مؤسسه فرهنگی هنری
دیباگران تهران

به نام خدا

امنیت سایبری امروز

حملات سایبری،امنیت شبکه و پیشگیری از تهدیدات

مؤلف:
Debrupa Palit

مترجم:
شهروز ستوده

مؤسسه فرهنگی هنری دیباگران تهران

◂ عنوان کتاب: **امنیت سایبری امروز**

حملات سایبری،امنیت شبکه و پیشگیری از تهدیدات

◂ مترجم : **شهروز ستوده**

◂ **ناشر: موسسه فرهنگی هنری دیباگران تهران**

◂**ویراستار:** مهدیه مخبری

◂**صفحه آرایی:** نازنین نصیری

◂**طراح جلد:**داریوش فرسایی

◂ **نوبت چاپ:** اول

◂ **تاریخ نشر:** ۱۴۰۴

◂ **چاپ و صحافی:**صدف

◂ **تیراژ:**۱۰۰ جلد

◂ **قیمت:**۵۰۰۰۰۰۰ ریال

◂ **شابک:** ۰-۹۴۴-۲۱۸-۶۲۲-۹۷۸

نشانی واحد فروش: تهران، خیابان انقلاب، خیابان شهدای ژاندارمری-بین ۱۲ فروردین و فخر رازی- پلاک۸۸ طبقه دوم-واحد۶ تلفن: ۶۶۹۵۶۸۹۴-۶۶۹۶۵۷۴۹

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

سرشناسه:پالیت،دبروپا Palit,Debrupa

عنوان و نام پدیدآور:امنیت سایبری امروز:حملات سایبری،امنیت شبکه و پیشگیری از تهدیدات/(دبروپا پالیت)؛مترجم:شهروز ستوده؛ ویراستار:مهدیه مخبری.

مشخصات نشر: تهران : دیباگران تهران :۱۴۰۴

مشخصات ظاهری:۳۳۴ ص:مصور،

شابک: ۰-۹۴۴-۲۱۸-۶۲۲-۹۷۸

وضعیت فهرست نویسی: فیپا

یادداشت:عنوان اصلی: Cybersecurity:cyber attacks,network security, and threat prevention

عنوان دیگر:حملات سایبری،امنیت شبکه و پیشگیری از تهدیدات.

موضوع:شبکه های کامپیوتری-تدابیر ایمنی

موضوع:computer networks-security measures

موضوع:کامپیوترها-ایمنی اطلاعات-تدابیر ایمنی

موضوع:computer security-securrity measures

موضوع:هک کردن-پیشگیری

موضوع:hacking-prevention

شناسه افزوده:ستوده،شهروز،۱۳۵۳-مترجم

رده بندی کنگره:TK ۵۹/۵۱۰۵

رده بندی دیویی:۸/۰۰۵

شماره کتابشناسی ملی:۱۰۱۴۸۴۰۷

نشانی تلگرام:@mftbook نشانی اینستاگرام دیبا dibagaran_publishing

فهرست مطالب

فصل ۲

فصل ۳

فصل ۴

فصل ۵

فصل ۶

فصل ۷

فصل ۸

فصل ۹

روندهای نوظهور و مباحث پیشرفته در امنیت سایبری ۳۰۸

مقدمه ناشر

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

هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

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 و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم وسرعت 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 قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که در دست دارید تألیف **"جناب آقای شهروز ستوده"** است که با تلاش همکاران ما در نشر دیباگران تهران منتشرگشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات وخواسته های خود،به ما کمک کنید تا بهتر و دقیق تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم.برای رساندن پیام هایتان به ما از رسانه های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران

dibagaran@mftplus.com

پیشگفتار

کتاب حاضر به‌صورت جامع به مباحث اساسی و پیشرفته امنیت سایبری می‌پردازد؛ از مفاهیم پایه‌ای تا مباحث پیشرفته هک، قوانین سایبری، شناسایی بدافزارها، شبکه‌های بی‌سیم و راهکارهای امنیتی برای حضور امن در دنیای دیجیتال. با پرداختن به این حوزه‌ها، کتاب درکی فراگیر از فناوری‌ها و تهدیداتی که محیط آنلاین ما را شکل می‌دهند، ارائه می‌دهد. این اثر با تشریح دقیق پیچیدگی‌های امنیت سایبری، افراد مبتدی را توانمند می‌سازد تا با اطمینان در فضای دیجیتال حرکت کرده و از خود و دارایی‌های دیجیتالشان در برابر تهدیدات نوظهور محافظت کنند؛ و بدین ترتیب در ایجاد محیطی آنلاین امن‌تر برای همگان نقش‌آفرینی نمایند.

