقييم الذاتي المستمر على الحد من المخاطر. كما تُمثل مراعاة التحيزات المُحتملة عاملاً حيوياً في التقييم الذاتي المُفيد. ويُعد التنفيذ الإجرائي للنتائج عنصراً ضرورياً لأي جهد مبذول في التقييم الذاتي. ونظراً لأن مستوى الأمن يرتبط بقيمة أو أهمية أو حساسية ما يجري تأمينه، فليس هناك نمط واحد يتعين تبنيه أو تطبيقه ببساطة. وبدلاً من ذلك، سيعتمد المستوى المرغوب من الأمن السيبراني على المعايير المُختارة ومستوى الأداء الذي يلزم ضمانه.

نتائج التعلم

سيتمكن الطلاب من

- استيعاب أهمية أدوات التدقيق والتقييم الأمني، و
- تقييم وتطبيق أدوات وتقنيات التقييم الذاتي المناسبة في سياق وطني.

مسائل يمكن مراعاتها في الوحدات والنهُج المحتملة

قد تشمل الموضوعات التي يلزم تناولها ما يلي:

- الممارسات الجيدة في المنظمات التي تستخدم التقييم الذاتي
- مناقشة دراسات حالة بالنسبة للحالات التي يمكن أن يكون الوعي الذاتي فيها قد عمل على زيادة الأمن

طريقة/تقييم التعلم

ينبغي على الطلاب التدريب باستخدام أداة وطنية للتقييم الذاتي إن وجدت، وإن لم تكن متوفرة، يمكنهم استخدام أداة تقييم الأمن السيبراني (CSET) المتوفرة من خلال وزارة الأمن الداخلي الأمريكية أو استخدام نهج مماثل. قد يكون من المفيد مقارنة أي طريقة وطنية موجودة، أياً كانت، بالطريقة التي تتبناها وزارة الأمن الداخلي الأمريكية.

ينبغي تطوير نظام التقييم بما يتوافق مع مستوى المعرفة والدراية المناسبة للدورات التدريبية المستمدة من هذه المنهج المرجعي.

المراجع

إيفان ألكوفورادو، "الاستفادة من معايير الصناعة لمعالجة مخاطر الأمن السيبراني الصناعي"، *مجلة اتحاد تدقيق ومراقبة أنظمة المعلومات*، المجلد 6، 2014؛ الرقم التسلسلي المعياري الدولي للمجلة: 1944-1967.

ستيفان لوب، راينر بوهمي (إدارة نظم المعلومات، جامعة مونستر، ألمانيا؛ معهد علوم الحاسوب، جامعة إنسبروك، النمسا)، "اقتصاديات الإبلاغ الإلزامي عن المخالفات الأمنية للسلطات". متوفر على: http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_laube.pdf

يوليا شيردانتسيفا، وآخرون "مراجعة أساليب تقييم مخاطر الأمن السيبراني لأنظمة SCADA". دراسة إلكترونية. متوفرة في المكتبة البريطانية، المرجع: رقم المُعرِّف الفريد: ETOCvdc_100030733535.0x000001.

أبهيجيت غوبتا، سوبارنا شكيا، "تدقيق نظم المعلومات؛ دراسة للأمن والتحديات في نيبال"، في المجلة الدولية لعلوم الحاسوب وأمن المعلومات، المجلد 13، العدد 11 (نوفمبر 2015) الصفحات 4-1. الرقم التسلسلي المعياري الدولي للمجلة: 1947-5500.

بيلجي كاراباكاك وسيفجي أوزكان يلديريم ونازييف بيكال. "النهج التنظيمية للأمن السيبراني للبُنى التحتية الحيوية: دراسة حالة تركيا." مجلة مراجعة قانون وأمن الحاسوب 32، العدد 3 (2016): 526-539.

