CYBERSÉCURITÉ
PROGRAMME DE RÉFÉRENCE GÉNÉRIQUE

CYBERSÉCURITÉ
PROGRAMME DE RÉFÉRENCE GÉNÉRIQUE

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.

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

NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
QUARTIER GÉNÉRAL DU COMMANDANT SUPRÊME ALLIÉ
TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

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

À : Voir liste de distribution

OBJET : Entérinement du programme de référence pour la cybersécurité élaboré par le groupe de travail sur les défis de sécurité émergents du Groupement PPP en tant que document de référence en matière de formation OTAN

DATE : 27 septembre 2016

1. Afin de répondre aux besoins spécifiques de certains partenaires en matière de formation et d'entraînement, le groupe de travail sur les défis de sécurité émergents (ESCWG) du Groupement d'institutions d'études de défense et de sécurité du Partenariat pour la paix (Groupement PPP) a élaboré un programme de référence pour la cybersécurité. Il convient de saluer le travail, le professionnalisme et le dévouement de celles et ceux qui ont contribué à ce projet.

2. Ce programme de référence a été jugé compatible avec le système OTAN de formation et d'entraînement à la cyberdéfense, et j'ai la conviction qu'il pourra servir de référence aux pays partenaires désireux de concevoir et d'élaborer des programmes et des formules de cours dans le domaine de la formation militaire professionnelle à la cybersécurité. Il contribuera également à améliorer l'interopérabilité militaire entre l'OTAN et ses partenaires ainsi qu'à renforcer la collaboration dans la perspective d'un système de formation et d'entraînement capable de s'adapter à l'évolution des besoins.

3. J'ai le plaisir d'apporter mon soutien au groupe de travail sur les défis de sécurité émergents du Groupement PPP en publiant ce programme de référence pour la cybersécurité en tant que document OTAN. J'invite tous les concepteurs de programmes de formation associés à l'élaboration d'offres pédagogiques dans ce domaine au sein des pays partenaires à exploiter pleinement ce manuel.

4. Pour toute question, veuillez contacter M. Salih Cem Kumsal, point de contact pour la discipline de formation et d'entraînement OTAN « cyberdéfense » (tél. : +1 (757) 747-3386, NCN : 555-3386, e-mail : cem.kumsal@act.nato.int).

POUR LE COMMANDANT SUPRÊME ALLIÉ TRANSFORMATION :

(signé) Stefano Vito Salamida
Général de division aérienne, ITAAF
Chef d'état-major adjoint pour l'instruction des forces interarmées

À propos de ce programme de référence

Le présent document est le fruit du travail d'une équipe multinationale d'universitaires et de chercheurs bénévoles issus des 17 nations associées au Groupe de travail sur les défis de sécurité émergents (ESCWG, Emerging Security Challenges Working Group) du Groupement du Partenariat pour la paix. L'objectif initial de ce projet était de mettre sur pied une approche à la fois flexible et intégrée de la question de la cybersécurité.

Le présent document a pour but d'aborder la question de la cybersécurité dans ses grandes lignes, mais néanmoins de façon suffisamment détaillée pour que les non-spécialistes puissent appréhender l'ensemble des enjeux technologiques qu'elle implique, d'une part, et que les experts en technologie puissent affiner leur compréhension des politiques de sécurité nationale et internationale et de leurs implications sur les questions de défense, d'autre part. Nous proposons une subdivision logique de cette grande thématique en différentes catégories, en suggérant le niveau de connaissance à acquérir par les différents publics auxquels ce document s'adresse et en indiquant des références utiles. Chaque État adoptant le programme pourra ainsi adapter le présent cadre de référence à ses besoins et aux profils des apprenants.

Nous remercions tout particulièrement le Groupement d'institutions d'études de défense et de sécurité du Partenariat pour la paix (PPP), dirigé par Raphael Perl, et les présidents de l'ESCWG, Detlef Puhl (OTAN) et Gustav Lindstrom (Centre de politique de sécurité de Genève), ainsi que les groupes de travail sur le programme de renforcement de la formation « Défense » (DEEP, Defence Education Enhancement Programme) et sur l'éducation du Groupement PPP, dirigés par Al Stolberg, Jean d'Andurain et David Emelifeonwu. Le rôle d'encadrement joué par plusieurs nations partenaires, dont l'Arménie, la Géorgie et la Moldavie, et le soutien direct et concret qu'elles ont apporté, ont grandement contribué au succès de cette initiative. Nous tenons aussi, et avant tout, à exprimer notre plus grande reconnaissance à toutes les personnes qui ont accepté d'apporter leur concours à l'élaboration de ce document. Lorsque nous leur avons proposé de participer à cette plongée de deux ans dans les arcanes de l'éducation à la cybersécurité, aucune n'a reculé devant l'ampleur de la tâche. Nous aimerions à ce titre adresser nos remerciements tout particuliers à Scott Knight, Dinos Kerigan-Kyrou, Philip Lark, Chris Pallaris, Daniel Peder Bagge, Gigi Roman, Natalia Spinu, Todor Tagarev, Ronald Taylor et Joseph Vann. Sans leur contribution, ce document n'aurait tout simplement pas pu voir le jour.

Sean S. Costigan et Michael A. Hennessy,
coordonnateurs de publication.

I. OBJECTIF DU PRÉSENT DOCUMENT

Le domaine de la cybersécurité[1] évolue très rapidement et de nouveaux défis ne cessent d'émerger. Le Groupement PPP a dès lors estimé qu'il était nécessaire de lancer cette initiative, qui s'inscrit dans la volonté de l'OTAN de mieux faire comprendre les enjeux de la cybersécurité, de mieux nous préparer aux menaces qu'elle implique et de renforcer ainsi notre cyber-résilience.

Les cas de piratage informatique, de violation de données, de fraude électronique, d'interruption de services gouvernementaux ou de perturbation de leurs infrastructures critiques, de vol de propriété intellectuelle, de fuites de renseignements de sécurité nationale, et de façon générale, le potentiel destructeur des « armes » cyber, font chaque jour les grands titres des journaux. Toutes ces activités, considérées à une époque comme relevant de la guerre électronique ou de la guerre informatique, alors apanage des experts en sécurité des réseaux, se fondent aujourd'hui en un domaine bien plus large, que l'on appelle « cybersécurité ».

Pour faire face à cette problématique émergente, dont la terminologie de base ne fait d'ailleurs toujours pas consensus, l'ESCWG a souhaité, à travers l'élaboration de ce programme de référence, apporter davantage de clarté et parvenir à un dénominateur commun sur les éléments qu'elle recouvre. Nous avons adopté la convention orthographique « cybersécurité » (en un mot, sans trait d'union) de façon cohérente dans le document et employons le préfixe « cyber » pour recentrer ou préciser la portée de certains termes.

Pour élaborer le présent document, nous avons sondé l'opinion de toutes les institutions membres du Groupement PPP et d' autres collèges de défense et avons analysé les programmes de formation militaire de l'OTAN et des pays partenaires du Groupement PPP dans le but de dresser l'inventaire des matières enseignées jusqu'alors. Notre volonté était de dépasser les frontières traditionnelles des structures gouvernementales et militaires afin d'identifier les lacunes et les approches partagées. La plus grande faille observée dans ce cadre portait sur une compréhension insuffisante, chez les responsables des politiques de sécurité nationale et de défense, des technologies de cybersécurité et des pratiques de mitigation de la menace et des risques. Des lacunes similaires ont également été identifiées parmi les experts techniques à l'égard des cadres d'orientation nationaux.

Le présent programme se propose donc d'offrir une base de référence cohérente, qui permettra de développer ou d'améliorer l'enseignement des problématiques de cybersécurité aux officiers supérieurs, aux fonctionnaires de l'État et aux membres des personnels civils et militaires d'échelon intermédiaire. À l'instar des autres programmes de référence élaborés par le Groupement PPP, l'objectif du présent document reste modeste : nous ne le présentons aucunement comme un cours magistral que tous devraient suivre à la lettre. Son contenu, le niveau de détail des thématiques abordées et les approches présentées ne tendent pas non plus vers un quelconque objectif d'exhaustivité. Nous sommes néanmoins d'avis que ce document offre une approche heuristique utile à l'égard des différents domaines qu'il aborde, y compris une introduction complète aux questions associées à la cybersécurité et aux pratiques qui en découlent. Les lecteurs n'ayant qu'un faible bagage technique y trouveront une première approche introductive, d'un niveau de complexité abordable, qui leur permettra de mieux comprendre la nécessité d'approfondir leurs connaissances techniques de certains aspects. Pour les lecteurs disposant déjà de connaissances techniques, la matière présentée ici peut être considérée comme un récapitulatif utile des domaines qu'ils maîtrisent et une introduction au domaine plus étendu des politiques et des pratiques internationales, nationales et juridiques. Nous espérons ainsi que tout un chacun y trouvera une quelconque utilité.

Les lecteurs qui souhaitent utiliser le présent document pour aborder la question de la cybersécurité dans leur pays respectif sont invités à analyser les pratiques et les exigences en vigueur sur leur territoire afin d'adapter le contenu à leurs besoins spécifiques. Ce document propose une série de lignes directrices permettant d'identifier les domaines qui méritent attention, ainsi qu'une liste de références et d'approches considérées comme essentielles.

II. CYBERSÉCURITÉ ET RISQUES

Les mesures de sécurité découlent la plupart du temps d'une évaluation de la menace et du risque. Nous abordons ces deux concepts de façon détaillée. Mais pour dire les choses simplement, disons que le cyberespace est rempli de menaces, mais que les mesures visant à en limiter l'impact doivent reposer sur l'évaluation du risque. L'Organisation internationale de normalisation (ISO, International Organization for Standardization) définit le risque comme « l'effet de l'incertitude sur l'atteinte des objectifs » (l'effet peut prendre la forme d'un écart positif ou négatif par rapport aux attentes). Puisque les mesures prises pour sécuriser un environnement doivent être proportionnelles à la valeur de l'objet de cette sécurisation, on peut dénombrer différents niveaux de sécurité en fonction de l'évaluation de la valeur et du risque. La sécurisation du cyberespace implique par conséquent un nombre d'éléments à prendre en considération pour limiter l'impact des risques et des menaces, tout en encourageant simultanément l'accessibilité et l'ouverture des différents réseaux et dispositifs interconnectés que nous utilisons. Trouver le juste équilibre entre accès, exploitabilité et sécurité constitue ainsi le défi majeur et central de notre entreprise. Ce programme explore différentes méthodes d'évaluation, d'identification et de mitigation de la menace et du risque, sur le plan technique et au niveau des politiques de sécurité des structures institutionnelles ou gou-

[1] Nous nous appuyons, de façon générale, sur la définition proposée par le département de la Sécurité intérieure des États-Unis (U.S. Department of Homeland Security), lequel entend par cybersécurité l'activité, le processus, la capacité ou l'état par lequel les systèmes d'information et de communication, de même que les informations qu'ils contiennent, font l'objet d'une protection et/ou d'une défense contre toute dégradation, utilisation, modification ou exploitation non autorisée.-

vernementales. Cette exploration passe par l'analyse des meilleures pratiques recommandées dans le domaine de la cybersécurité et par une comparaison des politiques existantes au sein de certains États ou organisations.

III. STRUCTURE DE CE PROGRAMME

Comme nous l'avions déjà mentionné dans d'autres documents analogues, un programme de référence est un programme de formation spécifique, éventuellement composé d'une série de cours, qui décrit les supports d'enseignement, d'apprentissage et d'évaluation ainsi que les méthodes appropriées pour dispenser un programme d'études donné. Le programme qui en résulte forme par conséquent une « feuille de route » retraçant les éléments auxquels les apprenants sont susceptibles d'être confrontés. Comme tout exercice de cartographie, notre projet implique un certain niveau d'abstraction et toutes les routes et tous les détails n'y sont peut-être pas représentés. Nous avons néanmoins veillé à ce qu'il reprenne les grands axes de connaissance et les principaux chemins à emprunter.

Un programme de référence générique se compose généralement d'une structure imbriquée, comprenant de nombreux sous-domaines et thèmes qui forment ensemble un cadre plus large[2]. Ces nombreux éléments imbriqués sont associés aux objectifs plus larges d'un programme d'études. Compte tenu de l'interconnexion des questions et des sujets qui y sont abordés, nous ne recommandons pas d'étaler le présent programme de référence sur trois phases de perfectionnement. Nous reviendrons sur ce point ultérieurement dans nos recommandations sur la meilleure façon d'utiliser ce programme de référence.

Dans notre volonté de conserver la structure adoptée pour les précédents programmes de référence du Groupement PPP, le présent document se compose de quatre thématiques, dont chacune contient différents blocs, qui auraient encore pu faire l'objet d'un nouveau découpage. Ces subdivisions sont appelées respectivement Thématiques (T) et Blocs (B), conformément à la structure de la Table des matières (voir infra).

Les quatre thématiques de ce programme de référence sont les suivantes :

Première thématique : cyberespace et fondamentaux de la cybersécurité

Deuxième thématique : vecteurs de risque

Troisième thématique : cybersécurité internationale – organisation, politiques et normes

Quatrième thématique : gestion de la cybersécurité dans le contexte national

Chaque thématique fait l'objet d'une description détaillée dans ce document, mais s'accompagne aussi de nombreux domaines et questions qui lui sont propres.

Plusieurs sujets spécifiques sont ainsi intégrés à chaque thématique. Chacun d'eux est abordé dans un bloc général, qui peut ensuite lui-même être subdivisé en différents modules d'apprentissage, dont des cours magistraux, des présentations ponctuelles, des démonstrations, des visites sur le terrain, des exercices de mise en situation ou toute activité similaire. Pour la majeure partie des blocs, nous avons décidé de ne pas proposer de modules et de cours magistraux distincts, puisque ce niveau de détail est directement tributaire des besoins individuels et devra donc être adapté aux spécificités locales. Ensemble, les différents blocs forment la structure de chaque thématique. Ils proposent des objectifs et des acquis d'apprentissage, eux-mêmes associés aux objectifs plus larges de la thématique.

Les blocs peuvent être dispensés ensemble, de façon combinée, ou divisés en modules distincts. Cet aperçu ne formule pas de recommandations sur la façon d'utiliser chacun des blocs, mais dans chacun des blocs ou modules, la matière peut être dispensée sous la forme de cours magistraux, de présentations, d'ateliers participatifs, de visites sur le terrain, de démonstrations ou d'exercices de mise en situation.

IV. COMMENT UTILISER CE PROGRAMME

Le programme de référence repose sur un certain nombre de postulats implicites.

Tout d'abord, tous les documents répertoriés dans ce programme sont non classifiés. Cependant, les utilisateurs qui adoptent ce cadre de référence peuvent, s'ils le souhaitent, ajouter des documents classifiés.

Deuxièmement, nous partons du principe que les institutions adoptant ce programme de référence consacreront le temps et les ressources nécessaires pour identifier, avec l'aide d'une équipe d'experts, les politiques et les procédures nationales au niveau de détail correspondant à leur public cible. Si la mémorisation « par cœur » de certains aspects techniques peut s'avérer nécessaire, l'objectif premier reste d'offrir une meilleure compréhension au sens large des défis de la cybersécurité sur l'ensemble du spectre des problématiques rencontrées.

Lors de l'adaptation de ce programme en vue d'un usage à l'échelon national, il peut être envisagé de le dispenser de façon progressive et séquentielle sur différentes phases de carrière, mais il conviendra quand même d'en conserver la structure générale à tous les niveaux. L'objectif général de ce programme de référence est davantage stratégico-opérationnel que purement tactique. Lors de l'élaboration de cours spé-

[2] Pour en savoir plus sur l'origine et l'utilité de l'agencement choisi, nous vous renvoyons aux documents analogues précédemment publiés.

cifiques fondés sur ce programme de référence, nous recommandons que les responsables tiennent compte du temps et des ressources disponibles, du niveau de formation des apprenants et des fonctions que ces apprenants seront amenés à remplir ou susceptibles de remplir, indépendamment de leur grade.

Troisièmement, aucun bloc n'est proposé sur la « cyberguerre », sur les « cyberconflits » ou sur les réseaux sociaux en tant que canal de propagande ou de désinformation. Le comité d'élaboration du programme a décidé de laisser ces questions de côté pour les développer plus en détail ultérieurement.

Enfin, précisons à nouveau que ce programme de référence n'est pas un cours à part entière, ni même une proposition de cours. Il a plutôt pour vocation de servir de document de référence reprenant les principales problématiques et les principaux sujets associés au domaine de la cybersécurité. Il peut faire office de guide pour les membres du personnel technique souhaitant situer leurs attributions sur le large spectre de problématiques. De façon analogue, ce document peut être utilisé dans le cadre de cours introductifs pour des hauts responsables de politique de sécurité nationale afin de permettre à ces derniers de mieux évaluer et de mieux situer leurs politiques nationales en connaissant le contexte technique. Les trois éléments dont il faut tenir compte en priorité lors de l'élaboration d'un cours à partir de cette référence seront de bien définir l'objectif ou la finalité du cours, de tenir compte du profil des apprenants, et plus particulièrement de leur niveau de connaissance technique et de la nature de leur fonction, et de bien évaluer le temps disponible pour dispenser la matière. Ces trois éléments doivent servir de base pour définir le niveau de technicité abordé et la nature des exercices d'apprentissage demandés (cours magistraux, exemples, visites sur le terrain, démonstration, jeux de guerre, etc.)

V. SOURCES COMPLÉMENTAIRES

Le nombre de publications générales et techniques en rapport avec la cybersécurité est en pleine expansion. Les concepteurs de programmes sont invités à établir leur propre liste de références clés. Nous avons néanmoins ajouté un grand nombre de références présentant de nombreuses perspectives nationales et internationales différentes que nous estimons pertinentes. Dans la mesure du possible, nous avons aussi ajouté des liens vers des ressources en ligne. En plus des nombreuses références listées dans le présent document, le site web de l'OTAN propose toute une série d'articles actuels sur les questions d'intérêt pour la communauté de l'OTAN. Les sources répertoriées à l'adresse www.natolibguides.info/cybersecurity sont les suivantes :

- Articles/vidéos de la revue de l'OTAN sur les cyberattaques et édition de juin 2013 de Cyber—the good, the bad and the bug-free (vidéos, photos, ligne du temps, infographies, etc.).
- L'article NATO's Cyber Capabilities : Yesterday, Today, and Tomorrow de Healey et van Bochoven (février 2012) offre un bon aperçu des cybercapacités de l'OTAN.
- Le rapport On Cyberwarfare (2012) de Fred Schreier comprend un glossaire et une excellente sélection de bibliographies thématiques (documents officiels, OTAN, OCDE, par pays, guerre informatique, cybersécurité, ouvrages).
- La Cyber Special Edition de *Strategic Studies Quarterly* 6, n° 3 (automne 2012).
- L'édition Cybersecurity : Shared Risks, Shared Responsibilities de I/S : *A Journal of Law and Policy for the Information Society* 8, n° 2 (2012).
- L'article Cyberspace Is Not a Warfighting Domain (2012) de Martin Libicki.
- *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (2012). Manuel de 300 pages rédigé par un groupe de 20 chercheurs sur invitation du Centre d'excellence de cyberdéfense coopérative de l'OTAN à Tallinn, en Estonie.
- Le projet « Tallinn 2.0 », consécutif au Manuel de Tallinn, est destiné à étendre la portée du Manuel original. Le projet Tallinn 2.0 conduira à la publication de la seconde édition du Manuel de Tallinn aux éditions Cambridge University Press en 2016 (source : NATO CCD COE).
- Le National Cyber Security Framework Manual (2012) du NATO CCD COE.
- Le cours d'apprentissage électronique du NATO CCD COE sur la sensibilisation à la cyberdéfense (accès gratuit sur inscription).
- La Cyber Conflict Bibliography de la Jacob Burns Law Library, George Washington University Law School.
- Le briefing Cyber defence in the EU : Preparing for cyber warfare? (31 octobre 2014) du Service de recherche du Parlement européen.
- Le Tallinn Paper n° 8, publié en avril 2015 : « The Role of Offensive Cyber Operations in NATO's Collective Defence ».

Autres références utiles :

- Business Continuity Institute, *Good Practices Guidelines 2013, Global Edition : A Guide to Global Good Practice in Business Continuity* (England, 2013). http://www.thebci.org/index.php/resources/the-good-practice-guidelines
- Gustav Lindstrom, "Meeting the Cyber Security Challenge," GCSP Geneva Papers—Research Series no. 7 (June 2012).
- International Auditing and Assurance Standards Board, ISAE 3402 Standard for Reporting on Controls at Service Organizations.
- ISO/IEC 15408 : Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4.
- ITU-D Study Group 1, Final Report, *Question 22-1/1 : Securing Information and Communication Networks : Best Practices for Developing a Culture of Cybersecurity*, 5th Study Period 2010–2014. See http://www.itu.int/ITU-D/study_groups or http://www.itu.int/pub/D-STG-SG01.22.1-2014.
- J. Lewis and K. Timlin, "Cybersecurity and Cyberwarfare : Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, Washington, DC, 2011.
- National Initiative for Cybersecurity Careers and Studies http://niccs.us-cert.gov/glossary
- Neil Robinson, Luke Gribbon, Veronika Horvath and Kate Robertson, *Cybersecurity Threat Characterisation : A Rapid Comparative Analysis* (Santa Monica, CA : Rand Corporation, 2013), prepared for the Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, Stockholm.
- NIST Special Publication 800-82 : Guide to Industrial Control Systems Security, June 2011.
- Ron Deibert and Rafal Rohozinski, *Shadows in the Cloud : Investigating Cyber Espionage 2.0*, joint report by the Information Warfare Monitor and Shadowserver Foundation, JR-03-2010, April 6, 2010. http://shadows-in-the-cloud.net
- U.S. Department of Defense, *The DoD Cyber Strategy*, April 2015, Washington, DC.
- World Economic Forum, *Partnering for Cyber Resilience : Towards the Quantification of Cyber Threats*. Industry Agenda item (in collaboration with Deloitte), Ref. 301214, 2015.

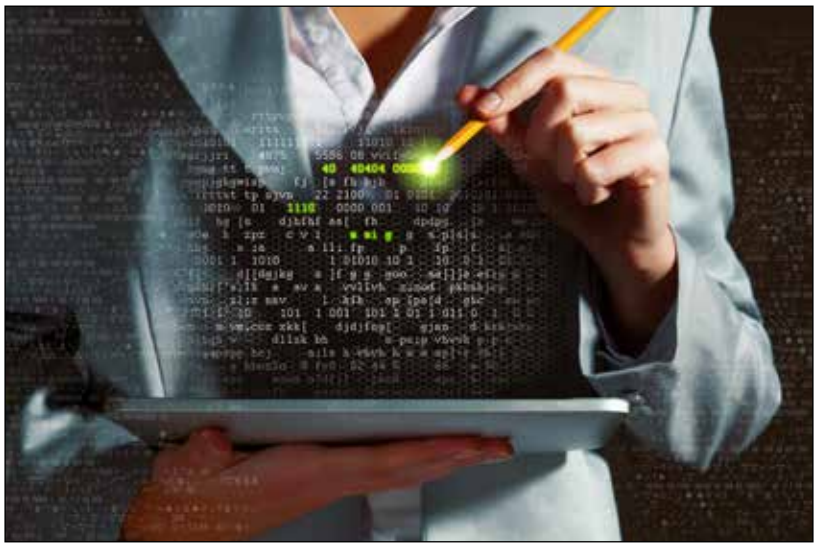


TABLE DES MATIÈRES

Première thématique : cyberespace et fondamentaux de la cybersécurité

Objectif

L'objectif général de cette thématique est de dispenser les connaissances de base pour toutes les formations qui suivent en identifiant les composantes structurelles du cyberespace[3], son architecture de base et les rudiments de la cybersécurité. L'identification et la gestion du risque constituent la principale problématique reliant les différentes thématiques et les différents sujets abordés dans ce programme.