این کتاب، شالوده‌ای از اصول امنیت سایبری، شناختی عملی از روش‌ها و تاکتیک‌های هکرها، درکی روشن از چارچوب‌های قانونی، و مهارت‌های ضروری برای شناسایی و مقابله مؤثر با تهدیدات سایبری در اختیار خواننده قرار می‌دهد؛ دانشی که او را برای حضور آگاهانه و مطمئن در فضای دیجیتال توانمند می‌سازد.

کتاب شامل نه فصل است که به ترتیب به مفاهیم ارتباطات داده و شبکه، هک، قوانین سایبری، جزئیات مربوط به بدافزارها، مبانی رمزنگاری، شبکه‌های بی‌سیم و چالش‌های امنیتی آن‌ها، امنیت ابری، امنیت در جهان دیجیتال و روندهای نوظهور در امنیت سایبری می‌پردازد. بنابراین، فراگیران با تمام جنبه‌های کلیدی امنیت سایبری آشنا خواهند شد. توضیحات فصل‌ها به شرح زیر است:

◄ فصل ۱: مبانی ارتباطات داده و شبکه

این فصل به‌طور جامع اصول پایه‌ای لازم برای درک سیستم‌های ارتباطی مدرن را بررسی می‌کند. با ارائه یک دید کلی اولیه آغاز می‌شود و سپس به بررسی دقیق مفاهیم ارتباطات داده و شبکه می‌پردازد. مدل‌های مرجع شبکه، از جمله مدل‌های OSI و TCP/IP مورد مقایسه و تحلیل قرار می‌گیرند و نقش آن‌ها در برقراری ارتباطات بدون اختلال تشریح می‌شود.

این فصل همچنین به بررسی پروتکل‌های بنیادینی نظیر هندشیک سه‌مرحله‌ای و فلگ‌های TCP پرداخته و اهمیت آن‌ها در تضمین انتقال مطمئن داده‌ها را برجسته می‌سازد. مفاهیم ترجمه آدرس شبکه (NAT) نیز مورد بررسی قرار می‌گیرند تا درکی از نقش آن در مدیریت شبکه‌ها ارائه شود. سپس به تدریج به حوزه مهم امنیت اطلاعات وارد شده، اهداف اصلی آن نظیر محرمانگی، یکپارچگی و دسترس‌پذیری را تبیین می‌کند. افزون بر این، مفاهیم پایه رمزنگاری و نهان‌نگاری نیز معرفی می‌شوند تا پایه‌ای برای درک نقش این علوم در حفظ امنیت اطلاعات در محیط‌های شبکه‌ای فراهم گردد.

◄ فصل ۲: رمزگشایی هک

این فصل به بررسی انواع مختلف هک و هکرها می‌پردازد و چشم‌اندازی دقیق از فضای پیچیده جرائم سایبری و انواع آن، همچنین تفاوت‌های اساسی میان حملات غیرفعال و فعال امنیتی ارائه می‌دهد. مفاهیم کلیدی نظیر تهدید، آسیب‌پذیری، هدف ارزیابی، حمله و بهره‌برداری به‌تفصیل شرح داده می‌شوند و پایه‌ای قوی برای درک خوانندگان از فضای امنیت سایبری ایجاد می‌گردد.

تأکید فصل بر جنبه‌های اخلاقی هک نیز، درک متعهدانه‌ای از این حوزه پویا و در حال تحول فراهم می‌آورد و آن را به منبعی ارزشمند برای کسانی که به دنبال نگاهی دقیق و متوازن به مسئله هک هستند، تبدیل می‌سازد.

◄ فصل ۳: حقوق سایبری

این فصل به بررسی ابعاد قانونی فعالیت‌های سایبری می‌پردازد. مباحثی کلیدی همچون قوانین سایبری، جرایمی نظیر هک، سرقت داده، جعل هویت، فریب از جعل ایمیل، ارسال پیام‌های توهین‌آمیز، تماشاگری جنسی و تروریسم سایبری پوشش داده می‌شوند. بحث کاملی در خصوص مجازات‌های قانونی این جرائم در هند ارائه شده و درکی عمیق از عواقب قانونی آن‌ها به خوانندگان منتقل می‌شود.