معهد استمرارية الأعمال، *المبادئ التوجيهية للممارسات الجيدة 2013، الطبعة العالمية: دليل الممارسات الجيدة العالمية في استمرارية الأعمال* (إنجلترا)، 2013. http://www.thebci.org/index.php/resources/the-good-practice-guidelines

المجلس الدولي لمعايير مراجعة الحسابات والضمان، معيار ISAE 3402 بشأن الإبلاغ عن الضوابط في منظمات الخدمة http://isae3402.com/ISAE3402_overview.html

المنظمة الدولية للمعايير/اللجنة الكهروتقنية الدولية، *ISO/IEC 15408: المعايير المشتركة لتقييم أمن تكنولوجيا المعلومات، الإصدار 3.1، النسخة المنقحة 4,* CCMB-2012-09-001، سبتمبر 2012. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

كيث ستوفر وجوفالكو وكارين سكارفون، *المنشور الخاص بالمعهد الوطني للمعايير والتقنية 82-800: دليل أمن نظم التحكم الصناعية*، المعهد الوطني للمعايير والتقنية، وزارة التجارة الأمريكية، يونيو 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

وزارة الأمن الداخلي الأمريكية، *مراجعة المرونة السيبرانية (CRR): حزمة التقييم الذاتي*، جامعة كارنيجي ميلون، فبراير 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf

وزارة الأمن الداخلي الأمريكية، *مراجعة المرونة السيبرانية (CRR): مجموعة أسئلة مع التوجيه*، جامعة كارنيجي ميلون، فبراير 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

الاختصارات

APT	التهديد المستمر المتقدم
AS	النظام المستقل (تقسيم فرعي منفصل للإنترنت)
ASN	رقم النظام المستقل
BGP	بروتوكول البوابة الحدودية
BSA	البنية الأمنية الأساسية
BYOD	نظام "أحضر جهازك الخاص"
CERT	فريق الاستجابة للطوارئ السيبرانية
COBIT	أهداف التحكم في المعلومات والتكنولوجيا ذات الصلة
COMSEC	أمن الاتصالات
CSET	أداة تقييم الأمن السيبراني
CSET	أداة تقييم الأمن السيبراني
DDoS	رفض الخدمة الموزع
DHS	وزارة الأمن الداخلي الأمريكية
DNS	نظام اسم النطاق
DoS	رفض الخدمة
ENISA	الوكالة الأوروبية لأمن الشبكات والمعلومات
ESCWG	فريق العمل المعني بالتحديات الأمنية الناشئة
FTP	بروتوكول نقل الملفات
HTTP	بروتوكول نقل النص التشعبي
HTTP	بروتوكول نقل النص التشعبي الأمن
IANA	سلطة أرقام الإنترنت المخصصة
ICANN	هيئة الإنترنت للأسماء والأرقام المخصصة
ICS	نظام التحكم الصناعي
ICT	تكنولوجيا المعلومات والاتصالات
IDS	نظام كشف التسلل
IGF	منتدى إدارة الإنترنت
IP	بروتوكول الإنترنت
IS	أمن المعلومات
ISACA	اتحاد تدقيق ومراقبة أنظمة المعلومات
ISO	المنظمة الدولية للمعايير
ISP	مزود خدمة الإنترنت
IT	تكنولوجيا المعلومات
ITU	الاتحاد الدولي للاتصالات
LAN	شبكة المنطقة المحلية
NIR	سجل الإنترنت الوطني
NIST	المعهد الوطني للمعايير والتقنية (بالولايات المتحدة)
PfPC	اتحاد الشراكة من أجل السلام التابع لأكاديميات الدفاع ومعاهد الدراسات الأمنية
PIT نظام	نظام تكنولوجيا معلومات المنصات
RACI	المسؤولية والمساءلة والقيادة والمعلومات
SCADA	التحكم الاشرافي والاستحواذ على البيانات
SCRM	إدارة مخاطر سلسلة التوريد
SFTP	بروتوكول نقل الملفات الآمن
SIEM	إدارة المعلومات والأحداث الأمنية
SME	خبير متخصص

البروتوكول البسيط لنقل البريد	**SMTP**
لغة الاستعلامات المركبة	**SQL**
الصدفة الآمنة	**SSH**
طبقة مآخذ التوصيل الآمنة	**SSL**
بروتوكول التحكم في الإرسال	**TCP**
نموذج تقييم التهديدات والمخاطر	**نموذج TRA**
معهد الأمم المتحدة لبحوث نزع السلاح	**UNIDIR**

مسرد المصطلحات

ملاحظة: لا تظهر جميع المصطلحات الواردة أدناه في النص السابق، ولكن قد يكون العديد منها مفيدًا في صياغة تمارين تعلُّم محددة وما إلى ذلك.