Description

Pour relever les défis du cyberespace et de la cybersécurité, il ne suffit pas de rebaptiser les organisations gouvernementales responsables de la sécurité des systèmes d'information (SSI) ou de la sécurité des communications (COMSEC). L'omniprésence des systèmes informatiques modernes et la capacité de communiquer ou d'interagir à travers un grand nombre de supports, allant des dispositifs mobiles aux ordinateurs portables, impliquent un grand nombre de vulnérabilités intrinsèques et de vecteurs d'attaque possibles, à la fois pour les acteurs étatiques et non étatiques. L'exploitation des vulnérabilités peut avoir de grandes répercussions sur la sécurité nationale : actes délibérés d'espionnage, dégradation d'infrastructures de commandement et de contrôle, vol de droits de propriété intellectuelle et de données à caractère personnel sensibles, interruption ou perturbation de services et d'infrastructures critiques, dommages économiques et industriels, etc.

Au fil des cinq blocs de cette thématique, les apprenants pourront se familiariser avec la structure de base du cyberespace et avec l'approche de la cybersécurité fondée sur le risque. Le bloc T1B1 « Cybersécurité et cyberespace – Introduction » explore les origines et l'agencement général du cyberespace et présente le concept de cybersécurité. Le bloc T1-B2 « Sécurité et risque informatique » se penche sur les fondements de la méthodologie d'analyse du risque de sécurité informatique et explore une approche de l'évaluation fondée sur la menace. Le bloc T1-B3 « Structures du cyberespace : dorsale internet et infrastructures nationales » explore l'exploitation et l'architecture de l'internet mondial et sa gouvernance. Le bloc T1-B4 « Protocoles et plateformes » présente les normes de la technologie réseau et de la technologie de l'information afin d'explorer les fondements de la conception et de l'exploitation réseau. Enfin, le bloc T1-B5 « Architecture de sécurité et gestion de la sécurité » présente les fondements de l'architecture de sécurité fondée sur l'analyse de la menace, du risque et de la vulnérabilité. L'analyse de risque doit guider et irriguer le développement des architectures informatiques et de la stratégie afin de limiter les vulnérabilités et les menaces connues et inconnues au niveau de l'organisation et de l'État. Les apprenants recevront une introduction aux méthodes d'analyse et de gestion du risque cyber utilisées pour développer des architectures système et des stratégies de mitigation du risque.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- décrire ce que l'on entend par cyberespace et cybersécurité ;
- exposer certaines vulnérabilités de base des pays développés face aux menaces informatiques, comme l'espionnage économique visant à servir des intérêts nationaux, le profilage individuel et d'entreprise, le vol de données, la corruption de bases de données ou le piratage de systèmes de contrôle industriel ou de contrôle des procédés (p. ex. SCADA) ;
- décrire la topologie de base du cyberespace, notamment ses structures physiques et la façon dont il est régi par les protocoles et les procédures ;
- énoncer les principes de base d'une architecture de sécurité appropriée.

Références recommandées

Lukasz Godon, "Structure of the internet." http://internethistory.eu/index.php/structure-of-the-internet/

Dave Clemente, "Cyber Security and Global Interdependence : What is Critical?," Chatham House Paper, *The Royal Institute of International Affairs*, ISBN 978-1-86203-278-1, February 2013.

Communications Security Establishment Canada (CSEC), *Harmonized Threat and Risk Assessment (TRA) Methodology*, 23 October 2007.

D.P. Cornish, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks,* European Parliament Directorate-General for External Policies of the Union, Directorate B—Policy Department, February 2009, EP/EXPO/B/AFET/FWC/2006-10/Lot4/15 PE 406.997. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

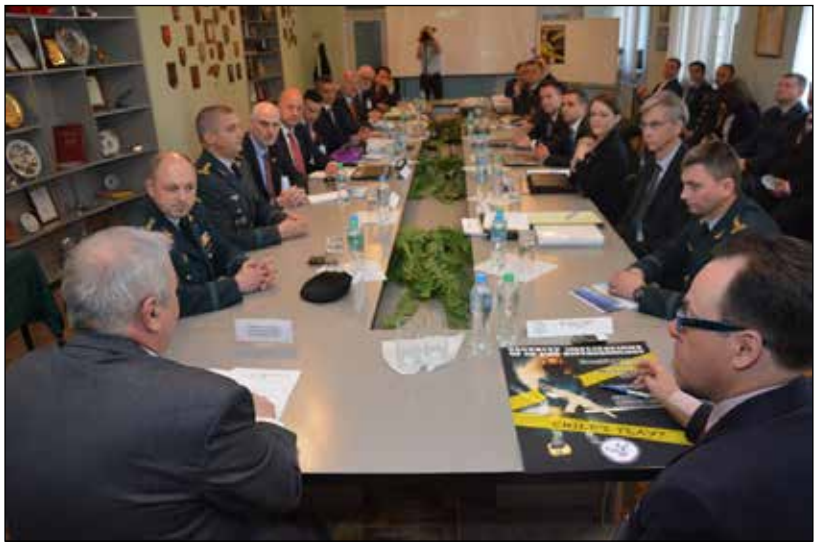
Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X : Resilience of the internet Interconnection Ecosystem—Full Report*, ENISA, April 2011. http://www.enisa.europa.eu

R. Tehan, *Cybersecurity : Authoritative Reports and Resources, by Topic*, Congressional Research Service, CRS Report 7-7500 R42507, 15 April 2015. http://www.crs.gov

[3] Le cyberespace est le monde électronique créé par des réseaux interconnectés formés de systèmes TI et de l'information qui se trouve sur ces réseaux (source : Stratégie de cybersécurité du Canada, 2014).

The White House, *Cyberspace Policy Review*, 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Ethan Zuckerman and Andrew McLaughlin, "Introduction to internet Architecture and Institutions." https://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html



Atelier du comité de rédaction du programme de référence sur la cybersécurité à Chisinau.

Bloc T1-B1 : Cybersécurité et cyberespace – Introduction

Description

Le cyberespace se compose de différents systèmes informatiques reliés en réseaux et de systèmes de télécommunication intégrés. Devenu partie intégrante de la société moderne, le cyberespace optimise ou permet des communications rapides, des systèmes de commandement et de contrôle répartis, un stockage et un transfert de données de masse et toute une série de systèmes hautement distribués. Tous ces avantages sont aujourd'hui considérés comme des acquis par la société et sont devenus des éléments essentiels de la vie économique, de notre quotidien et des services que nous fournissons et utilisons. Notre dépendance à l'égard d'un cyberespace devenu omniprésent se retrouve jusque dans les sphères militaires, où communications, commandement et contrôle, renseignement et frappes de précision reposent tous sur de nombreux systèmes informatiques et sur les infrastructures de communication qui y sont associées. Cette omniprésence de systèmes interconnectés a induit une certaine forme de dépendance et de vulnérabilité difficile à prévoir, à gérer, à limiter et à empêcher chez les individus, dans les entreprises et les gouvernements. Certaines nations considèrent ces dépendances vulnérables comme une nouvelle préoccupation de sécurité et de défense nationale et ont chargé des éléments existants de leurs forces de sécurité d'y parer, tandis que d'autres nations ont créé de toutes nouvelles organisations pour gérer et coordonner les politiques nationales de cybersécurité. La cybersécurité est donc devenue une problématique transverse importante, qui nécessite des réponses des individus, des sociétés privées, des organisations non gouvernementales, de l'ensemble des organes gouvernementaux (approche pangouvernementale) et d'une série d'agences et d'organes internationaux.

Ce bloc a pour objectif de familiariser les apprenants avec les technologies de l'information et de la communication (TIC), en soulignant leur omniprésence et la dépendance qu'elles induisent. Le but est de faire appréhender aux apprenants les spécificités sociologiques, techniques et culturelles des technologies de l'information modernes, leurs multiples rôles et l'impact de cet environnement virtuel sur la vie moderne, sur les décisions politiques et sur les communications mondiales. Ce bloc se présente comme une première approche de la sécurité nationale et entend permettre aux apprenants de comprendre clairement la topologie et les constructions du cyberespace et de la cybersécurité.

Pour garantir la clarté de la définition, nous nous sommes fondés sur la définition du cyberespace telle que formulée par le NIST (*National Institute of Standards and Technology*) aux États-Unis, à savoir le réseau interdépendant des infrastructures de technologie de l'information, englobant l'internet, les réseaux de télécommunication, les systèmes informatiques, les processeurs et les contrôleurs dédiés. La cybersécurité est définie comme l'activité, le processus, la capacité ou l'état par lequel les systèmes d'information et de communication, de même que les informations qu'ils contiennent, font l'objet d'une protection et/ou d'une défense contre toute dégradation, utilisation, modification ou exploitation non autorisée. Cette définition a formé le point de départ de la matière traitée dans le présent document.

Acquis d'apprentissage

L'apprenant sera capable de démontrer un niveau approprié de connaissance et de compréhension de ce qui suit :

- l'importance des technologies de l'information et de la communication et la façon dont elles modifient le tissu des sociétés modernes ;
- les nuances de la cybersécurité dans différents contextes nationaux et culturels, avec un accent plus marqué sur l'approche et les politiques adoptées à l'échelon national ;
- les défis clés que représentent les technologies de l'information et de la communication, les principaux fournisseurs, les principales sources politiques, les acteurs clés, les responsabilités légales et fonctionnelles ;
- les incidences à la fois positives et négatives du cyberespace sur la société ;
- les menaces et les risques associés à l'exploitation efficace et sécurisée du cyberespace ;
- la gouvernance, l'exploitation et la gestion de l'internet par un réseau d'institutions publiques, privées et sans but lucratif ;
- les contextes nationaux uniques associés aux prises de décisions politiques et à la gouvernance locale de l'internet ;
- le rôle des normes et des protocoles dans la conception de l'internet ;
- les impératifs militaires et politiques associés au cyberespace et à la gouvernance de l'internet.

Thèmes de modules possibles et approches à envisager

Le niveau de détail de la matière abordée dépendra du public et de la durée de la formation. Néanmoins, les modules relatifs à l'internet national et à l'infrastructure de télécommunication, aux principaux fournisseurs de services et au partage actuel des responsabilités des politiques et des pratiques de sécurité au sens large au sein des organisations gouvernementales et de défense peuvent être abordés séparément pour plus de clarté et de mise en relief.

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure des cours magistraux donnés par des spécialistes du domaine, des séminaires, des ateliers pratiques, des exercices et des mises en situation.

Les apprenants devront être évalués sur leur participation et sur les discussions menées lors d'exercices de lecture collective et les débats, ainsi que par un test de connaissances sur la matière du cours.

Références

Les spécialistes du domaine travailleront avec le pays hôte pour sélectionner les lectures appropriées en fonction de l'objectif du cours et des contraintes de temps.

Les lectures sélectionnées néanmoins pourront inclure les références suivantes :

"G.I.G.O. Garbage In, Garbage Out' (1969) Computer History—A British View," YouTube, accessed 25 April 2015. http://youtu.be/R2ocgaq6d5s

James R. Beniger, T*he Control Revolution : Technological and Economic Origins of the Information Society* (Cambridge, Mass. : Harvard University Press), 1986.

Vinton G. Cerf (Chair) et al., *ICANN's Role in the internet Governance Ecosystem*, report of the ICANN Strategy Panel, 20 February 2014.

Paul E. Ceruzzi, *A History of Modern Computing,* 2nd ed. (Cambridge, Mass. : MIT Press), 2003.

Paul Hoffman, ed., "The TAO of IETF : A Novice's Guide to the internet Engineering Task Force," internet Engineering Task Force, 2015.

Barry Leiner, Vinton Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolff, "Brief History of the internet," accessed 25 April 2015. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Marie-Laure Ryan, Lori Emerson and Benjamin J. Robertson, eds., *The Johns Hopkins Guide to Digital Media* (Baltimore : Johns Hopkins University Press), 2014.

Lance Strate, "The Varieties of Cyberspace : Problems in Definition and Delimitation," *Western Journal of Communication* 63, no. 3 (1999) : 382–412. doi :10.1080/10570319909374648

The White House, *International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World* (Washington, DC : Executive Office of the President of the United States, National Security Council), 2011.

Jie Wang, A. Zachary Kissel, "Introduction to Network Security: Theory and Practice", Singapore: Wiley, 2015. ISBN 9781118939505. UIN: BLL01017585410.

EU ENISA, "Cybersecurity as an Economic Enabler" Heraklion, Crete, Greece. March 2016. Available at: www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler (Retrieved July 14, 2016).

Bundesamt für Sicherheit in der Informationstechnik (BSI), "The State of IT Security in Germany, 2015". Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2

F. Lantenhammer, A. Scholz, A. Seidel, A. Schuttpelz, A, "Cyber Defence und IT-Security Awareness", in, Europäische Sicherheit & Technik : ES&T. No.8,, 2012. Journal ISSN: 2193-746X. UIN: ETOCRN316565061.

Jie Wang, A. Zachary Kissel, «Introduction to Network Security: Theory and Practice», Singapore: Wiley, 2015. ISBN 9781118939505. UIN: BLL01017585410.

EU ENISA, «Cybersecurity as an Economic Enabler» Heraklion, Crete, Greece. March 2016. Available at: www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler (Retrieved July 14, 2016).

Bundesamt für Sicherheit in der Informationstechnik (BSI), «The State of IT Security in Germany, 2015». Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2

F. Lantenhammer, A. Scholz, A. Seidel, A. Schuttpelz, A, «Cyber Defence und IT-Security Awareness», in, Europäische Sicherheit & Technik : ES&T. No.8,, 2012. Journal ISSN: 2193-746X. UIN: ETOCRN316565061.

T1-B2 : Sécurité et risque informatique

Description

De façon générale, la *sécurité de l'information* (SI) concerne les grandes catégories d'information – privée, publique, sensible, classifiée, etc. –, qu'elles soient au format numérique ou non, devant faire l'objet de mesures ou de protocoles de gestion spécifiques. Dans le domaine cyber, ce sont avant tout les hackers, les criminels et les services de renseignement étrangers qui cherchent à exploiter les failles du système SI. Ce bloc offre une introduction au concept général de la sécurité et du risque informatique, en mettant l'accent sur le domaine cyber[4]. Les apprenants étudieront ultérieurement plus en détail l'approche de sécurité de l'information mise en œuvre par leur pays (voir la quatrième thématique). Cette section fera la transition entre la façon dont l'information est classée et la distinction entre sécurité de l'information et assurance de l'information. S'ensuivront une exploration des différents types de vulnérabilités de cybersécurité et une analyse du processus d'attaque ou de la cinématique d'un cyberincident (« *cyber kill chain* »). La discussion portera ensuite sur la gestion du risque de sécurité de l'information par le biais d'approches telles que le modèle d'évaluation de la menace et du risque (TRA, *Threat and Risk Assessment*)[5], tout particulièrement à la lumière des menaces persistantes avancées (APT, *advanced persistent threats*)[6]. Sans passer par une exploration détaillée, les apprenants devront acquérir à ce stade des connaissances générales des principaux organes nationaux et des organismes responsables de l'élaboration des politiques, des procédures et des pratiques de sécurité informatique.

Contexte

La sécurité de l'information englobe les mécanismes et les processus qui autorisent l'accès à des actifs physiques et à des données présentes sur des systèmes ou circulant entre ces systèmes. La sécurité de l'information est centrée sur la technologie et les opérations en lien avec les applications et l'infrastructure de sécurité. L'assurance de l'information (intitulé pouvant varier selon les pays) couvre les aspects sécurité de l'information, mais aussi la gestion de l'information, l'intégrité des données et les régimes et les protocoles de protection dans le but de réduire ou de gérer les risques globaux et de limiter l'impact des incidents. Les principaux objectifs de sécurité comprennent généralement la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation. On dénombre différentes pratiques et différents régimes en matière de sécurité de l'information en fonction des individus, des organisations/entreprises et des pays.

Acquis d'apprentissage

L'apprenant sera capable de démontrer sa compréhension ou sa connaissances des éléments suivants :

- les normes de classification de sécurité pour les informations ainsi que pour les systèmes d'information et électroniques ;
- l'analyse de la menace et du risque au niveau approprié ;
- différents cas de *cyber kill chain*.

Les apprenants seront par ailleurs capables de :

- définir les principaux termes pertinents au domaine (données, connaissances, informations, sécurité de l'information, *cyber kill chain*) ;
- comprendre le concept d'assurance de l'information et l'importance des objectifs de sécurité en lien avec la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation ;
- expliquer le rôle de l'analyse des risques de vulnérabilité à la menace dans la gestion de la sécurité de l'information ;
- identifier les organisations responsables de l'élaboration de leurs politiques, procédures et pratiques de sécurité de l'information à l'échelon national.

Thèmes de modules possibles et approches à envisager

- Évolution de la sécurité de l'information
- Références de bonnes pratiques internationales
- Identification des principales autorités nationales en matière de cybersécurité

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure des cours magistraux et des démonstrations avec illustrations de pratiques actuelles et études de cas. Les apprenants devront être capables de définir la sécurité de l'information, la cinématique d'une attaque cyber (*cyber kill chain*), les menaces persistantes avancées (APT) et le modèle d'évaluation de la menace et du risque (TRA).

[4] Le plus souvent, la sécurité des informations électroniques vise au moins à préserver la continuité du service, la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation (c.-à-d. offrir aux utilisateurs autorisés un accès idoine au niveau approprié).

[5] Comme nous le détaillerons ultérieurement, le modèle TRA évalue les actifs, les menaces, les vulnérabilités et les contrôles informatiques.

[6] Dans ce contexte, le terme « avancé » signifie coordonné, déterminé et sophistiqué. Le terme « persistant » signifie continu. De façon plus spécifique, les menaces persistantes avancées impliquent l'intervention d'agents « intelligents » ayant l'intention de nuire et recherchant des moyens de lire, d'altérer, de dégrader, d'exploiter et de détruire des cybercapacités, ainsi que d'en empêcher l'accès.

Références

Ross J. Anderson, *Security Engineering : A Guide to Building Dependable Distributed Systems*, 2nd Edition (Indianapolis, IN : Wiley), 2008.

Australian Government, Department of Defence, Intelligence and Security, *2015 Australian Government Information Security Manual : Controls*, issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. http://www.protectivesecurity.gov.au

Australian Government, Department of Defence, Intelligence and Security, *2015 Australian Government Information Security Manual : Principles*, issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. http://www.protectivesecurity.gov.au

Communications Security Establishment Canada, *Harmonized Threat and Risk Assessment (TRA) Methodology*, 23 October 2007.

D.E. Gelbstein, *Information Security for Non-Technical Managers*, 1st Edition, 2013. ISBN 978-87-403-0488-6.

Eric M. Hutchins, Michael J. Clopperty and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Proceedings of the 6th International Conference on Information Warfare and Security*, Washington, DC, 17–18 March 2011.

Information Systems Audit and Control Association (ISACA), *Advanced Persistent Threat Awareness Study Results, USA*, 2014.

Richard Kissel, ed., *Glossary of Key Information Security Terms*, NIST Interagency Report (IR) 7298 Revision 2, NIST, Computer Security Division, Information Technology Laboratory, May 2013.

Gil Klein, "Unlocking the Secrets of Cybersecurity : Industry experts discuss the challenges of hacking, tracking, and attacking in a virtual world," University of Maryland University College Achiever (Spring 2013) : 6–20. https://www.umuc.edu/globalmedia/upload/Spring2013-Achiever.pdf

Gary Stoneburner, *NIST Special Publication 800-33 : Underlying Technical Models for Information Technology Security*, NIST, December 2001.

"Common Criteria for Information Technology Security Evaluation," accessed 17 July 2015. http://www.commoncriteriaportal.org/

International Organization for Standardization Information Technology series :

1) ISO/IEC 27001 :2013 Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information
2) ISO/IEC 27005 :2011 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information
3) ISO/IEC 27031 :2011 Technologies de l'information — Techniques de sécurité — Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité
4) ISO/IEC 27032 :2012 Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

A. Rutowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin and T. Takahashi, "CYBEX – The Cybersecurity Information Exchange Framework (X.1500)," ACM SIGCOMM Computer Communication Review, Vol. 40, no. 5, 2010. Available at: http://www.beepcore.org/p59-3v40n5i-takahashi3A.pdf

Babak Akhgar et al «Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies». Amsterdam: Butterworth-Heinemann, 2015. ISBN 9780128019733. British Library Shelfmark: General Reference Collection DRT ELD.DS.28766. UIN: BLL01017039420.

M. Watin-Augouard, «Cyber-Menaces: Un Trait Saillant du Livre Blanc», in, Administration: Revue d'étude et d'information Publiée par l'Association du Corps Préfectoral et des Hauts Fonctionnaires du Ministère de l'intérieur. No.239, 2013. Journal ISSN: 0223-5439.

H. Fukatsu, «IT Security Against Cyber Attacks; A Common Thread for Both Developed and Developing Countries», in, Nihon Igaku Ho shasen Gakkai zasshi ; Asian Oceanian Congress of Radiology; AOCR 2014; Kobe, Japan. Journal ISSN: 0048-0428. British Library Shelfmark: 6113.254000. UIN: ETOCCN087891561

Safa, Nader Sohrabi, Rossouw Von Solms, and Lynn Futcher. «Human aspects of information security in organisations.» Computer Fraud & Security 2016, no. 2 (2016): 15-18.

Alshaikh, Moneer, Sean B. Maynard, Atif Ahmad, and Shanton Chang. «Information Security Policy: A Management Practice Perspective.» arXiv preprint arXiv:1606.00890 (2016).

T1-B3 : Structures du cyberespace : dorsale internet et infrastructures nationales

Description

Ce bloc a pour objectif de familiariser les apprenants au tissu technique du cyberespace, avec un ciblage sur les infrastructures au niveau mondial, national et d'entreprise. Seront entre autres étudiés l'architecture de l'internet, les réseaux informatiques et les réseaux cellulaires. La logique de la structure générale et la topologie nationale particulière (spécificités de l'infrastructure nationale des réseaux, fournisseurs de télécommunication, canaux de routage, etc.) doivent être le fil conducteur de ce bloc.

