امنیت سایبری

نصاب تحصیلی

عمومی مرجع

امنیت سایبری

نصاب تحصیلی

عمومی مرجع

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.

دفاع ملی
دفتر قوماندان
گروه پرسونل نظامی
P.O.BOX 17000 Station Forces
Kingston, ON K7K7B4
4500-1 (SSO EE)
6 اکتوبر 2016
امنیت سایبری: نصاب تحصیلی عمومی مرجع

دفاع ملی
دفتر قوماندان
گروه پرسونل نظامی
CP 17000, Succursale Forces
Kingston, ON K7K7B4
4500-1 (OSEM PED)
6 اکتوبر 2016
امنیت سایبری: نصاب تحصیلی عمومی مرجع

اعضا و شرکای محترم ناتو،

مسرت داریم که سند حاضر تحت عنوان نصاب تحصیلی عمومی مرجع برای امنیت سایبری را با شما شریک می‌سازیم: این سند از طرف ناتو و کانسورسیوم مشارکت برای صلح آکادمی‌های دفاعی و انستیتوت‌های مطالعات امنیتی و توسط یک تیم چند ملیتی و متخصص تهیه شده است. هدف از این سند اینست که به ناتو و شرکای ناتو در زمینه تدوین اهداف جامع یادگیری و نصاب تحصیلی برای کورس‌های آکادمیک مرتبط با امنیت سایبری کمک نماید.

نصاب تحصیلی مرجع برای امنیت سایبری متشکل از چهار موضوع است: 1) فضای سایبری و مبانی امنیت سایبری، 2) حامل های خطر، 3) سازمان‌ها، پالیسی‌ها و استندردهای بین‌المللی امنیت سایبری و 4) مدیریت امنیت سایبری در بستر ملی. چهار موضوع متذکره با دقت انتخاب شده‌اند تا بتوانند طیف وسیعی از مسائل و موضوعات امنیت سایبری را شامل ساخته و مناسب‌ترین سطح تحصیلات را ارائه نمایند.

این سند بهترین منبع برای ناتو و آن دسته از شرکای ناتو می‌باشد که قصد انکشاف و درک بیشتر مسائل مختلف ملی و بین‌المللی (درگیر اقدامات امنیت سایبری) را دارند.

سند حاضر با این امید ارائه می گردد که بتواند در وقت مناسب توسط ناتو و از طریق کمیته‌های مربوطه مورد توجه قرار گیرد. قدم بعدی مورد نظر اینست که با ادارات تحصیلات دفاعی ملی در زمینه پذیرش و اجرای کامل این نصاب تحصیلی و یا بخش‌هایی از آن کار صورت گیرد. برای شرکای ناتو این روند در چارچوب پلان عمل مشارکت (IPAP) صورت می‌گیرد.

این سند تنها از طریق گفتگو و مبادله دیدگاه‌ها می‌تواند باعث تقویت رشد مسلکی و قابلیت همکاری بین کشورهای عضو و شرکای نظامی ناتو شود. من از اعضای هیأت‌ها دعوت می‌نمایم که این سند را به صورت گسترده در کشورهای مربوطه‌شان توزیع نمایند.

اگر راجع به این نصاب تحصیلی سؤالی دارید، از اعضای هیأت خود بخواهید که با آقای شان کاستیگان در مرکز اروپایی جورج سی. مارشال برای مطالعات امنیت به آدرس ایمیل sean.costigan@pfp-consortium.org و یا هم با داکتر مایکل هنسی، پروفسور تاریخ و مطالعات حرب در کالج سلطنتی نظامی کانادا به آدرس ایمیل hennessy-m@rmc.ca ارتباط برقرار کنند.

با بهترین آرزوها

[امضا شده توسط] تورن جنرال ترمبلی

(Major-General J.G.E. Tremblay)

NATO UNCLASSIFIED
Releasable to Montenegro

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

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

TO: See Distribution

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

DATE: 27 September 2016

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

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

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

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

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

for

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

Releasable to Montenegro
NATO UNCLASSIFIED

سازمان پیمان آتلانتیک شمالی
قوماندانی اعلی ناتو در امور تحول

7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

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

عنوانی: به لست توزیع مراجعه نمایید

موضوع: **تصویب نصاب تحصیلی مرجع امنیت سایبری گروه کاری چالش‌های امنیتی در حال ظهور کانسورسیوم مشارکت برای صلح به عنوان یک سند مرجع تحصیلاتی ناتو**

تاریخ: سپتامبر 2016

1. در تلاش برای تأمین نیازهای مشخص تحصیلی و تعلیمی، گروه کاری چالش‌های امنیتی در حال ظهور کانسورسیوم مشارکت برای صلح این نصاب تحصیلی مرجع را در زمینه امنیت سایبری تدوین نموده است. تلاش، مسلک‌گرایی و تعهد تمام کسانی که در انکشاف این نصاب تحصیلی سهیم بوده‌اند قابل قدرمی‌باشد.

2. اطمینان دارم که این نصاب تحصیلی با تحصیلات و تعلیمات ناتو در زمینه دفاع سایبری سازگار بوده و می‌تواند به عنوان یک سند مرجع در زمینه تدوین و انکشاف طرح کورس‌ها و برنامه‌های تحصیلات نظامی امنیت سایبری عمل نماید. این سند همچنین زمینه تقویت قابلیت همکاری نظامی بین ناتو و شرکای آن را فراهم کرده و همکاری جهت انکشاف یک سیستم تحصیلی و تعلیمی پاسخگو را تقویت می‌نماید.

3. با مسرت حمایت خود را از طریق انتشار این نصاب تحصیلی مرجع امنیت سایبری به عنوان یک سند ناتو، از گروه کاری چالش‌های امنیتی در حال ظهور کانسورسیوم مشارکت برای صلح اعلام می‌نمایم. تمام طراحان آموزشی مربوطه در کشورهای شریک که در زمینه انکشاف فرصت‌های یادگیری دخیل می‌باشند را تشویق می‌نمایم تا از این سند کمال استفاده را ببرند.

3. چنانچه سؤالی در رابطه با این سند وجود داشته باشد، لطفا با مسئول ارتباطی ما آقای صالح جم کومسال، بخش تحصیلی و تعلیمی دفاع سایبری ناتو به تلفون و یا آدرس ایمیل زیر ارتباط برقرار کنید.
تلفون: +1 (757) 477-3386, NCR 555-3386
آدرس ایمیل cem.kumsal@act.nato.int

از طرف قوماندان اعلی ناتو در امور تحول:

استفانو ویتو سالامیدا
تورن جنرال، قوای هوایی ایتالیا
معاون لوی درستیز و آموزگار قوای مشترک

درباره این نصاب تحصیلی مرجع

این سند نتیجه کار یک تیم چند ملیتی متشکل از افراد آکادمیک داوطلب و محققین از 14 کشور مرتبط با گروه کاری چالش‌های امنیتی در حال ظهور (ESCWG) کانسورسیوم مشارکت برای صلح (PfPC) می‌باشد. هدف ما تهیه رویکرد مناسب و قابل انعطاف و عموماً جامع برای مسئله امنیت سایبری بود.

هدف اینست که این سند به حیث یک مرجع به طور گسترده به بررسی امنیت سایبری بپردازد، اما در عمقی کافی که به متخصصین غیر فنی کمک کند تا تصویر کامل‌تری از موضوعات تکنالوژی داشته باشند و متخصصین تکنالوژی درک کامل‌تری از پیامدهای پالیسی‌های امنیتی و دفاعی ملی و بین المللی داشته باشند. ما تفکیک منطقی از عناوین را بر اساس حوزه‌های کاری مشخص ارائه می‌دهیم که سطح دانشی که توسط مخاطبین مختلف باید کسب شود را تعیین می‌کند و مراجع مفید کلیدی را نشان می‌دهد تا هر کشور پذیرنده بتواند این چارچوب را با نیازهای خود و محصلین مورد نظر وفق دهد.

ما مخصوصا از کانسورسیوم مشارکت برای صلح اکادمی‌های دفاعی و انستیتوت‌های مطالعات امنیتی تحت رهبری رافائل پرل و روسای گروه کاری چالش‌های امنیتی در حال ظهور، داکتر دتلف پل (NATO) و گوستاو لیندستروم (GCSP) و همچنین حمایت پروگرام ارتقاء تحصیلات دفاعی کانسورسیوم مشارکت برای صلح و گروه کاری تحصیلی تحت رهبری داکتر آل استول برگ، داکتر جین دی اندورین و داکتر دیوید ایملیفیونو سپاسگذاری می‌کنیم. علاوه بر این، رهبری کشورهای مختلف پارتنر از جمله ارمنستان، گرجستان و مولدوا از طریق حمایت مستقیم و ملموس خود به امکان عملی شدن این تلاش کمک کردند. در آخر از همه داوطلبانی که بحیث اشتراک کننده معرفی شده‌اند مراتب قدردانی خود را اعلام می‌کنیم. وقتی از آنها درخواست کردیم که آیا مایلند به یک تلاش دو ساله متعهد شوند که آنها را به عمق تحصیلات امنیت سایبری بکشاند، همه پذیرفتند. به ویژه می‌خواهیم از اسکات نایت، دینوس کریگان کایرو، فیلیپ لارک، کریس پالاریس، دنیل پدر باگی، جی جی رومن، ناتالیا اسپینو، تودور تاگارف، رونالد تیلور، و جوزف وان تشکر کنیم. بدون آنها، این سند به راحتی گردآوری نمی‌شد.

شان اس. کاستیگان و مایکل اِی. هنسی

I. هدف از این سند

سرعت سریع و بی وقفه تغییرات و چالش‌های امنیت سایبری نیروی محرکه‌ای بود که گروه کاری چالش‌های امنیتی در حال ظهور را تحریک به درخواست این نصاب تحصیلی نمود، مطابق با تاکید بیشتر ناتو روی بهبود آگاهی، آمادگی و تاب آوری امنیت سایبری.[1]

عناوین خبری مملو از اشاره به هک های تجارتی، نقص‌های وارده ناشی از حمله به دیتا (data)، تقلب الکترونیکی، اختلال در خدمات حکومتی و یا زیربناهای حیاتی، سرقت مالکیت‌های فکری، افشای اسرار امنیت ملی و تخریب سایبری است. عرصه‌هایی که زمانی به عنوان جنگ الکترونیکی یا جنگ معلوماتی تحت نظر متخصصین امنیت شبکه شناخته می‌شد، امروزه به عرصه گسترده‌تری تبدیل شده که از آن به عنوان "امنیت سایبری" یاد می‌شود.

ازآنجایی‌که امنیت سایبری یک مسئله در حال رشد است و هنوز هم روی اصطلاحات بنیادی آن اختلاف نظر وجود دارد، گروه کاری چالش‌های امنیتی در حال ظهور تلاش نموده تا با ایجاد این نصاب تحصیلی مرجع موجب قدری وضاحت و مشترکاتی بر این موضوع شود. در مورد املای "امنیت سایبری" به عنوان یک کلمه cybersecurity به توافق رسیدیم و اصطلاح "cyber" یا سایبری را به عنوان صفت در این نصاب تحصیلی مرجع به کار می‌بریم.

در تهیه این سند، نظریات و پیشنهادات تمام انستیتوت‌های عضو کانسورسیوم مشارکت برای صلح و کالج‌های دفاعی را خواستیم و پروگرام‌های تعلیمات نظامی کشورهای پارتنر ناتو و کانسورسیوم مشارکت برای صلح را بررسی نمودیم تا بدانیم چه تدریس می‌شود. ما در صدد تشخیص خلاءها و رویکردهای مشترکی بودیم که در مرزهای سنتی حکومتی و ساختارهای نظامی موجود است. عدم درک کافی از تکنالوژی امنیت سایبری و همچنین از شیوه‌های کاهش تهدید و خطر در بین رهبران امنیت ملی و پالیسی دفاعی بزرگترین خلائی بود که مشاهده نمودیم. یک خلاء مشابه نیز راجع به درک چارچوب‌های پالیسی ملی در میان متخصصین تخنیکی شناسایی شد.

این نصاب تحصیلی مرجع نقطه شروع منسجمی را فراهم می‌کند که انکشاف مسائل مربوط به تدریس امنیت سایبری به افسران ارشد، کارمندان ملکی و کارمندان سطح متوسط نظامی و ملکی از آن برخواسته است. مانند سایر نصاب‌های تحصیلی مرجع که توسط کانسورسیوم مشارکت برای صلح تهیه شده، هدف این سند محافظه کارانه است. این نصاب تحصیلی خطوط کلی یک کورس ماستری واحد را برای همه ارائه نمی‌دهد. از نظر محتوا، جزئیات یا رویکردها به موضوع کامل نیست. اما معتقدیم که یک رویکرد اکتشافی مفید در چندین حوزه ایجاد کرده، زیرا شامل یک مقدمه جامع راجع به مسائل بهم‌پیوسته اقدامات و شیوه‌های امنیت سایبری است. به نظر افرادی که پیشینه تخنیکی کمی دارند مقدمه در سطح پیچیدگی قابل مدیریت است و اینکه کجا و به چه دلیل عمق تخنیکی لازم است را بهتر درک خواهند کرد. به نظر افرادی که دارای پیشینه تخنیکی هستند می‌تواند این مطالب مروری مفید روی عرصه‌هایی باشد که با آن آشنایی دارند و مقدمه‌ای برای مسائل گسترده‌تری از پالیسی‌ها و روش‌های بین‌المللی، ملی و حقوقی فراهم کند. معتقدیم همه موضوعی ارزشمند در این سند خواهند یافت.

کسانی که مایل به استفاده از این سند هستند باید نیازها و روش‌های مشخص ملی خود را تجزیه و تحلیل کنند تا این سند را مطابق با نیازهای خود تعدیل کنند. این سند در تشخیص عرصه‌هایی که نیاز به توجه دارد یک رهنمود است و منابع و رویکردهای کلیدی را پیشنهاد می‌کند.

II. امنیت سایبری و خطرات

اقدامات امنیتی معمولا براساس میزان تهدیدات و خطرات اتخاذ می‌گردد. هر دو مفهوم به طور کاملتر مورد بررسی قرار می‌گیرد. با این حال، به زبان ساده فضای سایبری پر از تهدید است اما برای کاهش این تهدیدات، اقدامات باید بر اساس میزان خطرها اتخاذ گردد. سازمان بین المللی استندردسازی (ISO) خطر را به عنوان " اثرعدم اطمینان بر تامین اهداف" تعریف می‌کند (تاثیر می‌تواند انحراف مثبت یا منفی از نتایج مورد انتظار باشد). ازآنجایی‌که اقدامات امنیتی اتخاذ شده برای تامین امنیت چیزی باید متناسب با ارزش آن چیز باشد، سطوح امنیتی مختلفی وجود دارد که متناسب با میزان ارزش و خطر است. بنابراین، امنیت فضای سایبری برای کاهش خطرات و تهدیدات ضمن تشویق به دسترسی و باز بودن انواع مختلف شبکه‌ها و دستگاه‌های بهم پیوسته ملاحظات زیادی را در پی دارد. ایجاد تعادل لازم بین دسترسی، قابلیت استفاده و امنیت چالش اصلی است. این نصاب تحصیلی رویکردهای ارزیابی، تشخیص و کاهش تهدیدات و خطرات را از طریق کاوش عملکردهای خوب توصیه شده و مقایسه با پالیسی‌های منتشر شده کشورها و سازمان‌های خاص در سطوح تخنیکی و پالیسی‌های اداره و حکومت بررسی می‌کند.

III. ساختار این نصاب تحصیلی

همانطور که در اسناد نصاب‌های تحصیلی مرجع قبلی بیان شده، یک نصاب تحصیلی عبارت از یک پروگرام خاص یادگیری و یا شاید مجموعه کورس‌هایی باشد که به صورت جمعی مواد و روش‌های تدریس، یادگیری و ارزیابی برای یک رشته تحصیلی را تشریح می‌کند. بنابراین، این نصاب تحصیلی حاصله نشان‌دهنده نقشه راهی است که شاگردان می‌توانند با آن آشنا شوند. مانند هر نقشه، این نصاب تحصیلی حاوی نکات و زمینه‌های کلیدی است و ممکن است همه مسیرها یا جزئیات را نشان ندهد، اما آنچه که یادگیرنده باید بیاموزد را بیان می‌کند.

اساساً یک نصاب تحصیلی عمومی دارای یک ساختار بنیادی و گسترده می‌باشد که شامل عناوین فرعی و موضوعات زیادی در یک چارچوب گسترده است.[2] این بخش‌های بنیادی و گسترده با اهداف گسترده یک رشته تحصیلی مرتبط هستند. با توجه به ارتباط موضوعات و مسائل موجود در نصاب تحصیلی مرجع، توصیه نشده است که این نصاب تحصیلی به سه مرحله انکشافی افسران تقسیم شود. در این مورد وقتی به نحوه استفاده از این نصاب تحصیلی بپردازیم بیشتر صحبت خواهیم کرد.

1 برای وضاحت در مورد مفهوم امنیت سایبری، به تعریف وزارت امنیت داخلی ایالات متحده اتکاء نمودیم. "امنیت سایبری عبارت از فعالیت یا پروسه، توانایی یا وضعیتی می‌باشد که در آن از سیستم‌های معلوماتی و مخابراتی و همچنین معلومات موجود در آن در برابر آسیب، استفاده غیر مجاز، تغییر یا بهره‌جویی محافظت می‌شود".

مطابق با ساختارهای پذیرفته‌شده در سایر نصاب‌های تحصیلی کانسورسیوم مشارکت برای صلح، این سند با چهار موضوع ارائه شده است، هر موضوع به بخش‌های جداگانه تقسیم شده که به طور طبیعی می‌تواند بیشتر تقسیم شود. این تقسیمات موضوعات (T) و بخش‌ها (B) را تعیین می‌کند، همانطور که در فهرست مطالب منعکس شده است (بررسی کنید).

چهار موضوع این نصاب تحصیلی:

موضوع 1: فضای سایبری و مبانی امنیت سایبری

موضوع 2: حامل های خطر

موضوع 3: سازمان‌ها، پالیسی‌ها و استندردهای بین‌المللی امنیت سایبری

موضوع 4: مدیریت امنیت سایبری در بستر ملی

هر موضوع در یک جایی از این سند به طور مفصل تشریح شده است، اما هر یک از موضوعات دارای عرصه‌ها و مسائل گسترده مشخص می‌باشد که باید به آن رسیدگی شود.

در چارچوب هر موضوع چندین عنوان متفاوت دسته‌بندی شده است. هر عنوان در یک بخش اساسی مورد بررسی قرار می‌گیرد که ممکن است خودش به قسمت‌های یادگیری متفاوت تقسیم شده باشد، مانند لکچرها، پرزنتیشن‌ها، نمایشات، سفرها، تمرینات سناریویی و فعالیت‌های مشابه. معمولا چون این نصاب تحصیلی مرجع محتاج سازگاری محلی است و این سطح از جزئیات به نیاز فردی بستگی دارد، قسمت‌ها و لکچرهای متفاوتی پیشنهاد نکرده‌ایم. بخش‌های مختلف به صورت دسته جمعی به هر موضوع معنی و محتوا می‌بخشد. پیشنهاد شده تا اهداف و نتایج یادگیری محقق شود؛ اینها به نوبه خود به اهداف گسترده‌تری از موضوعات مرتبط هستند.

بخش‌ها می‌تواند بصورت مجموعی، ترکیبی یا قسمت‌های مجزای تقسیم‌بندی شده ارئه شود. این طرح چیزی در مورد اینکه کدام بخش با چه روشی بحث شود بیان نمی‌کند اما در هر بخش یا قسمت روش‌های تدریس می‌تواند شامل لکچرها، پرزنتیشن‌ها، تمرینات مشارکتی، سفرها، نمایشات یا سهمگیری در تمرینات سناریویی باشد.

IV. استفاده از این نصاب تحصیلی

این نصاب تحصیلی بر چندین فرض تلویحی استوار است.

اول اینکه مواد مشخص شده در این سند طبقه‌بندی نشده است. کسانی که این چارچوب را قبول می‌کنند ممکن است در صورت نیاز مایل به دسترسی به مواد طبقه‌بندی‌شده باشند.

ثانیاً، احتمالاً موسساتی که این نصاب تحصیلی مرجع را قبول می‌کنند، زمان و منابع مناسبی را به همراه یک تیم متخصص جهت تشخیص طرزالعمل‌ها و پالیسی‌های ملی در سطح جزئیات مورد نیاز برای مخاطبین اختصاص خواهند داد. ممکن است به دانش حفظی بر اساس تکرار موضوعات تخنیکی گذرا نیاز باشد اما هدف در اینجا رسیدن به درک گسترده‌تری از چالش‌های امنیت سایبری در طیف وسیعی از مسائل است.

در تطبیق این نصاب تحصیلی برای استفاده محلی، می‌توان آن را به شکل تدریجی و متوالی در مراحل مختلف شغلی اجرا نمود، اما باید خطوط کلی را در همه سطوح دنبال نمود. با این حال، هدف گسترده این نصاب تحصیلی مرجع بیشتر عملیاتی-استراتژیک است تا تاکتیکی. برای تدوین کورس‌های خاص از این نصاب تحصیلی مرجع، پیشنهاد می‌شود که طراحان کورس محلی زمان و منابع موجود، سطح تحصیلی شاگردان و فعالیت‌هایی که انتظار می‌رود آنها انجام دهند یا انجام خواهند داد را بدون توجه به رتبه آنها در نظر داشته باشند.

سوم اینکه هیچ بخشی برای جنگ سایبری، منازعه سایبری یا رسانه‌های اجتماعی به عنوان مجرای تبلیغات یا معلومات نادرست در این نصاب تحصیلی مرجع وجود ندارد. کمیته طراحی تصمیم گرفت که به این مسائل متمرکز در نصاب‌های تحصیلی بعدی بپردازد.

در آخر، مجدداً تاکید می‌کنیم که این نصاب تحصیلی مرجع یک ساختار درسی واحد یا کورس پیشنهادی نیست. بلکه به عنوان یک مرجع کلیدی که خطوط کلی، مسائل و موضوعات مربوط به امنیت سایبری را ارائه می‌دهد به بهترین شکل مورد استفاده قرار می‌گیرد. این سند می‌تواند به عنوان رهنمودی برای پرسنل متخصص مورد استفاده قرار گیرد تا ببینند که تمرکز مشخص آنها در کجای این طیف وسیع قرار دارد. همچنین این سند می‌تواند تدوین‌گران ارشد پالیسی امنیت ملی را با کورس‌های مقدماتی آشنا کند تا آنها بتوانند پالیسی‌های امنیتی را با آگاهی از بستر تخنیکی بهتر درک کنند. زمانی که هر کورس واحد از این طرح اقتباس گردد، سه عنصر که بیشترین نگرانی هدف یا مقصد این کورس می‌باشد عبارتند از: شاگردان پیشنهادی، به ویژه سطح دانش تخنیکی، ماهیت اشتغال آنها و زمان موجود. این سه عنصر باید رهنمودی برای سطح جزئیات تخنیکی مورد بحث و ماهیت تمرینات یادگیری باشد (لکچرها، مثال‌ها، سفرهای ساحوی، نمایشات، بازی‌های حربی و غیره).

