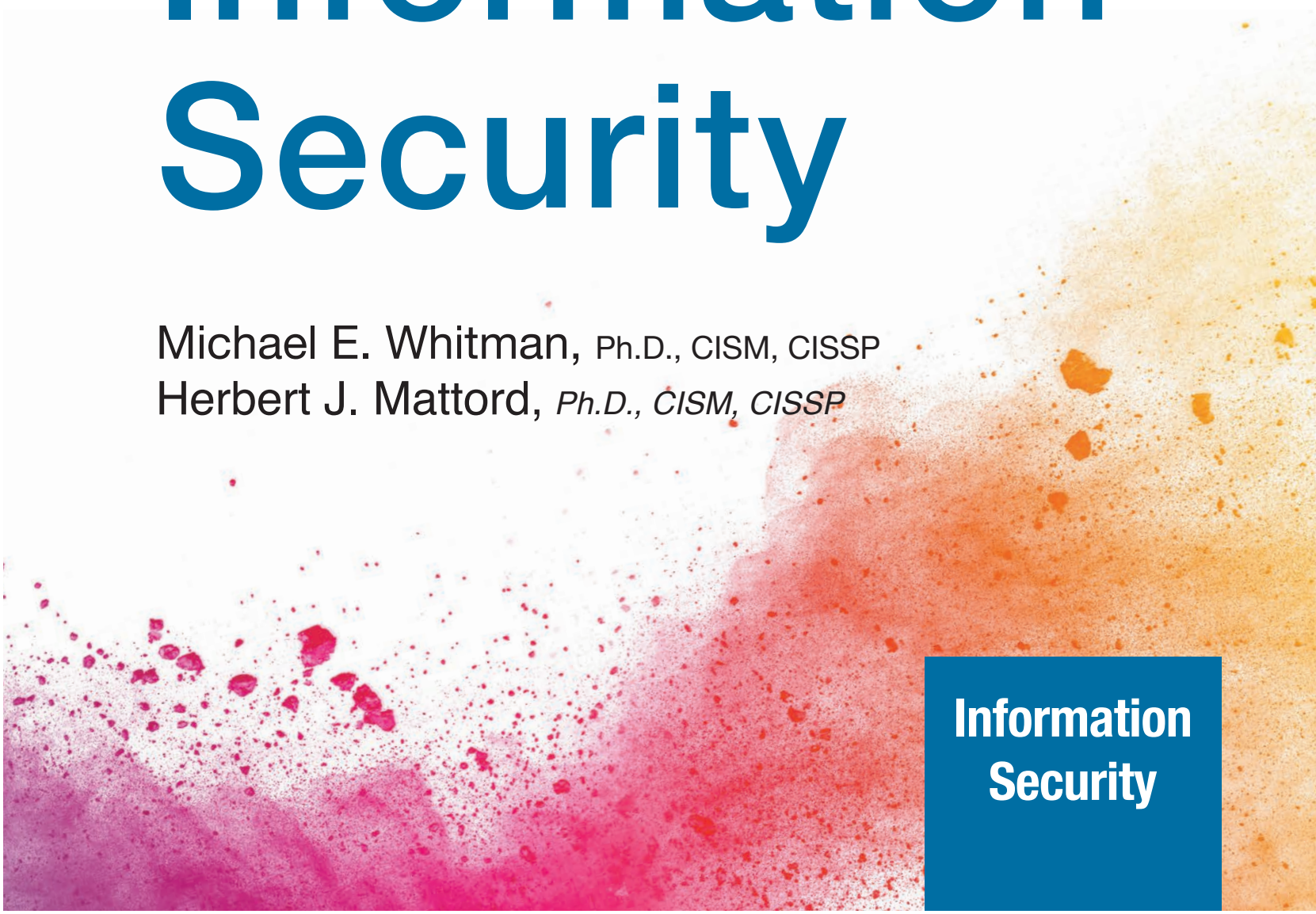
Azərbaycanın uzunmüddətli etibarlı tərəfdaşı və iri neft-qaz layihələrinin əməliyyatçısı olan BP şirkəti ölkənin həyatının ən mühüm sahələrinə – təhsilə, yerli icmalarda imkanların yaradılmasına, kiçik və orta biznesin inkişafına, ətraf mühitin qorunmasına, xalqın zəngin mədəni irsinin və tarixinin tədqiqi və təbliğinə, milli idmanın inkişafına öz töhfəsini verməklə Azərbaycanın gələcəyinin möhkəm təməllər üzərində qurulmasında iştirak edir.

Bu kitabın Azərbaycan dilinə tərcüməsi və nəşri BP-nin ölkədə təhsilin inkişafına verdiyi dəstəyin bir hissəsidir. Kitab bu sahədə ixtisaslaşan təhsil müəssisələrinə və insanlara BP-nin hədiyyəsidir.

Seventh Edition

Principles of Information Security

Michael E. Whitman, Ph.D., CISM, CISSP
Herbert J. Mattord, *Ph.D., CISM, CISSP*



Cengage

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

Principles of Information Security,
7th Edition
Michael E. Whitman and Herbert J. Mattord

SVP, Higher Education Product Management: Erin Joyner

VP, Product Management: Thais Alencar

Product Director: Mark Santee

Associate Product Manager: Danielle Klahr

Product Assistant: Tom Benedetto

Executive Director, Learning: Natalie Skadra

Learning Designer: Mary Clyne

Vice President, Product Marketing: Jason Sakos

Portfolio Marketing Manager: Mackenzie Paine

Senior Director, Content Creation: Rebecca von Gillern

Content Manager: Christina Nyren

Director, Digital Production Services: Krista Kellman

Senior Digital Delivery Lead: Jim Vaughey

Developmental Editor: Dan Seiter

Production Service/Composition: SPi Global

Design Director: Jack Pendleton

Designer: Erin Griffin

Text Designer: Erin Griffin

Cover Designer: Erin Griffin

Cover image(s): Vandathai/Shutterstock.com

Library of Congress Control Number: 2021909680

ISBN: 978-0-357-50643-1

Cengage
200 Pier 4 Boulevard
Boston, MA 02210
USA

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com**.

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com.**

Printed in the United States of America
Print Number: 01 Print Year: 2021

İnformasiya təhlükəsizliyi

prinsipləri

Maykl E. Vitman
Herbert J. Mattord

İnformasiya təhlükəsizliyi

TEAS PRESS

Azərbaycan Respublikası Elm və Təhsil Nazirliyi
İnformasiya Texnologiyaları İnstitutunun
Elmi Şurasının qərarı ilə çapa tövsiyə olunmuşdur

Maykl E. Vitman, Herbert C. Mattord.

İnformasiya təhlükəsizliyinin prinsipləri

(ingilis dilindən tərcümə)

Layihə rəhbəri: Ülkər Hüseynova

Təhsil üzrə məsləhətçilər: Elmina Kazımzadə
Rahid Ələkbərli

Tərcüməçilər: İsmayıl Sadıqov
Anar İbrahimov

İxtisas redaktorları: Fərid Musayev
Müşərrəf Məmmədova

Nəşriyyat redaktoru: Famil Cəfərli

Texniki redaktor: Vüsalə Babayeva

Çapa məsul: Rəşad İsmixanov

Korrektor: Flora Əliyeva

Dizayner: Mahir Allahverdiyev

Bakı, TEAS Press Nəşriyyat evi, 2024, 556 səh.