Contexte

L'architecture de la dorsale internet inclut les principaux chemins de données entre les gros systèmes de réseaux informatiques et les routeurs de cœur. Des centres de réseaux haute capacité – commerciaux, gouvernementaux, universitaires ou autres – hébergent ces réseaux et ces routeurs. Ils contrôlent les points d'échange internet et les points d'accès réseau et assurent l'acheminement du trafic internet entre les pays et les continents. De façon générale, les grands fournisseurs de services internet (FSI) (p.ex. réseaux de première catégorie) participent à l'acheminement du trafic sur la dorsale internet dans le cadre d'accords d'interconnexion négociés entre parties privées. Les fournisseurs de services internet qui gèrent les subdivisions distinctes de l'internet appelées systèmes autonomes (AS, Autonomous Systems) sont enregistrés et se voient attribuer un numéro de système autonome (ASN). Le routage et l'accessibilité entre les systèmes autonomes sont mis en œuvre par le biais d'un ensemble de routeurs de cœur implémentant le protocole BGP (Border Gateway Protocol). La gestion de la corrélation entre les noms de domaine (p.ex : www.google.com) et les adresses internet routables contrôlées par l'AS est assurée par le système DNS (Domain Name System) et ses autorités d'enregistrement.

Un registre internet national (NIR, *National Internet Registry*) est une organisation responsable de la coordination de l'attribution des adresses IP pour une zone géographique donnée, ainsi que d'autres fonctions de gestion de ressources internet au niveau national, sous la tutelle d'un registre internet international. Ilest également possible que les pouvoirs publics organisent les FSI sur leur territoire économique.

Les réseaux de téléphones cellulaires/dispositifs mobiles représentent aujourd'hui un élément majeur de l'infrastructure de distribution internet. Regroupés sous le terme « web mobile », ces réseaux sont connectés à l'internet. Leur architecture générale et les spécificités nationales doivent également être passées en revue au cours de ce bloc.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- comprendre de façon détaillée la topologie physique et virtuelle et la gouvernance de la dorsale internet ;
- expliquer le rôle des ASN dans l'interconnexion mondiale de l'internet et la responsabilité de l'IANA (*Internet Assigned Numbers Authority*) ;
- comprendre les liens entre les FSI de haut niveau (première catégorie), les FSI secondaires et les réseaux locaux (LAN, local area network) de l'utilisateur ;
- expliquer le rôle des serveurs de noms faisant autorité dans l'interconnexion mondiale de l'internet et la responsabilité de l'ICANN (*Internet Corporation for Assigned Names and Numbers*) ;
- comprendre la topologie et la géographie de leur cyberespace national, notamment les registres nationaux et les autorités en charge des FSI ;
- comprendre la structure et la gouvernance des réseaux cellulaires/mobiles et leur connectivité internet dans le contexte national.

Thèmes de modules possibles et approches à envisager

Pour une introduction pertinente et utile à des publics non experts, les enseignants utilisant ce programme de référence pour mettre sur pied un ou plusieurs cours spécifiques devront bien veiller à rechercher le niveau de détail technique approprié afin de s'assurer que la matière du cours est compréhensible par leurs apprenants.

Le réseau national et les infrastructures de télécommunications peuvent également être étudiés, dans une plus ou moins grande mesure.

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure des cours magistraux et des démonstrations. Des visites d'infrastructures nationales, des interventions d'experts et des examens oraux et pratiques peuvent accroître l'intérêt et la qualité du programme.

Références

ICANN, "Beginner's Guide to Domain Names," 6 December 2010.

internet Assigned Numbers Authority, *The IANA Functions : An Introduction to the internet Assigned Numbers Authority (IANA) Functions*, ICANN, June 2015.

Paul Krzyzanowski, "Understanding Autonomous Systems : Routing and Peering," 5 April 2013, accessed 17 July 2015. https://www.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html

Michael Miller, "How Mobile Networks Work," Pearson Education, Que Publishing, 14 March 2013, accessed 17 July 2015.

Ram Mohan, "Attacking the internet's Core," SecurityWeek website, 16 March 2011, accessed 17 July 2015. http://www.securityweek.com/attacking-internets-core

Jeff Tyson, "How WAP Works," HowStuffWorks website, accessed 17 July 2015. http://computer.howstuffworks.com/wireless-internet3.htm

Rudolph van der Berg, "How the 'Net works : An introduction to peering and transit," 2 September 2008, accessed 17 July 2015. http://arstechnica.com/features/2008/09/peering-and-transit/4/

Konstantinos Moulinos, Rossella Mattioli, EU ENISA, «Communication network interdependencies in smart grids», Heraklion, Crete, Greece. March 2016. Available at: www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids (Retrieved July 14, 2016).

Abdulrahman Alqahtani. «Towards a framework for the potential cyber-terrorist threat to critical national infrastructure: A quantitative study» Information and computer security. Vol 23, No 5; 2015; 532-569. Journal ISSN: 2056-4961. British Library Shelfmark: 4481.796000. UIN: ETOCvdc_100027180236.0x000001

E. Sitnikova, E. Foo, R.B. Vaughn, «The Power of Hands-On Exercises in SCADA Cyber Security Education», International Federation for Information Processing -Publications-IFIP.; Information security education; Heidelberg; Springer; 2013. Journal ISSN: 1868-4238. British Library Shelfmark: 4540.183500. UIN: ETOCCN085265877

O. Netkachov, P. Popov, K. Salako, «Quantification of the Impact of Cyber Attack in Critical Infrastructures», in, Journal on Data Semantics; Reliability and Security Aspects for Critical Infrastructure Protection, Florence, Italy, 2014; Sep, 2014, pp 316-327. Journal ISSN: 0302-9743. UIN: ETOCCN088306466.

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson, eds. The Turn to Infrastructure in Internet Governance. Springer, 2016.

T1-B4 : Protocoles et plateformes

Description

Pour l'échange de messages, les systèmes de communication utilisent des formats de message bien définis, appelés protocoles. Un protocole de communication est un système de règles régissant l'échange de données à l'intérieur d'un ordinateur ou entre plusieurs ordinateurs (en réseau ou non). Les protocoles peuvent être comparés aux différentes informations figurant sur une enveloppe postale, avec le nom de l'expéditeur, le nom du destinataire et leurs coordonnées respectives. Chaque message est envoyé avec l'intention précise d'obtenir une réponse spécifique parmi un ensemble de réponses prédéterminées pour la situation en question. Un protocole doit donc définir la syntaxe (règles), la sémantique (signification) et la synchronisation de la communication. Le comportement déterminé est généralement indépendant de la façon dont le message sera traité ou des systèmes par lesquels il est susceptible de passer pour atteindre la destination voulue.

Chaque couche et chaque processus de protocole présentent des vulnérabilités et des risques spécifiques, qu'il est possible d'aborder à différents niveaux d'expertise. Cette question peut être examinée à un niveau tout à fait élémentaire, mais elle peut également, en fonction du public, être étudiée à un niveau classifié.

Contexte

Un système en réseau peut être visualisé ou conceptualisé de deux façons.

Sous l'angle logique, le fonctionnement de l'internet repose sur des protocoles, ou plus exactement sur des piles de protocoles, implémentations logicielles d'un ensemble de normes de protocoles de communication. Ces piles de protocoles régissent la façon dont les données sont empaquetées et acheminées. Les implémentations de protocoles sont généralement organisées selon une architecture en couches (d'où le terme de pile), celles en bas de la pile assurant les services de communication primitifs, comme la communication de base de petits blocs de données vers un autre ordinateur sur le réseau local (p. ex. Ethernet). Plus haut dans la pile, les protocoles fournissent des services comme l'adressage commun pour les réseaux mondiaux (p. ex. IP), la correction d'erreurs et le réassemblage d'objets de données de plus grande taille (p. ex. TCP). Les protocoles des couches supérieures assurent les services de niveau application les plus abstraits comme la remise du courrier électronique (SMTP) ou la navigation web (HTTP). Les couches les plus élevées dans la pile de protocoles sont tributaires des services de base des couches inférieures.

Sous l'angle physique, on peut décrire l'internet par les dispositifs et plates-formes réseau (comme les commutateurs et les routeurs, les passerelles, les proxys et les pare-feux) sur lesquels les protocoles sont implémentés et par les formes d'interconnexion entre ces dispositifs réseau. Ainsi, les commutateurs réseau implémentant le protocole Ethernet peuvent connecter des ordinateurs sur le réseau local (LAN). Les LAN peuvent être connectés à des routeurs IP pour rediriger les paquets de données entre les réseaux et éventuellement le reste de l'internet. Un serveur de messagerie connecté au réseau est susceptible d'implémenter le protocole SMTP.

Sur les réseaux actuels, le déploiement de dispositifs et de réseaux virtuels complique l'identification du lien entre les dispositifs physiques et leurs fonctions dans l'implémentation de protocoles. Dans ces réseaux, les dispositifs réseau et leur interconnexion peuvent être implémentés virtuellement par des logiciels exécutés sur de gros serveurs (comme c'est le cas dans un environnement cloud). La virtualisation de ces systèmes, qui rend plus complexe le maintien de la sécurité, est un thème nouveau qui doit être abordé.

Les piles de protocoles peuvent être conçues et implémentées pour des applications spécialisées. Les systèmes de contrôle industriel (SCI) tels que SCADA sont un exemple de piles de protocoles de communication réseau utilisées pour enregistrer des mesures relevées par des capteurs et envoyer des messages de contrôle. Sur un réseau de distribution électrique, par exemple, ces systèmes peuvent surveiller les connexions d'alimentation en courant électrique (charge et commutation) en fonction de la demande. La sécurité des systèmes SCADA est un élément important dans le domaine de la sécurité des infrastructures nationales en raison de l'importance que revêtent les systèmes qu'ils contrôlent. Par ailleurs, bon nombre de systèmes d'armes modernes font appel à des systèmes électroniques similaires à ceux des systèmes SCADA et peuvent donc également être vulnérables.

Chaque couche de protocole présente des risques et des vulnérabilités spécifiques, autant d'aspects qui peuvent être explorés à différents niveaux d'expertise, allant des connaissances générales aux connaissances les plus pointues (avec informations classifiées).

Définition du protocole de sécurité réseau

En règle générale, les protocoles de sécurité réseau garantissent la sécurité et l'intégrité des données en transit sur une connexion réseau. Ils définissent les processus et la méthodologie de sécurisation des données réseau. Mais aucun protocole de sécurité ne garantit la sécurité. Chaque protocole offre plutôt une façon spécifique de parer un certain type d'attaque d'un système ou d'un réseau. Note : certaines définitions nationales spécifiques ou admises à l'échelle internationale peuvent s'appliquer.

Les protocoles de sécurité réseau emploient souvent des techniques de cryptographie et de chiffrement pour sécuriser les données afin que ces dernières ne puissent être déchiffrées ou modifiées que par un algorithme spécifique, une clé logique, une formule mathématique ou une combinaison de ces éléments. Les protocoles de sécurité réseau les plus connus sont les suivants : Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) et Secure Socket Layer (SSL).

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- décrire et commenter le rôle et les fonctions de chaque couche de la pile de protocoles réseau standard (suite de protocoles internet TCP/IP) ;
- décrire les dispositifs réseau les plus courants tels que les concentrateurs, les commutateurs, les routeurs, les passerelles et les serveurs d'applications, le lien entre l'implémentation des couches de la pile de protocoles réseau et leur rôle fonctionnel sur le réseau ;
- décrire les concepts de base de la virtualisation des dispositifs réseau et des réseaux SDN, les incidences de ces concepts sur l'architecture réseau et leurs liens avec les environnements cloud ;
- décrire les éléments de base d'un environnement SCI articulé autour d'un système SCADA (avec éventuellement les composantes SCI spécifiques et les fondements de leur exploitation dans des protocoles internet standard) ;
- indiquer et décrire les protocoles de sécurité les plus courants, leurs liens avec l'architecture réseau en couches et la vulnérabilité de sécurité particulière à laquelle chaque protocole est censé répondre.

Thèmes de modules possibles et approches à envisager

Les systèmes de contrôle industriel (p. ex. SCADA) et les systèmes informatiques des plateformes militaires (systèmes PIT) peuvent être étudiés de manière plus ou moins approfondie afin d'identifier leur vulnérabilité et leur attractivité en tant que cible potentielle.

Méthode d'apprentissage et évaluation

Cours magistraux, démonstrations et études de cas sont recommandés. L'évaluation doit de préférence se faire par écrit. Elle doit être adaptée au niveau de connaissance défini pour les cours.

Références

IEEE Standards Association, IEEE 802 Standards. http://standards.ieee.org/about/get/

internet Engineering Task Force, Request for Comments (RFC), accessed 17 July 2015. https://www.ietf.org/rfc.html

Certiology, Network Devices, accessed 17 July 2015. http://www.certiology.com/computing/computer-networking/network-devices.html

Cisco Systems Inc., Virtual LANs VLAN Trunking Protocol (VLANs VTP), accessed 17 July 2015. http://www.cisco.com/c/en/us/tech/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/index.html

D. Clark, "The Design Philosophy of the DARPA internet Protocols," *Proceedings of SIGCOMM* '88, 106–14 (New York : Association for Computing Machinery), August 1988.

Kevin R. Fall and W. Richard Stevens, *TCP/IP Illustrated, Volume 1 : The Protocols*, 2nd edition, Addison-Wesley Professional Computing Series (Boston, MA : Addison Wesley Professional), 15 November 2011.

Juniper Networks, Inc., "White Paper : Architecture for Secure SCADA and Distributed Control System Networks," 2010, accessed 17 July 2015. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf

Radia Perlman, "Tutorial on Bridges, Routers, Switches, Oh My!," accessed 17 July 2015. https://www.ietf.org/proceedings/62/slides/protut-0.pdf

Bart Preneel, "internet Security Protocols," video of lecture given at SecAppDev 2013, Leuven, Belgium. https://www.youtube.com/watch?v=CZzd3i7Bs2o

Andrew S. Tanenbaum and David J. Wetherall, Computer Networks, 5th edition (New York : Pearson), 27 September 2010.

E. van Baars, R. Verbrugge, R. «A communication algorithm for teamwork in multi-agent environments», Journal of Applied Non-Classical Logics, Logic and information security; Leiden, The Netherlands, 2008; Sep, 2009, 431-462, Lavoisier; 2009. British Library Shelf Mark: 4943.400000, UIN: ETOCCN074941483

C.W. Chan «Key Exchange Protocols for Multiparty Communication Services», International Symposium on Cyber Worlds; Tokyo, 2002. Conference ISBN: 0769518621. British Library Shelfmark: 4550.208900. UIN: ETOCCN046776823.

Jan Jatzkowski, Bernd Kleinjohann, «Self-Reconfiguration of Real-Time Communication in Cyber-Physical Systems», 2016. Electronic paper held at the British Library. UIN: ETOCvdc_100033448082.0x000001.

J. Ivimaa, T. Kirt, «Evolutionary Algorithms for Optimal Selection of Security Measures». Proceedings of the 10th European Conference on Information Warfare and Security at the Tallinn University of Technology Tallinn, Estonia July 7-8, 2011, pp. 172-184. Rain Ottis (eds). ISBN 9781908272065 (pbk.) UIN: BLL01015873308.

Qadir, Junaid, Arjuna Sathiaseelan, Liang Wang, and Barath Raghavan. «Approximate Networking for Global Access to the Internet for All (GAIA).» arXiv preprint arXiv:1603.07431 (2016).

T1-B5 : Architecture de sécurité et gestion de la sécurité

Description

Ce bloc porte sur l'architecture de sécurité de base (BSA, *basic security architecture*), ses aspects techniques et opérationnels ainsi que les contextes humains et de gestion qui influencent sa structure. Au niveau national, la BSA définit une architecture et des pratiques de sécurité couvrant notamment l'infrastructure (p.ex. : dorsales de télécommunication), les filtres de contenu au niveau national et les structures de gouvernance de la cybersécurité. L'objectif général de ce bloc est d'enseigner aux apprenants comment concevoir/construire des environnements de sécurité sur la base d'une analyse du risque afin de maintenir ce dernier à un niveau acceptable. Cette architecture est articulée autour de contrôles techniques (p. ex. pare-feux, systèmes de détection d'intrusion, gestion des journaux (logs), etc.), de contrôles physiques (p. ex. gestion d'accès, alarmes incendie et régulation hygrométrique, etc.), de politiques de sécurité et de modules de formation. Les apprenants découvriront comment effectuer une analyse du risque et une configuration de sécurité au niveau national, ainsi qu'à des niveaux individuels et organisationnels.

La BSA tient compte des politiques de sécurité nationale, des différentes normes de sécurité en vigueur, du cycle de vie du système, des principes de conception et des éléments architecturaux physiques. Dans l'analyse de la conception des BSA, ce bloc examine également les concepts complémentaires de contrôle approprié des actifs, de contrôle physique et environnemental, de plan de gestion, d'aspect humain – notamment les contrôles des antécédents des employés –, la continuité des opérations, les plans d'intervention d'urgence et la cyberrésilience des systèmes.

Contexte

L'architecture de sécurité repose sur les politiques. Il s'agit donc d'abord de bien comprendre les actifs informationnels qui font l'objet d'une gestion. Tout doit partir de la valeur de ces actifs informationnels aux yeux du défenseur (c.àd. l'impact potentiel de leur perte ou de leur dégradation) et de la valeur de ces mêmes actifs aux yeux de possibles agents de menace. C'est de cette phase d'identification et d'évaluation des actifs que dépend la mise sur pied des politiques régissant le contrôle de l'accès à l'information.

La phase d'évaluation de la menace identifie les agents de menace susceptibles de nuire aux actifs répertoriés ainsi que leur capacité technique. La mise sur pied de l'architecture de sécurité est également guidée par le besoin de concevoir un système physique assorti des critères d'assurance et des procédures d'exploitation permettant de réduire le risque que des agents de menace puissent compromettre les actifs identifiés. À cela peuvent venir s'ajouter des normes nationales d'évaluation de la menace et du risque, des normes présentant les aspects liés à la conception et des documents d'orientation pour la sélection des mécanismes de contrôle d'accès et les modèles d'architecture.

La sélection et l'organisation de l'architecture de sécurité d'entreprise s'inscrivent souvent dans le cadre d'une défense en profondeur, schéma dans lequel l'utilisation coordonnée de multiples mécanismes de sécurité assure la protection de l'intégrité des actifs informationnels. La défense de ces actifs se fait de l'intérieur vers l'extérieur, depuis des contrôles sur l'accès aux données jusqu'au périmètre de sécurité du réseau d'entreprise – où s'effectue la jonction avec l'infrastructure réseau mondiale – en passant par les mécanismes de sécurité des applications qui ont accès aux données, les ordinateurs hôtes sur lesquels les applications sont exécutées et le tissu du réseau de l'entreprise.

L'architecture de sécurité d'entreprise intègre une suite de mécanismes destinés à limiter les risques auxquels cette entité en particulier est exposée. Parmi les mécanismes, ou éléments architecturaux, courants permettant la mise en œuvre de la politique de sécurité figurent le zonage réseau, les pare-feux, les systèmes de détection d'intrusion, les applications antivirus, les techniques de cryptographie et les systèmes de supervision des informations et des événements de sécurité (SIEM). Aucun de ces systèmes ne garantira la sécurité. Les techniques d'attaque sont diverses et peuvent exploiter les vulnérabilités présentes dans les nombreux protocoles, systèmes et applications logicielles que compte l'infrastructure d'entreprise.

Les activités d'assurance de la sécurité sont des actions prises pendant le développement et l'évaluation de l'architecture de sécurité d'entreprise pour s'assurer que les mesures de sécurité en place sont efficaces. Note : ces mesures relèvent parfois davantage du domaine théorique que du domaine pratique. Supposons par exemple qu'un dispositif de sécurité soit annoncé comme capable d'assurer toute une série de fonctionnalités de sécurité. Au titre des activités d'assurance, ces fonctionnalités pourraient être testées méthodiquement par un organisme de normalisation reconnu, auquel il serait demandé de certifier que le dispositif en question assure effectivement les fonctionnalités annoncées, sans erreur. Bien d'autres activités d'assurance peuvent être effectuées, notamment : revues de conception formelles ou semi-formelles, élaboration de directives et de manuels de sécurité pour la communauté des utilisateurs et les opérateurs des systèmes, gestion des cycles de vie des composantes de sécurité, gestion des configurations, gestion de la sécurité des environnements des développeurs/fabricants des composantes de l'architecture, livraison dans un cadre de confiance des composantes de l'architecture par le développeur/fabricant. À cela peuvent encore venir s'ajouter des programmes organisant le contrôle des antécédents du personnel et l'octroi d'habilitations de sécurité, initiatives permettant d'établir une confiance dans les utilisateurs et les opérateurs des systèmes.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- présenter la façon dont les multiples couches des mécanismes de sécurité s'organisent sur l'ensemble de l'architecture d'entreprise dans le cadre d'une défense en profondeur afin d'assurer une redondance en cas de défaillance des contrôles de sécurité ou d'exploitation d'une vulnérabilité ;
- proposer, à un niveau rudimentaire, un zonage de sécurité approprié et la mise en place de mesures telles que des pare-feux à l'aide d'un diagramme de réseau ;
- saisir l'utilité et comprendre la portée des normes nationales et des documents d'orientation pour la conduite des évaluations de la menace et du risque, la mise en place de politiques de sécurité au niveau de l'entreprise/l'organisation et la mise en œuvre d'une architecture de sécurité ;
- comprendre le lien entre la phase d'identification des actifs de l'évaluation de la menace et du risque (TRA) et les spécificités de la politique de sécurité pour l'entreprise ;
- comprendre le lien entre la phase d'évaluation de la menace et l'identification des vulnérabilités exploitables par des agents de menace potentiels, et comprendre l'effet des résultats de cette évaluation sur les mesures de sécurité à déployer sur l'architecture d'entreprise ;
- saisir l'utilité et comprendre la portée du système national de classification de sécurité pour la protection des documents et des informations, et décrire le lien entre ce système et les programmes de contrôle des antécédents et d'habilitation de sécurité du personnel.

Thèmes de modules possibles et approches à envisager

Il faudrait examiner les différentes formes de gestion de l'architecture système et du zonage de sécurité réseau pour que les apprenants soient en mesure d'évaluer les modèles que leur organisation a mis en place ou devrait mettre en place.

Il pourrait être nécessaire d'examiner dans le détail les problématiques de l'exploitation de l'ingénierie sociale et de l'ingénierie des facteurs humains.

Le système national de classification de sécurité de base régissant l'accès physique, la protection des documents et des informations et les programmes de contrôle des antécédents et d'habilitation de sécurité du personnel peuvent également être passés en revue et faire l'objet d'un récapitulatif.

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure un travail en groupes sur les aspects humains, technologiques et opérationnels.

Des présentations données par des intervenants externes issus d'organisations privées et publiques sont susceptibles d'animer les discussions et d'améliorer la qualité de la formation.

Les méthodes d'évaluation dépendront du niveau de connaissance attendu des apprenants.

