

۱۵۱۵۱۴۰

۹۶,۵,۲

به نام خدا



آنچه هر مهندس در باره

امنیت سایبری

باید بداند

مترجمین :

دکتر شهناز محمدی مجد

مهندس محمد علی کاشی

هر گونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی
ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق
مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

آنچه هر مهندس در باره

امنیت سایبری باید بداند

عنوان کتاب اصلی:

What every Engineer should know
About Cyber Security and Digital Forensics

مترجمین: دکتر شمس‌الدین محمد مجد

مهندس محمد علی کاشی

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

حروفچینی و صفحه‌آرایی: مانا جال آباد

طرح روی جلد: داریوش فرسای

ویراستار: فرانک شاه مرادی

چاپ: نگین

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۶

تیراژ: ۱۰۰ جلد

قیمت: ۲۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۱۲۴-۶۳۷-۱

نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

کد پستی: ۱۳۱۴۹۸۳۱۸۵

پست الکترونیکی: bookmarket@mftmail.com

فروش اینترنتی: www.mftshop.com

www.mftbook.ir

سرشناسه: دفرانکو، جوآنا اف .

DeFranco, Joanna F

عنوان و نام پدید آور: آنچه هر مهندس در باره امنیت
سایبری باید بداند / [جوآنا اف دفرانکو] مترجمین: شهناز
محمدی مجد، محمد علی کاشی

مشخصات نشر: تهران- دیباگران تهران- ۱۳۹۶

مشخصات ظاهری: ۱۸۶ ص. مصور.

شابک: ۹۷۸-۶۰۰-۱۲۴-۶۳۷-۱

وضعیت فهرست نویسی: فیا

یادداشت: عنوان اصلی: What every Engineer should know

About Cyber Security and Digital Forensics - 2014

موضوع: شبکه های کامپیوتری - تدابیر ایمنی

موضوع: computer networks-security measures

موضوع: کام - و تر ها - ایمنی اطلاعات

موضوع: computer security

موضوع: چرا - کام - رای - ایمنی جویی

موضوع: computer crime investigation

شناسه افزوده: محمدی مجد، شهناز - ۱۳۹۶ - مترجم

شناسه افزوده: کاشی، محمد علی - ۱۳۹۶ - مترجم

رده بندی کنگره: TK ۱۱۰۵/۵۹/۵۷۸۳ ۱۳۹۶

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۴۷۷۳۱۶۸

نشانی اینستاگرام: [Dibagaran_publishing](https://www.instagram.com/Dibagaran_publishing)

نشانی تلگرام: [@mftbook](https://www.t.me/mftbook)

فهرست مطالب

فصل اول	۱۱
تهدیدات امنیتی	۱۱
۱-۱ مقدمه	۱۲
۱-۲ مهندسی اجتماعی	۱۴
۱-۳ حاکم	۱۸
۱-۴ دستگاه‌های اِنل	۱۹
۱-۵ اینترنت	۲۰
۱-۶ فضای ابری	۲۱
۱-۷ تجهیزات سایبری	۲۴
۱-۸ سرقت	۲۵
فصل دوم	۲۷
امنیت سایبری و فرصت‌های شغلی پزشکی قانونی دیجیتال	۲۷
۲-۱ مقدمه	۲۸
۲-۲ فرصت‌های شغلی	۲۸
۲-۲-۱ فهرست خلاصه‌ای از وظایف شغلی امنیت فناوری اطلاعات	۳۱
۲-۲-۲ فهرست خلاصه‌ای از وظایف شغلی پزشکی قانونی دیجیتال	۳۴
۲-۳ گواهی‌نامه‌ها	۳۹
۲-۳-۱ گواهی‌نامه‌های امنیت فناوری اطلاعات	۴۰
۲-۳-۲ گواهی‌نامه‌های پزشکی قانونی دیجیتال	۵۲
فصل سوم	۵۷
امنیت سایبری	۵۷

۵۸ ۳-۱ مقدمه

۵۹ ۳-۲ امنیت اطلاعات

۶۲ ۳-۳ معماری امنیت

۶۳ ۳-۴ کنترل‌های دسترسی

۶۸ ۳-۵ رمزنگاری

۷۱ ۳-۵-۱ انواع رمزنگاری یا الگوریتم‌های رمزنگاری

۷۲ ۳-۶ امنیت شبکه و ارتباطات راه دور

۷۳ ۳-۷ امنیت سیستم‌عامل

۷۵ ۳-۸ امنیت توسعه نرم‌افزار

۷۸ ۳-۹ امنیت پایگاه داده

۷۹ ۳-۱۰ تداوم کسب‌وکار و بازیابی (BC/DR)