خوانندگان با ماهیت در حال تحول تهدیدات سایبری، ساختارهای قانون‌گذاری جهت مقابله با آن‌ها و اهمیت بازدارندگی قانونی در عصر دیجیتال آشنا می‌شوند. این فصل منبعی حیاتی برای افرادی است که قصد دارند به‌درستی در فضای پیچیده حقوق سایبری حرکت کرده و پیامدهای قانونی هر نوع فعالیت سایبری را درک کنند.

◄ فصل ۴: بدافزار

این فصل دیدگاهی جامع در خصوص نرم‌افزارهای مخرب و تهدیدات مرتبط با آن‌ها ارائه می‌دهد و دانش لازم برای محافظت در برابر حملات سایبری را در اختیار خوانندگان قرار می‌دهد. انواع مختلف بدافزار از جمله ویروس‌ها، کرم‌ها، تروجان‌ها، جاسوس‌افزارها، تبلیغ‌افزارها و باج‌افزارها معرفی شده و ویژگی‌ها و شیوه عملکرد هریک به‌تفصیل بیان می‌گردد.

همچنین دسته‌بندی ویروس‌های رایانه‌ای شامل ویروس‌های فایل، ویروس‌های بوت سکتور و ویروس‌های ماکرو شرح داده شده‌اند. علائم حملات بدافزاری و نرم‌افزارهای آنتی‌ویروس معروف و روش‌های شناسایی آن‌ها (امضامحور، مبتنی‌بر تحلیل رفتار یا مبتنی‌بر فضای ابری) نیز مورد بررسی قرار می‌گیرند.

افزون بر این، ابزارهایی نظیر VirusTotal جهت تحلیل بدافزار، حملات DOS وDDOS ، سیستم‌های تشخیص نفوذ (IDS) و پیشگیری از نفوذ(IPS) ، کی‌لاگرها، فایروال‌ها و تهدیدات مرتبط با BOT و BOTNET توضیح داده می‌شوند. تهدیدات مبتنی‌بر وب نظیر تزریق اسکریپت از طریق سایت(XSS) ، تزریق SQL و حملات فیشینگ نیز پوشش داده شده‌اند تا مخاطبان را برای دفاع مؤثر در برابر تهدیدات در حال تحول دیجیتال توانمند سازند.

◄ فصل ۵: دنیای رمزنگاری

در این فصل، خوانندگان با دنیای جذاب رمزنگاری و روش‌های محافظت از ارتباطات دیجیتال آشنا می‌شوند. فصل با معرفی اصول پایه رمزنگاری آغاز شده و سپس به بررسی دقیق رمزنگاری متقارن (با کلید مشترک) و نامتقارن (با جفت کلید عمومی/خصوصی) می‌پردازد. نقش توابع هش در حفظ یکپارچگی داده و امضای دیجیتال برای تأیید صحت و اصالت پیام‌ها نیز به‌طور جامع تحلیل می‌شوند.

پروتکل‌های رمزنگاری و روش‌های تحلیل رمز نیز مورد بررسی قرار گرفته‌اند. با ارائه توضیحات شفاف و مثال‌های عملی، فصل خوانندگان را به درک جامعی از مکانیزم‌های پیچیده سیستم‌های رمزنگاری مدرن می‌رساند و توانایی لازم برای استفاده از این ابزارها جهت حفظ امنیت اطلاعات حساس در دنیای به‌هم‌پیوسته امروزی را در اختیارشان قرار می‌دهد.

◄ فصل ۶: شبکه‌های بی‌سیم و چالش‌های امنیتی آن‌ها

این فصل نگاهی جامع به پیچیدگی‌های شبکه‌های بی‌سیم در عصر دیجیتال دارد. مفاهیم پایه مانند پروتکل‌های رمزگذاری Wi-Fi و آسیب‌پذیری‌های رایج در سیستم‌های بی‌سیم معرفی می‌شوند. با تحلیل‌های دقیق، فصل به بررسی بهترین راهکارها برای ایمن‌سازی مؤثر اتصالات بی‌سیم می‌پردازد تا خوانندگان را در مقابله با تهدیدات احتمالی و محافظت از شبکه در برابر نفوذ و سرقت داده توانمند سازد.