2 برای ریشه و کاربرد این ساختار به اسناد نصاب تحصیلی قبلی مراجعه کنید.

۷ . منابع دیگر

حجم مطالب عمومی و تخنیکی راجع به امنیت سایبری به سرعت در حال رشد است. طراحان کورس را تشویق می‌کنیم تا لیست منابع کلیدی خود را تهیه و منتشر کنند. منابع مختلفی که منعکس‌کننده دیدگاه‌های متعدد ملی و بین‌المللی مرتبط با موضوعات تعریف‌شده برای این نصاب تحصیلی عمومی مرجع باشد را شامل ساختیم. همچنین در صورت دسترسی به اینترنت، لینک‌هایی را به منابع اینترنتی ایجاد کردیم. علاوه بر بسیاری از منابع ذکر شده در این سند، وب سایت ناتو مقالات و معلومات زیادی را در مورد مسائل مورد علاقه جامعه ناتو ارائه می‌دهد. منابع ذکر شده در سایت www.natolibguides.info/cybersecurity شامل موارد زیر است:

- NATO Review's articles/videos on cyber attacks as well as the June 2013 edition on Cyber—the good, the bad and the bug-free (includes videos, photos, a timeline, infographics, etc.).
- The article NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow by Healey and van Bochoven (February 2012) provides a good overview of NATO's cyber capabilities.
- The report On Cyberwarfare (2012) by Fred Schreier includes a glossary and very good selected and thematic bibliographies (Official Documents, NATO, OECD, by country, Information Warfare, Cyber Security, Books).
- The Cyber Special Edition of *Strategic Studies Quarterly* 6, no. 3 (Fall 2012).
- The Cybersecurity: Shared Risks, Shared Responsibilities edition of *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012).
- The article Cyberspace Is Not a Warfighting Domain (2012) by Martin Libicki.
- *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (2012).

- The 300-page manual was written by a group of 20 researchers at the invitation of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.
- The follow-up "Tallinn 2.0" project to the *Tallinn Manual on the International Law Applicable to Cyber Warfare* is designed to expand the scope of the original *Tallinn Manual*. Tallinn 2.0 will result in the second edition of the *Tallinn Manual* and be published by Cambridge University Press in 2016 (source: NATO CCD COE).
- The National Cyber Security Framework Manual (2012) by the NATO CCD COE.
- The NATO CCD COE's e-learning course on Cyber Defence Awareness (which is available for free but registration is required).
- The Cyber Conflict Bibliography by the Jacob Burns Law Library, George Washington University Law School.
- The briefing Cyber defence in the EU: Preparing for cyber warfare? (31 October 2014) by the European Parliamentary Research Service.
- The Tallinn Paper no. 8, published in April 2015: "The Role of Offensive Cyber Operations in NATO's Collective Defence."

منابع مفید دیگر به شرح زیر است:

- 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 2014. See http://www.itu.int/ITU-D/study_groups or http://www.itu.int/pub/D-STG-SG01.22.1-2014

- 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.
- 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.

فهرست موضوعات

موضوع 1: فضای سایبری و مبانی امنیت سایبری

هدف

هدف این موضوع اینست که با تعریف مولفه‌های ساختاری فضای سایبری، معماری اساسی و همچنین مبانی امنیت سایبری، اساسات دانش را برای کلیه دستوالعمل‌ها ایجاد کند.[3] شناسایی و مدیریت خطر اصلی‌ترین چالش مشترکی است که موضوعات و مطالب مختلفی را به هم پیوند می‌دهد و در این نصاب تحصیلی به آن پرداخته شده است.

شرح

چالش‌های فضای سایبری و امنیت سایبری به چیزی بیش از یک نام گذاری مجدد ساده ادارات حکومتی مسئول برای امنیت تکنالوژی معلوماتی (IT Security) یا امنیت ارتباطات (COMSEC) نیاز دارد. گسترش سیستم‌های کمپیوتری مدرن و توانایی برقراری ارتباط یا تعامل توسط ابزارهای مختلف، از دستگاه‌های موبایل گرفته تا و کمپیوترهای قابل پوشیدن، آسیب‌پذیری‌های ذاتی و حامل‌های احتمالی حمله (بردارحمله) را برای بازیگران دولتی و غیر دولتی بوجود آورده است. بهره‌جویی از آسیب‌پذیری‌ها می‌تواند پیامدهای گسترده‌ای در عرصه امنیت ملی از طریق اقدامات عمدی جاسوسی، تخریب تسهیلات سوق و اداره، سرقت مالکیت فکری و معلومات حساس شخصی، ایجاد اختلال در خدمات و زیربناهای حیاتی، یا خسارات اقتصادی و صنعتی داشته باشد.

از طریق پنج بخش این موضوع، شاگردان با ساختار اساسی فضای سایبری و رویکرد مبتنی بر ریسک امنیت سایبری آشنا می‌شوند. بخش T1-B1، امنیت سایبری و فضای سایبری – مقدمه‌ای که در آن منشا و شکل کلی فضای سایبری بررسی شده و مفهوم امنیت سایبری تعریف می‌شود. بخش T1-B2، ریسک و امنیت معلومات – به اساسات متدولوژی تجزیه و تحلیل ریسک امنیت معلومات می‌پردازد و رویکرد مبتنی بر ارزیابی تهدید را بررسی می‌کند. بخش T1-B3، ساختارهای فضای سایبری – ستون فقرات اینترنت و زیربناهای ملی، عملیات و معماری و همچنین اینترنت جهانی و حاکمیت آن را بررسی می‌کند. بخش T1-B4، پروتکل‌ها و پلتفرم‌ها، استندردهای تکنالوژی شبکه و تکنالوژی معلوماتی را به منظور بررسی اساسات طراحی و عملیات‌های شبکه معرفی می‌کند. بخش T1-B5، معماری امنیت و مدیریت امنیت – اصول معماری امنیتی را بر اساس تجزیه و تحلیل تهدید، ریسک و آسیب‌پذیری معرفی می‌کند. تجزیه و تحلیل ریسک باید رهنمودی برای تدوین معماری و استراتژی سایبری جهت کاهش آسیب‌پذیری‌ها و تهدیدهای شناخته شده و ناشناخته در سطح سازمانی و ملی باشد. بنابراین، شاگردان جهت تدوین معماری و استراتژی سیستم‌ها به منظور کاهش خطرات با متدولوژی و مدیریت اساسی تجزیه و تحلیل ریسک سایبری آشنا می‌شوند.

نتایج یادگیری

شاگردان قادر خواهند بود

- فضای سایبری و امنیت سایبری را تشریح کنند؛
- برخی از آسیب‌پذیری‌های اساسی کشورهای پیشرفته را در رابطه با تهدیدات سایبری تشریح کنند مانند جمع آوری معلومات اقتصادی برای منافع ملی، مشخصات فردی و سازمانی، سرقت دیتا (data)، خرابی دیتابیس یا در اختیار گرفتن سیستم‌های کنترول صنعتی یا سیستم‌های کنترول پروسه (به عنوان مثال اسکادا)؛
- توپولوژی اساسی فضای سایبری را تشریح کنند، از جمله ساختارهای فیریکی و نحوه اداره آن از طریق پروتکل‌ها و طرزالعمل؛ و
- ملاحظات اساسی را برای معماری مناسب امنیتی تشریح کنند.

مراجع پیشنهادی

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

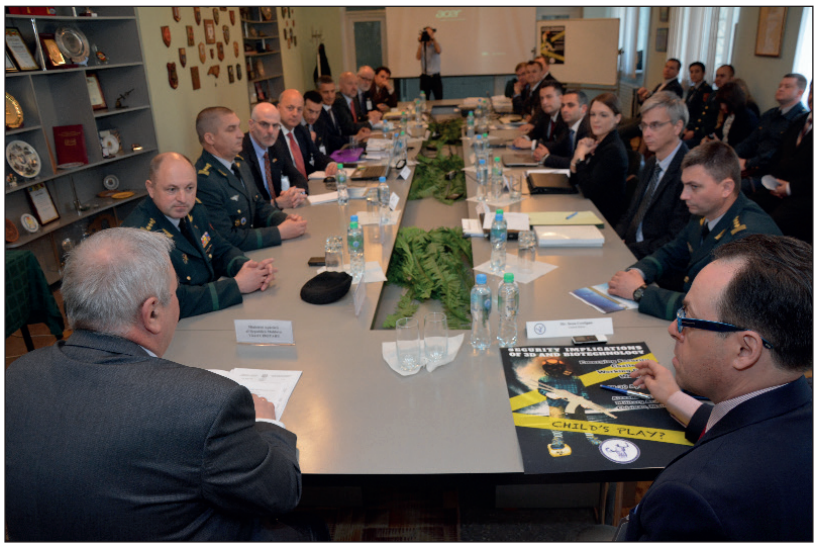
Chris Hall, Richard Clayton, Ross Anderson and Evangelos Ouzounis, *Inter-X: Resilience of the Internet Interconnection Ecosystem—Full Report,* ENISA, April 2011. http://www.enisa.europa.eu

[3] فضای سایبری در این سند به عنوان دنیای الکترونیکی ایجاد شده توسط شبکه‌های به هم پیوسته تکنالوژی معلوماتی و معلومات در آن شبکه‌ها تعریف شده است. برگرفته از استراتژی امنیت سایبری کانادا، 2014.

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

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



ورکشاپ تیم‌های تدوین‌کننده نصاب تحصیلی عمومی مرجع برای امنیت سایبری در کیشیناو.

بخش T1-B1: امنیت سایبری و فضای سایبری- مقدمه

شرح

فضای سایبری متشکل از سیستم‌های کمپیوتری متصل به شبکه و سیستم‌های مخابراتی می‌باشد. فضای سایبری به یکی از ویژگی‌های مدرن جامعه تبدیل شده است که ارتباطات سریع، سیستم‌های توزیع شده (از راه دور) سوق و اداره، سیستم‌های توزیع شده، ذخیره‌سازی و انتقال گسترده معلومات را تقویت و امکان‌پذیر می‌کند. همه این‌ها توسط جامعه امری بدیهی تلقی شده و برای تجارت، زندگی روزمره و ارائه خدمات ضروری است. این جهانی بودن و وابستگی به فضای سایبری حتی در عرصه‌های نظامی قابل مشاهده است، جایی‌که ارتباطات، سوق و اداره، فعالیت‌های استخباراتی و عناصر حمله دقیق همگی به" سیستم‌های سایبری" و سیستم‌های ارتباطی مربوطه متکی هستند. گسترش این سیستم‌های بهم پیوسته، درجه‌ای از وابستگی و آسیب‌پذیری را برای افراد، صنایع و حکومت به ارمغان آورده است که پیش‌بینی، مدیریت، کاهش یا جلوگیری از آن دشوار است. برخی از کشورها چنین وابستگی‌های آسیب‌پذیر را به عنوان یک نگرانی در حال رشد امنیت ملی یا دفاع ملی می‌دانند و عناصر موجود نیروهای امنیتی خود را موظف به پاسخگویی می‌کنند، درحالی‌که سایر کشورها، سازمان‌های کاملا جدیدی را ایجاد کرده‌اند که وظیفه آنها مدیریت یا هماهنگی پالیسی‌های ملی امنیت سایبری است. امنیت سایبری به عنوان یک مسئله مهم که در زمینه‌های دیگر هم مطرح شده است نیاز به پاسخگویی افراد، شرکت‌های خصوصی، سازمان‌های غیر حکومتی "تمام حکومتی" و همچنین ادارات و نهادهای مختلف بین‌المللی دارد.

این بخش با هدف آشنایی شاگردان با تکنالوژی معلوماتی و مخابراتی (ICTs)، فراگیر بودن آن و وابستگی حاصله ما به چنین سیستم‌هایی را آشکار می‌کند. هدف اینست تا درک شاگردان در مورد موضوعات اجتماعی، تخنیکی و فرهنگی تکنالوژی معلوماتی مدرن، نقش‌های متعدد آن و تاثیر نظری فضای سایبری بر زندگی مدرن، ارتباطات کشوری و جهانی گسترش یابد. این بخش مقدماتی را برای شاگردان امنیت ملی فراهم می‌کند تا درک درستی از توپولوژی و ساختارهای فضای سایبری و همچنین امنیت سایبری داشته باشند.

برای وضاحت در مورد مفهوم فضای سایبری و امنیت سایبری، به تعریف موسسه ملی استندردها و تکنالوژی (NIST) ایالات متحده اتکاء نمودیم. طبق اعلام این موسسه " فضای سایبری عبارتست از شبکه متکی به زیربناهای تکنالوژی معلوماتی که شامل اینترنت، شبکه‌های مخابراتی، سیستم‌های کمپیوتری، پروسسورهای جاسازی‌شده و کنترول‌کننده‌ها می‌باشد". "امنیت سایبری عبارت از فعالیت یا پروسه، توانایی یا وضعیتی می‌باشد که از سیستم‌های معلوماتی و مخابراتی و همچنین معلومات موجود در آن در برابر آسیب، استفاده غیر مجاز، تغییر یا بهره‌جویی محافظت می‌شود و یا از آن دفاع می‌شود." این تعریف اساسی تمامی موارد گنجانده شده در این سند را در برمی‌گیرد.

نتایج یادگیری

شاگردان نشان خواهند داد که موراد زیر را در سطح مناسب درک نمودند

- اهمیت تکنالوژی معلوماتی و مخابراتی وچگونگی تغییر ساختار جوامع مدرن؛
- تفاوت‌های دقیق و ظریف امنیت سایبری در بسترهای مختلف ملی و فرهنگی با تاکید بر رویکردها و پالیسی‌های ملی آنها؛
- چالش‌های کلیدی تکنالوژی معلوماتی و مخابراتی، ارائه کنندگان عمده، منابع کلیدی پالیسی‌ها، جوانب اصلی، مسئولیت‌های حقوقی و وظیفوی؛
- تأثیرات مثبت و منفی فضای سایبری بر جامعه؛
- آگاهی گسترده از تهدیدات و خطرات در مورد عملکرد موثر و ایمن فضای سایبری؛
- نحوه اداره، راه اندازی و نگهداری اینترنت توسط موسسات دولتی، خصوصی و غیر انتفاعی؛
- بستر های ملی مشخص در تدوین پالیسی و نحوه ادره محلی اینترنت؛
- نقش استندردها و پروتکل‌ها در طراحی اینترنت؛ و
- الزامات نظامی و سیاسی مرتبط با فضای سایبری و حاکمیت اینترنت.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

عمق بررسی به مخاطب و زمان موجود بستگی دارد، اما قسمت‌های مربوط به زیربنای‌های ملی اینترنت و مخابرات، ارائه‌کنندگان عمده خدمات و تقسیم مسئولیت‌ها در قبال پالیسی‌ها و عملکردهای گسترده امنیتی در حکومت‌های ملی و سازمان‌های دفاعی ممکن است بطور جداگانه به تمام آنها به منظور وضاحت و تاکید پرداخته شود.

روش یادگیری/ارزیابی

روش‌های تدریس در این بخش می‌تواند شامل لکچرها توسط متخصصین موضوعی، سیمینارها، نمایشات، تمرینات و شبیه سازی در صنف باشد.

شاگردان از طریق سهمگیری و بحث در تمرینات و مناظره‌ها و سپس از طریق امتحان مطالبی که از کورس آموختند ارزیابی می‌شوند.

مراجع

متخصصین موضوعی در زمینه انتخاب مواد درسی کلیدی مناسب برای مطالعه بر اساس تمرکز پلان شده کورس و زمان مورد نیاز با کشور میزبان کار خواهند نمود.

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.

متخصصین موضوعی در زمینه انتخاب مواد درسی کلیدی مناسب برای مطالعه بر اساس تمرکز پلان‌شده کورس و زمان مورد نیاز با کشور میزبان کار خواهند نمود.

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

James R. Beniger, *The 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.

T1-B2: ریسک و امنیت معلومات

شرح

به طور کلی امنیت معلومات (information security) به چندین دسته گسترده معلومات ارتباط می‌گیرد - خصوصی، دولتی، حساس، محرمانه و غیره – که برای مدیریت چه به شکل دیجیتالی یا سایر اشکال به شیوه‌ها و پروتکل‌ها نیاز دارد. در حوزه سایبری، هکرها، مجرمان و سرویس‌های استخباراتی خارجی علامند بهره‌جویی از هر گونه ضعف مدیریتی در زمینه امنیت معلومات هستند. این بخش با تاکید بر حوزه مربوط به سایبر شاگردان را با مفهوم کلی ریسک و امنیت معلومات آشنا می‌کند.[4] بعدا در این کورس به آنها توضیحات دقیق‌تری در مورد رویکرد ملی به "امنیت معلومات" داده خواهد شد (نگاه کنید به موضوع 4). دراین‌جا، بحث باید از نحوه طبقه‌بندی معلومات به تفاوت بین امنیت معلومات و اطمینان از معلومات (information assurance) تغییر کند و سپس انواع آسیب‌پذیری‌های امنیت سایبری و پروسه حمله یا زنجیره کشتن (kill chain) برای حوادث سایبری مورد بررسی قرار گیرد. سپس بحث به سمت مدیریت ریسک و امنیت معلومات از طریق رویکردهایی مانند مودل ارزیابی تهدید و ریسک (TRA)[5] به خصوص در پرتو تهدیدات پیشرفته مستمر (APTs) تغییر می‌کند.[6] علاوه بر بررسی دقیق این مرحله، شاگردان باید از نهادهای عمده سازمانی و ملی که مسئولیت تدوین پالیسی‌ها، طرزالعمل‌ها و شیوه‌های امنیت معلومات را بر عهده دارند مطلع شوند.

پیشینه

امنیت معلومات شامل مکانیزم‌ها و پروسه‌هایی است که امکان دسترسی به دارایی‌های فیزیکی و اطلاعات یا داده‌های (data) موجود یا جاری در آن سیستم‌ها را فراهم می‌کند. امنیت معلومات روی تکنالوژی و عملیات‌های مربوط به اپلیکیشن‌ها و زیربناهای امنیتی متمرکز است. اطمینان از معلومات (که ممکن است در سطح ملی به آن عناوین مختلفی داده شود) شامل مسائلی در مورد امنیت معلومات است، اما بر روی مدیریت معلومات، یکپارچگی (سلامت) معلومات، سازمان‌های حفاظتی و پروتکل‌های امنیتی برای کاهش یا مدیریت خطرات کلی و کاهش تأثیر حوادث نیز متمرکز است. اهداف عمده امنیتی معمولا شامل محرمیت، یکپارچگی، در دسترس بودن، احراز هویت و عدم انکار است. شیوه‌ها و سیستم‌های امنیت معلومات در سطوح فردی، سازمانی/ شرکتی و ملی وجود دارد.

نتایج یادگیری

شاگردان نشان خواهند داد که با موارد زیر آشنایی دارند

- استندردهای طبقه‌بندی امنیتی (حفاظتی) برای معلومات و سیستم‌های معلوماتی و الکترونیکی؛
- تجزیه و تحلیل تهدیدات و خطرات در سطح مناسب؛
- نمونه‌های مختلف "زنجیره کشتن سایبری
- قادر به تعریف اصطلاحات کلیدی مربوطه مانند (دیتا، دانش، معلومات، امنیت معلومات و زنجیره کشتن سایبری) خواهند بود؛
- قادر به درک اطمینان از معلومات و اهمیت اهداف امنیتی محرمیت، یکپارچگی، در دسترس بودن، احراز هویت و عدم انکار خواهند بود؛
- قادر به توضیح نقش مودل امنیتی (TVRA) در زمینه مدیریت امنیت معلومات خواهند بود؛
- قادر به تشخیص سازمان‌های مسئول تدوین و بیان پالیسی‌ها، شیوه‌ها و طرزالعمل‌های امنیت معلومات ملی خواهند بود.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

- تکامل امنیت معلومات
- منابعی برای عملکردهای خوب بین‌المللی
- تشخیص مقامات ملی امنیت سایبری

روش یادگیری/ارزیابی

روش‌های تدریس در این بخش می‌تواند شامل لکچرها، نمایشات با تصویرهایی از عملکردها و قضایای واقعی باشد. شاگردان باید قادر به تعریف امنیت معلومات، زنجیره کشتن سایبری، تهدیدات پیشرفته مستمر (APT) و ارزیابی تهدید و خطر (TRA) باشند.

مراجع

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.

[4] هدف امنیت معلومات الکترونیکی اطمینان از تداوم خدمات، محرمانه بودن، یکپارچگی یا سلامت، در دسترس بودن، احراز هویت و عدم انکار می‌باشد - به عنوان مثال، دسترسی مناسب کاربران مجاز در سطح مناسب.

[5] مودل ارزیابی تهدید و ریسک (TRA) دارایی‌های معلوماتی، تهدیدات، آسیب‌پذیری‌ها و کنترول‌کننده‌ها را ارزیابی می‌کند.

[6] کلمه "پیشرفته" در اینجا به معنی هماهنگ، هدفمند و پیچیده است در حالی که کلمه "مستمر" به معنای مداوم است. به ویژه، تهدیدات پیشرفته مستمر (APTs) برای یافتن فرصتی برای خواندن، تغییر، خراب کردن، انکار دسترسی، بهره‌جویی یا از بین بردن قابلیت‌های سایبری به عوامل "هوشمند" نیاز دارند.

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 Information Technology—Security Techniques—Information Security Management Systems—Requirements
2) ISO/IEC 27005:2011 Information Technology—Security Techniques—Information Security Risk Management
3) ISO/IEC 27031:2011 Information Technology—Security Techniques—Guidelines for Information and Communications Technology Readiness for Business Continuity
4) ISO/IEC 27032:2012 Information Technology—Security Techniques—Guidelines for Cybersecurity

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).

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.

T1-B3: ساختارهای فضای سایبری: ستون فقرات اینترنت و زیربناهای ملی

شرح

هدف این بخش آشنایی شاگردان با ساختار تخنیکی فضای سایبری با تمرکز بر زیربناهای جهانی، ملی و سازمانی می‌باشد که این شامل معماری اینترنت، شبکه‌های کمپیوتری و شبکه‌های سلولی یا شبکه‌های مخابراتی بی‌سیم می‌گردد. منطق اساسی ساختار کلی و توپولوژی خاص ملی (به عنوان مثال، مشخصه زیربنای ملی که از شبکه‌ها، ارائه‌کنندگان خدمات مخابراتی و کانال های مسیریابی پشتیبانی می‌کند) باید تمرکز اصلی این بخش را شکل دهد.