Références

Australian Government, Department of Defence, Intelligence and Security, *Australian Government Information Security Manual : Controls*, issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. See www.protectivesecurity.gov.au

Australian Government, Department of Defence, Intelligence and Security, *Australian Government Information Security Manual : Principles*, issued under the authority of Dr. Paul Taloni, Director, Australian Signals Directorate, Commonwealth of Australia, 2015. See www.protectivesecurity.gov.au

Deborah J. Bodeau and D.J. Graubart, "Cyber Resiliency Engineering Framework," MITRE Technical Report MTR 110237 (Bedford, MA : The MITRE Corp.), September 2011.

Communications Security Establishment Canada, *Baseline Security Requirements for Network Security Zones in the Government of Canada* (ITSG-22), June 2007.

Communications Security Establishment Canada, *Harmonized Threat and Risk Assessment (TRA) Methodology (TRA-1)*, 23 October 2007.

Communications Security Establishment Canada, *Information Technology Security Guideline : Network Security Zoning : Design Considerations for Placement of Services within Zones (ITSG-38)*, May 2009.

Communications Security Establishment Canada, *Information Technology Security Guideline : User Authentication Guidance for IT Systems (ITSG-31)*, March 2009.

George Farah, "Information Systems Security Architecture—A Novel Approach to Layered Protection : A Case Study," GSEC Practical Version 1.4b, SANS Institute, 9 September 2004. www.sans.org

D.E. Gelbstein, *Information Security for Non-Technical Managers*, 1st Edition, 2013. ISBN 978-87-403-0488-6.

Gil Klein, "Unlocking the Secrets of Cybersecurity : Industry Experts Discuss the Challenges of Hacking, Tracking, and Attacking in a Virtual World," University of Maryland University College Achiever (Spring 2013) : 6–20. https://www.umuc.edu/globalmedia/upload/Spring2013-Achiever.pdf

Alexander Klimburg, ed., National Cyber Security Framework Manual, NATO CCD COE Publication, Tallinn, Estonia, 2012. ISBN 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

William Pelgrin, "A Model for Positive Change : Influencing Positive Change in Cyber Security Strategy, Human Factors, and Leadership," Center for internet Security.

Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman and Lukas Ruf, "What is a Security Architecture?," paper by the Working Group Security Architecture, Information Security Society Switzerland (ISSS), 29 September 2008.

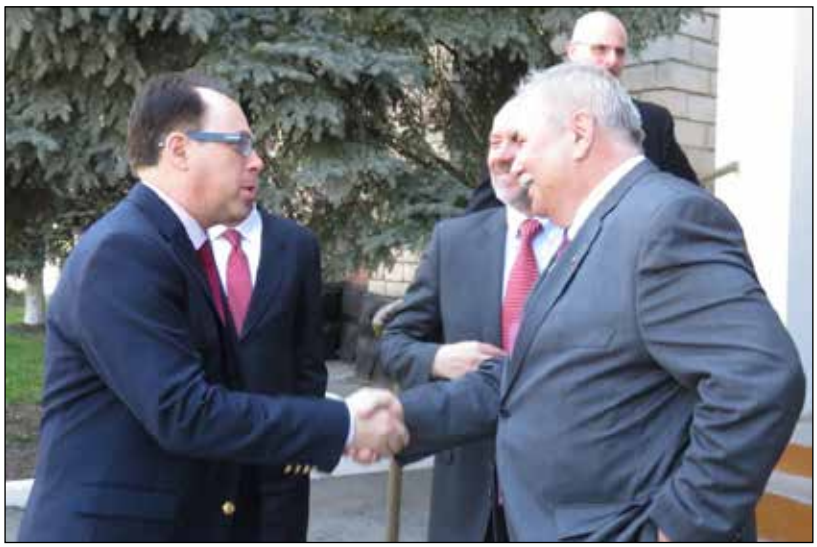
S.A. Chun, V. Atluri, B.B. Bhattacharya, «Risk-Based Access Control for Personal Data Services», Statistical Science and Interdisciplinary Research; International Conference on Information Systems Security; Algorithms, Architectures; Kolkata, India, 2006; Dec, 2009, 263-284. Journal ISSN: 1793-6195. Conference ISBN: 9789812836236; 9812836233. British Library Shelf Mark: 8448.954000. UIN: ETOCCN071364080.

Gérard Desmaretz, Cyber Espionnage, Ou, Comment Tout le Monde épie Tout le Monde!, Paris: Chiron, 2007. ISBN 9782702712122 (pbk.) UIN: BLL01014343705.

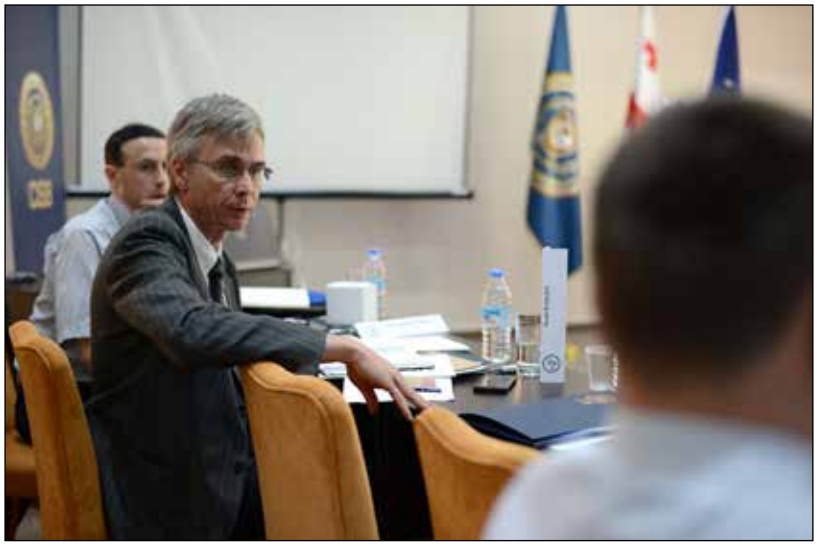
A. Rutowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin and T. Takahashi, "CYBEX – The Cybersecurity Information Exchange Framework (X.1500)," ACM SIGCOMM Computer Communication Review, Vol.40, No.5, 2010.

I. Atoum, A. Otoom, A.A. Ali, «A Holistic Cyber Security Implementation Framework», in, Information Management & Computer Security, Vol.22; No 3, 2014, pp 251-264. Journal ISSN: 0968-5227. UIN: ETOCRN359424579.

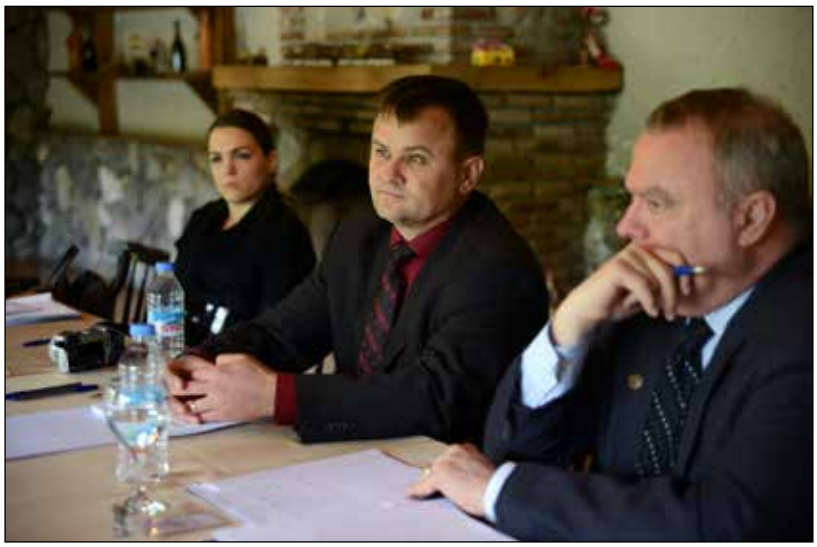
Yoo, Hyunguk, and Taeshik Shon. «Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture.» Future Generation Computer Systems 61 (2016): 128-136.



Des représentants des pays OTAN et non OTAN ont uni leurs forces pour créer le programme de référence sur la cybersécurité. Réunion du ministre moldave de la Défense et des coordinateurs de publication du programme.



Atelier du comité de rédaction du programme de référence sur la cybersécurité à Tbilissi (Participants de l'Université de Greenwich et du Collège militaire royal du Canada).



Atelier du comité de rédaction du programme de référence sur la cybersécurité à Tbilissi (Participants de l'École de l'OTAN d'Oberammergau, d'i-intelligence et de SLCE).

Deuxième thématique : vecteurs de risque

Objectif

Cette thématique propose une présentation générale des vulnérabilités de sécurité propres au cyberespace et des divers vecteurs ou chaînes d'attaque permettant de les exploiter. Comprendre ces vulnérabilités constitue un aspect essentiel de la politique d'évaluation et de limitation du risque, sur laquelle nous reviendrons par la suite.

Description

Ce programme de référence souscrit à la proposition du rapport remis par le National Cyber Study Group au directeur du renseignement national des États-Unis, selon laquelle toutes les cybervulnérabilités peuvent être classées dans quatre catégories de vecteurs de risque (voir références, Chabinsky 2010) : accès par la chaîne d'approvisionnement et les fournisseurs ; accès à distance ; accès à proximité ; accès en interne. Cette thématique s'articule donc autour de quatre blocs. Le bloc T2-B1, Chaîne d'approvisionnement et fournisseurs, met en lumière les failles de sécurité (et les contrôles) pouvant survenir au niveau du site de production, des sous-traitants, des expéditions, de l'entreposage et de la maintenance. Le bloc T2-B2, Attaques exploitant un accès à distance ou à proximité, se penche sur les vulnérabilités associées à l'accès non autorisé (sans privilèges). Le bloc T2-B3, Accès en interne (attaques depuis un point d'accès local), passe en revue les vulnérabilités associées à un accès aux systèmes par une personne autorisée. Enfin, le bloc T2-B4, Risques liés à la mobilité, BYOD et tendances émergentes, s'intéresse aux risques associés aux politiques d'utilisation des dispositifs personnels sur le lieu de travail (BYOD, *Bring Your Own Device*), au cloud et à d'autres problèmes posés par la mobilité.

L'objectif général de cette thématique est de fournir des connaissances de base sur les vulnérabilités propres aux diverses composantes du cyberespace. Néanmoins, les enseignants élaborant un cours en prenant pour référence le présent document peuvent orienter le contenu et le dispenser à un niveau expert et classifié, pour pouvoir aborder des questions telles que des politiques et procédures établies à l'échelon national.

Objectifs d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- appréhender l'importance de la chaîne d'approvisionnement et des points d'accès (à distance, à proximité et en interne), et comprendre les incidences possibles de leur compromission pour identifier les vulnérabilités liées au cyberespace et celles associées aux solutions destinées à favoriser la mobilité ;
- identifier les types de compromis à consentir en termes de sécurité face à l'essor de la mobilité et aux autres vecteurs de risque présentés dans la présente thématique.

Références recommandées

Steven R. Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line," *Journal of National Security Law & Policy* 4, no. 27 (August 2010): 27–39. http://jnslp.com/wp-content/uploads/2010/08/04_Chabinsky.pdf

Wenke Lee and Bo Rotoloni, *Emerging Cyber Threats Report 2015*, report prepared by the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI) for the Georgia Cyber Security Summit, 2014. https://www.gtisc.gatech.edu/pdf/Threats_Report_2015.pdf

Louis Marinos, *ENISA Threat Landscape 2013: Overview of Current and Emerging Cyber-threats*, ENISA, 11 December 2013, ISBN 978-92-79-00077-5. http://www.enisa.europa.eu, doi:10.2788/14231

Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka and Jason Frye, Cyber Threat Metrics, Sandia National Laboratories, March 2012. http://fas.org/irp/eprint/metrics.pdf

Francesca Spinalieri, *Joint Professional Military Education Institutions in an Age of Cyber Threat*, report, Pell Center for International Relations and Public Policy, Salve Regina University, August 2013.

U.S. Office of Director of National Intelligence, Understanding Cyber Threats: A Guide to Small and Medium Sized Businesses, Intelligence Community Analyst, Private Sector Program, 2014.

ISO standards on Risk Assessment/Risk Management.

T2-B1 : Chaîne d'approvisionnement/Fournisseurs

Description

Ce bloc aborde les vulnérabilités de la chaîne d'approvisionnement et présente le concept des bonnes pratiques en matière de gestion des risques de la chaîne d'approvisionnement (SCRM, *Supply Chain Risk Management*).

Toutes les étapes de la chaîne sont vulnérables. La surveillance et la sécurisation des chaînes d'approvisionnement peuvent constituer des défis majeurs au niveau du marché mondial. À titre d'exemples, citons le contrôle de l'intégrité, de la qualité et de la sécurité, mais aussi la prévention des perturbations, des exploits et des attaques subséquentes. Les chaînes d'approvisionnement mondiales incluent les trajets empruntés par les équipements sensibles de la phase de production à l'expédition, qu'il s'agisse de composants isolés ou de produits finis comme le matériel ou les logiciels. Ces chaînes d'approvisionnement sont vulnérables aux perturbations : les produits peuvent être interceptés et altérés, et des éléments défectueux ou du code malveillant peuvent être introduits à différents stades de leur fabrication, expédition, entreposage, installation ou réparation — sans compter qu'il est possible de collecter des données sensibles lors de la mise au rebut des équipements. Il est donc potentiellement possible d'altérer le produit à n'importe quel stade de son cycle de vie. D'autres nœuds d'une infrastructure institutionnelle ou nationale peuvent être également compromis par l'intermédiaire des fournisseurs ou de la chaîne d'approvisionnement, entraînant ainsi des violations de sécurité. Vos fournisseurs peuvent-ils garantir un niveau de sécurité suffisant ? Quelles mesures doivent être prises pour sécuriser l'intégralité de la chaîne ?

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- comprendre les principaux défis liés à tous les stades du cycle de vie des produits ;
- expliquer le rôle de la gestion de configuration (c.-à-d. la conception des systèmes) dans la sécurisation de la chaîne d'approvisionnement ;
- comprendre le rôle et la nécessité de politiques et pratiques clairement définies en matière de gestion des risques de la chaîne d'approvisionnement.

Thèmes de modules possibles et approches à envisager

- Vulnérabilité de la chaîne d'approvisionnement aux actes de cyberespionnage et aux cyberdélits
- Méthodes et bonnes pratiques en matière de limitation des risques
- Politiques et pratiques nationales existantes en matière de limitation des risques de la chaîne d'approvisionnement

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure des études de cas et des cours magistraux sur les violations de sécurité et leurs conséquences.

Exercice individuel : trouver un exemple de compromission d'une chaîne d'approvisionnement et identifier les solutions possibles.

Autre exercice possible : cartographier une chaîne d'approvisionnement et identifier les étapes à risque.

Références

Jon Boyens, Celia Paulsen, Rama Moorthy and Nadya Bartol, Supply Chain Risk Management for Federal Information Systems and Organizations, NIST Special Publication 800-161, Second Public Draft, U.S. Department of Commerce, Washington, DC, 2014.

Steven R. Chabinsky "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Lines," *Journal of National Security Law & Policy* 4, no. 1 (2010): 27.

Trusted Computing Group. Fact Sheet. 2009. http://www.trustedcomputinggroup.org/files/resource_files/7f38fa36-1d09-3519-add14cb3d28efea6/fact%20sheet%20May202009.pdf

Luca Urciuoli, Toni Männistö, Juha Hinsta and Tamanna Kahn. "Supply Chain Cyber Security—Potential Threats," *Information & Security: An International Journal* 29, no. 1 (2013): 51–68. http://www.ndm.net/ips/pdf/junipernetworks/Juniper%20Architecture%20for%20Secure%20SCADA%20and%20Distributed%20Control%20System%20Networks.pdf

U.S. Government Accountability Office, "Addressing Potential Security Risks of Foreign-Manufactured Equipment," testimony of Mark L. Goldstein, Director, Physical Infrastructure Issues, before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives, U.S. Government Accountability Office, GAO-13-652T, 21 May 2013. http://www.gao.gov/assets/660/654763.pdf

ISO 28000 Standards statements.

A. Sokolov, V. Mesropyan, A. Chulok, A, Aje, «Supply Chain Cyber Security: A Russian outlook», Technovation: an International Journal of Technical Innovation and Entrepreneurship. 2014. Vol 34; No. 7; 2014, 389-391. Journal ISSN: 0166-4972. British Library Shelfmark: 8761.150000. UIN: ETOCRN353289650.

Florin Gheorghe Filip, Luminita Duta, «Decision Support Systems in Reverse Supply Chain Management», Elsevier Paper, 2015. UIN: ETOCvdc_100030799942.0x000001.

Dmitry Ivanov, Alexandre Dolgui, Boris Sokolov, Boris, Frank Werner, Marina Ivanova, «A Dynamic Model and an Algorithm for Short-Term Supply Chain Scheduling in the Smart Factory Industry 4.0», in International Journal of Production Research, Vol.54, Issue 2, (2016); 2016; pp 386-402. Journal ISSN: 0020-7543. (Electronic). Britsh Library Shelfmark: ELD Digital store 4542.486000. UIN: ETOCvdc_100031962439.0x000001

J. Sztipanovits, et al. «OpenMETA: A Model-and Component-Based Design Tool Chain for Cyber-Physical Systems», in Journal on Data Semantics. No. 8415, (2014), pp 235-248. Journal ISSN: 0302-9743. UIN: ETOCRN350535700.

Lu, Tianbo, Xiaobo Guo, Bing Xu, Lingling Zhao, Yong Peng, and Hongyu Yang. «Next Big Thing in Big Data: The security of the ict supply chain.» In Social Computing (SocialCom), 2013 International Conference on, pp. 1066-1073. IEEE, 2013.

T2-B2 : Attaques exploitant un accès à distance ou à proximité

Description

Les cyberattaques peuvent être perpétrées depuis un point local ou à distance. En ce qui concerne les attaques locales, on peut distinguer les attaques réalisées par un point d'accès à proximité ou exécutées par un intervenant interne dont l'accès est autorisé. Les attaques internes sont abordées séparément dans le bloc T2-B3. Le concept d'accès distant fait référence ici à toutes les méthodes et tactiques permettant d'accéder aux réseaux ou d'en perturber le fonctionnement sans disposer d'un accès physique apparent au matériel du système. Lors d'une attaque à distance, il est possible que le cyberpirate n'ait pas eu un accès physique préalable au système ciblé. Il y accède via le réseau ou un autre dispositif de communication, sans disposer a priori de privilèges d'accès au système. À l'inverse, en cas d'attaque en local, le pirate possède généralement une forme quelconque d'accès ou de privilège sur le système et tente d'élever son niveau de privilège pour accéder aux informations de façon non autorisée. Lorsqu'elles sont menées par un agent malintentionné, externe à l'organisation, ces activités seront considérées comme des attaques exploitant un accès à proximité dans le présent document. Comme l'explique Chabinsky (2010), une attaque par un point d'accès à proximité fait référence à la capacité d'un agent malintentionné de perturber, d'intercepter ou d'accéder à des réseaux et systèmes informatiques en se plaçant à proximité de leurs différents composants, notamment des postes de travail, des câbles ou des récepteurs sans fil. L'accès de proximité constitue une forme d'accès distant. Parmi les techniques courantes utilisant l'accès de proximité pour exploiter des vulnérabilités, citons le « reniflage » réseau (interception et accès aux informations envoyées via des réseaux sans fil), l'enregistrement des frappes, les captures d'écran, l'interception par un intermédiaire (man-in-the-middle) et l'injection de code malveillant.

Ce bloc étudie les attaques par accès distant et par accès de proximité, l'accès interne étant abordé dans le bloc suivant. Il vise à mettre en lumière les risques connus les plus courants associés aux attaques susmentionnées et présente plusieurs méthodes possibles pour limiter ces risques et contrecarrer ces attaques.

Contexte

Les applications réseau classiques reposent sur le concept du client et du serveur. Une application « client » envoie des demandes à une application « serveur » suivant les modalités définies par un protocole de communication, afin d'obtenir des informations ou d'entraîner l'exécution d'une action. C'est toujours le client qui initie la communication. Le serveur, quant à lui, attend d'être contacté à une adresse connue du réseau. Les protocoles chargés de contrôler ces communications incluent les services web (HTTP ou HTTPS), les services de transfert des fichiers (FTP) et les services de messagerie (SMTP, POP3 ou IMAP). Les attaques à distance peuvent cibler des vulnérabilités présentes sur le serveur (erreurs de configuration ou dans le code du serveur) qui permettent au pirate d'accéder à des informations sur le système serveur, voire d'en prendre le contrôle à distance.

Le pirate peut lancer une attaque à distance côté serveur s'il parvient à identifier une mauvaise configuration ou une erreur dans le logiciel implémenté sur le serveur. Par exemple, une erreur dans les paramètres de configuration peut permettre à un pirate d'accéder de façon non autorisée à un mode réservé à la maintenance du système, qui assure un accès étendu à ce dernier. Un autre scénario consiste à lancer une attaque contre un serveur web HTTP qui utilise un système de base de données principal (back-end) pour fournir des données. Si elles n'ont pas été soigneusement vérifiées, les demandes de pages web envoyées par un pirate peuvent lui permettre de transmettre des chaînes de commandes illicites à la base de données principale et d'en prendre le contrôle. On parle, dans ce cas, d'attaque par injection de code SQL (*Structured Query Language*).

Compte tenu des progrès réalisés dans la protection des serveurs (pare-feux, contrôle d'accès, etc.), les pirates concentrent désormais leurs attaques sur les applications client. Toutefois, comme les applications client initient toujours la communication, il est impossible de les contacter directement sur le réseau. Le pirate doit donc trouver le moyen d'inciter l'utilisateur de l'application client à contacter un serveur malveillant capable de corrompre cette application client au cours de l'échange. Ces ruses ou leurres, connus sous diverses appellations, sont des stratagèmes qui font appel aux principes de l'ingénierie sociale pour convaincre l'utilisateur d'effectuer certaines actions, par exemple ouvrir une pièce jointe infectée.

Acquis d'apprentissage

Le principal objectif de ce bloc est de faire prendre conscience aux apprenants de tout le spectre de risques associés aux attaques par accès distant et par accès de proximité.

Les apprenants auront acquis les compétences suivantes :

- comprendre et décrire un scénario d'attaque par accès distant, identifier les composants d'une telle attaque et les comparer aux scénarios d'attaque par accès de proximité ;
- se familiariser avec la structure des applications client-serveur et leur topologie réseau, et pouvoir identifier les protocoles courants (HTTP, HTTPS, FTP et autres protocoles de messagerie) utilisés dans ce modèle ;

- décrire le mode opératoire des attaques côté serveur, notamment la première étape de collecte d'informations à l'aide de techniques telles que l'analyse des vulnérabilités réseau et les tests à données aléatoires ; et expliquer pourquoi les outils d'analyse des vulnérabilités réseau sont aussi utiles aux pirates qu'aux responsables de la sécurité informatique ;
- posséder des connaissances de base des scénarios d'attaque côté serveur, tels que l'exploitation de configurations incorrectes, l'usurpation d'adresses IP, le déni de service (DoS) et le déni de service distribué (DDos), l'injection de code SQL et les dépassements de mémoire tampon basés sur les protocoles réseau ;
- décrire comment les progrès techniques dans la protection du périmètre réseau et le renforcement de la sécurité des serveurs ont contribué au développement et à la prévalence de techniques d'attaque côté client ;
- posséder des connaissances de base des scénarios d'attaque côté client, par exemple les scripts intersites (*cross-site scripting*), la falsification des demandes intersites, les exploits de navigateur web et les documents incorporant des chevaux de Troie ;
- identifier et présenter la relation entre les attaques côté client et les techniques d'ingénierie sociale, notamment les attaques par phishing et par technique du point d'eau (*watering hole*).