A

access control mechanism (آلية التحكم في الوصول)
التعريف: تدابير أمنية مصممة لكشف ومنع الوصول غير المصرح به والسماح بالوصول المصرح به إلى نظام معلومات أو مرفق مادي.

الهجوم النشط التعريف: اعتداء فعلي من قبل مصدر تهديد متعمد يحاول تغيير نظام ما أو موارده أو بياناته أو عملياته.

التهديد (التهديدات) المتقدم المستمر التعريف: خصم يمتلك مستويات متطورة من الخبرة والموارد الكبيرة التي تسمح له بخلق فرص لتحقيق أهدافه باستخدام العديد من موجهات الهجوم (على سبيل المثال، السيبرانية والفيزيائية والخداعية). مأخوذ من: النسخة المنقحة رقم 4 من المنشور الخاص800-53 للمعهد الوطني للمعايير والتقنية

برنامج الحماية من الفيروسات التعريف: برنامج يراقب جهاز الحاسوب أو الشبكة للكشف عن أنواع رئيسية من التعليمات البرمجية الخبيثة أو التعرف عليها ولمنع أو احتواء حوادث البرامج الضارة، أحيانا عن طريق إزالة أو تحييد التعليمات البرمجية الخبيثة.

الهجوم التعريف: محاولة للوصول غير المصرح به إلى خدمات النظام أو موارده أو معلوماته أو محاولة لتعريض سلامة النظام للخطر.

نمط الهجوم التعريف: أحداث أو سلوكيات سيبرانية مماثلة قد تشير إلى أن هجومًا ما قد وقع أو يقع حالياً، مما يؤدي إلى انتهاك أمني أو انتهاك أمني محتمل.

توقيع الهجوم التعريف: خاصية أو نمط مميز يمكن البحث عنه أو يمكن استخدامه في إجراء مطابقة للهجمات المحددة سابقاً.

سطح الهجوم التعريف: مجموعة من الطرق التي يمكن للخصم دخول النظام من خلالها ويحتمل أن يسبب الضرر. تعريف موسع: خصائص نظام المعلومات التي تسمح للخصم بالفحص أو الهجوم أو الحفاظ على وجوده في نظام المعلومات. مُقتبس من: بي كيه مانهاتا وجيه إم وينج في قياس سطح الهجوم, http://www.cs.cmu.edu/~pratyus/as.html#introduction

التحقق التعريف: عملية التحقق من الهوية أو السمات الأخرى الخاصة بكيان ما (مستخدم أو عملية أو جهاز). تعريف موسع: تعني أيضاً عملية التحقق من مصدر البيانات وصحتها.

B

شبكة الروبوت التعريف: مجموعة ضخمة من أجهزة الحاسوب التي تم تعريضها للخطر من خلال التعليمات البرمجية الخبيثة والتحكم فيها عبر شبكة ما.

أمن البناء التعريف: مجموعة من المبادئ والممارسات والأدوات التي تُستخدم لتصميم وتطوير واستنباط أنظمة وبرامج المعلومات التي تعمل على تعزيز المرونة تجاه نقاط الضعف والأخطاء والهجمات.

C

القدرة التعريف: توافر الوسائل اللازمة لإنجاز مهمة أو وظيفة أو هدف ما.

الحوسبة السحابية التعريف: نموذج لتمكين وصول الشبكة عند الطلب لمجموعة مشتركة من قدرات أو موارد الحوسبة القابلة للتكوين (مثل الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بأقل جهد إداري أو تفاعل من مزود الخدمة.

تحليل دفاع الشبكة الحاسوبية التعريف: حيث يستخدم الشخص التدابير والمعلومات الدفاعية التي يتم جمعها من مجموعة متنوعة من المصادر لتحديد وتحليل والإبلاغ عن الأحداث التي تحدث أو قد تحدث داخل الشبكة من أجل حماية المعلومات ونظم المعلومات والشبكات من التهديدات.