پیشینه

معماری ستون فقرات اینترنت شامل مسیرهای اصلی دیتا (data) بین سیستم‌های اصلی شبکه‌های کمپیوتری بزرگ و روترهای اصلی اینترنت می‌باشد. این شبکه‌ها و روترها توسط مراکز تجارتی، حکومتی، اکادمیک و سایر مراکز شبکه‌ای با ظرفیت بالا میزبانی می‌شوند. آنها نقاط تبادله اینترنت و نقاط دسترسی شبکه را کنترول می‌کنند و در حال مبادله ترافیک اینترنت بین کشورها و قاره‌ها می‌باشند. معمولا ارائه‌کنندگان عمده خدمات اینترنتی (ISPs) (به طور مثال شبکه های ردیف اول Tier 1) با استفاده از توافق‌نامه‌های اتصال خصوصی در تبادل ترافیک ستون فقرات اینترنت سهم می‌گیرند. یک شماره سیستم مستقل (ASN) به هر سیستم مستقل (AS) اختصاص داده می‌شود، بنابراین ارائه‌کنندگان خدمات اینترنتی زیر مجموعه‌های مجزا اینترنت را به نام سیستم‌های مستقل مدیریت می‌کنند. مسیریابی و قابلیت دسترسی بین سیستم‌های مستقل از طریق مجموعه‌ای از روترهای اصلی اینترنت با استفاده از پروتکل درگاه مرزی (BGP) اجرا می‌شود. ارتباط بین نام های دومین (به طور مثال، wwww.google.com) و آدرس‌های اینترنتی قابل مسیریابی (که توسط سیستم‌های مستقل کنترول می‌شوند) توسط سیستم نام دومین (DNS) و مقامات ثبت کننده این نام مدیریت می‌شوند.

رجستری اینترنت ملی (NIR) سازمانی است که مسئولیت هماهنگی پروسه تخصیص پروتکل اینترنت (IP) و سایر توابع مدیریت منابع اینترنتی را در سطح ملی (از طریق رجستری اینترنت بین‌المللی) بر عهده دارد. یک حکومت ملی همچنین می‌تواند ارائه کنندگان خدمات اینترنتی را در منطقه اقتصادی خود تعیین کند.

امروزه شبکه‌های تلفن بی سیم/دستگاه موبایل عنصر بزرگی از زیربناهای توزیع اینترنت را تشکیل می‌دهند. این شبکه‌ها به اینترنت وصل هستند و به آنها "وب موبایل" می‌گویند. معماری کلی و مشخصات ملی آنها نیز باید در این بخش بررسی شود.

اهداف یادگیری

شاگردان قادر خواهند بود

- درک عمیقی از توپولوژی فیزیکی و مجازی و همچنین اداره ستون فقرات اینترنت خواهند داشت؛
- قادر به توضیح نقش "شماره سیستم مستقل" (ASNs) در شبکه جهانی اینترنت و "مسئولیت مرجع اعداد اختصاص یافته در اینترنت" (IANA) خواهند بود؛
- قادر به درک ارتباط بین ارائه‌کنندگان عمده خدمات اینترنتی (Tier 1)، ارائه کنندگان تابع خدمات اینترنتی، و کاربر نهایی در شبکه‌های محلی (LANs) خواهند بود؛
- قادر خواهند بود که نقش سرورهای معتبر(به عنوان مثال DNS) را در اتصال جهانی اینترنت و همچنین مسئولیت شرکت اینترنتی برای نامها و اعداد واگذار شده (ICANN) را توضیح دهند؛
- توپولوژی و جغرافیای فضای سایری ملی خود که شامل رجستری اینترنت ملی و مقامات اداره کننده خدمات اینترنتی می‌شود را درک خواهند کرد؛ و
- با ساختار و اداره شبکه های تلفن بیسیم/دستگاه موبایل و اتصال اینترنت در بستر ملی آشنایی خواهند داشت.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

برای فراهم نمودن یک مقدمه موثر به مخاطبان غیر فنی، آنهایی که از این نصاب تحصیلی مرجع برای برگزاری کورس یا کورس خاص استفاده می‌کنند باید توجه زیادی به یافتن سطح مناسب جزئیات تخنیکی داشته باشند تا اطمینان حاصل کنند که مطالب برای شاگردان قابل درک است.

زیربناهای ملی شبکه و مخابرات می‌تواند به صورت عمیق‌تر بررسی شود.

روش یادگیری/ارزیابی

شیوه‌های تدریس در این بخش می‌تواند شامل لکچرها و نمایشات باشد. بازدید از تسهیلات ملی، ارائه تشریحات متخصصین، امتحانات چالش برانگیز شفاهی و عملی می‌تواند به این نصاب تحصیلی مرجع رونق بیشتری ببخشد.

مراجع

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.

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," Security-Week 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/

T1-B4: پروتکل‌ها و پلتفرم‌ها

شرح

سیستم‌های ارتباطی از قالب‌های پیام کاملا مشخصی به نام پروتکل برای تبادل پیام‌ها استفاده می‌کنند. یک پروتکل ارتباطی (Communication Protocol) عبارتست از مجموعه قوانینی که زمینه تبادل دیتا (data) را در یا بین کمپیوترها (خواه به شبکه متصل باشد یا نه) فراهم می‌کند. این پروتکل‌ها را می‌توان شبیه اجزای آدرس روی پاکت پستی دانست که فرستنده، گیرنده و مختصات مربوطه آن مشخص می‌شود. هر پیام معنی دقیقی دارد که قصد دارد پاسخی را از مجموعه پاسخ‌های احتمالی از پیش تعریف شده برای یک وضعیت خاص بدست آورد. بنابراین یک پروتکل باید نحو یا قواعد (Syntax)، معناشناسی (Symantics) و همگام‌سازی (Synchronization) ارتباطات را تعریف کند؛ رفتار مشخص شده به طور معمول از نحوه اجرای آن یا سیستم‌های مختلفی که می‌تواند از آن عبور کند تا به مقصد مورد نظر برسد مستقل می‌باشد.

هر لایه پروتکل و پروسه آن آسیب پذیری‌ها و خطرات ذاتی خود را دارد که می‌تواند در چندین سطح تخصصی بررسی شود. این موضوع ممکن است در یک سطح بسیار اساسی مورد بحث قرار گیرد، اما با توجه به مخاطبان مناسب ممکن است در سطح طبقه بندی شده بررسی شود.

پیشینه

برای ترسیم و طراحی سیستم شبکه دو روش وجود دارد.

نمای منطقی اینکه چگونه اینترنت کار می‌کند می‌تواند مبتنی بر پروتکل پنداشته شود. پشته پروتکل (Protocol stack) عبارت از سافت‌ویر پیاده‌سازی مجموعه‌ای استندرد از پروتکل‌های ارتباطی می‌باشد. پشته پروتکل نحوه بسته‌بندی و انتقال دیتا (data) را اداره می‌کند. پیاده‌سازی پروتکل به طور معمول در یک ساختار لایه‌ای (به طور مثال، یک پشته) مرتب شده است. پیاده‌سازی پروتکل‌های نزدیک به لایه‌های پایین پشته (stack) خدمات ارتباطی ابتدایی‌تری را انجام می‌دهند، مانند ارتباط ابتدایی یک دیتای کوچک با یک کمپیوتر دیگر در شبکه محلی (به عنوان مثال اترنت). در لایه‌های بالاتر پشته، پروتکل‌ها خدماتی مانند آدرس‌دهی برای شبکه‌های جهانی (به طور مثال IP یا پروتکل اینترنت)، تصحیح خطا و سرهم‌بندی/مونتاژ مجدد دیتا از بانک‌های معلوماتی (به عنوان مثال TCP یا پروتکل کنترول انتقال) را فراهم می‌کنند. پروتکل‌ها در بالاترین سطح، انتزاعی‌ترین خدمات را مانند رساندن ایمیل (SMTP (پروتکل ساده انتقال نامه)) یا مرور صفحات وب (HTTP) را فراهم می‌کنند. لایه‌های بالاتر در پشته پروتکل به اساسی‌ترین خدمات لایه‌های پایین بستگی دارد.

متناوبا، نمای فیزیکی اینترنت می‌تواند از طریق نحوه اجرای پروتکل‌ها در دستگاه‌ها و پلتفرم‌های شبکه (مانند سوئیچ ها و روترها، گیت‌وی‌ها، پروکسی‌ها و فایروال‌ها) و اشکال اتصال بین این دستگاه‌های شبکه توضیح داده شود. به عنوان مثال، سوئیچ‌های شبکه که پروتکل اترنت را اجرا می‌کنند می‌توانند کمپیوترها را در شبکه محلی (LAN) به هم وصل کنند. شبکه‌های محلی ممکن است اتصالاتی به روترهای شبکه که پروتکل انترنت را برای هدایت مجدد بسته‌های دیتا (data) بین شبکه‌ها و احتمالاً بقیه اینترنت اجرا می‌کنند داشته باشند. یک میل سرور (Mail Sever) متصل به شبکه می‌تواند پروتکل ساده انتقال نامه (SMTP) را اجرا کند.

نقشه برداری مستقیم از رابطه بین دستگاه‌های فیزیکی و مسئولیت آنها در قبال اجرای پروتکل با معرفی دستگاه‌ها و شبکه‌های مجازی در شبکه‌های امروزی دشوار شده است. در چنین شبکه‌هایی، دستگاه‌های شبکه و اتصال آنها ممکن است به طور مجازی با استفاده از سافت‌ویری که روی سرورهای بزرگ (مانند مورد "محاسبات ابری") در حال اجرا است پیاده‌سازی شود. مجازی‌سازی این سیستم‌ها لایه‌ای از پیچیدگی به امنیت اضافه می‌کند و موضوعی در حال رشد است که باید به آن رسیدگی شود.

پشته پروتکل (Protocol stack) را می‌توان برای کاربردهای تخصصی طراحی و پیاده سازی کرد. سیستم‌های کنترول صنعتی (ICSs) مانند سیستم کنترول نظارتی و اکتساب دیتا (SCADA) نمونه‌ای از پشته پروتکل ارتباطی شبکه می‌باشد که برای گزارش در مورد معلومات اندازه گیری شده توسط سنسور و ارسال پیام‌های کنترول مورد استفاده قرار می‌گیرد. به طور مثال، ممکن است در یک توربین تولید برق مسئولیت نظارت بر بارگیری و تعویض اتصال منبع بر اساس تغییر تقاضا را بر عهده داشته باشد. تامین امنیت سیستم‌های اسکادا عنوان مهمی در عرصه امنیت زیربناهای ملی می‌باشد چراکه سیستم‌هایی که آنها کنترول می‌کنند ممکن است از اهمیت ملی برخوردار باشند. بسیاری از سیستم‌های مدرن تسلیحاتی از سیستم‌های الکترونیک مشابه به سیستم اسکادای صنعتی استفاده می‌کنند و ممکن است آسیب‌پذیر باشند.

هر لایه پروتکل خطرات و آسیب پذیری‌های ذاتی خود را دارد. این موارد می‌تواند در سطوح مختلف تخصصی، از معلومات عمومی تا سطح تخصصی (طبقه بندی شده) مورد بررسی قرار گیرد.

تعریف پروتکل امنیت شبکه

پروتکل‌های امنیتی شبکه عموما امنیت و سلامت دیتا راهنگام انتقال آن از طریق اتصال به شبکه تامین می‌کنند. پروتکل‌های امنیتی شبکه پروسه‌ها و روش‌های ایمن‌سازی دیتای شبکه (network data) را تعریف می‌کنند. هیچ پروتکل امنیتی امنیت را تضمین نمی‌کند. بلکه هر پروتکل روش خاصی را برای خنثی‌سازی یک رویکرد خاص حمله به سیستم یا شبکه ارئه می‌دهد. توجه: ممکن است تعاریف خاص ملی یا توافق شده بین‌المللی وجود داشته باشد.

پروتکل‌های امنیتی شبکه اغلب از رمزنگاری و رمزگذاری برای ایمن‌سازی دیتا استفاده می‌کنند که فقط با یک الگوریتم خاص، کلید منطقی، فرمول ریاضی و یا ترکیبی از آن رمزگشایی می‌شود یا تغییر می‌کند. پروتکل‌های محبوب شبکه عبارتست از پوسته امن (SSH) پروتکل امن انتقال فایل (SFTP) پروتکل امن انتقال ابرمتن (HTTPS) و امنیت لایه سوکت‌های امن (SSL).

نتایج یادگیری

شاگردان قادر خواهند بود

- راجع به نقش و مسئولیت‌های هر یک از لایه‌های استندرد پشته پروتکل شبکه (مجموعه پروتکل اینترنتی مبتنی بر TCP/IP یا پروتکل کنترول انتقال/ پروتکل اینترنت) بحث کنند؛
- راجع به دستگاه‌های معمول شبکه مانند هاب‌ها، سوئیچ‌ها، روترها، گیت‌وی‌ها، سرورهای کاربردی، رابطه بین پیاده‌سازی هاردویر لایه‌های پشته پروتکل شبکه و نقش عملکردی آنها در شبکه توضیح دهند؛
- راجع به مفاهیم اساسی مجازی‌سازی دستگاه‌های شبکه و شبکه‌های مبتنی بر سافت‌ویر (SDN)، تاثیر این مفاهیم بر معماری شبکه و ارتباط آنها با محیطهای محاسبات ابری (cloud computing) بحث کنند؛
- عناصر اساسی محیط سیستم کنترول صنعتی (ICS) مبتنی بر اسکادا (شامل اجزای مشخص سیستم کنترول صنعتی و پایه های عملیاتی آنها در پروتکل‌های استندرد اینترنت) را توضیح دهند؛
- پروتکل‌های معمول امنیتی، ارتباط آنها با ساختار چند لایه‌ای مبتنی بر پروتکل و آسیب پذیری‌های امنیتی خاص که هر پروتکل برای رسیدگی به آن طراحی شده است را تشخیص و توضیح دهند.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

سیستم‌های کنترول صنعتی (به طور مثال، اسکادا) و پلتفورم‌های سیستم‌های نظامی تکنالوژی معلوماتی می‌تواند با جزئیات برای شناسایی آسیب‌پذیری‌ها و جذابیت‌شان به عنوان اهداف بررسی شود.

روش یادگیری/ارزیابی

لکچرها، نمایشات و مطالعات موردی توصیه می‌شود. ارزیابی باید در سطح مناسب به شکل تحریری و با توجه به مشخصات هر کورس خاص که از این نصاب تحصیلی نشأت گرفته ایجاد شود.

مراجع

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).

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.

T1-B5:معماری امنیت و مدیریت امنیت

شرح

این بخش به مسئله معماری اساسی امنیت (BSA) می‌پردازد که جنبه‌های تکنالوژیکی، عملیاتی و بسترهای بشری و مدیریتی تاثیرگذار بر شکل آن را در بر می‌گیرد. در سطح ملی، معماری اساسی امنیت عبارتست از ارائه معماری و شیوه‌های امنیتی از جمله زیربناها (به طور مثال، ستون فقرات مخابرات)، فیلترهای محتوا و ساختارهای حکمرانی و اداره امنیت سایبری در سطح ملی. هدف کلی این بخش اینست که به شاگردان بیاموزد چگونه محیطهای امنیتی را بر اساس تجزیه و تحلیل خطر طراحی و ایجاد کنند تا اطمینان حاصل شود که خطرات بیش از حد آستانه قابل قبول نباشد. این معماری شامل کنترول‌های تخنیکی و فیزیکی و همچنین پایسی‌ها و تعلیمات است. نمونه‌هایی از کنترول‌های تخنیکی شامل فایروال‌ها، سیستم‌های تشخیص نفوذ و مدیریت ثبت وقایع می‌باشد. مدیریت دسترسی، هشدار آتش‌سوزی و کنترول رطوبت را می‌توان به عنوان نمونه‌هایی از کنترول‌های فیزیکی ذکر کرد. شاگردان نحوه تجزیه تحلیل خطر و تنظیم مجموعه‌ای از عملکردهای امنیتی را در سطح ملی و همچنین در سطوح فردی و سازمانی خواهند آموخت.

معماری اساسی امنیت بر اساس پالیسی‌های ملی، استندردهای مختلف امنیتی، چرخه حیات سیستم، اصول طراحی و عناصر معماری فیزیکی هدایت می‌گردد. این بخش به مفاهیم تکمیلی مناسب کنترول دارایی‌ها، کنترول فیزیکی و محیطی، پلان‌های مدیریتی، جنبه‌های بشری شامل بررسی سابقه کارمندان، تداوم عملیات‌ها، پلان‌های احتیاطی و تاب آوری سیستم‌های سایبری به منظور بررسی طراحی معماری اساسی امنیت می‌پردازد.

پیشینه

معماری امنیتی باید پالیسی محور باشد. یعنی با شناخت دارایی‌های معلوماتی تحت مدیریت آغاز می‌گردد. ارزش دارایی‌های معلوماتی برای مدافعین (به طور مثال، تأثیر از دست دادن یا تغییر آنها) و ارزش این دارایی‌ها برای بازیگران بالقوه مخرب محور اصلی این ملاحضات را تشکیل می‌دهد. این مرحله تشخیص و ارزشیابی دارایی است که منجر به انکشاف پالیسی کنترول دسترسی به معلومات می‌شود.

بازیگران مخربی که به طور منطقی از آنها انتظار می‌رود دارایی‌های معلوماتی مشخص را به خطر بیندازنند در مرحله ارزیابی تهدید شناسایی شده و همچنین توانایی تخنیکی آنها در این مرحله مشخص می‌شود. انکشاف معماری امنیت ناشی از الزام به طراحی یک سیستم فیزیکی، طرزالعمل‌های عملیاتی و معیارهای اطمینان مربوطه می‌باشد که خطرات بازیگران شناسایی شده مخربی که توانایی به خطر انداختن دارایی‌های معلوماتی را دارند را کاهش می‌دهد. ممکن است استندردهای ملی جهت ارزیابی تهدیدات و خطرات، معیارهای ملاحظات طراحی، و رهنمود در انتخاب مکانیزم‌های کنترول دسترسی و طرح‌های معماری وجود داشته باشد.

معماری امنیت سازمانی (enterprise security architecture) اغلب به صورت دفاع در عمق انتخاب و سازماندهی می‌شود که در آن با استفاده هماهنگ از چندین مکانیزم امنیتی از یکپارچگی (سلامت) دارایی‌های معلوماتی محافظت می‌شود. حفاظت از دارایی‌های معلوماتی با کنترول دسترسی بر روی داده‌ها/دیتا (data) آغاز شده و سپس توسط مکانیزم‌های امنیتی موجود در اپلیکیشن‌هایی که به داده‌ها دسترسی دارد، کمپیوترهای میزبانی که اپلیکیشن‌ها روی آنها اجرا می‌شود و معماری شبکه سازمانی به بیرون از محیط امنیتی سازمان جایی‌که به زیربنای شبکه جهانی می‌پیوندد منتقل می‌شود.

معماری امنیت سازمانی شامل مجموعه‌ای از میکانیزم‌های است که به منظور کاهش خطرات آن سازمان خاص طراحی شده است. مکانیزم‌های معمول یا عناصر معماری برای اجرای پالیسی‌های امنیتی شامل زون بندی شبکه، فایروال‌ها، سیستم‌های تشخیص نفوذ (IDS) اپلیکیشن‌های ضد ویروس، تکنیک‌های رمزنگاری و سیستم‌های مدیریت معلومات و رویدادهای امنیتی (SIEM) می‌باشد. هیچ یک از این سیستم‌ها امنیت را تضمین نمی‌کند. تکنیک‌های حمله متنوع هستند و امکان بهره‌جویی از آسیب‌پذیری‌ها را در بسیاری از پروتکل‌ها، سیستم‌ها و اپلیکیشن‌های تشکیل‌دهنده زیربنای سازمانی فراهم می‌کنند.

فعالیت‌های اطمینان از امنیت عبارتند از فعالیت‌هایی که در طول انکشاف و ارزیابی معماری امنیت سازمانی انجام می‌شود تا اطمینان حاصل شود که اقدامات امنیتی در نظر گرفته شده برای یک سیستم موثر باشد. توجه: در بعضی موارد ممکن است این اقدامات بیشتر نظری باشند تا واقعی. به طور مثال، یک محصول کنترول دسترسی دیتا دارای مجموعه‌ای تبلیغاتی در مورد قابلیت‌های امنیتی است. یک فعالیت اطمینان مربوطه می‌تواند تست متدولوژیکی این قابلیت توسط یک سازمان شناخته شده استندردها برای ارائه شواهدی از عملکرد صحیح محصول باشد، بدون خطا. نمونه‌های دیگر فعالیت‌های اطمینان عبارتند از بررسی رسمی یا نمیه رسمی طرح، تدوین اسناد رهنمودی و رهنمودهای امنیتی برای کاربران و گردانندگان سیستم‌ها، مدیریت اجزای امنیتی چرخه‌های حیات، مدیریت پیکربندی، مدیریت امنیت محیط‌های تدوین‌کننده یا سازنده مولفه‌های معماری و تحویل‌دهی مطمئن مولفه‌های معماری از تدوین‌کننده/سازنده تا محیط سازمانی. اطمینان از امنیت همچنین شامل برنامه‌هایی جهت بررسی سابقه و تاییدیه شفافیت امنیتی برای پرسنل به منظور ایجاد اعتماد در کاربران و اپراتورهای سیستم‌ها می‌باشد.

نتایج یادگیری

شاگردان قادر خواهند بود

- قادر به بحث راجع به نحوه فراگیری چندین لایه از مکانیزم‌های امنیتی در یک معماری سازمانی مبتنی بر دفاع درعمق جهت حمایت یا تامین اقدامات اضافی در

صورت عدم موفقیت کنترول‌های امنیتی یا زمانی‌که از یک آسیب پذیری بهره‌جویی شده باشد خواهند بود؛

- قادر به پیشنهاد زون‌بندی مناسب امنیتی و انجام اقدامات امنیتی در سطح مقدماتی خواهند بود مانند فایروال‌ها که از یک دیاگرام شبکه استفاده می‌کنند؛
- قادر به درک استنددها و اسناد رهنمودی ملی راجع به ارزیابی تهدید و خطر، تدوین پالیسی امنیت سازمانی و پیاده سازی معماری امنیتی خواهند بود؛
- رابطه مرحله تشخیص دارایی و ارزیابی تهدید و خطر با تعیین پالیسی امنیتی برای سازمان را درک خواهند کرد؛
- رابطه مرحله ارزیابی با تشخیص آسیب‌پذیری‌های قابل بهره‌جویی توسط بازیگران تهدید را درک خواهند کرد و همچنین درک اینکه چگونه این موارد منجر به الزامات اقدامات امنیتی بکارگرفته شده در معماری امنیت سازمانی می‌شود؛ و
- راجع به ساحه سیستم محرمانه امنیت ملی برای حفاظت از اسناد و معلومات آگاهی پیدا خواهند کرد و قادر به توصیف رابطه آن با برنامه‌های بررسی سابقه پرسنل و تاییدیه شفافیت امنیتی خواهند بود.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

اشکال مختلف مدیریت معماری سازمانی (سیستم‌ها) و زون‌بندی شبکه‌های امنیتی باید مورد بحث قرار گیرد تا شاگردان توانایی ارزیابی مودل‌هایی که سازمان‌شان آنها را قبول کرده یا باید قبول کند را داشته باشند.