ISBN 978 9952 563 56 6

Bu kitab ilk dəfə 2022-ci ildə "Cengage Learning" nəşriyyatı tərəfindən "Principles of İnformation Security" adı ilə nəşr olunub. Əsər "Cengage Learning" nəşriyyatının orijinalı əsasında TEAS Press Nəşriyyat evində tərcümə edilərək çapa hazırlanıb. Kitabın Azərbaycan dilinə tərcüməsi və nəşri hüququ TEAS Press Nəşriyyat evinə məxsusdur.

www.teaspress.az

Qısa mündəricat

Mündəricat

Modul 6

Modul 7

Modul 8

Modul 9

Modul 10

Azərbaycan nəşrinə ön söz

Dünya getdikcə daha da “kiçilir”. Əlinizdə tutduğunuz bu kitab bütün dünyada informasiya və kibertəhlükəsizlik müdafiəçilərinin əhatə dairəsini genişləndirmək məqsədi daşıyan layihənin bir hissəsi rolunu oynayır. Bu aparıcı dərslik sizin ondan rahat istifadə edə bilməyiniz üçün Azərbaycan dilinə tərcümə edilib. Əminik ki, kibertəhlükəsizlik üzrə mütəxəssislərin sayının artırılması və onların hazırlanması prosesinin təkmilləşdirilməsi yolu ilə bu sahədəki imkanlar da artırıla və daha yaxşı nəticələr əldə oluna bilər. Ümid edirik ki, kibertəhlükəsizlik üzrə mütəxəssislərin yeni nəsillərinin hazırlanması işini davam etdirərkən dil boşluğunun kiçik bir hissəsinin aradan qaldırılması peşəkar kadrlarla tədqiqatçıların əməkdaşlığını daha da gücləndirəcək.

Qlobal informasiya şəbəkələri genişlənməkdə davam etdikcə hər növ cihazın qarşılıqlı əlaqəsi kommunikasiya, hesablama və avtomatlaşdırma həllərinin problemsiz işləməsi qədər həyati əhəmiyyət daşıyır. Buna baxmayaraq, günbəgün inkişaf edən zərərverici proqram təminatı və fişinq hücumları kimi təhlükələr, eləcə də cinayətkar dəstələrə və rəqib hökumətlərə yaxın kiberhücumçuların uğurlu cəhdləri cari texniki mənzərənin zəif tərəflərini və informasiya sistemlərinin gücləndirilmiş təhlükəsizliyinin təmin edilməsi zərurətini nümayiş etdirir.

Şirkətlər cari və planlaşdırılan sistem və şəbəkələrin təhlükəsizliyini təmin etməyə cəhd göstərərkən informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə mütəxəssislərin təcrübələrindən yararlanmalıdır. Bununla belə, həmin şirkətlər gələcəkdə daha təhlükəsiz hesablama mühitini təkmilləşdirmək üçün yaranacaq mürəkkəb informasiya təhlükəsizliyi məsələlərini qabaqcadan sezə və idarə edə bilən düzgün bacarıq və təcrübə kompleksinə malik gələcək peşəkarlar nəslinə arxalanırlar. Beləliklə, kompüter elmləri üzrə təhsil alan tələbələrin mövcud sistemlərdəki təhlükə və zəifliklərlə tanış olması və lazımi təhlükəsizlik sistemlərini qurmağı və təkmilləşdirməyi öyrənməsi üçün kollec və universitetlərin professor-müəllim heyətinin səyləri ilə yanaşı dəstəkləyici materiallarla təkmilləşdirilmiş mətnlərə ehtiyac var. “İnformasiya təhlükəsizliyi prinsipləri” kitabının (yeddinci nəşri) məqsədi informasiya təhlükəsizliyi və kibertəhlükəsizlik fənləri üzrə hərtərəfli araşdırma aparan cari, yüksək keyfiyyətli akademik resurslara olan ehtiyacı qarşılamaqda davam etməkdir.

Tələbələrin bu sahələrin idarəetməsi və texniki aspektləri ilə tanış olması üçün hətta bu gün də kifayət qədər balanslaşdırılmış resurs yoxdur. Bu kitabda yazdıqlarımızı məxsusi olaraq ümumi biliklər toplusuna yönəltməklə bu boşluğu aradan qaldırmağa ümid edirik. Bundan əlavə, informasiya təhlükəsizliyi və kibertəhlükəsizliyin əsasları haqqında aydın fikir formalaşdırmaq və sistemin zəiflikləri üçün sahələrarası həllər tapmaq məqsədilə ədalət mühakiməsi, politologiya, kompüter elmləri, informasiya sistemləri və digər əlaqəli sahələrdən prinsiplərin daxil edilməsinə aydın ehtiyac var. Bu əsərin əsas prinsipi müasir bir şirkətdə informasiya təhlükəsizliyi və kibertəhlükəsizlik texnologiyasının təkbaşına həll edə bilməyəcəyi və idarəetmənin həll etməli olduğu problemlə bağlıdır. Başqa sözlə desək, şirkətin informasiya təhlükəsizliyi mühüm iqtisadi nəticələrə səbəb ola bilər, bu nəticələrə görə isə rəhbərlik məsuliyyət daşıyır.

Maykl E. Vitman
Herbert C. Mattord
Kenneso, Corciya, ABŞ
4 aprel, 2023

Giriş

Dünyada hər şey getdikcə bir-birinə daha sıx şəkildə bağlanmaqda davam edir. Qlobal informasiya şəbəkələri genişlənməkdə davam etdikcə müxtəlif görünüşlü cihazların qarşılıqlı əlaqəsi, kommunikasiya, hesablama və avtomatlaşdırma həllərinin düzgün işləməsi həyati əhəmiyyət kəsb edir. Bununla belə, zərərli proqramlar və kiberhücumlar kimi daim genişlənib artan təhdidlər və cinayətkarlıq halları hökumətləri yeni çağırışlarla üz-üzə qoyur, onlara kiberhücumların cari texniki mənzərənin zəif tərəflərini və informasiya sistemlərinin yüksək təhlükəsizliyini təmin etmək zəruriliyini diktə edir.

Ayrı-ayrı təşkilatlar sistemlərin və şəbəkələrin təhlükəsizliyini təmin etməyə başlayanda informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə təcrübənin mövcud qaydalarından istifadə etməyə məhkumdur. Bununla belə, həmin təşkilatlar gələcəkdə daha təhlükəsiz informasiya mühitini inkişaf etdirmək məqsədilə yaranacaq mürəkkəb informasiya təhlükəsizliyi məsələlərini qabaqcadan görmək və idarə etmək üçün düzgün bacarıqlara və təcrübəyə malik olan peşəkarların formalaşmasına ümid bəsləyir. Beləliklə, ali təhsil müəssisələri müəllimlərinin səyləri ilə yanaşı, təcrübi materiallarla təmin edilmiş mətnlər də müvafiq sahədə təhsil alan tələbələrin inkişafına və onların lazımi təhlükəsizlik sistemlərini dərindən öyrənməsinə kömək edəcək.

"İnformasiya təhlükəsizliyi prinsipləri" kitabının məqsədi informasiya təhlükəsizliyi və kibertəhlükəsizlik fənlərinin tam genişliyini tədqiq edən cari, yüksək keyfiyyətli akademik mənbəyə olan ehtiyacı ödəməkdir. Hətta günümüzdə belə bu sahədə dəqiq materiallara rast gəlmək çox çətindir. Bu kitabdakı materialları ümumi biliklər toplusuna tətbiq etməklə bu boşluğu aradan qaldıracağımıza ümid edirik. Bundan əlavə, informasiya təhlükəsizliyi və kibertəhlükəsizlik prinsiplərini aydın şəkildə başa düşmək üçün fənlərarası əlaqəni formalaşdıraraq hüquqi məsələləri, politologiya, kompüter elmləri, informasiya sistemləri və digər əlaqədar fənlərin prinsiplərini mənimsəməyə açıq-aşkar ehtiyac var. Bu kitabın əsas prinsipi müasir təşkilatda informasiya təhlükəsizliyi və kibertəhlükəsizlik idarəetməsinin həll etməli olduğu problemi izah etməkdir.

Yanaşma

"İnformasiya təhlükəsizliyi prinsipləri" kitabı informasiya təhlükəsizliyinin bütün sahəsinin geniş icmalını, bir çox əlaqədar elementlər haqqında məlumatları və bütövlükdə mövzunun başa düşülməsini asanlaşdırmaq üçün kifayət qədər təfərrüatları təqdim edir. Kitab özündə hekayəəsaslı terminologiyanı və informasiya təhlükəsizliyi proqramını idarə etmək üçün elementar strategiyaları ehtiva edir.