Thèmes de modules possibles et approches à envisager

- La technicité des modules peut varier considérablement selon le temps alloué et les connaissances techniques des apprenants.
- Présentation de divers types d'attaques faisant appel à l'ingénierie sociale

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure des cours magistraux et des démonstrations. Les présentations délivrées par les administrateurs réseau en poste peuvent porter sur les menaces persistantes en circulation. Il serait utile d'identifier et de proposer des cas concrets à l'échelon national pour illustrer les problèmes pratiques et immédiats. Diverses mesures d'évaluation pratique doivent être mises au point, selon le niveau de compétence technique que les apprenants sont censés acquérir.

Références

Steven R. Chabinsky, "Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Lines," *Journal of National Security Law & Policy* 4, no.1 (2010): 27.

Shirley Radack, ed., *Information Technology Laboratory Bulletin: Log Management: Using Computer and Network Records to Improve Information Security*, 1, 2 (October 2006), National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. http://csrc.nist.gov/publications/nistbul/b-10-06.pdf

Murugiah Souppaya and Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication 800-83, Revision1, U.S. Department of Commerce, July 2013. http://dx.doi.org/10.6028/NIST.SP.800-83r1

U.S. Department of Homeland Security, U.S. Computer Emergency Readiness Team, *Using Wireless Technology Securely*, US-CERT, 2008. http://www.us-cert.gov/reading_room/Wireless-Security.pdf

Emmanouil Tranos, Peter Nijkamp, Karima Kourtit «The Death of Distance Revisited: Cyber-Place, Physical and Relational Proximities», Journal of Regional Science, Vol.53, No.5, 2013. Journal ISSN: 1467-9787.

E. Anyefru, «Cyber-Nationalism: The imagined Anglophone Cameroon Community in Cyberspace», in African Identities, Vol.6, No.3, (2008), pp 253-274. Journal ISSN: 1472-5843. British Library Shelfmark: 0732.501500. UIN: ETOCRN234554771

A. Almalawi, X Yu, Z Tari, A. Fahad, I. Khalil, «An Unsupervised Anomaly-Based Detection Approach for Integrity Attacks on SCADA systems», in Computers & Security. Vol. 46, (2014), pp 94-110. Journal ISSN: 0167-4048 . British Library Shelfmark: 3394.781000. UIN: ETOCRN359669860 .

Y Li, L Shi, P Cheng, J Chen, D.E. Quevedo, «Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach», IEEE Transactions on Automatic Control. Vol.60; No.10, 2015. Journal ISSN: 0018-9286. UIN: ETOCRN375325720.

T2-B3 : Accès en interne (attaques depuis un point d'accès local)

Description

Une attaque informatique d'un réseau ou d'un système d'information exploite une faille du système ou d'un logiciel pour exécuter une action illégitime quelconque en vue de compromettre la confidentialité, l'intégrité ou la disponibilité des informations. Ces exploits peuvent être de deux types : distants ou locaux. Dans le cas des exploits locaux, les pirates ont préalablement établi un accès au système pris pour cible. En d'autres termes, ils possèdent déjà certains privilèges sur le système et les attaques ont pour but d'élever ces privilèges afin d'obtenir un accès non autorisé aux informations. Ce bloc s'intéresse aux attaques par accès local. Des collaborateurs internes malintentionnés qui bénéficient d'un accès physique à divers systèmes ou utilisent ces systèmes peuvent provoquer des dommages importants à une activité, une entreprise ou une organisation. Leurs motivations sont multiples : appât du gain, esprit de revanche, rancune ou différend idéologique. Toutefois, il est également possible que des pertes ou des perturbations de ce type soient imputables à une erreur d'un opérateur ou à une autre négligence.

Contexte

Dans le domaine de la sécurité informatique, le concept de privilège représente l'autorisation d'exécuter une action. Dans ce cas, l'autorisation est un droit octroyé à un utilisateur donné lui permettant d'accéder à une ressource système spécifique (p. ex. un fichier ou une application), d'utiliser certaines commandes système ou d'accéder à un service (p. ex. un dispositif réseau). En règle générale, la politique de gestion des privilèges utilisateur comprend un processus d'authentification de l'identité électronique de l'utilisateur et l'application d'une série de règles de contrôle d'accès (protocoles) déterminant les actions qu'un utilisateur est autorisé à exécuter sur le système, telles que la lecture, l'écriture ou l'exécution de programmes. Un pirate peut tenter « d'élever les privilèges » (obtenir des droits plus importants) pour accéder à davantage d'informations hébergées sur le système. Pour cela, il peut par exemple usurper l'identité d'un autre utilisateur, le plus souvent en prenant le contrôle d'un programme exécuté par un utilisateur détenant des privilèges plus élevés, ou en modifiant les protocoles intégrés de la politique de sécurité. S'il parvient à élever suffisamment ses privilèges, le pirate peut prendre le contrôle administratif du système. Dans un tel scénario, le pirate peut être un utilisateur autorisé du système, par exemple un collaborateur interne malintentionné tentant d'exécuter des actions non autorisées. Il est également possible qu'il s'agisse d'une personne externe à l'organisation exécutant une attaque à distance dans le but d'utiliser à son propre compte les identifiants d'un utilisateur doté de privilèges limités. À partir de ce point d'accès, le pirate peut utiliser les identifiants volés pour lancer une attaque par accès local en vue d'élever ses privilèges et d'étendre son accès. D'un point de vue technique, il est difficile de distinguer les deux scénarios puisque l'un et l'autre mettent en jeu des attaques par accès local et bon nombre des techniques utilisées pour limiter les risques sont similaires.

Pour limiter l'exposition aux attaques par accès local, l'une des règles fondamentales à respecter est le principe du « besoin d'en connaître », lequel suppose qu'un utilisateur doit accéder uniquement aux informations strictement nécessaires pour mener à bien ses tâches. Le principe du « privilège minimum » est appliqué à la conception et à l'application des règles et/ou de la politique de contrôle d'accès, afin de s'assurer que les utilisateurs accèdent uniquement aux ressources dont ils ont besoin. Cette philosophie est élargie pour inclure le principe de la « séparation des tâches », par exemple pour éviter qu'un administrateur puisse à la fois apporter des modifications à la politique de sécurité et les approuver.

Le cloisonnement représente une autre mesure classique pour limiter l'impact des attaques par accès local. Le zonage de sécurité du réseau est une technique de cloisonnement efficace. Il permet de limiter les risques en segmentant les services d'infrastructure par groupes logiques affectés des mêmes politiques et exigences de sécurité en matière de communications. Les zones sont séparées par des périmètres de sécurité définis au moyen de dispositifs réseau et de sécurité (pare-feux, systèmes IDS de détection des intrusions, logiciel de prévention des fuites de données).

Compte tenu du large spectre de vulnérabilités identifiées dans ce bloc, il est essentiel de concevoir et de mettre en place des programmes et procédures axés spécifiquement sur la protection de l'accès aux systèmes grâce à des méthodes de prévention, de détection et de dissuasion. Ces mesures seront étudiées en détail plus loin dans ce programme.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- être conscients des menaces posées par les collaborateurs internes d'une organisation ;
- décrire les attaques par accès local et identifier les composants d'une telle attaque ;
- expliquer les différences entre une attaque par accès distant ou par accès local ;
- comprendre les concepts des autorisations et des privilèges, ainsi que leur rôle dans le contrôle de l'accès utilisateur aux informations d'un système ;
- posséder des connaissances de base des techniques employées par les pirates pour utiliser leurs privilèges existants de manière illégitime et pour élever leurs privilèges ;
- expliquer comment appliquer les principes du privilège minimum et du besoin d'en connaître et les utiliser pour élaborer une politique de sécurité ;
- expliquer comment une politique de zonage de sécurité réseau bien conçue permet de cloisonner les informations.

Thèmes de modules possibles et approches à envisager

- Les acquis de ce bloc doivent inclure les politiques et programmes axés sur la formation du personnel, les niveaux d'autorisation, la limitation des risques et la sensibilisation générale à la problématique de l'accès physique aux systèmes et composants. Il est cependant possible de les étudier à différents niveaux de détail.
- L'utilisation de cas concrets intervenus dans le pays peut être un excellent moyen de sensibiliser et intéresser les apprenants au problème.
- Il est envisageable d'ajouter à la formation un examen des outils servant à détecter la présence des menaces actives dans un réseau et à en analyser les caractéristiques.

Méthode d'apprentissage et évaluation

Des cours magistraux et des démonstrations s'appuyant sur des exemples concrets sont recommandés.

Il sera intéressant d'examiner des études de cas, des exemples de scénario et d'aborder l'étude cybercriminalistique de cas concrets.

Exercice complexe possible : demander aux apprenants, travaillant en équipes, d'identifier et d'analyser un exemple réel d'attaque interne et de proposer des mesures qui auraient permis d'éviter la menace. Les apprenants peuvent s'appuyer sur un exemple de collaborateur interne indélicat qui abuse de ses privilèges pour compromettre des ressources auxquelles il ne devrait pas avoir accès en vertu du principe du besoin d'en connaître.

Les méthodes d'évaluation peuvent varier selon le niveau d'expertise attendu des apprenants, en ligne avec les objectifs d'apprentissage et de performances fixés.

Références

Centre for the Protection of National Infrastructure, "Insider misuse of IT systems," May 2013. https://www.cpni.gov.uk/documents/publications/2013/2013008-insider-misuse_of_it_systems.pdf?epslanguage=en-gb; also see "Cyber Insiders," https://www.cpni.gov.uk/advice/cyber/Cyber-research-programmes/Cyber-insiders/

Communications Security Establishment Canada, *Information Technology Security Guideline: Network Security Zoning: Design Considerations for Placement of Services within Zones* (ITSG-38), May 2009. https://cse-cst.gc.ca/en/system/files/pdf_documents/itsg38-eng_0.pdf

P.A. Legg et al., "Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection," Cyber Security Centre, Department of Computer Science, University of Oxford, 2013. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-insider_threat_detection.pdf?epslanguage=en-gb

Jason R.C. Nurse et al., "Understanding the insider threat: A framework for characterising attacks," IEEE 2014 Security and Privacy Workshops. https://www.cpni.gov.uk/documents/publications/2014/2014-04-16-understanding_insider_threat_framework.pdf?epslanguage=en-gb or http://www.ieee-secrity.org/TC/SPW2014/papers/5103a214.pdf

S. Sagan and M. Bunn, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge MA: American Academy of Sciences), 2014, ISBN 0-87724-097-3. https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderthreats.pdf

Derek A. Smith, National Cybersecurity Institute, "The Insider Threat," video. https://www.youtube.com/watch?v=z-CDyZdcGck

U.S. Department of National Defense, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security and Special Activities*, DoDM 5105.21-V3, 19 October 2012. http://www.dtic.mil/whs/directives/corres/pdf/510521m_vol3.pdf

Verizon Enterprise Solutions, "2015 Data Breach Investigations Report." www.verizonenterterprise.com

Markus Kont, Mauno Pihelgas, Jesse Wojtkowiak, Lorena Trinberg, Anna-Maria Osula, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015 «Insider Threat Detection Study». Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Insider_Threat_Study_CCDCOE.pdf

P. Gola and G. Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rechtsfragen und Handlungshilfen für die betriebliche Praxis, 5th ed., Cologne, 2009

F. Schwand, "Wenn Mitarbeiter Unternehmens-Laptops privat nutzen, besteht Regelungsbedarf," acant.service GmbH, 23 April 2014. [Online]. Available: http://www.acantmakler.de/2014/04/23/unternehmen-laptops-private-nutzung/. [Accessed 14 September 2015]

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon), "Isikuandmete töötlemine töösuhetes," 2011. [Online]. Available: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhe_58_tes%20juhendmaterjal26%2005%202014_0.pdf [Accessed 16 July 2015]

Deutscher Bundestag, "Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes," 15 December 2010. [Online]. Available at: http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf.

Atelier du comité de rédaction du programme de référence sur la cybersécurité à Garmisch (Participants de la République tchèque, du Royaume-Uni et des États-Unis).

T2-B4 : Risques liés à la mobilité, BYOD et tendances émergentes

Description

L'adoption des communications mobiles est un phénomène de société irréversible. Pourtant, ses ramifications sur la sécurité sont souvent mal comprises. En outre, les réseaux sociaux tels que Facebook et Twitter transforment les communications mondiales et interpersonnelles. L'empreinte numérique des personnes et des organisations, l'accès distribué depuis des dispositifs personnels mal sécurisés vers des systèmes parfois connectés à des systèmes sécurisés, les opérateurs commerciaux et de nombreuses évolutions récentes du même type constituent autant de facteurs de risque potentiels pour les systèmes et données sensibles. Ainsi, la perte ou le vol d'un ordinateur portable ou téléphone mobile contenant des contacts électroniques, des documents ou des raccourcis peuvent avoir des conséquences graves pour un individu, une organisation, une entreprise ou un pays. Ce bloc porte sur les problèmes de sécurité associés aux phénomènes et tendances précités.

Le BYOD (*Bring Your Own Device*) est une pratique qui permet aux collaborateurs d'une organisation d'apporter leurs dispositifs personnels (ordinateurs portables, tablettes, téléphones mobiles) sur leur lieu de travail et de les utiliser dans le cadre de leurs tâches professionnelles pour accéder à des informations et à des applications confidentielles. Cette pratique crée des tensions entre l'organisation, dont les politiques de sécurité doivent garantir la confidentialité et l'intégrité des informations, et les collaborateurs qui souhaitent rester propriétaires de leur dispositif et de leurs données personnelles tout en se protégeant contre une surveillance abusive. Les organisations doivent mettre en place des politiques et des procédures en cas de départ d'un collaborateur ou en cas de vol, de perte ou de vente de dispositifs pour éviter que des dispositifs non sécurisés soient utilisés par des pirates pour accéder aux systèmes d'entreprise via le réseau. L'utilisation du cloud pour le stockage des données pose des problèmes similaires au niveau du contrôle de l'accès et des configurations.

Contexte

Une pratique très répandue en entreprise consiste à concevoir une architecture de sécurité soigneusement cloisonnée en zones et à définir des points d'étranglement contrôlés pour gérer l'accès à Internet. Une politique BYOD pour les dispositifs connectables à Internet introduit de nouveaux points d'accès qui risquent d'échapper aux dispositifs ou mesures de contrôle prévus dans la politique de sécurité de l'entreprise. Selon un principe de base de la sécurité informatique, les couches supérieures d'un système informatique considèrent l'intégrité des couches inférieures comme un postulat de base. En ce qui concerne les applications d'entreprise, cela signifie qu'il est impossible d'implémenter sur le dispositif personnel des politiques de sécurité que son utilisateur (en général son propriétaire) ne puisse pas contourner. En d'autres termes, il n'est pas toujours possible d'installer des systèmes de sécurité d'entreprise (applications, etc.) sur les dispositifs personnels de manière systématique et uniforme, puisque leur propriétaire en conserve le contrôle administratif. Un dispositif non sécurisé, par exemple un smartphone personnel, ne peut pas être sécurisé par la simple installation d'outils de sécurité ou d'applications sécurisées. Il existe toutefois une série de pratiques qui permettent de renforcer la sécurité des dispositifs personnels ou de limiter les risques qu'ils posent. Celles-ci s'appuient sur l'architecture de sécurité pour limiter d'une part l'accès du dispositif au réseau d'entreprise, et d'autre part les informations qui peuvent être transmises au dispositif et stockées sur ce dernier. Les politiques de zonage régissant la segmentation et l'isolement réseau peuvent permettre la mise en œuvre d'une politique de mobilité des effectifs et une stratégie BYOD relativement sûre. Il faut toutefois noter que le choix de solutions très sécurisées peut nuire à la facilité d'utilisation des dispositifs personnels.

En outre, l'adoption croissante d'infrastructures IaaS (*Infrastructure as a Service*) au travers de technologies cloud conduit à une perte de contrôle potentielle sur l'architecture de sécurité de base (BSA, basic security architecture) et les pratiques de sécurité. Les dispositifs mobiles eux-mêmes créent des flux de données susceptibles d'intéresser les agences de renseignement et les entités commerciales étrangères. L'utilisation des réseaux sociaux expose également les individus au risque d'exploitation des informations communiquées à partir de leur dispositif mobile : le risque est de dévoiler une mine d'informations potentiellement compromettantes sur leurs relations, opinions, situations géographiques et habitudes. Ces sites de réseaux sociaux peuvent également représenter des vecteurs de menaces car ils constituent un point d'entrée vers divers systèmes informatiques, rendant ces derniers vulnérables aux infections ou aux intrusions. Ils peuvent être aussi utilisés à des fins de propagande ou de désinformation, de production participative (crowdsourcing), de communication de masse pour mobiliser les foules et autres activités similaires.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- comprendre les aspects positifs et négatifs des concessions vis-à-vis de la politique de sécurité qu'implique l'utilisation des réseaux sociaux dans l'environnement d'entreprise, tant du point de vue du personnel que de l'employeur ;
- être capables d'analyser les politiques BYOD et de mobilité dans le contexte de l'architecture de sécurité de l'entreprise et identifier les compromis à trouver entre sécurité et facilité d'utilisation ;

- analyser les politiques relatives à l'environnement cloud en ce qui concerne le stockage et le traitement des informations (p.ex. dossiers médicaux, données gouvernementales/militaires) dans des contextes nationaux ou internationaux.

Thèmes de modules possibles et approches à envisager

- Présentation des capacités des agents de menace, selon un niveau technique adapté au public visé
- Sensibilisation à la nécessité d'une sécurité adaptative face à des technologies qui ne cessent d'évoluer
- Besoins et limitations spécifiques des plateformes de communication mobiles, notamment dans la perspective du BYOD
- Besoins et limitations spécifiques en matière d'utilisation du cloud
- Élaboration et adoption des bonnes pratiques dans un environnement d'entreprise, sur la base des documents d'orientation nationaux et internationaux
- Exploitation des informations personnelles partagées sur les réseaux sociaux — Exercice visant à déterminer « ce que Google sait de vous » et discussion

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure des présentations, des discussions en classe, des ateliers de groupe et des discussions d'études de cas.

Une évaluation continue de la participation et des résultats des discussions de groupe et de classe est également recommandée.

Références

W. Arbaugh, D. Farber and J. Smith, "A Secure and Reliable Bootstrap Architecture," *Proceedings of the 1997 IEEE Symposium on Security and Privacy* (Oakland, CA) 1997, 65–71.

D.P. Cornish, "Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks," EU DG-For External Policies of the [European] Union Directorate B—Policy, February 2009. http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

Ravi Gupta and Hugh Brooks, *Using Social Media for Global Security* (Indianapolis, IN: John Wiley & Sons), 2013, ISBN 978-1-118-44231-9.

Zeb Hallock et al., *Cisco Unified Access (UA) and Bring Your Own Device (BYOD) CVD*, Cisco Systems, Inc., revised 28 August 2014, accessed 30 July 2015. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide.pdf

Raytheon Corp., *Security in the New Mobile Ecosystem*, Ponemon Institute Research Report, August 2014.

Murugiah Souppaya and Karen Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication 800-124, Revision 1, NIST, U.S. Department of Commerce, June 2013. http://dx.doi.org/10.6028/NIST.SP.800-124r1

U.S. DNI Defense Cyber Crime Center, *Countering Identity Theft Through Education and Technology*, October 2014.

U.S. Federal CIO Council and U.S. Department of Homeland Security, National Protection and Program Directorate, Mobile Security Reference Architecture, 23 May 2013. https://cio.gov/wp-content/uploads/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf

N. Mastali and J. I. Agbinya, "Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper," in 2010 Fifth International Conference on Broadband and Biomedical Communications (IB2Com), 2010.

H. Kärkkäinen, "Apple myy Suomessa vaarallisia puhelimia - ja sulkee kauppiaiden suut," 30 October 2014. [Online]. Available: http://www.digitoday.fi/tietoturva/2014/10/30/apple-myy-suomessa-vaarallisia-puhelimia--ja-sulkee-kauppiaiden-suut/201415103/66. [Accessed July 2016]

Teemu Väisänen, Alexandria Farar, Nikolaos Pissanidis, Christian Braccini, Bernhards Blumbergs, and Enrique Diez. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015 «Defending mobile devices for high level officials and decision-makers». Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Defending%20mobile%20devices%20for%20high%20level%20officials%20and%20decision-makers.pdf

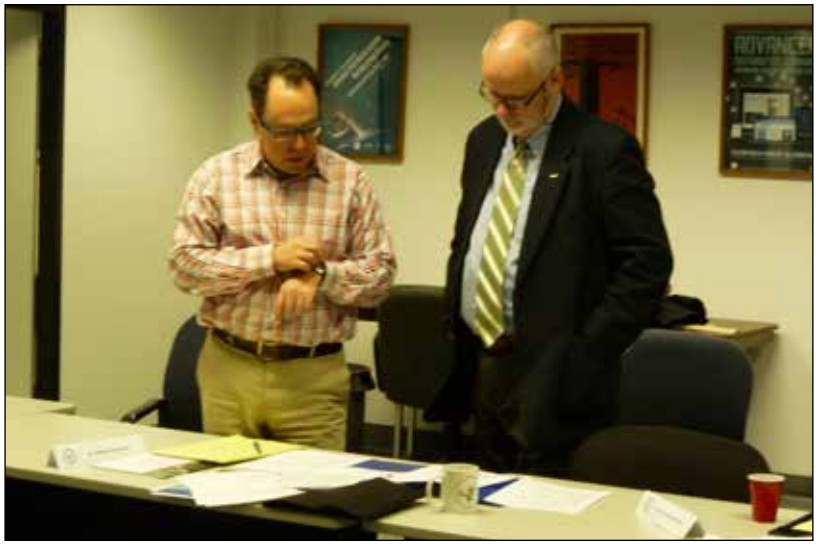
Gabriele Costa , Merlo Alessio, Luca Verderame, Konrad Wrona, «Developing a NATO BYOD Security Policy», 2016 International Conference on Military Communications and Information Systems (ICMCIS). IEEEm Brussels, Belguim, May 23-24, 2016. DOI: 10.1109/ICMCIS.2016.7496587. Available at: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?tp=&arnumber=7496587&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7496587

Ree C. Ho , Hiang K. Chua, «The Influence of Mobile Learning on Learner's Absorptive Capacity: A Case of Bring-

Your-Own-Device (BYOD) Learning Environment», in, Taylor's 7th Teaching and Learning Conference 2014 Proceedings, Singapore: Springer,2015. pp471-479. 2015. DOI: 10.1007/978-981-287-399-6_43. Print ISBN: 978-981-287-398-9. Online ISBN: 978-981-287-399-6.