مهندسی عوامل بشری و استراتژی‌های استفاده از مهندسی اجتماعی می‌تواند توجیه کننده بررسی دقیق باشد.

سیستم اساسی محرمانه امنیت ملی برای دسترسی فیزیکی، محافظت از اسناد و معلومات، بررسی سابقه کارمندان و برنامه های تاییدیه شفافیت امنیتی ممکن است نیاز به بررسی و جمع بندی داشته باشد.

روش یادگیری/ارزیابی

روش‌های تدریس می‌تواند شامل کار روی عرصه‌های بشری، تکنالوژیکی و عملیاتی در گروهای کوچک باشد.

سخنرانان مهمان از سازمان‌های خصوصی و دولتی با حضورشان می‌توانند به بحث و تجربه یادیگیری رونق بیشتری ببخشند.

ابزارهای ارزیابی به سطح دانش مورد نیاز برای شاگردان خاصی که آموزش داده می‌شوند بستگی خواهد داشت، طوری‌که مناسب برگزیده شده باشد.

مراجع

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.

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

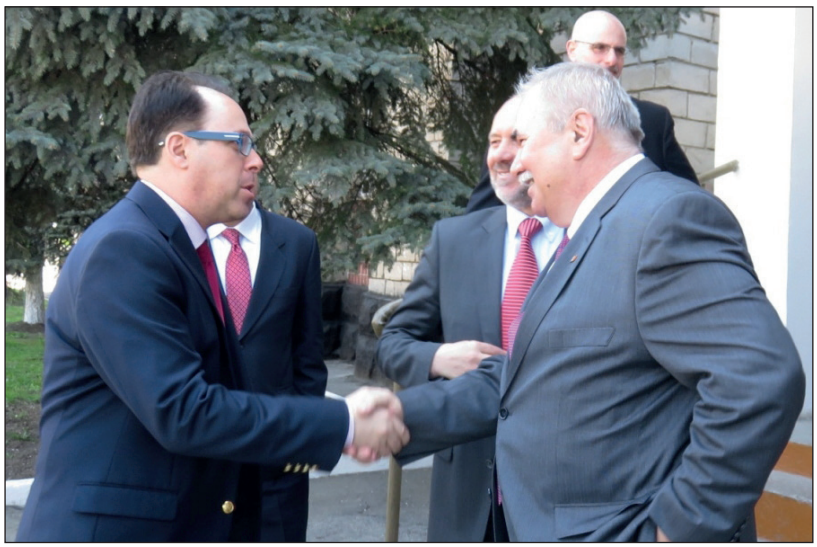
D.E. Gelbstein, *Information Security for Non-Technical Managers,* 1st Edition, 2013. ISBN 978-87-403-0488-6.

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

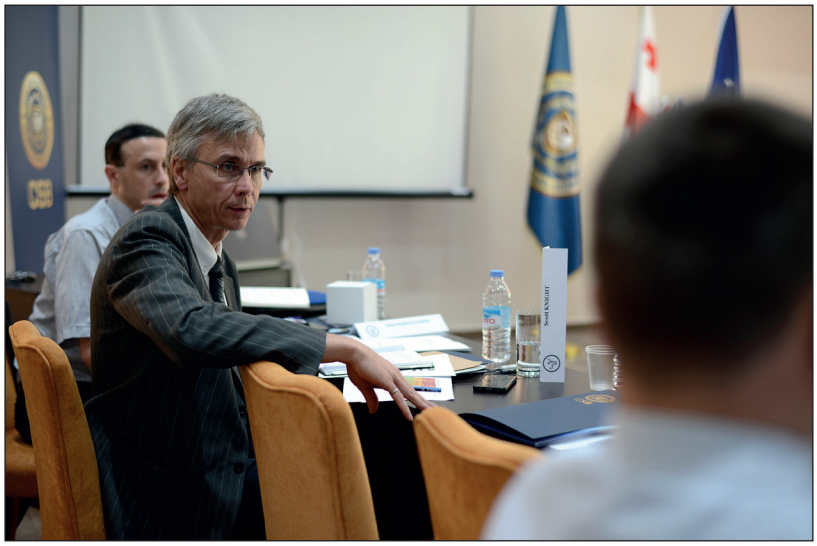
Alexander Klimburg, ed., *National Cyber Security Framework Manual,* NATO CCD COE Publication, Tallinn, Estonia, 2012. ISBN 978-9949-9211-2-6. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

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

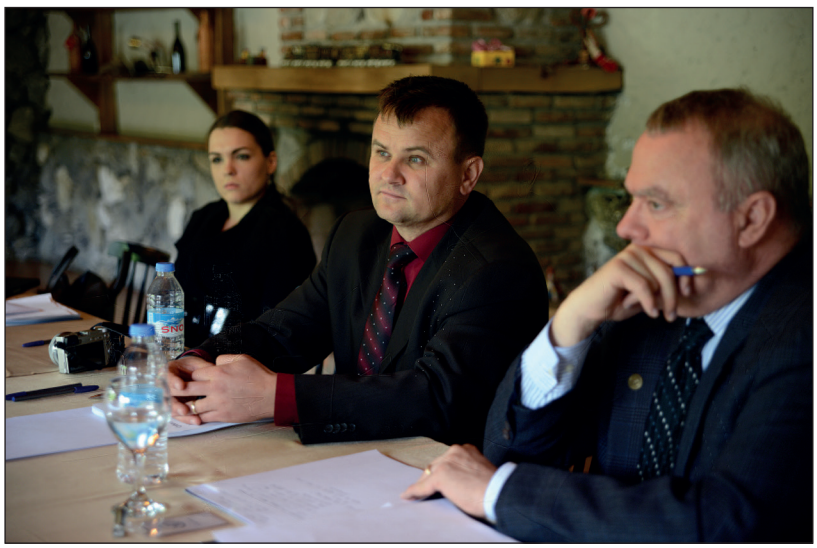
Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman and Lukas Ruf, "What is a Security Architecture?" paper by the Working Group Security Architecture, Information Security Society Switzerland (ISSS), 29 September 2008.



پیوستن کشورهای عضو و غیر عضو ناتو برای تالیف نصاب تحصیلی عمومی مرجع برای امنیت سایبری. دیدار وزیر دفاع مولدوا



ورکشاپ تیم‌های تدوین‌کننده نصاب تحصیلی عمومی مرجع برای امنیت سایبری در تبلیسی (شرکت‌کنندگان از پوهنتون گرینویچ و کالج سلطنتی نظامی کانادا).



ورکشاپ تیم‌های تدوین‌کننده نصاب تحصیلی عمومی مرجع برای امنیت سایبری در تبلیسی (شرکت‌کنندگان از مکتب ناتو در اوبرامیرگائو، آی انتلیجنس و اس ال سی ال).

موضوع 2: حامل‌های خطر

هدف

این موضوع به بررسی مقدماتی آسیب‌پذیری‌های ذاتی فضای سایبری و راه‌ها و روش‌های بهره‌جویی از این آسیب‌پذیری‌ها که از طریق حامل‌ها یا زنجیره‌های مختلف حمله فراهم می‌شود پرداخته است. درک این آسیب‌پذیری‌ها یکی از مولفه‌های ضروری پالیسی ارزیابی خطر و کاهش آن است که در ادامه مورد بررسی قرارخواهد گرفت.

شرح

این نصاب تحصیلی مرجع پیشنهادی را که در گزارش گروه مطالعات سایبری ایالات متحده به رئیس استخبارات ملی ایالات متحده آمده را قبول کرده، که گفته است آسیب‌پذیری‌های مختلف سایبری می‌تواند به راحتی بر اساس دسته‌بندی‌های حامل‌های خطر زیر طبقه‌بندی شود (Chabinsky 2010 به منابع مراجعه کنید): دسترسی به زنجیره عرضه و دسته‌بندی حامل‌ها؛ دسترسی از راه دور؛ دسترسی نزدیک و دسترسی درونی. بنابراین، در این موضوع، بخش T2-B1، به مسئله زنجیره عرضه/دسته‌بندی حامل‌ها می‌پردازد و مسائل امنیتی را از طبقه تولید تا قراردادی فرعی، کنترل حمل و نقل، کنترول انبارداری و نگهداری برجسته می‌کند. بخش T2-B2، حملات از راه دور و حملات مبتنی بر دسترسی نزدیک، آسیب‌پذیری‌های مرتبط با دسترسی غیر مجاز (بدون امتیاز) را بررسی می‌کند. بخش T2-B3، دسترسی درونی (حملات مبتنی بر دسترسی محلی)، آسیب‌پذیری‌های مرتبط با دسترسی ممتاز (امتیاز داده شده) را بررسی می‌کند و بخش T2-B4، خطرهای تحرک، بیود (BYOD) و روندهای در حال ظهور، در مورد خطرات مرتبط با پالیسی‌های بیود ("دستگاه خود را بیاورید")، محاسبات "ابری" و سایر مسائل تحرک بحث می‌کند.

هدف گسترده این موضوع فراهم آوردن زمینه‌ای کلی راجع به مسائل مختلف آسیب‌پذیری ذاتی اجزای فضای سایبری است. با این حال، کسانی که کورس‌هایی را با استفاده از این سند تهیه می‌کنند ممکن است این عمل را در سطح تخصصی و طبقه بندی‌شده انجام دهند تا پالیسی‌ها و طرزالعمل‌های ملی واقعی را بررسی کنند.

نتایج یادگیری

شاگردان قادر خواهند بود که

- اهمیت و تأثیر احتمالی بهره‌جویی از زنجیره عرضه، دسترسی از راه دور، نزدیک و درونی جهت هدف قرار دادن آسیب‌پذیری‌های فضای سایبری و موارد مرتبط با تسهیل تحرک ارتقاءیافته را درک خواهند کرد، و
- انواع مبادلات امنیتی مرتبط با تحرک ارتقاءیافته و سایر حامل‌های خطر در این عرصه را تشخصیص خواهند داد.

مراجع پیشنهادی

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: زنجیره عرضه/حامل‌ها

شرح

این بخش به موضوع آسیب‌پذیری‌های زنجیره عرضه پرداخته و مفهوم عملکردهای خوب را برای مدیریت ریسک زنجیره عرضه (SCRM) تعریف می‌کند.

کل زنجیره عرضه یک آسیب‌پذیری شناخته شده است. نظارت و امنیت زنجیره‌های عرضه می‌تواند در بازار جهانی بسیار چالش برانگیز باشد. چالش‌های امنیتی زنجیره عرضه شامل یکپارچگی و تضمین کیفیت و امنیت، جلوگیری از ایجاد اختلالات، بهره‌جویی و حملات متعاقب می‌باشد. زنجیره‌های عرضه جهانی شامل مسیرهایی می‌باشد که توسط تجهیزات حساس از مرحله تولید تا حمل و نقل طی می‌شود، هم برای تک قطعات و هم برای محصولات ساخته شده مانند هاردویر و سافت‌ویر. زنجیره‌های عرضه در برابر اختلال آسیب پذیر هستند: ممکن است با عناصر مخرب مانع انتقال محصولات به مقصد شوند یا آنها را با کدهای مخرب در مراحل مختلف تولید، حمل و نقل، انبار، نصب یا تعمیر دستکاری کنند و معلومات ارزشمندی هنگام دسترسی از آن استخراج کنند. بنابراین، دستکاری می‌تواند در هر نقطه از چرخه حیات محصول رخ دهد. گره‌های دیگر زیربناهای سازمانی یا ملی نیز می‌توانند از طریق زنجیره عرضه یا حامل به خطر بیفتند و منجر به نقض غیرمعمول شوند. آیا ارائه کنندگان شما می‌توانند امنیت کافی را تضمین کنند؟ برای ایجاد امنیت در کل زنجیره عرضه چه باید کرد؟

نتایج یادگیری

شاگردان

- چالش‌های کلیدی مرتبط با چرخه حیات محصولات را از گهواره تا گور درک خواهند کرد؛
- قادر به توضیح نقش مدیریت پیکربندی (به عنوان مثال، طراحی سیستم‌ها) در رابطه با امنیت زنجیره عرضه خواهند بود؛
- نقش و الزامات پالیسی‌ها و روش‌های بیان شده برای مدیریت ریسک زنجیره عرضه را درک خواهند کرد.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

- آسیب‌پذیری‌های زنجیره عرضه در برابر جرایم اینترنتی و جاسوسی
- رویکردهای کاهش خطر و عملکردهای خوب
- پالیسی‌ها و روش‌های ملی کاهش خطر زنجیره عرضه

روش یادگیری/ارزیابی

روش‌های تدریس می‌تواند شامل لکچرها و مطالعات موردی در مورد تخلفات و پیامدها باشد.

تمرینات فردی: نمونه‌ای از تخلف/نقض زنجیره عرضه را بیابید و راه‌حل‌های ممکن را جهت رفع آن شناسایی کنید.

احتمال: از یک زنجیره عرضه نقشه برداری کنید و نواحی خطر را شناسایی کنید.

مراجع

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). British 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.

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

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

T2-B2: حملات از راه دور و حملات مبتنی بر دسترسی نزدیک

شرح

حملات سایبری می‌تواند یا به شکل حملات از راه دور یا به شکل حملات محلی انجام شود. با این حال، حمله محلی می‌تواند در رده حملاتی قرار گیرد که از طریق دسترسی نزدیک به سیستم‌ها یا از طریق یک فرد قابل اعتماد درونی انجام شود. حمله درونی به طور جداگانه در بخش T2-B3 بررسی می‌شود. دسترسی از راه دور به همه روش‌ها و رویکردهای استفاده شده برای دسترسی به شبکه‌ها یا ایجاد اختلال در آنها زمانیکه دسترسی فیزیکی آشکار به هاردویر سیستم وجود ندارد، گفته می‌شود. در یک حمله از راه دور، حمله‌کننده ممکن است دسترسی فیزیکی قبلی به سیستم تحت حمله را نداشته باشد: دسترسی حمله کننده از طریق شبکه یا سایر دستگاه‌های ارتباطی انجام می‌شود و ممکن است حمله کننده هیچ نوع امتیاز تثبیت شده قبلی در سیستم نداشته باشد. برعکس، در حملات محلی یک حمله‌کننده عموما دارای نوعی دسترسی یا امتیاز تثبیت شده به سیستم است و تلاش می‌کند تا سطح امتیاز خود را برای دسترسی غیرمجاز به معلومات افزایش دهد. چنین فعالیتی توسط یک بازیگر شرور که فرد قابل اعتماد درونی نیست انجام می‌شود که ما در این سند به عنوان حمله مبتنی بر دسترسی نزدیک معرفی خواهیم کرد. چابینسکی در سال 2010 توضیح می‌دهد که "حمله مبتنی بر دسترسی نزدیک" به توانایی یک بازیگر شرور در ایجاد اختلال، غیر فعال کردن یا دسترسی به شبکه‌ها و سیستم‌های کمپیوتری از جمله ایستگاه های کار، کیبل‌ها یا گیرنده‌های بی سیم زمانیکه به اجزای مختلف آن نزدیک است اشاره دارد. دسترسی نزدیک نوعی دسترسی از راه دور است. تکنیک‌های متداول مانند " اسنیفینگ" وایرلس یا اسنیفینگ بی سیم (قطع و دسترسی به معلومات ارسال شده از طریق شبکه‌های بی سیم)، ثبت کلیدهای زده شده کیبورد، جذب عکس از صفحه اسکرین، قطع دسترسی توسط مرد میانی و درج کد مخرب از طریق ابزارهای فیزیکی روش‌هایی هستند که حمله کنندگان می‌توانند به بهره‌جویی از آسیب‌پذیری‌ها از طریق حمله مبتنی بر دسترسی نزدیک استفاده کنند.

این بخش به بررسی حملات از راه دور و حملات مبتنی بر دسترسی نزدیک (حملاتی که درونی نیستند) می‌پردازد. هدف این بخش واضح نمودن رایج‌ترین خطرات شناخته شده مرتبط با حملات از راه دور و حملات مبتنی بر دسترسی نزدیک می‌باشد و در مورد روش‌های مختلف برای کاهش یا خنثی کردن چنین تلاش‌هایی بحث می‌کند.

پیشینه

در برنامه‌های کلاسیک شبکه، مفهوم کلاینت و سرور وجود دارد. یک اپلیکیشن سافت‌ویر "کلاینت" درخواست‌ها را مطابق با برخی از پروتکل‌ها به یک اپلیکیشن سافت‌ویر "سرور" به منظور درخواست معلومات یا انجام عملی ارسال می‌کند. کلاینت همیشه ارتباط را آغاز می‌کند. سرور همیشه منتظر است تا به برخی از آدرس‌های شناخته شده در شبکه تماس گرفته شود. پروتکل‌های کنترل کننده این رفتار شامل خدمات وب، پروتکل انتقال ابرمتن (HTTP) یا پروتکل امن انتقال ابرمتن (HTTPS)، خدمات انتقال فایل از طریق پروتکل انتقال فایل (FTP) و خدمات ایمیل توسط پروتکل ساده انتقال نامه (SMTP)، پروتکل اداره پست (POP3) یا پروتکل دسترسی به پیام های اینترنتی (IMAP) هستند. حمله از راه دور می‌تواند نقاط ضعف موجود در سرور (خطاهای سافت‌ویری یا پیکربندی) را هدف قرار دهد که به حمله‌کننده امکان دسترسی به معلومات یا حتی کنترل از راه دور کمپیوتر سرور را می‌دهد.

زمینه انجام حملات از راه دور سمت سرور زمانی فراهم می‌شود که حمله‌کننده بتواند یک پیکربندی اشتباه یا خطا را در سافت‌ویر پیاده‌سازی‌شده در سرور شناسایی کند، به عنوان مثال، یک خطا در تنظیمات پیکربندی می‌تواند به حمله کننده اجازه دهد تا وارد حالت اختصاصی برای تعمیر و نگهداری سیستم شود و در نتیجه دسترسی بسیار گسترده‌ای به سیستم پیدا کند. مثال دیگر حمله بر روی یک وب سرور HTTP است که از دیتابیس خادم (Back end database) بخشی از یک سیستم کمپیوتری که مستقیما با کاربر سروکار ندارد) برای تهیه منابع دیتا (data) استفاده می‌کند. درخواست‌های نامناسب صفحه وب از طرف حمله‌کننده که توسط سرور به خوبی ارزیابی نشده می‌تواند به حمله کننده اجازه دهد تا رشته فرمان خطرناک دیتابیس را به دیتابیس خادم در سرور منتقل کند. این امر می‌تواند کنترل دیتابیس را در اختیار حمله‌کننده قرار دهد. این الگوی حمله به نام "تزریق اس کیو ال (زبان اس کیو ال)" یاد می‌شود.

ظهور روشی برای محافظت بهتر از سرورها (توسط فایروال‌ها، کنترل دسترسی و غیره) کانون حمله را از سرور به اپلیکیشن‌های کلاینت سوق داده است. با این وجود امکان برقراری ارتباط مستقیم اپلیکیشن‌های کلاینت با شبکه وجود ندارد. اپلیکیشن‌های کلاینت همیشه آغازگر مبادلات ارتباطی هستند. در عوض، حمله‌کننده باید راهی برای فریب کاربر اپلیکیشن کلاینت پیدا کند تا با یک سرور مخربی که بتواند اپلیکیشن کلاینت را هنگام تبادله خراب کند ارتباط برقرار کند. فعالیت‌های فریب یا تله‌گذاری که به نام‌های مختلفی یاد می‌شوند، فعالیت‌های متفاوتی هستند که از اصول مهندسی اجتماعی برای ترغیب اپراتورها برای انجام رفتارهایی مانند باز کردن ضمایم ایمیل آلوده استفاده می‌کنند.

نتایج یادگیری

هدف اصلی این بخش اطمینان از آشنایی شاگردان با ساحه وسیع خطرات مرتبط با حملات از راه دور و حملات مبتنی بر دسترسی نزدیک می‌باشد.

شاگردان

- قادر به بحث و درک سناریوی حمله مبتنی بر دسترسی از راه دور، تشخیص اجزای تشکیل دهنده چنین حمله‌ای و مقایسه آن با سناریوهای حمله مبتنی بر دسترسی نزدیک خواهند بود؛
- با ساختار اپلیکیشن‌های مبتنی بر کلاینت-سرور و توپولوژی شبکه آنها آشنا خواهند شد و قادر به تشخیص پروتکل-های رایج مانند پروتکل انتقال ابرمتن (HTTP)، پروتکل امن انتقال ابرمتن (HTTPS)، پروتکل انتقال

فایل (FTP) و پروتکل‌های ایمیل متناسب با این مودل خواهند بود؛

- قادر به توضیح اینکه چگونه حملات سمت سرور از طریق یک مرحله جمع‌آوری استخباراتی با استفاده از تکنیک‌هایی مانند ابزارهای تجزیه و تحلیل آسیب‌پذیری شبکه اتخاذ می‌گردد و همچنین توضیح اینکه چرا ابزار تجزیه و تحلیل آسیب‌پذیری شبکه هم برای حمله‌کنندگان و هم برای مدافعین ارزشمند است؛
- شناخت ابتدایی در مورد سناریوهای حمله سمت سرور مانند بهره‌جویی از تنظیمات ضعیف، جعل پروتکل اینترنت یا IP، انکار از خدمات (DoS) و انکار از خدمات توزیع شده (DDoS)، تزریق اس کیو ال و سرریز بافر مبتنی بر پروتکل (protocol–based buffer overflows) شبکه خواهند داشت.
- قادر خواهند بود که نحوه تکامل امنیتی در محیط شبکه را تشریح کنند و اینکه چگونه بهبود در امنیت سرور منجر به انکشاف و گسترش تکنیک‌های حمله سمت کلاینت می‌شود را درک خواهند نمود؛
- شناخت ابتدایی راجع به سناریوهای حمله سمت کلاینت مانند اسکریپت‌نویسی از طریق سایت، جعل درخواست بین سایت، بهره‌جویی از مرورگر وب و اسناد تروجان (Trojan documents) خواهند داشت؛ و
- قادر به تشخیص و بحث در مورد رابطه بین حملات سمت کلاینت و تکنیک‌های مهندسی اجتماعی مانند حملات فیشینگ و واترینگ هول (watering hole) خواهند بود.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

- عمق پوشش تخنیکی می‌تواند با توجه به محدودیت زمانی و سابقه تخنیکی شاگردان بسیار متفاوت باشد.
- تحقیق در مورد انواع حملاتی که از روش‌های مهندسی اجتماعی استفاده می‌کنند.