Kitabın strukturu və modulların qısa icmalı

"İnformasiya təhlükəsizliyi prinsipləri" kitabı informasiya təhlükəsizliyinin strateji aspektlərindən tutmuş informasiya təhlükəsizliyinə qədərki xarici təsirlərə, təşkilatın idarəetməsinə, risklərin idarə olunmasına və tənzimləmə üzrə strateji yanaşmalara yer verməklə strukturlaşdırılıb. Kitabda yuxarıda qeyd edilən aspektlərin bir-birinə uyğunluğuna, təşkilatda təhlükəsizliyin təşkili üzrə texniki və əməliyyat icrasına xüsusi yer verilir. Müəlliflərin kitabda bu yanaşmadan istifadə etməkdə məqsədi təlimçiləri və tələbələri informasiya təhlükəsizliyinin öyrənilməsi üçün dəstəkləyici, lakin həddən artıq dominant olmayan təməl materialla təmin etməkdən ibarətdir. Yuxarıda göstərilən məqsədlərə xidmət etmək üçün kitab ümumilikdə aşağıda göstərilən 12 moduldan təşkil olunub.

Modul 1 – İnformasiya təhlükəsizliyinə giriş

Bu modul açılış modulu olaraq əsas terminləri müəyyən etmək, onları başa düşmək, əsas anlayışları izah etmək, habelə bu sahənin mənşəyinin və onun informasiya təhlükəsizliyinin başa düşülməsinə təsirini nəzərdən keçirmək üçün böyük fürsətdir.

Modul 2 – İnformasiya təhlükəsizliyinə tələbat

Modul 2 informasiya təhlükəsizliyinin təhlil edilməsi prosesinin arxasında duran anlayışları, o cümlədən Modul 1-də təqdim olunan konsepsiyaları vurğulamaqla və onlara əsaslanmaqla mövcud təşkilati və texnoloji təhlükəsizlik ehtiyaclarını dərindən araşdırır, onları ətraflı şəkildə izah edir. Bu modulda təqdim olunan əsas konsepsiyalardan biri informasiya təhlükəsizliyinin texnoloji deyil, ilk növbədə idarəetmə məsələsi olmasıdır. Başqa sözlə desək, bu modul, əsasən, informasiya təhlükəsizliyi sahəsindəki ən yaxşı təcrübələrin texnologiyanın yalnız biznes ehtiyacları nəzərə alınandan sonra tətbiqinin nəzərdə tutulduğunu göstərir. Bütün bunlarla yanaşı, Modul 2 təşkilatların üzləşdiyi müxtəlif təhdidləri araşdırır və təşkilatlar öz təhlükəsizliyini planlaşdırma prosesinə başlayan kimi bu təhdidlərin sıralanması və prioritetləşdirilməsi üsullarını təqdim edir. Modul bu təhdidlər nəticəsində yarana biləcək hücum növlərini və həmin hücumların təşkilatın informasiya sistemlərinə necə təsir göstərə biləcəyini ətraflı surətdə araşdırmaqla davam edir. Bununla yanaşı, bu modul informasiya təhlükəsizliyinin əsas prinsiplərinin əlavə müzakirəsini təmin edir. Onların bəziləri Modul 1-də təqdim edilsə də, bu modulda daha geniş izahlar verilir. Bunlara məxfilik, bütövlük, əlçatanlıq, autentifikasiya, identifikasiya, avtorizasiya (səlahiyyətləndirmə), hesabatlılıq və gizlilik daxildir.

Modul 3 – İnformasiya təhlükəsizliyinin idarə edilməsi

Bu modul informasiya təhlükəsizliyi sahəsində müxtəlif idarəetmə funksiyalarını təqdim edir və informasiya təhlükəsizliyinin idarə edilməsini müəyyənləşdirir. İnformasiya təhlükəsizliyi siyasətinin, standartlarının, təcrübələrinin, prosedurlarının və təlimatlarının işlənib-hazırlanmasında, saxlanılmasında və tətbiqində rəhbərliyin rolu ilə davam edir. Modul həmçinin həm hərbi, həm də şəxsi məlumatların təsnifat sxemlərini, həmçinin təhlükəsizlik təhsili, təlimi və maarifləndirmə (SETA) proqramını izah edir. Modul informasiya təhlükəsizliyi planlarına dair müzakirələrlə yekunlaşır.

Modul 4 – Riskin idarə olunması

Bu modulda izah olunan əsas konsept ondan ibarətdir ki, informasiya təhlükəsizliyi üzrə analitiklər yeni informasiya təhlükəsizliyi həllinin layihələndirilməsinə başlamazdan əvvəl ilk növbədə təşkilatın hazırkı vəziyyətinin və onun informasiya təhlükəsizliyi ilə əlaqəsinin başa düşülməsini izah etməlidirlər. Modulun fokuslandığı əsas suallar bunlardır: təşkilatın hansısa formal informasiya təhlükəsizliyi mexanizmləri varmı? Onlar nə dərəcədə effektivdir? Hansı siyasət və prosedurlar qəbul edilib və təhlükəsizlik menecerlərinə və son istifadəçilərə paylanıb? Bu modul təhdidlərin və aktivlərin müəyyən olunması və prioritetləşdirilməsi prosedurlarını, eləcə də bu aktivləri təhdidlərdən qorumaqdan ötrü hansı nəzarət vasitələrinin mövcud olduğunu müəyyənləşdirmək üçün prosedurları təsvir etməklə fundamental informasiya təhlükəsizliyi qiymətləndirilməsinin necə aparılacağını izah edir. Modul həmçinin nəzarət mexanizmlərinin müxtəlif növlərini müzakirə edir və riskin ilkin qiymətləndirilməsinin həyata keçirilməsində iştirak edən addımları müəyyənləşdirir. Modul riskin idarə edilməsini riskin müəyyənləşdirilməsi, qiymətləndirilməsi və qəbul olunan səviyyəyə endirilməsi prosesi kimi müəyyən etməklə və bu risk səviyyəsini saxlamaq üçün effektiv nəzarət tədbirlərini həyata keçirmək yollarını göstərməklə davam edir. Modul 4 risk təhlilinin və müxtəlif mümkün təhlillərinin müzakirəsi ilə yekunlaşır.

Modul 5 – İnsidentə cavab və fövqəladə halların planlaşdırılması

Bu modul biznesin sürəkliliyini, fəlakətin bərpasını və insidentlərə reaksiyanı dəstəkləyən planlaşdırma prosesini araşdırır. O həmçinin insidentlər zamanı təşkilatın rolunu təsvir edir və təşkilatın hüquq-mühafizə orqanlarını nə vaxt cəlb etməli olduğunu müəyyənləşdirir. Modul ümumilikdə rəqəmsal kriminalistika mövzusunu əhatə edir.

Modul 6 – İnformasiya təhlükəsizliyində hüquq, etika və peşə məsələləri

Modul 6-da əhatə olunan əsas mövzular sahənin kritik aspekti ilə – biznesi tənzimləyən tənzimləyici məhdudiyyətlərə dair mühüm anlayışları təmin edən mövcud qanunvericiliyin, qaydaların və həm milli, həm də beynəlxalq qurumların ümumi etik gözləntilərinin diqqətlə araşdırılması ilə bağlıdır. Bu modul informasiya təhlükəsizliyi sahəsini formalaşdıran bir neçə əsas qanunu araşdırır və təhlükəsizliyi həyata keçirənlərin riayət etməli olduğu kompüter etikasını göstərir. Bu modul həmçinin bugünkü təşkilatlarda, eləcə də etik və hüquqi məsuliyyəti təşviq edən rəsmi və peşəkar təşkilatlarda rast gəlinən bir sıra ümumi hüquqi və etik problemləri təqdim edir.

Modul 7 – Təhlükəsizlik və işçi heyəti

Modul 7 icra mərhələsində kadr məsələlərini əhatə edir. Bu modul işçilərin təhlükəsizliyinə dair məsələlərin hər iki aspektini araşdırır: təhlükəsizlik üzrə işçiləri və personalın təhlükəsizliyini. Modul kadr məsələləri ilə yanaşı, peşəkar təhlükəsizlik sertifikatları, məşğulluq siyasəti və təcrübələrinin həyata keçirilməsi kimi məsələləri də əhatə edir. Bütün bunlarla yanaşı, Modul 7 informasiya təhlükəsizliyi siyasətinin məsləhətçilərə, müvəqqəti işçilərə və kənar biznes tərəfdaşlarına necə təsir göstərdiyini ətraflı şəkildə müzakirə edir.