Suri, Niranjan, Mauro Tortonesi, James Michaelis, Peter Budulas, Giacomo Benincasa, Stephen Russell, Cesare Stefanelli, and Robert Winkler. «Analyzing the applicability of Internet of Things to the battlefield environment.» In 2016 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1-8. IEEE, 2016.

Porche III, Isaac R. Emerging Cyber Threats and Implications. RAND Corporation, 2016.



Les coordinateurs de publication du programme de référence sur la cybersécurité.

Troisième thématique : Normes, politiques et organisations de cybersécurité internationales

Objectif

Dans cette troisième thématique, l'objectif général est de présenter aux apprenants les normes et les organismes internationaux, notamment l'*institut américain de normalisation et de technologie* (NIST), l'*institut britannique de normalisation* (BSI), ainsi que leur fonction et leur impact dans un cadre national. Les apprenants découvriront le rôle des organismes de normalisation internationaux et les principales organisations internationales dédiées à la cybersécurité. Ils devront par ailleurs examiner leurs politiques de cybersécurité nationales à la lumière des normes internationales et des pratiques recommandées, en comparant ces dernières à plusieurs exemples de politiques nationales. Enfin, cette thématique abordera l'évolution des cadres juridiques internationaux en matière de cybersécurité.

Description

Chaque pays devra adapter le contenu de la présente section à ses besoins spécifiques, en identifiant les organes nationaux responsables des politiques et pratiques de cybersécurité et en évaluant leur impact sur leurs organisations et politiques de cybersécurité. Même si les informations présentées varieront d'un pays à l'autre, la présentation de cette thématique peut être organisée comme suit : bloc T3-B1, « Organisations de cybersécurité internationales » (à adapter en fonction du contexte national) ; bloc T3-B2, « Normes et exigences internationales — Étude des organes et des pratiques » ; bloc T3-B3, « Cadres de cybersécurité nationaux » (analyse comparative des différents cadres nationaux) ; et bloc T3-B4, « La cybersécurité dans les législations nationales et internationales ».

Objectifs d'apprentissage

Comme il s'agit d'un problème de sécurité émergent, les diverses réponses nationales et internationales en matière de cybersécurité prennent forme dans des organisations existantes ou créées à cette fin. La cybersécurité constitue une problématique nationale et transversale qui exige des politiques et une coordination globales. Cela étant, les réponses varient considérablement d'un pays à l'autre.

Au travers de l'exploration des pratiques des États qui élaborent des politiques nationales en matière de cybersécurité gouvernementale, commerciale ou individuelle et soutiennent des acteurs non étatiques dans le développement de cadres de gestion des risques et des menaces, les apprenants devront acquérir les compétences suivantes :

- prendre conscience que les réponses nationales et internationales exigent une approche multilatérale ;
- identifier les principales organisations nationales responsables de la cybersécurité ;
- identifier et comprendre les rôles et les exigences des organismes de normalisation nationaux et internationaux ;
- comprendre l'importance de la relation entre cybersécurité, services de renseignement et institutions militaires ;
- analyser les pratiques et politiques nationales à la lumière des bonnes pratiques et normes internationales ;
- comprendre le rôle des principales organisations internationales en matière de cybersécurité
- connaître l'évolution du cadre juridique international et la position de principe du gouvernement national dans ce régime émergent.

Références recommandées

IT Governance Ltd., "Information Security & ISO 27001: An Introduction," IT Governance Green Paper, October 2013.

Klimburg, Alexander, ed., *National Cyber Security Framework Manual*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2012.

National Institute of Standards and Technology, U.S. Department of Commerce, *Security and Privacy Controls for Federal Information Systems and Organizations*, Joint Task Force Transformation Initiative, NIST Special Publication 800-53, Revision 4, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

PricewaterhouseCoopers LLP, "Why you should adopt the NIST Cybersecurity Framework," May 2014. https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

The White House, *Cyberspace Policy Review*. https://www.whitehouse.gov/cyberreview/documents

U.S. Government Accountability Office, *Report to Congress: Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606, July 2010.

T3-B1 : Organisations de cybersécurité internationales

Description

Le nombre d'organisations internationales, gouvernementales et non gouvernementales concernées par les questions de cybersécurité mondiales ou régionales va croissant. Leurs intérêts couvrent de nombreux domaines : enquêtes, réglementations, législations, défense des politiques, supervision et bien d'autres. Nombre d'entre elles s'efforcent d'élaborer des approches collectives à la résolution des problèmes liés au cyberespace, tandis que d'autres cherchent parfois à défendre les intérêts nationaux ou commerciaux. Pour ces raisons et d'autres, leurs recommandations doivent faire l'objet d'une analyse critique.

Le site web du Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCD COE – https://ccdcoe.org) propose des liens intéressants vers de nombreuses agences régionales concernées par les politiques et pratiques de cybersécurité au sens large. Parmi celles-ci, citons l'Union européenne, et plus particulièrement le travail de l'Agence européenne chargée de la sécurité des réseaux et de l'information, ENISA (www.enisa.europa.eu) ; l'Organisation pour la sécurité et la coopération en Europe, OSCE (www.osce.org) ; l'ONU (www.un.org/fr/index) ; et bien entendu l'OTAN (www.nato.int). Outre ces sources, on compte également des agences telles que le Global Forum for Incident Response and Security Teams (www.first.org), l'International Multilateral Partnership Against Cyber Threats (IMPACT) et l'Association des communications et de l'électronique des forces armées (AFCEA). L'ENISA gère et met régulièrement à jour une liste d'organisations de réponse aux cybercrises ou de centres de réponse aux incidents de sécurité informatique (CERT) des États membres de l'Union européenne.

Parmi les autres organes internationaux traitant des questions de cybersécurité, citons l'Organisation internationale de normalisation (abordée au bloc 2 de la présente thématique), l'ICANN (*Internet Corporation for Assigned Names and Numbers*), le Forum sur la gouvernance d'Internet (IGF) et l'Union internationale des télécommunications de l'ONU (UIT).

Ce bloc s'intéresse principalement aux interactions des gouvernements avec ces nombreuses organisations internationales et examine les pratiques communes qu'ils adoptent souvent sur la base de leurs recommandations.

Acquis d'apprentissage

Sur le plan de la cybersécurité, les apprenants auront acquis les compétences suivantes :

- exposer les différents enjeux auxquels les gouvernements sont confrontés et leurs interactions avec les organisations internationales ;
- identifier les principales organisations internationales, leurs priorités en matière de politiques et leur rôle dans l'information et le soutien de la cybersécurité nationale ;
- identifier les organisations nationales en charge du développement de la coopération et de l'engagement à l'échelon international.

Thèmes de modules possibles et approches à envisager

Il convient de faire appel à un expert national pour identifier les principaux organes internationaux à même de fournir à l'État des lignes directrices et dont il peut se servir pour exprimer ses préoccupations.

Autres thèmes possibles :

- principaux organes internationaux d'information sur les pratiques nationales : l'UE, l'OTAN, le gouvernement américain (Cyber Command, etc.) et Europol (voir www.europol.europa.eu/ec3) ;
- points de convergence entre les intérêts nationaux et les organisations internationales et leurs objectifs ;
- identification des aspects positifs et négatifs des approches des organisations internationales en matière de cybersécurité ;
- mesures et mécanismes nationaux mis en place pour résoudre ces défis d'envergure internationale ;
- utilisation d'Internet à des fins criminelles/terroristes transnationales.

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure l'analyse de problématiques actuelles. Les apprenants devront passer en revue et analyser des études de cas illustrant les réponses d'organisations internationales et examiner les principaux enjeux internationaux actuels et leur impact pour les pays.

L'évaluation portera sur un projet collectif impliquant une participation en classe et un devoir écrit sur la réponse d'une organisation internationale en matière de cybersécurité.

Références

Outre les ressources web susmentionnées, vous pouvez consulter les références suivantes :

N. Choucri, S. Madnick and J. Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," *Information Technology for Development* 20, no. 2 (2013): 96–121. http://dx.doi.org/10.1080/02681102.2013.836699

Takeshi Takahashi, Youki Kadobayashi, «Reference Ontology for Cybersecurity Operational Information», Computer Journal Vol.50, No 10, 2014. Journal ISSN: 1460-2067.

Farzan Kolini, Lech Janczewski, «Cyber Defense Capability Model: A Foundation Taxonomy», (2015). CONF-IRM 2015. Proceedings. Paper 32. Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015&context=confirm2015

Feng Xie, Yong Peng, Wei Zhao, Yang Gao, Xuefeng Han, «Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges», in, Computer Information Systems and Industrial Management, pp624-635, 2014. Springer Berlin Heidelberg. DOI: 10.1007/978-3-662-45237-0_57.Print ISBN: 978-3-662-45236-3. Online ISBN:978-3-662-45237-0.

Akinola Ajijola, Pavol Zavarsky, Ron Ruhl, «A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012». Paper presented at the 'World Congress on Internet Security (WorldCon)' 2014. pp66-73. 10.1109/WorldCIS.2014.7028169. Available from the IEEE at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7028169&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7028169

T3-B2 Normes et exigences internationales — Étude des organes et des pratiques

Description

Ce bloc présente les différentes normes internationales établies par les organismes de normalisation. Il permettra aux apprenants de mieux comprendre le rôle des normes et des exigences techniques internationales. Les apprenants devront se familiariser avec les normes ISO (Organisation internationale de normalisation), COBIT (Objectifs de contrôle dans les domaines de l'information et des technologies associées), ISACA (*Information Systems Audit and Control Association*) et ITIL (*International Technical Infrastructure Library*). Les discussions porteront sur divers organismes de normalisation dont l'institut américain de normalisation et de technologie (NIST, *National Institute of Standards and Technology*), l'institut britannique de normalisation (BSI, *British Standards Institute*), le bureau fédéral allemand pour la sécurité de l'information (BSI, *Bundesamt für Sicherheit in der Informationstechni*k), ASIS International (et éventuellement d'autres normes en fonction des besoins et des attentes) ; l'objectif étant de mettre en lumière les types de normes et les difficultés posées par leur mise en application ainsi que les problèmes présentés par des normes « concurrentes ». Ce bloc aborde par ailleurs la position des pays en matière d'adoption des normes internationales. Enfin, il présente les limitations des normes et les raisons pour lesquelles les institutions militaires, les organismes de défense et autres organismes gouvernementaux peuvent décider d'établir leurs propres normes.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- comprendre le rôle des normes et des exigences techniques internationales ;
- identifier les organismes de normalisation internationaux (p. ex. l'ISO, le NIST) ;
- identifier les sources de normes internationales guidant leur cyberstratégie nationale ;
- déterminer les enjeux et les difficultés associés à la mise en application de normes internationales ;
- savoir comment et par quels organes les normes de cybersécurité sont établies, gérées et promulguées dans leur organisation.

Thèmes de modules possibles et approches à envisager

Thèmes possibles :

- normes nationales et normes internationales adoptées à l'échelle nationale en rapport direct avec la cybersécurité ;
- normes nationales apparentées en matière de procédure ou d'organisation ;
- enjeux et difficultés associés à la mise en application de normes internationales.

Méthode d'apprentissage et évaluation

La méthodologie d'évaluation doit être adaptée au niveau de performance établi pour les cours et les leçons inspirés du présent programme de référence.

Un expert national résumera les différentes normes adoptées par le pays et expliquera leurs relations avec les normes de cybersécurité internationales et émergentes.

Les apprenants peuvent chercher et analyser des études de cas relatives à la mise en application de normes internationales.

Il peut être intéressant d'organiser une discussion de groupe sur les difficultés que pose la mise en application des normes internationales. Les exemples doivent idéalement se fonder sur des cas concrets auxquels ils ont été confrontés.

Références

ISACA, European Cybersecurity Implementation: Overview, ISACA Whitepaper, 2014. http://www.isaca.org or http://www.isaca.org/knowledge-center

ISACA, European Cybersecurity Implementation Series: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/european-cybersecurity-implementation-series.aspx; see also ISACA's reports on Resilience, Risk Guidance, Assurance and Audit programs.

PricewaterhouseCoopers LLP, *Why you should adopt the NIST Cybersecurity Framework*, May 2014. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf

Steve Purser, "Standards for Cyber Security" in M.E. Hathaway (ed.), *Best Practices in Computer Network Defense: Incident Detection and Response* (Amsterdam: IOS Press), 2014, 97–106. doi:10.3233/978-1-61499-372-8-97

Other standards series (in addition to ISO 27000):

- ISO 9000 (quality management)
- ISO 22300 (business continuity management)
- ISO 31000 (risk management)
- BSI PAS 555

Iñigo Barreira, Izenpe, Jerome Bordier, SEALWeb, Olivier Delos, Arno Fiedler, Nimbus Technologieberatung GmbH, Tomasz Mielnicki, Gemalto, Artur Miękina, Polish Security Printing Works, Jon Shamah, EJ Consultants, Clemens Wanko, TUV Informationstechnik GmbH, Clara Galan Manso, ENISA, Sławomir Górniak, ENISA, «Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards», EU ENISA, July 1, 2016. Available at: https://www.enisa.europa.eu/publications/tsp_standards_2015

Manmohan Chaturvedi, Abhishek Narain Singh , Manmohan Prasad Gupta, Jaijit Bhattacharya , (2014) «Analyses of issues of information security in Indian context», Transforming Government: People, Process and Policy, Vol. 8 Issue: 3, pp.374 - 397. DOI (available at): http://www.emeraldinsight.com/doi/abs/10.1108/TG-07-2013-0019

L. Zhang, Q. Wang, B.Tian, «Security Threats and Measures for the Cyber-Physical Systems», in, The Journal of China Universities of Posts and Telecommunications, Vol. 20, Supp.1, 2013, pp25-29. Journal ISSN: 1005-8885. UIN: ETOCRN339930374

Blaž Markelj, Sabina Zgaga, «Comprehension of Cyber Threats and their Consequences in Slovenia», in, Computer Law & Security Review: The International Journal of Technology Law and Practice. Vol. 32. Issue 3 (2016). Journal ISSN: 2212-473X (Electronic - British Library ELD Digital store). UIN: ETOCvdc_100032209717.0x000001.

Shackelford, Scott, Scott L. Russell, and Jeffrey Haut. «Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks.» UC Davis Business Law Journal (2016).

T3-B3 : Cadres de cybersécurité nationaux

Description

Dès lors qu'il s'agit d'un problème national transcendant les frontières traditionnelles entre l'État, les entreprises et les citoyens, la cybersécurité exige des politiques et une coordination globales. Compte tenu de l'interconnectivité des systèmes, de nombreux gouvernements ont admis avoir besoin d'une approche pangouvernementale dans le simple but de gérer la sécurité de leurs propres systèmes d'exploitation. C'est d'autant plus important lorsqu'il s'agit de minimiser les risques encourus par les entreprises et les particuliers. Toutefois, les réponses ont été très différentes d'un pays à l'autre. Certains pays ont créé des organes nationaux responsables de la gestion de la cybersécurité nationale, tandis que d'autres ont confié l'élaboration de leurs politiques à des organes de coordination, en laissant toutefois aux divers ministères le soin de gérer et de mettre en œuvre ces politiques. D'autres encore peinent à trouver un cadre approprié. De nombreux gouvernements sont allés au-delà de l'élaboration ou du soutien des mesures de cybersécurité réservées à la protection de l'appareil étatique pour considérer le problème comme un risque national. Ils ont dès lors mis en place des initiatives destinées à promouvoir les bonnes pratiques auprès des entreprises et des citoyens et à les sensibiliser à cette problématique. La promotion ou l'application de telles mesures visait plus particulièrement la protection des infrastructures critiques, souvent exploitées par des sociétés privées. Quoi qu'il en soit, il existe des exigences communes, comme la mise en place de rôles et responsabilités structurels, l'élaboration de documents d'orientation technique officiels, la définition des rôles et responsabilités pour la limitation des risques et les réponses à apporter aux problèmes urgents. Ce bloc a pour but de sensibiliser les apprenants aux politiques, stratégies et structures de cybersécurité de leur pays. Ils doivent connaître le cadre stratégique des politiques de leur pays (pour autant qu'il en existe un) et des organisations responsables de l'élaboration des spécifications techniques et des documents d'orientation nationaux . Les apprenants devront comparer les documents et approches stratégiques nationaux et internationaux en matière de cybersécurité afin de mieux comprendre les leurs et d'évaluer les domaines de risques et de responsabilité.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- identifier les organisations responsables de leurs politiques de cybersécurité nationales ;
- identifier les principales caractéristiques de leurs politiques de cybersécurité nationales ;
- identifier les organisations responsables et comprendre leur rôle dans la rédaction et la publication de directives et documents d'orientation techniques ;
- identifier les éléments clés des directives/documents d'orientation techniques ;
- connaître les sources de bonnes pratiques dans l'organisation de la cybersécurité nationale ;
- entreprendre une analyse critique de l'approche nationale en la comparant à des cadres de référence.

Thèmes de modules possibles et approches à envisager

- Approche centralisée ou multilatérale en matière de sécurité
- Approches nationales en matière de coopération, de coordination et de collaboration
- Organisations internationales : rôles et interactions dans le contexte national
- Cadres de référence en matière de politiques : examen de plusieurs exemples

Méthode d'apprentissage et évaluation

La méthodologie d'évaluation doit être adaptée au niveau de performance établi pour les cours et les leçons inspirés du présent programme de référence.

La méthode d'enseignement peut inclure des discussions, des interventions par des spécialistes du domaine, des études de cas comparatives, l'identification des bonnes pratiques et la visite d'organes nationaux de cybersécurité.

Références

Defense Science Board, U.S. Department of Defense, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

George Farah, *Information Systems Security Architecture: A Novel Approach to Layered Protection—A Case Study*, GSEC Practical Version 1.4b, SANS Institute, 9 September 2004. www.sans.org

Alexander Klimburg, ed., *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn, Estonia, 2012, ISBN 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, report by NIST Joint Task Force Transformation Initiative, NIST Special Publication 800-53, Revision 4, NIST, U.S. Department of Commerce, Washington, DC, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4

Organisation for Economic Co-operation and Development (OECD), *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, 2012. http://oe.cd/security

Sławomir Górniak, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, Jon Shamah, Sławomir Górniak, «Governance Framework of the European Standardization: Aligning Policy, Industry and Research, v1.0», Heraklion, Greece, ENISA, 2015, ISBN 9789292041540.

Tomas Minarik, «National Cyber Security Organisation: Czech Republic», 2nd Revised Ed, Tallinn, 2016. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CZE_032016.pdf

Vytautas Butrimas, «National Cyber Security Organisation: Lithuania», Tallinn, 2015. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf

Lea Hriciková, Kadri Kaska, «National Cyber Security Organisation: Slovakia», Tallinn, 2015. NATO CCD COE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SLOVAKIA_042015.pdf

Lehto, Martti, and Jarno Limnéll. «Cyber Security Capability and the Case of Finland.» In European Conference on Cyber Warfare and Security, p. 182. Academic Conferences International Limited, 2016.

T3-B4 : La cybersécurité dans les législations nationales et internationales

Description

Le paysage juridique de la cybersécurité est complexe et évolue rapidement. Certains s'interrogent sur l'applicabilité des lois existantes et émergentes (tant à l'échelle nationale qu'internationale) pour résoudre les problèmes et les enjeux de cybersécurité. On observe par ailleurs de grandes différences dans la façon dont les pays abordent la question dans leur propre législation nationale. Certains États ont adopté des lois spécifiques en matière de cybersécurité, d'autres non. La difficulté de l'attribution des responsabilités, c.-à-d. de l'identification de la source des cyberactivités malveillantes, dangereuses ou illégales, ne fait qu'aggraver le problème dans la sphère nationale et internationale

Les textes de loi nationaux et internationaux applicables à la cybersécurité ne cessent d'évoluer. Ce bloc a pour but de présenter les lois nationales et internationales traitant des questions de cybersécurité. De nombreux pays et leurs organisations sont soumis à diverses réglementations dont l'obligation de déclaration de certains types de transactions financières ou compromissions de données. Il existe par ailleurs un cadre régulièrement revu de normes et pratiques prescrites par les instances judiciaires et policières (comme les accords de coopération établis par Interpol). De nombreux États ont adopté les dispositions légales relatives à la déclaration des cyberincidents et un projet d'élaboration d'un code international de cyberéthique est en cours. Toutefois, il n'existe à l'échelle internationale aucun organe directeur ou instance dirigeante pour la supervision des aspects juridiques de la cybersécurité.

Ce bloc doit présenter aux apprenants les positions nationales en matière de droit national et international relatif au cyberespace, et plus particulièrement la cybersécurité. À l'échelon national, plusieurs domaines sont tout particulièrement visés, notamment le respect de la vie privée, le contrôle des systèmes, la conformité réglementaire ainsi que les répercussions sur les assurances commerciales dans les cadres juridiques internationaux et nationaux émergents.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- identifier les principaux enjeux d'une législation internationale sur le cyber et les sources des politiques ;
- expliquer les dispositions en vigueur et les responsabilités légales des parties prenantes à la cybersécurité nationale ;
- connaître les dispositions légales nationales en matière de cybersécurité (le cas échéant) et identifier les principales autorités judiciaires au sein de leurs organisations.

Thèmes de modules possibles et approches à envisager

- Des thèmes tels que le statut juridique international controversé des cyberattaques menées par des acteurs étatiques et non étatiques, les questions de cybersécurité dans la législation nationale, les exigences de conformité des organisations et la responsabilité juridique individuelle, peuvent faire l'objet d'une analyse plus ou moins détaillée.
- Discuter de la proposition de code de conduite international pour la sécurité des informations présentée par l'ONU
- Réglementations de conformité nationales
- Assurances commerciales et responsabilités en matière de cyberrisques

Méthode d'apprentissage et évaluation

Des cours magistraux doivent être élaborés en coordination avec des représentants légaux habilités à exprimer la position de leur pays sur ces questions.

Il est recommandé d'examiner des études de cas sur les réponses juridiques internationales et nationales aux incidents de cybersécurité.

L'outil d'évaluation doit consister en un court examen écrit, conforme au niveau de détail de la matière enseignée.

Références

Dan Arnaudo, "Research Note: The Fight to Define U.S. Cybersecurity and Information Sharing Policy," ASA Institute for Risk & Innovation, 2013. http://www.anniesearle.com/research.aspx?topic=researchnotes

Nils Melzer, Cyberwarfare and International Law, United Nations Institute for Disarmament Research (UNIDIR), Geneva, 2011. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

NATO, *Legal Gazette: Legal Issues Related to Cyber* 35 (December 2014). This issue addresses, in separate articles, (1) legal aspects of cybersecurity and cyber-related issues affecting NATO; (2) active cyber defense to responsive cyber defense; and (3) an exploration of the threshold of "armed attack" and related legal issues of attribution and participation in cyber warfare. https://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

NATO Cooperative Cyber Defence Centre of Excellence (Michael N. Schmitt, General Editor), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press), 2013. https://ccdcoe.org/tallinn-manual.html

Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?," *Stanford Law & Policy Journal* 25 (2014): 269–299.