روش یادگیری/ارزیابی

روش‌های تدریس می‌تواند شامل لکچرها و نمایشات باشد. پرزنتیشن‌های مدیران فعلی شبکه می‌تواند تهدیدات مستمر را بیان کند. مثال‌های واقعی ملی به منظور نشان دادن مسائل عملی و فوری باید تولید و شناسایی شود. اقدامات مختلف ارزیابی عملی باید بسته به سطحی که انتظار می‌رود شاگردان به آن برسند ایجاد شود.

مراجع

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.

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

T2-B3: دسترسی درونی (حملات مبتنی بر دسترسی محلی)

شرح

در یک حمله مبتنی به کمپیوتر به یک سیستم معلوماتی یا شبکه، حمله‌کننده از ضعف یک سیستم یا برنامه کمپیوتری برای انجام نوعی اقدام مخرب جهت به خطر انداختن محرمیت، یکپارچگی و در دسترس بودن معلومات بهره می‌گیرد. چنین "بهره‌جویی" می‌تواند یا از طریق حملات از راه دور و یا از طریق حملات محلی انجام شود. در حملات محلی، حمله کنندگان راه دسترسی به سیستم مورد حمله را قبلاً ایجاد کرده‌اند - یعنی آنها قبل از این برخی امتیازات روی سیستم دارند و سعی می‌کنند تا سطح امتیازات برای دسترسی غیرمجاز به معلومات را افزایش دهند. این بخش به حملات مبتنی بر دسترسی محلی می‌پردازد. افراد مخرب درونی که به طور فیزیکی به سیستم‌های مختلفی دسترسی دارند یا از آن استفاده می‌کنند می‌توانند موجب آسیب‌های جدی به یک عملیات، کمپنی یا سازمان شوند. آنها ممکن است این کار را برای پول، انتقام جویی یا بخاطر کینه‌ای که دارند و یا از نظر عقیدتی با سازمان مخالف هستند انجام دهند. اما، این امر همچنین ممکن است موجب خسارت یا اختلال مشابهی از طریق خطای اپراتور یا سهل‌انگاری دیگر شود.

پیشینه

"امتیاز" (privilege) در امنیت کمپیوتری عبارتست از مجوزی که جهت انجام عملی داده می‌شود. در این مورد، مجوز (permission) عبارت از حق دسترسی کاربران مشخص به منابع مشخص سیستم (مانند فایل‌ها یا اپلیکیشن‌ها) جهت استفاده از برخی دستورات سیستم یا دسترسی به خدمات مشخص (مانند دستگاه شبکه) است. به طور معمول پالیسی کنترل سطح امتیاز یک کاربر از طریق تأیید صحیح هویت الکترونیکی کاربر و بکارگیری مجموعه‌ای از قوانین کنترل دسترسی (پروتکل‌ها) حاکم بر اقدامات خواندن، نوشتن و اجرای برنامه کاربر روی سیستم کنترل می‌شود. حمله کننده ممکن است برای " افزایش امتیاز" و دسترسی به معلومات بیشتر سیستم از طریق در اختیار گرفتن هویت کاربری یک فرد دیگر (غالباً با تصاحب برنامه‌ای که با امتیاز بالاتر کاربری اجرا می‌شود) یا اصلاح پروتکل‌های تعبیه شده در پالیسی امنیتی تلاش کند. اگر حمله‌کنندگان از امتیاز کافی برخوردار شوند، می‌توانند کنترل اجرایی سیستم را بر عهده بگیرند. حمله کننده در چنین سناریویی ممکن است یک کاربر مجاز یک سیستم باشد - یک فرد مخرب درونی سعی در انجام اقدامات غیر مجاز دارد. متناوباً، حمله‌کننده می‌تواند یک فرد بیرونی (خارج از سازمان) باشد و یک حمله از راه دور را برای تصاحب اعتبارنامه یک کاربر که امتیازات محدودی دارد انجام دهد. سپس از این نقطه دسترسی، حمله‌کننده می‌تواند از اعتبارنامه سرقت‌شده برای انجام حمله محلی استفاده کند تا سطح امتیاز خود را افزایش دهد، بنابراین دسترسی گسترده‌تری پیدا می‌کند. از نظر تخنیکی، تفکیک بین این دو سناریو دشوار است، زیرا آنها عمدتا حملات مبتنی بر دسترسی محلی هستند و در بسیاری از تکنیک‌های تخفیف (mitigation techniques) شباهت‌هایی بین آنها وجود دارد.

یکی از اصول بنیادی مورد استفاده جهت محدود نمودن آسیب‌پذیری‌های حمله مبتنی بر دسترسی محلی، اصل "نیاز به دانستن" است که در آن کاربران فقط به معلومات لازم برای انجام وظایف رسمی خود دسترسی دارند. اصل "حداقل امتیاز" در طراحی و پیاده سازی پالیسی‌ها و قوانین کنترل دسترسی اعمال می‌شود تا اطمینان حاصل شود که کاربران تنها به منابعی که نیاز به دانستن آنها دارند دسترسی داشته باشند. این اصول شامل اصل "تفکیک وظایف" می‌شود - به عنوان مثال، اطمینان حاصل می‌شود که یک مدیر نمی‌تواند هم در پالیسی‌های امنیتی تغییراتی ایجاد کند و هم تغییرات را تأیید کند.

تقسیم‌بندی یک اصل کلاسیک جهت محدود نمودن تأثیرات حمله مبتنی بر دسترسی محلی است. زون بندی شبکه‌های امنیتی یک روش تقسیم‌بندی موثر است. از زون بندی شبکه برای کاهش خطرات توسط تقسیم خدمات زیربنایی به دسته‌های منطقی که پالیسی‌های امنیتی ارتباطی و الزامات امنیتی یکسانی دارند، استفاده می‌شود. زون‌ها توسط محیط امنیتی از طریق دستگاه‌های امنیتی و شبکه‌ای (فایروال‌ها، سیستم تشخیص نفوذ، سافت‌ویر پیشگیری از دست دادن دیتا) از هم جدا می‌شوند.

با توجه به آسیب‌پذیری‌های مختلف تشخیص داده شده در این بخش، منطق برنامه‌ها و طرز العمل‌های طراحی شده برای به حداقل رساندن آسیب‌پذیری‌های ذاتی دسترسی به سیستم با استفاده از رویکردهای پیشگیری، تشخیص و بازدارندگی باید پدیدار شود. این اقدامات بطورکاملتر در جاهای دیگر این نصاب تحصیلی بررسی خواهد شد.

نتایج یادگیری

شاگردان

- نشان خواهند داد که از تهدیدات سازمانی که ممکن است از طرف افراد داخل سازمان باشد آگاه هستند؛
- قادر به توصیف حمله مبتنی بر دسترسی محلی و تشخیص اجزای تشکیل دهنده چنین حمله‌ای خواهند بود؛
- قادر به توضیح تفاوت بین حمله مبتنی بر دسترسی از راه دور و حمله مبتنی بر دسترسی محلی خواهند بود؛
- نشان خواهند داد که مفاهیم مجوز و امتیازات و نحوه استفاده آن برای کنترل دسترسی کاربر به منابع معلوماتی یک سیستم را درک نمودند؛

- نشان خواهند داد راجع به تکنیک‌هایی که توسط حمله‌کنندگان جهت سوء استفاده از سطح امتیاز فعلی و افزایش امتیاز استفاده می‌شود شناخت اساسی دارند؛
- قادر به توضیح کاربرد اصول "حداقل امتیاز" و "نیاز به دانستن" و چگونگی استفاده از آنها برای ایجاد پالیسی امنیتی خواهند بود؛
- قادر به تشخیص اینکه چگونه پالیسی زون بندی شبکه‌های امنیتی برای تقسیم بندی معلومات مورد استفاده قرار می‌گیرد، خواهند بود.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

- پالیسی‌ها و برنامه‌های تعلیمی برای پرسنل، بررسی سوابق، کاهش تهدیدات و آگاهی عمومی از مشکلات ذاتی مرتبط با دسترسی فیزیکی به سیستم‌ها و اجزای آن باید از این بخش بیرون شود اما می‌تواند در سطوح مختلف جزئیات بررسی شود.
- استفاده از مثال‌های واقعی و ملی روش خوبی برای فراهم نمودن زمینه سهمگیری شاگردان در این موضوع است.
- ابزارهای مربوط به تشخیص وجود تهدیدات فعال در شبکه و تشخیص ویژگی‌های آنها را می‌توان مورد بحث قرار داد.

روش یادگیری/ارزیابی

لکچرها و نمایشات راجع به مثال‌ها توصیه می‌شود.

مطالعات موردی، مثال راجع به سناریوها و بررسی فارنزیک (جرم‌یابی قانونی دیجیتال) قضایای واقعی باید مورد بحث قرار گیرد.

تمرین پیچیده احتمالی: از شاگردان بخواهید که به صورت تیمی کار کنند، نمونه‌ای از یک حمله مخرب واقعی درونی را پیدا کنند و به تجزیه و تحلیل آن بپردازند و روش‌هایی که موجب جلوگیری از تهدیدات می‌شود را پیشنهاد کنند. شاگردان می‌توانند از نمونه‌ای که یک فرد مخرب درونی از امتیاز خود جهت بخطر انداختن منابعی که نیازی به دسترسی آنها ندارد استفاده کنند.

روش‌های ارزیابی به سطح دانشی که نیاز است شاگردان از خود نشان دهند مطابق با اهداف و عملکرد یادگیری مورد نظر برای کورس مشخصی که می‌توانند در آن شرکت کنند بستگی دارد.

مراجع

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 Arbeitnehmer-datenschutz, 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%B6suhe58tes%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

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 and 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

ورکشاپ تیم‌های تدوین‌کننده نصاب تحصیلی عمومی مرجع برای امنیت سایبری در گارمیش
(شرکت‌کنندگان از جمهوری چک، بریتانیا و ایالات متحده).

T2-B4: خطرهای تحرک، بیود (BYOD) و روندهای در حال ظهور

شرح

تبدیل شدن جامعه به ارتباطات سیار (مخابرات موبایل) یک پروسه برگشت‌ناپذیر است که تبعات امنیتی آن به خوبی درک نشده است. بعلاوه، ظهور رسانه‌های اجتماعی مانند فیس‌بوک و توییتر در حال دگرگونی ارتباطات بین فردی و جهانی است. ردپای دیجیتال افراد و سازمان‌ها، دسترسی توزیع شده از دستگاه‌های شخصی ناامن به سیستم‌هایی که ممکن است به سیستم‌های امن متصل باشد، حامل‌های تجارتی و مجموعه‌ای از تحولات مشابه و جدید خطراتی را برای داده‌ها/دیتا و سیستم‌های حساس ایجاد می‌کند. به عنوان مثال، از دست دادن یا سرقت معلومات یک لپ‌تاپ یا موبایل با تماس الکترونیکی، اسناد یا میانبرها می‌تواند به یک فرد، سازمان، شرکت یا یک کشور آسیب برساند. این بخش به مسائل امنیتی مرتبط با این روندها می‌پردازد.

"دستگاه خود را بیاورید" (Bring Your Own Device) به پالیسی اشاره دارد که به کارمندان اجازه می‌دهد تا دستگاه‌های سیار خود را (لپ تاپ، تبلت و موبایل) به محل کار خود آورده و از این دستگاه‌ها برای دسترسی به معلومات و اپلیکیشن‌های محرمانه در جریان کار خود استفاده کنند. این پالیسی باعث ایجاد تضاد بین سازمان و کارمندان می‌شود زیرا از یک طرف سازمان پالیسی‌های امنیتی را برای کنترول محرمیت و سلامت منابع معلوماتی طراحی کرده است و از طرف دیگر کارمندان مایل به حفظ مالکیت دستگاه‌ها و معلومات شخصی خود هستند و نمی‌خواهند دستگاه‌ها و معلومات شخصی آنها تحت نظارت و کنترول باشد. سازمان‌ها باید پالیسی‌ها و روش‌هایی را برای موقعیتی که کارمند وظیفه خود را ترک می‌کند یا هنگامی که دستگاهی مفقود می‌شود، به سرقت می‌رود یا فروخته می‌شود تعیین کنند و اطمینان حاصل کنند که حمله‌کنندگان نمی‌توانند از این دستگاه‌های ناامن برای دسترسی به سیستم‌های سازمانی استفاده کنند. استفاده از "ابر" یا فضای ذخیره سازی ابری (cloud for storage of data) برای ذخیره داده‌ها/دیتا مشکلات مشابهی در زمینه کنترول دسترسی و پیکربندی (کانفیگوریشن) به وجود می‌آورد.

پیشینه

یک روش امنیتی معمول برای سازمان‌ها، ساخت دقیق یک ساختار امنیتی زون‌بندی شده و تهیه "نقاط انسداد" کنترل‌شده جهت مدیریت دسترسی به اینترنت می‌باشد. پالیسی بیود (BYOD) برای دستگاه‌های فعال اینترنت نقاط دسترسی جدیدی را معرفی می‌کند که احتمالاً تحت کنترل پالیسی امنیتی سازمان نیستند. این یکی از اصول اساسی امنیت کمپیوتری است که در سیستم‌های کمپیوتری که به طور معمول یکپارچگی یا سلامت لایه‌های پایینی توسط لایه‌های بالایی تامین شده پنداشته می‌شود. این از اجراء پالیسی‌های امنیتی روی دستگاه‌های شخصی اپلیکیشن‌های سازمان‌ها جلوگیری می‌کند یعنی آن اپلیکیشن‌هایی که توسط شخصی که سیستم عامل "بیود" را کنترول می‌کند یعنی مالک نمی‌تواند تضعیف گردد. به عبارت دیگر، سیستم‌های امنیت سازمانی (اپلیکیشن‌ها و غیره) بر روی دستگاه‌های شخصی ممکن است به طور مداوم نصب نشوند، زیرا مالک نهایتاً کنترل اجرایی دستگاه را حفظ می‌کند. یک دستگاه ناامن، مانند تلفن هوشمند شخصی، نمی‌تواند با نصب ساده اپلیکیشن‌های امن یا ابزارهای امنیتی ایمن شود. روش‌های زیادی وجود دارد که می‌تواند دستگاه‌های شخصی را ایمن‌تر کند یا خطرات موجود در آنها را کاهش دهد. این روش‌ها برای محدود کردن دسترسی دستگاه به شبکه سازمانی و انتقال معلومات به دستگاه، به یک معماری امنیتی متکی می‌باشد. پالیسی‌های زون‌بندی که زمینه تقسیم بندی و جداسازی را فراهم می‌کند می‌تواند پیاده سازی تحرک قوای کار و امنیت استراتژی سیستم‌های بیود را نیز نسبتا تامین کند. با این حال، راه‌حل‌های ایمن‌تری وجود دارد که در تضاد با استفاده از دستگاه‌های شخصی می‌باشد.

علاوه بر این، حرکت به سمت استفاده از زیربنایی که به عنوان خدمات از طریق تکنالوژی‌های ابری فراهم می‌شود منجر به از دست دادن بالقوه کنترل اساسی معماری امنیت سازمانی و شیوه‌های امنیتی می‌شود. دستگاه‌های موبایل خود جریان‌های داده‌ای/دیتا ایجاد می‌کند که می‌تواند مورد توجه سازمان‌های استخباراتی خارجی و نهادهای تجارتی باشد. همچنین استفاده از رسانه‌های اجتماعی افراد را در معرض بهره‌جویی از معلوماتی که در دستگاه‌های موبایل خود باز، قابل دسترسی یا ذخیره کرده‌اند قرار می‌دهد و معلومات زیادی درباره روابط، عقاید، مکان‌ها و عادات در معرض خطر قرار می‌گیرد. همچنین رسانه‌های اجتماعی می‌توانند به عنوان مسیرهای تهدید عمل کنند و به عنوان مجرای ورودی به سیستم‌های مختلف تکنالوژی معلوماتی، آنها را در معرض خطر آلودگی یا نفوذ قرار دهند. علاوه بر این، رسانه‌های اجتماعی می‌توانند برای اشاعه تبلیغات و معلومات نادرست، جمع‌سپاری، پیام‌رسانی جمعی برای بسیج مردم و فعالیت‌های مشابه مورد استفاده قرار گیرند.

نتایج یادگیری

شاگردان

- نشان خواهند داد که جنبه‌های مثبت و منفی (مزایا و معایب) پالیسی امنیتی مرتبط با استفاده از رسانه‌های اجتماعی در محیط سازمان از دیدگاه کارمند و کارفرما را درک نمودند؛
- قادر به تجزیه و تحلیل پالیسی‌های تحرک و "دستگاه خود را بیاورید" در بستر معماری امنیت سازمانی و تشخیص مبادلات امنیتی و کاربردپذیری خواهند بود؛
- قادر به تجزیه و تحلیل پالیسی‌های محاسبات ابری با توجه به ذخیره سازی و پروسس معلومات (به عنوان مثال، سوابق صحی، دیتاهای حکومتی/نظامی) در بسترهای ملی و بین المللی خواهند بود.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

- توانایی بازیگران مخرب در سطح جزئیات مناسب برای مخاطبان خاص بررسی خواهد شد.
- بهبود آگاهی در مورد نیاز به سازگاری امنیت با تکنالوژی دایم التغییر.

- الزامات مشخص و محدودیت‌های پلتفرم‌های ارتباطات سیار، از جمله دستگاه شخصی خود را بیاورید.
- الزامات مشخص برای محدودیت‌های استفاده از ابر.
- استقرار و اتخاذ عملکردهای خوب در چارچوب سازمان بر اساس رهنمودهای ملی و بین‌المللی.
- بهره‌جویی از معلومات شخصی به اشتراک گذاشته شده در رسانه های اجتماعی - "آیا امروز خود را در گوگل جستجو کرده‌اید؟" بحث و تمرین.

روش یادگیری/ارزیابی

روش‌های تدریس می‌تواند شامل پرزنتیشن‌ها، بحث در صنف، گروههای کوچک و بحث در مورد مطالعات موردی باشد.

ارزیابی مداوم عملکرد و سهم گیری در صنف و بحث گروهی باید انجام شود.

مراجع

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 highlevel 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.

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

ویرایش‌کنندگان نصاب تحصیلی عمومی مرجع امنیت سایبری.

موضوع 3: سازمان‌ها، پالیسی‌ها و استندردهای بین‌المللی امنیت سایبری

هدف

هدف کلی این موضوع اینست که شاگردان را با استندردها و سازمانهای بین‌المللی مانند موسسه ملی استندردها و تکنالوژی ایالات متحده (NIST)، مؤسسه استندرد بریتانیا (BSI) (و احتمالاً سایر موارد) و شیوه‌هایی که از طریق آن به بسترهای ملی ارتباط می‌گیرد آشنا کند. شاگردان فرصت خواهند داشت که نقش نهادهای بین‌المللی استندردها را تشخیص داده و سازمان‌های عمده بین‌المللی را با نقش‌ها یا عملکردهای امنیت سایبری شناسایی نمایند. علاوه بر این، آنها باید پالیسی‌های ملی امنیت سایبری خود را در پرتو استندردهای بین‌المللی و عملکردهای خوب توصیه شده بررسی کنند و این امر را با مقایسه مثال‌های مختلف پالیسی‌های ملی خود انجام دهند. بالاخره اینکه، در ساحه این موضوع به بررسی رژیم‌های حقوقی در حال تکامل بین‌المللی در زمینه امنیت سایبری پرداخته خواهد شد.

شرح

هر کشور باید این بخش را با توجه به نیازهای خود تنظیم کند، نهادهای ملی مسئول پالیسی و شیوه‌های امنیت سایبری و نحوه تاثیر آنها بر پالیسی‌ها و سازمان‌های مرتبط با امنیت سایبری را شناسایی کند. اگرچه جزئیات مربوط به هر کشور متفاوت خواهد بود، اما رویکردی که برای ارائه این موضوع استفاده شده است می‌تواند این خطوط را دنبال کند. بخش T3-B1، سازمان‌های بین‌المللی امنیت سایبری و ارتباط آنها با بستر ملی؛ بخش T3-B2، استندردها و الزامات بین‌المللی - سروی نهادها و عملکردها؛ بخش T3-B3، چارچوب‌های ملی امنیت سایبری، هدف آن تجزیه و تحلیل چارچوب‌های ملی در مقایسه با سایر کشورها می‌باشد؛ و بخش T3-B4، امنیت سایبری در قوانین ملی و بین‌المللی.

نتایج یادگیری

امنیت سایبری یک مسئله امنیتی در حال رشد است که موجب شکل گیری واکنش‌های مختلف ملی و بین‌المللی در این زمینه در سازمان‌های موجود و جدید می‌شود. امنیت سایبری به عنوان یک مسئله ملی که در زمینه‌های دیگر هم مطرح شده است نیازمند پالیسی و هماهنگی در سطح بالایی است، اما پاسخ‌های ملی کاملاً متنوع بوده است.

از طریق بررسی شیوه‌های در حال ظهور دولت‌هایی که در حال تدوین پالیسی‌های ملی برای امنیت سایبری حکومتی، تجارتی و فردی هستند و از بازیگران غیردولتی در انکشاف سیستم‌ها جهت مدیریت خطرات و تهدیدات حمایت می‌کنند، شاگردان قادر خواهند بود که

- افزایش آگاهی لازم راجع به اینکه واکنش‌های ملی و بین‌المللی ایجاب نوعی رویکرد چند جانبه را نماید؛
- شناسایی اصلی‌ترین سازمان‌های ملی مسئول امنیت سایبری؛
- تعریف و درک نقش‌ها و نیازهای ادارات استندرد ملی و بین‌المللی؛
- درک اهمیت رابطه بین امنیت سایبری، استخبارات و نهادهای نظامی؛
- توانایی تجزیه و تحلیل عملکردها و پالیسی‌های ملی در پرتو استندردها و عملکردهای خوب بین‌المللی؛
- درک نقش سازمان‌های عمده بین‌المللی که در زمینه امنیت سایبری نقش مهمی ایفا می‌کنند؛
- آشنایی با چارچوب حقوقی در حال تکامل بین‌المللی و پالیسی ملی و مواضع رسمی حکومت در این رژیم درحال رشد.