Modul 8 – Təhlükəsizlik texnologiyası: erişim nəzarəti, təhlükəsizlik divarları və VPN-lər

Modul 8 təşkilatın sistemlərini təhlükəsiz internetdən ayırmaq üçün nəzərdə tutulmuş texnologiyaların konfiqurasiyasının və istifadəsinin ətraflı icmalını verir. Bu modul "təhlükəsizlik divarı" texnologiyalarının müxtəlif təriflərini və kateqoriyalarını, habelə təhlükəsizlik divarlarının yerləşdirilə biləcəyi arxitekturaları araşdırır. Modulda təhlükəsizlik divarlarının düzgün konfiqurasiyası və istifadəsi ilə bağlı qaydalar və təlimatlar müzakirə olunur. Modul 8 həmçinin uzaqdan "kommutasiyalı zəng" *(dial-up)* xidmətlərini və hələ də bu köhnə texnologiyanı tətbiq edən təşkilatlar üçün erişim nöqtələrinin təhlükəsizliyini təmin etməkdən ötrü lazım olan təhlükəsizlik tədbirlərini əhatə edir. Modul məzmun filtrləmə imkanlarını və mülahizələrini təqdim etməklə davam edir, səlahiyyətli istifadəçilərə uzaqdan erişimi virtual şəxsi şəbəkələr vasitəsilə təmin etmək üçün nəzərdə tutulmuş texnologiyaların araşdırılması ilə yekunlaşır.

Modul 9 – Təhlükəsizlik texnologiyası: müdaxilənin aşkarlanması, qarşısının alınması sistemləri və digər təhlükəsizlik vasitələri

Modul 9 kənar müdaxilə anlayışını və müdaxilələrin qarşısını almaq, aşkar etmək, reaksiya vermək və onları bərpa etmək üçün lazım olan texnologiyaları araşdıraraq təhlükəsizlik texnologiyalarının müzakirəsini əhatə edir. Modulda icazəsiz müdaxilənin aşkarlanması və qarşısının alınması sistemlərinin (IDPS) xüsusi növləri, – host IDPS, şəbəkə IDPS və proqram IDPS, – habelə onların müvafiq konfiqurasiyaları və istifadəsi təqdim və müzakirə edilir. Hücumçuları fırıldaqçı sistemlərə sövq etmək (beləliklə də, kritik sistemlərdən uzaqlaşmaq) və ya, sadəcə olaraq, hücumçunun bu saxtakarlıq sahələrinə daxil olmasını müəyyənləşdirmək üçün nəzərdə tutulmuş xüsusi aşkarlama texnologiyaları da bu modulda müzakirə edilir. Belə sistemlər "balqabı" tələsi, "balqabı" şəbəkəsi və "yastıqlı hücrə" sistemləri kimi tanınır. Bu müzakirələr zamanı təxribat sistemlərinə cəlb edilmiş hücumçuların əsl ünvanını izləmək üçün nəzərdə tutulmuş geriyə izləmə sistemləri də araşdırılır. Modul daha sonra informasiya təhlükəsizliyi üzrə mütəxəssislərin öz təşkilatlarının sistemlərinin cari vəziyyətini izləmək və təşkilatın ümumi təhlükəsizlik vəziyyətində potensial zəifliklərı və ya çatışmazlıqları müəyyənləşdirmək üçün istifadə edə biləcəyi əsas təhlükəsizlik alətlərini araşdırır. Modul 9 müasir əməliyyat sistemləri və biometrika sahəsindəki mövcud tətbiqlərə güclü autentifikasiyanı təmin edə bilən yeni texnologiyalar tərəfindən adətən tətbiq olunan erişimə nəzarət cihazlarının müzakirəsi ilə yekunlaşır.

Modul 10 – Kriptoqrafiya

Modul 10 müasir kriptosistemlərin əsas anlayışlarını, eləcə də onların arxitekturalarını və tətbiqlərini təsvir etməklə təhlükəsizlik texnologiyalarının öyrənilməsini özündə əks etdirir. Modul kriptoqrafiyanın tarixini ümumiləşdirməklə və bu tarixdə əsas rol oynamış müxtəlif şifr növlərini müzakirə etməklə başlayır. Bu modul həmçinin kriptosistemləri, o cümlədən "doğrama" *(hash)* funksiyalarını əhatə edən bəzi riyazi texnikaları araşdırır. Modul daha sonra ənənəvi simmetrik şifrləmə sistemlərini daha müasir asimmetrik şifrləmə sistemləri ilə müqayisə edərək və açıq açarlı şifrləmə sistemlərinin əsası kimi asimmetrik sistemlərin rolunu araşdıraraq bu müzakirəni genişləndirir. Bu müzakirələrdə HTTPS, S/MIME və SET də daxil olmaqla təhlükəsiz rabitədə istifadə olunan kriptoqrafiyaəsaslı protokollar da əhatə olunur. Daha sonra modulda steqanoqrafiya və onun məlumatı gizlətmək üçün effektiv vasitə kimi ortaya çıxan rolu müzakirə olunur. Modul xüsusi olaraq kriptosistemlərə yönəlmiş informasiya təhlükəsizliyinə edilən hücumları təkrar nəzərdən keçirməklə yekunlaşır.

Modul 11 – İnformasiya təhlükəsizliyinin tətbiqi

Bundan əvvəlki modullar təşkilatın öz informasiya təhlükəsizliyi proqramını necə tərtib edə biləcəyinə dair təlimatları təqdim edir. Modul 11 bu işlərin həyata keçirilməsi üçün vacib olan elementləri araşdırır. İnformasiya təhlükəsizliyinin həyata keçirilməsi üçün "öküz gözü" *(bull's-eye)* modeli və təşkilatın öz informasiya təhlükəsizliyi proqramının komponentlərini autsorsinq edib-etməməsinin müzakirəsi də bu modulun əsas sahələrinə daxildir. Modulda həmçinin dəyişikliklərin idarə edilməsi, proqramın təkmilləşdirilməsi və biznesin sürəkliliyi səyləri üçün əlavə planlaşdırma müzakirə olunur.

Modul 12 – İnformasiya təhlükəsizliyinin təmin edilməsi

Sonuncu və ən vacib modul olan bu modul tətbiq və dəyişikliyi müzakirə edir. Modul 12 təşkilatın öz informasiya sistemlərinin təhlükəsizliyini qorumaq üçün yerinə yetirməli olduğu informasiya təhlükəsizliyi proqramının davamlı texniki və inzibati qiymətləndirilməsini təsvir edir. Bu modul yeni təhlükəsizlik çatışmazlıqlarının qarşısını almaq üçün müasir informasiya sistemlərində dəyişikliklərin idarə olunmasını araşdırır. Bu modulun araşdırma sahəsinə zəifliyin təhlili üçün lazım olan xüsusi mülahizələr internetə daxilolma testindən tutmuş simsiz şəbəkə riskinin dəyərləndirməsinə qədərki məsələlər daxildir. Modul və ümumilikdə kitab fiziki təhlükəsizlik mülahizələrinin tam şəkildə əhatə olunması ilə yekunlaşır.