درک عمیق از امنیتWi-Fi ، استفاده از مکانیزم‌های رمزنگاری قوی و تأکید بر اقدامات پیشگیرانه و رویکردهای راهبردی از دیگر مباحث این فصل است که موجب می‌شود خوانندگان بتوانند در محیطی امن‌تر و مقاوم‌تر در برابر تهدیدات سایبری، به فعالیت خود ادامه دهند.

◄ فصل ۷: امنیت رایانش ابری

در این فصل، امنیت در فضای رایانش ابری به‌طور کامل بررسی می‌شود. فصل با معرفی مفاهیم پایه‌ای رایانش ابری، مدل‌های پیاده‌سازی (ابر عمومی، خصوصی، ترکیبی) و مدل‌های خدماتیIaaS ، PaaS، SaaSآغاز می‌شود. سپس به بررسی تهدیدات و ریسک‌های رایج در محیط‌های ابری مانند نفوذ به داده‌ها و دسترسی‌های غیرمجاز پرداخته می‌شود.

راهکارهای حفظ امنیت و حریم خصوصی داده‌ها، مدیریت هویت و دسترسی(IAM) ، و الزامات رعایت استانداردها، الزامات قانونی و چارچوب‌های حاکمیتی نیز در این فصل بررسی شده‌اند. در پایان، ابزارها و فناوری‌های متنوعی را معرفی می‌کند که می‌توانند در کاهش ریسک‌های امنیتی در محیط‌های ابری به‌کار روند.

◄ فصل ۸: امنیت در دنیای دیجیتال

این فصل به‌عنوان راهنمایی جامع برای محافظت فردی در فضای دیجیتال عمل می‌کند. اهمیت رمزهای عبور در محافظت از حساب‌های آنلاین تبیین شده و انواع رمزها از جمله رمزهای زیستی، تصویری مبتنی‌بر الگو و روش‌های ساخت رمز قوی تحلیل می‌شوند. همچنین به انواع حملات مبتنی‌بر رمز عبور و روش‌های مقابله با آن‌ها پرداخته شده است.

استراتژی‌هایی نظیر رمزگذاری داده‌های حساس، استفاده از بسته‌های نرم‌افزاری امنیتی، پیکربندی فایروال‌ها و به‌روزرسانی منظم سیستم‌عامل برای برطرف‌سازی آسیب‌پذیری‌ها نیز از دیگر نکات کاربردی این فصل است. با اجرای این اقدامات، خوانندگان می‌توانند با اطمینان بیشتری در فضای دیجیتال فعالیت نمایند.

◄ فصل ۹: روندهای نوظهور و موضوعات پیشرفته در امنیت سایبری

در این فصل، موضوعات حیاتی همچون امنیت ابری و مجازی‌سازی در عصر رایانش ابری بررسی می‌شود. چالش‌های امنیتی اینترنت اشیا (IoT) به‌دلیل رشد فزاینده دستگاه‌های متصل، از دیگر موضوعات محوری این فصل است. نقش یادگیری ماشین و هوش مصنوعی در ارتقاء توانایی شناسایی تهدیدات و پاسخ‌گویی به آن‌ها نیز مورد تحلیل قرار گرفته است.

فصل همچنین به بررسی فناوری بلاک‌چین در امنیت سایبری می‌پردازد و ماهیت غیرمتمرکز و تغییرناپذیر آن را به‌عنوان راهکاری نوآورانه در حفظ امنیت تراکنش‌ها و هویت‌های دیجیتال معرفی می‌کند. با ارائه پوشش جامع این موضوعات، خوانندگان درک عمیقی از چشم‌انداز در حال تحول امنیت سایبری و راهبردهای پیشرفته لازم برای مقابله با تهدیدات نوظهور به‌دست می‌آورند.

سخن مترجم

در عصری که مرزهای زندگی دیجیتال و فیزیکی به‌گونه‌ای بی‌سابقه درهم‌تنیده شده، امنیت سایبری از حاشیه به متن حیات فردی و جمعی ما کوچ کرده و به ضرورتی اجتناب‌ناپذیر بدل گشته است. ترجمه کتاب ارزشمند «امنیت سایبری امروز» اثر دیپروپا پالیت را فرصتی مغتنم می‌دانم تا گامی هرچند کوچک در مسیر ارتقای دانش و حساسیت جامعه فارسی‌زبان نسبت به این عرصه حیاتی بردارم. انتخاب این کتاب نه تصادفی که پاسخی آگاهانه به خلاء منابع آموزشی جامع، به‌روز و قابل‌هضم به زبان فارسی بود؛ منابعی که بتوانند از مفاهیم بنیادین شبکه و داده‌ها آغاز کنند و خواننده را تا پیچیده‌ترین مباحث هک اخلاقی، حقوق سایبری، رمزنگاری، امنیت ابری و روندهای نوظهور مانند اینترنت اشیا و هوش مصنوعی همراهی نمایند.