مراجع پیشنهادی

European Union External Action, “EU International Cyberspace Policy”. http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

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: سازمان‌های بین‌المللی امنیت سایبری

شرح

تعداد سازمان‌های بین‌المللی، حکومتی و غیرحکومتی مربوط به مسائل جهانی یا منطقوی امنیت سایبری زیاد و در حال رشد است. علاقه‌مندی آنها از تحقیق تا تنظیم مسائل حقوقی، حمایت از پالیسی، نظارت و یک رشته زمینه‌های دیگر را در بر می‌گیرد. بیشتر این سازمان‌ها در راستای رویکردهای جمعی برای حل چالش‌های سایبری فعالیت می‌کنند در حالی که شماری دیگر اهداف ملی یا تجارتی را تقویت می‌کنند. توصیه‌های متنوع آنها باید به دلایل مختلف به بطور اساسی بررسی شود.

وب سایت https://ccdcoe.org/ که توسط مرکز تعالی همکاری سایبری ناتو (CCD COE) حمایت می‌شود منبع خوبی برای وصل شدن به ادارات مختلف منطقوی در ارتباط با شیوه‌ها و پالیسی‌های امنیت سایبری است که از جمله شامل اتحادیه اروپا، به ویژه کار با اداره امنیت سایبری اتحادیه اروپا ENISA (https://www.enisa.europa.eu/) سازمان امنیت و همکاری اروپا OSCE (http://www.osce.org/) سازمان ملل (http://www.un.org/en/index.html)، و ناتو (http://www.nato.int/) می‌باشد.

علاوه بر این منابع اداراتی مانند مجمع جهانی تیم‌های امنیتی و پاسخگوی حوادث (www.first.org)، مشارکت چند جانبه بین‌المللی در برابر تهدیدات سایبری (IMPACT)، و انجمن ارتباطات و الکترونیک قوای مسلح (AFCEA) وجود دارد. اداره امنیت سایبری اتحادیه اروپا از سازمان‌های پاسخگوی بحران‌های سایبری یا تیم‌های عکس‌العمل سریع سایبری (CERTs) کشورهای عضو اتحادیه اروپا حمایت و آنها را به طور منظم به روزرسانی می‌کند.

سایر نهادهای بین‌المللی مرتبط با امنیت سایبری عبارتند از: سازمان بین‌المللی استندردسازی (در بخش 2 این موضوع بحث شده است)، شرکت اینترنتی برای نام‌ها و اعداد تخصیص داده شده (ICANN)، مجمع حاکمیت اینترنت (IGF) و اتحادیه بین‌المللی مخابرات (ITU) که مورد حمایت سازمان ملل می‌باشد.

این بخش بر نحوه تعامل حکومت‌ها با بسیاری از سازمان‌های بین‌المللی و اتخاذ شیوه‌های معمول که اغلب براساس توصیه‌های آنها است متمرکز می‌باشد.

نتایج یادگیری

تا جایی‌که به امنیت سایبری ارتباط می‌گیرد، شاگردان قادر خواهند بود:

- چالش‌های مختلف تاثیرگذار بر حکومت‌ها و تعاملات آنها را با سازمان‌های بین‌المللی بیان کنند؛
- شناسایی سازمان‌های عمده بین‌المللی، تمرکز پالیسی‌ها و نقش آنها در معرفی و حمایت از امنیت سایبری ملی؛
- شناسایی سازمان‌های ملی مسئول همکاری و مشارکت بین‌المللی.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

از یک متخصص موضوعی ملی باید جهت شناسایی نهادهای عمده بین‌المللی که کشورش جهت راهنمایی گرفتن به آن متکی است و از طریق آن نهادها نگرانی‌های خود را بیان می‌کند استفاده شود.

موضوعات دیگری که می‌تواند بررسی شود شامل موارد زیر است:

- نهادهای عمده بین‌المللی برای معرفی عملکردهای ملی: اتحادیه اروپا، ناتو، حکومت ایالات متحده (رهبری سایبری و غیره) و یوروپول (به‌سایت www.europol.europa.eu/ec3 **مراجعه کنید**)
- چگونه منافع ملی با سازمان‌های بین‌المللی و اهداف آنها مواجه می‌شود
- شناسایی جنبه‌های مثبت و منفی رویکردهای نظارتی و سازمانی بین‌المللی در عرصه امنیت سایبری
- راهکارها و مکانیزم‌های ملی برای حل چالش‌های بین‌المللی
- از اینترنت برای مقاصد جنایی/تروریستی/جرایم سازمان یافته فراملی استفاده می‌شود

روش یادگیری/ارزیابی

روش‌های تدریس می‌تواند شامل تجزیه و تحلیل مسائل موجود باشد. شاگردان باید مطالعات موردی را در مورد پاسخ‌های سازمانی بین‌المللی تحقیق و بررسی کنند و چالش‌های بین‌المللی شایع و تأثیر آنها را روی کشورها بررسی کنند.

ارزیابی باید از طریق یک پروژه گروهی به همراه سهم گیری در صنف و یک تمرین تحریری روی پاسخ یک سازمان بین‌المللی در زمینه امنیت سایبری باشد.

مراجع

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

علاوه بر منابع وبی که قبلاً ذکر شد، به موارد زیر مراجعه کنید:

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

T3-B2 استندردها و الزامات بین‌المللی - سروی نهادها و عملکردها

شرح

این بخش شاگردان را با مجموعه استندردهای بین‌المللی که توسط سازمان‌های تنظیم‌کننده استندردها مشخص شده است آشنا می‌کند. شاگردان نقش استندردها و الزامات تخنیکی بین‌المللی را درک خواهند کرد. آنها همچنین با استندردهای مختلفی از جمله شامل سازمان بین‌المللی استندردسازی (ISO)، کنترول اهداف و معلومات مربوط به تکنالوژی (COBIT)، انجمن حسابرسی و کنترل سیستم‌های معلوماتی (ISACA)، و کتابخانه بین‌المللی زیربنایی تخنیکی (ITIL) آشنا خواهند شد. مباحث شامل موسسه ملی استندردها و تکنالوژی ایالات متحده (NIST)، مؤسسه استندرد بریتانیا (BSI)، دفتر فدرال امنیت سایبری آلمان (Germany's Bundesamt für Sicherheit in der Informationstechnik)، انجمن امنیت صنعتی آمریکا (ASIS) (و در صورت امکان سایر استندردها) برای برجسته‌سازی روش‌ها و مسئولیت‌های ایجاد شده از طریق اجرای استندردها و چالش‌های ارائه شده توسط استندردهای رقابتی خواهد بود. به علاوه، این بخش رویکرد ملی را برای همسویی با استندردهای بین‌المللی برجسته می‌سازد. نهایتا، این بخش به محدودیت استندردها می‌پردازد و دلایلی را که بخاطر آن سازمان‌های نظامی، دفاعی یا سایر سازمان‌های حکومتی ممکن است استندردهای خاص خود را تنظیم کنند بررسی می‌کند.

نتایج یادگیری

شاگردان قادر خواهند بود

- درک نقش استندردهای (بین‌المللی) و الزامات تخنیکی بین‌المللی؛
- شناسایی سازمان‌های بین‌المللی تنظیم‌کننده و انکشاف استندردها (مانند ISO و NIST)؛
- شناسایی منابع استندردهای بین‌المللی مرتبط با استراتژی ملی سایبری کشورشان؛
- درک چالش‌ها و پیچیدگی‌های مربوط به اجرای استندردهای بین‌المللی؛
- درک اینکه چگونه و توسط کدام نهاد استندردهای امنیت سایبری سازمان آنها تاسیس، نگهداری و اعلام شده است.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

می‌تواند شامل موارد زیر باشد:

- استندردهای ملی و استندرهای بین‌المللی پذیرفته شده در سطح ملی که مستقیماً به بررسی امنیت سایبری می‌پردازد
- استندردهای سازمانی یا کارشیوه‌های ملی مربوطه
- چالش‌ها و پیچیدگی‌های مرتبط با اجرای استندردهای بین‌المللی

روش یادگیری/ارزیابی

ابزارها و روش‌های ارزیابی باید متناسب با سطح عملکرد تعیین شده برای کورس‌ها و دروس نشأت گرفته از این نصاب تحصیلی مرجع باشد.

یک متخصص ملی استندردهای مختلف تصویب شده توسط یک کشور را به‌طور مختصربیان کرده و رابطه آن را با استندردهای بین‌المللی و در حال ظهور امنیت سایبری توضیح خواهد داد.

شاگردان می‌توانند مطالعات موردی را در مورد اجرای استندردهای بین‌المللی شناسایی و تجزیه و تحلیل کنند.

بحث‌های گروهی باید روی چالش‌های اجرای استندردهای بین‌المللی صورت گیرد. مثال‌ها را باید از روی تجربه محلی تهیه کرد.

مراجع

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).

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: 106. doi:10.3233/978-1-61499-372-8-97

یک سری استندردهای دیگر (علاوه بر ISO 27000):

- ISO 9000 (مدیریت کیفیت)
- ISO 22300 (مدیریت تداوم تجارت)
- ISO 31000 (مدیریت ریسک)
- BSI PAS 555

T3-B3: چارچوب‌های ملی امنیت سایبری

شرح

امنیت سایبری به عنوان یک مسئله ملی که مرزهای سنتی بین حکومت، صنعت و شهروندان را پشت سر گذاشته نیاز به پالیسی و هماهنگی سطح بالایی دارد. با توجه به بهم پیوستگی سیستم‌ها، بسیاری از حکومت‌ها تشخیص داده‌اند که فقط برای مدیریت امنیت سیستم‌های عامل خود به یک رویکرد تمام حکومتی احتیاج دارند، چه رسد به اینکه بخواهند برای کاهش خطرات به صنعت و افراد کمک کنند. اما پاسخ‌های ملی کاملاً متنوع بوده است. برخی از کشورها نهادهایی ایجاد کرده‌اند که مسئولیت مدیریت امنیت سایبری ملی را بر عهده دارند، درحالیکه کشورهای دیگر نهادهای هماهنگ‌کننده‌ای ایجاد کرده‌اند که مسئولیت تدوین پالیسی‌های ملی را بر عهده دارند اما مدیریت و اجرای پالیسی‌ها را به سازمان‌های مختلف حکومتی واگذار کرده‌اند. سایر کشورها برای یافتن چارچوبی مناسب هنوز هم تلاش می‌کنند.

بسیاری از حکومت‌ها فقط برای محافظت از دستگاه اداری حکومت از ایجاد و حمایت از اقدامات امنیت سایبری فراتر رفته و این مسئله را به عنوان یکی از خطرات ملی پذیرفته‌اند، بنابراین تلاش می‌کنند که از عمکردهای خوب برای سکتور خصوصی و شهروندان پشتیبانی کنند. پشتیبانی یا اجرای چنین اقداماتی به ویژه در مورد محافظت از زیربناهای حیاتی که اغلب در مالکیت خصوصی می‌باشد پابرجا بوده است. با این وجود، برخی از الزامات مشترک وجود دارد، مانند ایجاد نقش‌های ساختاری و حسابدهی، صدور رهنمود معتبر تخنیکی، تعریف نقش‌ها و مسئولیت‌ها برای کاهش خطرات و پاسخ به مسائل فعال.

هدف این بخش آگاه نمودن شاگردان از پالیسی‌ها، استراتژی‌ها و ساختارهای امنیت سایبری کشورشان است. شاکردان باید از چارچوب پالیسی و استراتژی کشور خود (در صورت وجود) و همچنین از سازمان‌هایی که مسئولولیت رهنمود ملی و مشخصات تخنیکی را بر عهده دارند مطلع شوند. شاکردان برای درک بهتر اسناد کشورخود و ارزیابی زمینه‌های خطر و مسئولیت‌ها، اسناد و رویکردهای مختلف استراتژی ملی و بین‌المللی امنیت سایبری را مقایسه خواهند کرد.

نتایج یادگیری

شاگردان قادر خواهند بود

- شناسایی سازمان‌هایی که مسئولیت پالیسی ملی امنیت سایبری را بر عهده دارند؛
- شناسایی ویژگی‌های کلیدی پالیسی امنیت سایبری؛
- شناسایی سازمان‌های مسئول و درک نقش آنها در زمینه انکشاف و صدور رهنمودهای تخنیکی؛
- شناسایی ویژگی‌های کلیدی رهنمودهای تخنیکی؛
- بحث راجع به منابع عملکردهای خوب در زمینه سازماندهی امنیت سایبری ملی؛
- رویکرد ملی را در مقایسه با چارچوب‌های پالیسی مرجع به بطور اساسی تجزیه و تحلیل کنند.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

- رویکرد متمرکز در مقابل رویکرد چند جانبه برای امنیت سایبری
- رویکردهای ملی همکاری، هماهنگی و همیاری
- سازمانهای بین المللی: نقش و تعامل در بستر ملی
- چارچوب‌های پالیسی مرجع– مثال‌های مختلف را مرور کنید

روش یادگیری/ارزیابی

ابزارها و روش‌های ارزیابی باید متناسب با سطح عملکرد تعیین شده برای کورس‌ها و دروس حاصله از این نصاب تحصیلی مرجع باشد.

روش‌های تدریس می‌تواند شامل بحث، لکچرهای متخصصین موضوعی، مطالعات موردی مقایسه‌ای، تشخیص عملکردهای خوب و بازدید از نهادهای محلی امنیت سایبری باشد.

مراجع

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.

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

T3-B4:امنیت سایبری در قوانین ملی و بین المللی

شرح

دورنما و چشم انداز حقوقی امنیت سایبری پیچیده و به سرعت در حال تغییر است. استدلال‌هایی در ارتباط با کاربرد قوانین بین‌المللی و ملی موجود و در حال رشد جهت رسیدگی به موضوعات و چالش‌های امنیت سایبری وجود دارد. در قوانین داخلی نیز تنوع گسترده‌ای در مورد چگونگی رسیدگی کشورها به موضوعات امنیت سایبری وجود دارد. بعضی از کشورها قوانین خاص سایبری دارند، در حالی که شماری دیگر این قوانین خاص را ندارند. چالش انتساب - مشکلات مرتبط با جستجو یا ردیابی منبع فعالیت‌های سایبری مخرب، تهدیدآمیز یا غیرقانونی - مشکلات را در عرصه داخلی و بین المللی پیچیده‌تر می‌کند.

مطالب زیادی در مورد قوانین بین‌المللی و ملی مرتبط با امنیت سایبری وجود دارد. این بخش شاگردان را با قوانین مختلف بین‌المللی و ملی امنیت سایبری آشنا می‌کند. بسیاری از کشورها و سازمان‌ها تابع قوانین انطباقی هستند، مانند مواردی که نیاز به گزارش انواع خاصی از معاملات مالی یا نقض داده‌ها/دیتا دارد. همچنین هنجارها و رفتارهای بین‌المللی در حال تکامل در رابطه با حقوق و انفاذ آن وجود دارد (مانند رژیم های همکاری که توسط اینترپل ایجاد شده است). الزامات حقوقی برای گزارش حوادث سایبری توسط بسیاری از کشورها پذیرفته شده است و تلاش وافری در زمینه تعیین اصول بین‌المللی اخلاق سایبری در حال انجام است. اما هیچ نهاد یا سازمان بین‌المللی وجود ندارد که بر جنبه‌های حقوقی امنیت سایبری نظارت کند.

شاگردان با تأکید بر امنیت سایبری با مواضع ملی قوانین داخلی و بین‌المللی فضای سایبری آشنا می‌شوند. جنبه‌های مهم داخلی عبارتند از: حریم خصوصی، اطمینان از سیستم‌ها، اهمیت انطباق مقررات و الزامات بیمه تجارتی در رژیم‌های حقوقی ملی و بین‌المللی در حال رشد.

نتایج یادگیری

شاگردان قادر خواهند بود

- آگاهی از چالش‌های کلیدی و منابع پایسی در قوانین بین‌المللی سایبری؛
- مسئولیت‌های حقوقی جوانب ذیدخل و قوانین امنیت سایبری ملی را توضیح خواهند داد؛
- از قوانین مصوبه ملی در خصوص امنیت سایبری (در صورت وجود) آگاهی داشته و مراجع اصلی حقوقی در سازمان مربوطه را شناسایی خواهند کرد.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

- موضوعاتی مانند وضعیت حقوقی بین‌المللی مورد منازعه حملات سایبری به رهبری بازیگران دولتی و غیر دولتی، مسائل سایبری در قوانین داخلی، الزامات انطباقی سازمانی و مسئولیت حقوقی فردی می‌تواند به طور کامل‌تر بررسی شود.
- بررسی بحث راجع به منشور اخلاقی بین‌المللی برای امنیت معلومات که در سازمان ملل مطرح شده است.
- مقررات انطباقی داخلی
- بیمه تجارتی و مسئولیت در قبال خطرات سایبری

روش یادگیری/ارزیابی

لکچرها باید با هماهنگی نمایندگان حقوقی مسئول که بتوانند قاطعانه در مورد موضع ملی خود صحبت کنند تدوین شود.

مطالعات موردی روی پاسخ‌های حقوقی بین‌المللی و ملی در زمینه حوادث امنیت سایبری باید بررسی شود.

یک امتحان کوتاه کتبی متناسب با جزئیات تدریس شده به عنوان یک ابزار ارزیابی باید تهیه شود.

مراجع

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.

موضوع 4: مدیریت امنیت سایبری در بستر ملی

هدف

هدف اصلی این موضوع بررسی روش‌های مدیریت امنیت سایبری در بستر ملی است.

شرح

رویکردهای مدیریت مسائل امنیت سایبری ملی در بین کشورها بسیار متفاوت است. درحالی‌که ممکن است چالش‌ها و پاسخ‌ها جزء به جزء متفاوت باشد، لذا مشکلات کلی در کشورها یکسان است. چارچوب‌های ملی امنیت سایبری ممکن است از نظر مشخصات متفاوت باشد، اما یک رژیم جامع اغلب شامل موارد زیر است که نیاز به مدیریت و هماهنگی فعال دارد: (1) مدیریت دارایی فیزیکی تکنالوژی معلوماتی؛ (2) مدیریت کنترول‌ها؛ (3) مدیریت پیکربندی سیستم و تغییر آن؛ (4) تشخیص و مدیریت آسیب‌پذیری؛ (5) مدیریت حوادث؛ (6) مدیریت تداوم خدمات؛ (7) شناسایی تهدیدات و مدیریت آنها؛ (8) مدیریت وابستگی‌ها و پیوندها خارجی؛ (9) تعلیمات و آگاهی؛ و (10) حفظ آگاهی مبتنی بر وضعیت.[7]

این موضوع به بررسی عمیق شیوه‌های ملی مدیریت امنیت سایبری می‌پردازد و آمادگی امنیت ملی را در چارچوب خطرات مورد بررسی قرار می‌دهد. مخصوصاً بخش T4-B1، (شیوه‌ها، پالیسی‌ها و سازمان‌های ملی برای تاب آوری سایبری) پلاگذاری احتیاطی و بازیابی حوادث سایبری جهت به حداقل رساندن حوادث سایبری را بررسی می‌کند. بخش T4-B2، (چاچوب‌های ملی امنیت سایبری) روش‌های ملی مدیریت امنیت سایبری را معرفی می‌کند که شامل عملیات، واکنش به حوادث و کاهش خطرات است. بخش T4-B3، (فارنزیک سایبری) آن دسته از روش‌ها، طرزالعمل‌ها و ابزارهای فارنزیک که جهت جمع آوری، تجزیه و تحلیل و تفسیر داده‌ها/دیتا (data) برای انتساب و استخبارات استفاده می‌شود را به شاگردان تدریس می‌نماید. بخش T4-B4، (تفتیش و ارزیابی امنیت در سطح ملی) شاگردان را با عملکردهای خوب در ارزیابی آمادگی ملی امنیت سایبری آشنا می‌کند.

نتایج یادگیری

شاگردان

- رویکرد سیستم‌ها به پلانگذاری برای تاب آوری در برابر تهدیدات، حملات و حوادث مشابه را درک خواهند کرد؛
- قادر به قرار دادن شیوه‌های بکارگیری سیستم‌های تاب آور در بستر ملی خواهند بود؛
- قادر به تجزیه وتحلیل سودمندی چارچوب‌ها و ساختارهای پلانگذاری و تفویض اختیار خواهند بود؛
- نشان خواهند داد که انواع معمول سازمان‌های پاسخگوی ملی را درک نمودند و با نقش، صلاحیت‌ها و ساختار سیستم‌های ملی موجود و سازمان‌های مدیریت حوادث و بهران سازمانی آشنا هستند.

مراجع پیشنهادی

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] بر گرفته از Carnegie Mellon CERT-RMM.

T4-B1:شیوه‌ها، پالیسی‌ها و سازمان های ملی برای تاب آوری سایبری

شرح

امنیت سایبری از مرزهای سازمانی بسیاری از کشورها فراتر رفته است. تعدادی از کشورها یک رویکرد جامع تمام حکومتی را برای تعریف نقش‌ها و مسئولیت‌های مدیریت تاب آوری سایبری قبول کرده‌اند. هدف تاب آوری سایبری اینست که زیربناهای ملی سایبری در وضعیت بحرانی همچنان در حالت عملیاتی باقی بمانند و پس از ایجاد اختلال به سرعت و به طور موثر به بازیابی بپردازند. این بخش با در نظر گرفتن موضوع تاب آوری سایبری به روش‌های ملی و سازمانی در یک بستر تطبیقی پرداخته است.

در این بخش شاگردان با چندین نمونه از رویکردهای جامع راجع به امنیت‌سایبری که در رهنمود منتشر شده سطح بالا بیان شده است (مانند رهنمود بریتانیا یا ایالات متحده) آشنا می‌شوند تا توانایی تجزیه و تحلیل نقاط قوت و ضعف پالیسی‌های ملی خود را داشته باشند. پالیسی‌های ملی که به شاگردان مربوط می‌شود مقایسه خواهد شد. مخصوصا، بحث باید به سمت بررسی پالیسی‌ها و روش‌های موجود با هدف جلوگیری، محافظت، واکنش و مدیریت بازیابی حوادث سایبری تغییر کند. اقداماتی مانند تفتیش، تایید و ابزارهای بررسی مستقل نیز باید مورد توجه قرار گیرد.

نتایج یادگیری

شاگردان

- قادر به تفسیر اسناد ملی تاب آوری سایبری خواهند بود؛
- قادر به همکاری در انکشاف و گسترش طرزالعمل‌های ملی تاب آوری سایبری خواهند بود؛
- توانایی تشریح نقش و مسئولیت‌های افراد و سازمان‌های مسئول تاب آوری سایبری ملی را خواهند داشت؛
- قادر به درک چالش‌های هماهنگی عملیات سایبری در وضعیت‌های بحرانی خواهند بود؛
- قادر به درک پروسه‌های تجزیه و تحلیل تصمیم که در تصمیم‌گیری انطباقی در وضعیت‌های بحرانی استفاده می‌شود خواهند بود.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

یک متخصص موضوعی ملی باید پالیسی‌های ملی موجود را تجزیه و تحلیل کند تا معلومات مناسبی را برای استفاده در پلان‌های درسی بیرون کند.

