

بسمه تعالی

اصول و مفاهیم پایه‌ای امنیت سایبری

www.ketab.ir

تألیف:

حسن غفاری یوشانلوئی



چاپ ۱۴۰۳

پیشگفتار

رَبِّ اشْرَحْ لِي صَدْرِي وَيَسِّرْ لِي أَمْرِي وَاحْلُلْ عُقْدَةً مِنْ لِسَانِي يَفْقَهُوا قَوْلِي

پروردگارا سینه‌ام را گشاده دار، و کار را بر من آسان کن،
گره از زبانم بگشای تا سخنم را درک کنند.

با گسترش روزافزون فناوری و استفاده بیشتر از اینترنت در تمامی جوانب زندگی، امنیت سایبری به یکی از مهم‌ترین مسائل مورد توجه تبدیل شده است. اطلاعات حساس، ارتباطات شخصی، سیستم‌های مرتبط با حیاتی مانند بانکداری و بهداشت، همه اینها در معرض تهدیدات مختلفی قرار دارند که بدون امنیت سایبری، ممکن است منجر به خسارات جدی و حتی فاجعه‌باری شوند.

در این کتاب قصد داریم به بررسی اصول پایه امنیت سایبری بپردازیم. این اصول که اساس مبارزه با تهدیدات سایبری را تشکیل می‌دهند، شامل مفاهیم مهمی مانند صحت اطلاعات، دسترسی‌پذیری، تمامیت، و حفاظت از حریم خصوصی می‌باشد. با شناخت این اصول، می‌توانید بهترین راهکارها را برای محافظت از خود و داده‌هایتان در مقابل تهدیدات اینترنتی اتخاذ کنید.

با بررسی روش‌های عملی برای اجرای این اصول، شامل استفاده از فناوری‌های امنیتی مانند فایروال، آنتی‌ویروس، رمزنگاری، و همچنین ایجاد سیاست‌ها و

روش‌های مناسب باعث مدیریت امنیت می‌شود. علاوه بر این، باید به آموزش و آگاهی افراد پرداخت تا هر فرد بتواند خودش را در مقابل تهدیدات امنیتی محافظت کند. ارتقاء فرهنگ امنیتی و ایجاد هوش فنی و رفتاری در کاربران از جمله اقدامات مهمی است که باید انجام شود.

در نهایت، امنیت سایبری یک فرایند مداوم و پویا است که نیاز به تلاش مداوم و به‌روزرسانی دارد. با توجه به پیشرفت روزافزون فناوری و تغییرات در تهدیدات امنیتی، این اصول نیاز به بازبینی و به‌روزرسانی دائمی دارند تا بتوانیم در برابر تهدیدات جدید مقاومت کنیم و امنیت اطلاعات خود را تضمین کنیم.

با احترام

غفاری یوشانلوئی

مقدمه

با پیشرفت و گسترش بی حد و مرز فناوری‌های جدید در جوامع کنونی، فناوری اطلاعات در تمامی ابعاد زندگی و بهره‌گیری از آن در جهت خلق رفاه و زندگی اجتماعی مناسب، شاهد گسترش و توسعه‌ی دنیای مجازی در زندگی هستیم. از یک طرف گسترش شبکه‌های اطلاعاتی و دنیای مجازی به رفاه، آسایش و انجام کارها با سرعت و دقت بیشتر کمک می‌کند، از طرف دیگر چالش‌ها و موانعی نیز در به کارگیری فناوری اطلاعات و شبکه‌های اطلاعاتی رخ می‌دهد که یکی از مقوله‌ها امنیت فناوری اطلاعات یا امن بودن فضای تبادل اطلاعات است.