Kitabın xüsusiyyətləri

Aşağıda qeyd edilən xüsusiyyətlər bu kitabdan tədris vəsaiti kimi istifadə olunmasına imkan verən əsas töhfələrdir:

- *İnformasiya təhlükəsizliyi üzrə peşəkar mütəxəssislərin ümumi bilik təşkilatları* – müəlliflər həm informasiya təhlükəsizliyi üzrə ixtisaslaşmış menecer (CISM), həm də informasiya təhlükəsizliyi üzrə ixtisaslaşmış peşəkar mütəxəssis (CISSP) sertifikatlarına malik olduqları üçün onların bu sahədəki bilikləri kitabın mükəmməl olmasına müsbət təsir edib. Kitab sertifikatlaşdırma üzrə tədqiqat bələdçisinin hazırlanmasına töhfə verəcək informasiya təhlükəsizliyinin CISM və CISSP Ümumi Bilik Təşkilatının (CBK) inteqrasiyasını təmin edir.
- *Açılış və qapanış ssenariləri* – hər bir modul real həyatdakı təşkilatlarda tez-tez rast gəlinən informasiya təhlükəsizliyi problemləri ilə əhatə olunmuş xəyali şirkəti əks etdirən qısa hekayə ilə açılır və bağlanır. Hər bir modulun sonundakı ümumiləşdirici suallar toplusu tələbələrə və müəllimlərə hekayənin təklif etdiyi məsələləri müzakirə etmək və bu məsələlərin etik ölçülərini araşdırmaq imkanı verir.
- *Aydın şəkildə izah edilmiş əsas terminlər* – hər bir əsas termin terminin ilk istifadə olunduğu yerdə qeyd bölməsində ətraflı izah edilir. Bu da oxucuların terminləri daha aydın başa düşməsinə imkan verir. Mətnin özündə istifadə olunan terminlərə istinad edilərkən, təriflərin müzakirədən ayrılması əsas terminlərin daha asan təqdim olunmasına və bütün Vitman və Mattord işlərinin standartlaşdırılmasına dəstək olur.

- *Dərin izahatlar* – modullar boyunca bir-birinə səpələnmiş bu izahatlar maraqlı mövzuları və ətraflı texniki məsələləri vurğulayır və tələbələrə informasiya təhlükəsizliyi mövzularını daha dərindən araşdırmaq imkanı verir.
- *Təcrübə əsasında öyrənmə* – tələbələr hər modulun sonunda modulun icmalını, real təcrübələri nəzərdən keçirəcəklər. Real təcrübələri əhatə edən tapşırıqlar tələbələrin qarşısında öyrənmə məqsədlərini möhkəmləndirmək, oxuduqları anlayışları dərinləşdirmək və informasiya təhlükəsizliyi arenasını sinifdən kənarda yoxlamaq üçün araşdırma aparmaq, təhlil etmək və cavablar yazmaq tələbi qoyur.

Bu nəşrdəki yeniliklər

- Bütün qrafiklər və cədvəllər rəngli göstərilib.
- İnformasiya təhlükəsizliyi sahəsindəki ən yeni qanunlar və sənaye yenilikləri əhatə olunub.
- Fövqəladə halların planlaşdırılması və insidentlərə cavabla bağlı məzmun əhəmiyyətli dərəcədə təkmilləşdirilib və bu kritik mövzuya əlavə diqqət yetirmək üçün xüsusi modulda verilib.
- Risklərin idarə edilməsi metodologiyasında son dəyişiklikləri əks etdirmək üçün müvafiq modul tamamilə yenilənib.
- Kriptoqrafiyanı əhatə edən modul blokçeyn *(blockchain)* və ödəniş sisteminin təhlükəsizliyinin genişləndirilmiş əhatə dairəsini kitaba daxil etmək üçün təkmilləşdirilib.
- Sənayedə istifadə olunan terminologiya üçün artan görünmə dərəcəsi bu resursda və Vitman və Mattord seriyalarında əsas terminlərin görkəmli nümayişi ilə təmin edilib.
- Yenilənmiş və əlavə "Ətraflı məlumat üçün" bölmələri tələbələrin oxunuşda əhatə olunan fənlər haqqında daha çox məlumat tapa biləcəyi onlayn məkanları təmin edib.

İnformasiya təhlükəsizliyinin prinsipləri üçün "MindTap"

- *"İnformasiya təhlükəsizliyi prinsipləri"* kitabı üçün tam mətn və köməkçi fəaliyyətlər "Cengage"nin "MindTap" platformasında mövcuddur. Bu sizə kursunuzu tam nəzarətdə saxlamaq imkanı verir, beləliklə, siz cəlbedici məzmun təqdim edə, hər öyrənəni sınağa çəkə və onlarda özünəinam formalaşdıra bilərsiniz. Həmçinin o, yüksək prioritet mövzuları vurğulamaq üçün interaktiv proqramları fərdiləşdirmək, sonra öz materialınızı və ya qeydlərinizi elektron kitaba istədiyiniz kimi əlavə etmək imkanı verir. Nəticəyə əsaslanan bu proqram sizə tələbələri gücləndirmək və həm anlayışı, həm də performansı artırmaq üçün lazım olan alətləri təklif edir.

Ehtiyac duyduğunuz hər şeyə bir mənbədən daxil olun

Hazırlığa ayrılmış vaxtı əvvəlcədən yüklənmiş və təşkil edilmiş "MindTap" kurs materialları ilə azalda bilərsiniz. Həmçinin interaktiv multimedia, tapşırıqlar və viktorinaların köməyi ilə dərslərinizin səmərəsini artıra bilərsiniz. Bunlarla yanaşı, proqram vasitəsilə tələbələrinizə telefonlarında oxumaq, dinləmək və öyrənmək səlahiyyəti verə bilərsiniz və onlar da öz dərslərini rahat öyrənə bilərlər.

Tələbələrin öz potensiallarına çatması üçün onları gücləndirin

On iki fərqli göstərici sizə tələbənin cəlb edilməsinə dair praktiki ideyalar verir. Sinfinizi narahat edən mövzuları müəyyənləşdirin və çətinlik çəkən tələbələrlə dərhal əlaqə saxlayın. Tələbələr hədəflərinə doğru motivasiyalı qalmaq üçün öz qiymətlərini izləyə bilərlər. Siz birlikdə çox uğurlu ola bilərsiniz.

Kursunuza və məzmununuza nəzarət edin

Dərslik fəsillərini yenidən sıralamaq, öz qeydlərinizi əlavə etmək və açıq təhsil resursları (OER) da daxil olmaqla müxtəlif məzmunları daxil etmək üçün çeviklik əldə edə bilərsiniz. Kursun məzmununu tələbələrinizin ehtiyaclarına uyğunlaşdırın. Onlar hətta sizin qeydlərinizi oxuya, öz qeydlərini əlavə edə və öyrənmələrinə kömək etmək üçün əsas mətni vurğulaya da bilərlər.

Ehtiyac duyduğunuz zaman xüsusi bir komanda yaradın

"MindTap", sadəcə, bir vasitə deyil; o sizə dəstək olmaq istəyən fərdiləşdirilmiş komanda tərəfindən də dəstəklənir. Kursunuzun qurulmasında və onu xüsusi məqsədlərinizə uyğunlaşdırmaqda sizə kömək edə bilərik. Bilin ki, biz sizə və tələbələrinizə semestrin son gününə qədər kömək etmək üçün hazır olacağıq.

Vitman və Mattordun *"İnformasiya təhlükəsizliyi prinsipləri"* kitabı üçün "MindTap" fəaliyyətləri tələbələrə bugünkü işçi qüvvəsində ehtiyac duyduqları bacarıqları mənimsəməkdə kömək etmək üçün nəzərdə tutulub. Tədqiqatlar göstərir ki, işəgötürənlər sürətlə inkişaf edən, texnologiyaya əsaslanan dünyamızda aktual qalmaq üçün tənqidi düşünənlərə, problemləri həll edənlərə və yaradıcı problem həll edənlərə ehtiyac duyurlar. "MindTap" bunu əldə etməkdə sizə praktiki təcrübə, real həyatda uyğunluq və çətin anlayışların mənimsənilməsini təmin edən tapşırıq və fəaliyyətlərlə kömək edir. Tələbələr əsas bilik və anlayışdan daha çətin problemlərə doğru irəliləyən tapşırıqlar vasitəsilə istiqamətləndirilir.