البنية التحتية الحيوية التعريف: النظم والأصول، سواءً أكانت مادية أم افتراضية، ذات الأهمية الحيوية للمجتمع والتي يمكن أن يكون لعجزها أو تدميرها أثر مضاعف على الأمن أو الاقتصاد أو الصحة العامة أو السلامة أو البيئة أو أي مزيج من هذه الأمور.

التشفير التعريف: استخدام التقنيات الرياضية لتوفير خدمات الأمن، مثل السرية وسلامة البيانات والتحقق من الكيان والتحقق من مصدر البيانات.

النظام البيئي السيبراني التعريف: البنية التحتية المعلوماتية المترابطة بشأن التفاعلات بين الأشخاص والعمليات والبيانات وتكنولوجيا المعلومات والاتصالات، جنبًا إلى جنب مع البيئة والظروف التي تؤثر على تلك التفاعلات

الأمن السيبراني: تعريف مُختصر: "النشاط أو العملية أو القدرة أو الإمكانية أو الحالة التي يجري من خلالها حماية أنظمة المعلومات والاتصالات بالإضافة إلى المعلومات الواردة فيها و/أو الدفاع عنها ضد الضرر أو الاستخدام غير المصرح به أو التعديل أو الاستغلال." تعريف موسع: الاستراتيجية والسياسة والمعايير المتعلقة بأمن وعمليات الفضاء السيبراني، والتي تشمل المجموعة الكاملة من سياسات وأنشطة الحد من التهديدات والحد من الضعف والردع والمشاركة الدولية والاستجابة للحوادث والمرونة والتعافي، بما في

ذلك عمليات الشبكة الحاسوبية وضمان المعلومات وإنفاذ القانون والدبلوماسية والبعثات العسكرية والاستخباراتية من حيث صلتها بأمن واستقرار البنية التحتية العالمية للمعلومات والاتصالات. مُقتبس من: CNSSI 4009، النسخة المنقحة رقم 4 من المنشور الخاص 800-53 الصادر عن المعهد الوطني للمعايير والتقنية، NIPP، هدف التأهب الوطني لوزارة DHS؛ مجلة مراجعة سياسة الفضاء السيبراني بالبيت الأبيض، مايو 2009.

الفضاء السيبراني التعريف: العالم الإلكتروني الذي أنشأته شبكات مترابطة لتكنولوجيا المعلومات والمعلومات الموجودة على تلك الشبكات.

D

استخراج البيانات التعريف: العملية أو التقنيات المستخدمة في تحليل مجموعات كبيرة من المعلومات الموجودة لاكتشاف أنماط أو علاقات وثيقة لم يسبق اكتشافها.

رفض الخدمة التعريف: هجوم يمنع أو يعوق الاستخدام المصرح به لموارد نظام المعلومات أو خدماته.

التحليلات العدلية الرقمية التعريف: العمليات والتقنيات المتخصصة المُستخدمة في جمع واستبقاء وتحليل البيانات المتعلقة بالنظام (الأدلة الرقمية) لأغراض التحقيق.

إدارة الحقوق الرقمية التعريف: شكل من أشكال تكنولوجيا التحكم في الوصول لحماية وإدارة استخدام المحتوى الرقمي أو الأجهزة الرقمية وفقا لنوايا موفر المحتوى أو الجهاز.

رفض الخدمة الموزع التعريف: تقنية لرفض الخدمة تستخدم أنظمة متعددة لتنفيذ الهجوم بصورة متزامنة.

E

إدارة مخاطر المؤسسة التعريف: نهج شامل لإدارة المخاطر يعمل على إشراك الأفراد والعمليات والأنظمة عبر المنظمة لتحسين جودة اتخاذ القرارات المتعلقة بإدارة المخاطر التي قد تعرقل قدرة المنظمة على تحقيق أهدافها.

التغرة التعريف: تقنية لخرق أمن الشبكة أو نظام المعلومات فيما يمثل انتهاكاً للسياسة الأمنية.

F

جدار الحماية التعريف: إمكانية تعمل على الحد من المرور الشبكي بين الشبكات و/أو أنظمة المعلومات.