در دنیای امروزی که تکنولوژی و اینترنت به عنوان یکی از ابزارهای اصلی زندگی ما درآمده‌اند، امنیت سایبری به یکی از مسائل حیاتی و اساسی تبدیل شده است. هر روز شاهد حملات سایبری جدیدی هستیم که می‌توانند به فرد، سازمان یا حتی کل جوامع آسیب برسانند. برای مقابله با این تهدیدات، شناخت اصول پایه امنیت سایبری اساسی است. با پیشرفت و گسترش بی حد و مرز فناوری‌های جدید در جوامع کنونی، فناوری اطلاعات در تمامی ابعاد زندگی و بهره‌گیری از آن در جهت خلق رفاه و زندگی اجتماعی مناسب، شاهد گسترش و توسعه‌ی دنیای

مجازی در زندگی هستیم. از یک طرف گسترش شبکه‌های اطلاعاتی و دنیای مجازی به رفاه، آسایش و انجام کارها با سرعت و دقت بیشتر کمک می‌کند، از طرف دیگر چالش‌ها و موانعی نیز در به کارگیری فناوری اطلاعات و شبکه‌های اطلاعاتی رخ می‌دهد که یکی از مقوله‌ها امنیت فناوری اطلاعات یا امن بودن فضای تبادل اطلاعات است.

امیدواریم که این کتاب به شما کمک کند تا درک بهتری از امنیت سایبری پیدا کنید و بتوانید بهترین راهکارها را برای حفاظت از خود و اطلاعاتتان در مقابل تهدیدات اتخاذ کنید.

فهرست مطالب

فصل اول

۱۲	امنیت فناوری اطلاعات
۱۳	مقدمه ای از امنیت اطلاعات
۱۵	امنیت اطلاعات
۱۵	اهمیت امنیت در ارتباطات
۱۷	انواع تهدیدات
۱۸	مفاهیم اولیه
۱۹	امنیت اطلاعات در اینترنت

فصل دوم

۲۱	سیاستگذاری و استانداردسازی
۲۲	تجزیه و تحلیل خطرات سایبری در سازمان یا سیستم
۲۳	تدوین سیاستها و خدمات امنیت سایبری
۲۵	تعیین مکانیسمهای امنیتی
۲۶	لایه ها و سرویسهای امنیت سایبری

استانداردهای مدیریت امنیت سایبری ۳۰

فصل سوم

بررسی برخی از حملات سایبری ۳۹

تعریف حملات سایبری ۴۰

وظایف سرویس دهنده ۴۲

بررسی حملات شناسایی شده ۴۳

فصل چهارم

بررسی انواع کنترل دسترسی ۱۰۵

حفاظت از اطلاعات ۱۰۶

تکنیک‌های کنترل دسترسی ۱۰۸

تکنیک‌های احراز هویت ۱۱۵

روش‌های پیاده‌سازی احراز هویت ۱۲۰

تکنیک‌های کاربردی برای مقابله با حملات علیه سیستم کنترل دسترسی ۱۲۲

سرویس‌های اصلی کشف نفوذ ۱۲۳

نحوه‌ی شناسایی فعالیت‌های غیر مجاز ۱۲۵

فصل پنجم

آشنایی با رمزنگاری ۱۲۷

بررسی قسمت دیگری از امنیت سایبری ۱۲۸

تاریخچه رمزنگاری ۱۳۱

مفاهیم پایه ای رمزنگاری ۱۳۲

بررسی حملات به سیستم‌های رمزنگاری ۱۳۴

انواع الگوریتم‌های رمزنگاری ۱۳۶

الگوریتم‌های منتشر شده ۱۳۸

سرویس محرمانگی با بهره‌گیری از الگوریتم‌های نامتقارن ۱۵۰

سرویس احراز هویت با بهره‌گیری از الگوریتم‌های نامتقارن ۱۵۱

توابع درهم ریزی ۱۵۴

اجزاء زیرساخت کلید عمومی ۱۵۵

فصل شش

سیستم‌های تشخیص نفوذ ۱۵۹

سیستم‌های IDS/IPS ۱۶۰

پیاده‌سازی سیستم تشخیص نفوذ IDS ۱۶۱

پیاده‌سازی سیستم تشخیص نفوذ IPS ۱۶۳

۱۶۵	شباهت ها و تفاوت های IDS/IPS
۱۶۸	استفاده همزمان از IDS/IPS
۱۶۹	مشکلات و ایرادات IDS/IPS
۱۷۱	روش های تشخیص تهدید با IDS/IPS
۱۷۲	مدل جامع امنیتی

منابع

www.ketab.ir