۸۰ ۳-۱۱ امنیت فیزیکی

۸۱ ۳-۱۲ قوانین، مقررات، تطابق، و تحقیقات

۸۲ ۳-۱۳ امنیت عملیات

۸۳ ۳-۱۴ اداره امنیت اطلاعات و مدیریت ریسک

۸۷ فصل چهارم

۸۷ آمادگی برای حادثه

۸۸ ۴-۱ مقدمه

۸۹ ۴-۱-۱ چارچوب Zachman

۹۰ ۴-۱-۲ اقتباس از چارچوب Zachman برای آماده‌سازی پاسخ به حادثه

۹۴ ۴-۲ شناسایی مخاطرات

۹۷ ۴-۳ آماده‌سازی میزبان

۱۰۱ ۴-۴ آماده‌سازی شبکه

۴-۵ ایجاد سیاست‌ها و دستورالعمل‌های مناسب ۱۰۵

۴-۶ آماده‌سازی تیم پاسخ به حادثه ۱۱۴

۴-۷ آماده‌سازی ابزار پاسخ ۱۱۶

۴-۸ آموزش ۱۲۰

فصل پنجم ۱۲۵

واکنش حادثه و پزشکی قانونی دیجیتال ۱۲۵

۵-۱ مقدمه ۱۲۶

۵-۲ پاسخ به حادثه ۱۲۷

۵-۲-۱ آشکارسازهای حساس ۱۲۸

۵-۲-۲ مهار ۱۳۰

۵-۲-۳ قلع و قمع ۱۳۱

۵-۲-۴ بازسازی ۱۳۲

۵-۳ پاسخ به حادثه برای رایانش ابری ۱۳۴

۵-۴ پزشکی قانونی دیجیتال ۱۳۶

۵-۴-۱ آماده‌سازی ۱۳۷

۵-۴-۲ جمع‌آوری ۱۳۹

۵-۴-۳ تجزیه و تحلیل ۱۴۱

۵-۴-۴ گزارش ۱۴۴

۵-۵ پزشکی قانونی گوشی موبایل ۱۴۷

فصل ششم ۱۵۱

قانون ۱۵۱

۶-۱ مقدمه ۱۵۲

۶-۲ تطابق و پیروی ۱۵۲

۱۵۳.....	۶-۲-۱ قانون پاسخگویی و قابلیت انتقال بیمه سلامت (HIPAA)
۱۵۴.....	۶-۲-۲ استاندارد امنیت داده برای صنعت کارت پرداخت (PCI-DSS)
۱۵۵.....	۶-۲-۳ شرکت اطمینان برق آمریکای شمالی - کمیته حفاظت از زیرساخت حساس (NERC-CIP)
۱۵۶.....	۶-۲-۴ قانون Gramm-Leach-Bliley (GLBA)
۱۵۷.....	۶-۲-۵ قانون Sarbanes-Oxley (SOX)
۱۵۸.....	۶-۶ قانون مدیریت امنیت اطلاعات فدرال (FISMA)
۱۵۸.....	۶-۳ قانون اخذ شواهد و مدارک
۱۶۳.....	۶-۴ قوانین شهرداری و دیاب
۱۶۴.....	۶-۵ تحقیقات قضایی دیجیتال (E-discovery)
۱۶۶.....	۶-۶ موارد قانونی
۱۶۹.....	فصل هفتم
۱۶۹.....	از تئوری تا عمل
۱۷۰.....	۷-۱ مقدمه
۱۷۰.....	۷-۲ مطالعه موردی ۱: تا وقتی که چیزی پاک نشده باشد، همه چیز خوب است
۱۷۴.....	۷-۲-۱ گزارش پس از واکنش
۱۷۷.....	۷-۳ مطالعه موردی ۲: چگونه برای شما کار می‌کند؟
۱۷۹.....	۷-۳-۱ گزارش پس از واکنش
۱۸۰.....	۷-۴ مطالعه موردی ۳: ضعیف‌ترین اتصال
۱۸۰.....	۷-۴-۱ سابقه
۱۸۱.....	۷-۴-۲ جرم
۱۸۱.....	۷-۴-۳ محاکمه
۱۸۵.....	۷-۴-۴ گزارش پس از واکنش

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب الکترونیک است که تواند خواسته های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد

حمد و سپاس ایزد منان را که با الطاف بیکران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مرز واقع شویم.

گسترده گی علوم و توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی ترین و رایج ترین راه دستیابی به اطلاعات و اطلاع رسانی، بیش از پیش روشن می نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، نققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش های مستمر و بی وقفه برای رفع کمبودها و نیازهای موجود، منابعی پربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "سرکار خانم دکتر شهناز محمدی مجد- و جناب آقای مهندس محمد علی کاشی" و تلاش جمعی از همکاران این نشریات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش پژوه گرامی درخواست می نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که به دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران

Publishing@mftmail.com

مقدمه مترجمان :

خیلی از زمانی که می‌توانستیم بسادگی از اطلاعات خود محافظت کنیم، نمی‌گذرد. همانطور که با گذشت زمان پارادایم‌های فضای سایبری تغییر می‌کنند، دیوارهای آتش و نرم‌افزارهای ضدویروس برای حفاظت از دارائی‌های اطلاعاتی ما کافی نیستند. افراد و سازمان‌ها می‌بایست با آموزش مداوم خود را با تغییرات جدید سازگار کرده و راه‌های مقابله با خطرات جدید را فرا بگیرند.

این کتاب به هدف را دنبال می‌کند. اولین هدف آن است که مفاهیم امنیت سایبری را برای مهندسان توضیح دهیم. هدف دوم، نمایش نحوه استفاده از مفاهیم امنیتی ارائه شده است. این امر با معرفی پرونده‌های واقعی انجام می‌شود. و هدف نهایی، ارائه اطلاعات لازم برای گواهینامه‌ها در زمینه امنیت سایبری برای کسانی است که خواهند در این حوزه به طور حرفه‌ای فعالیت کنند.

نقطه نظرات، پیشنهادات و انتقادات خود را می‌توانید با آدرس ایمیل زیر با مترجمان در میان بگذارید:

mohammad.ali.kashi@gmail.com