Bütün "MindTap" fəaliyyətləri və tapşırıqları öyrənmə məqsədlərinə bağlıdır. Praktiki məşğələlər real həyatda tətbiq və təcrübəni təmin edir. Oxu materialları və "Whiteboard Shorts" mühazirəni dəstəkləyir, "Həyat üçün təhlükəsizlik" tapşırıqları isə tələbələri aktual olmağa və ömür boyu öyrənməyə təşviq edir. Kursdan əvvəlki və sonrakı qiymətləndirmələr sizə analitika və hesabatlardan istifadə edərək tələbələrin nə qədər öyrəndiklərini ölçmək imkanı verir ki, bu da auditoriyanın irəliləyiş, məşğulluq və tamamlama dərəcələri baxımından harada olduğunu görməyi təmin edir. Ətraflı məlumatı *www.cengage.com/mindtap/* saytından əldə edə bilərsiniz.

Müəllim üçün resurslar

Kursun tam resurs paketi *"İnformasiya təhlükəsizliyi prinsipləri"* kitabını öz kursları üçün qəbul edən bütün müəllimlərə pulsuzdur, bunu tək giriş (SSO) vasitəsilə əldə edə bilərlər. Bunun üçün müəllimlər *cengage.com* saytında SSO hesabı tələb edə bilərlər.

Resurslara aşağıdakılar daxildir:

- *Müəllim üçün vəsait* – bu vəsaitə kursun məqsədləri, əsas şərtlər, tədris planları və məsləhətlər, testlər və təliminizi planlaşdırmağa və asanlaşdırmağa kömək edəcək əlavə məlumatlar daxildir.
- *Həllər üzrə təlimat* – bu resurs özündə modulun sonundakı bütün nəzərdən keçirmə sualları və tapşırıqları üçün cavabları və izahatları ehtiva edir.
- *"Cognero" tərəfindən dəstəklənən "Cengage" testi* – çevik, onlayn sistem sizə mətnin test bankından və ya başqa yerdən məzmunu, o cümlədən öz sevimli test suallarınızı idxal etməyə, redaktə etməyə və adaptasiya etməyə imkan verir; bir anda birdən çox test versiyası yaradın və LMS-dən, sinif otağınızdan və ya istədiyiniz yerdə testləri çatdırın.
- *"PowerPoint" təqdimatları* – hər modul üçün "Microsoft PowerPoint" slaydları dəsti daxil edilir. Bu slaydlar sinif təqdimatları üçün tədris vəsaiti kimi istifadə edilmək, modulun nəzərdən keçirilməsi üçün tələbələrə təqdim olunmaq və ya sinifdə paylanması üçün çap edilmək üçün nəzərdə tutulub. Bəzi cədvəllər və rəqəmlər

"PowerPoint" slaydlarına daxil edilib; lakin hamısı onlayn təlimatçı resurslarında mövcuddur. Təlimatçılar öz slaydlarını əlavə etməkdə sərbəstdirlər.

- *"MindTap" nəşrində və müəllim üçün resurs dəstində (IRK) mövcud laboratoriya məşğələləri* – müəlliflər tərəfindən yazılmış bu təlimlərdən texniki təcrübəni təmin etmək üçün mətnlə birlikdə istifadə oluna bilər. Əlavə məlumat üçün "Cengage" öyrənmə məsləhətçinizlə əlaqə saxlayın.
- *Oxu nümunələri və keyslər* – "Cengage" həmçinin müəlliflər tərəfindən iki mətn hazırlayıb: "Readings and Cases in Management of Information Security" (ISBN-13: 9780619216276) və "Readings & Cases in Information Security: Law & Ethics" (ISBN-13: 9781435441576). Bunlar əla müşayiət mətnləridir. Əlavə məlumat üçün "Cengage" öyrənmə məsləhətçinizlə əlaqə saxlayın.
- *İnformasiya təhlükəsizliyi/kibertəhlükəsizlik üzrə təhsil proqramları üçün kurikulum modeli* – bu komandanın müəllifi olduğu mətnlərdən əlavə informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə təhsil proqramları üçün kurikulum modeli Kenneso Dövlət Universitetinin (KDU) Kibertəhlükəsizlik İşçi Qüvvəsinin İnkişafı İnstitutundan əldə edilə bilər. *(https://cyberinstitute.kennesaw.edu/docs/ModelCurriculum-2021.pdf).* Bu sənəddə müəlliflərin təhlükəsizlik üzrə kurs işlərinin və kurikulumların hazırlanmasındakı və həyata keçirilməsindəki təcrübələri, həmçinin təlimatlar və öyrənilmiş dərslər haqqında ətraflı məlumat verilir.

Müəllifin komandası

Maykl Vitman və Herbert Mattord bu mətni akademik tədqiqatlardan əldə edilən bilikləri iş dünyasının praktik təcrübəsi ilə birləşdirmək üçün birgə işləyib-hazırlayıblar.

***Maykl E. Vitman Ph.D., CISM, CISSP*,** informasiya təhlükəsizliyi və təminat üzrə professor və KDU Kibertəhlükəsizlik İşçi Qüvvəsinin İnkişafı İnstitutunun *(cyberinstitute.kennesaw.edu)* icraçı direktorudur. Dr. Vitman informasiya təhlükəsizliyi, ədalətli və məsuliyyətli istifadə siyasətləri, etik hesablamalar və kurikulumun hazırlanması metodologiyaları sahəsində fəal tədqiqatçıdır. Hazırda o, informasiya təhlükəsizliyi və kibertəhlükəsizliyin idarə edilməsi üzrə magistratura və bakalavr kursları üzrə dərs deyir. O öz sahəsində ən yaxşı jurnallarda, o cümlədən *"Information Systems Research", "Communications of the ACM", "Information and Management", "Journal of International Business Studies", "Journal of Computer Information Systems"* nəşrlərində məqalələrini dərc etdirib. Dr. Vitman həm də Mattordla birgə *"Journal of Cybersecurity Education, Reserach and Practice"* jurnalının baş redaktorudur. Dr. Vitman həmçinin "Cengage" tərəfindən nəşr olunan digər kitablarla yanaşı, *"Management of Information Security"* və *"Principles of Incident Response and Disaster Recovery"* kitablarının da həmmüəllifidir. Dr. Vitman akademik karyerasına başlamazdan əvvəl ABŞ ordusunun zabiti olub və avtomatlaşdırılmış məlumatların emalı sistemləri təhlükəsizliyi üzrə mütəxəssis (ADPSSO) kimi məsul vəzifəni icra edib.

Herbert C. Mattord, Ph.D., CISM, CISSP, 2002-ci ildə KDU-nun fakültəsinə qoşulmazdan əvvəl proqram tərtibatçısı, verilənlər bazası inzibatçısı, layihə meneceri və informasiya təhlükəsizliyi üzrə mütəxəssis kimi IT sənayesində 24 illik təcrübəni başa vurub. Dr. Mattord KDU Kibertəhlükəsizlik İşçi Qüvvəsinin İnkişafı İnstitutunun *(cyberinstitute.kennesaw.edu)* təhsil və təşkilat direktorudur. Dr. Mattord həm də Vitmanla birgə *"Journal of Cybersecurity Education, Reserach and Practice"* jurnalının baş redaktorudur. IT mütəxəssisi kimi karyerası ərzində o, KDU-da, Marietta Cənubi Politexnik Dövlət Universitetində (Corciya), Ostin İcma Kollecində (Texas) və Texas Dövlət Universitetində (San-Markos) köməkçi professor olub. Hazırda o, informasiya təhlükəsizliyi və kibertəhlükəsizlik üzrə magistratura və bakalavr kursları üzrə dərs deyir. O, əvvəllər "Georgia-Pacific Corporation"da korporativ informasiya texnologiyaları təhlükəsizliyi üzrə menecer olub, bu resursdakı praktiki biliklərin çoxunu burada əldə edib. Dr. Mattord həmçinin "Cengage" tərəfindən nəşr olunan *"Management of Information Security", "Principles of Incident Response and Disaster Recovery"* və digər əsərlərin həmmüəllifidir.

Minnətdarlıq

Müəlliflər bu layihəyə həsr olunmuş zamana, əksər hallarda “ailənin əlindən alınan” saatlara, habelə dəstək və anlayışlarına görə ailələrinə təşəkkür edirlər.