H

المتسلل التعريف: مُستخدم غير مصرح له يُحاول الوصول أو يتمكن من الوصول إلى نظام المعلومات.

I

تهديد سلسلة التوريد الخاصة بنظام ICT التعريف: تهديد اصطناعي يتحقق من خلال استغلال سلسلة التوريد الخاصة بنظام تكنولوجيا المعلومات والاتصالات (ICT)، بما في ذلك عمليات الاستحواذ.

التهديد من الداخل التعريف: شخص أو مجموعة أشخاص من داخل المنظمة يُشكلون خطراً محتملاً من خلال انتهاك سياسات الأمن. تعريف موسع: واحد أو أكثر من الأفراد الذين لديهم حق الوصول و/أو المعرفة الداخلية بالشركة أو المنظمة أو المؤسسة مما يسمح لهم باستغلال نقاط الضعف الموجودة بأمن هذا الكيان أو أنظمته أو خدماته أو منتجاته أو مرافقه بقصد إلحاق الضرر به.

إدارة المخاطر المتكاملة التعريف: النهج المنظم الذي يمكّن المؤسسة أو المنظمة من تبادل المعلومات المتعلقة بالمخاطر وتحليل المخاطر ومزامنة استراتيجيات إدارة المخاطر المستقلة التكميلية لتوحيد الجهود عبر المؤسسة.

التسلل التعريف: تصرف غير مصرح به يتمثل في تجاوز الآليات الأمنية لإحدى الشبكات أو أنظمة المعلومات.

كشف التسلل التعريف: العملية والطرق المستخدمة لتحليل المعلومات من الشبكات ونظم المعلومات لتحديد ما إذا كان قد حدث خرق أو انتهاك أمني.

K

المسجّل الأساسي التعريف: البرامج أو الأجهزة التي تتعقب النقرات على المفاتيح وأحداث لوحة المفاتيح، عادةً ما تكون بشكل خفي/سري، لمراقبة الأفعال التي يقوم بها مستخدم نظام المعلومات.

M

التعليمات البرمجية الخبيثة التعريف: رموز برمجية تهدف إلى أداء وظيفة أو عملية غير مصرح بها يكون لها تأثير سلبي على سرية نظام المعلومات أو سلامته أو توافره.

البرامج الضارة التعريف: برامج تضر بتشغيل النظام عن طريق أداء وظيفة أو عملية غير مصرح بها.

N

مرونة الشبكة التعريف: قدرة الشبكة على (1) توفير التشغيل المستمر (أي مقاومة بدرجة عالية للتوقف وقادرة على العمل في وضع متدهور إذا لحق بها ضرر)؛ و(2) التعافي بشكل فعال إذا حدث فيها فشل و(3) الارتقاء بالأداء لتلبية مطالب سريعة أو لا يمكن التنبؤ بها.

عدم التنصل التعريف: خاصية تتحقق من خلال أساليب التشفير للحماية ضد إنكار الفرد أو الكيان على نحو كاذب قيامه بعمل معين يتعلق بالبيانات. تعريف موسع: خاصية توفر القدرة على تحديد ما إذا كان شخص معين قد قام بعمل مُعين، مثل إنشاء معلومات أو إرسال رسالة أو الموافقة على معلومات أو استلام رسالة.

P

الهجوم السلبي التعريف: اعتداء فعلي من قبل مصدر تهديد متعمد يحاول معرفة أو استخدام المعلومات الموجودة على النظام ولكن دون محاولة تغيير النظام أو موارده أو بياناته أو عملياته.

التصيد الاحتيالي التعريف: صورة رقمية من صور الهندسة الاجتماعية التي تهدف إلى خداع الأفراد لحثهم على تقديم معلومات حساسة.

R

التكرار التعريف: أنظمة أو أنظمة فرعية أو أصول أو عمليات إضافية أو بديلة تحتفظ بدرجة من الأداء الوظيفي الكلي في حالة فقدان أو فشل الأنظمة أو الأنظمة الفرعية أو الأصول أو العمليات الأخرى.

المرونة التعريف: القدرة على التكيف مع الظروف المتغيرة والاستعداد للتعطل ومقاومته والتعافي منه سريعاً.