روش یادگیری/ارزیابی

روش‌های تدریس در این بخش می‌تواند شامل لکچرها، نمایشات، بازدید حضوری و تمرینات کتبی باشد. ارزیابی باید متشکل از تایید کتبی و شفاهی باشد.

مراجع

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.

یک متخصص موضوعی باید پالیسی‌ها و مراجع ملی مناسب را جمع‌آوری کند. منابع عمومی‌تر عبارتند از:

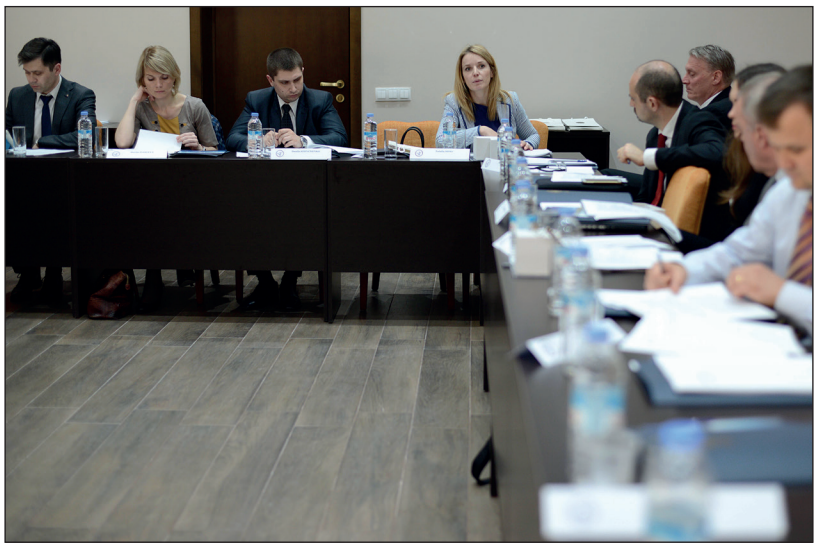
Deborah J. Bodeau and D.J. Graubart, *Cyber Resiliency Engineering Framework,* MITRE Technical Report MTR 110237 (Bedford, MA: The MITRE Corp.), September 2011.

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



ورکشاپ تیم‌های تدوین‌کننده نصاب تحصیلی عمومی مرجع برای امنیت سایبری در تبلیسی.

T4-B2:چارچوب‌های ملی امنیت سایبری

شرح

این بخش زمینه درک استراتژی ملی امنیت سایبری و اجرای آن را در زمینه مدیریت عملیات سایبری، رسیدگی به حوادث امنیت سایبری و مدیریت خطرات ملی امنیت سایبری در سطح ملی برای شاگردان فراهم می‌کند. تمرکز باید بر روی چارچوب‌هایی باشد که به تخصیص منابع، تعریف نقش‌ها و مسئولیت‌های سازمانی و تعیین اقدامات در امتداد زنجیره فرماندهی با توجه به مسئولیت‌پذیری و گزارش‌دهی کمک کند.

این بخش بر اساس استندردهای بین‌المللی و ملی به مبانی و چارچوب‌های امنیتی می‌پردازد و همچنین برای تعریف نقش‌ها و مسئولیت‌های مدیریت خطرات امنیت سایبری و پاسخگویی به حوادث آن چارچوب‌های جامع مختلفی را بررسی می‌کند. چنین چارچوب‌هایی اغلب در قالب ماتریس تفویض مسئولیت، حسابدهی، فرماندهی و معلومات (RACI) خلاصه می‌شوند. ابزارهای تفویض برای مدیریت عملیات‌های امنیت سایبری نیز مناسب‌اند. به عنوان مثال چارت RACI برای الگوی تدریس استفاده می‌شود. شاگردان قبل از رسیدگی به ساختارهای ملی تفویض مسئولیت و حسابدهی با طرح کلی این ابزارها آشنا خواهند شد. در صورت امکان، ابزارهای پالیسی ملی (واقعی) جهت مدیریت چنین تفویض مسئولیت‌ها و وظایفی تشخیص و بررسی خواهد شد. این بحث به ابزارهای پشتیبانی از تصمیم، ابزارها و چارچوب‌های مدیریت ریسک و شیوه‌ها و مسئولیت‌های آن می‌پردازد. در نهایت، شاگردان چارچوب مدیریت تفویض شده امنیت سایبری را که توسط حکومت ملی یا حداقل توسط سازمان آنها قبول شده است را بررسی خواهند نمود.

تاب آوری سیستم‌های سایبری می‌تواند شامل فعالیت های زیر باشد: مدیریت دارایی، مدیریت کنترول‌ها، مدیریت پیکربندی سیستم و تغییر آن، مدیریت تهدیدات و آسیب پذیری‌ها، پلانگذاری و مدیریت تداوم خدمات، مدیریت وابستگی‌های خارجی، تعلیمات، آگاهی سازمانی و فردی و مدیریت فعال آگاهی مبتنی بر وضعیت.

نتایج یادگیری

شاگردان

- نشان خواهند داد که مفهوم ماتریس پلانگذاری و ماتریس تفویض مسئولیت را درک خواهند نمود؛
- قادر به بررسی مسائل کلی پیرامون اجرای استراتژی ملی امنیت سایبری آنها خواهند بود؛
- نحوه برقرای ارتباط با ساختارهای ملی سوق و اداره و پاسخ به حوادث را درک خواهند نمود؛
- قادر به درک مدیریت تفویض شده عملیات‌های سایبری در سطح ملی خواهند بود؛
- قادر به درک نحوه مدیریت خطرات سایبری در بستر پالیسی ملی خواهند بود؛
- قادر به درک جنبه‌های مثبت و منفی چارچوب‌های رسمی مدیریت منابع را که در بستر امنیت سایبری ملی اعمال می‌شود خواهند بود.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

موضوعاتی مانند سیستم RACI و یا ابزارهای مشابه ماتریس تفویض مسئولیت برای رسیدگی به حوادث و بازیابی و مدیریت پاسخ گویی می‌تواند بررسی شود.

روش یادگیری/ارزیابی

یک متخصص موضوعی ملی باید قبل از تشخیص جاییکه مراجع ملی و سازمانی و رهنمودهای واضح وجود دارد یک سروی مختصر از روش‌ها را طرح کند (مانند چارت RACI) سپس متخصص موضوعی می‌تواند مرتبط ترین مسائل مربوط به مشخصات شاگردان را تعیین کند.

طرح ارزیابی باید مطابق با سطح دانش و آشنایی شاگردان متناسب با کورسی که از این نصاب تحصیلی مرجع تهیه شده مهیا شود.

مراجع

IU. V. Nesteriak, (IUrii Vasyl'ovych). "Derzhavna informatsiina 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 Cyber-security Bureau". Online Presentation by the Cyber-security Bureau of Georgia, 2015. Available at: www./slideplayer.com/slide/9759466/

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

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.

T4-B3: فارنزیک سایبری

شرح

فارنزیک سایبری (Cyber forensics) با بکارگیری از تکنیک‌ها و روش‌های تحقیق و تجزیه و تحلیل برای جمع آوری، استفاده و حفظ شواهد دیجیتالی مورد استفاده قرار می‌گیرد. این حوزه فعالیت متشکل از فارنزیک دیجیتالی، فارنزیک هاردویری و فاکتورهای بشری فارنزیک می‌باشد. در حالیکه فعالیت فارنزیک برای نگهداری روزمره سیستم و کارایی عملیاتی ضروری است، ممکن است کنترول دقیق تری بر فعالیت‌های فارنزیک برای تهیه مواد اثبات کننده جرایم لازم باشد. سرانجام، عملکردهای خوب فارنزیک، ابزارهای مهمی را برای درک اینکه چگونگه مجرمان در تلاش برای بهره‌جویی از آسیب‌پذیری‌های سیستم‌های موجود هستند را فراهم می‌کند، به عنوان مثال، با افشای چگونگی دستیابی آنها به نقاط سوق و اداره یا نحوه طراحی یک سافت‌ویر مخرب یا ملویر(malware).

این بخش به ارائه چالش‌های کلیدی فارنزیک در زمینه مدیریت حوادث سایبری می پردازد. تکنیک‌های فارنزیک می‌تواند برای تحقیق در مورد حوادث سایبری، جمع آوری معلومات و تعقیب عدلی توسط انفاذ قانون مورد استفاده قرار گیرد. ابزارها و تکنیک‌ها برای به دست آوردن دیتا (data) از چندین منبع، تجزیه و تحلیل دیتا و ایجاد زمانبندی رویدادها مواردی است که باید به آن پرداخته شود. این موارد می‌تواند برای ایجاد یک قضیه انتسابی یا برای اشکال مختلف فعالیت‌های تعقیب از ردیابی و نظارت بر فعالیت‌ها گرفته تا ایجاد قضیه جرم علیه عاملان مورد استفاده قرار گیرد. شاگردان همچنین نحوه جمع آوری، تشخیص و استخراج اطلاعات یا داده‌های فارنزیک برای جرایم مالی مانند پولشویی را بررسی خواهند کرد.

شاگردان راجع به مسائل مربوط به جمع آوری داده‌های فارنزیک از چندین منبع از جمله کمپیوترها، شبکه‌ها، دستگاه‌های موبایل، دیتابیس‌ها و سنسورها خواهند آموخت.

نتایج یادگیری

شاگردان نشان خواهند داد که موارد زیر را درک نمودند

- مسائل مربوط به جمع آوری داده‌های فارنزیک (forensic data) از چندین منبع از جمله کمپیوترها، شبکه‌ها، دستگاه‌های موبایل، دیتابیس‌ها و سنسورها ؛
- اهمیت تجزیه و تحلیل داده‌های فارنزیک برای ایجاد زمانبندی و تعیین انتساب؛
- قوانین و مقررات ملی مرتبط با جمع آوری دیتا در حمایت از انفاذ قانون.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

- ایجاد یک سیستم تاب‌آور جهت پشتیبانی از بازیابی پس از یک حادثه سایبری
- بررسی فارنزیک عناصر مهندسی اجتماعی که برای دسترسی به سیستم‌ها مورد استفاده قرار می‌گیرد
- دستگاه‌های هاردویری که می‌تواند از نظر فارنزیک با ارزش باشند
- استفاده از نتایج فارنزیک برای تعقیب عدلی در ارتباط با جرایم
- ابزارهای خودکار برای اقدامات اساسی فارنزیک

روش یادگیری/ارزیابی

روش‌های تدریس متشکل است از لکچرها، نمایشات و بحث راجع به مطالعات موردی مختلف که عناصر مختلف فارنزیک را تشریح می‌کند.

طرح ارزیابی باید مطابق با سطح دانش و آشنایی شاگردان متناسب با کورسی که از این نصاب تحصیلی مرجع نشأت گرفته تدوین شود.

شاگردان باید به شکل شفاهی و کتبی ارزیابی شوند.

مراجع

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_Open-SourceLogManagementSolutions.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.

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

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

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. 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

T4-B4: تفتیش و ارزیابی امنیتی در سطح ملی

شرح

ارزیابی آمادگی امنیتی (Assessment of security preparedness) نقش مهمی برای کشورها دارد. این ارزیابی در امتحان کنترول‌های امنیتی و همچنین شناسایی خلاءها در زیربناها و پالیسی‌های امنیتی کمک می‌کند. ارزیابی امنیتی می‌تواند در چندین سطح انجام شود. اول، می‌توان کنترول‌های امنیتی فردی را با استفاده از ابزارهای تفتیش امتحان نمود. دوم، ارزیابی می‌تواند از طریق تمرینات و شبیه‌سازی‌های زمان واقعی یا بی‌درنگ در یک سطح جامع، سیستمی یا سازمانی انجام شود. این بخش ابزارها و پروسه‌های تفتیش و ارزیابی امنیتی را معرفی می‌کند. این امر به شگردان کمک می‌کند تا یاد بگیرند که چگونه ارزیابی آسیب‌پذیری‌های باقیمانده در سیستم‌ها قابل شناسایی و توزین است؛ علاوه بر این، تفتیش و ارزیابی به چگونگی سنجش آمادگی سیستم‌های سایبری برای مقابله با انواع خاص بازیگران مخرب شناخته شده و آماده شدن برای فعالیت‌ها کمک می‌کند، جایی‌که تهدید ناشناخته‌ای رخ می‌دهد (که به نام تهدیدات فوری یا حملات روز صفر (Zero-day exploit) یاد می‌شود زیرا بدون هشدار آغاز شده و فقط در صورت بروز تشخیص داده می‌شود) .

ابزارها و تکنیک‌های خودآگاهی فردی و سازمانی در حوزه امنیت سایبری متنوع هستند، از پرسشنامه گرفته تا ابزارهای تخنیکی. هدف این بخش افزایش درک نقش خودآگاهی در ارتباط با امنیت سایبری برای فرد و سازمان است. تجزیه و تحلیل نقاط قوت و ضعف ابزارها و رویکردهای مختلف برای درک ارزش آنها حیاتی است. خود ارزیابی مداوم می‌تواند خطرات را کاهش دهد. همچنین در نظر گرفتن سوگیری‌های بالقوه برای خود ارزیابی حیاتی می‌باشد. عملیاتی نمودن نتایج جزء ضروری هر گونه تلاش برای خود ارزیابی می‌باشد. از آنجایی که سطح امنیت به ارزش، اهمیت یا حساسیت آنچه که امنیت آن باید تامین شود بستگی دارد، الگویی واحدی که به سادگی قبول و اعمال شود وجود ندارد. بلکه سطح مطلوب امنیت سایبری به استندردهای انتخاب شده و سطح عملکردی که نیاز به اطمینان دارد بستگی دارد.

نتایج یادگیری

شاگردان

- اهمیت ابزارهای تفتیش و ارزیابی امنیتی را درک خواهند کرد، و
- قادر به ارزیابی و اعمال ابزارها و تکنیک‌های خودارزیابی در بستر ملی خواهند بود.

مسائلی که برای رویکردها و قسمت‌ها بالقوه می‌تواند مد نظر گرفته شود

موضوعات زیر می‌تواند بررسی شود:

- عملکردهای خوب در سازمان‌هایی که از خود ارزیابی استفاده می‌کنند
- بحث در مورد مطالعات موردی وضعیت‌هایی که در آن خودآگاهی می‌تواند باعث افزایش امنیت شود

روش یادگیری/ارزیابی

شاگردان باید از یک ابزار ارزیابی ملی اگر وجود دارد استفاده کنند و در غیر اینصورت می‌توانند از ابزار ارزیابی امنیت سایبری (CSET) که از طریق وزارت امنیت داخلی ایالات متحده (DHS) ارائه شده یا رویکرد مشابهی استفاده کنند. مقایسه هر روش ملی موجود با روش مورد حمایت وزارت امنیت داخلی ایالات متحده می‌تواند مثمر ثمر باشد.

طرح ارزیابی باید مطابق با سطح دانش و آشنایی شاگردان متناسب با کورسی که از این نصاب تحصیلی مرجع نشأت گرفته مهیا شود.

مراجع

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.

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

مخفف‌ها

APT	تهدیدهای پیشرفته مستمر
AS	سیستم مستقل (زیرمجموعه مجزا اینترنت)
ASN	شماره سیستم مستقل
BGP	پروتکل درگاه مرزی
BSA	معماری اساسی امنیت
BYOD	دستگاه خود را بیاورید
CERT	تیم عکس‌العمل سریع سایبری
COBIT	کنترول اهداف و معلومات مربوط به تکنالوژی
COMSEC	امنیت ارتباطات
CSET	ابزار ارزیابی امنیت سایبری
CSET	ابزار ارزیابی امنیت سایبری
DDoS	انکار از خدمات توزیع شده
DHS	وزارت امنیت داخلی ایالات متحده
DNS	سیستم نام دومین
DoS	انکار از خدمات
ENISA	اداره امنیت سایبری اروپا
ESCWG	گروه کاری چالش‌های امنیتی در حال ظهور
FTP	پروتکل انتقال فایل
HTTP	پروتکل انتقال ابرمتن
HTTPS	پروتکل امن انتقال ابرمتن
IANA	مرجع تخصیص اعداد در اینترنت
ICANN	شرکت اینترنتی برای نام‌ها و اعداد تخصیص داده شده
ICS	سیستم کنترول صنعتی
ICT	تکنالوژی معلوماتی و مخابراتی
IDS	سیستم تشخصیص نفوذ
IGF	مجمع حاکمیت اینترنت
IP	پروتکل اینترنت
IS	امنیت معلومات
ISACA	انجمن تفتیش و کنترول سیستم‌های معلوماتی
ISO	سازمان بین‌المللی استندردسازی
ISP	ارائه‌کنندگان خدمات اینترنتی
IT	تکنالوژی معلوماتی
ITU	اتحادیه بین‌المللی مخابرات
LAN	شبکه محلی
NIR	رجستری اینترنت ملی
NIST	موسسه ملی استندردها و تکنالوژی ایالات متحده
PfPC	کانسورسیوم مشارکت برای صلح
PIT	پلتفرم‌های سیستم تکنالوژی معلوماتی
RACI	مسئولیت، حسابدهی، فرماندهی و معلومات
SCADA	کنترول نظارتی و اکتساب دیتا
SCRM	مدیریت ریسک زنجیره عرضه
SFTP	پروتکل امن انتقال فایل
SIEM	مدیریت معلومات و رویدادهای امنیتی
SME	متخصص موضوعی

SMTP	پروتکل ساده انتقال نامه
SQL	زبان اس کیو ال
SSH	پوسته امن
SSL	لایه سوکت‌های امن
TCP	پروتکل کنترول انتقال
TRA	مودل ارزیابی تهدید و خطر
UNIDIR	موسسه تحقیقی خلع سلاح سازمان ملل متحد

تعاریف

توجه: همه اصطلاحات زیر در متن پیشین وجود ندارد، اما بسیاری از آنها می‌توانند در ایجاد تمرینات یادگیری خاص و غیره مفید باشند.

A

تعریف ***مکانیزم کنترل دسترسی (access control mechanism)***: اقدامات امنیتی طراحی شده برای شناسایی و جلوگیری از دسترسی غیرمجاز و اجازه دسترسی مجاز به سیستم‌های معلوماتی یا تأسیسات فیزیکی.

تعریف ***حمله فعال (active attack)***: یک حمله واقعی که توسط یک منبع تهدید عمدی انجام می‌شود و برای تغییر یک سیستم، منابع، دیتا یا عملیات‌های آن تلاش می‌کند.

تعریف ***تهدیدات پیشرفته مستمر***: حمله کننده‌ای که دارای تخصص بالایی بوده و از منابع مهمی برخودار است که این امر به وی اجازه می دهد تا فرصت‌هایی را جهت دستیابی به اهداف خود با استفاده از حامل های مختلف حمله ایجاد کند. (به طور مثال، سایبری، فیزیکی و فریب). برگرفته از: NIST SP 800-53 Rev 4.

تعریف ***سافت‌ویر آنتی ویروس (antivirus software)***: برنامه‌ای که به منظور کشف یا شناسایی کد مخرب و جلوگیری یا محدود نگاه داشتن حوادث یک سافت‌ویر مخرب یا ملویر(malware) از کمپیوتر یا شبکه نظارت می‌کند، گاهی اوقات از طریق حذف یا خنثی‌سازی کد مخرب.

تعریف ***حمله (attack)***: عبارت از هر گونه تلاش برای دستیابی به دسترسی غیر مجاز به خدمات، منابع یا معلومات سیستم یا هر گونه تلاش برای به خطر انداختن یکپارچگی (سلامت) سیستم می‌باشد.

تعریف ***الگوی حمله (attack pattern)***: رویدادها یا رفتارهای سایبری مشابهی که می‌تواند نشان دهد که آیا حمله‌ای که به نقض امنیت یا نقض بالقوه امنیتی منجر می‌شود رخ داده است یا در حال وقوع است.

تعریف ***امضای حمله (attack signature)***: یک الگوی مشخص یا متمایز که می‌تواند در تطبیق حملات تشخیص داده شده قبلی مورد استفاده قرار گیرد.

تعریف ***سطح حمله (attack surface)***: مجموعه‌ای از راه های نفوذ یک حمله‌کننده به سیستم که به طور بالقوه به آن آسیب می‌رساند. تعریف گسترده: مشخصات سیستم معلوماتی که به حمله کننده اجازه تحقیق، حمله یا حفظ حضور در یک سیستم معلوماتی را می‌دهد. بر گرفته از Manadhata, P.K., & Wing, J.M. in Attack Surface Measurement,http://www.cs.cmu.edu/~pratyus/as.html#introduction

تعریف ***احراز هویت (authentication)***: پروسه‌ای که در آن درستی هویت یا سایر ویژگی های یک نهاد تأیید می‌گردد (کاربر، پروسه، دستگاه). تعریف تکمیلی: همچنین پروسه‌ای که طی آن منبع و یکپارچگی (سلامت) داده‌ها/دیتا تأیید می‌گردد.

B

تعریف ***باتنت (botnet)***: مجموعه‌ای از کمپیوترها که توسط کد مخرب به خطر افتاده و در سراسر شبکه کنترل می‌شوند.

تعریف ***ایجاد امنیت (Build Security)***: مجموعه‌ای از اصول‌ها، روش‌ها و ابزارهایی جهت طراحی، انکشاف و تکامل سیستم‌های معلوماتی و سافت‌ویری که مقاومت در برابر آسیب‌پذیری‌ها، خطاها و حملات را افزایش می‌دهد.

C

تعریف ***قابلیت (capability)***: ابزار یا وسیله‌ای برای انجام یک ماموریت، عملکرد یا هدف است.

تعریف ***محاسبات ابری (cloud computing)***: مدلی است برای فراهم نمودن دسترسی آسان بر حسب تقاضای شبکه به مجموعه‌ای از منابع محاسباتی قابل تغییر و پیکربندی (همانند شبکه‌ها، سرورها، فضای ذخیره سازی، اپلیکیشن ها و خدمات) که این دسترسی بتواند با کمترین نیاز مدیریتی و یا نیاز به دخالت ارئه کننده خدمات به سرعت تهیه و منتشر شود.

تعریف ***تجزیه و تحلیل دفاع از شبکه کمپیوتری (Computer Network Defense Analysis)***: اقدامات دفاعی و معلومات جمع‌آوری شده از منابع مختلف توسط یک فرد به منظور تشخیص، تجزیه و تحلیل و گزارشدهی رویدادهایی که در شبکه رخ می‌دهد یا ممکن است رخ دهد تا از معلومات، سیستم‌های معلوماتی و شبکه‌ها در برابر تهدیدات محافظت شود.