Əsərə töhfə verənlər

Bir neçə şəxs və təşkilat da bu resurs üçün materiallar təqdim edib və biz onlara töhfələrinə görə təşəkkür edirik:

- Mətnin bir çox hissələrində istifadə olunan bəzi istinadların, cədvəllərin, rəqəmlərin və digər məzmunun mənbəyi Milli Standartlar və Texnologiya İnstitutudur (NIST).

Rəyçilər

Kitabın modullarının nəzərdən keçirilməsi zamanı öz əvəzedilməz rəylərinə görə aşağıdakı rəyçilərə borcluyuq:

- Paul Vitman, Kaliforniya Lüteran Universiteti
- Mia Plaçkinova, Kenneso Dövlət Universiteti

Xüsusi təşəkkürlər

- Müəlliflər “Cengage”də redaksiya və istehsal qruplarına təşəkkür edirlər. Onların çalışqan və peşəkar səyləri son məhsulu əhəmiyyətli dərəcədə təkmilləşdirdi:
- Den Zeyter, inkişaf üzrə redaktor
- Daniel Klar, assosiativ məhsul meneceri
- Kristina Nayren, kontent meneceri

Bundan əlavə, bir neçə peşəkar təşkilat, kommersiya təşkilatları və şəxslər məlumat və ilham verərək mətnin inkişafına kömək ediblər. Müəlliflər aşağıdakı şəxslərin töhfələrini etiraf etmək istəyirlər:

- Donn Parker
- Kenneso Dövlət Universitetinin İnformasiya sistemləri departamenti və Koulz Biznes Kollecindəki həmkarlarımız

Bizim öhdəliyimiz

Müəlliflər bu resursun istifadəçilərinin ehtiyaclarına xidmət etməyə çalışırlar. Mətn və köməkçi materiallarla bağlı rəy almaqdan məmnunluq və qürur duyuruq. Bizimlə infosec@kennesaw.edu ünvanında əlaqə saxlaya bilərsiniz.

Ön söz

İnformasiya təhlükəsizliyi elmdən daha çox sənətdir. Məlumatı qorumaq ustalığı böyük həcmdə məlumat, həmçinin təcrübə və bacarıq haqqında multidisiplinar bilik tələb edir. Müəlliflər hər bir mövzunu təqdim etmək üçün real həyat ssenarilərindən istifadə edərək sizi təhlükəsizlik sistemlərinin inkişaf dövrü boyunca müşayiət etdikləri üçün bu resursda sizə lazım olanların çoxunu burada tapa bilərsiniz. Müəlliflər bu mətndə əks etdirilən zəngin öyrənmə təcrübəsi üçün öz akademik yanaşmaları ilə çoxillik həyat təcrübələrini birləşdirərək öz perspektivlərini təqdim edirlər. Siz müəllifləri və bu mənbəni yaxşı seçmisiniz.

Bunu oxuduğunuz üçün, çox güman ki, informasiya təhlükəsizliyi sahəsində karyera qurmağa çalışırsınız və ya ən azı informasiya təhlükəsizliyi ilə ciddi maraqlanırsınız. Təhlükəsizliyin onların işinə qoyduğu məhdudiyyətlərə hər kəsin nifrət bəslədiyini təxmin etməlisiniz. Buraya öhdəsindən gəlmək üçün bir problem olaraq qurduğumuz təhlükəsizliyi bəyənən zərərli hakerlər istisna olmaqla həm yaxşı adamlar, həm də pis adamlar daxildir. Biz günahkarları dayandırmağa qəsdən diqqət yetiririk, çünki bu, təsadüfən səhv edənlərin də dayandırılmasına aiddir. Bilməyərəkdən səhv edənlərdən qorunmaq üçün lazım olan təhlükəsizlik qəsdən səhv edənlərə münasibətdə kifayət deyil.

Mən həyatımın 40 ilini həyəcanlı və faydalı saydığım bir sahəyə sərf etmişəm, kompüterlərlə işləmişəm və pisniyyətli insanlara qarşı olmuşam. Təhlükəsizliyə nəzarət və təcrübələrə daxil olmaq və söndürmək, parollardan istifadə etmək, mühüm məlumatların şifrlənməsi və ehtiyat nüsxəsinin çıxarılması, qapıların və siyirmələrin kilidlənməsi, maraqlı tərəflərin təhlükəsizliyi dəstəkləməyə həvəsləndirilməsi və antivirus proqramının quraşdırılması daxildir.

Bu müdafiə vasitələrinin heç bir faydası yoxdur. Yaxşı təhlükəsizlik pis heç nə baş verməyəndə qüvvədə olur. Pis heç nə baş verməyəndə təhlükəsizlik kimə lazımdır? Hazırda təhlükəsizliyə ehtiyacımızın səbəblərindən biri də qanunların, tənzimləmələrin və auditlərin bunu tələb etməsidir – xüsusilə də digərlərinin şəxsi məlumatları, elektron pul, intellektual mülkiyyət və rəqabətdə üstünlük qazanmaq kimi məsələlərlə məşğul oluruqsa...

İşəgötürəninizin məlumat və sistemlərinin kifayət qədər təhlükəsiz olduğunu və yaxşı maaş aldığınızı, fövqəladə hallarda diqqət mərkəzində olduğunuzu və pis adamlara qarşı ağlınızdan istifadə etdiyinizi bilmək böyük məmnuniyyət hissi doğurur. Bu, təhlükəsizlik işinizin mənfi tərəflərini tamamlayır. Mükəmməlliyə meyilli şəxslər üçün bu, iş deyil, çünki siz, demək olar ki, heç vaxt tam uğur qazana bilməyəcəksiniz, sizin bilmədiyiniz və ya pis adamların əvvəlcə kəşf etdiyi zəifliklər həmişə olacaq. Düşmənlərimizin bizdən böyük üstünlüyü var. Onlar seçdikləri vaxtda elektron və ya fiziki olaraq məlum yerdə hücum etmək üçün yalnız bir zəiflik və bir hədəf tapmalıdır, biz isə özümüzü artıq bir kompüter otağında olmayan aktivlərə və zəifliklərə qarşı potensial olaraq milyonlarla hücumdan müdafiə etməliyik. Bu, rəqiblərinizi və onların harada olduqlarını, nə etdiklərini və ya bunu niyə etdiklərini bilmədiyiniz bir oyun oynamaq kimidir və onlar oynayarkən qaydaları gizlicə dəyişirlər. Siz çox etik və ehtiyatlı olmalı, müdafiə olunmalı, gizli qalmalısınız. İstifadə etdiyiniz böyük təhlükəsizlik sistemləri ilə düşməni dəf edə bilməlisiniz. Yaşadığınız bir neçə uğurdan həzz alın, çünki onlardan bəziləri haqqında heç xəbəriniz belə olmayacaq. Unutmayın ki, təhlükəsizlikdə işləyərkən işəgötürəninizi və maraqlı tərəflərinizi düşmənlərindən müdafiə edən virtual ordudasınız. Sizin nöqteyi-nəzərinizə görə, düşmənlər, yəqin ki, məntiqsiz düşünəcək və hərəkət edəcəklər, lakin onların nöqteyi-nəzərindən, onlar tamamilə rasionaldırlar, həll edilməli olan məsələlər ciddi şəxsi problemləri və təhlükəsizliyinizi pozmaqla əldə ediləcək qazanclarla bağlıdır. Siz artıq sistemlərdə və şəbəkələrdə texnoloji nəzarətlərin quraşdırılması kimi çətin işi olan, sadəcə, texniki mütəxəssis deyilsiniz. İşinizin çoxu potensial qurbanlara özlərini informasiya çətinliklərindən qorumaqda kömək etmək və ağıllı, lakin çox vaxt irrasional düşmənlərinizlə məşğul olmaqdan ibarət olmalıdır, baxmayaraq ki, siz onları nadir hallarda görürsünüz və ya hətta müəyyən edirsiniz. Mən təhlükəsizlik karyeramın əsas hissəsini kompüter cinayətkarlarını ovlamaqla, onlarla və onların qurbanları ilə müsahibə aparmaqla, hücumlarından daha yaxşı müdafiə olunmaq üçün anlayışlar əldə etməyə çalışmaqla keçirdim. Eynilə hücumçuları axtarmaq, onların hərəkətlərinə nəyin səbəb olduğunu və necə işlədiyini anlamaq üçün hər fürsətdən istifadə etməlisiniz. Bu təcrübə hətta bir neçə düşmənə minimal məruz qalma ilə belə əsl və unikal ekspert kimi sizə böyük imkan verir. Əhatəlilik real təkliflər üçün oynadığınız oyunun vacib hissəsidir, çünki düşmən, çox güman ki, hələ tam qorumadığınız və ya mövcudluğunu bilmədiyiniz zəifliklərə və aktivlərə hücum etmək üçün ən asan yolu axtaracaq. Məsələn, təhdid siyahılarında nadir hallarda rast gəlinən təhlükə aktivlərin təhlükəyə atılmasıdır – informasiya aktivlərini zərərə salmaqdır. Təhlükə həm də təhlükəsizlik mütəxəssisləri öz təhlükəsizlik və itki təcrübələri haqqında çox şey aşkar etdikdə ən çox rast gəlinən pozuntulardan biridir.