ساختار منسجم و گام‌به‌گام کتاب، نقطه قوت ممتاز آن است. کتاب با تشریح اصول ارتباطات داده و شبکه‌ها (فصل ۱) پایه‌ای مستحکم می‌سازد، سپس وارد عرصه پرهیاهو اما ضروری هک و انواع آن (فصل ۲) و پیامدهای قانونی فعالیت‌های سایبری (فصل ۳) می‌شود. فصل‌های میانی با تمرکز بر شناخت عمیق بدافزارها و تهدیدات مرتبط (فصل ۴) و کالبدشکافی دنیای پیچیده رمزنگاری (فصل ۵)، خواننده را برای درک چالش‌های امنیت در شبکه‌های بی‌سیم (فصل ۶) و محیط‌های رایانش ابری (فصل ۷) آماده می‌کند. کتاب با ارائه راهکارهای ملموس برای امنیت فردی در دنیای دیجیتال (فصل ۸) و نگاهی آینده‌نگرانه به روندهای نوظهور و پیشرفته (فصل ۹) به پایان می‌رسد. این سیر منطقی نه‌تنها درک جامعی از اکوسیستم امنیت سایبری ارائه می‌دهد، بلکه کاربردی بودن را سرلوحه قرار داده است: از تحلیل مکانیزم‌های حملات رایج مانند XSS، تزریق SQL، فیشینگ و DDoS و راه‌های مقابله با آنها، تا معرفی ابزارهای عملیاتی مانند VirusTotal و سیستم‌های IDS/IPS، و ارائه دستورالعمل‌های شفاف برای ایمن‌سازی شبکه‌های وای‌فای، محیط‌های ابری و دستگاه‌های شخصی.

فرآیند ترجمه این اثر فنی، خود سفری چالش‌برانگیز بود. یافتن معادل‌های دقیق و پذیرفته‌شده برای انبوهی از اصطلاحات تخصصی نیازمند مشورت با منابع معتبر و متخصصان حوزه بود. حفظ تعادل ظریف میان روانی بیان برای مخاطب غیرمتخصص و دقت فنی مورد انتظار خواننده حرفه‌ای، همواره مدنظر قرار داشت. همچنین، بومی‌سازی برخی مثال‌ها، به‌ویژه در فصل حقوق سایبری که به قوانین خاص هند اشاره داشت، برای ارتباط بیشتر با مخاطب ایرانی ضروری بود. امیدوارم حاصل این تلاش، متنی باشد که هم دقت علمی را رعایت کرده و هم برای طیف گسترده‌ای از خوانندگان فارسی‌زبان — از دانشجویان و متخصصان فناوری اطلاعات و امنیت که به دنبال مرور اصول یا آشنایی با حوزه‌های جدید هستند، تا مدیران سازمان‌ها که نیازمند درک ریسک‌های سایبری و الزامات حفاظتی‌اند، و حتی کاربران عادی که خواهان مهارت‌های محافظت از حریم خصوصی و داده‌های خود در فضای آنلاین می‌باشند — قابل‌استفاده و الهام‌بخش باشد.

در نهایت، عمیقاً امیدوارم این ترجمه سهمی هرچند اندک در توانمندسازی دیجیتال جامعه، افزایش تاب‌آوری در برابر تهدیدات، و نهایتاً کمک به شکل‌گیری فضای سایبری امن‌تر و قابل‌اعتمادتر برای تمامی فارسی‌زبانان داشته باشد. در این مسیر پرپیچ‌وخم، دانش نورافکنی است که راه را روشن می‌کند، و کتاب حاضر تلاشی است برای فراهم آوردن این نور. سپاس فراوان از ناشر گرامی که امکان عرضه این گنجینه دانش به جامعه فارسی‌زبان را فراهم ساخت.

با احترام،

شهروز ستوده