تحليل المخاطر التعريف: الفحص المنهجي لمكونات وخصائص المخاطر.

تقييم المخاطر التعريف: المنتج أو العملية التي يتم فيها جمع المعلومات وتعيين القيم للمخاطر لغرض الاستفادة منها في الأولويات أو تطوير أو مقارنة مسارات العمل والاستفادة منها في عملية صنع القرار. تعريف موسع: تقدير المخاطر التي تواجه الكيان أو الأصول أو النظام أو الشبكة أو العمليات التنظيمية أو الأفراد أو المنطقة الجغرافية أو المنظمات الأخرى أو المجتمع؛ ويشمل تحديد الحد الذي يمكن عنده أن تؤدي الظروف أو الأحداث المعاكسة إلى عواقب ضارة.

إدارة المخاطر التعريف: عملية تحديد وتحليل وتقييم ومشاركة المخاطر وقبولها وتجنبها ونقلها أو السيطرة عليها عند مستوى مقبول مع مراعاة التكاليف والمنافع المرتبطة بأي إجراءات يتم اتخاذها. تعريف موسع: تشمل (1) إجراء تقييم للمخاطر؛ و(2) تنفيذ استراتيجيات لتخفيف المخاطر؛ و(3) رصد المخاطر باستمرار مع مرور الوقت؛ و(4) توثيق البرنامج العام لإدارة المخاطر.

S

الرسائل الاقتحامية التعريف: إساءة استخدام أنظمة المراسلة الإلكترونية لإرسال رسائل جماعية غير مرغوب فيها بشكل عشوائي.

الانتحال التعريف: تزوير عنوان الإرسال في رسالة ما للحصول على دخول غير قانوني (غير مصرح به) إلى نظام آمن.

برامج التجسس التعريف: البرامج التي يتم تثبيتها سرا أو خفيةً في نظام المعلومات دون علم مستخدم النظام أو مالكه.

التحكم الاشرافي والاستحواذ على البيانات (SCADA) التعريف: اسم عام لنظام محوسب قادر على جمع ومعالجة البيانات وتطبيق الضوابط التشغيلية على الأصول المشتتة جغرافيا عبر مسافات طويلة.

سلسلة التوريد التعريف: نظام يتكون من المنظمات والأفراد والأنشطة والمعلومات والموارد اللازمة لإنشاء ونقل المنتجات، بما في ذلك مكونات المنتج و/أو الخدمات التي تُقدّم من الموردين إلى عملائهم.

إدارة مخاطر سلسلة التوريد التعريف: عملية تحديد وتحليل وتقييم مخاطر سلسلة التوريد وقبولها وتجنبها ونقلها أو السيطرة عليها عند مستوى مقبول مع مراعاة التكاليف والمنافع المرتبطة بأي إجراءات يتم اتخاذها.

T

التهديد التعريف: ظرف أو حدث يتضمن أو يشير إلى إمكانية استغلال نقاط الضعف والتأثير سلبًا (خلق عواقب سلبية) على العمليات التنظيمية أو الأصول التنظيمية (بما في ذلك المعلومات وأنظمة المعلومات) أو الأفراد أو المنظمات الأخرى أو المجتمع.

جهة التهديد الفاعلة/عنصر التهديد التعريف: فرد أو جماعة أو منظمة أو حكومة تمارس أو تعتزم القيام بأنشطة ضارة.

تقييم التهديد التعريف: منتج أو عملية تحديد أو تقييم الكيانات أو الإجراءات أو الحوادث، سواء كانت طبيعية أو اصطناعية، التي تتضمن أو تشير إلى احتمال إلحاق الضرر بالحياة و/أو المعلومات و/أو العمليات و/أو الممتلكات.

موجه التهديد التعريف: وسائل إيقاع التهديد على الهدف أو مسار النهج المتخذ لتحقيق التهديد.

حصان طروادة التعريف: برنامج حاسوبي يبدو أنه يتمتع بوظيفة مفيدة ولكنه لديه أيضاً وظيفة خفية وربما خبيثة تهرب من آليات الأمن، أحياناً عن طريق استغلال تصريحات مشروعة لكيان نظام يطلب البرنامج.