Siz hərtərəfli və vasvası olmalısınız, çünki səriştəniz şübhə altına alınarsa və Sarbeyns-Oksli qanununun tələblərinə cavab verərsə, hər şeyi sənədləşdirməlisiniz. Sənədlərinizi təhlükəsiz şəkildə kilidli saxlayın. Sənədləşmə vacibdir ki, çətinliyə düşəndə və oyunu uduzduqda itkiyə baxmayaraq, çalışqan olduğunuzu sübut edəcəksiniz. Əks halda, karyeranız zədələnə və ya ən azı effektivliyiniz azala bilər.

Məsələn, əgər itki rəhbərliyin sizə adekvat büdcə və tələb etdiyiniz təhlükəsizlik dəstəyi verməməsi səbəbindən baş veribsə, siz hadisə baş verməzdən əvvəl bu uğursuzluğu sənədləşdirməlisiniz. Təhlükəsizliyinizlə öyünməyin, çünki o, həmişə məğlub edilə bilər. Hər şey üçün yoxlama siyahılarını saxlayın və genişləndirin: təhdidlər, zəifliklər, aktivlər, əsas potensial qurbanlar, qanunsuzluqda şübhəli bilinənlər, təhlükəsizliyin tərəfdarları və tərəfdarları olmayanlar, hücumlar, düşmənlər, cinayət ədaləti mənbələri, auditorlar, tənzimləyicilər və hüquq məsləhətçiləri. Məlumat və sistemlərinin ön cəbhədə müdafiəçiləri olan maraqlı tərəflərinizə kömək etmək üçün onların nəyi qorumalı olduqlarını müəyyənləşdirin ki, öz təhlükəsizliklərinin real ölçüsünü bilsinlər.

Yuxarı rəhbərliyin və hesabat verdiyiniz digər insanların işinizin mahiyyətini və onun məhdudiyyətlərini başa düşdüyünə əmin olun.

Yaxşı bir nümunə göstərmək üçün mümkün olan ən yaxşı təhlükəsizlik təcrübələrindən özünüz istifadə edin. İşinizi yerinə yetirmək üçün çoxlu həssas parol kolleksiyanız olacaq. Bu etimadnamələri əlçatan, lakin təhlükəsiz şəkildə saxlamaq üçün bir yol tapın – məsələn, smartfon proqramı ilə. Təşkilatınızdakı sistemlər və şəbəkələr haqqında mümkün qədər çox məlumat əldə edin və qalanını bilən mütəxəssislərə erişim əldə edin. Yerli və milli ədliyyə məmurları, təşkilatınızın hüquqşünasları, sığorta riski menecerləri, insan resursları işçiləri, obyekt menecerləri və auditorlarla dostluq edin.

Auditlər təşkilatınızın sahib olduğu ən güclü nəzarətlərdən biridir. Unutmayın ki, insanlar təhlükəsizliyə nifrət edirlər və o işləməsi üçün cəzalar və mükafatlar tərəfindən düzgün motivasiya edilməlidir. Təhlükəsizliyi effektiv saxlamaqla onu maraqlı tərəflər üçün görünməz və ya şəffaf etməyin yollarını axtarın. Maraqlı tərəflərin dəstəkləməyəcəyi nəzarətləri və ya təcrübələri tövsiyə etməyin və ya quraşdırmayın, çünki onlar hər dəfə nəzarətləri effektiv olmadıqda bunu göstərib sizi məğlub edəcəklər – vəziyyət, ümumiyyətlə, təhlükəsizliyin olmamasından daha pisdir.

İşin ən maraqlı hissələrindən biri təşkilatınızın daxili işləri və sirləri, biznesi və mədəniyyəti haqqında əldə etdiyiniz fikirlərlə bağlıdır. İnformasiya təhlükəsizliyi üzrə məsləhətçi kimi mənə dünyanın 250-dən çox ən böyük korporasiyasının mədəniyyəti və sirləri haqqında məlumat almaq imtiyazı verilmişdi. Dəyərli vaxtlarının bir neçə dəqiqəsi olsa da, ən güclü biznes rəhbərləri ilə müsahibə almaq və onlara məsləhət vermək imkanım oldu. Siz həmişə "gümüş güllə" ilə hazır olmalısınız ki, bu da müəssisənin təhlükəsizliyinin ən böyük faydasından ötrü qısa müddət ərzində top menecmentə tövsiyə etmək üçün yüksək təsirli həldir.

Rəhbərliyin təhlükəsizlik iştahasının sərhədlərini diqqətlə öyrənin. İstər dövlət idarəsi olsun, istərsə də qızğın rəqabətli biznes olsun, işin mahiyyətini bilin. Bir dəfə direktorlar şurası ilə görüşdə anladım ki, onların ən böyük ticarət sirri olan yeni birdəfəlik uşaq bezlərinin istehsal prosesinin qorunması intensiv müzakirə edilir.

Nəhayət, son vacib məsləhətə gəlirik. Etibarlı olun və yoldaşlarınız arasında qarşılıqlı inamı inkişaf etdirin. Ən mühüm məqsədləriniz təkcə risklərin azaldılması və təhlükəsizliyin artırılması deyil. Onlar həmçinin səhlənkarlıq və təhlükədən qaçmaq üçün səy göstərməyi, bütün qanunlara və standartlara riayət etməyi, təhlükəsizlik rəqabətli və ya büdcə məsələsinə çevrildikdə imkanları əhatə edir. Bu məqsədlərə nail olmaq üçün yoldaşlarınız arasında ən həssas təhlükəsizlik kəşfiyyatının etibarlı mübadiləsini inkişaf etdirməlisiniz ki, təşkilatınızın digər müəssisələrə nəzərən harada olduğunu biləsiniz. Ancaq bu məsələdə təmkinli və diqqətli olun. Siz ümumi qəbul edilmiş və cari təhlükəsizlik həllərini bilməlisiniz. Mübadilə etdiyiniz məlumat ifşa olunsa, bu, karyeranızı və başqalarını məhv edə və təşkilatınız üçün fəlakət yarada bilər. Sizin şəxsi və etik performansınız ləkəsiz olmalıdır və nəyin bahasına olursa olsun, öz nüfuzunuzu qorumalısınız. Bu resursun etika bölməsinə xüsusi diqqət yetirin. Tövsiyə edirəm ki, İnformasiya Sistemlərinin Təhlükəsizliyi Assosiasiyasına üzv olasınız, orada fəallaşasınız və ixtisasa yiyələnən kimi peşəkar sertifikat alasınız. Mənim sevimli sertifikatım Beynəlxalq İnformasiya Sistemlərinin Təhlükəsizliyi Sertifikatlaşdırma Konsorsiumunun "İnformasiya sistemlərinin təhlükəsizliyi üzrə ixtisaslaşmış peşəkar mütəxəssis" (CISSP) sertifikatıdır.

Donn B. Parker, *CISSP təqaüdçüsü*
*Sanniveyl, Kaliforniya*Principles of Information Security,
7th Edition

Michael E. Whitman and Herbert J. Mattord

SVP, Higher Education Product Management: Erin Joyner

VP, Product Management: Thais Alencar

Product Director: Mark Santee