Hong XU. «Cyber law in China» Alphen aan den Rijn: Kluwer Law International, 2010. ISBN 9789041133335. British Library Shelfmark: YC.2011.a.9251. UIN: BLL01015641102

Radziwill Yaroslav, «Cyber-Attacks and the Exploitable Imperfection of International Law.» Leiden: Brill Nijhoff, 2015. ISBN 9789004298330.

Anna-Maria Osula and Henry Rõigas (eds), International Cyber Norms: Legal, Policy & Industry Perspectives (2015). NATO CCD COE. E-Book. Full Book Available at: https://ccdcoe.org/multimedia/international-cyber-norms-legal-policy-industry-perspectives.html

Zeinab Krake, Sheikha Lubna Al Qasimi, Cyber Security in Developing and Emerging Economies, 2010, Cheltenham: Edward Elgar Publishing.

Fidler, David P., Richard Pregent, and Alex Vandurme. «NATO, Cyber Defense, and International Law.» Journal of International and Comparative Law 4, no. 1 (2016): 1.

Saran, Samir. «Striving for an International Consensus on Cyber Security: Lessons from the 20th Century.» Global Policy 7, no. 1 (2016): 93-95.

Quatrième thématique : Gestion de la cybersécurité dans le contexte national

Objectif

L'objectif général de cette thématique est d'explorer la pratique de la gestion de la cybersécurité dans le contexte national.

Description

L'approche de la gestion des problèmes de cybersécurité nationaux variera considérablement selon les pays. Cependant, si les réponses et les enjeux nationaux présentent leurs spécificités, la nature des problèmes rencontrés sera similaire dans tous les pays. Les cadres de cybersécurité nationaux peuvent différer sur des points de détail, mais un cadre exhaustif englobe généralement les questions suivantes, qui nécessitent une gestion et une coordination actives : (1) gestion des actifs informatiques physiques ; (2) gestion des contrôles ; (3) gestion de la configuration des systèmes et des modifications de configuration ; (4) identification et gestion des vulnérabilités ; (5) gestion des incidents ; (6) gestion de la continuité des services ; (7) gestion de l'identification et du traitement des menaces ; (8) gestion des dépendances et liens externes ; (9) formation et sensibilisation ; et (10) maintien de la connaissance de la situation[7].

Cette thématique explore en profondeur les pratiques nationales de gestion de la cybersécurité et contextualise le niveau de préparation national en matière de sécurité dans un cadre de gestion des risques. En particulier, le bloc T4-B1, Pratiques, politiques et organisations nationales de cyberrésilience, se penche sur l'élaboration de plans d'intervention d'urgence et la reprise sur cyberincident en vue de minimiser les défaillances. Le bloc T4-B2, Cadres de cybersécurité nationaux, présente les pratiques nationales de gestion de la cybersécurité, notamment en matière d'opérations, de réponse aux incidents et de limitation des risques. Le bloc T4-B3, Cybercriminalistique, initie les apprenants aux outils, pratiques et procédures de cybercriminalistique permettant de recueillir, d'analyser et d'interpréter les données à des fins d'attribution de la responsabilité et de collecte d'informations. Le bloc T4-B4, Audit et évaluation de la sécurité au niveau national, présente aux apprenants les bonnes pratiques d'évaluation du niveau de préparation national en matière de cybersécurité.

Objectifs d'apprentissage

Les apprenants doivent acquérir les compétences suivantes :

- comprendre l'approche appliquée aux systèmes pour la planification de la résilience aux menaces, aux attaques et à d'autres événements similaires ;
- inscrire l'utilisation de systèmes résilients dans un contexte national ;
- analyser l'utilité des cadres et matrices pour la planification et la délégation ;
- connaître les types courants d'organisations nationales de réponse aux incidents et se familiariser avec le rôle, le mandat et la structure de leur système national actuel et des organisations de gestion des crises et incidents organisationnels.

Références recommandées

Deborah J. Bodeau and Richard Graubart, *Cyber Resiliency Engineering Framework*, MITRE Technical Report MTR 110237, The MITRE Corporation, September 2011. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

Mohamed Dafir Ech-Cherif El Kettani and Taïeb Debbagh, "A National RACI Chart for an Interoperable 'National Cyber Security' Framework," *Proceedings of the European Conference on Information Warfare & Security*, January 2009.

Nicole Falessi, Razvan Gavrila, Maj. Ritter Kleinstrup and Konstantinos Moulinos, National Cyber Security Strategies: Practical Guide on Development and Execution, European Network and Information Security Agency, December 2012. https://www.enisa.europa.eu

Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem*, Full Report, ENISA, April 2011.

Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman and Lukas Ruf, "What is a Security Architecture?," paper by the Working Group Security Architecture, Information Security Society Switzerland, 29 September 2008.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide*, Carnegie Mellon University, February 2014.

See resources at Carnegie Mellon University CERT Software Engineering Institute, CERT-RMM (CERT Resilience Management Model): www.cert.org/resilience/rmm.html

[7] Inspiré du modèle de gestion de la résilience CERT-RMM de Carnegie Mellon.

T4-B1 : Pratiques, politiques et organisations nationales de cyberrésilience

Description

La cybersécurité transcende de nombreuses frontières organisationnelles. Un certain nombre d'États ont adopté une approche pangouvernementale globale de l'attribution des rôles et responsabilités en matière de gestion de la cyberrésilience. La cyberrésilience vise à garantir que la infrastructure cyber nationale reste opérationnelle en mode de crise et qu'elle est rétablie rapidement et efficacement après une défaillance. Ce bloc présente une analyse comparée des pratiques nationales et organisationnelles dans le contexte de la résilience.

Dans le cadre de ce bloc, les apprenants découvriront divers exemples d'approches globales de la cybersécurité, telles que décrites dans les documents d'orientation de haut niveau publiés (comme ceux du Royaume-Uni ou des États-Unis), afin d'être en mesure d'analyser les points forts et les faiblesses de leur politique nationale. Les politiques nationales pertinentes pour le groupe d'apprenants seront ensuite comparées. La discussion doit en particulier être axée sur l'examen des politiques et pratiques existantes visant à assurer la prévention, la protection, la réponse et la gestion de la reprise sur cyberincident. Les mesures telles que l'audit, la vérification et les moyens d'un examen indépendant doivent également être abordées.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- interpréter des documents nationaux traitant de la cyberrésilience ;
- contribuer à l'élaboration et au développement de procédures nationales de cyberrésilience ;
- décrire les rôles et responsabilités des personnes et organisations responsables de la cyberrésilience nationale ;
- comprendre les difficultés liées à la coordination des cyberopérations en situation de crise ;
- comprendre les processus d'analyse décisionnelle motivant les décisions relatives à la conformité en situation de crise.

Thèmes de modules possibles et approches à envisager

Un expert national doit analyser les politiques nationales existantes afin d'identifier le niveau d'informations approprié à utiliser dans le cadre des cours.

Méthode d'apprentissage et évaluation

La méthode d'enseignement peut inclure des cours magistraux, des démonstrations, des visites sur le terrain et des exercices écrits. L'évaluation doit reposer sur un examen oral et écrit.

Références

Un expert devra compiler les politiques et références nationales pertinentes. Parmi les exemples de références plus générales, citons :

Deborah J. Bodeau and D.J. Graubart, *Cyber Resiliency Engineering Framework, MITRE Technical Report MTR 110237 (Bedford, MA: The MITRE Corp.), September 2011*.

Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem*, Full Report, ENISA, April 2011.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide*, Carnegie Mellon University, February 2014.

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Question Set with Guidance*, Carnegie Mellon University, February 2014.

See resources at Carnegie Mellon University's CERT Software Engineering Institute CERT-RMM (CERT Resilience Management Model): www.cert.org/resilience/rmm.html

Clausewitz Gesellschaft; Bundesakademie für Sicherheitspolitik. «Sicherheitspolitik im Cyber-Zeitalter: Reicht passive Abwehr aus?» Bonn, Germany : Mittler Report Verlag, 2014, British Library Identifier: 016828758. Document Supply Number: 3829.361655 UIN: BLL01016828758

Guido Nannariello, «E-commerce e tutela del consumatore: indagine sui codici di condotta ed i processi di certificazione», Ispra: Joint Research Centre, Institute for the Protection and Security of Citizen, Cybersecurity Sector, 2001. UIN: BLL01011092147.

F. Cassim, «Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South Africa and Other Regional Role Players», in, Comparative and International Law Journal of Southern Africa, Vol.44, No.1, 2011, pp123-138 (University of South Africa). Journal ISSN: 0010-4051. UIN: ETOCRN296687880.

N. Shirazi, «A Framework for Resilience Management in the Cloud», in, Elektrotechnik und Informationstechnik, Vol. 132; No.2, 2015, pp122-132. Journal ISSN: 0932-383X. UIN: ETOCRN370071353.

Kallberg, Jan. «Assessing India's Cyber Resilience: Institutional Stability Matters.» Strategic Analysis 40, no. 1 (2016): 1-5.

Atelier du comité de rédaction du programme de référence sur la cybersécurité à Tbilissi.

T4-B2 : Cadres de cybersécurité nationaux

Description

Ce bloc permet aux apprenants de comprendre la stratégie de cybersécurité nationale et sa mise en œuvre dans le cadre de la gestion des cyberopérations, du traitement des incidents de cybersécurité de niveau national et de la gestion des risques de cybersécurité nationaux. L'accent doit être mis sur les cadres qui facilitent l'allocation des ressources, définissent les rôles et responsabilités organisationnels et précisent les mesures à prendre tout au long de la chaîne de commandement pour ce qui concerne la responsabilité et l'élaboration de rapports.

S'appuyant sur les normes nationales et internationales, ce bloc s'intéresse aux fondements et cadres de sécurité, et examine plusieurs cadres globaux visant à définir les rôles et responsabilités en matière de gestion des risques de cybersécurité et de réponse aux incidents de cybersécurité. Ces cadres sont souvent résumés sous la forme d'une matrice de délégation RACI (*Responsibility, Accountability, Command and Information*). Ces outils de délégation sous forme de matrice sont également adaptés à la gestion des opérations de cybersécurité. Un exemple de matrice RACI sera utilisé comme outil pédagogique. Les apprenants se familiariseront avec la conception générale de ce type d'outil avant de traiter leur matrice nationale de responsabilité et de réponse. Dans la mesure du possible, les outils associés aux politiques nationales servant à gérer la délégation des responsabilités et des tâches seront identifiés et examinés. La discussion portera sur les outils d'aide à la décision ainsi que sur les outils, cadres, pratiques et responsabilités liés à la gestion des risques. Enfin, les apprenants examineront le cadre de gestion déléguée de la cybersécurité adopté par leur gouvernement national ou au moins par leur organisation.

La cyberrésilience des systèmes peut inclure les activités suivantes : gestion des actifs, gestion des contrôles, gestion de la configuration et des modifications, gestion des menaces et des vulnérabilités, planification et gestion de la continuité des services, gestion des dépendances externes, formation, sensibilisation au niveau organisationnel et individuel, et gestion active de la connaissance de la situation.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- comprendre le concept de matrice de responsabilité pour la planification et la délégation ;
- examiner les problèmes généraux liés à la mise en œuvre de leur stratégie de cybersécurité nationale ;
- comprendre les modes d'interaction avec les structures nationales de commandement et de contrôle de la réponse aux incidents ;
- comprendre la gestion déléguée des cyberopérations au niveau national ;
- comprendre comment les cyberrisques sont gérés dans le contexte de la politique nationale ;
- appréhender les aspects positifs et négatifs des cadres officiels de gestion des ressources appliqués au contexte de la cybersécurité nationale.

Thèmes de modules possibles et approches à envisager

Les sujets abordés peuvent inclure le système RACI ou des outils de matrice de responsabilité similaires pour le traitement des incidents et la gestion des interventions et reprises sur incident.

Méthode d'apprentissage et évaluation

Un expert doit dresser un panorama succinct des méthodes (telles que la création d'une matrice RACI) avant d'identifier les autorités nationales et organisationnelles et les documents d'orientation explicites, s'ils existent. L'expert peut ensuite identifier les plus pertinents d'entre eux pour le groupe d'apprenants concerné.

Le type d'évaluation doit être adapté au niveau de connaissance défini spécifiquement pour les cours inspirés de ce programme de référence.

Références

Paul Cichonski, Tom Millar, Tim Grance and Karen Scarfone, *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*, Special Publication NIST 800-61, Revision 2, U.S. Department of Commerce, August 2012.

Mohamed Dafir Ech-Cherif El Kettani and Taïeb Debbagh, "A National RACI Chart for an Interoperable 'National Cyber Security' Framework," *Proceedings of the European Conference on Information Warfare & Security*, 2009.

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

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Question Set with Guidance*, Carnegie Mellon University, February 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

International Standards Organization ISO 22300 series and ISO 27000 series—see earlier list.

IU. V. Nesteriak, (IUriĭ Vasyl'ovych). «Derzhavna informatsiĭna polityka Ukraïny: teoretyko-metodolohichni zasady», Kiev, Ukraine, 2014. Monograph. ISBN 9789666193554. UIN: BLL01017709318.

Francis Domingo, «Cyber Policy in China», Europe-Asia Studies, 2015. DOI: 10.1080/09668136.2015.1102519. Available at: http://www.tandfonline.com/doi/full/10.1080/09668136.2015.1102519

Tuija Kuusisto, Rauno Kuusisto, «Leadership for Cyber Security in Public-Private Relations», in R. Koch, G. Rodosek (eds), Procedings of the 15th Conference on Cyber Warfare and Security, Munich, July, 2016. ISBN1910810932, 9781910810934.

Mari Malvenishv, «Role and Objectives of the Cybersecurity Bureau». Online Presentation by the Cybersecurity Bureau of Georgia, 2015. Available at: www./slideplayer.com/slide/9759466/

Sarma, Sanghamitra. «Cyber Security Mechanism in European Union.» (2016).

T4-B3 : Cybercriminalistique

Description

La cybercriminalistique est l'application de techniques d'investigation et d'analyse en vue de recueillir, d'exploiter et de conserver des preuves numériques. Ce domaine d'activité englobe la criminalistique appliquée aux objets numériques, aux équipements matériels et au facteur humain. Si une activité d'analyse est essentielle à la maintenance quotidienne des systèmes et à l'efficacité opérationnelle, un contrôle plus rigoureux peut être nécessaire pour fournir des éléments de preuve dans le cadre d'enquêtes criminelles. Enfin, les bonnes pratiques en matière de criminalistique offrent des outils extrêmement utiles pour comprendre comment les pirates tentent d'exploiter l'accès aux systèmes existants. Elles permettent par exemple de révéler comment ils entreprennent d'accéder à des systèmes de commande et de contrôle, ou comment ils conçoivent les malwares.

Ce bloc présente les principales difficultés associées à la criminalistique dans le cadre de la gestion des cyberincidents. Les techniques criminalistiques peuvent être appliquées à l'analyse des cyberincidents, à la collecte de renseignements et aux poursuites engagées par les autorités judiciaires. Les ressources abordées incluent les outils et techniques permettant d'obtenir des données de diverses sources, d'analyser les données et d'établir une chronologie des événements. Ceux-ci peuvent être utilisés pour monter un dossier d'attribution de la responsabilité ou pour diverses formes de tâches de suivi, de la surveillance et supervision des activités à l'élaboration d'un dossier pénal contre les auteurs. Les apprenants étudieront également la collecte et l'examen des données criminalistiques dans le cadre des affaires de criminalité financière, par exemple dans les cas de blanchiment d'argent.

Les apprenants découvriront les problèmes liés à la collecte de données criminalistiques provenant de sources multiples, telles que les ordinateurs, les réseaux, les dispositifs mobiles, les bases de données et les capteurs.

Acquis d'apprentissage

Les apprenants démontreront la compréhension des éléments suivants :

- problèmes liés à la collecte de données criminalistiques provenant de sources multiples, telles que les ordinateurs, les réseaux, les dispositifs mobiles, les bases de données et les capteurs ;
- importance de l'analyse des données criminalistiques pour la création d'une chronologie et l'attribution de la responsabilité ;
- lois et réglementations nationales en matière de collecte des données destinée à faciliter le travail des forces de l'ordre.

Thèmes de modules possibles et approches à envisager

- Création d'un système résilient favorisant la reprise sur cyberincident
- Examen criminalistique des éléments d'ingénierie sociale exploités pour accéder aux systèmes
- Dispositifs matériels susceptibles de présenter un intérêt criminalistique
- Utilisation des résultats d'investigation criminalistique dans le cadre des poursuites judiciaires
- Outils automatisés pour la criminalistique opérationnelle de base

Méthode d'apprentissage et évaluation

La méthode d'enseignement doit inclure des cours magistraux, des démonstrations et des discussions portant sur l'examen de plusieurs études de cas illustrant différents éléments criminalistiques.

Le type d'évaluation doit être adapté au niveau de connaissance défini spécifiquement pour les cours inspirés de ce programme de référence.

L'évaluation des apprenants doit reposer sur un examen oral et écrit.

Références

Santhosh Baboo and S. Mani Megalai, "Cyber Forensic Investigation and Exploration on Cloud Computing Environment," *Global Journal of Computer Science and Technology B: Cloud and Distributed* 15 (Issue 1, Version 1), 2015. https://globaljournals.org/GJCST_Volume15/1-Cyber-Forensic-Investigation.pdf

Ibrahim Baggili and Frank Breitinger, University of New Haven Cyber Forensics Research and Education Lab, "Data Sources for Advancing Cyber Forensics: What the Social World Has to Offer," *Papers from the 2015 AAAI Spring Symposium* (Palo Alto, CA Stanford University), March 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

Risto Vaarandi, Paweł Niziński, NATO Cooperative, Cyber Defence Centre of Excellence, Tallinn, Estonia. 2013 «A Comparative Analysis of Open-Source Log Management Solutions for Security Monitoring and Network Forensics». Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/VaarandiNizinski2013_OpenSourceLogManagementSolutions.pdf

Xiuzhen Cheng, Miroslaw Kutyłowski, Kuai Xu, Haojin Zhu, «Special Issue on Cybersecurity, Crime, and Forensics of Wireless Networks and Applications.» Security and Communications Networks. Vol.8, Issue 17. 2015. Journal ISSN:1939-0122.

Å uteva, NataÅ¡a, Mileva Aleksandra; Loleski Mario, «Finding Forensic Evidence for Several Web Attacks», International Journal of Internet Technology and Secured Transactions, Vol6., No.1, 2015. Journal ISSN: 1748-5703.

Akinola Ajijola, Pavol Zavarsky, Ron Ruhl, «A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012». Paper presented at the 'World Congress on Internet Security (WorldCon)' 2014. pp66-73. 10.1109/WorldCIS.2014.7028169. Available from the IEEE at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=7028169&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7028169

Choi, Yangseo, Joo-Young Lee, Sunoh Choi, Jong-Hyun Kim, and Ikkyun Kim. «Introduction to a network forensics system for cyber incidents analysis.» In 2016 18th International Conference on Advanced Communication Technology (ICACT), pp. 50-55. IEEE, 2016.

T4-B4 : Audit et évaluation de la sécurité au niveau national

Description

L'évaluation du niveau de préparation national en matière de sécurité constitue une étape critique. Cette évaluation permet de mettre à l'épreuve les contrôles de sécurité et d'identifier les lacunes éventuelles dans l'infrastructure et la politique de sécurité. L'évaluation de la sécurité peut se faire à plusieurs niveaux. Tout d'abord, les contrôles de sécurité individuels peuvent être testés à l'aide d'outils d'audit. Ensuite, l'évaluation peut être réalisée au niveau global, organisationnel ou des systèmes par le biais d'exercices et de simulations en temps réel. Ce bloc présente les outils et procédures utilisés dans le cadre des audits et évaluations de la sécurité. Les apprenants découvriront ainsi comment l'évaluation permet d'identifier et de mesurer les vulnérabilités résiduelles des systèmes. Par ailleurs, ces audits et évaluations permettent de déterminer comment estimer la capacité des cybersystèmes à faire face à des types spécifiques d'agents de menace connus, et comment se préparer à l'émergence d'une menace inconnue (appelées menaces « jour zéro » parce qu'il n'existe aucune indication de leur mode d'attaque ou action malveillante spécifique).

Les outils et techniques de sensibilisation personnelle et organisationnelle à la cybersécurité sont nombreux et prennent des formes aussi diverses que des questionnaires ou des outils techniques. L'objectif de ce bloc est de permettre aux apprenants de prendre conscience de l'importance de la sensibilisation des individus et des organisations dans le contexte de la cybersécurité. Il est essentiel d'analyser les atouts et les faiblesses des différents outils et approches pour comprendre leur valeur. L'autoévaluation continue permet de réduire les risques. Pour garantir la pertinence d'une autoévaluation, il est également indispensable de prendre en compte les éventuels préjugés potentiels. L'opérationnalisation des résultats est un élément nécessaire de toute autoévaluation. Dans la mesure où le niveau de sécurité est lié à la valeur, à l'importance ou au caractère sensible de l'élément sécurisé, il n'existe pas de modèle unique pouvant simplement être adopté et appliqué. En réalité, le niveau de cybersécurité souhaité dépendra des normes adoptées et du niveau de performances requis.

Acquis d'apprentissage

Les apprenants auront acquis les compétences suivantes :

- comprendre l'importance des outils d'audit et d'évaluation de la sécurité ;
- évaluer et appliquer des outils et techniques d'autoévaluation appropriés dans le contexte national.

Thèmes de modules possibles et approches à envisager

Autres thèmes possibles :

- Bonnes pratiques dans les organisations qui ont recours à l'autoévaluation
- Examen d'études de cas où la sensibilisation aurait pu améliorer la sécurité

Méthode d'apprentissage et évaluation

Les apprenants doivent s'entraîner à utiliser un outil d'autoévaluation national, s'il en existe. Dans le cas contraire, ils peuvent utiliser l'outil CSET (*Cyber Security Evaluation Tool*) disponible via le ministère américain de la Sécurité nationale, ou une approche similaire. Il peut être utile de comparer les approches nationales éventuelles à celle recommandée par le ministère américain de la Sécurité nationale.

Le type d'évaluation doit être adapté au niveau de connaissance défini spécifiquement pour les cours inspirés de ce programme de référence.

Références

Business Continuity Institute, *The Good Practice Guidelines 2013, Global Edition: A Guide to Global Good Practice in Business Continuity* (England), 2013. www.thebci.org/index.php/resources/the-good-practice-guidelines

International Auditing and Assurance Standards Board, ISAE 3402 Standard for Reporting on Controls at Service Organizations. http://isae3402.com/ISAE3402_overview.html

International Organization for Standardization/International Electrotechnical Commission, *ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*, CCMB-2012-09-001, September 2012. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

Keith Stouffer, Joe Falco and Karen Scarfone, *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, U.S. Department of Commerce, June 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Self Assessment Package*, Carnegie Mellon University, February 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf

U.S. Department of Homeland Security, *Cyber Resilience Review (CRR): Question Set with Guidance*, Carnegie Mellon University, February 2014. https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

Ivan Alcoforado, «Leveraging Industry Standards to Address Industrial Cybersecurity Risk», ISACA Journal, Vol 6, 2014; Journal ISSN: 1944-1967.