تعریف ***زیربنای حیاتی (critical infrastructure)***: عبارت است از سیستم‌ها و دارایی‌های حیاتی، اعم از فیزیکی یا مجازی که ناتوانی یا نابودی آنها می‌تواند موجب اثرات منفی بر امنیت، اقتصاد، صحت عامه یا ایمنی یا ترکیبی از این موارد شود.

تعریف ***رمزنگاری (cryptography)***: استفاده از تکنیک‌های ریاضی به منظور ارائه خدمات امنیتی مانند محرمیت، یکپارچگی (سلامت) دیتا، احراز هویت نهاد، و احراز هویت منبع دیتا می‌باشد.

تعریف ***اکوسیستم سایبری (cyber ecosystem):*** زیربنای معلوماتی به هم پیوسته پیرامون تعاملات میان افراد، پروسه‌ها، داده‌ها و تکنالوژی معلوماتی و مخابراتی به همراه محیط و شرایط تأثیرگذار بر این تعاملات می‌باشد

تعریف ***امنیت سایبری (cybersecurity):*** تعریف کوتاه: عبارت از فعالیت یا پروسه، توانایی یا وضعیتی که در آن از سیستم‌های معلوماتی و مخابراتی و همچنین معلومات موجود در آن در برابر آسیب، استفاده غیر مجاز، تغییر یا بهره‌جویی محافظت می‌شود. تعریف گسترده: امنیت سایبری عبارتست از مجموعه‌ای از استراتژی‌ها، پالیسی‌ها و استندردهای مرتبط با امنیت و عملیات در فضای سایبر که شامل طیف وسیعی از فعالیت‌ها و پالیسی‌ها برای کاهش تهدیدات، کاهش آسیب‌پذیری‌ها، بازدارندگی، سهمگیری بین‌الملل، واکنش به حوادث، پالیسی‌های تاب آوری و بازیابی و همچنین عملیات‌های شبکه کمپیوتری، اطمینان از معلومات، انفاذ قانون، دیپلماسی، مأموریت‌های نظامی و استخباراتی مرتبط با امنیت و ثبات زیربناهای معلوماتی و ارتباطی جهانی. بر گرفته از CNSSI 4009، نسخه اصلاح شده شماره 4 نشریه ویژه 800-53 موسسه ملی استندردها و تکنالوژی ایالات متحد، NIPP، هدف آمادگی ملی وزارت امنیت داخلی ایالات متحده، بررسی پالیسی فضای سایبری کاخ سفید، ماه می 2009.

تعریف ***فضای سایبری (cyberspace):*** عبارت از دنیای الکترونیکی ایجاد شده توسط شبکه‌های به هم پیوسته تکنالوژی معلوماتی و معلومات در آن شبکه‌ها می‌باشد.

D

تعریف ***استخراج دیتا (data mining):*** عبارت از پروسه یا تکنیک‌هایی که برای تجزیه و تحلیل مجموعه وسیعی از معلومات موجود برای کشف الگوها یا رابطه‌های نهان کشف نشده استفاده می‌شود.

تعریف ***انکار از خدمات (denial of service):*** حمله‌ای که مانع از استفاده مجاز از منابع یا خدمات سیستم معلوماتی می‌شود.

تعریف ***فارنزیک دیجیتال (digital forensics):*** پروسه‌ها و تکنیک‌های تخصصی برای جمع آوری، نگهداری و تجزیه و تحلیل دیتاهای (data) مربوط به سیستم (شواهد دیجیتالی) که برای اهداف تحقیقی مورد استفاده قرار می‌گیرد.

تعریف ***مدیریت حقوق دیجیتال (digital rights management):*** عبارتست از نوعی تکنالوژی کنترل دسترسی برای محافظت و مدیریت استفاده از محتوای دیجیتال یا دستگاه‌های دیجیتال یا توجه به اهداف ارائه‌دهنده محتوا یا دستگاه.

انکار از خدمات توزیع شده (distributed denial of service): تکنیک انکار از خدمات از سیستم‌های زیادی برای انجام حمله به طور همزمان استفاده می‌کند.

E

مدیریت ریسک سازمانی (enterprise risk management): یک رویکرد جامع برای مدیریت ریسک که افراد، پروسه‌ها و سیستم‌ها را در سراسر سازمان در بر می‌گیرد تا کیفیت تصمیم‌گیری مدیریت ریسک را بهبود بخشد، ریسکی که ممکن است مانع توانایی سازمان جهت کسب اهداف شود.

تعریف ***بهره‌جویی (exploit):*** تکنیکی که امنیت یک شبکه یا سیستم معلوماتی را با تخطی از پالیسی امنیتی نقض می‌کند.

F

تعریف ***فایروال (firewall):*** توانایی برای محدود کردن ترافیک شبکه بین شبکه‌ها و/ یا سیستم‌های معلوماتی می‌باشد.

H

تعریف ***هکر (hacker):*** یک کاربر غیر مجاز که برای دسترسی به یک سیستم معلوماتی تلاش می‌کند.

I

تعریف ***تهدید زنجیره عرضه در بستر تکنالوژی معلوماتی و مخابراتی (ICT supply chain threat):*** تهدیدی ساخته دست بشر است که از طریق بهره‌جویی از سیستم زنجیره عرضه در بستر تکنالوژی معلوماتی و مخابراتی حاصل می‌شود شامل پروسه‌های اکتساب.

تعریف ***تهدید درونی (inside(r) threat):*** یک فرد یا گروهی از افراد درون سازمانی که با نقض پالیسی‌های امنیتی خطری بالقوه را ایجاد می‌کنند. تعریف گسترده: یک یا چندین فرد دارای دسترسی و/ یا شناخت درونی از یک کمپنی یا سازمان که این امر به آنها اجازه می‌دهد تا از آسیب‌پذیری‌های امنیتی، سیستم‌ها، خدمات، محصولات یا امکانات به قصد ضرر رساندن به آن استفاده کنند.

تعریف ***مدیریت ریسک یکپارچه (integrated risk management):*** رویکرد ساختار یافته‌ای که یک شرکت یا سازمان را قادر می‌سازد تا معلومات مربوط به ریسک و تجزیه و تحلیل آن را به اشتراک بگذارد و استراتیژی‌های مدیریت ریسک مستقل و تکمیلی را به منظور توحید تلاش‌های داخل سازمان هماهنگ کند.

تعریف ***نفوذ (intrusion):*** عملی غیر مجاز برای دور زدن مکانیزم‌های امنیتی شبکه یا سیستم معلوماتی.

تعریف ***تشخیص نفوذ (intrusion detection):*** پروسه و روش‌های مورد استفاده برای تجزیه و تحلیل معلومات شبکه‌ها و سیستم‌های معلوماتی جهت تعیین اینکه آیا نقض امنیتی یا تخطی امنیتی رخ داده است.

K

تعریف ***کی‌لاگر (keylogger):*** سافت‌ویر یا هاردویری است که ضربات کلید و رویدادهای صفحه کلید یا کیبورد را به صورت پنهانی/مخفیانه برای نظارت بر فعالیت‌های کاربر یک سیستم معلوماتی ذخیره یا دنبال می‌کند.

M

تعریف ***کد مخرب (malicious code):*** کد برنامه‌ای که برای انجام یک عملکرد یا پروسه غیرمجاز در نظر گرفته شده است که تأثیر منفی بر محرمیت، یکپارچگی (سلامت) یا در دسترس بودن یک سیستم معلوماتی خواهد گذاشت.

تعریف ***سافت‌ویر مخرب یا ملویر (malware):*** سافت‌ویری که با انجام عملکرد یا پروسه غیرمجاز، عملکرد سیستم را به خطر می‌اندازد.

N

تعریف ***تاب آوری شبکه (network resilience):*** توانایی شبکه برای (1) فراهم کردن عملکرد مستمر (یعنی بسیار مقاوم در برابر اختلال و در صورت خراب شدن قادر به فعالیت در مد تخریب شده (degraded mode) باشد)، (2) بازیابی موثر در صورت خرابی، (3) گنجایش روبرو شدن به خواسته‌های سریع یا غیر قابل پیش بینی دارد.

تعریف ***عدم انکار (non-repudiation):*** آثار بدست آمده از طریق روش‌های رمزنگاری برای محافظت در برابر شخص یا نهادی که به دروغ انجام فعالیت مشخصی راجع به دیتا را انکار نموده است تعریف گسترده: قابلیتی که امکان تعیین اینکه آیا فرد مشخصی فعالیت خاصی را انجام داده است فراهم می‌کند مانند ایجاد معلومات، ارسال پیام، تأیید معلومات یا دریافت پیام.

P

تعریف ***حمله غیرفعال (passive attack):*** یک حمله واقعی که توسط یک منبع تهدید به طور عمدی انجام می‌شود که برای یادگیری یا استفاده از معلومات یک سیستم تلاش می‌کند اما هیچ تلاشی برای تغییر سیستم، منابع، دیتا یا عملکردهای آن نمی‌کند.

تعریف ***فیشینگ (phishing):*** عبارت از شکل دیجیتالی مهندسی اجتماعی که هدف آن فریب افراد برای به دست آوردن معلومات حساس می‌باشد.

R

تعریف ***اقدامات اضافی (Redundancy):*** عبارت سیستم‌ها، زیر سیستم‌ها، دارایی‌های معلوماتی یا پروسه‌های اضافی یا جایگزین که در صورت از بین رفتن یا خرابی سیستم، زیر سیستم، دارایی معلوماتی یا پروسه درجه‌ای از عملکرد کلی سیستم تضمین شود.

تعریف ***تاب آوری (resilience):*** توانایی سازگاری با شرایط و موقعیت‌های متغیر و آماده بودن برای مقاومت، بازیابی سریع و بهبودی در برابر اختلال می‌باشد.

تعریف ***تجزیه و تحلیل ریسک (risk analysis):*** بررسی سیتماتیک مؤلفه‌ها و مشخصه‌های ریسک است.

تعریف ***ارزیابی ریسک (risk assessment):*** پروسه جمع آوری معلومات و تعیین اندازه ریسک به منظور ارئه معلومات راجع به اولویت‌بندی، انکشاف یا مقایسه اقدامات به تصمیم‌گیرندگان است. تعریف گسترده: ارزیابی ریسکی که یک نهاد، دارایی، سیستم یا شبکه، عملیات سازمانی، افراد، منطقه جغرافیایی، سایر سازمان‌ها یا جامعه با آن روبرو است، شامل تعیین اینکه میزان شرایط منفی یا حوادث به چه اندازه می‌تواند منجر به آسیب دیدن آنها شود.

تعریف ***مدیریت ریسک (risk management):*** پروسه شناسایی، تجزیه و تحلیل، ارزیابی و ارتباط ریسک، پذیرش، عدم پذیرش، انتقال یا کنترول ریسک در سطح قابل قبولی با توجه به هزینه‌ها و مزایای مربوط به فعالیت‌های انجام شده می‌باشد. تعریف گسترده: شامل (1) انجام ارزیابی ریسک؛ (2) اجرای استراتژی برای کاهش ریسک؛ (3) نظارت مداوم بر ریسک؛ و (4) مستند کردن پروگرام مدیریت ریسک می‌باشد.

S

تعریف ***اسپم (spam):*** عبارت از سوء استفاده از سیستم های پیام رسان الکترونیکی برای ارسال بی رویه پیام‌های ناخواسته است.

تعریف ***جعل (spoofing):*** وضعیتی که در آن برای ورود غیرقانونی (غیر مجاز) به یک سیستم امن آدرس ارسال‌کننده را جعل می‌کنند.

تعریف ***سافت‌ویر جاسوسی (spyware):*** سافت‌ویری که به طور مخفیانه یا پنهانی بدون اطلاع کاربر یا مالک سیستم در یک سیستم معلوماتی نصب می‌شود.

تعریف ***سیستم کنترل نظارتی و اکتساب دیتا (SCADA):*** یک نام عمومی برای یک سیستم کمپیوتری که قادر به جمع آوری و پروسس داده‌ها/دیتا و اعمال کنترول‌های عملیاتی بر دارایی‌های که از لحاظ جغرافیایی پراکنده می‌باشد و در مسافت‌های طولانی است.

تعریف ***زنجیره عرضه (supply chain):*** سیستمی متشکل از سازمان‌ها، افراد، فعالیت‌ها، معلومات و منابع مورد نیاز برای ایجاد و حمل و نقل تولیدات که شامل اجزای تولید و/ یا خدماتی است که از تأمین‌کنندگان به مشتریان آنها ارائه می‌شود.

تعریف ***مدیریت ریسک زنجیره عرضه (supply chain risk management):*** پروسه شناسایی، تجزیه و تحلیل و ارزیابی ریسک زنجیره عرضه و پذیرش، عدم پذیرش، انتقال و یا کنترل آن در سطح قابل قبول، با توجه به هزینه‌ها و مزایای مربوط به فعالیت های انجام شده.

گرفته شده از لغت‌نامه ابتکار ملی برای مشاغل و مطالعات در زمینه امنیت سایبری (NICCS) وزارت امنیت داخلی ایالات متحده، و سایر مطالب.

T

تعریف ***تهدید (threat):*** شرایط یا رویدادی که توانایی بهره‌جویی از آسیب‌پذیری‌ها را دارد و بر (ایجاد پیامدهای منفی برای) عملیات‌های سازمانی، دارایی‌های سازمانی (از جمله معلومات و سیستم‌های معلوماتی)، افراد، سایر سازمان‌ها یا جامعه تاثیر منفی دارد.

تعریف ***بازیگر/عامل تهدید (threat actor/agent):*** یک فرد، گروه، سازمان یا حکومتی که فعالیت‌های زیانباری را انجام می‌دهد یا قصد انجام آن را دارد.

تعریف ***ارزیابی تهدید (threat assessment):*** محصول یا پروسه شناسایی یا ارزیابی نهاد، فعالیت یا وقایع (اعم از طبیعی یا ساخته دست بشر) که توانایی آسیب رساندن به زندگی، معلومات، عملیات‌ها و/ یا اموال را دارد یا نشان می‌دهد.

تعریف ***حامل تهدید (threat vector):*** وسیله‌ای برای عملی نمودن تهدید برای دستیابی به اهداف یا مسیری که به وسیله آن یک تهدید عملی می‌شود.

تعریف ***تروجان (Trojan horse):*** یک برنامه کمپیوتری که به نظر می‌رسد عملکرد مفیدی دارد اما دارای عملکرد مخفی و مخربی است که مکانیزم‌های امنیتی را دور می‌زند، گاهی یا استفاده از مجوزهای قانونی موجودیت سیستم که برنامه را فرا می‌خواند از مکانیزم‌های امنیتی فرار می‌کند.

U

تعریف ***دسترسی غیرمجاز (unauthorized access):*** هر دسترسی که پالیسی امنیتی اعلام شده را نقض کند.

V

تعریف ***ویروس (virus):*** یک برنامه کمپیوتری است که می‌تواند خود را تکثیر کند، بدون اجازه یا اطلاع کاربر کمپیوتری را آلوده کند و سپس به کمپیوتر دیگری گسترش یا انتشار یابد.

تعریف ***آسیب پذیری (vulnerability):*** مشخصه یا ضعف خاصی که باعث می‌شود یک سازمان یا دارایی (مانند معلومات یا یک سیستم معلوماتی) در معرض بهره‌جویی از یک آسیب‌پذیری توسط یک تهدید مشخص قرار گیرد یا یا در برابر خطرات خاصی آسیب‌پذیر باشد.

W

تعریف ***ورم (worm):*** برنامه‌ای خود تکثیر، خود تکثیریافته که از مکانیزم‌های شبکه برای گسترش یا انتشار خود استفاده می‌کند.

Z

تعریف ***تهدیدات فوری یا حمله روز صفر (Zero-day exploit):*** حمله‌ای که از یک آسیب‌پذیری که تا پیش از آن ناشناخته بوده است بهره می‌گیرد، بدون هشدار آغاز شده و فقط در صورت بروز تشخیص داده می‌شود.

مسئولین تیم و ویرایشگران: شان اس. کاستیگان و مایکل هنسی
مشاورین و اعضای تیم مربوط به نصاب تحصیلی:

نام	کشور	اداره مربوطه	
داکتر آتا آتالایی	ترکیه	مسئول دیپارتمنت، منشی عمومی، شورای امنیت ملی	
خانم ماریا آودیوا	اوکراین	مدیر انکشاف بین‌الملل دانشگاه ملی حقوق خارکوف	
خانم الکساندرا بیلسکا	پولند	مشاور، آی انتلیجنس	
آقای جویسی پی کونتی	ایتالیا	مسئول ارشد تکنالوژی، تریلوجیس	
آقای شان اس. کاستیگان	ایالات متحده آمریکا	پروفسور، مرکز اروپایی جورج سی. مارشال برای مطالعات امنیتی	
آقای جین دی اندریان	فرانسه	هماهنگ کننده، برنامه‌های تحصیلات دفاعی	
آقای دیرک دوبوئیس	بلژیک	کالج امنیتی و دفاعی اروپا	
داکتر دیوید امیلی فیونو	کانادا	افسر ارشد فعالیت‌ها، همکاری‌های تحصیلی، وزارت دفاع ملی	
آقای دیوید فرانکو	ایالات متحده آمریکا	مامور خاص نظارتی، دفتر تحقیقات فدرال	

داکتر پیوتر گافلیچک	پولند	نماینده امور پوهنتون برای نوآوری پوهنتون دفاع ملی	
داکتر سانجی گوئل	ایالات متحده آمریکا	رئیس تحقیقات، مرکزفارنزیک و اطمینان از معلومات ایالت نیویورک پوهنتون ایالتی نیویورک در آلبانی	
آقای آندریا گوتسیریدز	گرجستان	رئیس دفتر امنیت سایبری وزارت دفاع	
آقای آرمان گریگوریان	ارمنستان	مسئول تیم امنیت سایبری، موسسه مطالعات استراتژیک ملی	
داکتر مایکل اِی. هنسی	کانادا	پروفسور/ معاون رئیس، در امور تحقیقات کالج سلطنتی نظامی کانادا	
آندریاس هیلدنبراند	جرمنی	پروفسور، مرکز اروپایی جورج سی. مارشال برای مطالعات امنیتی	
داکتر دینوس کریگان کایرو	ایرلند	استاد، دیپارتمنت علوم کمپیوتر و ریاضیات پوهنتون گرینویچ	
داکتر اسکات نایت	کانادا	پروفسور/مسئول دیپارتمنت انجینری برق و کمپیوتر کالج نظامی رویال کانادا	
آقای فردریک لابار	کانادا	مدیر پروگرام، کانسورسیوم مشارکت برای صلح اکادمی‌های دفاعی و انستیتوت‌های مطالعات امنیتی	
آقای فیلیپ لارک	ایالات متحده آمریکا	رئیس، پروگرام امنیت سایبری مرکز اروپایی جورج سی. مارشال برای مطالعات امنیت	

داکتر گستاو لیندستروم	سوئد	مسئول پروگرام چالش های امنیتی در حال ظهور مرکز پالیسی امنیتی ژنو	GCSP
داکتر واختانگ مایسایا	گرجستان	پروفسور، ماستری امنیت بین‌الملل پوهنتون بین‌المللی قفقاز	
داکتر پتار مولوف	بلغاریا	پوهندوی، موسسه تحقیقات پیشرفته دفاعی	
آقای کریس پالاریس	بریتانیا	رئیس، آی انتلیجنس	I-INTELLIGENCE
آقای دنیل پدر باگی	جمهوری چک	متخصص پالیسی امنیت سایبری اداره امنیت ملی جمهوری چک	NBU
آقای رافائل پرل	ایالات متحده آمریکا	رئیس، کانسورسیوم مشارکت برای صلح اکادمی‌های دفاعی و انستیتوت‌های مطالعات امنیتی	
خانم ماکا پتریاشویلی	گرجستان	رئیس منابع انسانی، وزارت دفاع	
خانم استلا پتروا	بلغاریا	مشاور، شبکه رهبری اروپا	European Leadership Network
دکتر بنیامین پوگوسیان	ارمنستان	معاون، موسسه مطالعات استراتژیک ملی	
آقای اولکساندر پوتیل	اوکراین	پروفسور امنیت تکنالوژی معلوماتی، پوهنتون ملی نیروی هوایی خارکوف	

داکتر دتلف پوهل	جرمنی	مشاور ارشد، بخش چالش‌های امنیتی در حال ظهور ناتو،	
آقای نیل رابینسون	بریتانیا	رئیس تحقیق مؤسسه تحقیق و انکشاف (رند) اروپا	
آقای جیجی رومن	رومانیا	یادگیری توزیع شده پیشرفته، مکتب ناتو	
غنادی صافونوف	مولدوا	دیپارمنت ارتباطات و انفورماتیک آکادمی دفاعی مولدوا	
آقای دانیلو شیفشینکو	اوکراین	مدیر پروژه، مرکز تحقیقات استراتژیک و نوآوری	
خانم ناتالیا اسپینو	مولدوا	رئیس، مرکز امنیت سایبری، ساختمان صدارت	
داکتر آل استولبرگ	ایالات متحده آمریکا	هماهنگ کننده، تحصیلات دفاعی مؤسسه تحقیق و انکشاف (رند)	
دکتر تودور تاگارف	بلغاریا	پروفسور/مسئول، مسئول تکنالوژی معلوماتی دیپارتمنت امنیت و مرکز مدیریت امور امنیتی و دفاعی	
دکتر رونالد تیلور	ایالات متحده آمریکا	رئیس، مرکز رهبری استراتژیک محیط های پیچیده	
آقای بودگان اودریست	رومانیا	متخصص امنیت سیستم‌های معلوماتی، مأموریت نظارتی اتحادیه اروپا	
آقای جوزف وان	ایالات متحده آمریکا	پروفسور، مرکز اروپایی جورج سی. مارشال برای مطالعات امنیتی	

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

تیم ویرایش و توزیع

ویرایشگران:

شان اس. کاستیگان
پروفسور
مرکز اروپایی جورج سی. مارشال برای مطالعات امنیتی
Gernackerstrasse 2
82467 گارمیش-پارتنکرچین، آلمان
sean.costigan@pfp-consortium.org

داکتر مایکل اِی. هنسی
پروفسور تاریخ و مطالعات حرب
معاون در امور تحقیقات
کالج سلطنتی نظامی کانادا
ص.پ STN FORCES 17000
کینگستون، انتاریو، کانادا
K7K 7B4
Hennessy-m@rmc.ca

هماهنگ کننده ترتیب/توزیع:

گابریلا لورویگ-جوندارم
اداره بین المللی ناتو
lurwig.gabriella@hq.nato.int