U

الوصول غير المصرح به التعريف: أي وصول ينتهك سياسة الأمن المُعلنة.

V

الفيروس التعريف: برنامج حاسوبي يمكنه تكرار نفسه وإصابة جهاز حاسوب دون إذن أو معرفة المستخدم ثم الانتشار أو التفشي في جهاز حاسوب آخر.

نقطة الضعف التعريف: خاصية أو ضعف محدد يجعل المنظمة أو الأصول (مثل المعلومات أو نظام المعلومات) معرضاً للاستغلال من خلال تهديد معين أو عرضة لأخطار معينة.

W

الدودة الحاسوبية التعريف: برنامج مستقل ذاتي التكرار وذاتي الانتشار يَستخدم الآليات الشبكية لنشر نفسه.

Z

الثغرة الفورية التعريف: هجوم يستغل ضعف غير معترف به، يتم إطلاقه دون سابق إنذار ولا يُكتشف إلا وقت حدوثه.

مستمد ومنقول من مسرد مصطلحات المبادرة الوطنية لوظائف الأمن السيبراني ودراساته (NICCS) لدى وزارة الأمن الداخلي الأمريكية، إلى جانب مواد أخرى.

قادة الفرق والمحررون: أعضاء فريق ومستشارو المناهج - سين إس. كوستيجان ومايكل هينيسي:

الاسم	الجنسية	المؤسسة التابع لها	
د. عطا أتالاي	تركيا	رئيس قسم، سكرتير عام، مجلس الأمن القومي	
السيدة/ ماريا أفديفا	أوكرانيا	مدير تطوير دولي جامعة خاركوف الوطنية للقانون	
السيدة/ ألكسندرا بيلسكا	بولندا	مستشار، آي انتليجنس	
السيد/ جويسيبي كونتي	إيطاليا	كبير مسؤولي التكنولوجيا، تريلوجيس	
السيد/ سين إس كوستيجان	الولايات المتحدة الأمريكية	أستاذ، مركز جورج كاتليت مارشال الأوروبي للدراسات الأمنية	
السيد/ جون دي أندوراين	فرنسا	منسق، برامج تعليم الدفاع موظفو الناتو الدوليين	
المقدم/ ديرك دوبويس	بلجيكا	كلية الدفاع والأمن الأوروبية	
د. ديفيد إمليفيونو	كندا	ضابط أركان أول، الشراكة التعليمية، تكوين الأفراد العسكريين وزارة الدفاع الوطني	
السيد/ ديفيد فرانكو	الولايات المتحدة الأمريكية	عميل خاص إشرافي، مكتب التحقيقات الفدرالي	

د. بيوتر غوليتشيك	بولندا	ممثل شؤون الجامعة للابتكار جامعة الدفاع الوطني	
د. سانجاي جول	الولايات المتحدة الأمريكية	مدير أبحاث، مركز نيويروك للتحاليل العدلية وضمان المعلومات جامعة ألباني بولاية نيويورك	
السيد/ أندريا جوتسيريدز	جورجيا	مدير مكتب الأمن السيبراني وزارة الدفاع	
السيد/ أرمان جريجوريان	أرمينيا	رئيس فريق الأمن السيبراني، معهد الدراسات الاستراتيجية الوطنية	
د. مايكل أيه هينيسي	كندا	أستاذ/ مساعد نائب الرئيس، الأبحاث الكلية العسكرية الملكية في كندا	
القائد أندريس هيلدنبراند	ألمانيا	أستاذ، مركز جورج كاتليت مارشال الأوروبي للدراسات الأمنية	
د. دينوس كيريجان-كيرو	أيرلندا	مُعلّم، قسم الحاسوب والعلوم الرياضية جامعة جرينيتش	
د. سكوت نايت	كندا	أستاذ/رئيس قسم الحاسوب والعلوم الرياضية الكلية العسكرية الملكية في كندا	
السيد/ فريدريك لابار	كندا	مدير برامج، اتحاد الشراكة من أجل السلام التابع لأكاديميات الدفاع ومعاهد الدراسات الأمنية	
السيد/ فيليب لارك	الولايات المتحدة الأمريكية	مدير، برنامج بشأن الأمن السيبراني مركز جورج كاتليت مارشال الأوروبي للدراسات الأمنية	