Stefan Laube, Rainer Böhme (Department of Information Systems, University of Munster, Germany; Institute of Computer Science, University of Innsbruck, Austria), «The Economics of Mandatory Security Breach Reporting to Authorities». Available at: http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_laube.pdf

Yulia Cherdantseva, et al. «A Review of Cyber Security Risk Assessment Methods for SCADA systems.» Electronic monograph. Available at the British Library, reference: UIN: ETOCvdc_100030733535.0x000001.

Abhijit Gupta, Subarna Shakya, «Information System Audit; A study for security and Challenges in Nepal», in, International Journal of Computer Science and Information Security, Vol.13, No. 11 (Nov 2015) pp 1-4. Journal ISSN 1947-5500.

Karabacak, Bilge, Sevgi Ozkan Yildirim, and Nazife Baykal. «Regulatory approaches for cyber security of critical infrastructures: The case of Turkey.» Computer Law & Security Review 32, no. 3 (2016): 526-539.

Abréviations

APT	Advanced Persistent Threat (menace persistante avancée)
AS	Autonomous System (système autonome) [subdivision discrète d'internet]
ASN	Autonomous System Number (numéro de système autonome)
BGP	Border Gateway Protocol
BSA	Basic Security Architecture (architecture de sécurité de base)
BYOD	Bring Your Own Device (utilisation des dispositifs personnels sur le lieu de travail)
CERT	Cyber Emergency Response Team (centre de réponse aux incidents de sécurité informatique)
COBIT	Control Objectives for Information and Related Technology (Objectifs de contrôle dans les domaines de l'information et des technologies associées)
COMSEC	Communications Security (sécurité des communications)
CSET	Cyber Security Evaluation Tool (outil d'évaluation de la cybersécurité)
DDoS	Distributed Denial of Service (déni de service distribué)
DHS	Department of Homeland Security (ministère américain de la Sécurité nationale)
DNS	Domain Name System (système de noms de domaine)
DoS	Denial of Service (déni de service)
ENISA	European Agency for Network and Information Security (Agence européenne chargée de la sécurité des réseaux et de l'information)
ESCWG	Emerging Security Challenges Working Group (Groupe de travail sur les difficultés émergentes en matière de sécurité)
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority (Autorité d'attribution des numéros sur Internet)
ICANN	Internet Corporation for Assigned Names and Numbers (Société pour l'attribution des noms de domaine et des numéros sur Internet)
ICS	Industrial Control System (système de contrôle industriel)
TIC	technologies de l'information et de la communication
IDS	Intrusion Detection System (système de détection des intrusions)
IGF	Internet Governance Forum (Forum sur la gouvernance de l'internet)
IP	Internet Protocol
SSI	sécurité des systèmes d'informations
ISACA	Information Systems Audit and Control Association (Association des professionnels de la vérification et du contrôle des systèmes d'information)
ISO	International Organization for Standardization (Organisation internationale de normalisation)
FAI	fournisseur d'accès Internet
TI	technologies de l'information
UIT	Union internationale des télécommunications
LAN	Local Area Network (réseau local)
NIR	National Internet Registry (registre Internet national)
NIST	National Institute of Standards and Technology (Institut national américain des normes et technologies)
PfPC	Partnership for Peace Consortium (Partenariat pour la paix)

PIT (system)	Platform IT system (système informatique basé sur une plateforme)
RACI	Responsibility, Accountability, Command and Information (responsabilité, approbation, consultation et information)
SCADA	Supervisory Control and Data Acquisition (système de contrôle et d'acquisition de données)
SCRM	Supply Chain Risk Management (gestion des risques de la chaîne d'approvisionnement)
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management (supervision des événements et des informations de sécurité)
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TRA (model)	Threat and Risk Assessment model (modèle d'évaluation de la menace et du risque)
UNIDIR	United Nations Institute for Disarmament Research (Institut des Nations unies pour la recherche sur le désarmement)

Glossaire

Note : Tous les termes ci-dessous n'apparaissent pas dans le texte précédent, mais un grand nombre d'entre eux seront utiles pour l'élaboration d'exercices spécifiques.

A

accès non autorisé
Accès qui enfreint la politique de sécurité officielle.

agent de menace
Individu, groupe, organisation ou gouvernement menant ou ayant l'intention de mener des activités préjudiciables.

analyse du risque
Examen systématique des composantes et caractéristiques du risque.

analyse de la défense des réseaux informatiques
Utilisation de mesures défensives et d'informations provenant de sources diverses en vue d'identifier, d'analyser et de signaler les événements qui surviennent ou pourraient survenir à l'intérieur du réseau, afin de protéger les informations, les systèmes d'information et les réseaux contre les menaces.

attaque
Tentative d'accès non autorisé aux services, ressources ou informations d'un ou de plusieurs systèmes, ou tentative de compromission de l'intégrité d'un ou de plusieurs systèmes.

attaque active
Attaque perpétrée intentionnellement par un agent de menace qui tente d'altérer un système, ses ressources, ses données ou ses opérations.

attaque passive
Attaque perpétrée intentionnellement par un agent de menace qui tente d'obtenir ou d'utiliser des informations provenant d'un système mais ne tente pas d'altérer le système, ses ressources, ses données ou ses opérations.

authentification
Processus de vérification de l'identité ou d'autres attributs d'une entité (utilisateur, processus ou dispositif). Définition élargie : Correspond également au processus de vérification de la source et de l'intégrité des données.

B

botnet (réseau de robots)
Ensemble d'ordinateurs compromis par du code malveillant et contrôlés en réseau.

Build Security In
Ensemble de principes, pratiques et outils utilisés pour concevoir, développer et faire évoluer les systèmes d'information et les logiciels qui améliorent la résistance aux vulnérabilités, aux failles de sécurité et aux attaques.

C

capacité
Moyen d'accomplir une mission, une fonction ou un objectif.

chaîne d'approvisionnement
Système regroupant les organisations, les personnes, les activités, les informations et les ressources nécessaires à la création et au transfert de produits, y compris des composants de produit et/ou des services, depuis les fournisseurs jusqu'à leurs clients.

cheval de Troie
Programme informatique semblant avoir une fonction utile, mais possédant également une fonction dissimulée potentiellement malveillante capable de contourner les mécanismes de sécurité, parfois en exploitant les autorisations légitimes d'une entité système qui invoque le programme.

cybercriminalistique
Processus et techniques spécialisées permettant la collecte, la conservation et l'analyse des données système (preuves numériques) à des fins d'investigation.

cryptographie
Utilisation de techniques mathématiques pour fournir des services de sécurité, telles que la confidentialité, l'intégrité des données, l'authentification des entités et l'authentification de l'origine des données.

cyberécosystème
Infrastructure d'informations interconnectée gérant les interactions entre personnes, processus, données et technologies d'information et de communication ; ainsi que l'environnement et les conditions qui influencent ces interactions.

cybersécurité :
Définition succincte : Activité ou processus, capacité ou état par lequel les systèmes d'information et de communication, ainsi que les informations qu'ils contiennent, sont protégés contre les dommages et les utilisations, les modifications et l'exploitation non autorisées.

Définition élargie : Ensemble des stratégies, politiques et normes relatives à la sécurité du cyberespace et aux opérations qui y sont exécutées, englobant tout l'éventail des politiques et activités de neutralisation des menaces, de réduction des vulnérabilités, de dissuasion, de coopération internationale, de réponse aux incidents, de résilience et de reprise sur incident, y compris les opérations de réseaux informatiques et

les missions liées à la qualité de l'information, l'application des lois, la diplomatie, l'armée et le renseignement afférentes à la sécurité et la stabilité de l'infrastructure mondiale d'information et de communication. Adapté de : CNSSI 4009, NIST SP 800-53 Rév. 4, NIPP, DHS National Preparedness Goal ; White House Cyberspace Policy Review, Mai 2009.

cyberspace
Univers électronique créé par des réseaux interconnectés de technologies de l'information et les informations qui y résident ou y transitent.

D

déni de service (DoS)
Attaque empêchant ou entravant l'utilisation autorisée des ressources ou services du système d'information.

déni de service distribué (DDoS)
Technique de déni de service exploitant un grand nombre de systèmes qui exécutent l'attaque simultanément.

détection des intrusions
Processus et méthodes permettant d'analyser les informations provenant des réseaux et systèmes d'information en vue de déterminer si une compromission ou une violation de sécurité est survenue.

E

enregistreur de frappes
Logiciel ou matériel qui enregistre les frappes au clavier et les événements de clavier, généralement à l'insu de l'utilisateur, afin de surveiller les actions de l'utilisateur d'un système d'information.

environnement cloud
Modèle permettant un accès réseau à la demande à un pool partagé de capacités ou ressources informatiques configurables (p. ex. réseaux, serveurs, dispositifs de stockage, applications et services). Celles-ci peuvent facilement être provisionnées ou mises hors service avec une intervention minimale de l'équipe informatique ou du fournisseur de services.

évaluation de la menace
Produit ou processus d'identification ou d'évaluation des entités, actions ou événements d'origine naturelle ou humaine ayant ou manifestant la capacité potentielle de porter atteinte à la vie, aux informations, aux opérations et/ou aux biens matériels.

évaluation des risques
Produit ou processus qui collecte des informations et attribue des valeurs aux risques en vue de guider l'établissement des priorités, de permettre l'élaboration ou la comparaison de plans d'action et d'éclairer la prise de décisions. Définition élargie : Estimation des risques auxquels sont exposés une entité, un actif, un système ou réseau, des opérations organisationnelles, des individus, une région géographique, d'autres organisations ou la société ; inclut la détermination de la mesure dans laquelle des circonstances ou événements défavorables pourraient entraîner des conséquences néfastes.

exploit
Technique permettant de porter atteinte à la sécurité d'un réseau ou d'un système d'information dans le cadre d'une infraction à la politique de sécurité.

exploit « jour zéro »
Attaque exploitant une vulnérabilité non reconnue, lancée sans avertissement et uniquement détectée en cours d'exécution.

exploration des données
Processus ou techniques utilisés pour analyser de vastes ensembles d'informations existantes en vue de découvrir des constantes ou des corrélations précédemment non identifiées.

G

gestion des droits numériques
Forme de technologie de contrôle d'accès permettant de protéger et de gérer l'utilisation des contenus ou dispositifs numériques conformément aux intentions du fournisseur du contenu ou du dispositif.

gestion des risques
Processus d'identification, d'analyse, d'évaluation et de communication des risques ; acceptation, évitement, transfert ou contrôle des risques pour atteindre un niveau acceptable, compte tenu des coûts et bénéfices associés aux mesures prises.

Définition élargie : Comprend (1) la réalisation d'une évaluation des risques ; (2) l'implémentation de stratégies visant à réduire les risques ; (3) la surveillance continue des risques au fil du temps ; et (4) la documentation du programme de gestion des risques global.

gestion des risques de la chaîne d'approvisionnement
Procédure d'identification, d'analyse et d'évaluation des risques relatifs à la chaîne d'approvisionnement ; acceptation, évitement, transfert ou contrôle des risques pour atteindre un niveau acceptable, compte tenu des coûts et bénéfices associés aux mesures prises.

gestion des risques d'entreprise
Approche globale impliquant le personnel, les processus et les systèmes de tous les niveaux d'une organisation dans le but de favoriser la prise de décisions judicieuses permettant à l'organisation d'atteindre ses objectifs en matière de gestion des risques.

gestion intégrée des risques
Approche structurée permettant à une entreprise ou à une organisation de partager les informations sur les risques et l'analyse du risque, et de synchroniser des stratégies de gestion des risques indépendantes mais complémentaires afin d'unifier les efforts déployés au sein de l'entreprise.

I

infrastructure critique
Systèmes et actifs physiques ou virtuels qui jouent un rôle tellement crucial pour la société que leur indisponibilité ou destruction est susceptible d'avoir un impact délétère sur la sécurité, l'économie, la santé ou la sécurité publique, l'environnement ou toute combinaison de ces domaines.

intrusion
Action non autorisée consistant à contourner les mécanismes de sécurité d'un réseau ou d'un système d'information.

L

logiciel antivirus
Programme assurant la surveillance d'un ordinateur ou réseau en vue de détecter ou d'identifier les principaux types de code malveillant, et de prévenir ou d'endiguer les incidents causés par un malware, parfois en supprimant ou en neutralisant le code malveillant.

M

mécanisme de contrôle d'accès
Mesures de sécurité conçues pour identifier et refuser les accès non autorisés, et permettre les accès autorisés à un système d'information ou à un site physique.

menace
Circonstance ou événement ayant ou manifestant la capacité potentielle d'exploiter des vulnérabilités et de porter atteinte aux opérations organisationnelles, aux actifs organisationnels (y compris les informations et les systèmes d'information), aux individus, à d'autres organisations ou à la société.

menace APT (menace persistante avancée)
Menace présentant un niveau de complexité technique élevé et disposant de ressources importantes qui optimisent sa capacité d'atteindre ses objectifs par le biais de plusieurs vecteurs d'attaque (p. ex. cyberattaque, attaque physique, leurre). Source : NIST SP 800-53 Rév. 4.

menace pour la chaîne d'approvisionnement des systèmes TIC
Menace d'origine humaine, exécutée par l'exploitation de la chaîne d'approvisionnement d'un système TIC, notamment des processus d'acquisition.

menace interne
Personne ou groupe de personnes au sein d'une organisation posant un risque potentiel par des actions enfreignant la politique de sécurité.

Définition élargie : Un ou plusieurs individus disposant de connaissances internes ou d'un accès à une entreprise ou une organisation susceptibles de leur permettre d'exploiter les vulnérabilités de la sécurité ainsi que des systèmes, services, produits ou installations de cette entité, avec l'intention de nuire.

modèle d'attaque
Ensemble de cyberévénements ou comportements similaires pouvant indiquer qu'une attaque est survenue ou est en cours, entraînant une violation de sécurité réelle ou potentielle.

N

non-répudiation
Propriété obtenue grâce à des méthodes cryptographiques offrant une protection contre la dénégation frauduleuse par un individu ou une entité d'une action particulière liée aux données.

Définition élargie : Fonctionnalité offrant la capacité de déterminer si un individu donné a exécuté une action particulière, telle que la création d'informations, l'envoi d'un message, l'approbation d'informations ou la réception d'un message.

P

pare-feu
Fonctionnalité permettant de limiter le trafic réseau entre des réseaux et/ou systèmes d'information.

pirate
Utilisateur non autorisé qui tente d'accéder ou accède à un système d'information.

phishing
Forme numérique d'ingénierie sociale visant à inciter des individus à fournir des informations sensibles par des moyens frauduleux.

R

redondance
Caractéristique de systèmes, sous-systèmes, actifs ou processus supplémentaires ou alternatifs maintenant un certain degré de fonctionnalité globale en cas de perte ou de défaillance d'un autre système, sous-système, actif ou processus.

résilience
Capacité à s'adapter à l'évolution des conditions et à se préparer à une défaillance, y résister et se rétablir rapidement une fois l'incident terminé.

résilience du réseau
Capacité d'un réseau à (1) assurer un fonctionnement continu (réseau extrêmement résistant aux défaillances et capable de fonctionner dans un mode dégradé s'il est endommagé) ; (2) se rétablir efficacement en cas de panne ; et (3) évoluer pour répondre à une augmentation ou une diminution rapide ou imprévisible des demandes.

S

signature d'attaque
Éléments caractéristiques ou distinctifs pouvant être recherchés ou utilisés pour établir des similitudes avec des attaques identifiées précédemment.

spam
Utilisation abusive des systèmes de messagerie électronique en vue d'envoyer en masse du courrier non sollicité.

spoofing
Contrefaçon de l'adresse d'expédition d'une transmission en vue d'obtenir un accès illégal (non autorisé) à un système sécurisé.

spyware
Logiciel installé secrètement ou subrepticement sur un système d'information, à l'insu de l'utilisateur ou du propriétaire du système.

(SCADA) Supervisory Control and Data Acquisition
Definition: Nom générique d'un système informatisé capable de recueillir et de traiter les données, et d'appliquer des contrôles opérationnels à des actifs géographiquement dispersés sur de longues distances.

surface d'attaque
Ensemble des moyens pouvant être exploités par un cyberpirate pour pénétrer dans un système et causer des dommages. Définition élargie : Caractéristiques d'un système d'information permettant à un cyberpirate de sonder ou d'attaquer un système d'information, ou d'y maintenir sa présence. Adapté de : Manadhata, P.K., & Wing, J.M. in Attack Surface Measurement, http://www.cs.cmu.edu/~pratyus/as.html#introduction.

V

vecteur de menace
Moyen d'introduire une menace dans une cible ou approche adoptée pour concrétiser une menace.

ver
Programme autonome capable de se répliquer et de se propager automatiquement, qui utilise des mécanismes propres aux réseaux pour se diffuser.

virus
Programme informatique capable de se répliquer, d'infecter un ordinateur sans permission de l'utilisateur ou son insu, puis de se propager à un autre ordinateur.

vulnérabilité
Faiblesse caractéristique ou spécifique qui rend une organisation ou un actif (tel que des informations ou un système d'information) vulnérable à son exploitation par une menace donnée ou à un danger donné.

Rédigé à partir du glossaire de la National Initiative for Cybersecurity Careers and Studies (NICCS) du ministère américain de la Sécurité nationale. Sources documentaires supplémentaires.

Chefs de groupe et coordinateurs de publication : Sean S. Costigan et Michael A. Hennessy
Membre de l'équipe du programme et conseillers :

Nom	Nationalité	Affiliation institutionnelle	
Dr. Ata ATALAY	Turquie	Chef de département Secrétariat général, Conseil national de sécurité	
Mme. Mariia AVDEEVA	Ukraine	Directrice du développement international Université nationale des sciences juridiques de Kharkov	
Mme. Alexandra BIELSKA	Pologne	Consultante i-intelligence	
M. Guiseppi CONTI	Italie	Directeur de la technologie (CTO) Trilogis	
M. Sean S. COSTIGAN	États-Unis	Directeur Windrose Research LLC	
M. Jean d'ANDURAIN	France	Coordinator, Coordinateur, Programmes de formation de défense OTAN	
LTC Dirk DUBOIS	Belgique	Collège européen de sécurité et de défense	
Dr. David EMELIFEONWU	Canada	Officier supérieur, Engagement dans l'éducation, Formation du personnel militaire Ministère de la Défense nationale	
M. David FRANCO	États-Unis	Agent spécial de surveillance Bureau d'enquête fédéral (FBI)	

Dr. Piotr GAWLICZEK	Pologne	Représentant du rectorat à l'innovation Université de la Défense nationale	
Dr. Sanjay GOEL	États-Unis	Directeur de la recherche, NYS Center for Information Forensics and Assurance SUNY Albany	
M. Andria GOTSIRIDZE	Géorgie	Directeur du bureau de cybersécurité Ministère de la Défense	
M. Arman GRIGORYAN	Arménie	Directeur du groupe de cybersécurité Institut d'études nationales stratégiques	
Dr. Michael A. HENNESSY	Canada	Professeur/Vice-principal adjoint, Recherche Collège militaire royal du Canada	
CDR Andreas HILDENBRAND	Allemagne	Professeur Centre européen d'études de sécurité George C. Marshall	
Dr. Dinos KERIGAN-KYROU	Irlande	Agent de formation, Département des sciences informatiques et mathématiques Université de Greenwich	
Dr. Scott KNIGHT	Canada	Professeur/Directeur du département d'ingénierie informatique et électrique Collège militaire royal du Canada	
M. Frederic LABARRE	Canada	Directeur de programme Groupement du Partenariat pour la paix (GPPP)	
M. Philip LARK	États-Unis	Directeur, Programme sur la cybersécurité Centre européen d'études de sécurité George C. Marshall	

Dr. Gustav LINDSTROM	Suède	Directeur de programme, Défis de sécurité émergents Centre de politique de sécurité de Genève	
Dr. Vakhtang MAISAIA	Géorgie	Professeur, Master en sécurité internationale Université du Caucase	
Dr. Petar MOLLOV	Bulgarie	Chargé de cours Centre de recherche avancée sur la défense	
M. Chris PALLARIS	Royaume-Uni	Directeur i-intelligence	
M. Daniel PEDER BAGGE	République tchèque	Expert en cybersécurité/politique NSA CZ	
M. Raphael PERL	États-Unis	Directeur Groupement du Partenariat pour la paix (GPPP)	
Mme. Maka PETRIASHVILI	Géorgie	Directrice des ressources humaines Ministère de la Défense	
Mme. Stela PETROVA	Bulgarie	Consultante European Leadership Network	
Dr. Benyamin POGHOSYAN	Arménie	Directeur adjoint Institut d'études nationales stratégiques	
M. Oleksandr POTIL	Ukraine	Professeur de sécurité informatique Université de la force aérienne de Kharkov	

Dr. Detlef PUHL	Allemagne	Haut conseiller Division des défis de sécurité émergents, OTAN	
M. Neil ROBINSON	Royaume-Uni	Directeur de recherche RAND Europe	
M. Gigi ROMAN	Roumanie	ADL École de l'OTAN	
LTC Ghenadie SAFONOV	Moldavie	Département des communications et de l'informatique Académie de défense de Moldavie	
M. Danylo SHEVCHENKO	Ukraine	Chef de projet Centre de recherche stratégique et d'innovation	
Mme. Natalia SPINU	Moldavie	Directrice Centre de cybersécurité, Chancellerie d'État	
Dr. Alan G. STOLBERG	États-Unis	Coordinateur, Éducation à la défense RAND	
Dr. Todor TAGAREV	Bulgarie	Professeur/Directeur Département de sécurité informatique & Centre de gestion de sécurité et de défense	
Dr. Ronald TAYLOR	États-Unis	Président Centre de leadership stratégique en environnements complexes	
M. Bodgan UDRISTE	Roumanie	Expert en sécurité des systèmes informatiques Mission de surveillance de l'Union européenne	
M. Joseph VANN	États-Unis	Professeur Centre européen d'études de sécurité George C. Marshall	

Équipe de rédaction et distribution

Rédacteurs :

Sean S. Costigan
Professeur
Centre européen d'études de sécurité George C. Marshall
Gernackerstrasse 2
82467 Garmisch-Partenkirchen, Allemagne
sean.costigan@pfp-consortium.org

Michael A. Hennessy, PhD
Professeur d'histoire et d'études de guerre
Vice-recteur associé – Recherche
Collège militaire royal du Canada
P.O. Box 17000 STN FORCES
K7K 7B4, Kingston (ON), Canada
hennessy-m@rmc.ca

Coordonnatrice présentation et distribution :
Gabriella Lurwig-Gendarme
Secrétariat international de l'OTAN
Division Affaires politiques et politique de sécurité
lurwig.gabriella@hq.nato.int

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