د. جوستاف ليندستروم	السويد	رئيس برامج، التحديات الأمنية الناشئة مركز جنيف للسياسة الأمنية	GCSP
د. فاختانغ مايسايا	جورجيا	أستاذ، برنامج ماجستير في الأمن الدولي جامعة القوقاز الدولية	
د. بيتار مولوف	بلغاريا	أستاذ مساعد، معهد بحوث الدفاع المتقدمة	
السيد/ كريس بالاريس	المملكة المتحدة	مدير، آي انتليجنس	I-INTELLIGENCE
السيد/ دانيال بيدر باج	جمهورية التشيك	متخصص في مجلس الأمن/السياسة السيبرانية، هيئة الأمن الوطني	NBU
السيد/ رفائيل بيرل	الولايات المتحدة الأمريكية	مدير، اتحاد الشراكة من أجل السلام التابع لأكاديميات الدفاع ومعاهد الدراسات الأمنية	
السيدة/ ماكا بترياشفيلي	جورجيا	رئيس قسم الموارد البشرية، وزارة الدفاع	
السيدة/ ستيلا بتروفا	بلغاريا	مستشار، شبكة القيادة الأوروبية	European Leadership Network
د. بنيامين بوغوسيان	أرمينيا	نائب مدير، معهد الدراسات الاستراتيجية الوطنية	
السيد/ أوليكساندر بوتيل	أوكرانيا	أستاذ أمن تكنولوجيا المعلومات، جامعة خاركوف للقوات الجوية	

د. ديتليف بوهل	ألمانيا	مستشار أول، قسم التحديات الأمنية الناشئة، موظفو الناتو الدوليين	
السيد/ نيل روبنسون	المملكة المتحدة	قائد فريق البحوث راند يوروب	
السيد/ جيجي رومان	رومانيا	التعليم الموزع المتقدم، مدرسة الناتو في أوبرميرجاو	
المقدم/ جينادي سافونوف	مولدوفا	قسم الاتصالات والمعلوماتية أكاديمية مولدوفا العسكرية	
السيد/ دانيلو شيفشينكو	أوكرانيا	مدير مشروعات، مركز الأبحاث الاستراتيجية والابتكار	
السيدة/ ناتاليا سبينو	مولدوفا	رئيس، مركز الأمن السيبراني، مستشارية الدولة في مولدوفا	
د. ألان جي ستولبرج	الولايات المتحدة الأمريكية	منسق، التعليم الدفاعي مؤسسة راند	
د. تودور تاجاريف	بلغاريا	أستاذ/رئيس، قسم "تكنولوجيا المعلومات للأمن" ومركز إدارة الأمن والدفاع	
د. رونالد تايلور	الولايات المتحدة الأمريكية	رئيس، مركز القيادة الاستراتيجية في البيئات المعقدة	
السيد/ بوجدان أودريست	رومانيا	خبير أمن نظم المعلومات، بعثة الرصد التابعة للاتحاد الأوروبي	
السيد/ جوزيف فان	الولايات المتحدة الأمريكية	أستاذ، مركز جورج كاتليت مارشال الأوروبي للدراسات الأمنية	

1217-16 NATO Graphics & Printing – ISBN 978-92-845-0196-0

فريق التحرير ومحررو

التوزيع:

سين إس كوستجان
أستاذ
مركز جورج كاتليت مارشال الأوروبي للدراسات الأمنية
جيرناكيرستراس 2
82467 غارميش-بارتنكيرشن، ألمانيا
sean.costigan@pfp-consortium.org

مايكل إيه هينيسي، دكتور
أستاذ التاريخ ودراسات الحرب
مساعد نائب المدير - البحوث
الكلية العسكرية الملكية في كندا
ص.ب STN FORCES 17000
كينجستون، أونتاريو كندا
K7K 7B4
Hennessy-m@rmc.ca

منسق التخطيط/التوزيع:

غابرييلا لودويغ-جيندارم
فريق العمل الدولي للناتو
lurwig.gabriella@hq.nato.int